https://t.me/learningnets

Contents

The data, insights, and events in this report are from July 2021 through June 2022 (Microsoft fiscal year 2022), unless otherwise noted.

For the best experience viewing and navigating this report, we recommend using Adobe Reader, available as a free download from the Adobe website.

Report Introduction 02

The State of Cybercrime 06

An overview of The State of Cybercrime 07
Introduction 08
Ransomware and extortion: A nation-level threat 09
Ransomware insights from front-line responders 14
Cybercrime as a service 18
The evolving phishing threat landscape 21
A timeline of botnet disruption from Microsoft's early days of collaboration 25
Cybercriminal abuse of infrastructure 26
Is hacktivism here to stay? 28

Nation State Threats 30

An overview of Nation State Threats 31
Introduction 32
Background on nation state data 33
Sample of nation state actors and their activities 34
The evolving threat landscape 35
The IT supply chain as a gateway to the digital ecosystem 37
Rapid vulnerability exploitation 39
Russian state actors' wartime cyber tactics threaten Ukraine and beyond 41
China expanding global targeting for competitive advantage 44
Iran growing increasingly aggressive following power transition 46
North Korean cyber capabilities employed to achieve regime's three main goals 49
Cyber mercenaries threaten the stability of cyberspace 52
Operationalizing cybersecurity norms for peace and security in cyberspace 53

Devices and Infrastructure 56

An overview of Devices and Infrastructure 57
Introduction 58
Governments acting to improve critical infrastructure security and resilience 59
IoT and OT exposed: Trends and attacks 62
Supply chain and firmware hacking 65
Spotlight on firmware vulnerabilities 66
Reconnaissance-based OT attacks 68

Cyber Influence Operations 71

An overview of Cyber Influence Operations 72
Introduction 73
Trends in cyber influence operations 74
Influence operations during the COVID-19 pandemic and Russia's invasion of Ukraine 76
Tracking the Russian Propaganda Index 78
Synthetic media 80
A holistic approach to protect against cyber influence operations 83

Cyber Resilience 86

An overview of Cyber Resilience 87
Introduction 88
Cyber resiliency: A crucial foundation of a connected society 89
The importance of modernizing systems and architecture 90
Basic security posture is a determining factor in advanced solution effectiveness 92
Maintaining identity health is fundamental to organizational well-being 93
Operating system default security settings 96
Software supply chain centrality 97
Building resilience to emerging DDoS, web application, and network attacks 98
Developing a balanced approach to data security and cyber resiliency 101
Resilience to cyber influence operations: The human dimension 102
Fortifying the human factor with skilling 103
Insights from our ransomware elimination program 104
Act now on quantum security implications 105
Integrating business, security, and IT for greater resilience 106
The cyber resilience bell curve 108

Contributing Teams 110

https://t.me/learningnets

Introduction by Tom Burt

Corporate Vice President, Customer Security & Trust

"The trillions of signals we analyze from our worldwide ecosystem of products and services reveal the ferocity, scope, and scale of digital threats across the globe"

A snapshot of our landscape...

Scope and scale of threat landscape

The volume of password attacks has risen to an estimated 921 attacks every second – a 74% increase in just one year.

Dismantling cybercrime

To date, Microsoft removed more than 10,000 domains used by cybercriminals and 600 used by nation state actors.

Addressing vulnerabilities

93% of our ransomware incident response engagements revealed insufficient controls on privilege access and lateral movement.

On February 23, 2022, the cybersecurity world entered a new age, the age of the hybrid war. On that day, hours before missiles were launched and tanks rolled across borders, Russian actors launched a massive destructive cyberattack against Ukrainian government, technology, and financial sector targets. You can read more about these attacks and the lessons to be learned from them in the Nation State Threats chapter of this third annual edition of the Microsoft Digital Defense Report (MDDR). Key among those lessons is that the cloud provides the best physical and logical security against cyberattacks and enables advances in threat intelligence and end point protection that have proven their value in Ukraine.

While any survey of the year's developments in cybersecurity must begin there, this year's report provides a deep dive into much more. In the report's first chapter, we focus on activities of cybercriminals, followed by nation state threats in chapter two. Both groups have greatly increased the sophistication of their attacks which has dramatically increased the impact of their actions. While Russia drove headlines, Iranian actors escalated their attacks following a transition of presidential power, launching destructive attacks targeting Israel, and ransomware and hack-and-leak operations targeting critical infrastructure in the United States. China also increased its espionage efforts in Southeast Asia and elsewhere in the global south, seeking to counter US influence and steal critical data and information.

Foreign actors are also using highly effective techniques to enable propaganda influence operations in regions around the globe, as covered in the third chapter. For example, Russia has worked hard to convince its citizens, and the citizens of many other countries, that its invasion of Ukraine was justified – while also sowing propaganda discrediting COVID vaccines in the West and simultaneously promoting their effectiveness at home. In addition, actors are increasingly targeting Internet of Things (IoT) devices or Operational Technology (OT) control devices as entry points to networks and critical infrastructure which is discussed in chapter four. Finally, in the last chapter, we provide the insights and lessons we have learned from over the past year defending against attacks directed at Microsoft and our customers as we review the year's developments in cyber resilience.

Each chapter provides the key lessons learned and insights based on Microsoft's unique vantage point. The trillions of signals we analyze from our worldwide ecosystem of products and services reveal the ferocity, scope, and scale of digital threats across the globe. Microsoft is taking action to defend our customers and the digital ecosystem against these threats, and you can read about our technology that identifies and blocks billions of phishing attempts, identity thefts, and other threats to our customers.

https://t.me/learningnets

Introduction by Tom Burt

Continued

We also use legal and technical means to seize and shut down infrastructure used by cybercriminals and nation state actors and notify customers when they are being threatened or attacked by a nation state actor. We work to develop increasingly effective features and services that use AI/ML technology to identify and block cyber threats and security professionals defend against and identify cyber-intrusions more rapidly and effectively.

Perhaps most importantly, throughout the MDDR we offer our best advice on the steps individuals, organizations, and enterprises can take to defend against these increasing digital threats. Adopting good cyber hygiene practices is the best defense and can significantly reduce the risk of cyberattacks.

https://t.me/learningnets

The state of cybercrime

Cybercriminals continue to act as sophisticated profit enterprises. Attackers are adapting and finding new ways to implement their techniques, increasing the complexity of how and where they host campaign operation infrastructure. At the same time, cybercriminals are becoming more frugal. To lower their overhead and boost the appearance of legitimacy, attackers are compromising business networks and devices to host phishing campaigns, malware, or even use their computing power to mine cryptocurrency.

Find out more on p6

> "The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict."

Nation state threats

Nation state actors are launching increasingly sophisticated cyberattacks designed to evade detection and further their strategic priorities. The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict. Russia has also supported its war with information influence operations, using propaganda to impact opinions in Russia, Ukraine, and globally. Outside Ukraine, nation state actors have increased activity and have begun using advancements in automation, cloud infrastructure, and remote access technologies to attack a wider set of targets. Corporate IT supply chains that enable access to ultimate targets were frequently attacked. Cybersecurity hygiene became even more critical as actors rapidly exploited unpatched vulnerabilities, used both sophisticated and brute force techniques to steal credentials, and obfuscated their operations by using opensource or legitimate software. In addition, Iran joins Russia in the use of destructive cyberweapons, including ransomware, as a staple of their attacks.

These developments require urgent adoption of a consistent, global framework that prioritizes human rights and protects people from reckless state behavior online. All nations must work together to implement norms and rules for responsible state conduct.

Find out more on p30

Devices and infrastructure

The pandemic, coupled with rapid adoption of internet-facing devices of all kinds as a component of accelerating digital transformation, has greatly increased the attack surface of our digital world. As a result, cybercriminals and nation states are quickly taking advantage. While the security of IT hardware and software has strengthened in recent years, the security of IoT and OT devices security has not kept pace. Threat actors are exploiting these devices to establish access on networks and enable lateral movement, to establish a foothold in a supply chain, or to disrupt the target organization's OT operations.

Find out more on p56

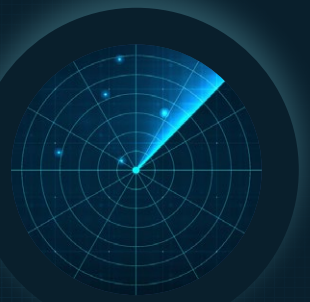
Introduction by Tom Burt

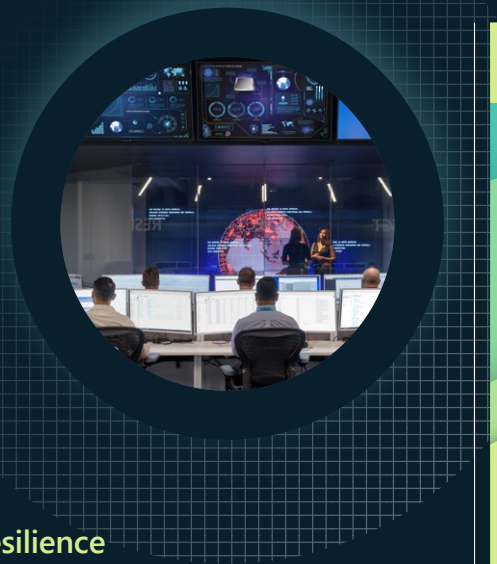
Continued

Cyber influence operations

Nation states are increasingly using sophisticated influence operations to distribute propaganda and impact public opinion both domestically and internationally. These campaigns erode trust, increase polarization, and threaten democratic processes. Skilled Advanced Persistent Manipulator actors are using traditional media together with internet and social media to vastly increase the scope, scale, and efficiency of their campaigns, and the outsized impact they are having in the global information ecosystem. In the past year, we have seen these operations used as part of Russia's hybrid war in Ukraine, but have also seen Russia and other nations, including China and Iran, increasingly deploy propaganda operations powered by social media to extend their global influence on a range of issues.

Find out more on p71





Cyber resilience

Security is a key enabler of technological success. Innovation and enhanced productivity can only be achieved by introducing security measures that make organizations as resilient as possible against modern attacks. The pandemic has challenged us at Microsoft to pivot our security practices and technologies to protect our employees wherever they work. This past year, threat actors continued to take advantage of vulnerabilities exposed during the pandemic and the shift to a hybrid work environment. Since then, our principal challenge has been managing the prevalence and complexity of various attack methods and increased nation state activity. In this chapter, we detail the challenges we have faced, and the defenses we have mobilized in response with our more than 15,000 partners.

Find out more on p86

Our unique vantage point

37bn
email threats blocked

34.7bn
identity threats blocked

43tn
signals synthesized daily, using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

8,500+
engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across 77 countries.

2.5bn
endpoint signals analyzed daily

15,000+
partners in our security ecosystem who increase cyber resilience for our customers.

July 1, 2021 through June 30, 2022

https://t.me/learningnets

Introduction by Tom Burt

Continued

We believe Microsoft—independently and through close partnerships with others in private industry, government, and civil society—has a responsibility to protect the digital systems that underpin the social fabric of our society and promote safe, secure computing environments for every person, wherever they are located. This responsibility is the reason we have published the MDDR each year since 2020. The report is the culmination of Microsoft's vast data and comprehensive research. It shares our unique insights on how the digital threat landscape is evolving and the crucial actions that can be taken today to improve the security of the ecosystem.

We hope to instill a sense of urgency, so readers take immediate action based on the data and insights we present both here and in our many cybersecurity publications throughout the year. As we consider the gravity of the threat to the digital landscape—and its translation into the physical world—it is important to remember that we are all empowered to take action to protect ourselves, our organizations, and enterprises against digital threats.

Thank you for taking the time to review this year's Microsoft Digital Defense Report. We hope you will find that it provides valuable insight and recommendations to help us collectively defend the digital ecosystem.

Tom Burt
Corporate Vice President,
Customer Security & Trust

Our objective with this report is twofold:

1. To illuminate the evolving digital threat landscape for our customers, partners, and stakeholders spanning the broader ecosystem, shining a light on both new cyberattacks and evolving trends in historically persistent threats.
2. To empower our customers and partners to improve their cyber resiliency and respond to these threats.

https://t.me/learningnets

The State of Cybercrime

As cyber defenses improve and more organizations are taking a proactive approach to prevention, attackers are adapting their techniques.

An overview of The State of Cybercrime 07
Introduction 08
Ransomware and extortion: A nation-level threat 09
Ransomware insights from front-line responders 14
Cybercrime as a service 18
The evolving phishing threat landscape 21
A timeline of botnet disruption from Microsoft's early days of collaboration 25
Cybercriminal abuse of infrastructure 26
Is hacktivism here to stay? 28

https://t.me/learningnets

An overview of

The State of Cybercrime

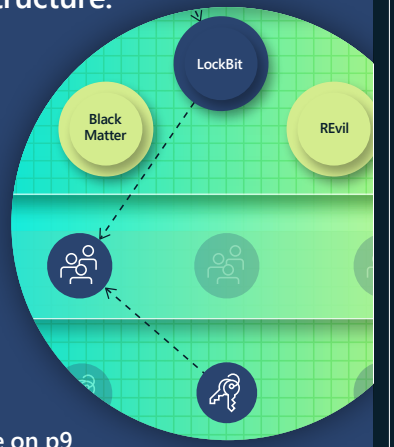
As cyber defenses improve and more organizations are taking a proactive approach to prevention, attackers are adapting their techniques.

Cybercriminals continue to act as sophisticated profit enterprises. Attackers are adapting and finding new ways to implement their techniques, increasing the complexity of how and where they host campaign operation infrastructure. At the same time, cybercriminals are becoming more frugal. To lower their overhead and boost the appearance of legitimacy, attackers are compromising business networks and devices to host phishing campaigns, malware, or even use their computing power to mine cryptocurrency.

Cybercrime continues to rise as the industrialization of the cybercrime economy lowers the skill barrier to entry by providing greater access to tools and infrastructure.

Find out more on p18

The threat of ransomware and extortion is becoming more audacious with attacks targeting governments, businesses, and critical infrastructure.

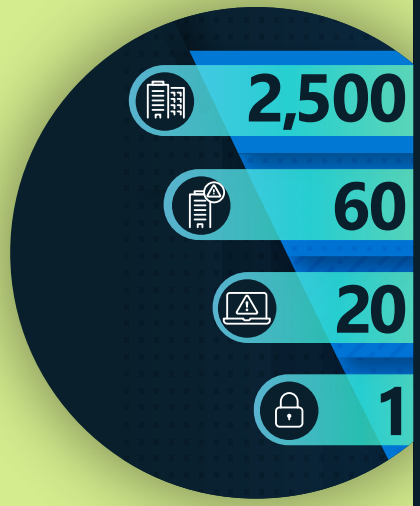


Find out more on p9

Attackers increasingly threaten to disclose sensitive data to encourage ransom payments.

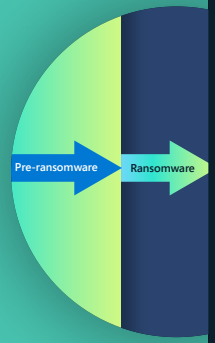
Find out more on p10

Human operated ransomware is most prevalent, as one-third of targets are successfully compromised by criminals using these attacks and 5% of those are ransomed.



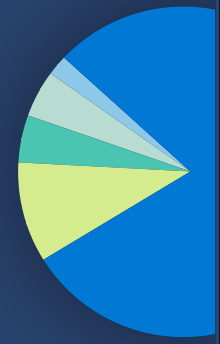
Find out more on p9

The most effective defense against ransomware includes multifactor authentication, frequent security patches, and Zero Trust principles across network architecture.



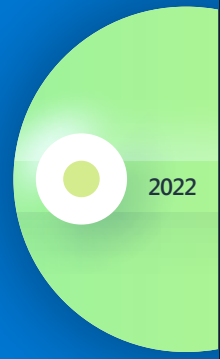
Find out more on p13

Credential phishing schemes which indiscriminately target all inboxes are on the rise and business email compromise, including invoice fraud, poses a significant cybercrime risk for enterprises.



Find out more on p21

To disrupt the malicious infrastructures of cybercriminals and nation state actors, Microsoft relies on innovative legal approaches and our public and private partnerships.



Find out more on p25

https://t.me/learningnets

Introduction

Cybercrime continues to rise, with increases in both random and targeted attacks.

As cyber defenses improve and more governments and businesses take a proactive approach to prevention, we see attackers using two strategies to gain access required to facilitate cybercrime. One approach is a campaign with broad targets that relies on volume. The other uses surveillance and more selective targeting to increase the rate of return. Even when revenue generation is not the objective—such as nation state activity for geopolitical purposes—both random and targeted attacks are used. This past year, cybercriminals continued to rely on social engineering and exploitation of topical issues to maximize the success of campaigns. For example, while COVID-themed phishing lures were used less frequently, we observed lures soliciting donations to support the citizens of Ukraine increasing.

Attackers are adapting and finding new ways to implement their techniques, increasing the complexity of how and where they host campaign operation infrastructure. We have observed cybercriminals becoming more frugal and attackers are no longer paying for technology. To lower their overhead and boost the appearance of legitimacy, some attackers increasingly seek to compromise businesses to host phishing campaigns, malware, or even use their computing power to mine cryptocurrency.

In this chapter, we also examine the rise in hacktivism, a disruption caused by private citizens conducting cyberattacks to further social or political goals. Thousands of individuals around the world, both experts and novices, have mobilized since February 2022 to launch attacks such as disabling websites and leaking stolen data as part of the Russia-Ukraine war. It is too soon to predict whether this trend will continue after the end of active hostilities.

Organizations must regularly review and strengthen access controls and implement security strategies to defend against cyberattacks. However, that is not all they can do. We explain how our Digital Crimes Unit (DCU) has used civil cases to seize malicious infrastructure used by cybercriminals and nation state actors. We must fight this threat together through both public and private partnerships. We hope that by sharing what we have learned over the past 10 years, we will help others understand and consider the proactive measures they can take to protect themselves and the wider ecosystem against the continually growing threat of cybercrime.

Amy Hogan-Burney
General Manager, Digital Crimes Unit

https://t.me/learningnets

Ransomware and extortion: A nation-level threat

Ransomware attacks pose an increased danger to all individuals as critical infrastructure, businesses of all sizes, and state and local governments are targeted by criminals leveraging a growing cybercriminal ecosystem.

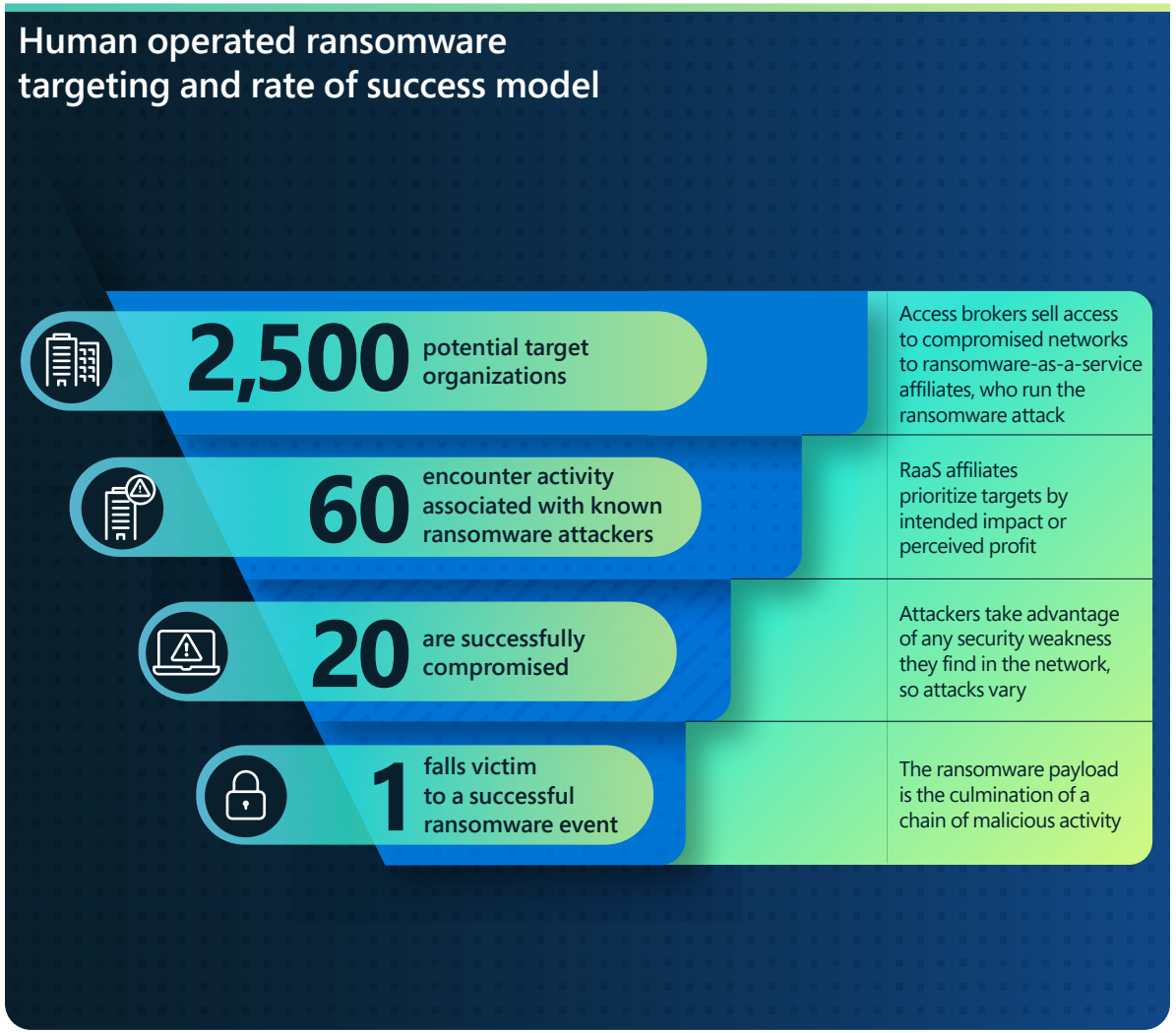
Over the past two years, high profile ransomware incidents—such as those involving critical infrastructure, healthcare, and IT service providers—have drawn considerable public attention. As ransomware attacks have become more audacious in scope, their effects have become more wide ranging. The following are examples of attacks we've seen already in 2022:

- In February, an attack on two companies affected the payment processing systems of hundreds of gas stations in northern Germany.[1]
- In March, an attack against Greece's postal service temporarily disrupted mail delivery and impacted the processing of financial transactions.[2]
- In late May, a ransomware attack against Costa Rican government agencies forced a national emergency to be declared after hospitals were shut down and customs and tax collection disrupted.[3]
- Also in May, an attack caused flight delays and cancellations for one of India's largest airlines, leaving hundreds of passengers stranded.[4]

The success of these attacks and the extent of their real-world impacts are the result of an industrialization of the cybercrime economy, enabling access to tooling and infrastructure and expanding cybercriminal capabilities by lowering their skill barrier to entry.

In recent years, ransomware has moved from a model where a single "gang" would both develop and distribute a ransomware payload to the ransomware as a service (RaaS) model. RaaS allows one group to manage the development of the ransomware payload and provide services for payment and extortion via data leakage to other cybercriminals—the ones who actually launch the ransomware attacks—referred to as "affiliates" for a cut of the profits. This franchising of the cybercrime economy has expanded the attacker pool. The industrialization of cybercriminal tooling has made it easier for attackers to perform intrusions, exfiltrate data, and deploy ransomware.

Human operated ransomware[5]—a term coined by Microsoft researchers to describe threats driven by humans who make decisions at every stage of the attacks based on what they discover in their target's network and delineate the threat from commodity ransomware attacks—remains a significant threat to organizations.



Model based on Microsoft Defender for Endpoint (EDR) data (January–June 2022).

https://t.me/learningnets

Ransomware and extortion: A nation-level threat

Continued

Ransomware attacks have become even more impactful as the adoption of a double extortion monetization strategy has become a standard practice. This involves exfiltrating data from compromised devices, encrypting the data on the devices, and then posting or threatening to post the stolen data publicly to pressure victims into paying a ransom.

Although most ransomware attackers opportunistically deploy ransomware to whatever network they get access, some purchase access from other cybercriminals, leveraging connections between access brokers and ransomware operators.

Our unique breadth of signal intelligence is gathered from multiple sources—identity, email, endpoints, and cloud—and provides insight into the growing ransomware economy, complete with an affiliate system which includes tools designed for less technically-abled attackers.

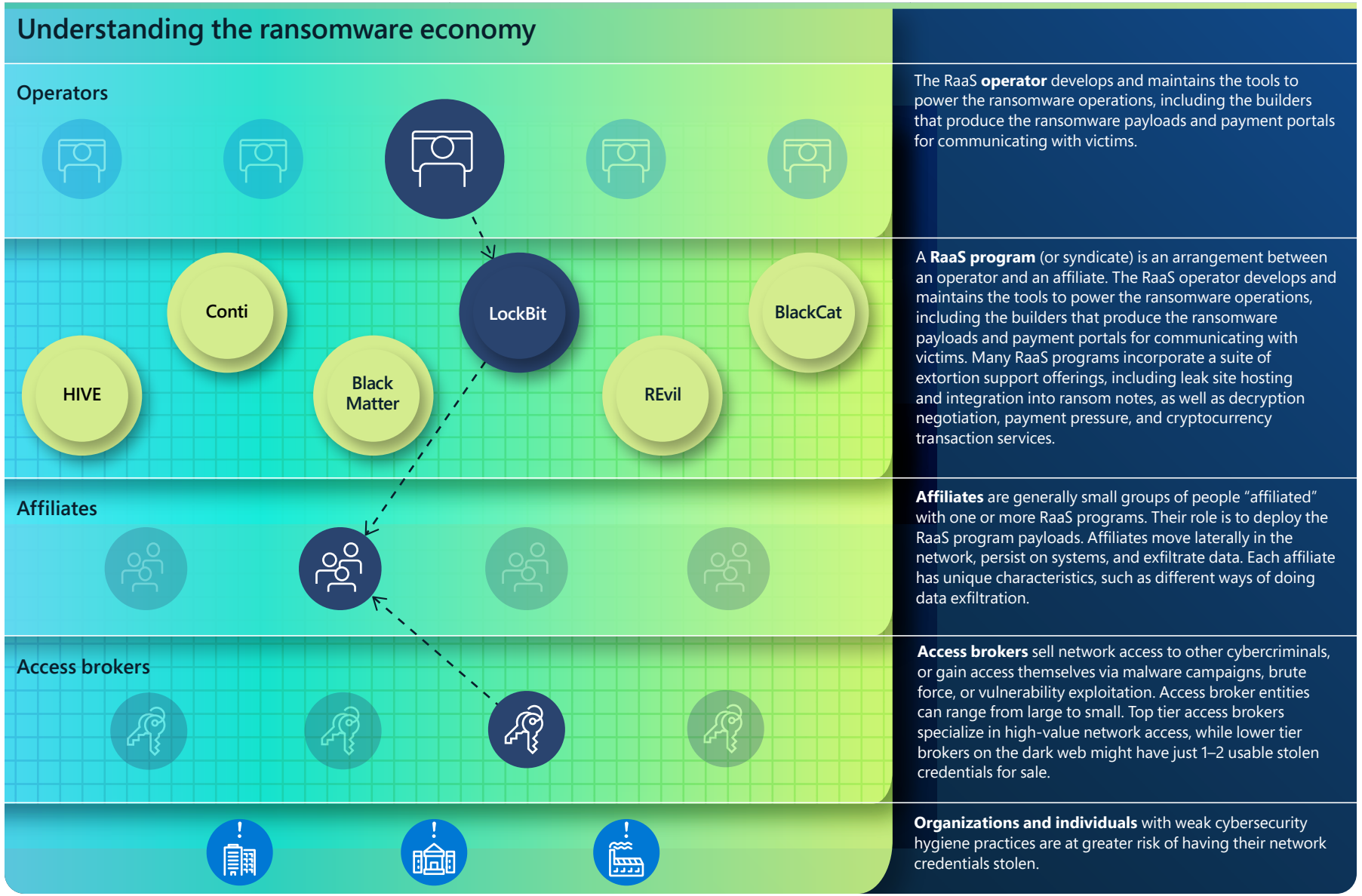
Expanding relationships between specialized cybercriminals have increased the pace, sophistication, and success of ransomware attacks. This has driven the evolution of the cybercriminal ecosystem into connected players with different techniques, goals, and skillsets that support each other on initial access to targets, payment services, and decryption or publication tools or sites.

Ransomware operators can now purchase access to organizations or government networks online or obtain credentials and access via interpersonal relationships with brokers whose main objective is solely to monetize the access they have gained.

The operators then use the purchased access to deploy a ransomware payload bought via dark web marketplaces or forums. In many cases, negotiations with victims are conducted by the RaaS team, not the operators themselves. These criminal transactions are seamless and the participants risk little chance of being arrested and charged due to the anonymity of the dark web and difficulty enforcing laws transnationally.

A sustainable and successful effort against this threat will require a whole-of-government strategy to be executed in close partnership with the private sector.

https://t.me/learningnets



Contrary to how ransomware is sometimes portrayed in the media, it is rare for a single ransomware variant to be managed by one end-to-end "ransomware gang." Instead, there are separate entities that build malware, gain access to victims, deploy ransomware, and handle extortion negotiations. The industrialization of the criminal ecosystem has led to:

- Access brokers that break in and hand off access (access as a service).
- Malware developers that sell tooling.
- Criminal operators and affiliates that conduct intrusions.
- Encryption and extortion service providers that take over monetization from affiliates (RaaS).

All human-operated ransomware campaigns share common dependencies on security weaknesses. Specifically, attackers usually take advantage of an organization's poor cyber hygiene, which often includes infrequent patching and failure to implement multifactor authentication (MFA).

https://t.me/learningnets

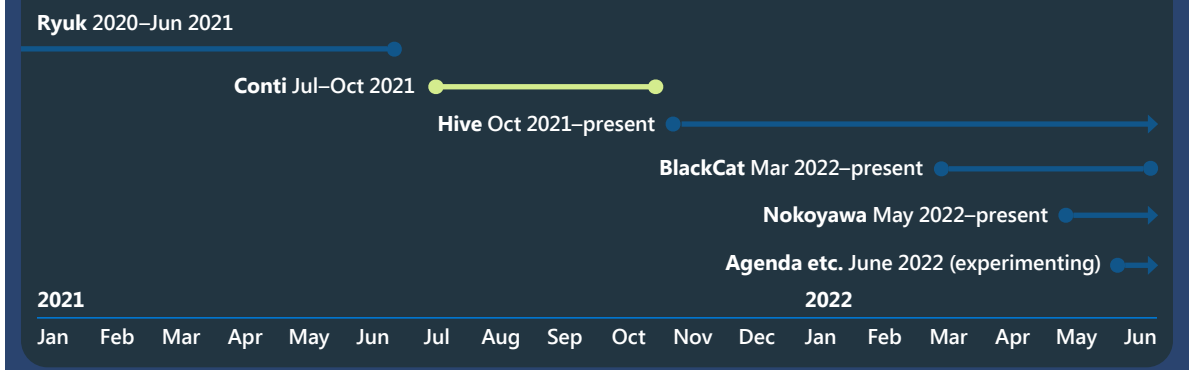
Case study: The dissolution of Conti

Conti, one of the top ransomware variants over the past two years, began shutting down operations in mid-2022, with the Microsoft Threat Intelligence Center (MSTIC) observing a significant decrease in activity in late March and early April. We observed the last Conti ransomware deployments in mid-April. However, much like the shuttering of other ransomware operations, Conti's dissolution did not have a significant impact on ransomware deployments, as MSTIC observed Conti affiliates pivoting to deploy other ransomware payloads, including BlackBasta, Lockbit 2.0, LockbitBlack, and HIVE. This is consistent with data from previous years and suggests that when ransomware gangs go offline, they re-emerge months later or redistribute their technical capabilities and resources to new groups.

Our Microsoft threat intelligence teams track ransomware threat actors as individual groups (labeled as DEVs) based on their specific tools, rather than tracking them by the malware they use. This meant that when Conti's affiliates dispersed, we were able to continue tracking these DEVs through their use of other tools or RaaS kits. For example:

- DEV-0230, which is affiliated with Trickbot, had been a prolific user of Conti. In late April, MSTIC observed it using QuantumLocker.
- DEV-0237 shifted from Conti's ransomware kit to HIVE and Nokoyawa, including using HIVE in the May 31 attack against Costa Rican government agencies.
- DEV-0506, another prolific user of the Conti ransomware kit, was observed using BlackBasta.

Example of an affiliate (DEV-0237) quickly shifting between RaaS programs



After a RaaS program such as Conti is shut down, the ransomware affiliate shifts to another one (Hive) almost immediately.

RaaS evolves the ransomware ecosystem and hinders attribution

Because human-operated ransomware is driven by individual operators, attack patterns vary based on the target and alternate throughout the duration of an attack. In the past, we observed a close relationship between the initial entry vector, tools, and ransomware payload choices in each campaign of a single ransomware strain. This made attribution easier. The RaaS affiliate model, however, decouples this relationship. As a result, Microsoft tracks ransomware affiliates deploying payloads in specific attacks, rather than tracking the ransomware payload developers as operators.

Put another way, we no longer assume the HIVE developer is the operator behind a HIVE ransomware attack; it is more likely to be an affiliate.

The cybersecurity industry has struggled to adequately capture this delineation between developers and operators. The industry still often reports a ransomware incident by its payload name, giving the false impression that a single entity, or ransomware gang, is behind all attacks using that particular ransomware payload, and all incidents associated with it share common techniques and infrastructure. To support network defenders, it is important to learn more about the stages that precede different affiliates' attacks—such as data exfiltration and additional persistence mechanisms—and the detection and protection opportunities that might exist.

More so than malware, attackers need credentials to succeed in their operations. The successful human operated ransomware infection of an entire organization relies on access to a highly privileged account.

https://t.me/learningnets

Spotlight on human-operated ransomware attacks

Over the past year, Microsoft's ransomware experts conducted deep investigations into more than 100 human-operated ransomware incidents to track attackers' techniques and understand how to better protect our customers.

It is important to note that the analysis we share here is possible only for onboarded, managed, devices. Non-onboarded, unmanaged devices represent the least secure part of an organization's hardware assets.

Most prevalent ransomware phase techniques:

75%
Use admin tools.

75%
Use acquired elevated compromised user account to spread malicious payloads through SMB protocol.

99%
Attempt to tamper with discovered security and backup products using OS-built tools.

https://t.me/learningnets

The typical human-operated attack

Human-operated ransomware attacks can be categorized into the pre-ransomware phase and the ransomware deployment phase. During the pre-ransomware phase, attackers prepare to infiltrate the network by learning about the organization's typology and security infrastructure.

Stop the attackers before they reach the ransomware deployment phase	Deployment!
Pre-ransomware	Ransomware
This phase can range from a few days to several weeks or months, although it has been shortening over the past two years.	This phase can last only minutes.
Attackers prepare to infiltrate the network by learning as much as possible about the topology and security infrastructure. Attackers may also exfiltrate data in this phase.	Attackers aim to encrypt as much data as possible.

Our investigations found most actors behind human-operated ransomware attacks take advantage of similar security weaknesses and share common attack patterns and techniques.

A durable security strategy

Combating and preventing attacks of this nature requires a shift in an organization's mindset to focus on the comprehensive protection required to slow and stop attackers before they can move from the pre-ransomware phase to the ransomware deployment phase.

Enterprises must apply security best practices consistently and aggressively to their networks, with the goal of mitigating classes of attacks. Due to the human decision making these ransomware attacks can generate multiple, seemingly disparate security product alerts which can easily get lost or not responded to in time. Alert fatigue is real, and security operations centers (SOCs) can make their lives easier by looking at trends in their alerts or grouping alerts into incidents so they can see the bigger picture. SOCs can then mitigate alerts using hardening capabilities like attack surface reduction rules. Hardening against common threats can not only reduce alert volume, but also stop many attackers before they get access to networks.

Organizations must maintain continuous high standards of security posture and network hygiene to protect themselves from human-operated ransomware attacks.

Actionable insights

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in disrupting the cybercriminal economy.

1. Build credential hygiene. More so than malware, attackers need credentials to succeed in their operations. The successful human-operated ransomware infection of an entire organization relies on access to a highly privileged account like a Domain Administrator, or abilities to edit a Group Policy.
2. Audit credential exposure.
3. Prioritize deployment of Active Directory updates.
4. Prioritize cloud hardening.
5. Reduce the attack surface.
6. Harden internet-facing assets and understand your perimeter.
7. Reduce SOC alert fatigue by hardening your network to reduce volume and preserve bandwidth for high priority incidents.

Links to further information

- RaaS: Understanding the cybercrime gig economy and how to protect yourself | Microsoft Security Blog
- Human-operated ransomware attacks: A preventable disaster | Microsoft Security Blog

Ransomware insights from front-line responders

Organizations worldwide experienced a steady growth in human-operated ransomware attacks beginning in 2019. However, law enforcement operations and geopolitical events in the last year had a significant impact on cybercriminal organizations.

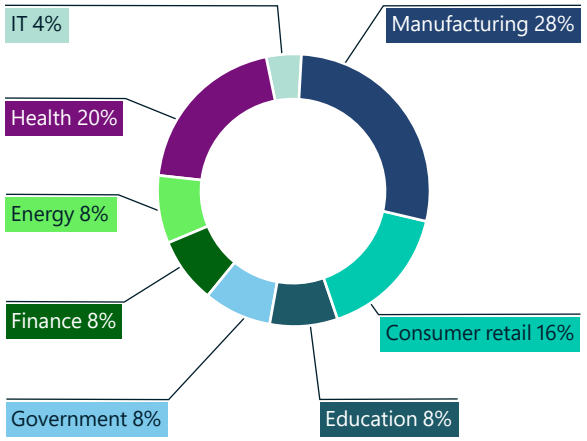
Microsoft's Security Service Line supports customers through an entire cyberattack, from investigation to successful containment and recovery activities. The response and recovery services are offered via two highly integrated teams, with one focusing on the investigation and groundwork for recovery and the second one on containment and recovery. This section presents a summary of findings based on ransomware engagements over the past year.

93%

of Microsoft investigations during ransomware recovery engagements revealed insufficient privilege access and lateral movement controls.

https://t.me/learningnets

Ransomware incident and recovery engagements by industry

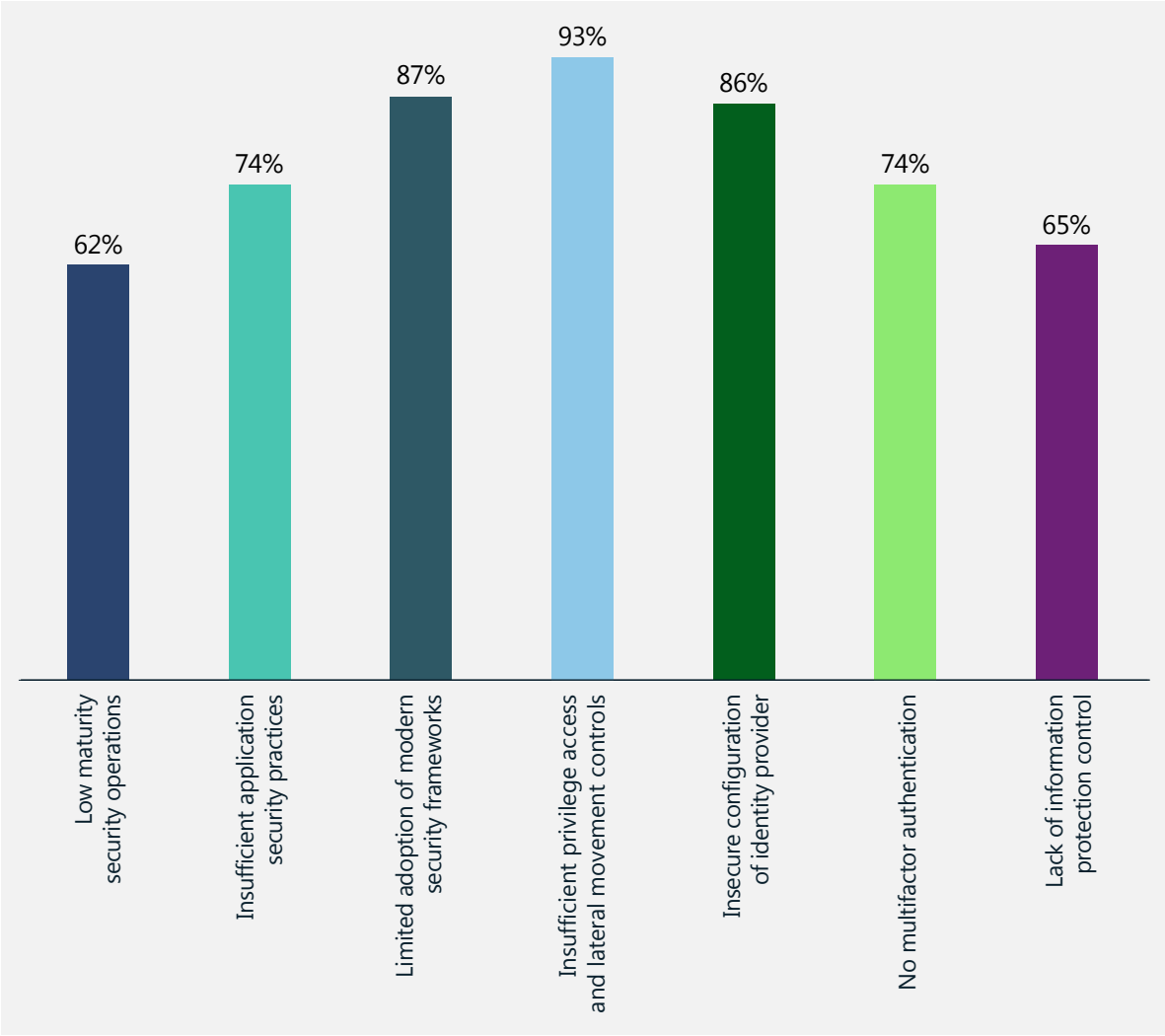


As new small groups and threats emerge, defending teams must be aware of evolving ransomware threats while protecting against previously unknown ransomware malware families. The rapid development approach used by criminal groups led to the creation of intelligent ransomware packaged in easy-to-use kits. This allows greater flexibility in launching widespread attacks on a higher number of targets.

The following pages provide a deeper look at the most commonly observed contributing factors to weak protection against ransomware, grouped into three categories of findings:

1. Weak identity controls
2. Ineffective security operations
3. Limited data protection

Summary of most common findings in ransomware response engagements



The most common finding among ransomware incident response engagements was insufficient privilege access and lateral movement controls.

Ransomware insights from front-line responders

Continued

The three main contributing factors seen in our onsite response engagements:

① **Weak identity controls:** Credential theft attacks remain one of the top contributing factors

② **Ineffective security operations** processes do not just present a window of opportunity for attackers but significantly impact the time to recover

③ Eventually it boils down to data—organizations struggle to implement an effective **data protection strategy** which aligns with their business needs

① Weak identity controls

Human-operated ransomware continues to evolve and employ credential theft and lateral movement methods traditionally associated with targeted attacks. Successful attacks are often the result of long-running campaigns involving compromise of identity systems, like Active Directory (AD), that allow human operators to steal credentials, access systems, and remain persistent in the network.

Active Directory (AD) and Azure AD security

88%

of impacted customers did not employ AD and Azure AD security best practices. This has become a common attack vector as attackers exploit misconfigurations and weaker security postures in critical identity systems to gain broader access and impact to businesses.

Least privilege access and use of Privileged Access Workstations (PAW)

None of the impacted organizations implemented proper administrative credential segregation and least privilege access principles via dedicated workstations during the management of their critical identity and high-value assets, such as proprietary systems and business-critical applications.

Privilege account security

88%

of engagements, MFA was not implemented for sensitive and high privileged accounts, leaving a security gap for attackers to compromise credentials and pivot further attacks using legitimate credentials.

84%

Administrators across 84 percent of organizations did not use privilege identity controls such as just-in-time access to prevent further nefarious use of compromised privileged credentials.

https://t.me/learningnets

Ransomware insights from front-line responders

Continued

② Ineffective security operations

Our data shows organizations which suffered ransomware attacks have significant gaps in their security operations, tooling, and information technology asset lifecycle management. Based on the available data, the following gaps were most observed:

Patching:

68%

of impacted organizations did not have an effective vulnerability and patch management process, and a high dependence on manual processes versus automated patching led to critical openings. Manufacturing and critical infrastructure continue to struggle with maintenance and patching of legacy operational technology (OT) systems.

Lack of security operations tooling:

Most organizations reported a lack of end-to-end security visibility due to a lack or misconfiguration of security tools, leading to a decrease in detect and response effectiveness.

60%

of organizations reported no use of an EDR[6] tool, a fundamental technology for detection and response.

60%

did not invest in security information and event management (SIEM) technology leading to monitoring silos, limited ability to detect end-to-end threats and inefficient security operations. Automation remains a key gap in SOC tooling and processes, forcing SOC staff to spend countless hours making sense of security telemetry.

84%

of impacted organizations did not enable integration of their multi-cloud environments into their security operations tooling.

Response and recovery processes:

76%

Lack of an effective response plan was a critical area observed in 76 percent of impacted organizations, preventing proper organizational crisis readiness and negatively impacting time to respond and recover.

③ Limited data protection

Many compromised organizations lacked proper data protection processes leading to a severe impact on recovery times and the capability to return to business operations. The most common gaps encountered include:

Immutable backup:

44%

of organizations did not have immutable backups for the impacted systems. Data also shows administrators did not have backups and recovery plans for critical assets such as AD.

Data loss prevention:

Attackers usually find their way to compromise systems via exploiting vulnerabilities in the organization, exfiltrating critical data for extortion, intellectual property theft, or monetization.

92%

of impacted organizations did not implement effective data loss prevention controls to mitigate these risks, leading to critical data loss.

https://t.me/learningnets

Ransomware declined in some regions and increased in others

This year we observed a drop in the overall number of ransomware cases reported to our response teams in North America and Europe compared to the previous year. At the same time, cases reported in Latin America increased.

One interpretation of this observation is cybercriminals pivoted away from areas perceived to have a higher risk of triggering law enforcement scrutiny in favor of softer targets. Since Microsoft did not observe a substantial improvement in enterprise network security worldwide to explain the decrease in ransomware-related support calls, we believe the most likely cause is a combination of law enforcement activity in 2021 and 2022 which increased the cost of criminal activity, along with some geopolitical events of 2022.

One of the most prevalent RaaS operations belongs to a Russian-speaking criminal group known as REvil (also known as Sodinokibi) that has been active since 2019. In October 2021, REvil's servers were taken offline as part of the international law enforcement Operation GoldDust.[7] In January 2022, Russia arrested 14 alleged REvil members and raided 25 locations associated with them.[8] This was the first time Russia acted against ransomware operators on its soil.

While law enforcement activities likely slowed the frequency of attacks in 2022, threat actors might well develop new strategies to avoid being caught in the future. Moreover, tension between Russia and the United States over Russia's invasion of Ukraine appears to have put an end to Russia's nascent cooperation in the global fight against ransomware. After a brief period of uncertainty following the REvil arrests, the United States and Russia ceased cooperation in pursuing ransomware actors, which means cybercriminals might view Russia as a safe haven once more.

Looking ahead, we predict the pace of ransomware activities will depend on the outcome of some key questions:

1. Will governments take action to prevent ransomware criminals from operating within their borders, or seek to disrupt actors operating from foreign soil?
2. Will ransomware groups change tactics to remove the need for ransomware and resort to extortion style attacks?
3. Will organizations be able to modernize and transform their IT operations faster than criminals can exploit vulnerabilities?
4. Will advancements in tracking and tracing ransom payments force ransom recipients to change tactics and negotiations?

Actionable insights

1. Focus on holistic security strategies, as all of the ransomware families take advantage of the same security weaknesses to impact a network.
2. Update and maintain security basics to increase defense-in-depth base level of protection and modernize security operations. Moving to the cloud allows you to detect threats more quickly and respond faster.

Links to further information

- Protect your organization from ransomware | Microsoft Security
- 7 ways to harden your environment against compromise | Microsoft Security Blog
- Improving AI-based defenses to disrupt human-operated ransomware | Microsoft 365 Defender Research Team
- Security Insider: Explore the latest cybersecurity insights and updates | Microsoft Security

While law enforcement activities likely slowed the frequency of attacks in 2022, threat actors might well develop new strategies to avoid being caught in the future.

2X

Ransomware attacks decreased in some regions, but ransom demands more than doubled.

https://t.me/learningnets

Cybercrime as a service

Cybercrime as a service (CaaS) is a growing and evolving threat to customers worldwide. The Microsoft Digital Crimes Unit (DCU) observed continued growth of the CaaS ecosystem with an increasing number of online services facilitating various cybercrimes, including BEC and human-operated ransomware. Phishing continues to be a preferred attack method as cybercriminals can acquire significant value from successfully stealing and selling access to stolen accounts.

In response to the expanding CaaS market, DCU enhanced its listening systems to detect and identify CaaS offerings across the entire ecosystem of internet, deep web, vetted forums,[9] dedicated websites, online discussion forums, and messaging platforms.

Cybercriminals are now collaborating across time zones and languages to deliver specific results. For example, one CaaS website administered by an individual in Asia maintains operations in Europe, and creates malicious accounts in Africa. The multi-jurisdictional nature of these operations present complex law and enforcement challenges. In response, DCU focuses its efforts on disabling malicious criminal infrastructure used to facilitate CaaS attacks and collaborating with law enforcement agencies around the world to hold criminals accountable.

Cybercriminals are increasingly using analytics to maximize reach, scope, and gain. Like legitimate businesses, CaaS websites must ensure the validity of products and services to maintain a solid reputation. For example, CaaS websites routinely automate access to compromised accounts to ensure the validity of compromised credentials. Cybercriminals will discontinue sales of specific accounts when passwords are reset or vulnerabilities patched. Increasingly, we identified CaaS websites providing buyers with on-demand verification as a quality control process. As a result, buyers can feel confident the CaaS website sells active accounts and passwords while reducing potential costs to the CaaS merchant if the stolen credentials are remediated prior to sale.

DCU also observed CaaS websites offering buyers the option to purchase compromised accounts from specific geographic locations, designated online service providers, and specifically targeted individuals, professions, and industries. Frequently ordered accounts focus on professionals or departments that process invoicing, such as CFOs or "Accounts Receivable." Similarly, industries participating in public contracting are often targeted due to the quantity of information that is made available through the public bidding process.

DCU investigations into CaaS surfaced a number of key trends:

The number and sophistication of services is increasing.

One example is the evolution of web shells which typically consist of compromised web servers used to automate phishing attacks. DCU observed CaaS resellers simplifying the upload of phishing kits or malware through specialized web-dashboards. CaaS sellers often subsequently attempt to sell additional services to the threat actor through the dashboard such as spam message services and specialized spam recipient lists based on defined attributes including geographic location or profession. In some instances, we observed a single web shell being used in multiple attack campaigns, which suggests threat actors might maintain persistent access to the compromised server. We also observed an increase in anonymization services available as part of the CaaS ecosystem as well as offers for virtual private networks (VPN) and virtual private server (VPS) accounts. In most instances, the VPN/VPS offered were initially procured through stolen credit cards. CaaS websites also offered a larger number of remote desktop protocol (RDP), secure shell (SSH), and cPanels for use as a platform to orchestrate cybercrime attacks. CaaS merchants configure the RDP, SSH, and cPanels with appropriate tools and scripts to facilitate various types of cyberattacks.

Homoglyph domain creation services are increasingly requiring payment in cryptocurrencies.

Homoglyph domains impersonate legitimate domain names by utilizing characters that are identical or nearly identical in appearance to another character. The aim is to deceive the viewer into thinking the homoglyph domain is the genuine domain. These domains are a ubiquitous threat and a gateway for a significant amount of cybercrime. CaaS sites now sell custom homoglyph domain names, which allows buyers to request specific company and domain names to impersonate. After payment is received, the CaaS merchants use a homoglyph generator tool to select the domain name and then register the malicious homoglyph. Payment for this service is almost exclusively in cryptocurrency.

2,750,000

site registrations successfully blocked by DCU this year to get ahead of criminal actors that planned to use them to engage in global cybercrime.

https://t.me/learningnets

Cybercrime as a service

Continued

CaaS sellers increasingly offer compromised credentials for purchase.

Compromised credentials enable unauthorized access to user accounts including email messaging service, corporate file sharing resources, and OneDrive for Business. If administrator credentials are compromised, unauthorized users could gain access to confidential files, Azure resources, and company user accounts. In many instances, DCU investigations identified unauthorized use of the same credential across multiple servers as a means to automate verifying credentials. This pattern suggests the compromised user might be a victim of multiple phishing attacks or have device malware allowing botnet keyloggers to collect credentials.

CaaS services and products with enhanced features are emerging to avoid detection.

One CaaS seller offers phishing kits with increased layers of complexity and anonymization features designed to circumvent detection and prevention systems for as little as $6 USD per day. The service offers a series of redirects that perform checks before allowing traffic to the next layer or site. One of these runs over 90 checks for fingerprinting the device, including whether it is a virtual machine, gathering details about the browser and hardware being used, and more. If all checks pass, traffic is sent to a landing page used for phishing.

End-to-end cybercrime services are selling subscriptions to managed services.

Typically, each step in the commission of an online crime can expose threat actors if operational security is poor. The risk of exposure and identification increases if services are purchased from multiple CaaS sites. DCU observed a concerning trend in the dark web whereby there is an increase in services offering to anonymize software code and genericize website text to reduce exposure. End-to-end cybercrime subscription service providers manage all services and guarantee results which further reduce exposure risks to the subscribing OCN. The reduced risk has increased the popularity of these end-to-end services.

Phishing as a service (PhaaS) is one example of an end-to-end cybercrime service. PhaaS is an evolution of prior services known as fully undetectable services (FUD) and is offered on a subscription basis. Typical PhaaS terms include keeping phishing websites active for a month.

DCU also identified a CaaS merchant offering distributed denial of service (DDoS) on a subscription model. This model outsources the creation and maintenance of the botnet necessary to carry out attacks to the CaaS merchant. Each DDoS subscription customer receives an encrypted service to enhance operational security and one year of 24/7 support. The DDoS subscription service offers different architectures and attack methods, so a purchaser simply selects a resource to attack and the seller provides access to an array of compromised devices on their botnet to conduct the attack. The cost for the DDoS subscription is a mere $500 USD.

PhaaS, cybercriminals offer multiple services within a single subscription. In general, a purchaser needs to take only three actions:

Once these steps are completed, the PhaaS merchant creates services with three or four layers of redirect and hosting resources to target specific users. The campaign is subsequently launched, and victim credentials are harvested, verified, and sent to the email address provided by the purchaser. For a premium, many PhaaS merchants offer to host phishing sites on the public blockchain so they can be accessed by any browser and redirects can point users to a resource on the distributed ledger.

DCU's work to develop tools and techniques which identify and disrupt CaaS cybercriminals is ongoing. The evolution of CaaS services presents significant challenges, particularly in disrupting cryptocurrency payments.

https://t.me/learningnets

Criminal use of cryptocurrencies

As the adoption of cryptocurrency becomes mainstream, criminals are increasingly using it to evade law enforcement and anti-money laundering (AML) measures. This heightens the challenge for law enforcement to track and trace cryptocurrency payments to cybercriminals.

Worldwide spending on blockchain solutions grew by approximately 340 percent over the last four years, while new cryptocurrency wallets grew by around 270 percent. There are more than 83 million unique wallets globally, and the total market capitalization of all cryptocurrencies was approximately $1.1 trillion USD as of July 28, 2022.[10]

Source: Twitter.com—@PeckShieldAlert (PeckShield is a China-based blockchain security company).

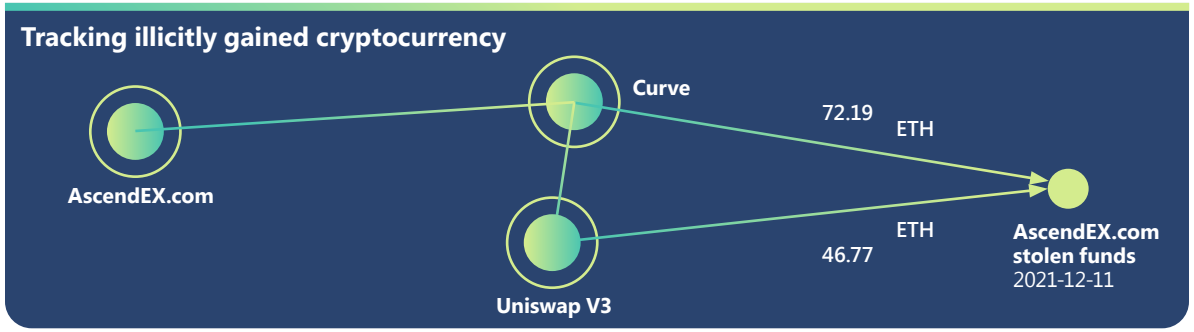
Tracking ransomware payments

Ransomware is one of the largest sources of illicitly gained cryptocurrency. In an effort to disrupt malicious technical infrastructure used in ransomware attacks—for example, the disruption of Zloader in April 2022[11]—Microsoft's DCU tracks criminal wallets to enable cryptocurrency tracking and recovery capabilities.

DCU investigators have observed ransomware actors evolving their communication tactics with victims to conceal the money trail. Originally, cybercriminals included Bitcoin addresses in their ransom notes. However, this made it easy to follow payment transactions on the blockchain, so ransomware actors stopped including wallet addresses and instead appended email addresses or links to chat websites to communicate ransom payment addresses to victims. Some actors even created unique webpages and logins for each victim to prevent security researchers and law enforcement from obtaining the criminals' wallet addresses by pretending to be victims. Despite criminals' efforts to hide their tracks, some ransom payments can still be recovered by working with law enforcement and crypto analysis companies that can track movement on the blockchain.

Trending: DEX laundering of illicit proceeds

A key issue for cybercriminals is the conversion of cryptocurrency to fiat currency. Cybercriminals have several potential avenues for conversion, each of which carries a different degree of risk. One method used to reduce risk is to launder proceeds through a decentralized exchange (DEX) before cashing out via available cash-out options, such as centralized exchanges (CEX), peer-to-peer (P2P) and over the counter (OTC) exchanges. DEXes are an attractive laundering location because they often do not follow AML measures.



Using the cryptocurrency investigative tool Chainalysis, Microsoft's Digital Crimes Unit discovered the AcendEX hackers swapped their stolen funds at a smaller DEX called Curve in addition to Uniswap. This diagram illustrates the laundering routes the team uncovered. Each circle represents a cluster of wallets and the numbers on each line represent the total amount of Ethereum transmitted for laundering purposes.

In December 2021, hackers attacked the global cryptocurrency trading platform AscendEx and stole approximately $77.7 million USD in cryptocurrency belonging to its customers.[12] AscendEx hired blockchain analytics firms and contacted other CEXs so the wallets receiving stolen funds could be blacklisted. Additionally, addresses where the coins were sent were labeled as such on the Ethereum blockchain explorer Etherscan.[13] In order to circumvent the alerting and blacklisting, the hackers sent $1.5 million USD in Ethereum to Uniswap, one of the world's largest DEXs, on February 18, 2022.[14]

The adoption of stronger AML measures by DEXs could blunt laundering activity on their platforms and force cybercriminals to use other obfuscation methods like coin tumbling or unlicensed exchanges. As an example, Uniswap recently announced it will start to use blacklists to block wallets known to be involved in illicit activities from transacting on the exchange.[15]

Actionable insights

1. If you are a victim of cybercrime who has paid the criminal using cryptocurrency, contact local law enforcement who might be able to help track and recover lost funds.
2. Become familiar with the ALM measures in place when selecting a DEX.

Links to further information

- Hardware-based threat defense against increasingly complex cryptojackers | Microsoft 365 Defender Research Team

https://t.me/learningnets

The evolving phishing threat landscape

Credential phishing schemes are on the rise and remain a substantial threat to users everywhere because they indiscriminately target all inboxes. Among the threats our researchers track and protect against, the volume of phishing attacks is orders of magnitude greater than all other threats.

Using data from Defender for Office, we see malicious email and compromised identity activity. Azure Active Directory Identity Protection provides still more information through compromised identity event alerts. Using Defender for Cloud Apps, we see compromised identity data access events, and Microsoft 365 Defender (M365D) provides cross-product correlation. The lateral movement metric comes from Defender for Endpoint (attack behavior alerts and events), Defender for Office (malicious email) and again M365D for cross-product correlation).

710 million
phishing emails blocked per week.

https://t.me/learningnets

1hr 12m
The median time it takes for an attacker to access your private data if you fall victim to a phishing email.[16]

1hr 42m
The median time for an attacker to begin moving laterally within your corporate network once a device is compromised.[17]

Microsoft 365 credentials remain one of the most highly sought-after account types for attackers. Once login credentials are compromised, attackers can log in to corporate-tied computer systems to facilitate infection with malware and ransomware, steal confidential company data and information by accessing SharePoint files, and continue the spread of phish by sending additional malicious emails using Outlook, among other actions.

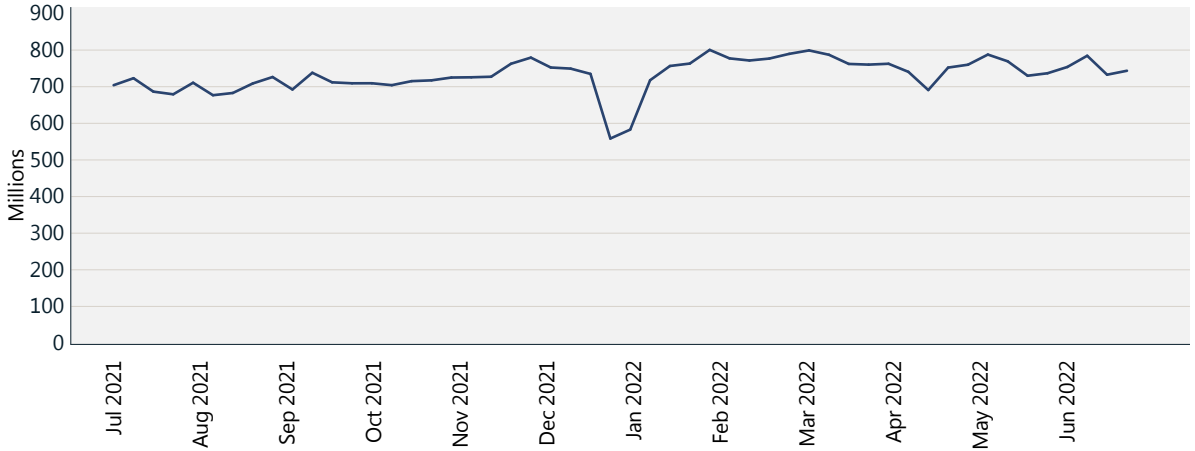
In addition to campaigns with broader targets, phishing for credentials, donations, and personal information, attackers are targeting selective businesses for larger payouts. Email phishing attacks against businesses for financial gain are collectively referred to as BEC attacks.

Microsoft detects millions of BEC emails every month, equivalent to 0.6 percent of all phishing emails observed. A report from IC3[18] published in May 2022 indicates an upward trend in exposed losses due to BEC attacks.

The techniques used in phishing attacks continue to increase in complexity. In response to countermeasures, attackers adapt new ways to implement their techniques and increase the complexity of how and where they host campaign operation infrastructure. This means organizations must regularly reassess their strategy for implementing security solutions to block malicious emails and strengthen access control for individual user accounts.

531,000
In addition to the URLs blocked by Defender for Office, our Digital Crimes Unit directed the takedown of 531,000 unique phishing URLs hosted outside of Microsoft.

Detected phish emails



The number of phish detections per week continue to rise. The decrease in December–January is an expected seasonal drop, also reported in last year's report. Source: Exchange Online Protection signals.

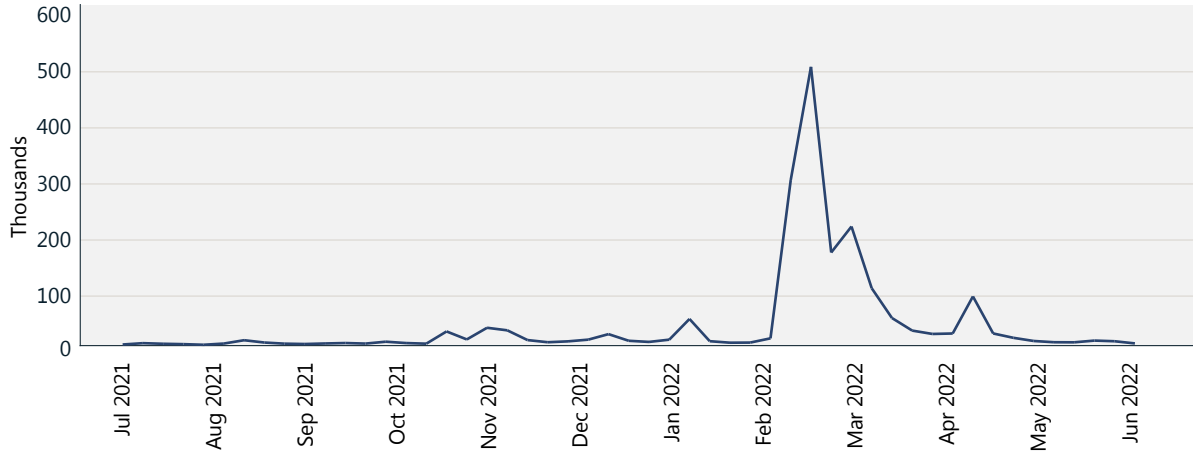
The evolving phishing threat landscape

Continued

We continue to observe a steady year-over-year increase in phishing emails. The shift to remote work in 2020 and 2021 saw a substantial increase in phishing attacks aiming to capitalize on the changing work environment. Phish operators are quick to adopt new email templates using lures aligned with major world events such as the COVID-19 pandemic and themes linked to collaboration and productivity tools such as Google Drive or OneDrive file sharing. While COVID-19 themes have diminished, the war in Ukraine became a new lure starting in early March 2022. Our researchers observed a staggering increase of emails impersonating legitimate organizations soliciting cryptocurrency donations in Bitcoin and Ethereum, allegedly to support Ukrainian citizens.

Only a few days after the start of the war in Ukraine in late February 2022, the number of detected phishing emails containing Ethereum addresses encountered across enterprise customers increased dramatically. Total encounters peaked in the first week of March when half a million phishing emails contained an Ethereum wallet address. Prior to the start of the war, the number of Ethereum wallet addresses across other emails detected as phish was significantly less, averaging a few thousand emails per day.

Phishing emails with Ethereum wallet addresses



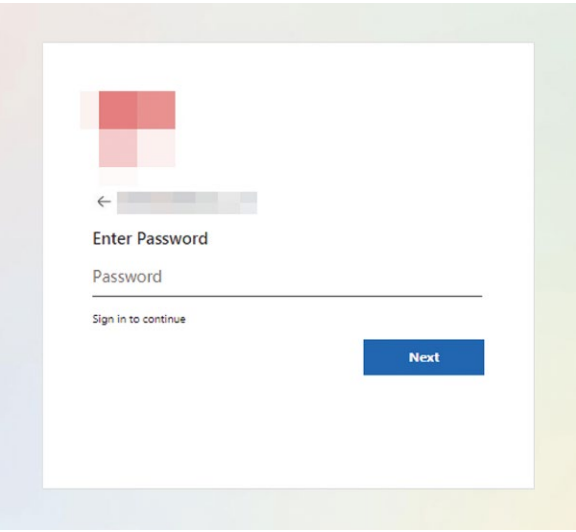
Total emails detected as phish containing Ethereum wallet addresses increased at the start of the Ukraine-Russia conflict and tapered off after the initial push.

More than ever, phishers are relying on legitimate infrastructure to operate, driving a rise in phishing campaigns aimed at compromising various aspects of an operation so they do not have to purchase, host, or operate their own. For example, malicious emails might originate from compromised sender accounts. Attackers benefit from using these email addresses which have a higher reputation score and are seen as more trustworthy than newly created accounts and domains. In some more advanced phishing campaigns, we observed attackers preferring to send and spoof from domains which have DMARC[19] incorrectly set up with a "no action" policy, opening the door for email spoofing.

Large phish operations tend to use cloud services and cloud virtual machines (VMs) to operationalize large scale attacks. Attackers can fully automate the process of deploying and delivering emails from VMs using SMTP email relays or cloud email infrastructure to benefit from the high deliverability rates and positive reputation of these legitimate services. If malicious email is allowed to be sent through these cloud services, defenders must rely on strong email filtering capabilities to block emails from entering their environment.

Microsoft accounts remain a top target for phishing operators, as evidenced by the numerous phishing landing pages which impersonate the Microsoft 365 login page. For example, phishers attempt to match the Microsoft login experience in their phish kits by generating a unique URL customized to the recipient. This URL points to a malicious webpage developed to harvest credentials, but a parameter in the URL will contain the specific recipient's email address. Once the target navigates to the page, the phish kit will pre-populate user login data and a corporate logo customized to the email recipient, mirroring the appearance of the targeted company's custom Microsoft 365 login page.

Phishing page impersonating a Microsoft login with dynamic content



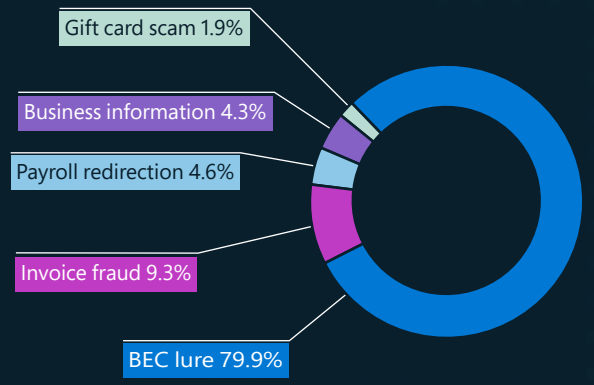
https://t.me/learningnets

Spotlight on business email compromise

Cybercriminals are developing increasingly complex schemes and techniques to defeat security settings and target individuals, businesses, and organizations. We are investing significant resources to further enhance our BEC enforcement program in response.

BEC is the costliest financial cybercrime, with an estimated $2.4 billion USD in adjusted losses in 2021, representing more than 59 percent of the top five internet crime losses globally.[20] To understand the scope of the problem and how best to protect users against BEC, Microsoft security researchers have been tracking the most common themes used in attacks.

BEC themes (January–June 2022)



BEC themes by percentage of occurrence

BEC trends

As a point of entry, BEC attackers normally attempt to start a conversation with potential victims to establish rapport. Posing as a colleague or business acquaintance, the attacker gradually leads the conversation in the direction of a monetary transfer. The introduction email, which we track as a BEC lure, represents close to 80 percent of detected BEC emails. Other trends identified by Microsoft security researchers over the past year include:

- The most frequently used techniques in BEC attacks observed in 2022 were spoofing[21] and impersonation.[22]
- The BEC subtype causing the most financial damage to victims was invoice fraud (based on volume and requested dollar amounts seen in our BEC campaign investigations).
- Business information theft such as accounts payable reports and customer contacts enable attackers to craft convincing invoice fraud.
- Most payroll redirection requests were sent from free email services and seldom from compromised accounts. Email volume from these sources spiked around the first and fifteenth of each month, the most common pay dates.
- Despite being well-known avenues for fraud, gift card scams comprised only 1.9 percent of the BEC attacks detected.

Actionable insights

Defending against phish

To reduce your organization's exposure to phish, IT administrators are encouraged to implement the following policies and features:

1. Require the use of MFA across all accounts to limit unauthorized access.
2. Enable conditional access features for highly privileged accounts to block access from countries, regions, and IPs that do not typically generate traffic at your organization.
3. Consider using physical security keys for executives, employees involved in payment or purchase activities, and other privileged accounts.
4. Enforce the use of browsers which support services such as Microsoft SmartScreen to analyze URLs for suspicious behaviors and blocks access to known malicious websites.[23]
5. Use a machine-learning based security solution that quarantines high probability phish and detonates URLs and attachments in a sandbox before email reaches the inbox, such as Microsoft Defender for Office 365.[24]
6. Enable impersonation and spoofing protection features across your organization.
7. Configure DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication Reporting & Conformance (DMARC) action policies to prevent delivery of non-authenticated emails that might be spoofing reputable senders.
8. Audit tenant and user created allow rules and remove broad domain and IP based exceptions. These rules often take precedence and can allow known malicious emails through email filtering.
9. Regularly run phishing simulators to gauge the potential risk across your organization and to identify and educate vulnerable users.

Links to further information

- From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud | Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC)

https://t.me/learningnets

Homoglyph deception

BEC and phishing are common social engineering tactics. Social engineering plays a significant role in crime, persuading a target to interact with the criminal by gaining trust.

In physical commerce, trademarks are used to secure trust in the origin of a product or service, and counterfeit products are an abuse of the trademark. Similarly, cybercriminals pose as a contact familiar to the target during a phishing attack, using homoglyphs to deceive potential victims.

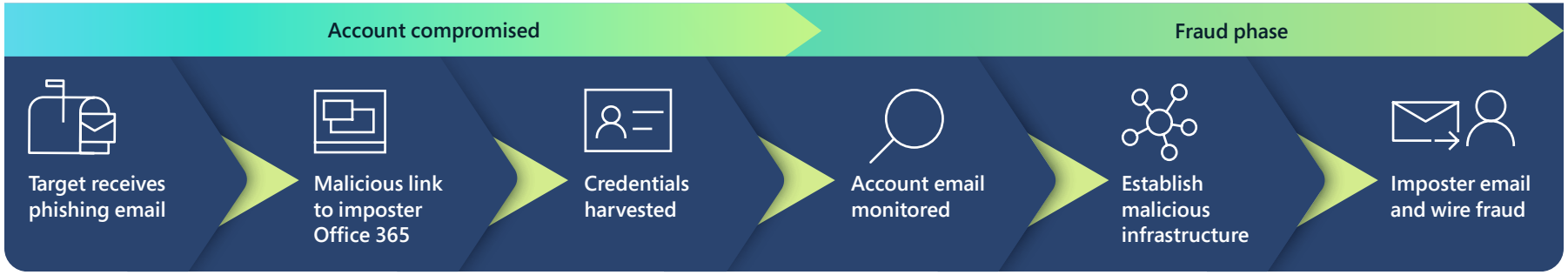
A homoglyph is a domain name used for email communication in BEC, in which a character is replaced by one that is identical or nearly identical in appearance, in order to deceive the target.

Homoglyph techniques used in BEC attempts

BEC generally has two phases, the first of which involves compromise of credentials. These types of credential leaks can be a result of phishing attacks or large data breaches. The credentials are then sold or traded on the dark web.

The second phase is the fraud phase, where attackers use compromised credentials to engage in sophisticated social engineering using homoglyph email domains.

Progression of a BEC attack



Technique	% of domains showing homoglyph technique
sub l for I	25%
sub i for l	12%
sub q for g	7%
sub rn for m	6%
sub .cam for .com	6%
sub 0 for o	5%
sub ll for l	3%
sub ii for i	2%
sub vv for w	2%
sub l for ll	2%
sub e for a	2%
sub nn for m	1%
sub ll for I, sub l for i	1%
sub o for u	1%

Analysis of over 1,700 homoglyph domains between January–July 2022. While 170 homoglyph techniques were used, 75% of domains used just 14 techniques.

A homoglyph in action

A homoglyph domain that looks identical to a mail domain the victim recognizes is registered on a mail provider with a username that is identical. A hijacked email is then sent from the hijacked domain with new payment instructions.

Leveraging open-source intelligence and access to email threads, the criminal identifies individuals who have responsibility for invoicing and payments. They then create an impersonation of an email address of the individual sending invoices. This impersonation is composed of an identical username and mail domain that is a homoglyph of the genuine sender.

The attacker copies an email chain containing a legitimate invoice, then changes the invoice to contain their own bank details. This new, modified invoice is then resent from the homoglyph impersonation email to the target. Because the context makes sense and the email looks genuine, often the target follows the fraudulent instructions.

Actionable insights

1. Enforce the use of browsers that support services to analyze URLs for suspicious behaviors and blocks access to known malicious websites such as Safe Links and SmartScreen.[25]
2. Use a machine-learning based security solution that quarantines high probability phish and detonates URLs and attachments in a sandbox before email reaches the inbox.

Links to further information

- Internet Crime Complaint Center (IC3) | Business Email Compromise: The $43 Billion Scam
- Spoof intelligence insight—Office 365 | Microsoft Docs
- Impersonation insight—Office 365 | Microsoft Docs

https://t.me/learningnets

A timeline of botnet disruption from Microsoft's early days of collaboration

For more than a decade, DCU has worked to proactively stop cybercrime resulting in 26 malware and nation state disruptions. As the DCU team uses more advanced tactics and tools to shut down these illicit operations, we see the cybercriminals also evolve their approaches in an attempt to stay a step head. Here is a timeline showing a sample of the botnets disrupted by DCU and the strategies Microsoft adopted to shut them down.

2008

Conficker botnet

Description: A fast-spreading worm targeting the Windows OS, infecting millions of computers and devices in a common network; created network outages worldwide.

Collaboration: Formation of the Conficker Working Group, the first consortium of its kind. Microsoft partnered with 16 organizations across the globe to defeat the bot.

Microsoft response: The group collaborated across many international jurisdictions and was successful bringing Conficker down.

2009

Waledac botnet

Description: A complex spam botnet with US domains that collected email addresses and distributed spam that infected up to 90,000 computers across the world.[26]

Collaboration: Creation of another consortium, the Microsoft Malware Protection Center (MMPC) with a focus on close collaboration with academics.[27]

Microsoft response: Microsoft used tiered disruption approach of C2 and surprised bad actors by seizing US-based domains without notice.[28] Microsoft granted temporary ownership of nearly 280 domains used by Waledac's servers.

2011

Microsoft Digital Crimes Unit is formed

Collaboration: Designed to thwart cybercrime impacting the Microsoft ecosystem through close integration across a team of investigators, lawyers, and engineers.

Microsoft approach: The goal is to better understand the technical aspects of various malware and provide these insights to Microsoft's legal team to develop an effective disruption strategy.

2013

Rustock botnet

Description: A backdoor trojan spam email bot using internet providers as primary C2s; designed to sell pharmaceuticals.

Collaboration: Microsoft forged a partnership with Pfizer Pharmaceuticals to understand the drugs sold by Rustock and worked closely with Dutch law enforcement officials.[29]

Microsoft response: Microsoft worked with US Marshalls and law enforcement in the Netherlands to take down the C2 servers in that country. Registered and blocked all future domain generator algorithms (DGAs).

Sirefef/Zero Access botnet

Description: An advertising botnet designed to direct people to dangerous websites that would install malware or steal personal information; infected more than two million computers and cost advertisers more than $2.7 million USD per month; primarily in US and Western Europe.

Collaboration: Worked closely with the FBI and Europol's Cybercrime Center to bring down the peer-to-peer infrastructure.

Microsoft response: Joined the Zero Access network, replaced the criminal C2 servers, and successfully seized download server domains.

2019

Trickbot botnet

Description: A sophisticated botnet with fragmented infrastructure across the globe that targeted the financial services industry; compromised IoT devices.

Collaboration: Microsoft partnered with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to bring down Trickbot.[30]

Microsoft response: DCU built a system to identify and track bot infrastructure and generated notifications for active internet providers, taking into account specific laws in various countries.

2022

Continued focus on disruption

Description: Microsoft disrupted the infrastructure of seven threat actors over the past year, preventing them from distributing additional malware, controlling victims' computers, and targeting additional victims.

Collaboration: In partnership with internet service providers, governments, law enforcement, and private industry, Microsoft shared information to remediate over 17 million malware victims worldwide.

Looking ahead

DCU continues to innovate and is looking to use its experience in botnet disruptions to conduct coordinated operations that go beyond malware. Our continued success requires creative engineering, sharing of information, innovative legal theories, and public and private partnerships.

https://t.me/learningnets

Cybercriminal abuse of infrastructure

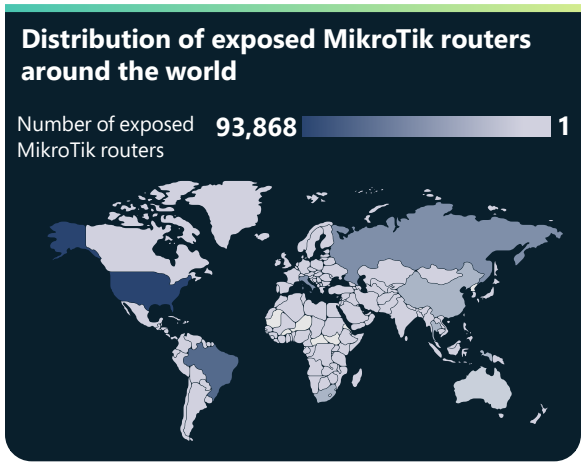
Internet gateways as criminal command and control infrastructure

IoT devices are becoming an increasingly popular target for cybercriminals using widespread botnets. When routers are unpatched and left exposed directly to the internet, threat actors can abuse them to gain access to networks, execute malicious attacks, and even support their operations.

The Microsoft Defender for IoT team conducts research on equipment ranging from legacy industrial control system controllers to cutting-edge IoT sensors. The team investigates IoT- and OT-specific malware to contribute to the shared list of indicators of compromise.

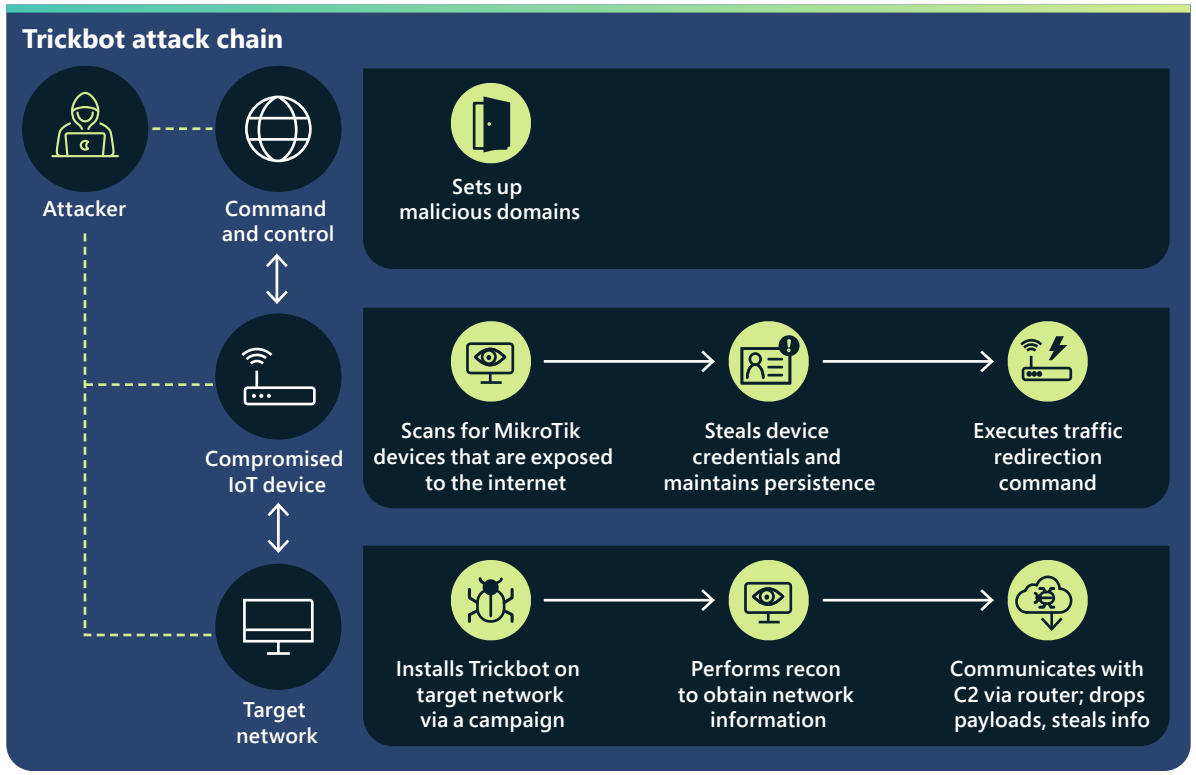
Routers are particularly vulnerable attack vectors because they are ubiquitous across internet-connected homes and organizations. We have been tracking the activity of MikroTik routers, a popular router around the world residentially and commercially, identifying how they are utilized for command and control (C2), domain name system (DNS) attacks, and crypto mining hijacking.

More specifically, we identified how Trickbot operators utilize compromised MikroTik routers and reconfigure them to act as part of their C2 infrastructure. The popularity of these devices compounds the severity of their abuse by Trickbot, and their unique hardware and software enable threat actors to evade traditional security measures, expand their infrastructure, and compromise more devices and networks.



Exposed routers are at risk of having potential vulnerabilities exploited.

By tracking and analyzing traffic containing secure shell (SSH) commands, we observed attackers using MikroTik routers to communicate with Trickbot infrastructure after obtaining legitimate credentials to devices. These credentials can be obtained through brute force attacks, exploiting known vulnerabilities with readily available patches, and using default passwords. Once a device is accessed, the attacker issues a unique command that redirects traffic between two ports in the router, establishing the line of communication between Trickbot-affected devices and the C2.



Trickbot attack chain showing the use of MikroTik IoT devices as proxy servers for C2.

We have aggregated our knowledge of the various methods of attacking MikroTik devices, beyond just Trickbot, as well as known common vulnerabilities and exposures (CVEs) into an open-source tool for MikroTik devices, which can extract the forensic artifacts related to attacks on these devices.[31]

Devices acting as reverse proxies for malware C2 are not just unique to Trickbot and MikroTik routers. In collaboration with the Microsoft RiskIQ team, we traced back to the C2 involved and, through observing SSL certificates, identified Ubiquiti and LigoWave devices that are impacted as well.[32] This is a strong indication that IoT devices are becoming active components of nation state coordinated attacks and a popular target for cybercriminals using widespread botnets.

https://t.me/learningnets

Crypto criminals abusing IoT devices

Gateway devices are an increasingly valuable target for threat actors as the number of known vulnerabilities has grown consistently from year to year. They are being used for crypto mining and other types of malicious activity.

As cryptocurrency has become more popular, many individuals and organizations have invested computational power and network resources from devices such as routers to mine coins on the blockchain. However, mining cryptocurrency is a time- and resource-intensive process with a low probability of success. To increase the likelihood of mining a coin, miners pool together in distributed, cooperative networks, receiving hashes relative to the percentage of the coin they succeeded in mining with their connected resources.

In the past year, Microsoft observed a growing number of attacks that abuse routers for redirecting cryptocurrency mining efforts. Cybercriminals compromise routers connected to mining pools and redirect mining traffic to their associated IP addresses with DNS poisoning attacks, which alters the DNS settings of targeted devices. Affected routers register the wrong IP address to a given domain name, sending their mining resources—or hashes—to pools used by threat actors. These pools might mine anonymous coins associated with criminal activities or use legitimate hashes generated by miners to acquire a percentage of the coin that they mined, thus reaping the rewards.

With more than half of known vulnerabilities found in 2021 lacking a patch, updating and securing routers on corporate and private networks remains a significant challenge for device owners and administrators.

Compromising devices for illegal crypto mining.

DNS poisoning of gateway devices compromises legitimate mining activities and redirects resources to criminal mining activities.

Virtual machines as criminal infrastructure

The widespread move to the cloud includes cybercriminals who leverage private assets of unwitting victims obtained through phishing or distributing malware credential stealers. Many cybercriminals are choosing to set up their malicious infrastructures on cloud-based virtual machines (VMs), containers, and microservices.

Once the cybercriminal has access, a sequence of events can occur to set up infrastructure—such as a series of virtual machines through scripting and automated processes. These scripted, automated processes are used to launch malicious activity including large scale email spam attacks, phishing attacks, and web pages hosting nefarious content. It can even include setting up a scaled virtual environment carrying out cryptocurrency mining, causing the end victim a bill of hundreds of thousands of dollars at the end of the month.

Cybercriminals understand their malicious activity has a limited life span before it is detected and shut down. As a result, they have scaled up and now operate proactively with contingencies top of mind. They have been observed preparing compromised accounts ahead of time and monitoring their environments. As soon as an account (set up using hundreds of thousands of virtual machines) is detected, they traverse to the next account—already prepared by scripts to be immediately activated—and their malicious activity continues with little to no interruption.

Like cloud infrastructure, on-premises infrastructure can be used in attacks with virtual local environments that are unknown to the on-premises user. This requires the initial access point to remain open and accessible. On-premises private assets have also been abused by cybercriminals to initiate an onward chain of cloud infrastructure, set up to obfuscate their origin to avoid suspicious infrastructure creation detection.

Actionable insights

1. Implement good cyber hygiene and provide cybersecurity training for employees with guidance for avoiding being socially engineered.
2. Conduct regular automated user activity anomaly checks through detections at scale to help reduce these types of attacks.
3. Update and secure routers on corporate and private networks.

https://t.me/learningnets

Is hacktivism here to stay?

While hacktivism is not a new phenomenon, the war in Ukraine saw a surge of volunteer hackers, including some directed by governments to deploy cyber tools to damage the reputation or assets of political opponents, organizations, and even nation states.

In February 2022, the Ukrainian government called on private civilians around the world to conduct cyberattacks on Russia as part of its 300,000 strong "IT Army."[33] At the same time, established hacktivist groups such as Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans, and RaidForum2 began conducting attacks in support of Ukraine. Other groups, including some of the Conti ransomware gang, sided with Russia.[34]

In the months that followed, Anonymous's activities were highly visible. Hackers acting in the group's name—or in that of one of its affiliates—temporarily disabled thousands of Russian and Belarusian websites, leaked hundreds of gigabytes of stolen data, hacked Russian TV channels to play pro-Ukrainian content, and even offered to pay Bitcoin for surrendered Russian tanks.

The rise of citizen hackers

Social media platforms enabled the rapid organization and mobilization of thousands of would-be citizen hackers, who were provided directions for conducting easily executable attacks such as DDoS attacks. Organizers leveraged Twitter, Telegram, and private forums to rally hackers, organize operations, and disseminate hacking instruction manuals.

However, most of these hackers likely have limited skills, even with instruction. This suggests two potential futures: one in which hundreds or thousands of individuals with rudimentary technical capabilities use attack templates to conduct future coordinated or individual hacktivist attacks against targets, or a second future where the eventual end of hostilities in Ukraine sees them leaving their hacktivism behind, at least until the next political or social issue inspires them to action.

Politicization of hackers

The greater risk posed by this political mobilization is the deployment of tech-savvy hackers who might continue to conduct cyberattacks against foreign government targets to support their own national priorities, either on a self-initiated basis or at the behest of their government.

Iran, China, and Russia already use hacktivism as a feeder for recruitment into their state hacking groups. For example, in April 2022, the pro-Russian hacking group Killnet launched DDoS attacks against Czech railroads, regional airports, and Czechia's civil service server, even though Czechia is not directly involved in the war.[35] At the same time, some governments might use hacktivism as a cover for traditional cyberespionage or sabotage operations—for example, Iranian activities against Israel.

In an environment of increased DDoS attacks linked to hacktivism, the technology industry is challenged to quickly decipher the difference between normal and abnormal traffic flow to a website. Microsoft and its partners have developed a collection of tools which distinguish malicious DDoS traffic and trace it back to its origin. In addition, Microsoft's Azure platform can identify machines on the platform that produce extraordinarily high levels of outbound traffic and shut them down.

Emergence of protestware

Protestware has emerged as a direct result of emotional reactions to the war between Russia and Ukraine. Some open source software developers used the popularity of their software as a means to speak up or take action against an unfolding geopolitical situation. This included harmless text files opened on a desktop or a browser to spread messages of peace, but also included targeted attacks based on IP address geolocation and destructive actions such as wiping a hard drive. As other global events unfold, we can expect to see protestware surface again in the future. Since these are generally cases where well-respected open-source maintainers are deciding to make personal statements using their own open source components, there is currently no protection in place to stop these types of changes from occurring in the source file packages and users should maintain awareness of potential impact.

Social media platforms enabled the organization and mobilization of thousands of would-be citizen hackers, who were provided directions for conducting easily executable attacks such as DDoS attacks.

Actionable insights

1. The technology industry must come together to design a comprehensive response to this new threat.
2. Leading technology companies, including Microsoft, have tools to identify malicious traffic associated with DDoS attacks and disable the responsible machines.
3. Open source users should keep a heightened watch during times of geopolitical strife.

https://t.me/learningnets

Endnotes

1 https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2 https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/
3 https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4 https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5 https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6 Endpoint detection and response. https://www.microsoft.com/en-us/security/business/threat-protection/
7 https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8 https://www.bbc.com/news/technology-59998925
9 A Vetted Forum is an online discussion forum that requires an existing member to vouch for the addition of a new member.
10 https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11 https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12 https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13 https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14 https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15 https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16 Data source: Defender for Office (malicious email/compromised identity activity), Azure Active Directory Identity Protection (compromised identity events/alerts), Defender for Cloud Apps (compromised identity data access events), and M365D (cross product correlation).
17 Data source: Defender for Endpoint (attack behavior alerts/events), Defender for Office (malicious email), and M365D (cross product correlation).
18 https://www.ic3.gov/Media/Y2022/PSA220504
19 Domain-based Message Authentication, Reporting and Conformance: An email authentication, policy, and reporting protocol designed to give email domain owners the ability to protect their domain from unauthorized use.
20 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21 https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22 https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23 https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24 https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25 https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26 Microsoft Corporation v. John Does 1-27, et. al., No. 1:10CV156, (E.D.Va. Feb 22, 2010).
27 See Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., Sep 27, 2011.
28 Specifically, Rule 65 of the Federal Rules of Civil Procedure allows a party to seek such remedy if: 1) the party will suffer immediate and irreparable harm if the relief is not granted, and 2) the party attempts to provide the other side notice in a timely manner. Moreover, the law requires that a balancing test be applied, one which balances the defendant's right to notice against the quantum of harm to the public.
29 Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. Feb 9, 2011).
30 Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. Aug. 12, 2021).
31 https://github.com/microsoft/routeros-scanner
32 RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33 https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34 https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35 https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

https://t.me/learningnets

Nation State Threats

Nation state actors are launching increasingly sophisticated cyberattacks to evade detection and further their strategic priorities.

An overview of Nation State Threats 31
Introduction 32
Background on nation state data 33
Sample of nation state actors and their activities 34
The evolving threat landscape 35
The IT supply chain as a gateway to the digital ecosystem 37
Rapid vulnerability exploitation 39
Russian state actors' wartime cyber tactics threaten Ukraine and beyond 41
China expanding global targeting for competitive advantage 44
Iran growing increasingly aggressive following power transition 46
North Korean cyber capabilities employed to achieve regime's three main goals 49
Cyber mercenaries threaten the stability of cyberspace 52
Operationalizing cybersecurity norms for peace and security in cyberspace 53

https://t.me/learningnets

An overview of

Nation State Threats

Nation state actors are launching increasingly sophisticated cyberattacks to evade detection and further their strategic priorities. The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict.

Russia has also supported its war with information influence operations, using propaganda to impact opinions in Russia, in Ukraine, and globally. This first full-scale hybrid conflict has taught other important lessons. First, the security of digital operations and data can be best protected – both in cyberspace and in physical space – by moving to the cloud. Initial Russian attacks targeted on-premises services with wiper malware, and targeted physical data centers with one of the first missiles launched.

Ukraine responded by rapidly moving workloads and data to hyperscale clouds hosted in data centers outside Ukraine. Second, advances in cyber threat intelligence and endpoint protection powered by the data and advanced AI and ML services in the cloud have helped Ukraine defend against Russian cyberattacks.

Elsewhere, nation state actors have increased activity and are using advancements in automation, cloud infrastructure, and remote access technologies to attack a wider set of targets. Corporate IT supply chains that enable access to ultimate targets were frequently attacked. Cyber security hygiene became even more critical as actors rapidly exploited unpatched vulnerabilities, used both sophisticated and brute force techniques to steal credentials, and obfuscated their operations by using opensource or legitimate software. And Iran joins Russia in use of destructive cyberweapons, including ransomware, as a staple of their attacks.

These developments require urgent adoption of a consistent, global framework that prioritizes human rights and protects people from reckless state behavior online. All nations must work to implement agreed upon norms and rules for responsible state conduct.

Defending Ukraine: Early Lessons from the Cyber War — Microsoft On the Issues

Increased targeting of critical infrastructure particularly IT sector, financial services, transportation systems, and communications infrastructure.

Find out more on p35

IT supply chain being used as a gateway to access targets.

NOBELIUM

Find out more on p36

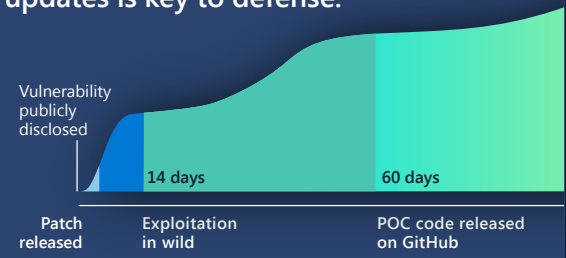
China expanding global targeting especially smaller nations in Southeast Asia, to gain intelligence and competitive advantage.

Find out more on p44

Iran grew increasingly aggressive following power transition, expanded ransomware attacks beyond regional adversaries to US and EU victims, and targeted high profile US critical infrastructure.

Find out more on p46

Identification and rapid exploitation of unpatched vulnerabilities has become a key tactic. Rapid deployment of security updates is key to defense.



Find out more on p39

North Korea targeted defense and aerospace companies, cryptocurrency, news outlets, defectors, and aid organizations, to achieve regime's goals: to build defense, bolster the economy, and ensure domestic stability.

Find out more on p49

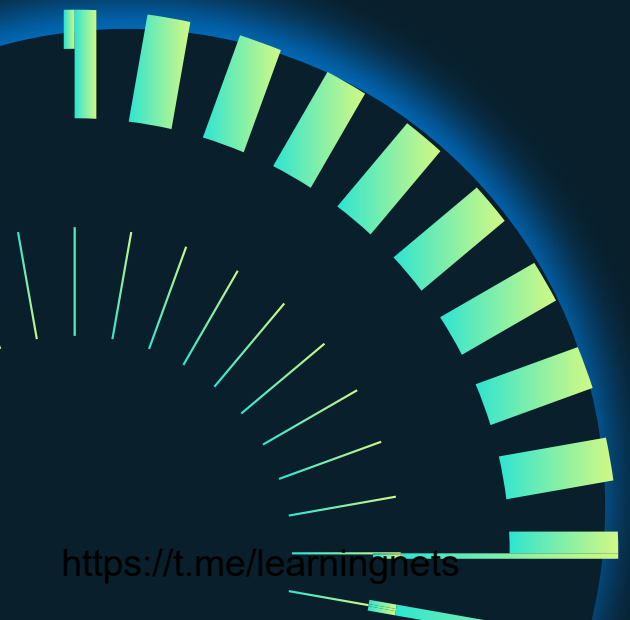
Cyber mercenaries threaten the stability of cyberspace as this growing industry of private companies is developing and selling advanced tools, techniques, and services to enable their clients (often governments) to break into networks and devices.

Find out more on p52

https://t.me/learningnets

Introduction

Following high-profile attacks in 2020 and 2021, nation state threat actors spent significant resources adapting to new security protections implemented by organizations to defend against sophisticated threats.



https://t.me/learningnets

Much like enterprise organizations, adversaries began using advancements in automation, cloud infrastructure, and remote access technologies to extend their attacks against a wider set of targets. These tactical adjustments resulted in new approaches and large scale attacks against corporate supply chains. IT security hygiene took on an even higher degree of importance as actors developed new ways to rapidly exploit unpatched vulnerabilities, expanded techniques for compromising corporate networks, and obfuscated their operations by using opensource or legitimate software. New attack techniques provided new and harder-to-detect vectors to gain access to a target's network. Finally, as wartime physical attacks escalated, we saw cyberattacks take a prominent role in military activity.

The conflict in Ukraine has provided an all-too-poignant example of how cyberattacks evolve to impact the world in parallel with military conflict on the ground. Power systems, telecommunication systems, media, and other critical infrastructure all became targets of both physical attacks and cyberattacks. Network compromise attempts commonly observed as part of espionage and information exfiltration campaigns became focused in hybrid war on destructive wiper malware attacks against critical infrastructure systems. Connecting the security of these systems to the cloud resulted in early detection and disruption of potentially devastating attacks.[1]

For the first time in a major cyber event, behavioral detections leveraging machine learning used known attack patterns to successfully identify and stop further attacks without prior knowledge of the underlying malware—even before humans were aware of the threats. We also confirmed the value of sharing threat intelligence in real-time with defenders protecting these systems, giving them vital information to anticipate and defend against active attacks.

Nation state threat actors around the world continue to expand their operations in new and old ways. China, North Korea, Iran, and Russia all carried out attacks on Microsoft customers. The IT services supply chain became a common target as actors shifted the focus to upstream services that can be access points to multiple organizations. We expect actors to continue to exploit trusted relationships in enterprise supply chains, emphasizing the importance of comprehensive enforcement of authentication rules, diligent patching, and account configuration for remote access infrastructure, and frequent audits of partner relationships to verify authenticity.

Nation state actors, much like ransomware and criminal operators, have responded to increased exposure by moving toward targeting poorly configured or unpatched enterprise systems (VPN/VPS infrastructure, on-premises servers, third-party software) to perform living-off-the-land attacks. Many have increased use of commodity malware and open source red team tools to obfuscate their malicious activity.

As a result, maintaining a strong baseline of IT security hygiene through prioritized patching, enabling anti-tamper features, using attack surface management tools like RiskIQ to get an outside-in view of an attack surface, and enabling multifactor authentication across the full enterprise have become baseline fundamentals to proactively defend against many sophisticated actors.

Nation state actors have also increased use of ransomware as a tactic in their attacks, often reusing ransom malware created by that criminal ecosystem in their attacks. We have seen both Iran- and North Korea-based actors, leveraging commodity ransomware tools to damage targeted systems, often including critical infrastructure, within regional rivals. Finally, we have seen the growing threat of cyber mercenaries developing and selling tools, techniques, and services to extend exploits against vulnerable third-party solutions. The sophistication and agility of attacks by nation state actors will continue to evolve each year. Organizations must respond by being informed of these actor changes and evolve defenses in parallel.

John Lambert
Corporate Vice President and Distinguished Engineer, Microsoft Threat Intelligence Center

Background on nation state data

Nation state threats are cyber threat activities that originate in a specific country with the apparent intent of furthering national interests. Nation state actors present some of the most advanced and persistent threats our customers face, including intellectual property theft, espionage, surveillance, credential theft, destructive attacks, and more.

We invest significant resources in discovering, understanding, and countering these threats. When an organization or individual account holder is targeted or compromised by observed nation state activities, Microsoft delivers an alert in the form of a nation state notification (NSN) directly to the customer, including the information they need to investigate the activity. As of June 2022, we had delivered over 67,000 NSNs since we began in 2018.

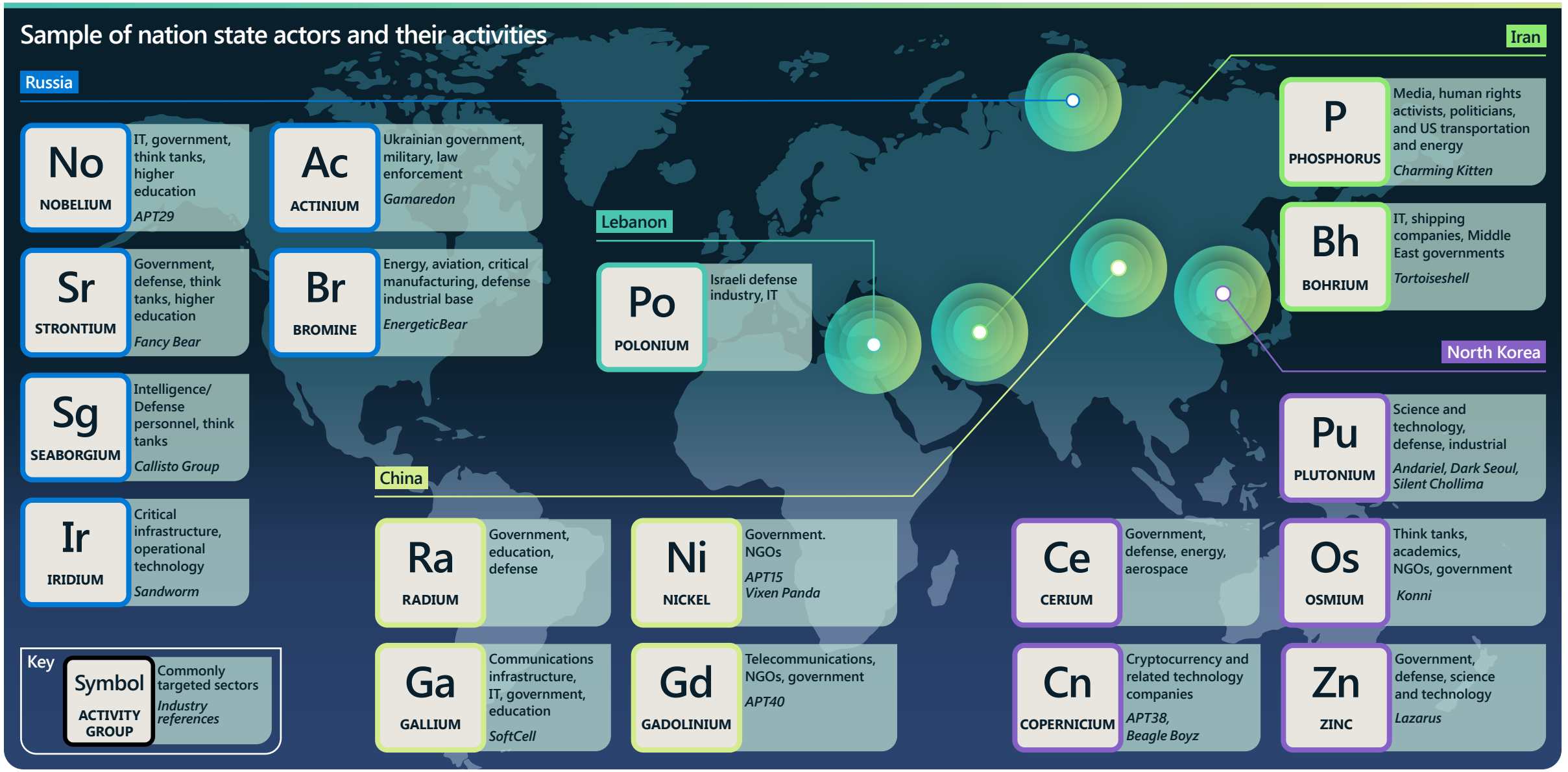
Microsoft NSN alert data are presented in this chapter to provide a view of measurable activity. The level of nation state activity shown in the charts is based on the number of NSNs Microsoft issued to customers in response to the detection of nation state actors targeting or compromising at least one account in the customer organization.

The four primary nation states whose threat groups we include in this report are Russia, China, Iran, and North Korea. These represent the countries of origin for the most commonly observed actors targeting Microsoft customers over the past year. The report also includes our observations about threat groups from Lebanon and from cyber mercenaries, or private sector offensive actors for hire.

Microsoft identifies nation state groups by chemical element names (such as NOBELIUM), just some of which are shown on the following page. We use DEV-#### designations as a temporary name given to an unknown, emerging, or developing cluster of threat activity, allowing us to track it as a unique set of information until we reach a high degree of confidence about the origin or identity of the actor behind the activity.

Once it meets the criteria, a DEV is converted to a named actor or merged with existing actors. Throughout this chapter, we cite examples of nation state and DEV groups to provide a deeper view into attack targets, techniques, and analysis of motivations. Although many of these groups use the same tools as cybercriminals, they present unique threats in the form of bespoke malware, the ability to discover and capitalize on zero-day vulnerabilities, and legal impunity.

https://t.me/learningnets



https://t.me/learningnets

The evolving threat landscape

Microsoft's mission to track nation state actor activity and notify customers when we see them being targeted or compromised is rooted in our mission to protect our customers from attacks.

This notification is a crucial part of our commitment to informing customers whether observed attacks are successfully prevented by our security product protections, or if the attacks are effective because of unknown security weaknesses. Tracking notifications over time helps Microsoft identify evolving threat trends by actors and focus product protections on proactively mitigating threats to customers across our cloud services.

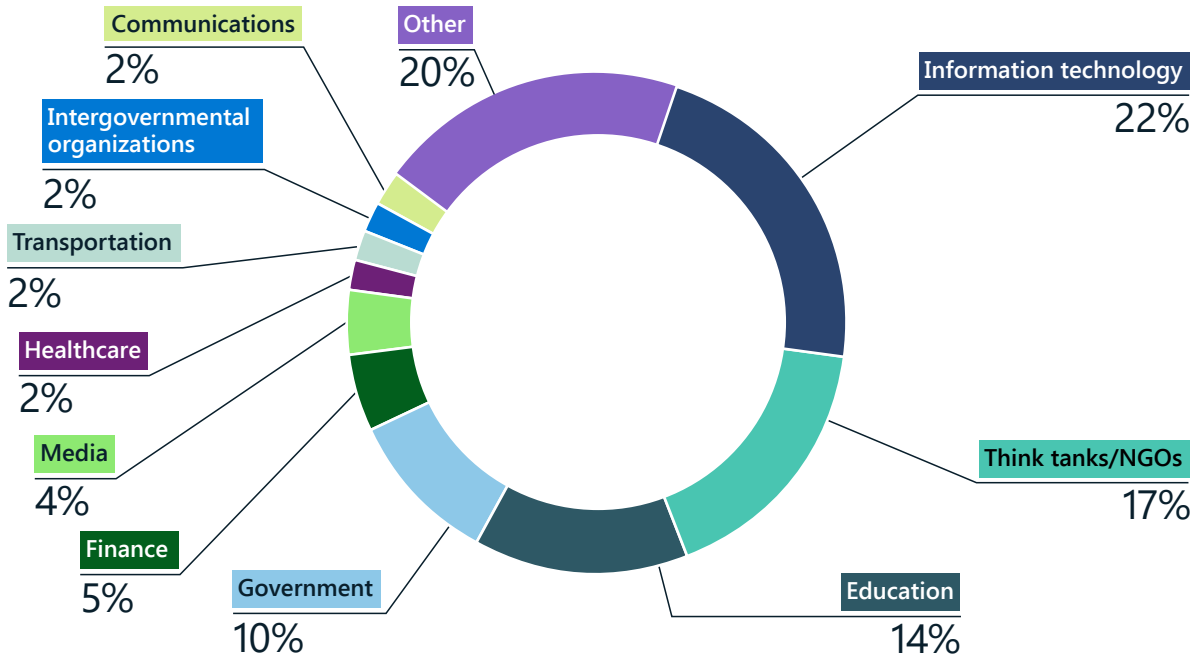
This tracking also allows us to share data and insights about what we see. The analysts tracking these actors and following their attacks rely on a combination of technical indicators and geopolitical expertise to understand the motivations of the actors, combining technical and global context into new insights. This curation provides a unique view into the priorities of nation state cyber actors and how their motivations might mirror the political, military, and economic priorities of the nation states employing them.

Political developments in the past year have shaped the priorities and risk tolerance of state-sponsored threat groups worldwide. As geopolitical relationships have broken down and hawkish elements have acquired more control in some nations, cyber actors have become more brazen and aggressive. For example:

- Russia relentlessly targeted the Ukrainian government and the country's critical infrastructure to complement its on-the-ground military action.[2]
- Iran aggressively sought inroads into US critical infrastructure such as port authorities.
- North Korea continued its campaign of stealing cryptocurrency from financial and technology companies.
- China expanded its global cyberespionage operations.

Although nation state actors can be technically sophisticated and employ a wide variety of tactics, their attacks can often be mitigated by good cyber hygiene. Many of these actors rely on relatively low-tech means, such as spear-phishing emails, to deliver sophisticated malware instead of investing in developing customized exploits or using targeted social engineering to achieve their objectives.

Industry sectors targeted by nation state actors



Nation state groups targeted a range of sectors. Russian and Iranian state actors targeted the IT industry as a means to access the IT firms' customers. Think tanks, nongovernmental organizations (NGOs), universities, and government agencies remained other common targets of nation state actors.

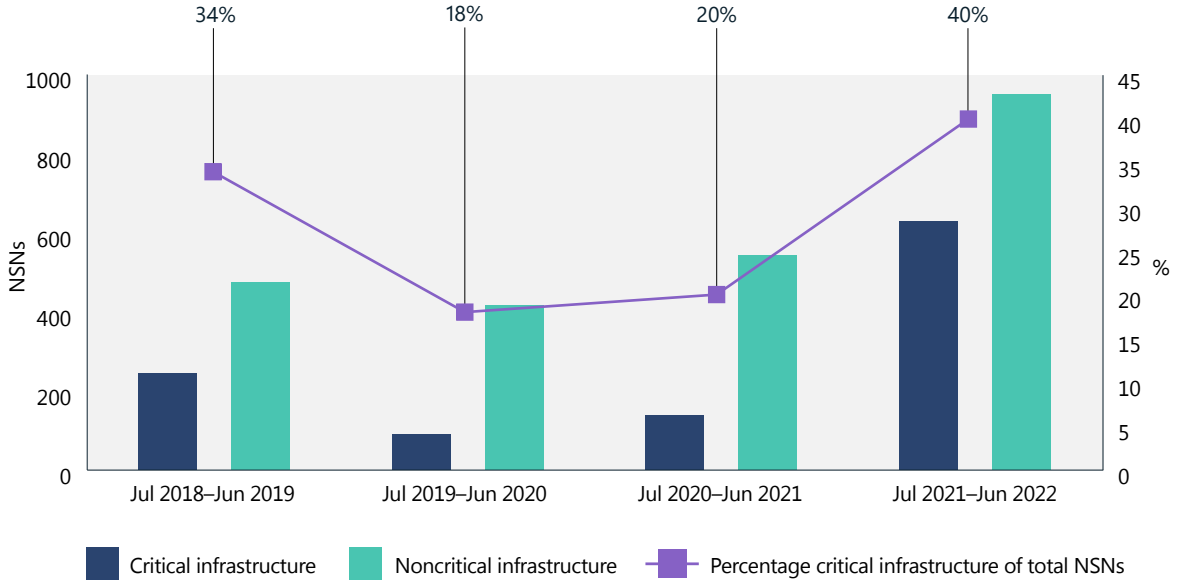
Nation state actors have a variety of objectives that can result in targeting specific groups of organizations or individuals. In the last year, supply chain attacks have increased, with a particular focus on IT companies. By compromising IT service providers, threat actors are often able to reach their original target through a trusted relationship with the company that manages connected systems, or potentially execute attacks on a much larger scale by compromising hundreds of downstream customers in one attack. After the IT sector, the most frequently targeted entities were think tanks, academics attached to universities, and government officials. These are desirable "soft targets" for espionage to collect intelligence on geopolitical issues.

https://t.me/learningnets

The evolving threat landscape

Continued

Critical infrastructure trends

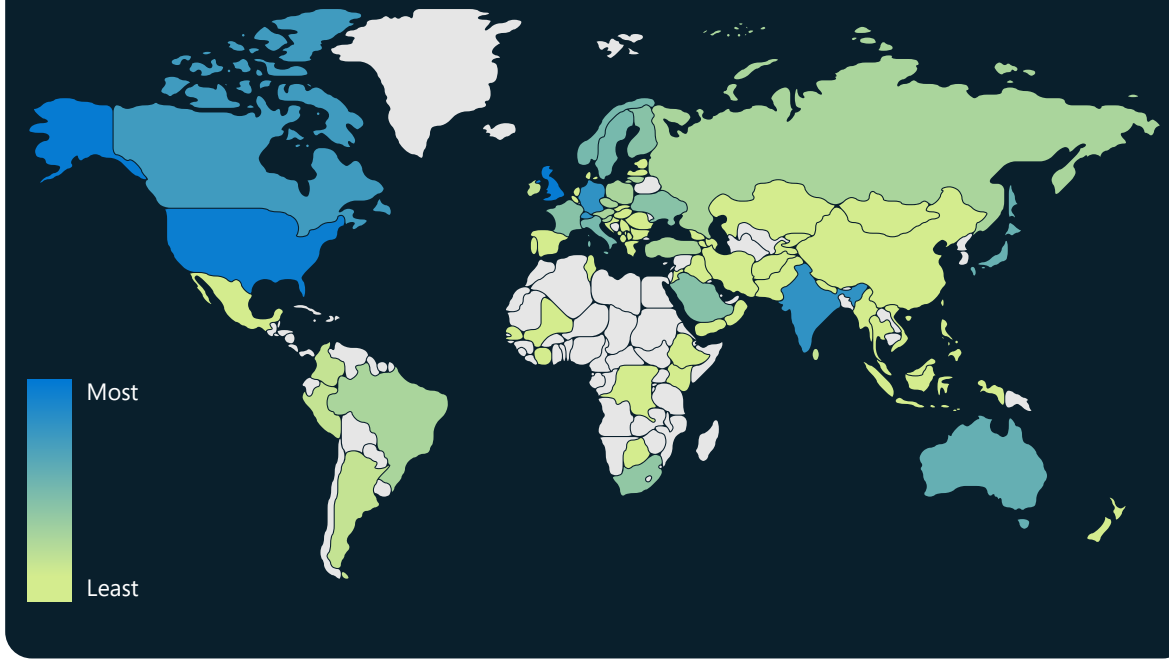


Nation state groups' targeting of critical infrastructure[3] increased in the past year, with actors' focusing on companies in the IT sector, financial services, transportation systems, and communications infrastructure.

"Before the invasion of Ukraine, governments thought that data needed to stay inside a country in order to be secure. After the invasion, migrating data to the cloud and moving outside territorial borders is now a part of resiliency planning and good governance."

Cristin Flynn Goodwin,
Associate General Counsel, Customer Security & Trust

Nation state actors' geographic targeting



Nation state groups' cyber targeting spanned the globe this past year, with a particularly heavy focus on US and British enterprises. Organizations in Israel, the UAE, Canada, Germany, India, Switzerland, and Japan were also among some of the most frequently targeted, according to our NSN data.

Actionable insights

1. Identify and protect your potential high-value data targets, at-risk technologies, information, and business operations which might align with the strategic priorities of nation state groups.
2. Enable cloud protections to provide identification and mitigation of known and novel threats to your network at scale.

https://t.me/learningnets

The IT supply chain as a gateway to the digital ecosystem

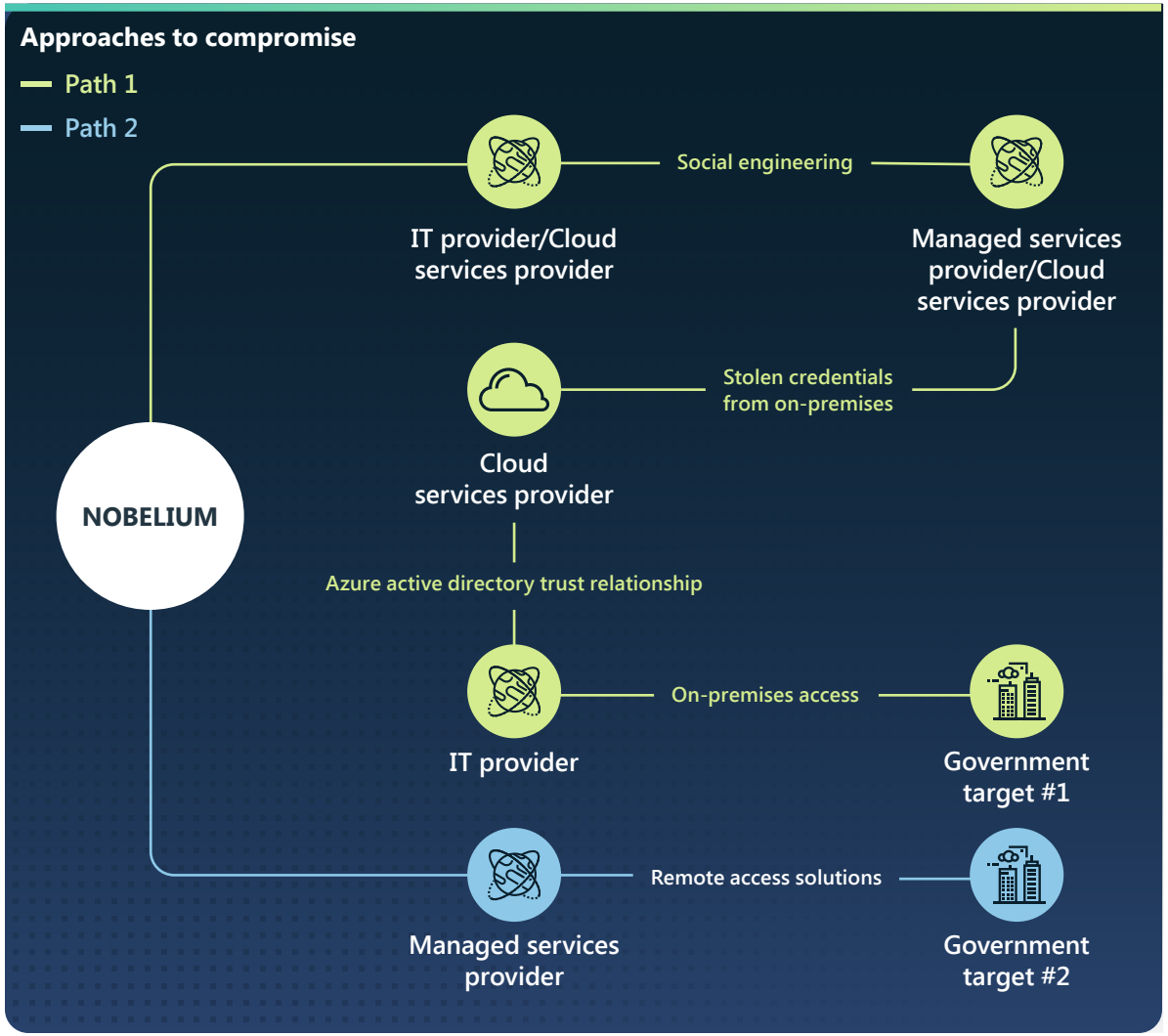
Nation state targeting of IT service providers might enable the threat actors to exploit other organizations of interest by taking advantage of trust and access granted to these supply chain providers. In the past year, nation state cyber threat groups targeted IT services providers to attack third-party targets and gain access to downstream clients in government, policy, and critical infrastructure sectors.

IT service providers are attractive intermediary targets as they serve hundreds of direct and thousands of indirect clients of interest to foreign intelligence services. If exploited, the routine business practices and the delegated administrative privileges these firms enjoy, might allow malicious actors to access and manipulate IT service provider client networks without immediately triggering alerts.

In the past year, NOBELIUM attempted to compromise and leverage privileged accounts at cloud solutions and other managed services providers to attempt targeted downstream access into primarily US and European government and policy customers.

NOBELIUM demonstrated how a "compromise one to compromise many" approach could be directed against a perceived geopolitical adversary. This past year, the threat actor pursued both third-party and direct intrusions into sensitive organizations based in member states of the North Atlantic Treaty Organization (NATO), which the Russian government perceives as an existential threat. Between July 2021 and early June 2022, 48 percent of Microsoft's customer notifications of Russian threat activity against online services customers went to IT sector firms based in NATO member countries, likely as intermediary access points. Overall, 90 percent of notifications about Russian threat activity during the same period went to customers based in NATO member states, primarily in the IT, think tanks and nongovernmental organizations (NGOs), and government sectors, suggesting a strategy of pursuing multiple means of initial access to these targets.

There has been a shift from exploiting the software supply chain to exploiting the IT services supply chain, targeting cloud solutions and managed services providers to reach downstream customers.



This diagram depicts NOBELIUM's multi-vectored approach to compromising its ultimate targets and the collateral damage to other victims along the way. In addition to the actions shown above, NOBELIUM launched password spray and phishing attacks against the entities involved, even targeting the personal account of at least one government employee as another potential route to compromise.

https://t.me/learningnets

The IT supply chain as a gateway to the digital ecosystem

Continued

Throughout the year, Microsoft Threat Intelligence Center (MSTIC) detected an increasing number of Iranian state and Iran-affiliated actors compromising IT companies. In many cases, actors were detected stealing sign-in credentials to gain access to downstream clients for a range of objectives, from intelligence collection to retaliatory destructive attacks.

- In July and August 2021, DEV-0228 compromised an Israeli business software provider to later compromise downstream customers in the Israeli defense, energy, and legal sectors.[4]
- From August to September 2021, Microsoft detected a spike in Iranian state actors targeting IT companies based in India. The lack of pressing geopolitical issues that would have prompted such a shift suggests this targeting is for indirect access to subsidiaries and clients outside India.
- In January 2022, DEV-0198, a group we assess is affiliated with the government of Iran, compromised an Israeli cloud solutions provider. Microsoft assesses the actor likely used compromised credentials from the provider to authenticate into an Israeli logistics company. MSTIC observed the same actor attempting to conduct a destructive cyberattack against the logistics company later that month.
- In April 2022, POLONIUM, a Lebanon-based group we assess collaborated with Iranian state groups on IT supply chain techniques, compromised another Israeli IT company to gain access to Israeli defense and legal organizations.[5]

This past year of activity demonstrates that threat actors like NOBELIUM and DEV-0228 are getting to know the landscape of an organization's trusted relationships better than the organizations themselves. This increased threat emphasizes the need for organizations to understand and harden the borders and entry points of their digital estates. It also underscores the importance for IT service providers to rigorously monitor their own cybersecurity health. For example, organizations should implement multifactor authentication and conditional access policies that make it harder for malicious actors to capture privileged accounts or spread throughout a network.

Conducting a thorough review and audit of partner relationships helps minimize any unnecessary permissions between your organization and upstream providers and immediately remove access for any relationships that look unfamiliar. Increasing familiarity with activity logs and reviewing available activity makes it easier to spot anomalies that could spark further investigation.

> Nation state targeting of third parties enables them to exploit sensitive organizations by taking advantage of trust and access in a supply chain.

Actionable insights

1. Review and audit upstream and downstream service provider relationships and delegated privilege accesses to minimize unnecessary permissions. Remove access for any partner relationships that look unfamiliar or have not yet been audited.[6]
2. Enable logging and review all authentication activity for remote access infrastructure and virtual private networks (VPNs), with a focus on accounts configured with single factor authentication, to confirm authenticity and investigate anomalous activity.
3. Enable MFA for all accounts (including service accounts) and ensure MFA is enforced for all remote connectivity.
4. Use passwordless solutions to secure accounts.[7]

Links to further information

- NOBELIUM targeting delegated administrative privileges to facilitate broader attacks | Microsoft Threat Intelligence Center (MSTIC)
- Iranian targeting of IT sector on the rise | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit
- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC)

https://t.me/learningnets

Rapid vulnerability exploitation

As organizations strengthen their cybersecurity postures, nation state actors respond by pursuing new and unique tactics to deliver attacks and evade detection. The identification and exploitation of previously unknown vulnerabilities—known as zero-day vulnerabilities—is a key tactic in this effort.

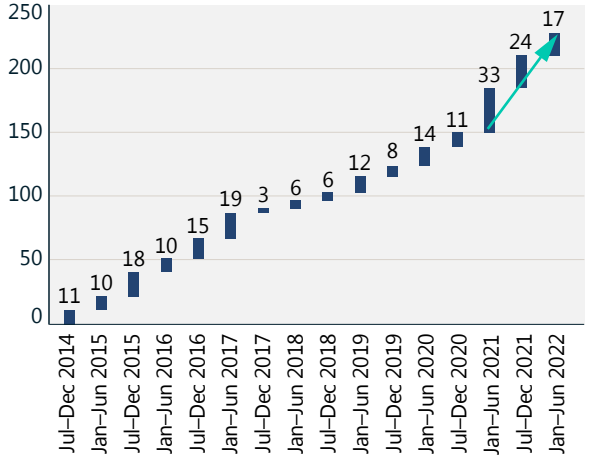
Zero-day vulnerabilities are a particularly effective means for initial exploitation and, once publicly exposed, vulnerabilities can be rapidly reused by other nation state and criminal actors. The number of publicly disclosed zero-day vulnerabilities over the past year is on par with those from the previous year, which was the highest on record.

As cyber threat actors—both nation state and criminal—become more adept at leveraging these vulnerabilities, we have observed a reduction in the time between the announcement of a vulnerability and the commoditization of that vulnerability. This makes it essential that organizations patch exploits immediately. Similarly, it is critical that organizations or individuals that uncover new vulnerabilities responsibly disclose or report them to affected vendors as soon as possible, in line with coordinated vulnerability disclosure procedures.

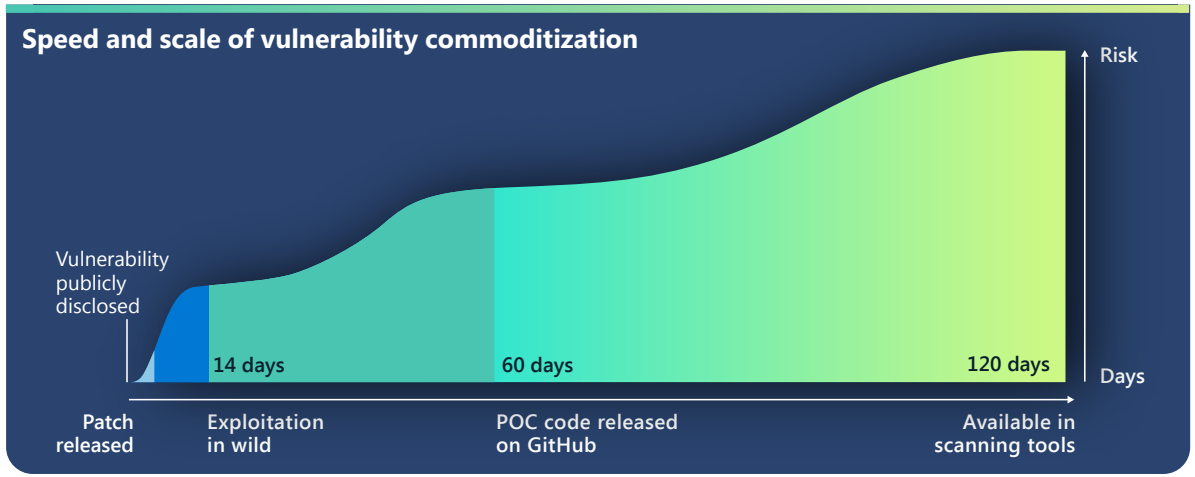
This ensures that vulnerabilities are identified, and patches developed in a timely manner to protect customers from previously unknown threats.

Many organizations assume they are less likely to be a victim of zero-day exploit attacks if vulnerability management is integral to their network security. However, the commoditization of exploits is leading them to come at a much faster rate. Zero-day exploits are often discovered by other actors and reused broadly in a short period of time, leaving unpatched systems at risk. Even though zero-day exploitation can be difficult to detect, actors' post-exploit actions are often easier to detect and, if coming from fully patched software, can act as a warning sign of a compromise.

Patches released for zero-day vulnerabilities



Numbers of publicly disclosed zero-day exploits from the List of Common Vulnerabilities and Disclosures (CVEs).



On average, it takes only 14 days for an exploit to be available in the wild after a vulnerability is publicly disclosed. This view provides an analysis of the timelines of exploitation of zero-day vulnerabilities, along with the number of systems vulnerable to the given exploit and active on the internet from the time of first public disclosure.

While zero-day vulnerability attacks tend to initially target a limited set of organizations, they are quickly adopted into the larger threat actor ecosystem. This kicks off a race for threat actors to exploit the vulnerability as widely as possible before their potential targets install patches.

While we observe many nation state actors developing exploits from unknown vulnerabilities, China-based nation state threat actors are particularly proficient at discovering and developing zero-day exploits. China's vulnerability reporting regulation went into effect September 2021, marking a first in the world for a government to require the reporting of vulnerabilities into a government authority for review prior to the vulnerability being shared with the product or service owner. This new regulation might enable elements in the Chinese government to stockpile reported vulnerabilities toward weaponizing them. The increased use of zero days over the last year from China-based actors likely reflects the first full year of China's vulnerability disclosure requirements for the Chinese security community and a major step in the use of zero-day exploits as a state priority. The vulnerabilities described below were first developed and deployed by China-based nation state actors in attacks, before being discovered and spread among other actors in the larger threat ecosystem.

https://t.me/learningnets

Rapid vulnerability exploitation

Continued

Even organizations that are not a target of nation state attacks have a limited period to patch zero-day vulnerabilities in impacted systems before they are exploited by the broader actor ecosystem.

These examples of newly identified vulnerabilities demonstrate that organizations have on average 60 days from the time a vulnerability is patched and a proof of concept (POC) code is made available online, and often picked up by other actors for reuse. Similarly, organizations have on average 120 days before a vulnerability is available in automated vulnerability scanning and exploitation tools such as Metasploit—which often result in the exploit being used on a massive scale. This highlights that even organizations that are not a target of nation state threat actors have a limited period to patch zero-day vulnerabilities in impacted systems before the vulnerabilities are exploited by the broader actor ecosystem.

CVE-2021-35211 SolarWinds Serv-U

In July 2021, SolarWinds released a security advisory for CVE-2021-35211, crediting Microsoft with the notification.[8] At the time, we discovered nation state aligned threat actor DEV-0322 actively exploiting the SolarWinds Serv-U vulnerability. Our RiskIQ team observed 12,646 IP addresses hosting internet connected versions of the impacted devices between June 15 and July 9.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

In September 2021, our researchers observed China-affiliated actors exploiting Zoho ManageEngine at several US-based entities. The vulnerability was publicly reported on September 6 as CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, which organizations typically use to handle password resets.[9] DEV-0322 exploited the vulnerability later in September, using it as an initial vector to gain a foothold in networks and performing additional actions including credential dumping, installing custom binaries, and dropping malware to maintain persistence. At the time of disclosure, RiskIQ observed 4,011 instances of these systems active and on the internet.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

In late October 2021, we observed DEV-0322 leveraging a vulnerability (CVE-2021-44077) in a second Zoho ManageEngine product, ServiceDesk Plus—an IT help-desk software with asset management. DEV-0322 used this vulnerability to target and compromise entities in healthcare, information technology, higher education, and critical manufacturing sectors. On December 2, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint advisory warning to the public about nation state threat actors leveraging the vulnerability. At the time of disclosure, RiskIQ observed 7,956 instances of these systems active and on the internet.

CVE-2021-42321 Microsoft Exchange

A zero-day exploit for an Exchange vulnerability CVE-2021-42321 was revealed during the Tianfu Cup, an international cybersecurity summit and hacking competition held October 16 and 17, 2021 in Chengdu, China. Security researchers at Microsoft observed the exploit for the Exchange vulnerability used in the wild on October 21, only three days after the vulnerability was revealed. At the time of disclosure, RiskIQ observed 61,559 instances of these systems active and on the internet, at the time of disclosure. We continued to observe exploitation activity into November 2021.

CVE-2022-26134 Confluence

A China-affiliated actor likely had the zero-day exploit code for the Confluence vulnerability (CVE-2022-26134) four days before the vulnerability was publicly disclosed on June 2, and likely leveraged it against a US-based entity. At the time of disclosure, RiskIQ observed 53,621 instances of vulnerable Confluence systems on the internet.

Vulnerabilities are being picked up and exploited on a massive scale, and in increasingly shorter timeframes.

Actionable insights

1. Prioritize patching of zero-day vulnerabilities as soon as they are released; don't wait for the patch management cycle to deploy.
2. Document and inventory all enterprise hardware and software assets to determine risk and to quickly determine when to act on patches.

https://t.me/learningnets

Russian state actors' wartime cyber tactics threaten Ukraine and beyond

This year saw Russian state actors launching cyber operations to complement military action during Russia's invasion of Ukraine, often using the same tactics and techniques deployed against targets outside of Ukraine. It is critical that organizations worldwide take measures to harden cybersecurity against digital threats stemming from Russia-aligned threat actors.

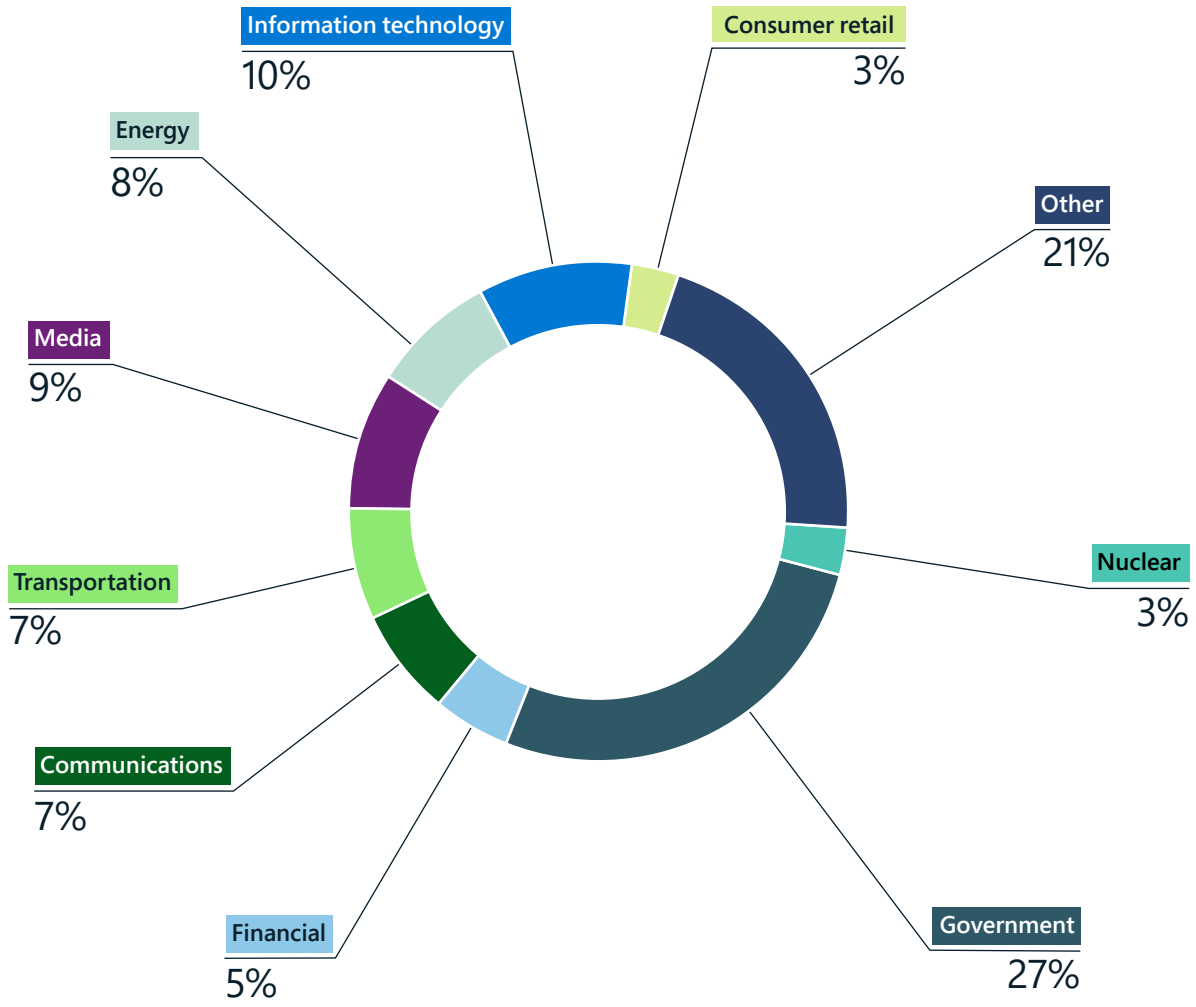
The situation on the ground continues to fluctuate as the military conflict persists, and Ukraine and its allies should be prepared to defend themselves if Russian state cyber operators increase the frequency or intensity of intrusions in line with military objectives. During the first four months of the war, Microsoft observed threat actors associated with the Russian military launch multiple waves of destructive cyberattacks against nearly 50 distinct Ukrainian agencies and enterprises and espionage-focused intrusions against many others. Excluding operations against online services customers, 64 percent of Russian threat activity against known targets was directed at Ukraine-based organizations between late February and June.

In each operation, Russian threat actors employed many of the tactics, techniques, and procedures (TTPs) we observed being used before invasion against targets both within and outside of Ukraine. These actors intended to destroy data and put Ukrainian government agencies off balance in the initial period of the conflict. They have since sought to derail the transport of military and humanitarian assistance to Ukraine, disrupt public access to services and media, and steal information of longer-term intelligence or economic value to Russia.

Targeting transportation threatens an area of critical importance to Ukrainian citizens trying to survive the conflict. According to a UNICEF-sponsored survey in May, respondents in conflict-affected urban areas were most worried about transport and fuel, supply disruptions, security, and limited access to food, medical services, and financial services.[10] In June, the UN Crisis Coordinator for Ukraine said at least 15.7 million people in Ukraine were in urgent need of humanitarian assistance, and the number would grow as the war continues.[11]

Outside of Ukraine, Microsoft detected Russian network intrusion efforts against 128 organizations in 42 countries between late February and June. The United States was Russia's number one target. Poland, through which much of the international military and humanitarian assistance to Ukraine transits, was also a significant target during this period. Threat actors affiliated with the Russian state pursued organizations in Baltic countries and computer networks in Denmark, Norway, Finland, and Sweden in April and May as well.

Most targeted industry sectors in Ukraine since the invasion



Federal, state, and local government organizations in Ukraine have remained priority targets for Russian state and state-affiliated threat groups throughout the conflict. The focus on transportation, energy, financial, and media sector organizations highlight the risk that these cyber operations pose to services on which Ukrainian citizens rely.

https://t.me/learningnets

Russian state actors' wartime cyber tactics threaten Ukraine and beyond

Continued

We have seen an increase in similar activity targeting the foreign ministries of NATO countries.

Russian state threat groups remained interested in compromising critical infrastructure both within and outside of Ukraine this past year. IRIDIUM deployed the Industroyer2 malware in a failed effort to leave millions of people in Ukraine without power. Outside of Ukraine, BROMINE conducted intrusions against organizations involved in manufacturing, and industrial control systems in early 2022.

Russian state and state-affiliated actors directed cyber operations against Ukraine, its allies, and other targets of intelligence value this year using many of the following TTPs:

Spear phishing with malicious attachments or links

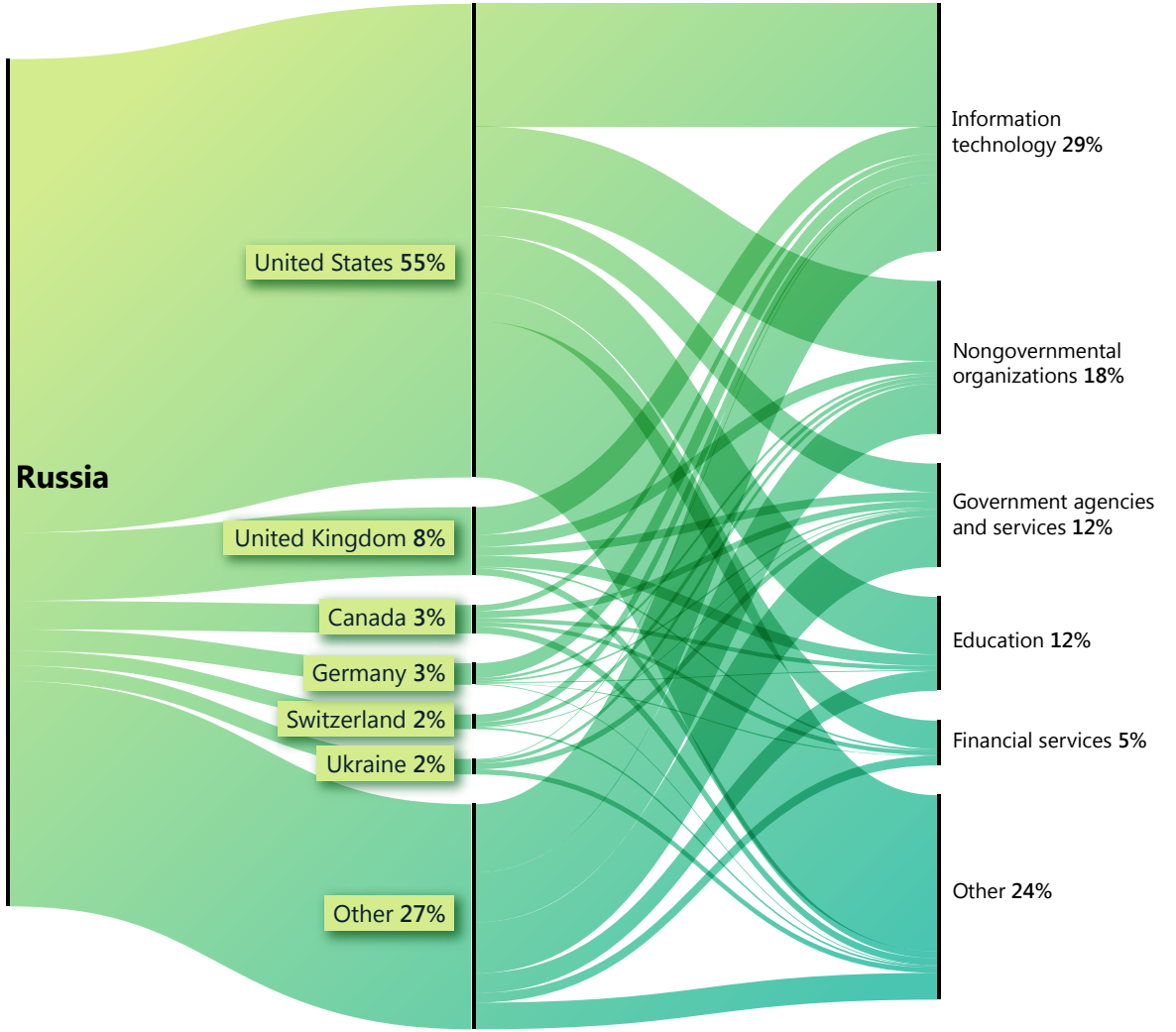
Russian state and Russia-affiliated groups like ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM, and IRIDIUM all used phishing campaigns to gain initial access to desired accounts and networks in organizations within and outside Ukraine. Many campaigns utilized compromised or spoofed accounts at targeted organizations or within the same industry and compelling themes to lure victims. NOBELIUM used compromised diplomatic accounts to send phishing mail disguised as diplomatic communications to foreign ministry employees across the globe. STRONTIUM created spoof accounts based on publicly available names of account holders at think tanks in the United States and sent phishing messages to gain access to accounts at those think tanks. SEABORGIUM phished using lures related to reporting on the Ukraine conflict to gain initial access to accounts at international affairs think tanks in the Nordic countries.

Exploitation of IT services supply chain to impact downstream customers

In late 2021, Russian state actors compromised IT services providers and used the access to facilitate website defacements and the deployment of Whispergate destructive malware by DEV-0586 in January.[12] DEV-0586 also compromised the network of an IT firm that built resource management systems for Ukraine's Ministry of Defense and other organizations in the communications and transportation sectors, indicating the group was exploring third-party attack options in those sectors as well.

Worldwide, but especially in the United States and Western Europe, NOBELIUM targeted IT services providers to gain access to government and other sensitive networks throughout 2021–2022 (see the discussion of supply chain vulnerabilities earlier in this chapter).

Russia: Top targeted countries and industry sectors



Despite an intensified focus on Ukraine-based organizations since early 2022, enterprises based in North America and Western Europe were still the online service customers Russian actors targeted most. NOBELIUM's campaign against the IT sector made it the most targeted sector this past year.

https://t.me/learningnets

Russian state actors' wartime cyber tactics threaten Ukraine and beyond

Continued

Exploitation of public-facing applications to gain initial access to networks

Since at least late 2021, STRONTIUM worked to develop and refine its capabilities to exploit public-facing services, such as Microsoft Exchange servers, to steal information. STRONTIUM exploited unpatched Exchange servers to access Ukrainian government accounts as well as military and defense industry-related organizations in the United States, Lebanon, Peru, and Romania, and other government agencies based in Armenia, Bosnia, Kosovo, and Malaysia. DEV-0586, also affiliated with the Russian military, exploited Confluence server vulnerabilities to gain initial access to government and IT sector organizations in Ukraine and other Eastern European countries.

Russian state and affiliated threat actors use many of the same TTPs to compromise organizations of interest during times of war and peace.

Use of administrative accounts and protocols, and native utilities for network discovery and lateral movement

After gaining initial access to a network, Microsoft observed Russian state actors leveraging legitimate accounts and software utilities used to perform basic maintenance tasks to evade detection for as long as possible. They relied on compromised identities with administrative capabilities and valid administration protocols, tools, and methods to move laterally within networks without immediately attracting the attention of automated monitors and network defenders.

Basic cyber hygiene and employment of endpoint detection and response tools can help mitigate the negative impact of these types of operations in peacetime as well as during times of war.

The unpredictability of the ongoing conflict demands that organizations worldwide take measures to harden cybersecurity against digital threats stemming from Russian state and Russia-affiliated threat actors.

Actionable insights

1. Minimize credential theft and account abuse by protecting the identities of your users by implementing MFA identity protection tools and enforcing least privilege access to secure the most sensitive and privileged accounts and systems.
2. Apply updates to ensure all your systems get the highest level of protection as soon as possible and are kept up to date.
3. Deploy anti-malware, endpoint detection, and identity protection solutions across your organization. A combination of defense-in-depth security solutions, paired with trained and capable personnel, can empower your organization to identify, detect, and prevent intrusions impacting your business.
4. Enable investigations and recovery in the event you detect or receive notification of a threat to your environment by backing up critical systems and enabling logging. Establishing an incident response plan is strongly encouraged.

Links to further information

- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- The hybrid war in Ukraine | Microsoft On the Issues
- Cyber threat activity in Ukraine: analysis and resources | Microsoft Security Response Center (MSRC)
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues
- Malware attacks targeting Ukraine government | Microsoft On the Issues
- MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

https://t.me/learningnets

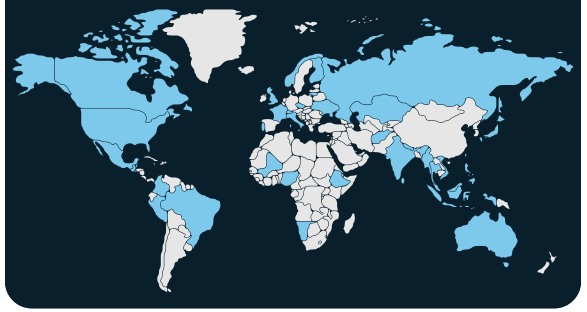
China expanding global targeting for competitive advantage

In today's complex geopolitical climate, Chinese state and state-affiliated threat actors conducting cyber operations often aim to further the country's strategic military, economic, and foreign relations goals as part of China's objective to attain competitive advantage. In the last year, Microsoft has observed widespread Chinese threat activity targeting countries around the world.

Since mid-2021, China has been maneuvering to ensure economic and financial stability amid the worst COVID-19 surge in two years.[13] China continued to juggle their position on geopolitical events, such as the struggle to balance their "limitless" partnership with Russia,[14] and maintain their position on the world stage.[15] In addition, China's stance against the United States and its allies over Taiwan[16] and the South China sea continued to strain foreign relations with many countries.[17]

Chinese state and state-affiliated threat groups increased targeting of smaller nations around the globe with a focus on Southeast Asia to gain competitive advantage on all fronts.

Countries targeted by Chinese state and state-affiliated groups

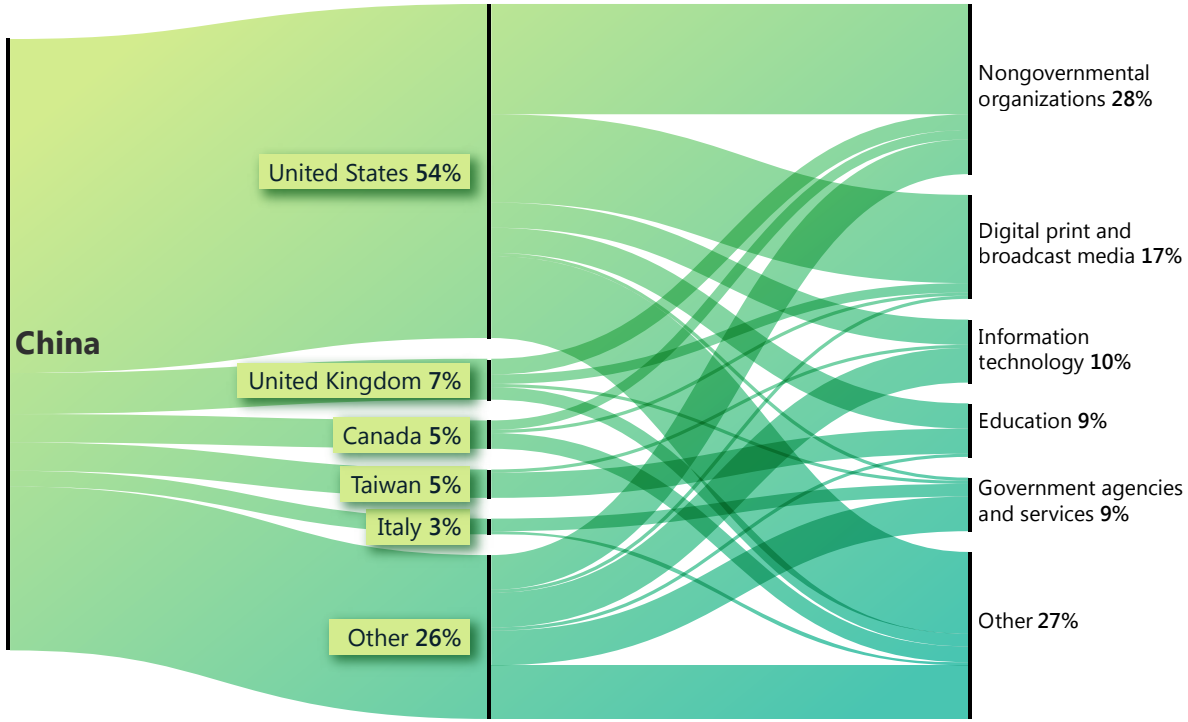


China also continued expanding its economic influence globally through previously established Belt and Road Initiatives (BRI), attempting to revive a comprehensive investment framework with the EU,[18] and negotiating a new regional trade agreement with 15 countries in Asia Pacific known as the Regional Comprehensive Economic Partnership.[19] Microsoft assesses China will continue to utilize cyber collection as a tool to help advance its strategic political, military, and economic goals due to observed cyber operations and the breadth of entities targeted.

Cyber targeting likely to advance economic and military interests.

Microsoft observed widespread targeting of smaller nations around the world by Chinese state and state-affiliated threat groups, suggesting China is likely using cyberespionage as a component of its global economic and military influence.

China: Top targeted countries and industry sectors



Think tanks/NGOs, media, IT, government, and education sectors were among the most targeted sectors for China-based threat groups, probably for persistent intelligence collection and reconnaissance.

The span of targets included, but were not limited to, countries in Africa, the Caribbean, the Middle East, Oceania, and South Asia, with a particular focus on those countries in Southeast Asia, and the Pacific Islands.

In line with China's BRI strategy, China-based threat groups targeted entities in Afghanistan, Kazakhstan, Mauritius, Namibia, and Trinidad and Tobago.[20] For example, Trinidad and Tobago was the first Caribbean country to endorse China's BRI strategy in 2018, and China considers it an important partner in the region. NICKEL has had persistent network operations targeting Trinidad and Tobago since 2021. For instance, in March 2022, NICKEL conducted reconnaissance activities targeting a government agency, likely for intelligence collection purposes.

https://t.me/learningnets

China expanding global targeting for competitive advantage

Continued

Meanwhile, Microsoft observed Chinese state and state-affiliated threat groups focusing their network operations against entities in Southeast Asia and expanding to Pacific Island countries as China shifted its military and economic priorities to cope with the challenges of the United States' renewed interest in the region. In January 2022, Microsoft observed RADIUM targeting an energy company and an energy-associated government agency in Vietnam, and an Indonesian government agency. RADIUM's activities likely aligned with China's strategic goals in the South China Sea.[21] In late February and early March, GALLIUM compromised more than 100 accounts affiliated with a prominent intergovernmental organization (IGO) in the Southeast Asia region. The timing of GALLIUM's targeting of the IGO in the region coincided with the announcement of a scheduled meeting between the United States and regional leaders. GALLIUM actors were likely tasked to monitor communications and collect intelligence before the event.

As China expanded its influence in Pacific Island countries, Chinese threat groups' activities followed. In April, China and the Solomon Islands signed a security agreement intended to "promote peace and security." The agreement potentially allows China to deploy armed police and military to the Solomon Islands.[22] In May, China hosted the second China-Pacific Island Countries (PICs) Foreign Ministers' Meeting in Fiji and proposed to advance a "comprehensive strategic partnership" to further political, cultural, social, security, and climate change interests and also to fight the pandemic.[23] Around the same time in May, Microsoft identified GADOLINIUM's malware on Solomon Islands government systems. RADIUM also ran malicious code on systems of a telecommunications company in Papua New Guinea. We assess these activities were likely for intelligence collection purposes to support China's overall regional strategy.

Microsoft disrupts NICKEL operations, but the threat group shows its persistence.

In December 2021, the Microsoft Digital Crimes Unit (DCU) filed pleadings with the US District Court for the Eastern District of Virginia seeking authority to seize 42 command and control (C2) domains controlled by NICKEL. These C2 domains were used in operations against governments, diplomatic entities, and NGOs across Central and South America, the Caribbean, Europe, and North America since September 2019.[24] Through these operations, NICKEL achieved long-term access to several entities and consistently exfiltrated data from some victims since late 2019.

As China continues to establish bilateral economic relations with more countries—often in agreements associated with BRI—China's global influence will continue to grow. We assess Chinese state and state-affiliated threat actors will pursue targets in their government, diplomatic, and NGO sectors to gain new insights, likely in pursuit of economic espionage or traditional intelligence collection objectives. Since Microsoft's disruption, NICKEL has targeted several government agencies, likely trying to regain lost access. Between late March and May 2022, NICKEL re-compromised at least five government agencies across the globe. This suggests the group had additional entry points to those entities or regained access through new C2 domains. NICKEL's persistence in repeatedly compromising the same government agencies globally indicates the importance of the task at a high level.

China is being more assertive with their stance on foreign policy. We assess cyber-enabled economic espionage and intelligence collection will likely continue.

Actionable insights

1. Boost cyber defense to mitigate cyber threats proactively. The persistence of Chinese threat actors requires organizations to identify, protect, detect, and respond possible intrusions in a timely fashion.
2. Threat actors abuse scheduled tasks[25] as a common method of persistence and defense evasion, ensure your environment employs additional security guidelines to protect against this commonly used technique.[26]
3. We continue to observe the use of web shells as an initial vector into targeted networks.[27] Organizations should harden their systems against web shells attacks that can provide attackers access to run remote commands.[28]

Links to further information

- NICKEL targeting government organizations across Latin America and Europe | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Protecting people from recent cyberattacks | Microsoft On the Issues

https://t.me/learningnets

Iran growing increasingly aggressive following power transition

Microsoft has observed Iranian state groups and affiliated actors increase the pace and scope of cyberattacks against Israel, expand ransomware attacks beyond regional adversaries to US and EU victims, and target high profile US critical infrastructure to at least pre-position for potential destructive cyberattacks.

Iranian state actors' growing cyber aggression has followed a transition of its presidential power. In the summer of 2021, hardline President Ibrahim Raisi replaced moderate President Hassan Rouhani. In sharp contrast to Raisi, who is a protégé of the Supreme Leader and a close ally of the Islamic Revolutionary Guard Corps (IRGC), former President Rouhani's penchant for diplomacy often brought him at odds with the Supreme Leader and IRGC senior leaders.[29] The hawkish views of the Raisi administration appear to have raised the willingness of Iranian actors to take bolder action against Israel and the West, particularly the United States, despite the resumption of diplomatic engagement to revive the nuclear deal with Iran.

Increased pace and scope of Iranian cyberattacks against Israel

Within weeks of Raisi completing the formation of his foreign policy team,[30] Iranian state actors resumed destructive cyberattacks against Israel at a faster pace than the prior year. These ransomware and hack-and-leak attacks were conducted every few weeks beginning in September and involved at least three Iran-affiliated actors, suggesting the attacks might have been part of a nationwide campaign of retaliation against Israel. In at least one case, Microsoft assessed a ransomware attack against an Israeli organization in late 2021 was meant to conceal an underlying data deletion attack. Microsoft malware analysis determined the ransomware delivered to the victim was programmed to execute wiper malware following encryption.

By 2022, Iranian cyberattacks escalated in target selection and form of attacks. In February, DEV-0198 attempted to conduct a destructive attack against Israeli critical infrastructure. Microsoft also assesses an Iran-affiliated actor was most likely responsible for a sophisticated cyberattack that set off emergency rocket sirens in Israel in June probably by using software that adjusts audio over IP networks.

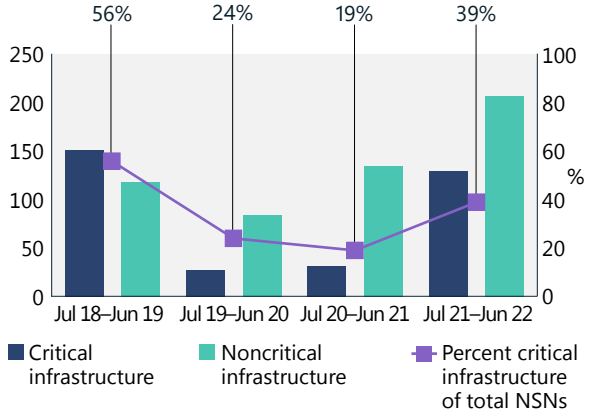
Iranian threat to US and Israeli critical infrastructure mounted throughout the year

Iranian state actors Microsoft assesses are affiliated with the IRGC (PHOSPHORUS and DEV-0198) targeted high-profile US and Israeli critical infrastructure from late 2021 to mid-2022. The likely aim was to provide Tehran with options to retaliate against the same sectors that senior IRGC officials blamed the United States and Israel for disrupting in Iran.[31] We assess this activity is tied to statements in late October 2021 by IRGC General Gholamreza Jalali, head of Iran's Passive Defense Organization, who echoed accusations from other influential figures within the regime that the United States and Israel conducted cyberattacks on Iran's ports, railways, and fueling stations.[32] Jalali delivered this accusation a second time in prepared remarks during a staged Friday prayer speech at a podium with the image of a missile striking the words "USA," suggesting his seniors held the same view.[33]

PHOSPHORUS began widespread scanning of US organizations in October 2021 for unpatched Fortinet and ProxyShell vulnerabilities. Once compromised, these unpatched systems were used to execute ransomware attacks, in several cases against critical infrastructure in the United States and other Western nations. These marked the first confirmed cases of Iranian state affiliated ransomware attacks outside the Middle East. Following the cyberattack against Iran's fueling stations in late October, Microsoft observed a spike in Iranian ransomware attacks against US companies, suggesting possible correlation.

At the same time, PHOSPHORUS moved into directed targeting, often via spear phishing, of high-profile US critical infrastructure companies including major seaports and airports of entry, transit systems, utility companies, and oil and gas companies. This targeting, often conducted via spear phishing, lasted until mid-2022. The targets directly align with the sectors Tehran has blamed the United States and Israel for attacking in Iran, and likely provided Iran with options for retaliation. The compromise of near identical targets would provide an opportunity to deter such future attacks, while seeking to avoid escalation by signaling the cause of attacks without admitting guilt.

Resurgence of Iranian infrastructure targeting



Iranian targeting of critical infrastructure increased to the highest levels observed since late 2018 to early 2019. We used US Presidential Policy Directive 21 (PPD-21) to determine whether a company fit the criteria of critical infrastructure. (July 2021–June 2022).

https://t.me/learningnets

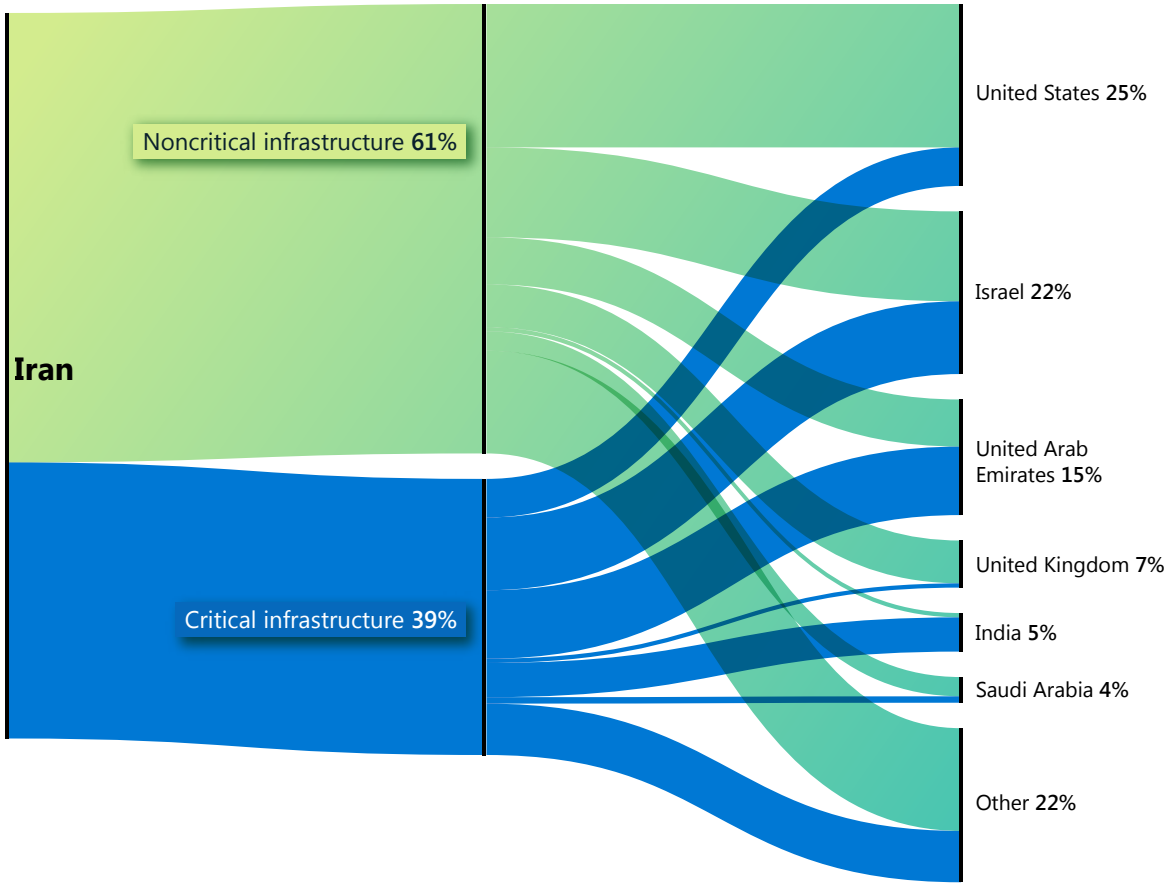
Iran growing increasingly aggressive following power transition

Continued

In Israel, DEV-0198 targeted Israeli railways, logistics companies, software providers of logistics companies, and fuel companies with a focus on gas stations. In early 2022, the group conducted a disruptive attack on the network of a major Israeli logistics company, which forced the company to shut down its computers and some of its operations to contain the attack. In another case, we observed the group attempt to access the network of a major Israeli transportation provider via stolen or reused credentials. Meanwhile, another Iranian actor, DEV-0343—whose targeting of defense, maritime transportation, and satellite imagery companies suggests links to the IRGC—compromised accounts at Israeli transportation and port-related entities throughout early 2021.

Iranian threat groups are likely to remain a threat to US and Israeli transportation and energy companies, particularly as diplomatic efforts to revive the Iranian nuclear deal wane and Washington, Tel Aviv, and Tehran seek alternative coercive means to lever concessions.

Iranian critical infrastructure targeting by country



Iranian targeting of critical infrastructure occurred most prominently against Israeli, Emirati, and US organizations.

Iranian actors are likely to remain a threat to US and Israeli transportation and energy companies in the coming year.

Iranian groups have expanded ransomware attacks beyond regional adversaries and are targeting high profile US and Israeli critical infrastructure targets.

Actionable insights

1. Improve your organization's overall cyber hygiene by enabling passwordless solutions such as MFA and enforcing its use for all remote connectivity to mitigate any potentially compromised credentials.
2. Evaluate the authenticity of all inbound email traffic to ensure the sender address is legitimate.
3. Patch early and often.[34]
4. Review and audit each one of your partner relationships with service providers to minimize any unnecessary permissions between your organization and upstream providers. Microsoft recommends immediately removing access for any partner relationships that look unfamiliar or have not yet been audited.[35]

Links to further information

- Iranian targeting of IT sector on the rise | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- Iran-linked DEV-0343 targeting defense, GIS, and maritime sectors | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

https://t.me/learningnets

Lebanon-based group with links to Iran targeting Israel

Microsoft monitors cyber threat activities regardless of platform, targeted victim, or geographical region. We maintain visibility and active threat hunting worldwide to write better detections for our customers.

Although threats from Russia, China, Iran, and North Korea represent the majority of our observed nation state actor activity, we also track and communicate about threats from NATO member countries and democratic nations. Last year, we featured activity by a Turkey-based actor (SILICON) and a Vietnam-based actor (BISMUTH). This year, we are expanding on the details of a Lebanon-based group that we previously disclosed publicly.[36]

Microsoft uncovered a previously undocumented Lebanon-based group that we assess with moderate confidence operated in coordination with actors affiliated with Iran's Ministry of Intelligence and Security (MOIS). Such collaboration or direction from Tehran would align with revelations since late 2020 that the Government of Iran is using third parties to carry out cyber operations, likely to enhance Iran's plausible deniability.

In the observed activity, POLONIUM targeted or compromised two dozen Israel-based organizations and one IGO with operations in Lebanon between February and May 2022, before Microsoft disrupted and publicly revealed its activity. Nearly half the Israeli organizations were part of Israel's defense industry or had links to Israeli defense companies, indicating the group has a similar set of interests as Iran in collecting intelligence on and/or directly countering Israel.[37]

POLONIUM's assessed links to MOIS groups are based on observed victim overlaps and commonality of tools and techniques.

- Victim overlap: An Iranian state group linked to Iran's MOIS, which Microsoft tracks as MERCURY, previously compromised multiple victims of POLONIUM, indicating a convergence of mission requirements or a possible "hand-off" of victims between groups.
- Common tools and techniques: Similar to POLONIUM, MSTIC observed DEV-0588 (also known as CopyKittens) commonly use AirVPN for operations and DEV-0133 (also known as Lyceum[38]) use OneDrive for C2 and exfiltration. Similar to Iranian state actors, POLONIUM used a cloud service provider to compromise an Israeli aviation company and law firm.[39]

POLONIUM deployed a series of custom implants using cloud services for C2 and data exfiltration—notably OneDrive and DropBox. POLONIUM often created unique OneDrive applications for targets, likely to evade detection.

As of June 2022, Microsoft suspended more than 20 POLONIUM-created OneDrive applications, notified affected organizations, and deployed a series of security intelligence updates to quarantine POLONIUM-developed tools.

Microsoft successfully detected and disabled POLONIUM's abuse of OneDrive as a C2.

Actionable insights

1. Update antivirus tools[40] and ensure cloud protection[41] is turned on to detect the related indicators.
2. For customers with service provider relationships, ensure review and audit of all partner relationships to minimize unnecessary permissions between your organization and upstream providers.[42] Immediately remove access for any partner relationships that appear unfamiliar or have not been audited.

Links to further information

- Exposing POLONIUM activity and infrastructure targeting Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)
- MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations | Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, Microsoft Defender Threat Intelligence

https://t.me/learningnets

North Korean cyber capabilities employed to achieve regime's three main goals

North Korea's cyber priorities over the past year reflected the government's stated global priorities. Kim Jong Un emphasized the three priorities of building defense capacity, bolstering the country's struggling economy, and ensuring domestic stability in several key addresses.[43] The actions taken by North Korean state actors clearly show that cyber is being utilized to achieve these three goals.

North Korean state threat groups, primarily CERIUM and ZINC, used a variety of tactics to attempt to penetrate networks of defense and aerospace companies around the globe. As North Korea embarked on its most aggressive period of missile testing ever in the first half of 2022, it used cyberespionage to help North Korean researchers gain an edge in developing indigenous defense systems and countermeasures for the advances its adversaries made.

We observed COPERNICIUM targeting a variety of cryptocurrency-related companies around the world, often with success, to help support North Korea's struggling economy. While we cannot confirm whether the group was able to exfiltrate money after a compromise, we observed COPERNICIUM infect dozens of machines by sending malicious documents masquerading as proposals from other cryptocurrency companies.

Finally, a group Microsoft tracks as DEV-0215 worked to uphold stability and loyalty in North Korea by targeting news organizations that report on North Korean issues. These outlets have sources both in North Korea and within communities of defectors, which Pyongyang views as an existential threat. In addition, the group worked to gain access to networks of Korean-speaking Christian groups, which tend to be outspoken against North Korea and work actively with North Korean defectors.

North Korean state actors used a variety of tactics to attempt to penetrate aerospace companies around the globe.

https://t.me/learningnets

Targeting of defense and aerospace companies

North Korean state actors led by CERIUM and ZINC put significant effort into developing tactics aimed at penetrating defense and aerospace companies. CERIUM repeatedly probed South Korean virtual private networks (VPNs) by downloading clients and looking for weaknesses. It also downloaded common applications used by South Korean military and government clients, likely looking for vulnerabilities. The group closely followed current events and wrote new lure documents which used high profile topics as bait to encourage targets to click on their malware executables and links.

Both ZINC and CERIUM used social media and social engineering in campaigns. ZINC was particularly adept at creating fake profiles on LinkedIn and other professional social media sites, where its operators posed as recruiters for major defense and aerospace companies. Using these profiles, they sent links or malicious file attachments to potential victims using direct messages on social media or email.

In addition to employees of corporations, CERIUM also broadly targeted members of the South Korean military, showing special interest in both South Korean military academies and military members working in academia.

Targeting cryptocurrency to balance losses

Since UN sanctions were levied in 2016, North Korea's economy has continued to contract, compounded by natural disasters such as floods[44] and drought[45] as well as a near-total lockdown of borders to imports since the onset of the COVID-19 pandemic in early 2020.[46] Although North Korea opened its borders for trade with China briefly in early 2022, they were soon closed again.[47] In mid-May, North Korea reported its first domestic case of COVID-19.[48] It has since applied a China-style "zero COVID" strategy of mass lockdowns to combat the virus which has negatively impacted North Korea's already fragile economy.

The North Korean state group COPERNICIUM tried to offset some of the lost revenue by stealing money—typically in the form of cryptocurrency—from any company whose networks it could penetrate. We saw dozens of machines compromised belonging to cryptocurrency-related companies in the United States, Canada, Europe, and throughout Asia. COPERNICIUM even compromised machines belonging to cryptocurrency-related companies within North Korea's strongest ally, China, both on the mainland and in Hong Kong. The group relied heavily on social media for its early reconnaissance and approaches to targets. Actors would build profiles pretending to be developers or senior officers in businesses related to cryptocurrency. They would then establish relationships with those in the industry, sending malicious links or files once they had built up rapport.

North Korean cyber capabilities employed to achieve regime's three main goals

Continued

A group related to PLUTONIUM develops and deploys ransomware

A group of actors originating from North Korea that Microsoft tracks as DEV-0530 began developing and using ransomware in attacks in June 2021. This group, which called itself H0lyGh0st, utilized a ransomware payload with the same name for its campaigns and successfully compromised small businesses in multiple countries as early as September 2021.

Microsoft assessed that DEV-0530 had connections with another North Korean-based group tracked as PLUTONIUM (also known as DarkSeoul or Andariel). While the use of H0lyGh0st ransomware in campaigns is unique to DEV-0530, MSTIC observed communications between the two groups, as well as DEV-0530 using tools created exclusively by PLUTONIUM.

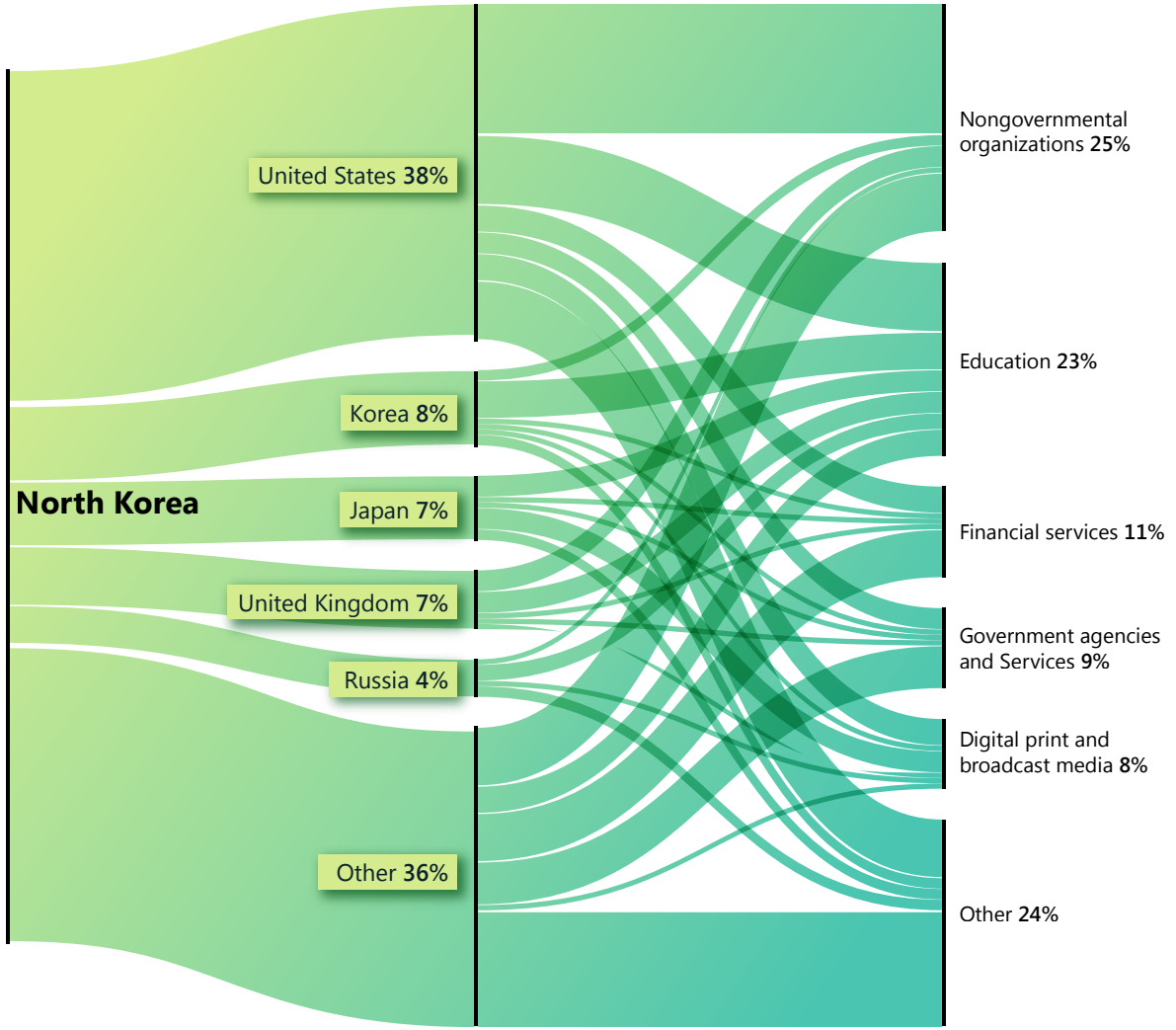
It is not certain that DEV-0530 activity was government-sponsored. Although ransomware attacks could have been ordered by the government for the same reason it sponsors theft from cryptocurrency companies, it is also possible the actors behind DEV-0530 were acting independently to earn money for themselves. If it were North Korean hackers operating independently, that would explain why the activity was not widespread compared to government-sponsored theft operations against cryptocurrency companies.

Targeting North Korean news outlets, defectors, religious groups, and aid organizations

In the last year, Supreme Leader Kim Jong Un was publicly more focused on internal security and loyalty than missiles and nuclear weapons. Reflecting this preoccupation with domestic issues, at least two North Korean state groups focused on aspects the regime would view as domestic threats.

The first was a group Microsoft tracks as DEV-0215, which targets media organizations that closely follow North Korean news. One likely reason for this targeting is these media outlets obtain their news from North Korean defectors, Chinese citizens who work closely with North Korea, and even some North Korean citizens based inside the country, using a variety of methods to communicate with the outside world. The North Korean government views these groups as an existential threat to its survival, particularly citizens inside North Korea who would be viewed as traitors and spies. DEV-0215 likely sought to identify these outlets' sources so they could neutralize potential information leaks.

North Korea: Top targeted countries and industry sectors



North Korea views the United States, South Korea, and Japan as its primary enemies. While Russia is a long-time ally, North Korean threat actors target Russian think tanks, academics, and diplomatic officials to obtain intelligence on Russian views of global affairs.

https://t.me/learningnets

North Korean cyber capabilities employed to achieve regime's three main goals

Continued

Microsoft also saw evidence of DEV-0215 targeting Korean-speaking Christian communities. Evangelical Christian Korean churches tend to be critical of both North Korea and South Korean governments that favor engagement with North Korea. These churches are likely to conduct outreach to defectors, and some engage in humanitarian work with North Korea. North Korea views them as a threat because, while the stream of defectors coming from North Korea almost dried up during the pandemic,[49] these Christian groups often play a critical role in helping defectors escape. DEV-0215 has generated fake documents about Christian conferences for Korean speakers as lures to target the group and discover who is helping organize defections.

Finally, state group OSMIUM showed steady interest in international aid organizations throughout the year, including organizations that have assisted North Korea in the past. While North Korea has generally shunned offers of help from outside the country, especially since the outbreak of COVID-19,[50] it is possible that North Korea is considering taking up offers of help, but is wary of the security ramifications of allowing foreign aid workers into the country. North Korea may be penetrating the networks of aid organizations worldwide to determine whether to allow such aid into their own country.

Actionable insights

1. North Korean state actors are skilled, relentless, and creative, but organizations can defend against them.
2. Most successful attacks can be stopped with basic cyber hygiene, such as two factor authentication or not opening attachments from unknown individuals in a virtual environment.

Links to further information

- North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware | Microsoft Threat Intelligence Center (MSTIC), Microsoft Digital Security Unit (DSU)

Among North Korea experts, there has long been debate over whether the North Korean government is in earnest with its public statements or whether it is posturing for effect. The alignment of cyberattacks with North Korea's announced priorities validates the belief that North Korea means what it says when it speaks publicly about its goals.

https://t.me/learningnets

Cyber mercenaries threaten the stability of cyberspace

There is a growing industry of private companies that develop and sell tools, techniques, and services that enable their clients—often governments—to break into networks, computers, phones, and internet-connected devices. An asset for nation state actors, these entities often endanger dissidents, human rights defenders, journalists, civil society advocates, and other private citizens. We refer to these as cyber mercenaries or private sector offensive actors.

A world where private sector companies create and sell cyberweapons is more dangerous for consumers, businesses of all sizes, and governments. These offensive tools can be used in ways that are inconsistent with the norms and values of good governance and democracy. Microsoft believes the protection of human rights is a fundamental obligation, and one we take seriously by curtailing "surveillance as a service" across the globe.

Microsoft has assessed certain state actors across democratic and authoritarian regimes outsource the development or use of "surveillance as a service" technology. This is how they avoid accountability and oversight, as well as acquire capabilities that would be difficult to develop natively.

> These cyberweapons provide nation states with surveillance capabilities they would not have been able to develop alone.

The market in which cyber mercenaries operate is opaque. Nevertheless, we continue to observe these groups using zero-day exploits and even zero-click exploits that require no victim interaction at all, enabling surveillance as a service.

Microsoft recently announced a European private sector offensive actor we call KNOTWEED, an Austria-based PSOA called DSIRF. Multiple news reports have linked the company to the development and attempted sale of a malware toolset called Subzero.[51] Victims include law firms, banks, and strategic consultancies in countries such as Austria, the UK, and Panama.[52]

Because these offensive surveillance capabilities are no longer highly classified capabilities created by defense and intelligence agencies, but rather commercial products now offered to companies and individuals, any regulatory regime for cyberweapons needs to move beyond export control. The impact of these cyberweapons can be devastating.

When a cyber mercenary exploits a vulnerability in a product or service, they put the entire computing ecosystem at risk. When vulnerabilities are identified publicly, companies are in a race against time to release protections before broad based attacks ensue (see our earlier discussion of vulnerability exploits). This is a dangerous and difficult cycle for both software suppliers (who must expediently develop patches) and consumers of products (who must implement the patches immediately).

As a founding member of the Cybersecurity Tech Accord[53]—a leading alliance bringing together more than 150 technology companies—Microsoft has made a commitment not to engage in offensive operations online. We stand by that commitment and by our human rights responsibilities in this area. We have engaged in technical disruptions and legal challenges to highlight the negative impacts caused by the services provided by cyber mercenaries and will continue to protect our customers when we see abuse.

> Cyber mercenaries create and provide "surveillance as a service" capabilities that are technologically sophisticated and broadly available, including advanced malware, and a range of techniques.

Actionable insights for governments

1. Implement transparency and oversight requirements for surveillance as a service, particularly in procurement, including the banning of these offensive actors, as the US has done with the Department of Commerce listing of companies on the Entity List.
2. Establish post-employment restrictions for former employees in this sector.
3. Aim to implement "know your customer" obligations and encourage companies to uphold their human rights commitments.

Links to further information

- Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- Continuing the fight against private sector cyberweapons | Microsoft On the Issues

https://t.me/learningnets

Operationalizing cybersecurity norms for peace and security in cyberspace

We urgently need a consistent, global framework that prioritizes human rights and protects people from reckless state behavior online. Nowhere is this more clearly demonstrated than in the ongoing war in Ukraine. In addition to a global strategic effort, governments can act now to have an immediate positive impact.

Five years ago, Microsoft called for a "Digital Geneva Convention" to advance responsibilities and obligations across sectors to defend peace and security online. Cyberspace was emerging as a distinct and volatile domain of conflict and competition between states, with attacks becoming more common, even in times of peace.

Today, there is still a clear need for such a framework—evidenced by Russian cyberattacks against Ukraine as part of Russia's invasion. This war has created a new front line that is dramatically different from any we have known before.

Bringing stability to cyberspace will require strengthening and reimagining global governance institutions to make them fit-for-purpose. Cyberspace is fundamentally different from other domains—it is borderless, synthetic, and maintained largely by private industry. This means asking the technology industry to take greater responsibility for both the security of products and services and the wider digital ecosystem. While there has been notable progress on all fronts, the challenges have grown dramatically.

We must redouble collective efforts to defend the security of cyberspace. We cannot take the rights and freedoms we have come to expect online for granted. While we struggle to address the challenges, malicious actors are planning how and where to strike next using AI, leveraging disinformation, and finding ways to undermine the fledgling metaverse. Human rights defenders, the technology industry, and rights-respecting governments must work together towards an affirmative vision for a safe and secure online world. The road ahead is long, but there are things governments can do now to immediately improve the cybersecurity ecosystem:

- Cite norms, laws, and consequences in attributions. One major improvement over the past five years has been the speed and coordination of government attributions of cyberattacks. Beyond simply naming and shaming, these statements need to highlight which international laws or norms are violated and what manner of consequences will be imposed to help strengthen recognition of international expectations.
- Clarify international law interpretation online. While governments agree that international law applies online, questions remain about how it applies in specific instances. This is particularly pertinent in the aftermath of the Ukraine invasion. Governments can go a long way toward setting expectations, avoiding misunderstandings, and building trust by stating how they understand their obligations under international law.
- Consult with other stakeholders. As international forums continue to discover the best ways to facilitate robust multistakeholder inclusion, governments can support informed dialogue by consulting with multistakeholder communities, in particular the technology industry, to ensure dialog benefits from those with indispensable expertise.
- Form a standing body to support responsible state behavior in cyberspace. The work of international diplomatic forums to advance responsible state behavior online has never been more important. There is a clear need for a permanent UN mechanism to deal with cyberspace as a domain of conflict.
- Define new norms for evolving threats. Cyberspace threats are constantly evolving alongside innovations in technology. While international norms should be technology neutral, they will need to be updated and attenuated based on changes in the threat landscape and how we use technology. Even today, we see gaps in the existing international framework being abused. States should commit to expressly protect core processes underpinning the digital ecosystem that are not currently protected, like the software update process. Moreover, specific areas deserve additional protections. For example, as we have learned amid the pandemic, norms for protecting healthcare are essential.

Nation state actors and attacks are increasing in volume and sophistication, creating a situation that is untenable.

Immediate action is imperative—there are things governments can do now to immediately improve the cybersecurity ecosystem, including implementing agreed upon norms and rules for state behavior in cyberspace and working with the broader multistakeholder community to address emerging gaps.

Multilateral institutions must be reimagined to address the pressing challenge of nation state cyberattacks.

Links to further information

- A moment of reckoning: the need for a strong and global cybersecurity response | Microsoft On the Issues
- Cyberattacks targeting health care must stop | Microsoft On the Issues
- The next chapter of cyber diplomacy at the United Nations beckons | Microsoft On the Issues

https://t.me/learningnets

Endnotes

1 https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2 https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3 Critical infrastructure in this chapter is defined by the Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (February 2013).
4 https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5 https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6 https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7 https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8 https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9 https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10 https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11 https://news.un.org/en/story/2022/06/1119672
12 https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13 https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14 https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15 https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16 https://twitter.com/MoNDefense
17 https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18 https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19 https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20 https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21 https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22 https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23 https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24 https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25 https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26 https://attack.mitre.org/techniques/T1053/
27 https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28 https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29 https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30 https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

https://t.me/learningnets

Endnotes continued

31 https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.

32 https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/

33 https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general

34 In particular, patch Exchange servers for ProxyShell vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065, CVE-2021-34473). Also, be sure to patch Fortinet FortiOS SSL VPN appliances for vulnerabilities.

35 https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide

36 https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

37 https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/

38 https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

39 https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/

40 https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide

41 https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus

42 https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide

43 https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
https://www.bbc.com/news/world-asia-59845636
https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/

44 https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods

45 https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/

46 https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html

47 https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html

48 https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html

49 https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades

50 https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms

51 Jan-Philipp Hein, In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, We unveil the "Subzero" state trojan from Austria, Europe-cities (2021), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister, We unveil the state Trojan "Subzero" from Austria, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.

52 As noted in our technical blog, the identification of targets in a country does not necessarily mean that a DSIRF customer resides in the same country, as international targeting is common.

53 Home | Cybersecurity Tech Accord (cybertechaccord.org)

https://t.me/learningnets

Devices and Infrastructure

With the acceleration of digital transformation, the security of digital infrastructure is more important than ever.

An overview of Devices and Insfrastructure 57
Introduction 58
Governments acting to improve critical infrastructure security and resilience 59
IoT and OT exposed: Trends and attacks 62
Supply chain and firmware hacking 65
Spotlight on firmware vulnerabilities 66
Reconnaissance-based OT attacks 68

https://t.me/learningnets

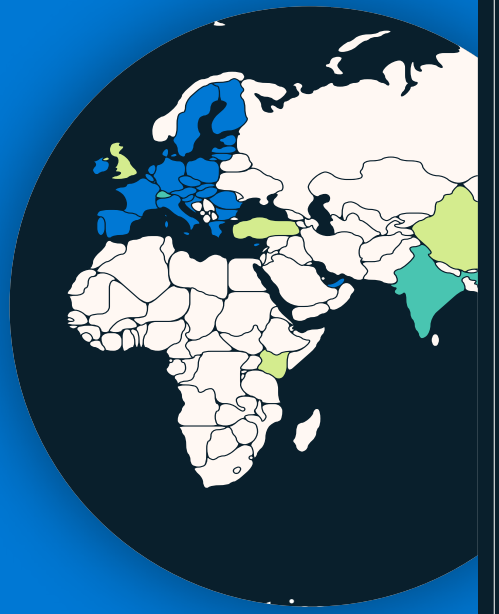
An overview of

Devices and Infrastructure

The pandemic, coupled with rapid adoption of internet-facing devices of all kinds as a component of accelerating digital transformation, has greatly increased the attack surface of the digital world.

Cybercriminals and nation-states are quickly taking advantage. While the security of IT hardware and software has strengthened in recent years, the security of Internet of Things (IoT) and Operational Technology (OT) devices has not kept pace. Threat actors are exploiting these devices to establish access on networks and enable lateral movement, to establish a foothold in a supply chain, or to disrupt the target organization's OT operations.

Governments worldwide are moving to protect critical infrastructure by improving IoT and OT security.

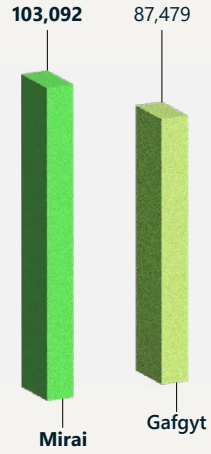


Find out more on p59

Globally consistent and interoperable security policies are needed to ensure broad adoption.

Find out more on p59

Malware as a service has moved into large scale operations against exposed IoT and OT in infrastructure and utilities as well as corporate networks.



Find out more on p63

Attacks against remote management devices are on the rise, with more than 100 million attacks observed in May of 2022—a five-fold increase in the past year.

Find out more on p62

Attackers are increasingly leveraging vulnerabilities in IoT device firmware to infiltrate corporate networks and launch devastating attacks.

Find out more on p65

32% of firmware images analyzed contained at least 10 known critical vulnerabilities.

Find out more on p66

https://t.me/learningnets

Introduction

Accelerating digital transformation has increased the cybersecurity risk to critical infrastructure and cyber-physical systems.

The last several years have seen unprecedented change in the digital world. Organizations are evolving to harness advances in computing capability from both the intelligent cloud and the intelligent edge. As a result of the pandemic forcing entities to digitize to survive and the rate at which industries worldwide are adopting internet-facing devices, the attack surface of the digital world is increasing exponentially.

This rapid migration has outpaced the security community's ability to keep up. Over the past year, we have observed threats exploiting devices in every part of the organization, from traditional IT equipment to operational technology (OT) controllers or simple Internet of Things (IoT) sensors. Although security of IT equipment has strengthened in recent years, IoT and OT device security has not kept pace. Threat actors are exploiting these devices to establish access on networks and enable lateral movement or disrupt the organization's OT operations. We have seen attacks on power grids, ransomware attacks disrupting OT operations, IoT routers being leveraged for increased persistency, and attacks targeting vulnerabilities in firmware.

While the prevalence of IoT and OT vulnerabilities is a challenge for all organizations, critical infrastructure is at increased risk because threat actors have learned that disabling critical services is a powerful lever. The 2021 ransomware attack on the Colonial Pipeline Company demonstrated how criminals can disrupt a critical service to increase the likelihood of a ransom payment. And Russia's cyberattacks against Ukraine demonstrate that some nation states view cyberattacks against critical infrastructure as acceptable sabotage to achieve its military objectives.

However, there is hope on the horizon. Policymakers and network defenders are acting to improve the cybersecurity of critical infrastructure, including the IoT and OT devices they rely on. Policymakers are accelerating the development of laws and regulations to build public trust in the cyber security of critical infrastructure and devices.

Microsoft is partnering with governments around the world to seize this opportunity to enhance cybersecurity and we welcome additional engagement. We are, however, concerned that inconsistent, bespoke, or complex requirements could have unintended effects, including decreasing security in some cases by diverting scarce security resources toward compliance with multiple duplicative certifications.

From a security operation standpoint network defenders take multiple approaches to improving their organization's IoT/OT security posture. One approach is to implement continuous monitoring of IoT and OT devices. Another is to "shift-left"—meaning to demand and implement better cybersecurity practices for the IoT and OT devices themselves. A third approach is to implement a security monitoring solution which spans both IT and OT networks. This holistic approach has the significant added benefit of contributing to critical organizational processes, such as "breaking the silos" between OT and IT, which in turn enables the organization to reach an enhanced security posture while meeting business objectives.

Michal Braverman-Blumenstyk
Corporate Vice President, Chief Technology Officer, Cloud and AI Security

https://t.me/learningnets

Governments acting to improve critical infrastructure security and resilience

Governments worldwide are developing and evolving policies to manage critical infrastructure cybersecurity risk. Many are also enacting policies to improve IoT and OT device security. The growing global wave of policy initiatives is creating enormous opportunity to enhance cybersecurity but also poses challenges to stakeholders across the ecosystem.

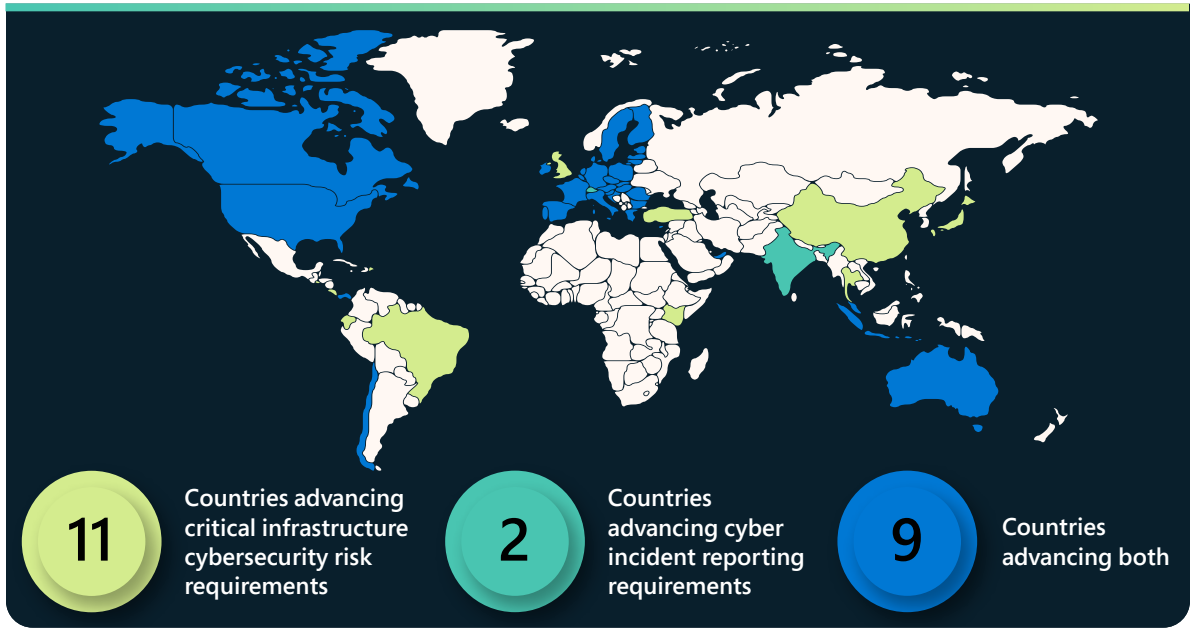
Developing a holistic vision for managing critical infrastructure cyber risk is critical, but complex, especially given the degree of interconnection across technologies and global suppliers, the range of technology uses and associated risks, and the need to invest in both short-and long-term strategies. Effectively scoped policies that drive iterative learning and improvements, and support global, cross-sector interoperability, can help manage complexity and enable a more security-minded digital transformation. However, a fragmented approach to legislation could lead to overlapping and inconsistent regulatory requirements. This could impact resources and ultimately undermine security objectives. For example, organizations could divert resources from innovation and security to formalistic compliance exercises.

Microsoft seeks to partner with governments around the world in pursuing effective critical infrastructure cybersecurity policies, increasing understanding of challenges and opportunities, and supporting efforts to enhance collective risk posture.

Policy developments in critical infrastructure cybersecurity risk management

During the last year, multiple jurisdictions including Australia, Chile, the European Union (EU), Japan, Singapore, the United Kingdom (UK), and the United States, have developed, updated, or implemented cross-sector or sector-specific cybersecurity requirements.[1] Many of these governments—and others such as India[2] and Switzerland[3]—already issued or are developing cybersecurity incident reporting requirements for critical infrastructure and essential service providers.[4]

Some notable policy developments occurred in Australia, the EU, Indonesia, and the United States during the last year. Australia enacted two laws to help it manage cross-sector critical infrastructure cybersecurity risks. The laws, among other things, designate new critical infrastructure sectors, require the development of risk management plans, mandate cybersecurity incident reporting, and empower the government to intervene if it determines a critical infrastructure operator is unwilling or unable to adequately respond to an incident.



The EU worked to update its NIS Directive of 2016, which provides a framework for EU member states to regulate technology services and products deemed critical to their economy and the functioning of society. The proposed NIS 2 includes revisions that would create a new category of critical digital infrastructure, increase requirements for cyber incident reporting, and impose additional cybersecurity risk management requirements, The EU also developed a proposed update to its Digital Operational Resilience Act (DORA), creating new requirements for information communication technologies used in the financial services sector.

In May, Indonesia issued a presidential regulation on the protection of vital information infrastructure ("IIV"), which will take effect in May 2024 and cover sectors such as energy, transportation, finance, and health, among others. Indonesia's objective with the regulation is to protect the continuity of the implementation of IIV, prevent cyberattacks, and increase preparedness in handling cyber incidents. IIV providers will be responsible for conducting secure and reliable protection, implementing effective cyber risk management, and reporting cyber risk results to corresponding government agencies. The regulation includes a requirement to report cyber incidents within 24 hours.

https://t.me/learningnets

Governments acting to improve critical infrastructure security and resilience

Continued

The US Congress passed a law that authorized the Cybersecurity and Infrastructure Security Agency (CISA) to issue regulations to require cyber incident reporting from critical infrastructure operators, and the US Transportation Security Administration (TSA) issued new sector-specific cybersecurity requirements in the transportation sector. In 2021, TSA issued two security directives to hazardous liquid and natural gas pipeline operators in response to the ransomware attack on the Colonial Pipeline Company:

- The first directive required operators to designate a cybersecurity coordinator, report cyber incidents within 12 hours, and conduct a vulnerability assessment of their systems.
- The second directive, which TSA revised in 2022, required them to implement specific mitigation measures to protect against ransomware attacks and other known threats to IT and OT systems, develop and implement a cybersecurity contingency and response plan within 30 days, and undergo an annual cybersecurity architecture design review.

Building on its regulations for pipelines, TSA issued two additional security directives later in 2021 that promulgated cybersecurity requirements to freight rail, passenger railroad carrier, or rail transit systems. The directives required that covered operators designate a cybersecurity coordinator, report cybersecurity incidents within 24 hours, develop and implement a cybersecurity incident response plan, and complete a cybersecurity vulnerability assessment. TSA simultaneously announced it also updated its aviation security programs to require airport and airline operators to implement the first two provisions, designating a coordinator and reporting incidents within 24 hours.

Policy developments in IoT and OT device security

Across dozens of countries, governments are active in developing requirements to advance the cybersecurity of information and communications technology (ICT) products and services, including IoT and OT devices. In the context of ICT products and services, the biggest concerns are software supply chain security and IoT security.

- The European Commission proposed the Cyber Resilience Act, which would establish cybersecurity requirements for standalone software and connected devices and ancillary services.[5] Relevant practices for software vendors include leveraging a secure software development lifecycle[6] and providing a Software Bill of Materials.[7] New security requirements would apply to connected devices and all manufacturers would be tasked with managing coordinated vulnerability disclosure[8] processes for released products.

Policymakers have also focused their attention on the continued proliferation of IoT devices and networked OT devices.

- In the UK, the draft Product Security and Telecommunications Infrastructure Bill will require manufacturers of consumer connectable products, such as smart TVs, to stop using default passwords that are an easy target for cyber criminals, to establish a vulnerability disclosure policy (such as a way to receive notice of security flaws), and to provide transparency about the minimum length of time during which they will provide security updates.[9]
- In the EU, new security standards or requirements are being implemented via multiple legislative instruments, including a delegated act to the Radio Equipment Directive that applies to wireless devices and seeks to improve network resilience, protect consumers' privacy, and reduce the risk of monetary fraud.[10] In addition, use of a cloud certification scheme,[11] currently in development as a result of the 2019 EU Cybersecurity Act,[12] might be required.

The need for consistency

In many cases, the range of activity across regions, sectors, technologies, and operational risk management areas is being pursued simultaneously, resulting in potential overlap or inconsistency in scope, requirements, and complexity for organizations seeking to leverage guidance or demonstrate compliance. Without a universally accepted definition of IoT, scope is especially challenging for IoT and OT device regulations. The examples above potentially apply to "connected products and ancillary services," "consumer connectable products," and "wireless devices." At the same time, many governments aim to implement more robust assessment regimes to better understand whether and how organizations and products meet current, emerging, and evolving requirements. As these trends merge, complexity will increase. Encouragingly, questions posed during the EU Cyber Resilience Act consultation explored how new regulation could potentially interact with existing cybersecurity regulation, indicating intent to avoid conflicting cybersecurity requirements.

Iterative approaches that are risk-based and outcome- or process-oriented (versus implementation-specific) could foster enhanced cybersecurity and continuous improvement. Likewise, a focus on enabling interoperability across sectors, regions, and policy areas could consistently raise cybersecurity across interconnected global supply chains.

https://t.me/learningnets

Governments acting to improve critical infrastructure security and resilience

Continued

There are increasingly complex critical infrastructure cybersecurity policies in development across regions, sectors, and topic areas. This activity brings great opportunities and significant challenges. How governments proceed will be crucial to the future of digital transformation and ecosystem-wide security.

Accelerating ecosystem-wide investments in software supply chain security and Zero Trust architecture

US Executive Order (EO) 14028 on improving cybersecurity has been a catalyst to expedite Microsoft's ongoing initiatives to invest in our own and ecosystem-wide supply chain security and to enable our customers to meet Zero Trust objectives.

We have long believed that enhancing the software supply chain requires sharing learnings and best practices, beginning with our public release of Microsoft's Security Development Lifecycle about 15 years ago.

In addition, we are partnering closely with the National Cybersecurity Center of Excellence to demonstrate approaches to Zero Trust Architecture applied to both on-premises and cloud technology and establishing new product capabilities, including the ability to enforce phishing-resistant authentication for hybrid and multi-cloud environments.

Today, we're going beyond the EO's requirements to demonstrate conformance with software supply chain security requirements and provide Software Bill of Materials (SBOM) information in two ways:

1. First, we're sharing an open-source version of our SBOM generator tool, which we built to be easily integrated with CI/CD pipelines supporting builds on Windows, Linux, Mac, iOS, and Android platforms.[13]
2. Second, we're contributing to the development of industry standards for Supply Chain Integrity, Transparency, and Trust (SCITT). This will allow for the automated exchange of verifiable supply chain information, including artifacts that demonstrate conformance with requirements such as those resulting from the EO's software supply chain guidance.

Actionable insights

1. Multilateral institutions must be reimagined to address the pressing challenge of nation state cyberattacks.
2. Develop cybersecurity policies that are consistent and interoperable across regions, sectors, and topic areas.

Links to further information

- Continued investments in supply chain security in support of the cybersecurity Executive Order | Microsoft Tech Community
- US Government sets forth Zero Trust architecture strategy and requirements | Microsoft Security Blog
- CYBER EO | Microsoft Federal
- Supply Chain Integrity, Transparency, and Trust | github.com
- Implementing a Zero Trust Architecture | NCCoE (nist.gov)

https://t.me/learningnets

IoT and OT exposed: Trends and attacks

The increasingly connected digital world means devices are rapidly coming online, communicating with larger systems, collecting data, and creating visibility across formerly obscured spaces. This brings opportunity for organizations and threat actors alike, with the business of cybercrime becoming both a multi-billion dollar industry and risk.

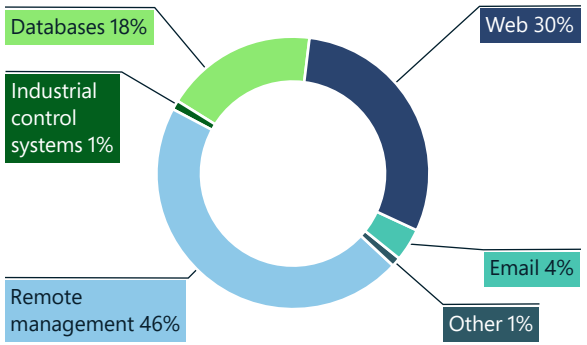
IoT devices—including everything from printers to web cameras, climate control devices, and building accesses controls—pose unique security risks to individuals, organizations, and networks. While critical to many organizations' operations, they can quickly become a liability and security risk. The rapid adoption of IoT solutions in almost every industry has increased the number of attack vectors and the exposure risk of organizations.

Malware as a service has moved into large scale operations against civil infrastructure and utilities (including hospitals, oil and gas, electrical grids, transportation services, and other critical infrastructure) as well as corporate networks. Significant research efforts are required by threat actors to uncover and exploit the configuration of operating environments and embedded IoT and OT devices.

IoT devices pose unique security risks as entry and pivot points in the network. Millions of IoT devices are unpatched or exposed.

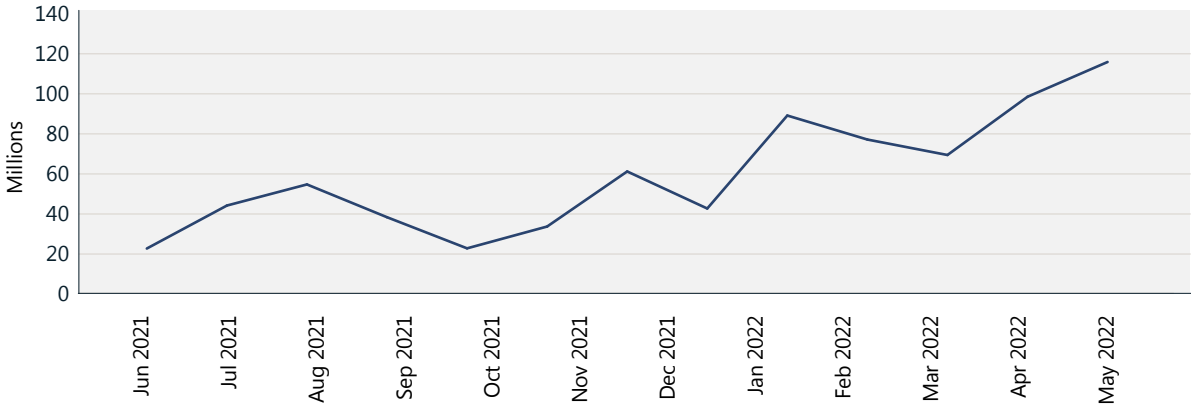
Exposed devices can be discovered through internet search tools by identifying services listening on open network ports. These ports are commonly used for remote management of devices. If not secured correctly, an exposed IoT device can be used as a pivot point into another layer of the enterprise network as unauthorized users can remotely access the ports. We have observed a variety of threat actors attempting to exploit vulnerabilities in internet exposed devices ranging from cameras to routers to thermostats. However, despite the risk, millions of devices remain unpatched or exposed.

Summary of attack types on IoT/OT



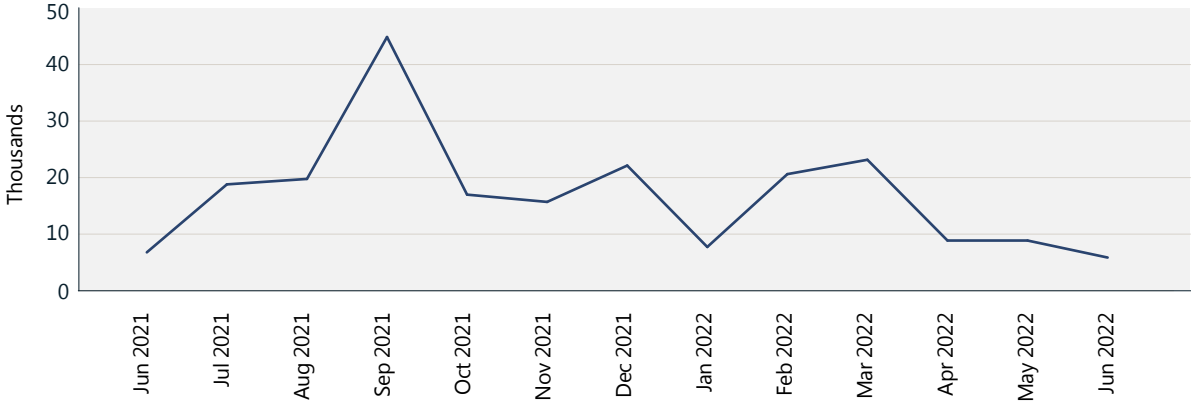
Attack types observed through MSTIC sensor network. Most prevalent were attacks against remote management devices, attacks via web, and attacks on data bases (brute forcing or exploits).

Attacks against remote management devices



Increasing attacks on remote management ports over time, as seen through the MSTIC sensor network.

Web attacks against IoT and OT



Web attack volume over time, as seen through the MSTIC sensor network. As the number of devices directly connected to the web continues to drop, attackers might eventually be less likely to probe for them.

https://t.me/learningnets

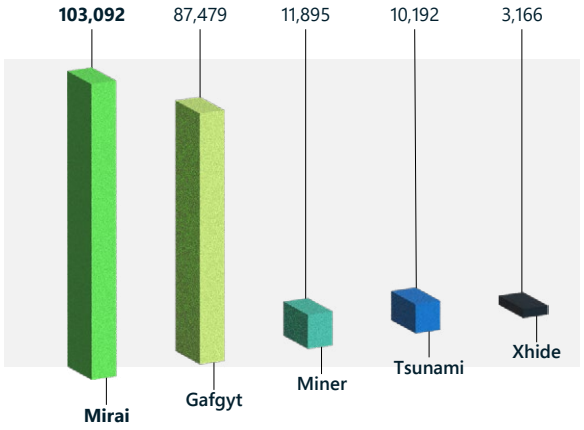
IoT and OT exposed: Trends and attacks

Continued

Revamped malware utility

As cybercrime groups have evolved, so has their deployment of malware and choice of targets. In the past year, we observed attacks against common IoT protocols—such as Telnet—drop significantly, in some cases as much as 60 percent. At the same time, botnets were repurposed by cybercrime groups and nation state actors. The persistence of malware, such as Mirai, highlights the modularity of these attacks and the adaptability of existing threats.

Top IoT malware detected in the wild



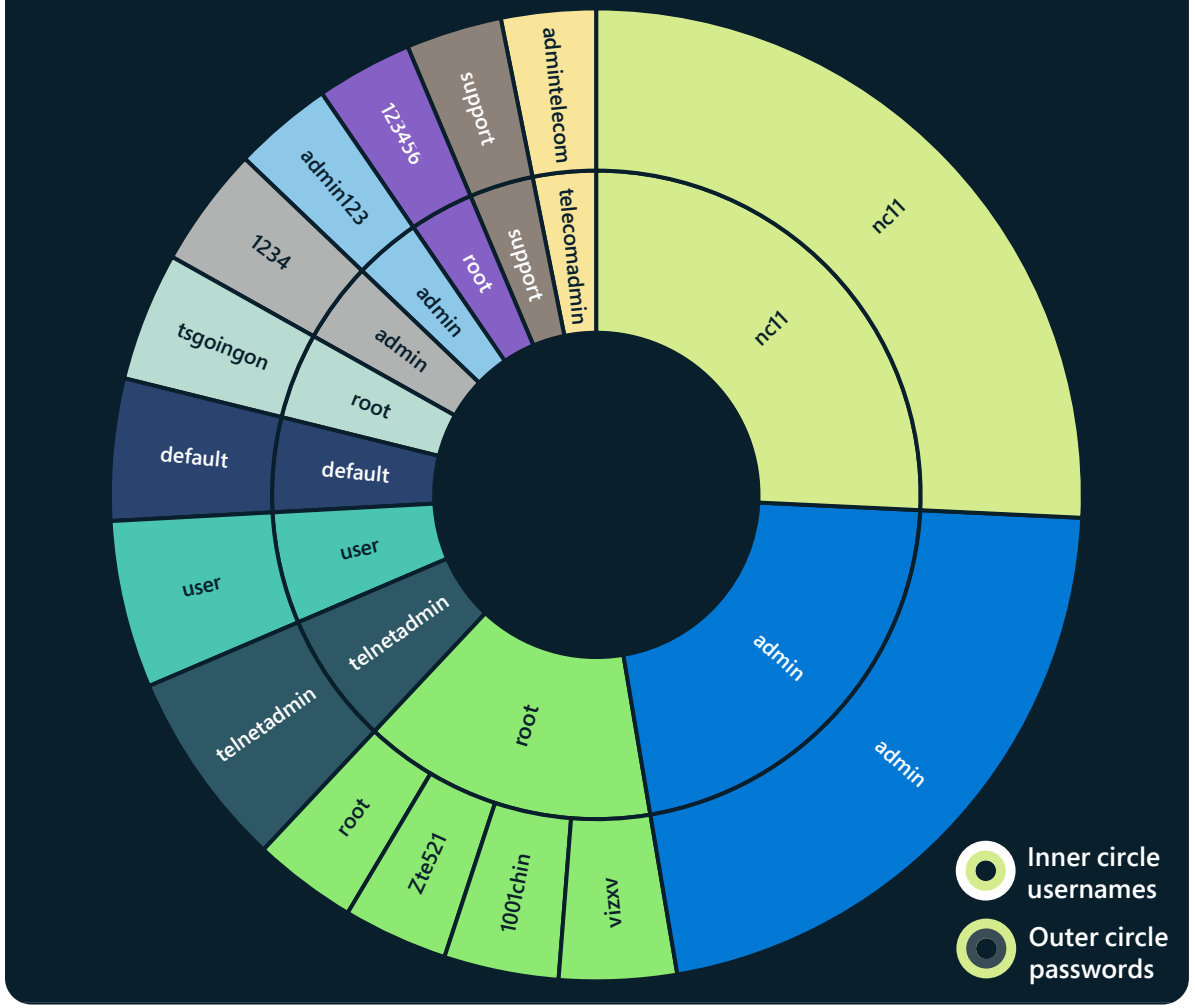
Mirai evolved to infect a wide range of IoT devices including internet protocol cameras, security camera digital video recorders, and routers. The attack vector bypassed legacy security controls and poses a risk for endpoints within the network by exploiting additional vulnerabilities and moving laterally. Mirai has been redesigned multiple times, with variants adapting to different architectures and exploiting both known and zero-day vulnerabilities to compromise new attack vectors.

The use of Mirai grew among both 32- and 64-bit x86 CPU architectures over the past year, and the malware was given new capabilities that were rapidly adopted by nation state and criminal groups. Nation state attacks now leverage new variants of existing botnets in distributed denial of service (DDoS) attacks on foreign adversaries.

As revenue from attacks against IoT devices declined in 2022, we observed several threat actor groups abusing vulnerabilities—such as Log4j and Spring4Shell—to deliver a malicious payload to devices such as servers, infecting them and recruiting them into large botnets carrying out DDoS attacks. The revamped utility of malware designed to target vulnerable IoT devices has serious implications for both organizations and nations, as lateral movement can expose backdoors to additional payloads and other devices on networks.

Many industrial control system protocols are unmonitored and therefore vulnerable to OT-specific attacks. This can mean increased risk for critical infrastructure.

Relative prevalence of user name and password pairs seen among IoT/OT devices in 45 days of sensor signals



Using common username and password pairs increases risk of compromise. Based on a sample size of over 39 million IoT and OT devices, those using identical usernames and passwords represented around 20 percent.

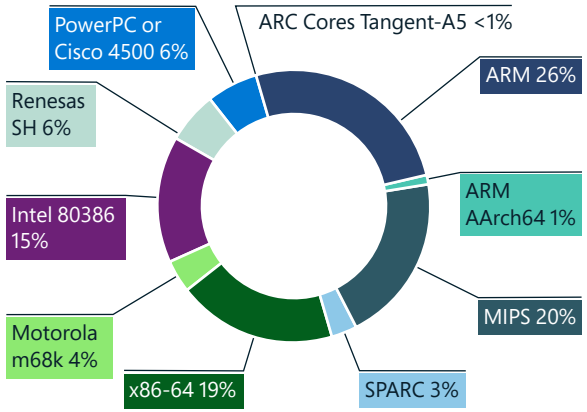
https://t.me/learningnets

IoT and OT exposed: Trends and attacks

Continued

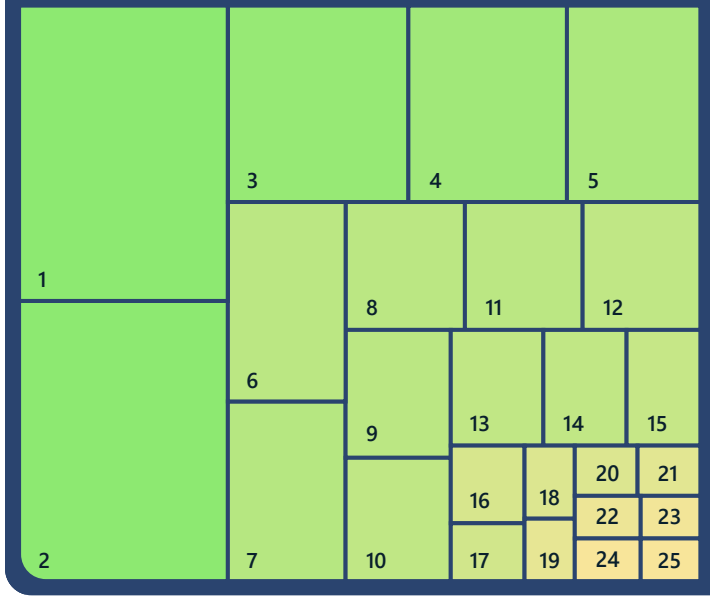
While weak configurations and default credentials still pose a risk to networks, Microsoft observed many web-based exploits utilizing HTTP. We observed this increase in attacks on web-based services using legacy botnets. Meanwhile, there was a decrease in the number of open telnet ports on the internet, a positive sign for network security as botnets which posed historical risk to devices are losing relevance. Despite this decrease in open telnet ports, we still observed persistent botnets in sensor networks.

Distribution of IoT malware by CPU architecture



Microsoft observed that IoT devices running on ARM are most targeted by malware, followed by MIPS, X86-64, and Intel 80386 CPU.

Industrial control system protocol prevalence



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet Real-Time
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC Agent
10. EtherNet/IP O/O
11. Honeywell Control Data Access
12. MMS
13. IEC-60870
14. Honeywell FDA Diagnostics
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

Industrial control system protocol vulnerabilities

We looked into OT data from our cloud connected sensors, revealing the most common industrial control system (ICS) protocols. These protocols provide insights into the nature of these devices and their attack surface. This is especially relevant to the security of critical infrastructure. Some key learnings are:

1. Most of the protocols represented are proprietary, so standard IT monitoring tools won't have adequate security visibility across these devices and protocols. As a result, networks are left unmonitored and therefore more vulnerable to OT-specific attacks.
2. There is a large variety of vendor-specific protocols. This means vendor-specific security solutions won't be able to adequately cover the whole network. Microsoft prioritizes a vendor agnostic approach, to provide security coverage for the broad variety of different devices.
3. Organizations should ensure these protocols are not exposed directly to the internet from their networks. This exposure could pose a major security risk due to vulnerabilities and the unsecure nature of these protocols.

Malware such as Mirai persists by developing new capabilities and is being adopted by cybercrime groups and nation state actors, leveraging new variants of existing botnets in DDoS attacks on foreign adversaries.

Actionable insights

1. Ensure devices are robust by applying patches, changing default passwords, and default SSH ports.
2. Reduce the attack surface by eliminating unnecessary internet connections and open ports, restricting remote access by blocking ports, denying remote access, and using VPN services.
3. Use an IoT/OT-aware network detection and response (NDR) solution and a security information and event management (SIEM)/security orchestration and response (SOAR) solution to monitor devices for anomalous or unauthorized behaviors, such as communication with unfamiliar hosts.
4. Segment networks to limit an attacker's ability to move laterally and compromise assets after initial intrusion. IoT devices and OT networks should be isolated from corporate IT networks through firewalls.
5. Ensure ICS protocols are not exposed directly to the internet.

https://t.me/learningnets

Supply chain and firmware hacking

Almost every internet-connected device has firmware, which is software embedded in the device's hardware or circuit board. Over the past few years, we have seen increased targeting of firmware to launch devastating attacks. As firmware is likely to continue to be a valuable target for threat actors, organizations must protect against firmware hacking.

Firmware is responsible for a device's primary functions, such as connecting to a network or storing data. Firmware is found in routers, cameras, televisions, and other devices used in Enterprises (IoT) along with industrial control equipment (OT) used in critical infrastructure. Historically, firmware has been written with unsecured code, creating significant vulnerabilities which can be exploited to take over the device or inject malicious code into the firmware.

This risk is compounded when it comes to the supply chain. Most devices are built using software and hardware components from numerous manufacturers as well as open-source libraries. In many cases device operators do not have visibility into the hardware and software bill of materials (H/SBOM) to evaluate the supply chain risk of devices on their network. In June 2020, vulnerabilities were disclosed in a networking stack used by many different manufacturers affecting hundreds of millions of IoT devices in the consumer and industrial equipment space.[14] In some cases, the network stack was rebranded by other vendors and there was no indication a device was vulnerable. We see a growing threat of malicious actors targeting this software and hardware supply chain of IoT/OT devices to compromise organizations.

The firmware updating process varies widely across devices, and the complexity and logistical challenge of performing it impacts the update frequency. It is not always possible to determine if a device is running the latest firmware, making it difficult for security professionals to monitor and ensure the security posture in their IoT and OT devices. In addition, some devices have firmware that is not cryptographically signed, enabling them to be updated without verification from the user. These weaknesses further open the devices up to supply chain attacks throughout the production and distribution chain.

To address these threats, Microsoft invests significantly in ensuring the security and integrity of the firmware as it moves through various stages of the supply chain, and in attesting at any time that it has not been tampered with during ingestion or along the way. This will allow us to validate trust between each pipeline segment and provide a certified and provable end-to-end chain of custody for every component we ship to customers. We are working with our partners to bring this chip-to-cloud security to all devices on the enterprise and OT network.

"ICT infrastructure suppliers are increasingly targets as they enable widespread replication of a single attack. At the same time, global legislation, regulation, and customer demands for supply chain security and resiliency are on the rise, often diverging in their requirements.

The solution is partnership. Together with suppliers and global governments, Microsoft is committed to addressing security across our supply chain ecosystem, exceeding demands from customers and regulators alike. To do this, we are driving a comprehensive approach to security and operational resiliency that is flexibly deployed across the supply chain.

Driving firmware integrity from design through to device operation is key to our collective approach. Ensuring suppliers' SDL processes and deploying hardware root of trust innovation are examples of how we can 'build in' supply chain integrity.

Our community is leveraging collective research and development spanning new anti-tampering techniques and cryptographic mechanisms, combined with ongoing monitoring and anomaly detection. Together, we are progressing in minimizing the allure of supply chain as an attack surface."

Edna Conway,
Vice President, Security & Risk Officer, Cloud Infrastructure

https://t.me/learningnets

Spotlight on firmware vulnerabilities

Attackers are increasingly leveraging vulnerabilities in IoT device firmware to infiltrate corporate networks. Unlike traditional IT endpoints that use XDR agents to identify weaknesses, vulnerability identification within IoT/OT devices is much more elusive.

A recent survey conducted by Microsoft and the Ponemon Institute highlights both the opportunity and the security challenge of IoT/OT devices in an enterprise.[15] While 68 percent of respondents believe the adoption of IoT/OT is critical to their strategic digital transformation, 60 percent recognize that IoT/OT security is one of the least secured aspects of the IT/OT infrastructure.

An example of attackers using vulnerabilities in IoT device firmware to infiltrate a network is the Trickbot trojan which leveraged default passwords and vulnerabilities in Mikrotik routers[16] to bypass corporate defense systems. The fundamental challenge with IoT device firmware is the lack of visibility into the security posture and vulnerabilities of devices.

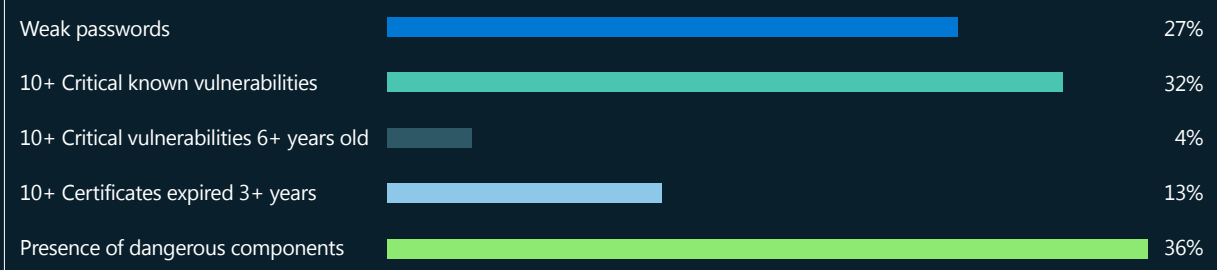
While there are solutions available to build secure devices, there are billions of devices already on the market and deployed in enterprises. These are known as brownfield devices. In 2021, Microsoft acquired ReFirm Labs to shine a light on brownfield device security and enable device builders to improve the security of their products. ReFirm Labs analyzes the binary firmware image of a device and produces a detailed report on potential security weaknesses.[17] This technology is being incorporated into a future release of Microsoft Defender for IoT.

Over the past year, we examined aggregate results of the unique firmware scanned by our customers. While not every weakness discovered might be exploitable, they underscore the fundamental challenge of device firmware security.

Note the types of weaknesses that exist in IoT/OT devices would never be acceptable on traditional Windows or Linux endpoints.

- Weak passwords: Twenty-seven percent of the firmware images scanned contained accounts with passwords encoded using weak algorithms (MD5/DES), which are easily broken by attackers.

Security weaknesses in firmware images analyzed



- Known vulnerabilities: Like other systems, IoT/OT device firmware extensively leveraged open-source libraries. However, devices frequently ship with out-of-date versions of these components. In our analysis, 32 percent of the images contained at least 10 known vulnerabilities (CVEs) rated as critical (9.0 or higher). Four percent contained at least 10 critical vulnerabilities that were more than six years old.
- Expired certificates: Certificates are used to authenticate connections and identities, as well as protect sensitive data, but 13 percent of the images analyzed contained at least 10 certificates that had expired more than three years ago.
- Software components: Thirty-six percent of the images contain software components Microsoft recommends be excluded in IoT devices such as packet capture tools (tcpdump, libpcap), which can be leveraged for network reconnaissance as part of an attack chain.

https://t.me/learningnets

Firmware attacks in the wild

Viasat: Using a firmware vulnerability to target satellite communication

In February 2022, a satellite network incident disconnected a strategic communication network with impacts felt across Europe. Viasat's KA-SAT system received a large amount of traffic that disconnected many modems and a denial of service attack was initiated against the network. As fixed broadband was disrupted, thousands of wind turbines became remotely inaccessible to operators and malicious wiper malware was deployed to affected modems. The disruption affected more than 30,000 satellite terminals used by companies and organizations for communication.

Cyclops Blink: Using a firmware supply chain attack to target firewall gateways

For threat actors, the development and expansion of command and control (C2) and attack infrastructure is a crucial component of success. As the need for a stable C2 infrastructure has grown, routers have become a desirable attack vector due to their infrequent patching and lack of comprehensive security solutions.

Microsoft is partnering with government and industry on firmware analysis technology to bring deeper visibility into device security and provide full lifecycle security for device builders and operators.

Since June 2019, a nation state-affiliated advanced persistent threat (APT) group used the modular malware Cyclops Blink to target vulnerable WatchGuard firewall devices and ASUS routers by executing malicious firmware updates and recruiting them to a large botnet. The malware successfully infects devices by exploiting a known vulnerability that allows a privilege escalation, enabling the threat actors to manage the device. Once infected, the malware allows further modules to be installed and evades firmware updates. Compromised devices have been observed connecting to C2 servers hosted on other WatchGuard devices. Issuing many SSL certificates for their C2 on various TCP ports, Cyclops Blink operators gained privileged remote access to networks by executing malicious firmware updates and by evading traditional security methods such as scanning.

How Microsoft is improving supply chain security

Microsoft is partnering with government and industry to address these IoT and OT device security challenges (see the discussion on page 66). Our contribution will include leveraging firmware analysis technology to provide device operators with visibility into the security posture of the devices on their network. This will enable customers to identify and prioritize devices in need of additional protections, upgrades, or replacement—and drive demand for device builders to invest in device security. At the same time, we are supporting builders with comprehensive solutions to architect secure devices and adopt secure development lifecycles.

Another key component is providing builders and operators robust infrastructure to allow device firmware to be updated as security issues are discovered and resolved. Microsoft is bringing together firmware analysis and Defender for IoT with Device Update for IoT Hub to provide a solution to address the full lifecycle of IoT and OT device security. These are important steps in realizing our vision for customers to secure the infrastructure by adoption of devices that support a Zero Trust approach to their IoT and OT solutions.[18]

Attackers are increasingly targeting vulnerabilities in IoT device firmware to infiltrate corporate networks.

Actionable insights

1. Gain deeper visibility into IoT/OT devices on your network and prioritize them by risk to the enterprise if they are compromised.
2. Use firmware scanning tools to understand potential security weaknesses and work with vendors to identify how to mitigate the risks for high-risk devices.
3. Positively influence the security of IoT/OT devices by requiring the adoption of secure development lifecycle best practices by your vendors.

Links to further information

- Assessment of the Critical Supply Chains Supporting the US Information and Communications Technology Industry

https://t.me/learningnets

Reconnaissance-based OT attacks

Complex supply chains use specific design information to plan the actual system. Of the myriad assets that compose this design information, the most sensitive is the project file, which defines the environment and its assets. This file is a crucial strategic target for threat actors seeking to gain access and deploy a successful attack wholly tailored to the environment.

Targeting industrial systems to disrupt operational processes involves two steps.

1. First, the attacker must access the OT network. This can be done by entering through IoT devices on the enterprise side of the network (Purdue Model Level 4) and crossing the IT-OT boundary, traditionally separated by firewalls and networking equipment, into the operation and control levels.
2. Second, the network devices must be identified. Industrial systems use standard devices and components in customized architectures specifically designed for their environments. One of these standard devices is the programmable logic controller (PLC). Every manufacturer develops unique interfaces and functions for their PLCs, which are a crucial component of industrial systems, and these devices are further configured with customized schemas specifically designed for the customer's environments.

The unique configuration of each PLC is described in the project file, which contains the definition of the environment and its assets, the ladder logic, and more.

In most environments that show evidence of an attack, analysis shows the timeline preceding the attack far exceeds the length of the attack itself. Threat actors often invest months in simulating the environment and its assets remotely, making many attempts to construct a model and prepare their targeted attack. As environments continuously change and integrate new devices, vulnerabilities are created specifically around the data in the project and configuration files. The theft of a project file can advance an attack by weeks or months and enable attackers to model the target environment rapidly and accurately, increasing the difficulty in detecting malicious activity.

Industroyer and Incontroller

We have observed increased attacks on organizations, critical infrastructure, and government targets by state sponsored actors using modular malware and attack frameworks. New attempts to interfere with critical operations in Ukraine underscore the growing threat of reconnaissance-based OT attacks that are highly tailored to their target environments. The extended reconnaissance and research phases carried out by nation state cyber actors points to a strategy of using cyber warfare to cripple infrastructure remotely to meet specific strategic or operational goals in blended cyber-kinetic operations and political strategy.

https://t.me/learningnets

Reconnaissance-based OT attacks

Continued

In early 2022, two adaptable critical OT attacks were identified. A cyber-physical attack on electrical substations and protection relays in Ukraine was carried out with customized malware, including a variant of Industroyer, a malware known to have caused power outages in Ukraine after its deployment in 2016.

Industroyer2 is the first known redeployment of malicious OT attack malware on a new target. It utilized the IEC104 protocol (standard protocol for power system monitoring and control) plugin developed for Industroyer and targeted mostly PLC-like remote terminal units with model number ABB RTU540/560. The writer of this malware used knowledge of the victim's environment to issue commands repeatedly to predetermined outputs, ensuring they could not be turned on manually. This ensured longer lasting power outages and a more damaging impact.

Incontroller, a modular attack framework identified during the same period, is a modular toolkit that significantly reduces the lead time to penetrate and attack OT devices, bypassing legacy security solutions. The general-purpose toolkit has data-collection, reconnaissance, and attack capabilities that are highly customizable to different environments and can greatly impact the research phase for an OT attack, reducing the time necessary to perform reconnaissance, supporting the simulation of environments by extracting information about devices and their configurations.

The Incontroller framework supports protocols for Schneider Electric and Omron PLCs and collects information, such as firmware version, model type, and connected devices. The toolkit can issue commands to change configurations and turn outputs on and off. Once an environment is accessed, the framework supports implanting backdoors in devices for the delivery of more payloads, issuing vulnerabilities to increase access points, uploading of ladder logic, and the ability to initiate DoS attacks. The generic nature of the toolkit enables a threat actor to attack an environment quickly without needing to write new attacks for every PLC or location. This allows the actor to easily interact with different types of machines potentially across many industries.

Actionable insights

1. Avoid transferring files which contain system definitions through unsecure channels, or to non-essential personnel.
2. When transferring such files is unavoidable, be sure to monitor activity on the network and ensure assets are secure.
3. Protect engineering stations by monitoring with EDR solutions.
4. Proactively conduct incident response for OT networks.
5. Deploy continuous monitoring, like Defender for IoT.

https://t.me/learningnets

Endnotes

1 See, e.g., Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience—GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST

2 Cert-In—Home Page

3 Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)

4 See, e.g., untitled (house.gov)

5 Cyber Resilience Act | Shaping Europe's digital future (europa.eu)

6 See, e.g., Microsoft Security Development Lifecycle

7 See, e.g., Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft—Engineering@Microsoft; see also, e.g., The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)

8 See, e.g., https://www.microsoft.com/en-us/msrc/cvd

9 The Product Security and Telecommunications Infrastructure (PSTI) Bill—product security factsheet—GOV.UK (www.gov.uk)

10 Commission strengthens cybersecurity of wireless devices and products (europa.eu)

11 Cloud Certification Scheme: Building Trusted Cloud Services Across Europe — ENISA (europa.eu)

12 Certification — ENISA (europa.eu)

13 https://github.com/microsoft/sbom-tool" GitHub - microsoft/sbom-tool: The SBOM tool is a highly scalable and enterprise ready tool to create SPDX 2.2 compatible SBOMs for any variety of artifacts.

14 https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come

15 IoT/OT Innovation Critical but Comes with Significant Risks (Dec 2021): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/

16 Uncovering Trickbot's use of IoT devices in C2 Infrastructure (Mar 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/

17 IoT Show on Channel 9 Episode on IoT Firmware Scanning (May 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot

18 How to apply a Zero Trust approach to your IoT solutions (May 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

https://t.me/learningnets

Cyber Influence Operations

Today's foreign influence operations utilize new methods and technologies, making their campaigns designed to erode trust more efficient and effective.

An overview of Cyber Influence Operations 72
Introduction 73
Trends in cyber influence operations 74
Spotlight on influence operations during the COVID-19 pandemic and Russia's invasion of Ukraine 76
Tracking the Russian Propaganda Index 78
Synthetic media 80
A holistic approach to protect against cyber influence operations 83

https://t.me/learningnets

An overview of

Cyber Influence Operations

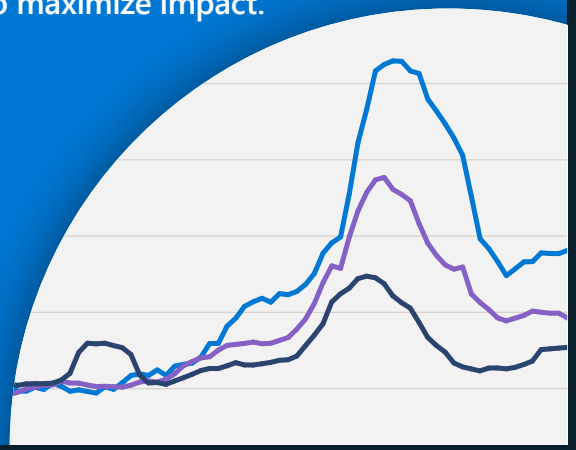
Today's foreign influence operations utilize new methods and technologies, making their campaigns designed to erode trust more efficient and effective.

Nation states are increasingly using sophisticated influence operations to distribute propaganda and impact public opinion both domestically and internationally. These campaigns erode trust, increase polarization, and threaten democratic processes. Skilled Advanced Persistent Manipulator actors are using traditional media together with internet and social media to vastly increase the scope, scale, and efficiency of their campaigns, and the outsized impact they are having in the global information ecosystem. In the past year, we have seen these operations used as part of Russia's hybrid war in Ukraine, but have also seen Russia and other nations, including China and Iran, increasingly turning to social-media powered propaganda operations to extend their global influence.

Cyber influence operations are becoming increasingly sophisticated as more governments and nation states are using these operations to shape opinion, discredit adversaries, and promote discord.

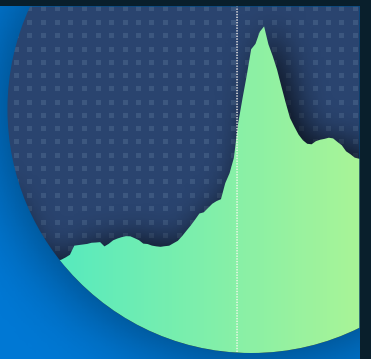
Find out more on p74

Russia's invasion of Ukraine demonstrates cyber influence operations integrated with more traditional cyberattacks and kinetic military operations to maximize impact.



Find out more on p76

Russia, Iran, and China employed propaganda and influence campaigns throughout the COVID-19 pandemic often as a strategic device to achieve broader political objectives.



Find out more on p76

Synthetic media is becoming more prevalent due to the proliferation of tools which easily create and disseminate highly realistic artificial images, videos, and audio. Digital provenance technology that certifies media asset origin holds promise to combat misuse.

Find out more on p80

A holistic approach to protect against cyber influence operations

Microsoft is building on its already mature cyber threat intelligence infrastructure to combat cyber influence operations. Our strategy is to detect, disrupt, defend, and deter propaganda campaigns by foreign aggressors.

Find out more on p83

https://t.me/learningnets

Introduction

Democracy needs trustworthy information to flourish. A key area of focus for Microsoft are the influence operations being developed and perpetuated by nation states. These campaigns erode trust, increase polarization, and threaten democratic processes.

Foreign influence operations have always been a threat to the information ecosystem. However, what differs in the age of the internet and social media is the vastly increased scope, scale, and efficiency of campaigns, and the outsized impact they can have on the health of the global information ecosystem.

The age-old adage that "a lie gets halfway around the world before the truth has a chance to put its shoes on," is now being borne out with data. A Massachusetts Institute of Technology (MIT) study[1] found that falsehoods are 70 percent more likely to be retweeted than the truth and they reach the first 1,500 people six times faster. The information ecosystem has become increasingly murky as propaganda campaigns flourish on the internet and social media and undermine trust in traditional news. In a 2021 study,[2] only seven percent of US adults said they have "a great deal" of trust and confidence in newspapers, television, and radio news reporting, while 34 percent reported "none at all."

Microsoft has been working to identify the main actors, threats, and tactics in the foreign cyber influence space and to share lessons learned. In June this year, we published a comprehensive report on the lessons learned from Ukraine, which contained a detailed look at Russia's cyber influence operations.[3]

We are also studying how advanced technologies such as deep fakes can be weaponized and undermine the credibility of journalists. And we are working with industry, government, and academia to develop better ways to detect synthetic media and restore trust—such as artificial intelligence (AI) systems that can spot fakes.

The rapidly changing nature of the information ecosystem and nation state online propaganda, including the melding of traditional cyberattacks with influence operations and the interference in democratic elections, requires a whole-of-society approach to mitigate against both online and offline threats to democracy.

Microsoft is dedicated to supporting a healthy information ecosystem in which trusted news and information thrive. We are developing tools and threat detection capabilities to combat the evolving and expanding risk of nation state driven influence operations. To enable this work, we recently acquired Miburo Solutions, we partner with third-party validators such as the Global Disinformation Index and NewsGuard, and we participate and at times lead multistakeholder partnerships, including the Coalition for Content Provenance and Authenticity (C2PA). Only by working together can we succeed in taking on those who seek to undermine democratic processes and institutions.

Teresa Hutson
Vice President, Technology and Corporate Responsibility

https://t.me/learningnets

Trends in cyber influence operations

Cyber influence operations are becoming increasingly sophisticated as technology evolves at pace. We are seeing an overlap and expansion of the tools used in traditional cyberattacks being applied to cyber influence operations. Additionally, we are seeing an increased coordination and amplification among nation states.

Microsoft invested in combating foreign influence operations this year by the acquisition of Miburo Solutions, a company specializing in analysis of foreign influence operations. Combining these analysts with Microsoft's threat context analysts, Microsoft formed the Digital Threat Analysis Center (DTAC). DTAC analyzes and reports on nation state threats, including both cyberattacks and influence operations, combining information and threat intelligence with geopolitical analysis to provide insights and inform effective response and protections.

More than three-quarters of people across the world said they worry about the weaponization of information,[4] and our data support these concerns. Microsoft and its partners have been tracking how nation state actors are using influence operations to achieve their strategic objectives and political goals. In addition to destructive cyberattacks and cyber espionage efforts, authoritarian regimes are increasingly using cyber influence operations to shape opinion, discredit adversaries, incite fear, promote discord, and distort reality.

These foreign cyber influence operations typically have three stages:

Pre-position

Like the pre-positioning of malware within an organization's computer network, foreign cyber influence operations pre-position false narratives in the public domain on the internet. The pre-positioning tactic has long helped more traditional cyber activities, especially if IT administrators scan their most recent network activity. Malware that lays dormant for an extended time on a network can make its subsequent use more effective. False narratives that lay unnoticed on the internet can make subsequent references seem more credible.

Launch

Often at the time most beneficial to achieve the goals of the actor, a coordinated campaign is launched to propagate narratives through government-backed and influenced media outlets and social media channels.

Amplification

Finally, nation state-controlled media and proxies amplify narratives inside targeted audiences. Often, unwitting tech enablers extend the narratives' reach. For example, online advertising can help finance activities and coordinated content delivery systems can flood search engines.

This three-step approach was applied in late 2021 to support the Russian false narrative around purported bioweapons and biolabs in Ukraine. This narrative was first uploaded to YouTube on November 29, 2021 as part of a regular English-language show by a Moscow-based American expatriate who claimed that US-funded biolabs in Ukraine were connected to bioweapons. The story went largely unnoticed for months. On February 24, 2022, just as Russian tanks crossed the border, the narrative was sent into battle. A data analytics team at Microsoft identified 10 Russian-controlled or influenced news sites that simultaneously published reports on February 24 pointing back to "last year's report" and seeking to give it credence. In addition, Russian Ministry of Foreign Affairs officials held press conferences that further seeded false claims about US biolabs in the information environment. Russian-sponsored teams then worked to amplify the narrative on social media and internet sites more broadly.

We are seeing authoritarian regimes around the world working together to pollute the information ecosystem to their mutual advantage. For instance, throughout the COVID-19 pandemic Russia, Iran, and China employed propaganda and influence operations using a blend of overt, semi-covert, and covert methods of dissemination to target democracies and further geopolitical goals (discussed further on page 76). The three regimes played on one another's messaging and information ecosystems to promote preferred narratives. Much of this coverage consisted of criticisms or conspiracy theories about the United States and its allies peddled by government figures in official statements while promoting their own vaccines and responses to COVID-19 as superior to the United States and other democracies. By amplifying one another, state operated media outlets created an ecosystem in which negative coverage of democracies—or positive coverage of Russia, Iran, and China—produced by one state media outlet was reinforced by others.

Illustration of how narratives about US biolabs and biological weapons spread via the three broad phases of many foreign influence operations—pre-position, launch, and amplification.

https://t.me/learningnets

Trends in cyber influence operations

Continued

To add to the challenge, private sector technology entities might unwittingly enable these campaigns. Enablers can include companies that register internet domains, host websites, promote material on social media and search sites, channel traffic, and help pay for these exercises through digital advertising. Organizations must be aware of the tools and methods employed by authoritarian regimes for cyber influence operations so they can detect and then prevent the spread of campaigns. There is also a growing need to help consumers develop a more sophisticated ability to identify foreign influence operations and limit engagement with their narratives or content.

Cyber influence operations, including authoritarian propaganda, are a threat to democracies worldwide as they erode trust, increase polarization, and threaten democratic processes.

Increased coordination and information sharing across government, the private sector, and civil society is needed to increase transparency and to expose and disrupt these influence campaigns.

Globally, more than three-quarters of people worry about how information is being weaponized.

https://t.me/learningnets

Spotlight on influence operations during COVID-19 and Russia's invasion of Ukraine

Nation states seeking to control the information environment throughout the pandemic and during the Russian invasion of Ukraine provide stark examples of how authoritarian regimes blend cyber and information operations.

COVID-19 propaganda

Russia, Iran, and China employed propaganda and influence campaigns throughout the COVID-19 pandemic. COVID-19 featured prominently in these campaigns in two central ways:

1. Representations of the pandemic itself.
2. Campaigns that used COVID-19 as a strategic device to achieve broader political objectives.

The broad objective of these types of campaigns is two-fold: first, to undermine democracies, democratic institutions, and the image of the United States and its allies on the global stage; and second, to bolster their own standing domestically and internationally.

An example of this can be seen in the messaging by known Russian accounts and media organizations targeting English language readers versus how the Russian government communicated with its own people regarding the vaccine and severity of COVID-19.

Topics covered by top 10 most-viewed coronavirus stories on RT.com
(October 2021–April 2022)

Anti-vaccine propaganda targets non-Russian readers

Russian (Translated below to English)	English
"Lockdowns and boosters prevent transmission"	"Vaccinations fail to curb transmission and are ineffective against new strains"
"Russian public figures are testing positive"	"Pfizer vaccine has dangerous side effects"
"Cases and deaths are increasing in Russia"	"Mass vaccination is politically motivated"
"The Sputnik V vaccine is highly effective"	"Pfizer and Moderna conduct unregulated trials"
"Vaccine proof needed on public transport"	

Russian COVID-19 messaging differs by language.

Campaigns that sought to obscure the origin of the COVID-19 virus offer another example. Since the start of the pandemic, Russian, Iranian, and Chinese COVID-19 propaganda boosted coverage from the others to amplify these central themes. Much of this coverage consisted of promoting criticisms or conspiracy theories about the United States. Regularly amplifying one another, state media outlets developed an ecosystem in which negative coverage of democracies or positive coverage of Russia, Iran, and China by one state media outlet was reinforced by the others time and again.

One such example is the early suggestion by Russian and Iranian state media that COVID-19 might be a bioweapon created by the United States. This claim circulated on fringe conspiracy websites early in the pandemic after an interview with a law professor who claimed he believed COVID-19 was created as a weapon.[6] After the interview was published on a few websites with limited reach, the story was picked up by state-owned media outlets. PressTV, an Iranian English and French language outlet sponsored by the Iranian government,[7] published an English-language story in February 2020 titled "Is coronavirus a US biowarfare weapon as Francis Boyle believes?" The article suggested the United States was behind the COVID-19 outbreak, writing, "in all US wars, radiological, chemical, biological and other banned weapons are used, inflicting a devastating toll on people in targeted areas."[8] Russian state media outlets and Chinese government accounts echoed the sentiment. Russia Today (RT)—a state-owned outlet known for its role in disseminating Kremlin propaganda[9]—published at least one story that promoted statements from Iranian officials claiming COVID-19 might be a "product of US 'biological attack' aimed at Iran & China"[10] and pushed out social media posts suggesting as much. For example, an RT tweet from February 27, 2020, read: "Show of hands, who isn't going to be surprised if it ever gets revealed that #coronavirus is a bioweapon?"[11]

The war in Ukraine—propaganda as a weapon of war

Russia's invasion of Ukraine provides a distinct example of how cyber influence operations can be melded with more traditional cyberattacks and on the ground military operations to maximize their impact.

In the lead up to the invasion of Ukraine, Microsoft threat intelligence analysts saw at least six separate Russia-aligned actors launch more than 237 cyberattacks against Ukraine. These campaigns sought to degrade services and institutions, disrupt Ukrainians' access to reliable information, and sow doubts about the country's leadership.

https://t.me/learningnets

Spotlight on influence operations during COVID-19 and Russia's invasion of Ukraine

Continued

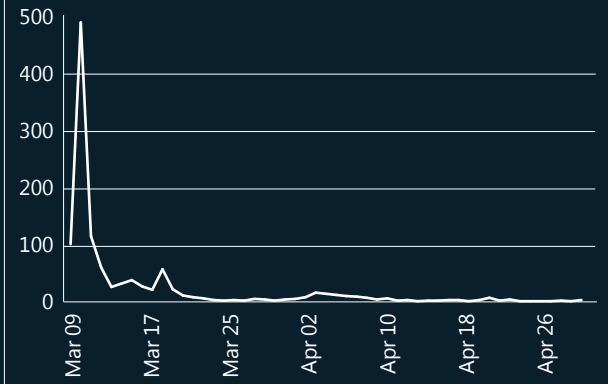
In a Microsoft report released in April 2022, we showcased how in an apparent attempt to control the information environment in Kyiv, Russia launched a missile strike against a TV tower in Kyiv on the same day it launched a destructive malware against a major Ukrainian media company.[12]

In another example of how cyberattacks and influence operations converge, a Russian threat actor sent Ukrainian citizens emails purporting to be from residents of Mariupol, blaming the Ukrainian government for the war's escalation and calling on their countrymen to push back against the government. These emails were specifically addressed (by name) to those receiving the email, indicating they might have had their information stolen in an earlier espionage related cyberattack. No malicious links were included, which suggests intent was pure influence operations.

Featuring purportedly hacked, leaked, or otherwise sensitive material is a common tactic used by Russian actors in influence operations. Throughout the war in Ukraine, pro-Russia social media channels have promoted what they claim are leaked or otherwise sensitive materials from Ukrainian sources. Leaked or sensitive material is used by pro-Russia social media channels and outlets as part of a broader influence strategy to degrade trust in institutions and cast doubt on mainstream narratives. This information can be manipulated to create propaganda targeting Ukraine and the West, diminish trust in digital security, and erode support for Western aid to Ukraine.

Russia used other information attacks to shape public opinion after events on the ground to obscure or undermine facts. For example, on March 7, Russia pre-positioned a narrative through a filing with the United Nations (UN) that a maternity hospital in Mariupol, Ukraine, had been emptied and was being used as a military site. On March 9, Russia bombed the hospital. After the news of the bombing broke, Russia's UN representative Dmitry Polyanskiy tweeted that coverage of the bombing was "fake news" and cited Russia's earlier claims about its alleged use as a military site. Russia then pushed this narrative broadly across Russian controlled websites for two weeks following the attack on the hospital.

Domains with traffic
(March 9, 2022–April 30, 2022)



Propaganda websites published stories about the maternity hospital for about two weeks with a brief revival beginning on April 1, 2022. Source: Microsoft AI for Good Lab.

Satellite images of a perinatal hospital in Mariupol in February and March 2022

Microsoft's own satellite image analysis showed the perinatal hospital was bombed. The first photo is from February 24, 2022 and the second is from March 24, 2022. Photo source: Planet Labs.

Russia's whitewashing of atrocities has continued as the war has progressed. For instance, in late June of 2022, Russian media outlets and influencers portrayed the bombing of a shopping mall as justified and necessary, falsely claiming it was not in use as a mall, but rather in use as an armory for Ukrainian territorial defense forces.[13] Several pro-Kremlin bloggers on Telegram posted and amplified content reinforcing the "false flag" narrative, with bloggers pointing to alleged indicators of fabrication including the presence of people in military uniform in footage from the scene[14] and the absence of women in the footage.[15] Russia launched campaigns by relying on a built-out system of propaganda messengers and mediums. The amplification of these stories online provides Russia the ability to deflect blame on the international stage and avoid accountability.

Nation states like Russia understand the value of using information derived from closed sources to influence public perceptions, using "hack and leak" campaigns to spread counter narratives and sow distrust.

Links to further information

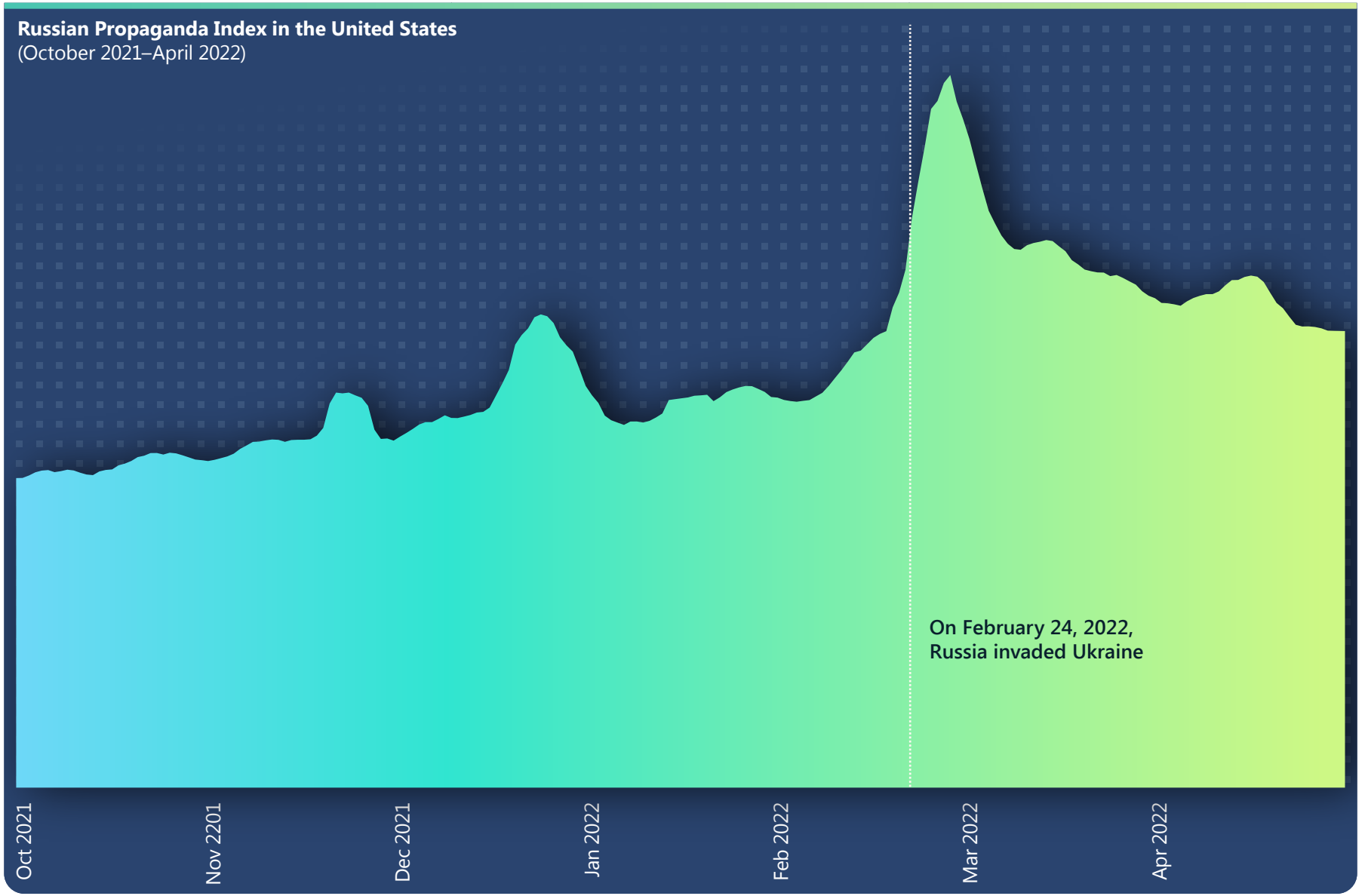
- Defending Ukraine: Early Lessons from the Cyber War | Microsoft On the Issues
- An overview of Russia's cyberattack activity in Ukraine | Microsoft Special Report
- Disrupting cyberattacks targeting Ukraine | Microsoft On the Issues

https://t.me/learningnets

Tracking the Russian Propaganda Index

In January 2022, nearly one thousand US websites were referring traffic to Russian propaganda websites. The most common topics for Russian propaganda websites targeting a US audience were the war in Ukraine, US domestic politics (either pro-Trump or pro-Biden) and COVID-19 and vaccine-related narratives.

The Russian Propaganda Index (RPI) monitors the flow of news from Russian state-controlled and sponsored news outlets and amplifiers as a proportion of overall news traffic on the internet. The RPI can be used to chart the consumption of Russian propaganda across the internet and in different geographies on a precise timeline. Microsoft notes, however, that we can only observe the Russian propaganda posted to previously identified websites. We do not have insight into propaganda on other types of websites, including authoritative news websites, unidentified websites, and social network groups.



https://t.me/learningnets

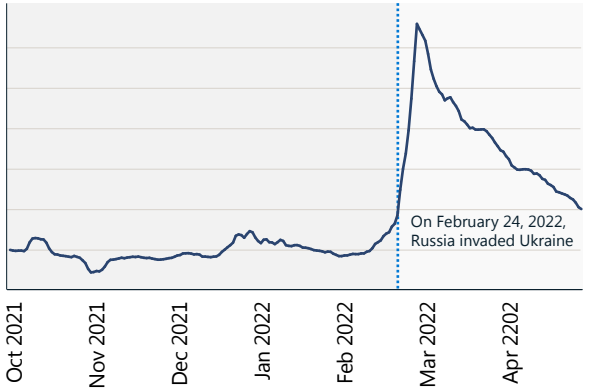
Tracking the Russian Propaganda Index

Continued

Russian Propaganda Index: Ukraine

When the Ukraine war began, we saw a 216 percent increase in Russian propaganda, peaking on March 2. The chart below shows how this sudden increase coincided with the invasion. The two graphs show how Russian propaganda surged soon after the invasion began.

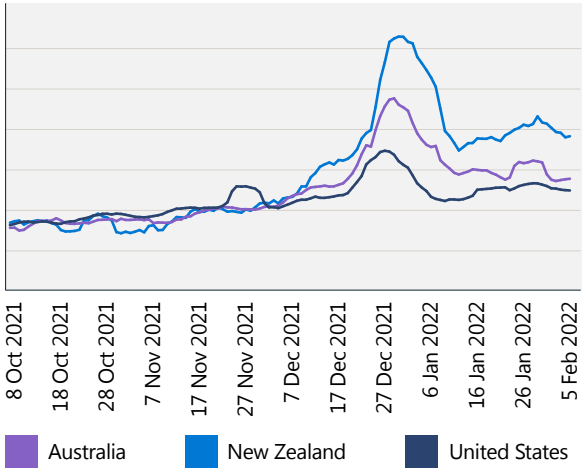
RPI, Ukraine
(October 7, 2021–April 30, 2022)



Russian Propaganda Index: New Zealand versus Australia and the United States

An assessment of the RPI in New Zealand showed a spike in late 2021 that was related to COVID-19 propaganda. This spike in Russian propaganda consumption in New Zealand preceded an increase in public protests in early 2022 in Wellington. A second spike was clearly related to the Russian invasion of Ukraine and exceeded the RPIs of Australia and the United States.

RPI, New Zealand versus Australia and the United States



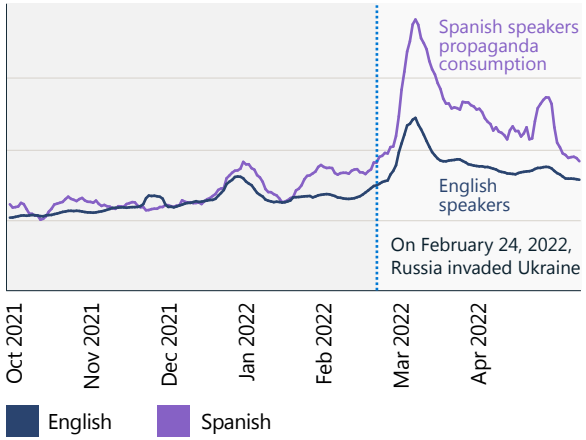
Russian propaganda consumption in New Zealand is similar to Australia until the first week of December 2021. After December, Russian propaganda consumption in New Zealand increased by over 30 percent relative to consumption in Australia and the United States.

Russian Propaganda Index in the United States: English and Spanish

The RPI also tracks propaganda across languages. Multiple outlets, including RT and Sputnik News, are available in over 20 languages. These include English, Spanish, German, French, Greek, Italian, Czech, Polish, Serbian, Latvian, Lithuanian, Moldavian, Belarusian, Armenian, Ossetian, Georgian, Azerbaijani, Arabic, Turkish, Persian, and Dari.

The following graph shows that the RPI for Spanish language news in the United States is much higher than for English language news.

Russian propaganda consumption is 2X higher among Spanish speakers



Russian propaganda consumption in the United States is two times higher among Spanish speakers.

Russian propaganda is high in Latin America

RT in Spanish is the international news outlet with the highest number of page views and Facebook followers.

Source: Microsoft AI for Good Research Lab

https://t.me/learningnets

Synthetic media

We are entering a golden era for AI-enabled media creation and manipulation. Microsoft analysts note this is driven by two key trends: the proliferation of easy-to-use tools and services for artificially creating highly realistic synthetic images, videos, audio, and text, and the ability to quickly disseminate content optimized for specific audiences.

Neither of these developments is inherently problematic on its own. AI-based technology can be used to create fun and exciting digital content, whether creating purely synthetic or enhancing existing material. These tools are being widely used by enterprises for advertising and communications and by individuals to create engaging content for their followers. However, synthetic media, when created and distributed with the intent to harm, has the potential to do serious damage to individuals, companies, institutions, and society. Microsoft has been a driving force in developing technologies and practices, both internally and across the wider media ecosystem, to limit this harm.

This section explores insights from Microsoft analysis on the current state of the art technology for creating damaging synthetic content, the harms that can arise if this content is widely disseminated, and technical mitigations that can defend against synthetic media based cyber threats.

Creating synthetic media

The field of synthetic text and media is advancing incredibly fast as techniques that were once only possible with the vast computing resources of large movie studios are now integrated into phone apps. At the same time, tools are becoming easier to use and can generate content with a level of realism that can fool even forensic media specialists. We are very close to reaching the point at which anyone can create a synthetic video of anyone saying or doing anything. It's not unreasonable to believe we are entering an era where a significant quantity of the content we see online is fully or partially synthetic using AI techniques.

> With the availability of more sophisticated, easy-to-use, and widely available tools, synthetic content creation is on the rise and will soon be indistinguishable from reality.

There are many high-quality free and commercial image, video, and audio editing tools. These tools can be used to make simple but potentially damaging changes to digital content like adding misleading text, face-swapping, and removing or altering context. Such "cheap fakes" are widely used to spread nefarious content, promote political ideologies, and damage reputations. A well-known example is the 2019[16] video of US Speaker of the House, Nancy Pelosi, slurring her speech and appearing inebriated. Although it was quickly determined that the video was slowed to create the effect, the "cheap fake" spread far and wide before the original video and context surfaced.

More sophisticated approaches to altering media content includes the application of advanced AI techniques to (a) create purely synthetic media, and (b) make more sophisticated edits of existing media. The term deepfake is often used for synthetic media that has been created using cutting-edge AI techniques (the name comes from the deep neural networks that are sometimes used). These technologies are being developed as standalone apps, tools, and services and integrated into established commercial and open-source editing tools.

Such technologies are weaponized by bad actors hoping to damage individuals and institutions. Examples of deepfake techniques include:

- **Face swap (video, images)**—replacing a face in a video with another. This technique can be used to attempt blackmail of an individual, company, or institution, or to place individuals in embarrassing locations or situations.
- **Puppeteering (video, images)**—using a video to animate a still image or second video. This can make it appear an individual said something embarrassing or misleading.
- **Generative adversarial networks (video, images)**—a family of techniques for generating photorealistic imagery.
- **Transformer models (video, images, text)**—creating rich imagery from text descriptions.

Such advanced AI-based techniques are not yet widely used in cyber influence campaigns today, but we expect the problem to grow as the tools become easier to use and more widely available.

The impact of synthetic media manipulation

The use of information operations to cause harm or expand influence is not new. However, the speed with which information can spread, and our inability to quickly sort fact from fiction, mean the impact and harm caused by fakes and other synthetically generated malicious media can be much greater, as demonstrated with the Pelosi example.

There are several categories of harm which we consider: market manipulation, payment fraud, vishing, impersonations, brand damage, reputational damage, and botnets. Many of these categories have widely reported real-world examples, which could undermine our ability to separate fact from fiction.

A longer-term and more insidious threat is to our understanding of what is true if we can no longer trust what we see and hear. Because of this, any compromising image, audio, or video of a public or private figure can be dismissed as fake—an outcome known as The Liar's Dividend.[17] Recent research[18] shows this abuse of technology is already being used to attack financial systems, although many other abuse scenarios are plausible.

https://t.me/learningnets

Synthetic media

Continued

Detecting synthetic media

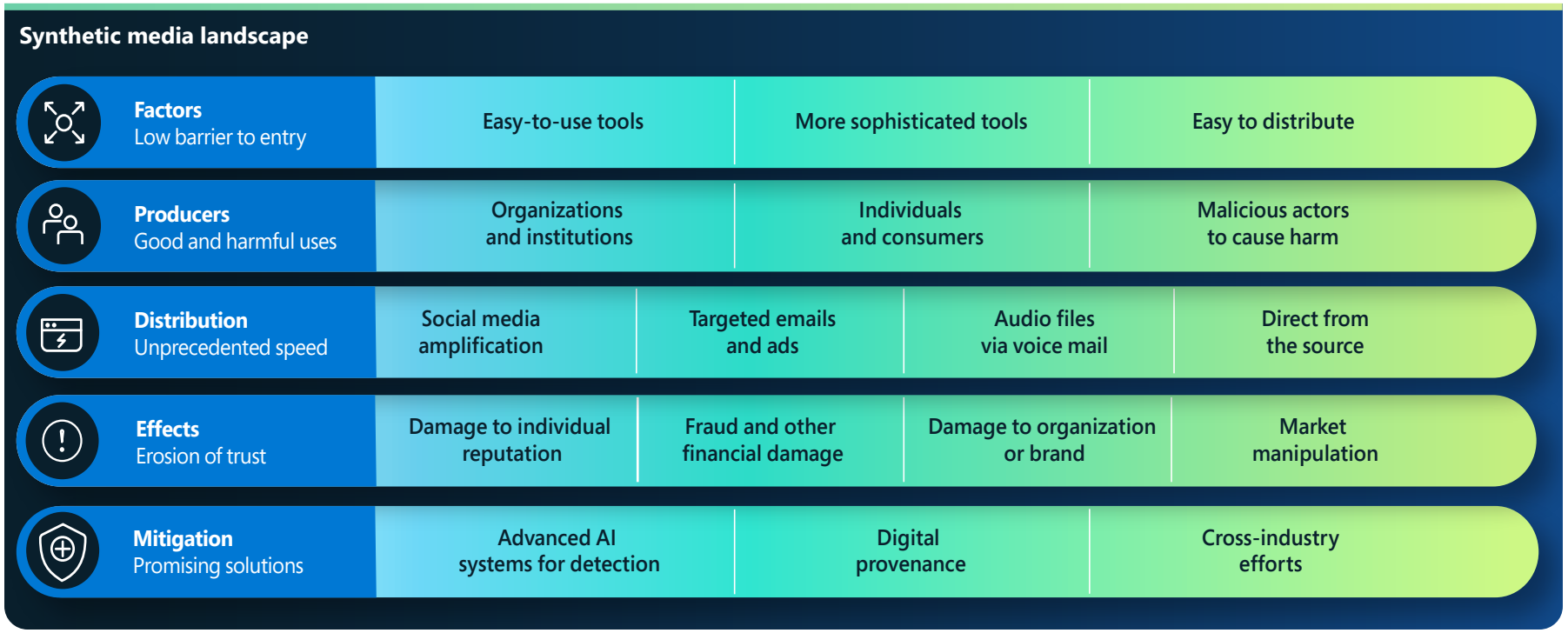
Efforts are underway across industry, government, and academia to develop better ways to detect and mitigate synthetic media and restore trust. There are several promising paths forward, as well as barriers that warrant consideration.

One approach is to build AI-based systems that can spot fakes—essentially "defensive" AI systems to counter the offensive AI systems. This is an area of active research where current systems for creating synthetic audio and video leave telltale artifacts that can be spotted by trained media forensic analysts and automated tools.

Unfortunately, while current fakes have revealing flaws, the precise artifacts tend to be specific to a particular tool or algorithm. This means training on known fakes does not usually generalize to other algorithms as demonstrated in a 2020 open competition to build deepfake image detectors.[19] It is tempting to increase investment in developing more advanced detectors, but Microsoft is highly skeptical this will result in meaningful improvements for two reasons:

First, we have excellent physical models that reflect the real world. Current fake creators cut corners, resulting in detectable artifacts, but newer models will become ever more realistic. There is nothing inherently special about a real-world scene captured by a camera that can't be modeled by a computer.

Second, advanced fake-creation algorithms use a technique called Generative Adversarial Networks (GANs) as part of the creation process. A GAN plays two AI systems against each other using a generator to create the fake and a discriminator to detect fake images and train the generator. Any investment in developing a better detector will only enable the generator to improve the quality of the fakes.



https://t.me/learningnets

Synthetic media

Continued

Provenance for digital assets

If detecting fakes is unreliable, what can be done to protect against the harmful uses of synthetic media? One important emerging technology is digital provenance—a mechanism that enables digital media creators with the ability to certify an asset and helps consumers identify whether or not the digital asset has been tampered with. Digital provenance is particularly important in the context of today's social media networks given the speed with which content can travel the internet and the opportunity for bad actors to easily manipulate content.

Digital Provenance Technology is a modern version of cryptographic document signing, designed to capture the source, edit history, and metadata of objects as they flow through today's web. The vision and technical methods for enabling this type of end-to-end tamper-proof certification of media was developed by a cross-team of researchers and scientists at Microsoft. We co-lead a cross-industry partnership aimed at bringing media provenance technology to life in Project Origin (founded by Microsoft, BBC, CBC/Radio-Canada, and the New York Times) and engage in the Content Authenticity Initiative (founded by Adobe). Microsoft also worked with partners in technology and media services to establish the Coalition for Content Provenance and Authenticity (C2PA). C2PA is a standards organization that recently published the most advanced digital provenance specification to utilize with media assets including images, videos, audio, and text.

A C2PA-enabled object carries a manifest that protects the object and metadata from tampering, and the accompanying certificate identifies the publisher.

Synthetic media was not originally designed to cause harm, but it is being weaponized by bad actors to undermine trust in individuals and institutions.

Digital provenance is a promising emerging technology that has the potential to help restore people's trust in online media content by certifying the origin of a media asset.

Publicly available solutions based on the C2PA specification are surfacing either as a new feature in existing products or new standalone apps and services. We expect most of the commonly used capture, editing, and authoring tools to be C2PA enabled in a few years. This presents an opportunity for enterprises to determine their needs and uses for digital provenance today, and to require this additional layer of protection in the tools they use in existing workflows.

Actionable insights

1. Take proactive steps to protect your organization against misinformation threats through proactive consideration of your PR and communication responses.
2. Use provenance technology to protect official communications.

Links to further information

- A promising step forward on disinformation | Microsoft On the Issues
- A Milestone Reached, January 31, 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Explore technical details about the system Project Origin uses for media authentication | Microsoft ALT Innovation

900%

year over year increase in proliferation of deepfakes since 2019.[20]

https://t.me/learningnets

A holistic approach to protect against cyber influence operations

Microsoft is building on its already mature cyber threat intelligence infrastructure to develop a broader, more inclusive view of cyber influence operations.

We use a framework for suggested response and mitigation strategies to combat the threat posed by operations, which can be divided into four key pillars: detect, disrupt, defend, and deter.

In addition, Microsoft has adopted four principles to anchor our work in this space. First is a commitment to respect freedom of expression and uphold our customers' ability to create, publish, and search for information via our platforms, products, and services. Second, we proactively work to prevent our platforms and products from being used to amplify foreign cyber influence sites and content. Third, we will not willfully profit from foreign cyber influence content or actors. Finally, we prioritize surfacing content to counter foreign cyber influence operations by utilizing internal and trusted third-party data on our products.

Detect

As with cyber defense, the first step in countering foreign cyber influence operations is developing the capacity to detect them. No single company or organization can hope to individually make the progress that is needed. New, broader collaboration across the tech sector will be crucial, with progress in analyzing and reporting cyber influence operations relying heavily on the role of civil society, including in academic institutions and nonprofit organizations.

Recognizing this role, researchers Jake Shapiro and Alicia Wanless at Princeton University and the Carnegie Endowment for International Peace respectively have mapped out plans to launch the new "Institute for Research on the Information Environment" (IRIE). With support from Microsoft, the Knight Foundation, and Craig Newmark Philanthropies, the IRIE will create an inclusive multistakeholder research institution modeled after the European Organization for Nuclear Research (CERN). It will combine expertise in data processing and analysis to speed up and scale new discoveries in this space. Findings will be shared to inform policymakers, technology companies, and consumers more broadly.

Defend

The second strategic pillar is to shore up democratic defenses, a longstanding priority in need of investment and innovation. It should take account of the challenges technology has created to democracy, and the opportunities technology has created to defend democratic societies more effectively.

Microsoft's strategy framework is aimed at helping cross-sectoral stakeholders detect, disrupt, defend, and deter against propaganda—particularly campaigns by foreign aggressors.

It is appropriate to start with one of the great technological challenges of our age—the impact of the internet and digital advertising on traditional journalism. Since the 1700s, a free and independent press has played a special role in supporting every democracy on the planet—uncovering corruption, documenting wars, and illuminating the largest societal challenges of this and every other time. However, the internet has gutted local news by devouring advertising revenue and luring away paid subscribers. Many local newspapers have collapsed. One of the many insights from our recent work is towns that lack a newspaper are unknowingly and inevitably exposed to a greater than average volume of foreign propaganda. For these reasons, one of democracy's critical defensive prongs must strengthen traditional journalism and a free press, especially at the local level. This requires ongoing investment and innovation that must reflect the local needs of different countries and continents. These issues are not easy, and they require multistakeholder approaches, which Microsoft and other tech companies are increasingly supporting.

We also need new innovations in public policy, which needs to be a public priority. This can include laws that enable publishers to negotiate advertising revenue collectively with technology companies, and legislation that provides tax credits to relieve local newsrooms of a portion of their payroll taxes for journalists they employ. Journalists need many other tools for their craft, including the ability to separate content from legitimate and fraudulent sources.

There is also a rapidly evolving need to help consumers develop a more sophisticated ability to identify nation state-driven information operations. While this might seem daunting, it resembles the work the tech sector has long pursued to combat other cyber threats. Consider the education of consumers to look more carefully at an email address to help spot spam or other fraudulent communications. Initiatives in the United States—such as the News Literacy Project and the Trusted Journalism.

A longer-term and more insidious threat is to our understanding of what is true if we can no longer trust what we see and hear.

https://t.me/learningnets

A holistic approach to protect against cyber influence operations

Continued

Program—are helping to develop better informed consumers of news and information. Globally, new technology like the browser plugin from NewsGuard can help move this effort forward much faster.

This also should remind us that part of the foundation for democracy is an education in civics. As always, this effort needs to start in schools. But we live in a world that requires we receive ongoing civics education throughout our lifetime. The new Civics at Work pledge, led by the Center for Strategic and International Studies, and of which Microsoft was an inaugural signatory and partner, seeks to reinvigorate civics literacy within corporate communities. It is a good example of the breadth of opportunity to strengthen our democratic defenses.

Disrupt

In recent years, Microsoft's Digital Crimes Unit (DCU) has refined tactics and developed tools to disrupt cyber threats ranging from ransomware to botnets and nation state attacks. We have learned many critical lessons, starting with the role of active disruption in countering a broad range of cyberattacks.

As we think about countering cyber influence operations, disruption might play an even more important role and the best approach to disruption is becoming clearer. The most effective antidote to broad deception is transparency. That is why Microsoft increased its capacity to detect and disrupt nation state influence operations by acquiring Miburo Solutions, a leading cyber threat analysis and research company specializing in the detection of and response to foreign cyber influence operations.

Our experience has shown that governments, technology companies, and NGOs should attribute cyberattacks carefully and with ample evidence. Understanding the impact of such disruption is vital and can be even more helpful in disrupting cyber influence. Witness the US government's information-sharing in the lead-up to Russia's invasion of Ukraine that put transparency into effective action—such as exposing Russian plans including specific campaigns like a plot to use a fake graphic video.

As shown in last summer's publication from the CyberPeace Institute in Geneva on ongoing cyberattacks inside and outside Ukraine, there is an opportunity for a broad range of civil society and private-sector organizations to advance transparency relating to cyber influence operations. Reliable reports about newly discovered and well-documented operations can help the public better evaluate what it reads, sees, and hears, especially on the internet. To this end, Microsoft will build on and extend its existing cyber reports and will release new reports, data, and updates related to what we discover about cyber influence operations, including attribution statements when appropriate. We will publish an annual report that uses a data-driven approach to look across the company at the prevalence of foreign information operations and next steps to ensure incremental improvement. We will also consider additional steps that build on this type of transparency.

The role of digital advertising is especially important, for instance, since advertising can help fund foreign operations while simultaneously creating an appearance of legitimacy for foreign-sponsored propaganda sites. New efforts will be needed to disrupt these financial flows.

Deter

Finally, we cannot expect nations to change behavior if there is no accountability for violating international rules. Enforcing such accountability is uniquely a governmental responsibility. Yet increasingly, multistakeholder action is playing an important role in strengthening and extending international norms. More than 30 online platforms, advertisers, and publishers—including Microsoft—signed on to the recently updated European Commission's Code of Practice on Disinformation, agreeing to strengthened commitments to tackle this growing challenge. Like the recent Paris Call, Christchurch Call, and Declaration on the Future of the Internet, multilateral and multistakeholder action can bring together the governments and public among democratic nations. Governments can then build on these norms and laws to advance the accountability the world's democracies need and deserve.

Through rapid radical transparency, democratic governments and societies can effectively blunt influence campaigns by attributing the source of nation state attacks, informing the public, and building trust in institutions.

We have increased technical capacity to detect and disrupt foreign influence operations and are committed to transparently reporting on these operations like our reporting on cyberattacks.

Actionable insights

1. Implement strong digital hygiene practices across your organization.
2. Consider ways to reduce any unintended enabling of cyber influence campaigns by your employees or your business practices. This includes reducing supply to known foreign propaganda sites.
3. Support information literacy and civic engagement campaigns as a key component to help societies defend against propaganda and foreign influence.
4. Engage directly with groups relevant to your industry working to address influence operations.

https://t.me/learningnets

Endnotes

1 https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2 https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3 Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)
4 https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5 Russian Foreign Ministry Spokeswoman Maria Zakharova: https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6 https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7 https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8 https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9 https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10 https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11 https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13 Russia's Kremenchuk Claims Versus the Evidence—bellingcat
14 https://t.me/oddr_info/39658
15 https://t.me/voenacher/23339
16 Fact check: "Drunk" Nancy Pelosi video is manipulated | Reuters
17 https://lawcat.berkeley.edu/record/1136469
18 https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19 Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20 Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas, and Kristjan Peterson, October 2020

https://t.me/learningnets

Cyber Resilience

Understanding the risks and rewards of modernization becomes crucial to a holistic approach to resilience.

An overview of Cyber Reslience 87
Introduction 88
Cyber resiliency: A crucial foundation of a connected society 89
The importance of modernizing systems and architecture 90
Basic security posture is a determining factor in advanced solution effectiveness 92
Maintaining identity health is fundamental to organizational well-being 93
Operating system default security settings 96
Software supply chain centrality 97
Building resilience to emerging DDoS, web application, and network attacks 98
Developing a balanced approach to data security and cyber resiliency 101
Resilience to cyber influence operations: The human dimension 102
Fortifying the human factor with skilling 103
Insights from our ransomware elimination program 104
Act now on quantum security implications 105
Integrating business, security, and IT for greater resilience 106
The cyber resilience bell curve 108

https://t.me/learningnets

An overview of

Cyber Resilience

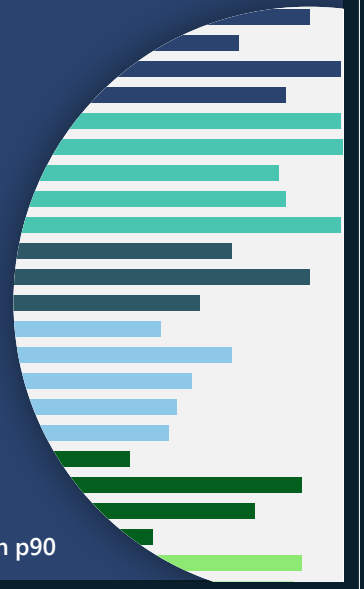
Cyber security is a key enabler of technological success. Innovation and enhanced productivity can only be achieved by introducing security measures that make organizations as resilient as possible against modern attacks.

The pandemic has challenged us to pivot our security practices and technologies to protect Microsoft's employees wherever they work. This past year, threat actors continued to take advantage of vulnerabilities exposed during the pandemic and the shift to a hybrid work environment. Since then, our principal challenge has been managing the prevalence and complexity of various attack methods and increased nation state activity.

Effective cyber resiliency requires a holistic, adaptive approach to withstand evolving threats to core services and infrastructure.

Find out more on p89

Modernized systems and architecture are important for managing threats in a hyperconnected world.

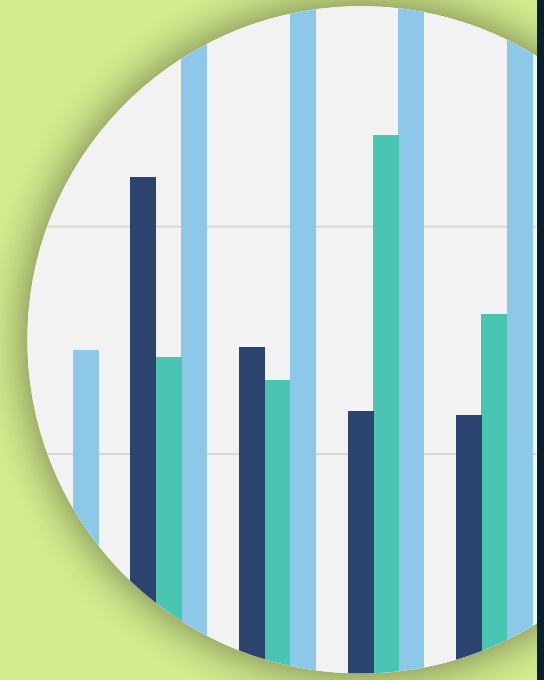


Find out more on p90

Basic security posture is a determining factor in advanced solution effectiveness.

Find out more on p92

While password-based attacks remain the main source of identity compromise, other types of attacks are emerging.



Find out more on p93

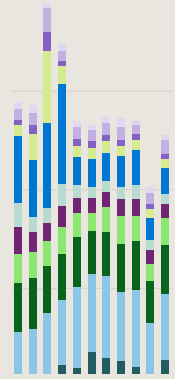
The human dimension of resilience to cyber influence operations is our ability to collaborate and cooperate.

Find out more on p102

The vast majority of successful cyberattacks could be prevented by using basic security hygiene.

Find out more on p108

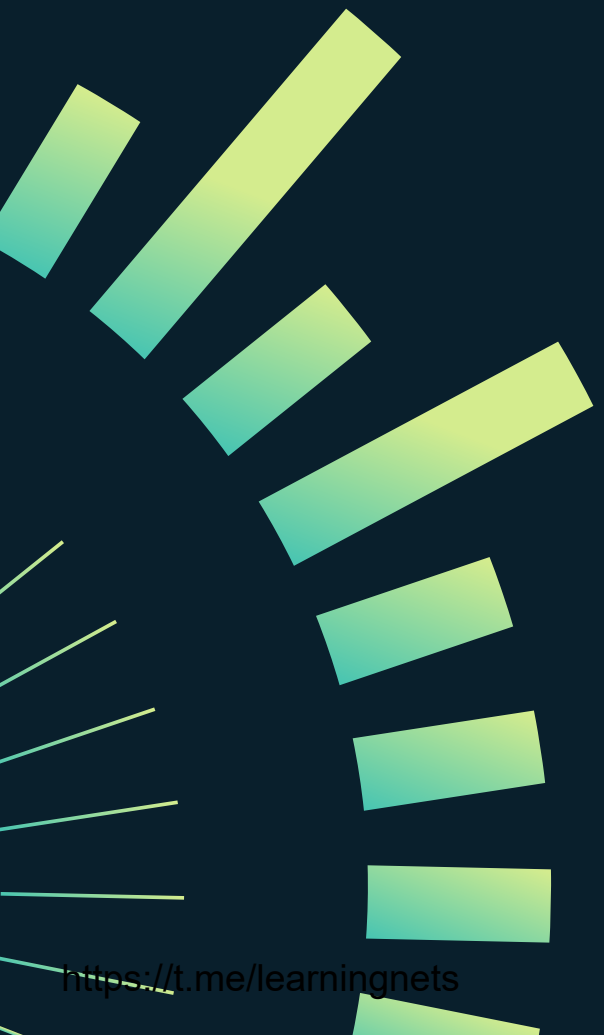
Over the past year, the world experienced DDoS activity that was unprecedented in volume, complexity, and frequency.



Find out more on p98

https://t.me/learningnets

Introduction



The pandemic challenged us to pivot our security practices and technologies to protect Microsoft's employees wherever they work. This past year, threat actors continued to take advantage of vulnerabilities exposed during the pandemic and the shift to a hybrid work environment. Since then, our principal challenge has been managing the prevalence and complexity of various attack methods and increased nation state activity.

Digital threat activity and the level of cyberattack sophistication increases every day. Many of today's complex attacks focus on compromising identity architectures, supply chains, and third parties with varying degrees of security controls. In particular, we have observed identity phishing attacks are a clear and present threat. However, these types of attacks are generally unsuccessful with good identity management, phishing control, and endpoint management practices.

As a result, we must remember the basics: ninety eight percent of attacks can be stopped with basic hygiene measures in place. At Microsoft, we manage identities and devices as part of our Zero Trust approach, which includes least privileged access and phish resistant credentials to effectively stop threat actors and keep our data protected.

Today, even threat actors who lack sophisticated technical skills can launch incredibly destructive attacks, as access to advanced tactics, techniques, and procedures become broadly available in the cybercrime economy. The war in Ukraine demonstrated how nation state actors have escalated their offensive cyber operations through the increased use of ransomware. Ransomware is now a sophisticated industry with threat actors using double or triple extortion tactics to extract a pay out and developers offering ransomware as a service (RaaS). With RaaS, threat actors utilize an affiliate network to carry out attacks, lowering the barrier to entry for less skilled cybercriminals and, ultimately, expanding the attacker pool.

As a result, Microsoft designed a ransomware elimination program. The goal of the program is to remediate gaps in controls and coverage, contribute to feature enhancements for services, and develop recovery playbooks for our security operations center and engineering teams in the event of a ransomware attack.

Recent supply chain and third-party supplier attacks indicate a major inflection point in the industry. The disruption these attacks cause for our customers, partners, governments, and Microsoft continues to increase, illustrating the importance of focused attention on cyber resiliency and collaboration across security stakeholders. Adversaries are also targeting on premises systems, reinforcing the need for organizations to manage vulnerabilities posed with legacy systems by modernizing and moving infrastructure to the cloud where security is more robust.

We live in an era where security is a key enabler of technological success. Innovation and enhanced productivity can only be achieved by introducing security measures that make organizations as resilient as possible against modern attacks. As digital threats increase and evolve, it's crucial to build cyber resilience into the fabric of every organization.

Bret Arsenault
Chief Information Security Officer

https://t.me/learningnets

Cyber resiliency: A crucial foundation of a connected society

The revolution in digital technology has seen organizations transform to become ever more connected in both the way they operate and the services they offer. As threats in the cyber landscape increase, building cyber resilience into the fabric of the organization is as crucial as financial and operational resilience.

Digital transformation has forever altered the way organizations interact with customers, partners, employees, and other stakeholders. New technologies provide huge opportunities to engage with people, transform products, and optimize operations. The pandemic accelerated the digital transformation by driving innovative technologies which allow people to collaborate in new ways and from any location.

As cyber threats become endemic, preventing them from compromising an organization becomes more difficult in our "always connected" world. Cyber resiliency represents an organization's ability to continue operations and sustain growth acceleration despite the barrage of attacks. Prevention must be balanced with survival and recovery capabilities and governments and enterprises are developing comprehensive models that extend beyond security and privacy to protect assets, data, and other resources as part of cyber resiliency.

Developing a holistic approach to cyber resiliency

Cyber resiliency requires a holistic, adaptive, and global approach that can withstand evolving threats to core services and infrastructure, including:

- Basic cyber hygiene as described in our cyber resilience bell curve.
- Understanding and managing the risk/reward trade-off of digital transformation.
- Real-time response capabilities that enable proactive detection of threats and vulnerabilities.
- Protection against known attacks and preventive activity against new and anticipated attack vectors, including ability to automatically remediate.
- Reduced impact of attacks and disasters through fault isolation and segmentation.
- Automated recovery and redundancy in the event of disruption.
- Prioritizing operational testing to find gaps and understanding shared responsibilities and dependencies on external resources such as cloud-based security solutions.

An effective cyber resiliency program begins with resource fundamentals such as understanding services available and having a reliable catalog of resources that can be called upon in the event of a disruption. Building on that foundation, the program must be able to assess its own effectiveness, measure the performance of critical services and their dependencies, test and validate capabilities across on-premises and cloud services, and feed continuous improvement across the organization's digital lifecycle.

To deliver a holistic approach, we are partnering with organizations to identify their most critical on-premises and online services, business processes, dependencies, personnel, vendors and suppliers. We also look to identify assets and resources associated with customer and market expectations, regulatory and contractual obligations, and internal operations. As these critical resources are identified, parallel efforts should detect and monitor threats, disruptions, potential attack vectors, and system and process vulnerabilities. The ability to do this under the current skills shortage requires rigor in prioritization based on overall risk posed to the organization.

This type of holistic approach needs to be adaptive against a backdrop of a continually evolving threat landscape, with a goal of driving measurable performance enhancement, reduced time to detect, respond and recover, and reduced radius of impact in the event of disruption. The approach must also recognize the increasing connectedness of threats. For example, a security incident might result in a data breach with privacy implications, requiring many internal and external teams to work together to respond quickly and minimize impact.

Cyber resiliency is the ability of an enterprise to continue operations and sustain growth acceleration despite disruptions, including cyberattacks.

Actionable insights

1. Build and manage technology systems that limit the impact of a breach and enable them to continue to operate securely and effectively, even if a breach is successful. Focus on common critical assets, support for agility, and architect for adaptability (for example, hybrid and multi-cloud, multi-platform), reduce attack surfaces (for example, remove unused applications and over-provisioned access rights), assume compromised resources, and expect adversaries to evolve.
2. When planning digital projects, consider potential threats alongside opportunities, and shared responsibilities for resilience across the digital technology supply chain, including cloud-based security solutions.
3. Build systems to embed security by design and take steps to anticipate, detect, withstand, adapt, and respond to future evolving threats.
4. Ensure business leaders consult with security teams as necessary to understand the risks associated with new developments. Likewise, security teams should consider business aims and advise leaders on how to pursue them securely.
5. Ensure clear operational practices and procedures for organizational resilience are in place for cyber incidents.

https://t.me/learningnets

The importance of modernizing systems and architecture

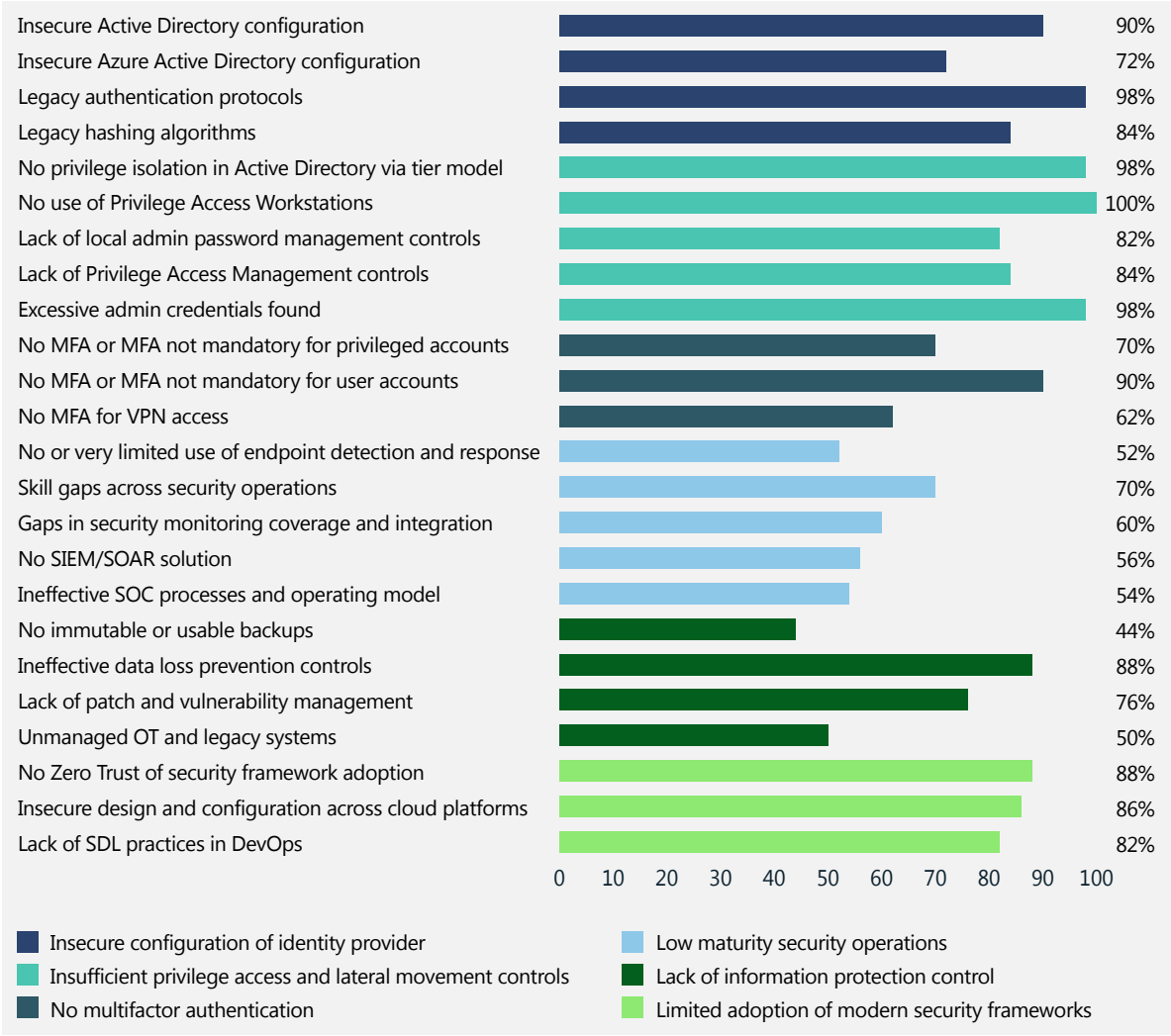
As we develop new capabilities for a hyperconnected world, we must manage the threats posed by legacy systems and software.

Legacy systems—those developed before modern connectivity tools such as smartphones, tablets, and cloud services became the norm-represent a risk to an organization still using them. This risk exposure is reinforced by the findings of the Microsoft Security Services for Incident Response team, a group of security professionals that helps customers respond to and recover from attacks.

Over the past year, issues found among customers recovering from attacks were related to six categories as shown in the chart on this page. The following page outlines actionable steps to take for improved resilience.

Over 80 percent of security incidents can be traced to a few missing elements that could be addressed through modern security approaches.

Key issues impacting cyber resiliency



This chart shows the percentage of impacted customers missing basic security controls which are critical to increasing organizational cyber resilience. Findings are based on Microsoft engagements over the past year.

"Leaders should think about cyber resilience as a critical facet of business resilience. They should plan for cyber disruptions in the same way they do natural disasters or other unforeseen events and bring together internal stakeholders like operations, communications, legal, and more, to craft strategies. Doing so will help ensure organizations bring their critical business systems back online as quickly as possible to resume normal business operations.

But it doesn't stop there. As many organizations rely on third-party suppliers and service providers, leaders should extend cyber resilience planning to their end-to-end value chain to further ensure business continuity and resilience."

Ann Johnson,
Corporate Vice President of Security, Compliance, Identity, and Management Business Development

https://t.me/learningnets

The importance of modernizing systems and architecture

Continued

There are clear areas which organizations can address to modernize their approach and protect from threats:

Problem	Actionable steps
Insecure configuration of identity provider Misconfiguration and exposure of identity platforms and its components are a common vector for gaining unauthorized high privilege access.	Follow security configuration baselines and best practices when deploying and maintaining identity systems such as AD and Azure AD infrastructure. Implement access restrictions by enforcing segregation of privileges, least privilege access and utilizing privileged access workstations (PAW) for managing identity systems.
Insufficient privilege access and lateral movement controls Administrators have excessive permissions across the digital environment and often expose administrative credentials on workstations subject to internet and productivity risks.	Secure and limit administrative access to make the environment more resilient and limit the scope of an attack. Employ Privilege Access Management controls such as just in time access and just enough administration.
No multifactor authentication (MFA) Today's attackers do not break in, they log on.	MFA is a critical and fundamental user access control that all organizations should enable. Coupled with conditional access, MFA can be invaluable in fighting cyber threats.
Low maturity security operations Most impacted organizations used traditional threat detection tools and did not have relevant insights for timely response and remediation.	A comprehensive threat detection strategy requires investments in extended detection and response (XDR) and modern cloud native tools employing machine learning to separate noise from signals. Modernize security operations tools by incorporating XDR that can provide deep security insights across the digital landscape.
Lack of information protection control Organizations continue to struggle to put together holistic information protection controls that have full coverage across data locations and remain effective throughout the information lifecycle and are aligned with business criticality of data.	Identify your critical business data and where it is located. Review information lifecycle processes and enforce data protection while ensuring business continuity.
Limited adoption of modern security frameworks Identity is the new security perimeter, enabling access to disparate digital services and computing environments. Integrating Zero trust principles, application security and other modern cyber frameworks enables organizations to proactively manage risks which otherwise organizations might struggle to envision.	Zero Trust frameworks enforce concepts of least privilege, explicit verification of all access, and always assume compromise. Organizations should also implement security controls and practices in DevOps and application lifecycle processes for higher assurance levels in their business systems.

https://t.me/learningnets

Basic security posture is a determining factor in advanced solution effectiveness

Through our analysis, we discovered a prevalence of common blind spots in organizational defenses which enable attackers to gain initial access, establish a toehold, and implement an attack, even in the presence of advanced security solutions.

In many cases, the outcome of a cyberattack is determined long before the attack begins. Attackers leverage vulnerable environments to gain initial access, conduct surveillance, and wreak havoc via lateral movement and encryption or exfiltration. Stopping an attacker at an early stage greatly increases the opportunity to reduce the overall impact.

Microsoft studied specific configurations in security postures to identify the most common shortcomings in actual practice in these environments. This enabled us to see the most common vulnerabilities exploited during human operated ransomware attacks that allowed the threat actors to gain access and travel through a network undetected.

Basic security configurations must be turned on

An organization's devices which are not onboarded or are outdated (both in relation to vulnerabilities and security agent status) serve as potential entry points and access establishment routes for attackers. We found that while ensuring organizational devices are onboarded with an updated endpoint detection and response[1] (EDR) and endpoint protection platform[2] (EPP) solution is an important step, it is not guaranteed to stop ransomware.

Advanced solutions such as EDR and EPP are critical in detecting an attacker early in the attack flow and enabling automatic remediation and protection. However, since these advanced solutions rely on a fundamental ability to detect an attack, they require basic security configurations to be turned on. In fact, we observed a prevalence of scenarios with advanced solutions in place that were undermined by the absence of basic security configurations.

Best practices in security configurations is a greater indicator of resilience than security operations center (SOC) analyst response time

We observed a 70 percent reduction in the time it takes a SOC analyst to view and act on a relevant alert over a six-month period across our customer and partner population. This increased awareness is a good sign. However, while security configuration visibility improved SOC analyst performance, enabling product visibility by onboarding and updating the organization's devices was a greater predictor of successful prevention.

Risk posed by unknown devices

In contrast to cloud networks, where customers know which assets are running on which operating systems, on-premises networks can contain a wide variety of devices such as IoT, desktops, servers, and network devices that are not monitored or managed by the organization.

The average enterprise network has over 3,500 connected devices that are not protected by an EDR agent and might have access to enterprise resources or even to high value assets. Microsoft Defender for Endpoint (MDE) uses network inspection to discover devices and provide information about device classifications for those connected to the network such as device name, operating system distribution, and device type.

3,500

average number of connected devices in an enterprise that are not protected by an endpoint detection and response agent.

For devices not supported by an EDR agent, at least be aware of their existence and act to protect them by assessing vulnerabilities, as well as restricting network access.

Actionable insights

1. Even advanced solutions can be undermined by the absence of basic security configurations.
2. Invest in best practices in security posture configurations to protect against future attacks. These basic settings produce a massive return on investment in terms of an organization's ability to defend against attacks.
3. Onboard all applicable devices to an EDR solution.
4. Be sure to update security agents and ensure protection from tampering to enable greater visibility and fuller protection benefits of products.

https://t.me/learningnets

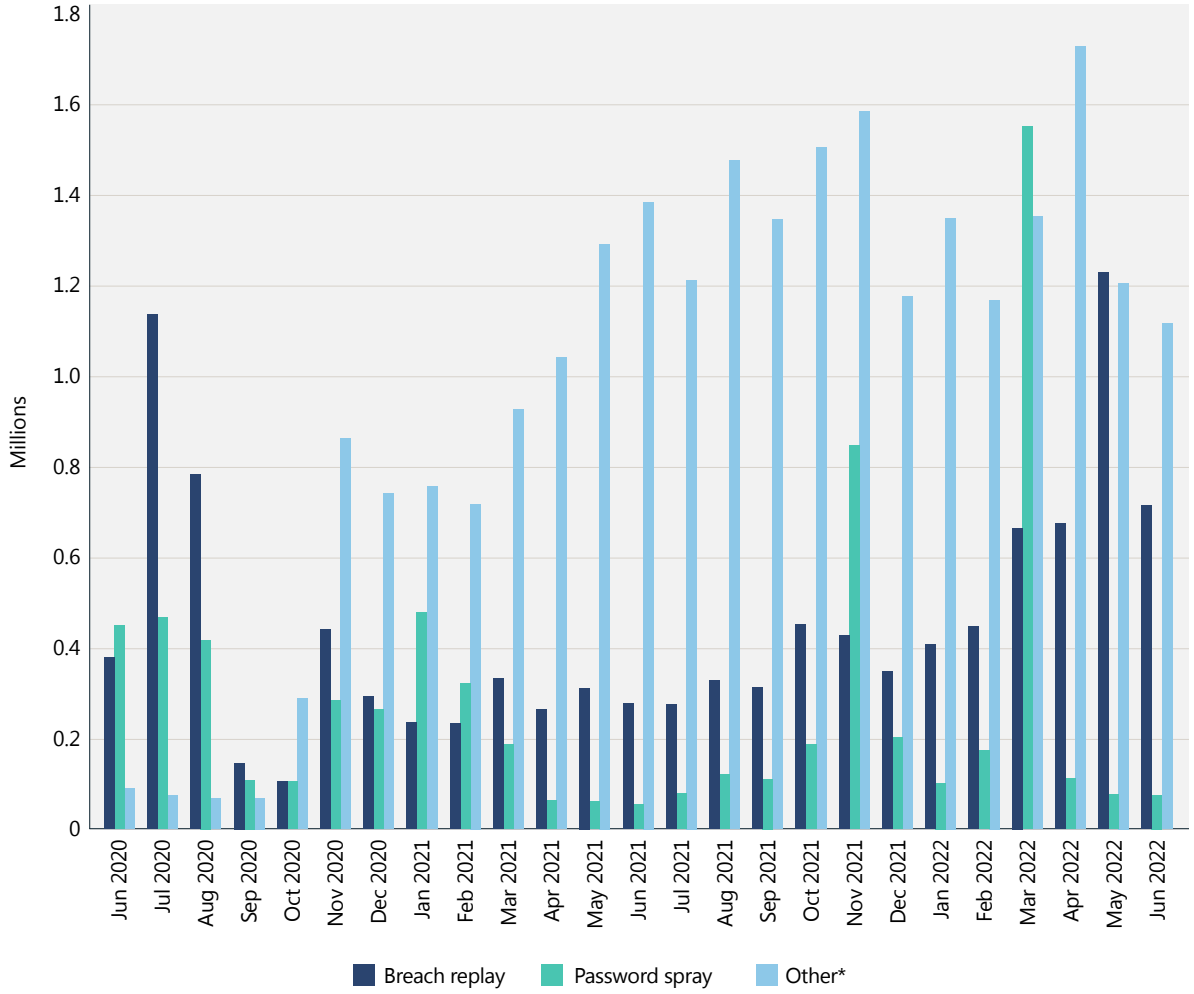
Maintaining identity health is fundamental to organizational well-being

Safeguarding identity is more important than ever. While password-based attacks remain the main source of identity compromise, other types of attacks are emerging. The volume of sophisticated attacks continues to increase relative to the previous norm of password spray and breach replay.

Password-based attacks are still common, and over 90 percent of accounts compromised via these methods are not protected with strong authentication. Strong authentication uses more than one factor of authentication, for example password + SMS and FIDO2 security keys.

We have seen a rise in targeted password spray attacks, with very large spikes in volume of attacker traffic spread across thousands of IP addresses.

Users compromised by attack category



Users compromised per month by attack category. Password spray attack volumes were highly volatile, as seen in the spikes in November 2021 and March 2022. These spikes represent thousands of users and thousands of IP addresses touched. *"Other" indicates attacks different from password spray and breach replay, including phishing, malware, man-in-the-middle, on-premises token issuer compromise, and others. Source: Azure AD Identity Protection.

4,500

In the time it takes to read this statement, we've defended against 4,500 password attacks.

https://t.me/learningnets

Maintaining identity health is fundamental to organizational well-being

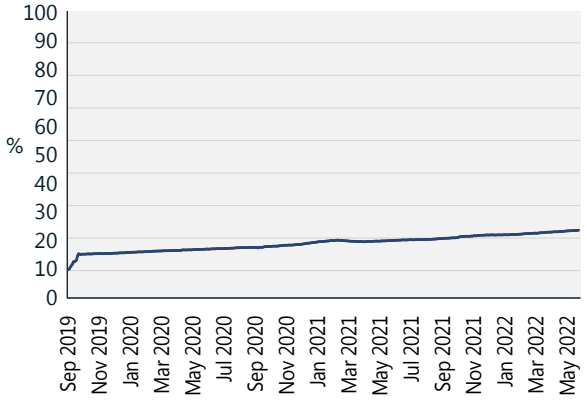
Continued

Strong authentication adoption

On a positive note, we are seeing steady growth in adoption of strong authentication amongst the Azure Active Directory (Azure AD) enterprise customer base. For Azure AD, strong authentication monthly active users (MAU) grew from 19 percent to 26 percent in the last year, while strong authentication MAU for administrative accounts grew from 30 to approximately 33 percent.

This trend is positive, but significant growth is still needed to reach majority coverage of strong authentication; customers not already using strong authentication in their environments should start the planning and deployment of strong authentication to protect their users.[3] While designing strong authentication deployment, passwordless authentication should be considered as it offers the most secure usable experience, eliminating the risk of password attacks.

Use of strong authentication
(September 2019–May 2022)

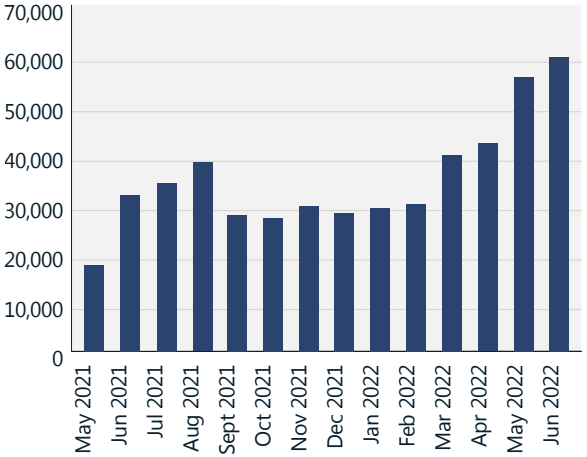


While strong authentication usage has doubled since 2019, just 26 percent of users and 33 percent of administrators are using strong authentication. Source: Azure Active Directory.

Steady rise in token replay attacks

The share of other forms of attack increased in 2022. We saw a rise in targeted attacks that specifically avoid password-based authentication to reduce the chance of detection. These attacks leverage browser single sign-on (SSO) cookies or refresh tokens obtained via malware, phishing, and other methods. In some cases, attackers choose infrastructure in locations near the geographic location of the targeted user to further reduce the chances of detection. We have seen a steady rise in token replay attacks, reaching over 40,000 detections per month in Azure AD Identity Protection. Token replay is the use of tokens that were issued to a legitimate user by an attacker that has possession of said tokens. Tokens are commonly obtained via malware, for example by exfiltrating the cookies from the user's browser or through advanced phishing methods.

Volume of detected token replay attacks



Detected token replay attacks per month. Source: Azure AD Identity Protection, unique sessions flagged by the anomalous token detection.

https://t.me/learningnets

Maintaining identity health is fundamental to organizational well-being

Continued

Extracting tokens

More than malware, attackers need credentials to achieve their goals. In fact, 100 percent of all human operated ransomware attacks include stolen credentials. Many sophisticated intrusions include credentials purchased from the dark web, initially stolen from unsophisticated and broadly distributed credential theft malware. This class of malware has evolved to steal tokens, including session information and MFA claims. This means that infections on home systems, where users log in to corporate assets, can lead to serious incidents on corporate networks.

Attackers can also extract tokens from victims' devices through man-in-the-middle attacks, in which the victim clicks a malicious link in a phishing email or instant message and is directed to a website that looks like the legitimate sign-in page of the identity provider. In reality, it is a web service spun up by the attacker that relays and intercepts all traffic between the user and the identity provider. The attacker is able to intercept the username and password and also to relay MFA challenges; resulting tokens issued by the identity provider and intercepted by the attacker might contain MFA claims that can be used by the attacker to satisfy MFA requirements.

Microsoft Defender for Cloud Apps has detected an average of 895 such attacks per month since the beginning of 2022. This form of attack can be prevented by using phish-resistant factors of MFA, such as Certificate Based Authentication, Windows Hello for Business, or FIDO2 security keys.

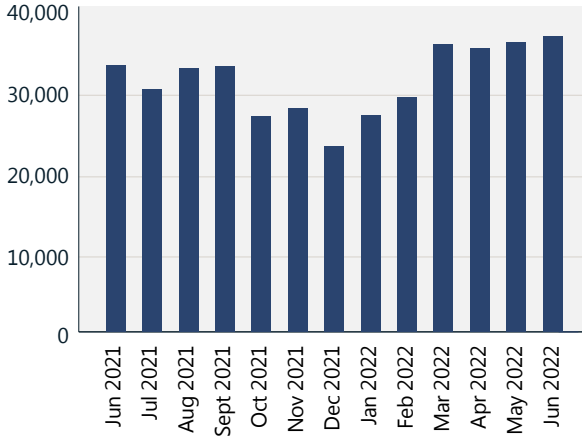
> Password-based attacks are the primary method by which accounts are compromised.

MFA fatigue

Using the concept of "MFA fatigue," attackers generate multiple requests for MFA to the victim's device, hoping that the victim will accept the request either inadvertently or as a result of fatigue. This attack can be prevented by using modern authenticator apps such as Microsoft Authenticator combined with features such as number matching[4] and enabling additional context.[5] Azure AD Identity Protection estimated there are 30,000 MFA fatigue attacks per month.

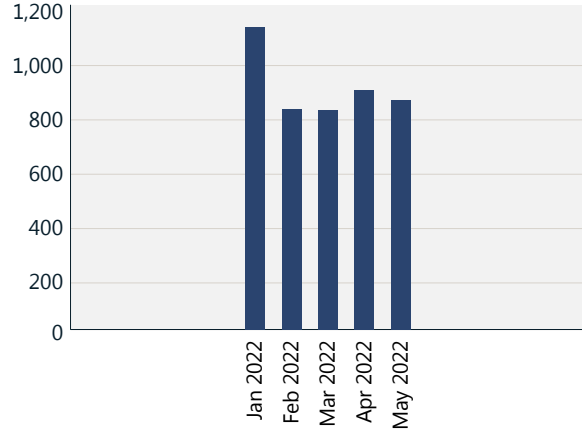
> The share of sophisticated attacks continues to rise, underscoring the need for phish-resistant factors of multifactor authentication.

Estimated instances of MFA fatigue attacks



Source: Azure AD Identity Protection.

Detected instances of phishing followed by man-in-the-middle attacks



Source: Microsoft Defender for Cloud Apps.

Actionable insights

1. Ensure all the accounts across your organization are protected by strong authentication measures.
2. Passwordless authentication offers the most secure and user-friendly experience, eliminating the risk of password attacks.
3. Disable legacy authentication across your entire organization.
4. Protect high value and administrative accounts with phish-resistant forms of strong authentication.
5. Modernize from an on-premises identity provider to a cloud identity provider and connect all your apps to the cloud-based identity provider for consistent user experience and security.

Links to further information

- This World Password Day consider ditching passwords altogether | Microsoft Security

https://t.me/learningnets

Operating system default security settings

With the continuously evolving security threat landscape, we see an increasing need for computer security configured by default to improve cyber resiliency. While operating system security is more urgent, complex, and business critical than ever before, it can be challenging to get right and manage.

In the past, computer and device security included built-in security features that the customer or IT professional was expected to configure to their own desired level. This approach is no longer adequate, as attackers are using more advanced tools in automation, cloud infrastructure, and remote access technologies to achieve their aims. It has become critical that all layers of security, from the chip to the cloud, are configured by default. Microsoft has evolved to configure Windows operating system security by default.[6]

Customers who embrace defense—in depth including a layered security posture, new security features, regular and consistent patching and updates, as well as security training and awareness to report phishing and other scams – can expect less malware.

To simplify defense in depth, Windows 11 has tightly integrated hardware and software protections turned on by default, including memory integrity, Secure Boot, and a Trusted Platform Module 2.0. Windows 10 users on capable hardware can also turn these features on in the Windows Settings app or in the BIOS menu.

Older devices in general often do not have as strong an alignment between hardware security and software security techniques. For devices where security is not enabled by default, manually configure them in settings where possible.[7]

For devices where security is not enabled by default, Microsoft recommends manually configuring them in settings where possible.

Be proactive about applying continuous operating system updates and security patches that help provide protection throughout the hardware and software lifecycle.

Actionable insights

1. Use a passwordless solution which binds sign-on credentials in the Trusted Platform Module, specifically look for a passwordless solution that meets the Faster Identity Online (FIDO) Alliance[8] industry standard.
2. Perform timely clean up of all unused and stale executables sitting on organizations' devices.
3. Protect advanced firmware attacks by enabling memory integrity, Secure Boot, and Trusted Platform Module 2.0, if not enabled by default, which hardens boot using capabilities built into modern CPUs.
4. Turn on data encryption and credential protection.
5. Enable application and browser controls for enhanced protection from untrusted applications and other built-in exploit protections.
6. Enable memory access protection to help protect against casual physical attacks such as someone plugging a malicious device into externally accessible ports.

Links to further information

- Windows Security Book | Commercial
- New security features for Windows 11 will help protect hybrid work | Microsoft Security Blog

https://t.me/learningnets

Software supply chain centrality

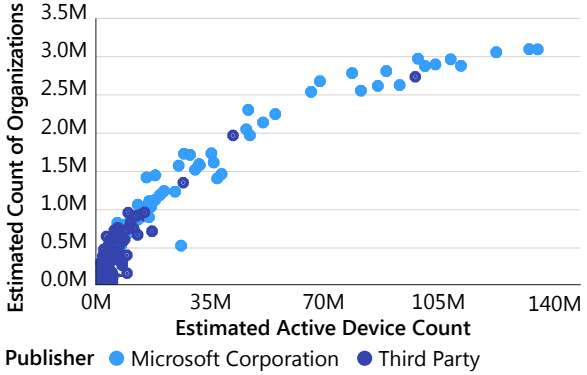
Attacks on third-party apps, plugins, and extensions can erode customer trust in suppliers that play a central role in the supply ecosystem. Using network theory to look at software centrality helps illuminate the criticality of patching, especially for central apps.

The Windows App Network of 18 million application executables is installed and used across five million organizations, providing a top-level view of our software ecosystem. Of the 100,000 most used applications, 97 percent are produced by third-party organizations whose updates and security patches are maintained by them. This illustrates two important traits of our commercial application ecosystem.

First, there is centrality in the Windows commercial application ecosystem. Only the top 100,000 (of the 18 million) applications are used on 1,000 or more devices. In other words, just over one half of 1 percent of these applications have this kind of broad-reaching effect among the device ecosystem.

Second, there is diversity in the manageability of those applications, where the top 10,000 application suppliers manage the updates and security patches of these most used commercial applications. This demonstrates the interdependence a company has on a diverse set of software suppliers' security, compliance, and management controls.

Commercial penetration of most-used applications



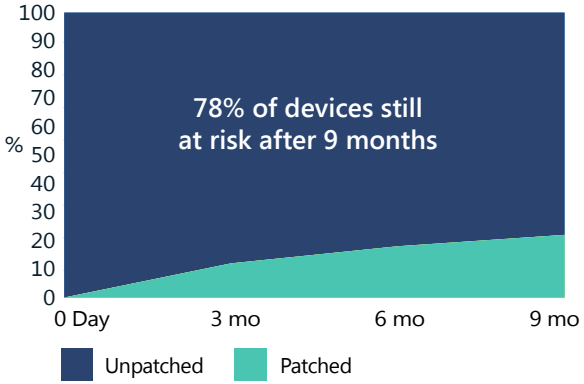
The top applications are used by millions of organizations and tens of millions of devices. Because they are near ubiquitous, adversaries are on constant lookout to exploit vulnerabilities in these top applications, which can impact millions of devices in the user base.

We observe millions of commercial devices still using vulnerable application versions many months after patch release or even years beyond the end of product support. For example, there are more than one million active Windows commercial devices running version of a PDF reader that has not been supported since 2017.

Old versions of applications which are unsupported remain in active use on millions of commercial devices. As a result, organizations are at risk of carrying vulnerabilities that will not be patched.

For in-support application versions, we see a plateauing of the speed of critical patch adoption, which is the opposite of the trend that will drive resiliency. Instead, the curve should show an exponential upwards adoption of patches month over month, to achieve the resiliency needed.

Rate of critical patch deployment



After examining a critical vulnerability that affected 134 versions of a set of browsers, we found that 78 percent, or millions of devices, still used one of the affected versions nine months after the patch was released.

We used the InterpretML[9] toolkit to identify characteristics correlated with organizations that are more likely to have devices with older app versions. The most important of these predictors included: low hours of engagement on devices; geographic areas such as Asia Pacific and Latin America; and industries such as automotive, chemicals, telecommunications, transport and logistics, health payors (claim handlers), and insurance.

Software resiliency maintenance should include regular disabling or uninstalling of unused applications.

The security and compliance of an organization depends on its own efforts and on the efforts of its software suppliers.

Actionable insights

1. Perform timely updates to all applications and endpoints through your organization.
2. Perform timely cleanup of all unused and stale executables sitting on organizations' devices.

Links to further information

- Microsoft Intune documentation | Microsoft Docs
- Manage apps | Microsoft Docs
- Microsoft Defender for Endpoint | Microsoft Security
- OSS Secure Supply Chain Framework | Microsoft Security Engineering
- Microsoft Open Source Software Secure Supply Chain Framework | GitHub

https://t.me/learningnets

Building resilience to emerging DDoS, web application, and network attacks

Accelerated digital transformation has brought an end to the traditional network and security perimeter model. Moving to the cloud means enterprises must adopt cloud-native network security to protect digital assets.

Attack complexity, frequency, and volume continue to grow and are no longer limited to holiday seasons, indicating a shift toward year-round attacks. This highlights the importance of ongoing protection beyond traditional peak traffic seasons.

Distributed denial of service (DDoS) attacks

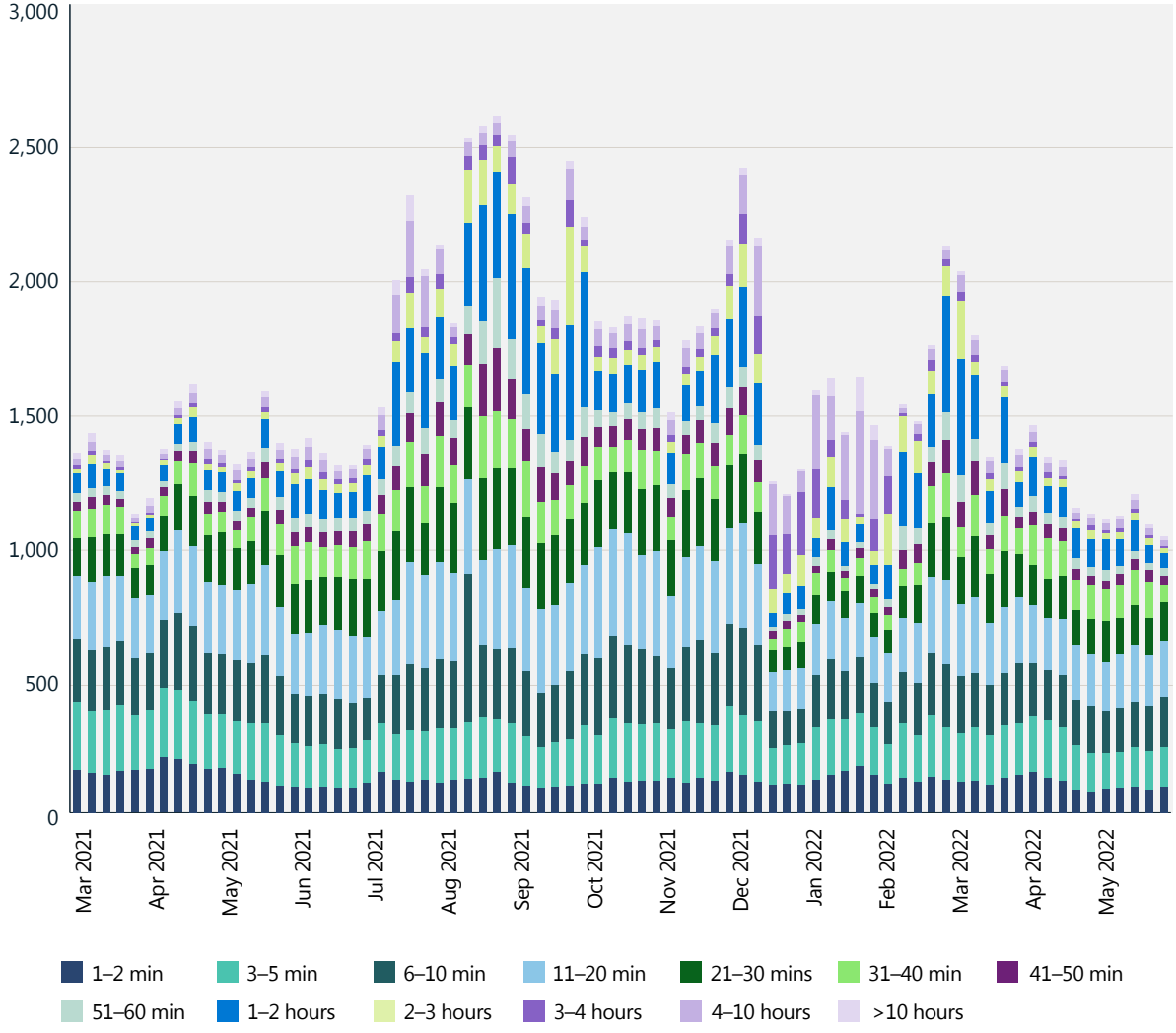
Over the past year, the world experienced DDoS activity that was unprecedented in volume, complexity, and frequency. This DDoS explosion was driven by a substantial increase in nation state attacks and continued proliferation of low-cost DDoS-for-hire services. Microsoft mitigated an average of 1,955 attacks per day, a 40 percent increase from the prior year. Previously, the peak number of attacks normally occurred during the end-of-year holiday season. This year, however, the most recorded in a day was on August 10, 2021. This might indicate a shift toward year-round attacks and highlights the importance of ongoing protection beyond traditional peak traffic seasons.

In November 2021, Microsoft thwarted a volumetric DDoS attack with a throughput of 3.4 terabits per second (Tbps) from approximately 10,000 sources spanning multiple countries. Similar high volumetric attacks above 2+Tbps were mitigated in 2022 highlighting that it's not just the complexity, frequency of attacks that's increasing, but also the volume (bandwidth) of attack.

Attack duration

Most attacks observed over this past year were short-lived. Approximately 28 percent of the attacks lasted less than 10 minutes, 26 percent lasted 10–30 minutes and 14 percent lasted 31–60 minutes. Thirty-two percent of the attacks were more than an hour in duration.

Number of DDoS attacks and duration distribution
(March 2021–May 2022)



Most attacks in the last year were short-lived. Approximately 28 percent of the attacks lasted less than 10 minutes.

https://t.me/learningnets

Building resilience to emerging DDoS, web application, and network attacks

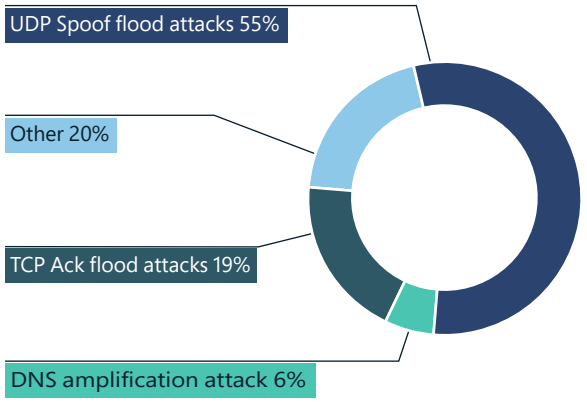
Continued

DDoS attack vectors

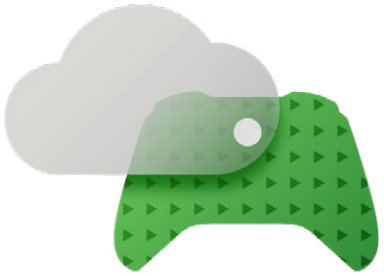
In the past year, the attack vectors commonly employed were User Datagram Protocol (UDP) reflection on port 80 using simple service discovery protocol (SSDP), connectionless lightweight directory access protocol (CLDAP), domain name system (DNS), and network time protocol (NTP) comprising one single peak. We also saw an increase in application layer DDoS attacks targeting websites, with 16.3 million peak RPS (requests per second) and 9.89 Tbps peak traffic.

In 2022, Microsoft mitigated nearly 2,000 DDoS attacks daily and thwarted the largest ever DDoS attack reported in history.

DDoS attack vectors



UDP Spoof flood attack rose to the top vector in the first half of 2022, from 16 percent to 55 percent. TCP Ack flood attack decreased from 54 percent to 19 percent.

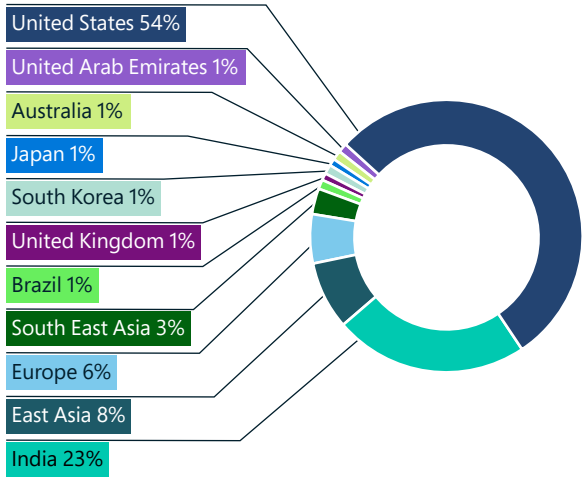


The gaming industry continues to be the top target of DDoS attacks, mostly from mutations of the Mirai botnet and low-volume UDP protocol attacks. Since UDP is commonly used in gaming and streaming applications, an overwhelming majority of the attack vectors were UDP spoof floods, while a small portion were UDP reflection and amplification attacks.

Geographic target regions

Of the DDoS attacks detected over the past year, 54 percent were conducted against targets in the United States, a trend that might partially be explained by the fact that most Azure and Microsoft customers are in the United States. We also saw a sharp uptick in attacks against India, from just 2 percent of all attacks in the second half of 2021 to 23 percent in first half of 2022. East Asia, Hong Kong in particular, remains a popular target at 8 percent. For Europe, we saw concentrations of attacks against Amsterdam, Vienna, Paris, and Frankfurt regions.

DDoS attack destination

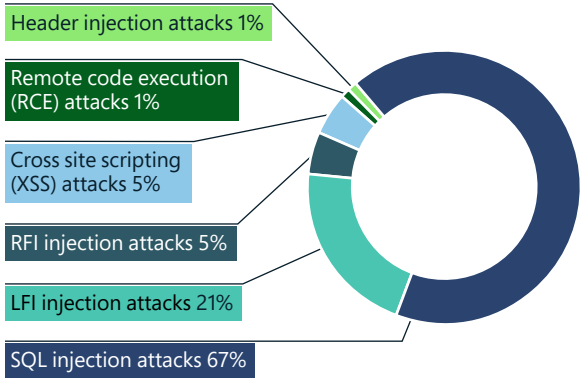


We attribute the high volume of attacks in Asia to the region's huge gaming footprint, especially in China, Japan, South Korea, and India. This footprint will continue to expand as increasing smartphone penetration drives the popularity of mobile gaming, suggesting this geographic target will only continue to grow.

Web application exploits

Web application firewall (WAF), in combination with DDoS protection, forms an integral part of defense-in-depth strategy for protecting web and application programming interface (API) assets. Microsoft observed upwards of 300 billion WAF rules triggered per month via Azure WAFs.

Distribution most prevalent attack types



Azure WAF detects billions of Open Web Application Security Project (OWASP) Top 10[10] attacks daily. According to our signals, attackers most attempted SQL injection attacks followed by local file injection and remote file injection attacks. This is in line with the OWASP Top Ten list showing injection attacks as the third most common type of web attacks.

There has also been an increase in bot attacks against Azure web applications, with an average of 1.7 billion bot requests per month and 4.6 percent of that traffic consisting of bad bots.

https://t.me/learningnets

Building resilience to emerging DDoS, web application, and network attacks

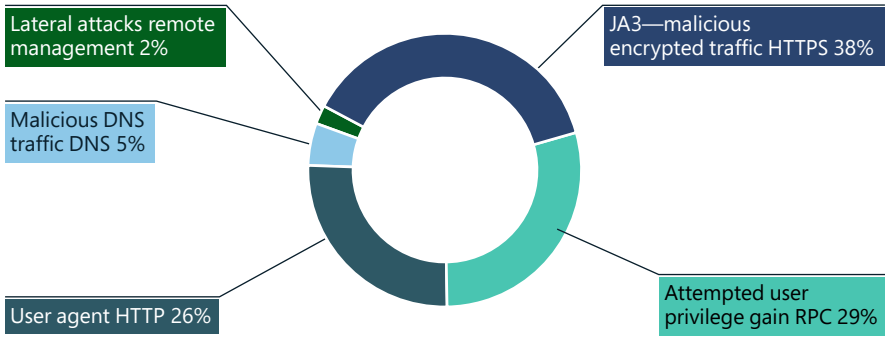
Continued

Due to an increasing number of bots performing credential stuffing attacks, credit card fraud, cyber influence campaigns, and supply chain attacks, we expect to see a steady increase in bot attacks against web applications.

Network intrusions: detection and prevention

We observed a significant increase in network layer exploits, particularly malware, in 2022. Azure Firewall intrusion detection and prevention system (IDPS) blocked more than 150 million connections in the month of June alone.

IDPS Deny traffic reason



IDPS traffic alert reasons

Analysis of IDPS alert and deny traffic shows the following approaches used by attackers. In the Deny traffic, we are seeing attackers using SSL to hide their activities and remote execution attacks are becoming more common. In the Alert traffic, we are seeing SMB/SMB2 protocols used to perform remote execution attacks.

Actionable insights

1. Inspect all traffic between systems within a data center or cloud service, and traffic seeking to access them.
2. Develop a robust all-year-round network security response strategy.
3. Use cloud native security services to implement a robust zero trust network security posture.

Links to further information

- Improve your security defenses for ransomware attacks with Azure Firewall | Azure Blog and Updates | Microsoft Azure
- Anatomy of a DDoS amplification attack | Microsoft Security Blog
- Intelligent application protection from edge to cloud with Azure Web Application Firewall | Azure Blog and Updates | Microsoft Azure

https://t.me/learningnets

Developing a balanced approach to data security and cyber resiliency

The digital transformation has fueled a vast expansion of data assets and a rise in security, compliance, and privacy risks. Cyber resilient organizations must balance investments in data protection, compliance, and recovery capabilities and integrate these with specialized regulatory response processes to address distinct types of breaches.

Data breaches are not a matter of if, but when. The IBM and Ponemon Institute's "Cost of a Data Breach, 2021" study reports a global average data breach cost of $4.24 million USD (up 10 percent from the previous year) and $9.05 million USD in the United States. Compliance failures were found to be the top cost-amplifying factor. Conversely, breach cost reductions were associated with best practices such as incident response (IR) planning, Zero Trust deployment maturity, security AI and automation, and use of encryption.

Data breaches are inevitable. Organizations that take a balanced resilience approach will reduce the frequency, impact, and cost of breaches.

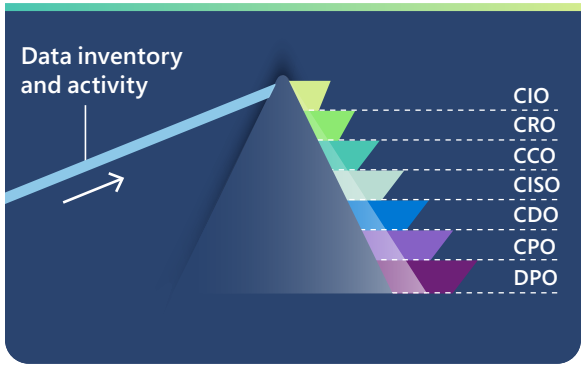
Data governance, security, compliance, and privacy are interdependent

We have seen data gain prominence in recent years as a crucial value creation engine for organizations. At the same time, the rise of privacy regulations requiring both data governance and security have blurred the lines between risk roles. While newer C-level roles such as the Chief Data Officer (CDO) or the Chief Privacy Officers (CPO) have a vested interest in security and compliance, the implementation and operationalization of data protection often relies on teams led by the Chief Information Officers (CIO) and/or Chief Information Security Officer (CISO). It is not a one-way street, as data governance initiatives led by CDOs also have security benefits. As a result of this interconnectedness, IT, data governance, security, compliance, and privacy teams need to work ever more closely to achieve efficiency and manage risk.

Unified data risk management platforms for the entire organization's data estate is the future

Aligning IT, data governance, security, compliance, and privacy management process is difficult in an environment of bespoke applications for each discipline and inconsistent coverage across the typical organization hybrid, multi-cloud data sprawl. We believe that organizations need a single pane of glass to locate and know their data, protect their data, govern the access, usage, and lifecycle of data, and prevent data loss across the data estate.

Working from the same data inventory and activity information facilitates cross-team processes, yields a more comprehensive risk picture, and allows organizations to better prepare and streamline their response to a breach.



The "single pane of glass" should act as a prism. Teams that have a stake in data security, compliance, and privacy need different yet consistent views of the same data inventory and activity to come into alignment and collaborate. Data activity includes data access, modification, and movement events, which are a valuable part of the data security equation.

Effective data governance, security, compliance, and privacy are interdependent and require cross-team collaboration.

Actionable insights

1. Balance defense with recovery and minimize data breach impact by investing in compliance, data protection, and response capabilities.
2. Develop and adopt processes and tools that cut across data risk silos and cover the full data estate.

Links to further information

- Microsoft Purview—Data Protection Solutions | Microsoft Security
- The future of compliance and data governance is here: Introducing Microsoft Purview | Microsoft Security Blog

https://t.me/learningnets

Resilience to cyber influence operations: The human dimension

Over the last five years, advances in graphics and machine learning have introduced easy-to-use tools capable of quickly generating high-quality, realistic content that can spread widely across the internet in seconds.

When it comes to events reported via text, audio, and visual content, we have reached a point where neither humans nor algorithms can reliably distinguish fact from fiction. The proliferation of these tools and their outputs are casting doubt on the trustworthiness of all digital media, disrupting our understandings of local and world events. New forms of influence operations enabled by advances in technology have grave implications for democratic processes.[11]

Questions arise about what we can do to prepare for a more resilient future against these cyber influence operations. Technology is only one part of the puzzle. It's going to take multiple efforts, including education aimed at media literacy, awareness, and vigilance, investments in quality journalism—with trusted reporters on the scene, locally, nationally, and internationally—networks of sharing and alerting about influence operations, and new kinds of regulations that penalize malevolent actors who generate or manipulate digital media with an aim to deceive.

We also recognize that restoring trust in digital content is an ambitious goal that will require diverse perspectives and participation. There is not one company, or institution, or government that can solve these threats on its own. Our superpower as humans is our ability to collaborate and cooperate. This is especially important now because it will require everyone—global governments, industries, academia, and especially news, social, and media organizations—working together for the betterment and health of our society.

Links to further information

- Applications for artificial intelligence in Department of Defense cyber missions | Microsoft On the Issues
- Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the Subcommittee on Cybersecurity, of the Senate Armed Services Committee, 117th Congress (May 3, 2022; Testimony of Eric Horvitz)

https://t.me/learningnets

Fortifying the human factor with skilling

Addressing the human factor is a key component of any cybersecurity skilling strategy. According to a Kaspersky Human Factor in IT Security study,[12] 46 percent of cybersecurity incidents involve careless or uniformed staff who inadvertently facilitate the attack.

Microsoft's Education and Awareness team in the Digital Security and Resilience organization is responsible for fortifying the human factor of cybersecurity by empowering employees to secure our own and our customers' systems and data. Our goals are to:

- Reduce risk to Microsoft and our customers by building a centralized enterprise-wide core security skill set across the employee population.
- Fortify employee security knowledge through a multi-phased training reinforcement approach to support desired behavior outcomes.
- Foster culture change by making a security mindset an intrinsic part of Microsoft's culture through annually required security training and events.
- Promote a one-stop centralized web resource for best practices, company policy information, and incident reporting for all things cybersecurity related.

A targeted, centralized cybersecurity skilling program reaches every Microsoft employee at least once each year. Training offerings are optimized to support current cybersecurity initiatives and deliver measurable behavior outcomes. Microsoft's Information Risk Management Council (IRMC) plays a key role in identifying important cybersecurity behavior change outcomes to be addressed by training.

With all of our cybersecurity skilling programs, we measure the solution's efficiency, effectiveness, and outcomes where possible. For example, our insider threat skilling offering has 95 percent training compliance, exceptional learner satisfaction, and has resulted in a significant increase in managers reporting possible insider threat cases via the company's Report It Now tool. The program includes:

Security Foundations: Centralized, enterprise-wide cybersecurity awareness and compliance training which addresses core security and privacy practices. This highly anticipated training series employs an edutainment model to make learning about cybersecurity engaging and interesting.

STRIKE: Microsoft's required technical training for engineers who build and maintain line-of-business solutions. This by-invitation-only training addresses timely and critical areas of cybersecurity hygiene best practice and uses a live hybrid delivery model tailored to audience needs.

Program specific: Targeted training programs support specific cybersecurity initiatives including Shadow IT, Insider Threat, and Microsoft Federal. These offerings are tightly integrated into the overall engagement strategy for their respective cybersecurity initiatives through executive sponsorship and scorecard reporting to prevent a "check the box" training approach.

MSProtect: Microsoft's centralized web resource provides best practices, company policy information, and incident reporting for all things cybersecurity related. This on-demand resource is the go-to for employees outside of formal training offerings.

Security skilling must not be seen as a compliance, check-the-box activity. Instead, focus on behavior change to allow outcomes to be monitored across identified target behaviors, and establish listening systems to determine the impact of offerings.

Actionable insights

1. Provide security training and resources to employees when and where they need it.
2. Develop a centralized skilling strategy informed by stakeholders from across the enterprise.
3. Ensure the impact of training is tracked and analyzed for efficiency (quantity), effectiveness (quality), and outcomes (business impact).

Links to further information

- Microsoft launches next stage of skills initiative after helping 30 million people

https://t.me/learningnets

Insights from our ransomware elimination program

Microsoft has been on its own Zero Trust journey[13] in the past five years to ensure identities and devices are robustly managed and healthy. As the risk of ransomware grows, we have developed a deep view to support our approach to protecting ourselves and our customers.

Following an in-depth internal evaluation, we built a ransomware elimination program to remediate gaps in controls and coverage, contribute to feature enhancements for services like Defender for Endpoint, Azure, and M365, and to develop playbooks for our SOC and engineering teams on how to recover in the event of a ransomware attack.

The first step was understanding the extent of our protection against a ransomware attack directed at Microsoft. Efforts were already well underway to deploy Defender for Endpoint and to ensure all devices are managed and compliant with our Zero Trust policies, but we needed to find a way to understand all facets of the bigger question as to whether we could effectively recover from an attack. To gain insight, we evaluated the NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile,[14] which aligns with our overall enterprise policy against our known list of controls. This analysis quickly identified gaps in coverage.

Next, we prioritized gaps across the Identify, Detect, Protect, Respond, and Recover functions of the CSF. We found strategic alignment to Zero Trust and other programs and also discovered gaps that had no existing workstream. Having assessed the amount of work and effort needed to remediate these gaps, we separated them into two pillars:

- **Protect the enterprise (PtE):** Define work items that we need to do as an enterprise to protect ourselves and be able to recover from an attack, should one be successful.
- **Protect the customer (PtC):** Build capabilities into our offerings to protect our customers as well as our business.

Embedding findings into our own enterprise

To remediate the top risks and protect our critical services against a ransomware attack, we plan to focus investments over the next 6 to 12 months on achieving the five scenarios below as part of a dedicated ransomware program. Once we succeed in each of the scenarios, we will gradually expand the scope of the program to reach all parts of the enterprise.

Scenario 1: Security team members understand the overall risk associated with a ransomware attack and have a process established to provide awareness to the executives on control gaps and risk status.

Scenario 2: Security team members have access to playbooks designed to help them and other teams within Microsoft respond to and recover critical services from a ransomware attack.

Scenario 3: Enterprise Resilience team members have a standard to follow for the backup of critical systems. Playbooks exist and regular exercises of backup and recovery are done to ensure data can be recovered in the event of a ransomware attack.

Scenario 4: Service owners understand and implement the required security and operational controls and policies to protect their service, customer data, endpoints and network assets against ransomware attacks with special focus on services prioritized as Microsoft critical services.

Scenario 5: All employees can access educational and training resources which describe how to recognize a ransomware attack and how to notify the security team and initiate the response.

Actionable insights

1. Document and validate end-to-end recovery and remediation activities related to ransomware attacks against critical services.
2. Involve stakeholders in updating your Enterprise Crisis Management playbooks to include ransomware specific activities and a decision process and guidance to determine if/when to pay for ransomware.
3. Improve detection and protection coverage by enabling capabilities available in your deployed security products (e.g. Defender for Endpoint Attack Surface Reduction rules).
4. Work with the security standards team to define a baseline for protection against a ransomware attack, and provide training and documentation to engineering teams on how to protect against a ransomware attack.
5. Put automation in place to make the deployment of security and operations policies easier on the DevOps teams and ensure that if a system drifts from compliance it is quickly flagged and remediated.

Links to further information

- Sharing how Microsoft protects against ransomware | Microsoft Inside Track

https://t.me/learningnets

Act now on quantum security implications

The pressure is on to manage the threat quantum computing poses to today's cryptography and everything it protects. The recently issued Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems[15] builds on US Executive Order 10428[16] for Improving the Nation's Cybersecurity highlights software supply chain security as critical to addressing future nation-state attacks.

What are quantum computers?

Quantum computers are machines using the properties of quantum physics to store data and perform computations. This can be extremely advantageous for certain tasks where they could vastly outperform even our best supercomputers. Quantum computing is already opening new horizons for data encryption and processing. Studies predict quantum computing will become a multi-billion dollar (USD) quantum industry as early as 2030.[17] In fact, quantum computing and quantum communication are poised to have a transformative effect across a multitude of industries, ranging from healthcare and energy to finance and security.

Quantum computing is a threat to today's cryptography and everything it protects.

The threat to today's cryptography

With Shor's 1994 algorithm and an industrial-scale quantum computer of more than a few million physical qubits, all our current, widely deployed public-key cryptographic algorithms could be efficiently broken. It is critical to consider, evaluate, and standardize "quantum-safe" cryptosystems that are efficient, agile, and safe against an adversarial quantum-based attack. Software migration to "post-quantum cryptography," namely existing classical algorithms and protocols robust to quantum attack, will take years—if not a decade or more—to achieve.[18]

This means the pressure is on to manage the threat to today's cryptography and everything it protects. Adversaries can record encrypted data now and exploit it later once a quantum computer is available. Waiting for quantum computing to arrive before addressing its cryptographic implications will be too late.

As cryptography is used throughout the cyber ecosystem, this means our cryptography-based security services could be compromised. For example, this includes services for communications (TLS, IPSec), messaging (email, web conferencing), identity and access management, web browsing, code signing, payment transaction and other services that are dependent upon cryptography for protection.

As quantum computers become a reality, third-party software components containing implementations of cryptographic algorithms and capabilities will require additional scrutiny as well. This requires all organizations along the value chain to do their part to ensure the chain stays secure. Industry bodies and governments are increasing efforts to define software supply chain security requirements and, in some cases, introducing new mandates for securing the chain. National Security Memorandum NSM-8[19] establishes requirements and timelines for implementing post-quantum cryptography in National Security Systems (NSS). It calls out timing expectations within 180 days for "modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary."

Standardization is a long lead-time activity in the transition to quantum-safe cryptography. Standards bodies that work on standards using public key cryptography must begin to experiment with and adapt to post-quantum algorithms now.

New post-quantum cryptography (PQC) algorithms—classical algorithms thought to be robust to quantum attack—are now under review through NIST's Post-Quantum Standardization Project.[20] This work will influence global efforts within standards bodies. Although there will be some overlap with US government algorithm selections, differing national body/regulatory choices for compliant algorithms could present international challenges. This fragmentation will in turn complicate product and service engineering.

New post-quantum cryptography algorithms are under review through NIST's Post-Quantum Cryptography Standardization program. This work will influence global efforts within standards bodies.

Actionable insights

Alongside SAFECode and partnering members, immediate shorter-term activities should be taken by industry to prepare for the PQC transition.[21] These include:

1. Take an inventory of your products/codes that use cryptography.
2. Implement a crypto agility strategy across your organization that includes minimizing the code churn required when cryptography changes.
3. Pilot the use of candidate quantum-safe algorithms in your products or services that use cryptography.
4. Be prepared to use different public key algorithms for encryption, key exchange, and signatures.
5. Test your applications for the impact of very large key sizes, ciphers, and signatures.

Links to further information

- Microsoft has demonstrated the underlying physics required to create a new kind of qubit | Microsoft Research

https://t.me/learningnets

Integrating business, security, and IT for greater resilience

Robust cyber resiliency depends on business leaders working with security teams to implement security. In Microsoft's experience, security leadership is a challenging discipline that requires support from organizational leaders to most effectively protect the organization.

Security leaders navigate a spectrum of dynamic challenges spanning topics related to risk, technology, economics, organizational process, business models, culture transformation, geopolitical interests, espionage, and international sanctions compliance. Each of these carries nuances to be understood and closely managed.

Security leaders are also tasked with thwarting both intelligent, well-funded, and highly motivated human attackers, and low-skilled, yet effective, cybercriminals. Their teams must defend complex technical estates often built up incrementally over 30 or more years when security was a low or nonexistent priority. Decisions made years ago can pose risks today until we pay off the technical debt and address the gaps in security.

Organizational leaders and policymakers can have a significant positive impact on security by actively supporting security leaders and helping to build a bridge between integrated security and the rest of the organization. When Microsoft works with customers that have this alignment, we see them building a more resilient organization and also improving their agility to adapt and innovate.

Organizational leadership can support security leaders by focusing on three key areas:

1. Build security by design

Security is sometimes viewed as an obstacle or an afterthought in business processes, often being considered in decisions only when it is too late to avoid a risk or fix cheaply and easily.

Organizational leaders and policymakers should ensure that they:

Include security early on new initiatives. New digital initiatives and cloud adoption should prioritize security to ensure organizational risk does not increase with each new application or digital capability. Once security is reliably included, you can use those processes to modernize legacy systems to get both security and productivity benefits at the same time.

Normalize preventive maintenance for security. Ensure basic security maintenance—like applying security updates and patches and secure configurations—has full organizational support allocated (including budgets, scheduled downtime, acquisition requirements for vendor product support).

Unfortunately, many organizations delay, defer, or apply these common practices only partially. This provides extensive opportunities for attackers to exploit. The need for security normalization is captured in US NIST 800-40.[22]

2. Engage with security

Organizational leaders should actively participate in and sponsor key security processes to ensure prioritization of resources and preparedness for security disasters. This includes engaging in:

Identify critical business assets. Security leaders and teams need to know which assets are business-critical to focus security resources on what matters most. This is often a new exercise that includes asking and answering new questions that have not been previously addressed.

Cybersecurity business continuity and disaster recovery exercises. Cyberattacks can become major events that disrupt or halt most or all business operations. Ensuring teams throughout the organization are prepared to handle these situations will reduce the time to restore business operations, limit damage to the organization, and help sustain the trust and confidence of customers, citizens, and constituents. This should be integrated within an existing business continuity and disaster recovery process.

Security risk decisions are best made by business or mission owners who have full visibility across all risks and opportunities.

https://t.me/learningnets

Integrating business, security, and IT for greater resilience

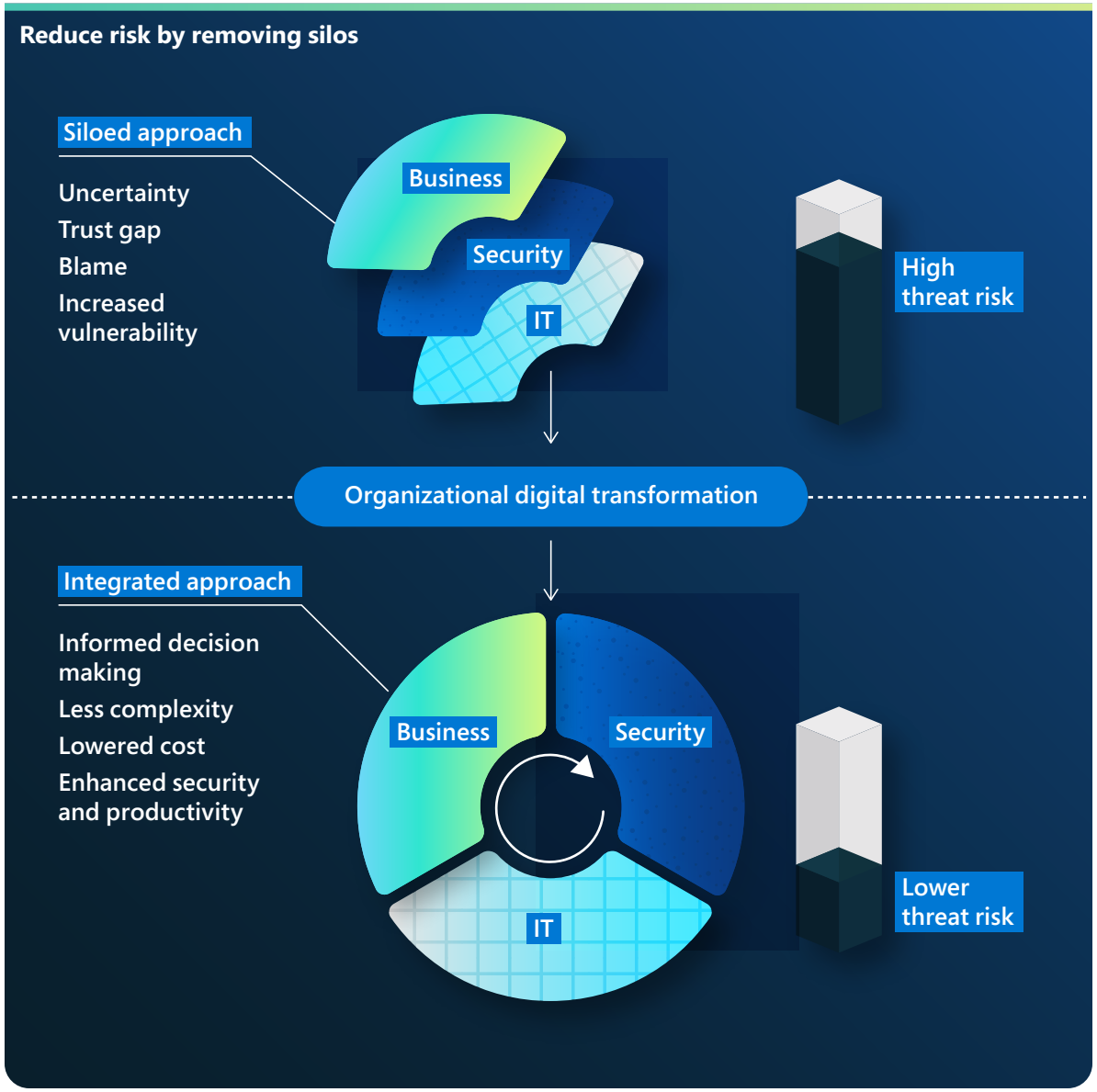
Continued

3. Position security correctly

The way organizations structure security risk accountability often sets them up for poor security risk decision making. Risk decisions are best made by business or mission owners who have full visibility across all risks and opportunities, but organizations often (implicitly or explicitly) assign security risk accountability to subject matter experts in the security team instead. This places an unhealthy burden on security teams while depriving business owners of visibility and control over a key risk to their business. Organizations can correct this by:

Preparing business owners: Educate business owners about security risk overall and how these threats can and will affect their business. Engaging security teams directly in this effort also increases the collaborative relationship with security and overall business agility.

Assigning security risk to business owners: As business owners become informed enough to understand and accept security risk, the organization should explicitly shift accountability for security risk to them while still holding security teams responsible for managing that risk and providing informed expertise and guidance to the owner.



"Cyber resilience is on a sliding scale from classic business continuity and disaster recovery starting with good data backup; progressing to recovery capabilities for processes, technology, and their dependencies (including people and third parties); and moving to always on, self healing services, resilience for critical roles, and failovers for critical third parties. The most resilient organizations promote integration between IT, business managers, and security professionals. Great resilience includes designing for resilience from the start, having safe change management, and granular fault isolation. Cyber resilience is just one scenario in a good all-hazards planning program. As cyber risks increase and the intersection between cybersecurity and resilience becomes more important, the connection of the Chief Information Security Officer (CISO) to the enterprise resilience program grows stronger. Every year, more CISOs are taking ownership for company-wide resilience."

Lisa Reshaur
General Manager, Risk Management, Microsoft

Links to further information

- From resilience to digital perseverance: How organizations are using digital technology to turn the corner in unprecedented times | Official Microsoft Blog
- How IT and security teams can work together to improve endpoint security | Microsoft Security

https://t.me/learningnets

The cyber resilience bell curve

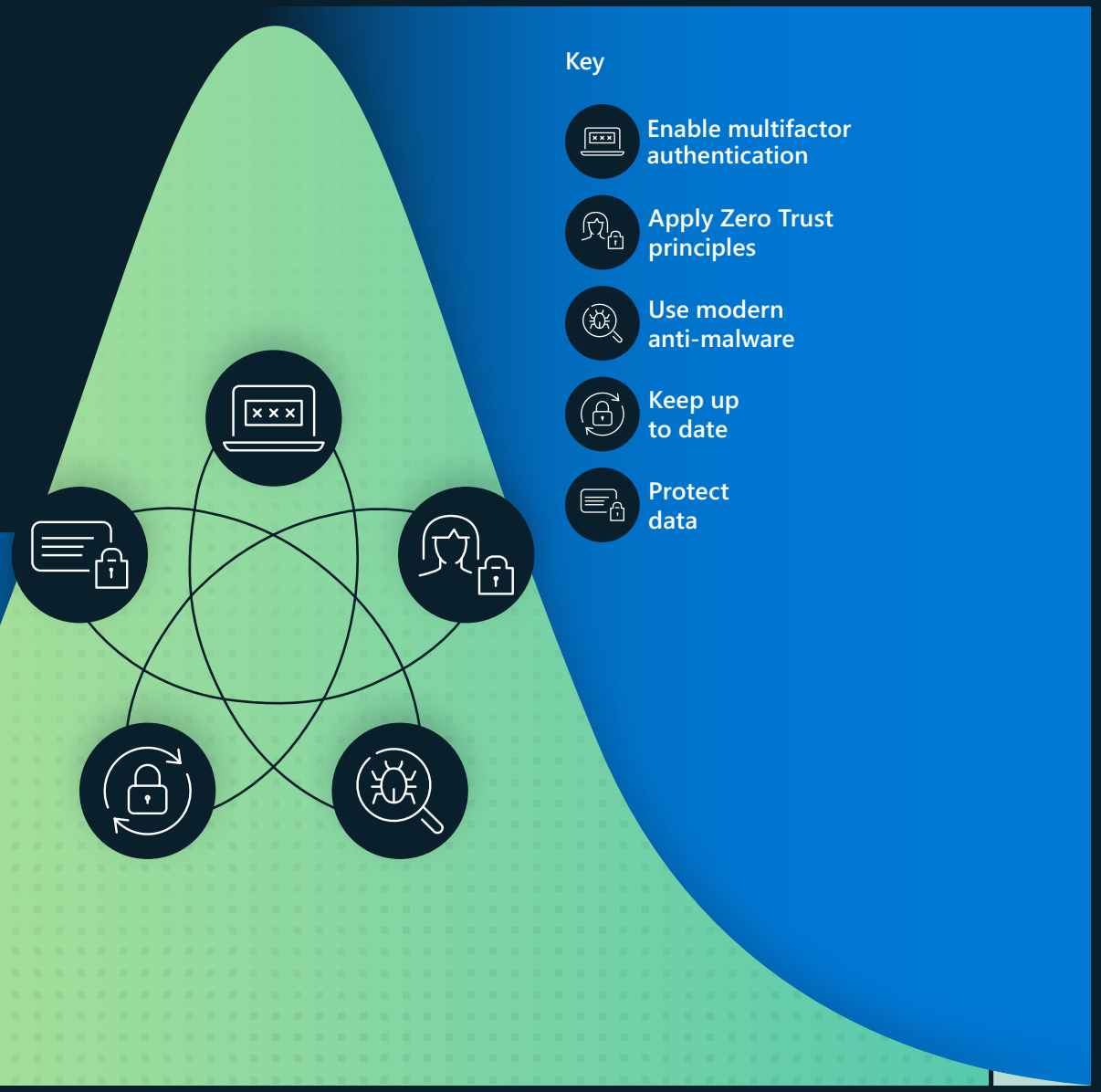
Resilience success factors every organization should adopt

As we have seen, many cyberattacks are successful simply because basic security hygiene has not been followed. The minimum standards every organization should adopt are:

- **Enable multifactor authentication (MFA):** To protect against compromised user passwords and helps to provide extra resilience for identities.
- **Apply Zero Trust principles:** The cornerstone of any resilience plan limiting the impact on an organization. These principles are:
  - Explicitly verify—ensure users and devices are in a good state before allowing access to resources.
  - Use least privilege access—only allow the privilege that is needed for access to a resource and no more.
  - Assume breach—assume system defenses have been breached and systems might be compromised. This means constantly monitoring the environment for possible attack.
- **Use extended detection and response anti-malware:** Implement software to detect and automatically block attacks and provide insights to the security operations. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
- **Keep up to date:** Unpatched and out of date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system and applications.
- **Protect data:** Knowing your important data, where it is located and whether the right systems are implemented is crucial to implementing the appropriate protection.

98%

Basic security hygiene still protects against 98% of attacks



https://t.me/learningnets

Endnotes

1 Endpoint Detection and Response (EDR) is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Endpoint detection and response capabilities provide advanced attack detections that are near real-time and actionable. Security analysts can prioritize alerts effectively, gain visibility into the full scope of a breach and take response actions to remediate threats.

2 An Endpoint Protection Platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts.

3 https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

4 https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match

5 https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context

6 Windows Security book: Commercial

7 New security features for Windows 11 will help protect hybrid work | Microsoft Security Blog

8 FIDO Alliance: Open Authentication Standards More Secure than Passwords

9 https://interpret.ml/

10 OWASP Top Ten | OWASP Foundation

11 https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/

12 https://www.kaspersky.com/blog/the-human-factor-in-it-security/

13 https://aka.ms/ZTatMSFT

14 https://csrc.nist.gov/publications/detail/nistir/8374/final

15 https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

16 Executive Order 14028 Improving the Nation's Cybersecurity

17 https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth

18 "The Long Road Ahead to Transition to Post-Quantum Cryptography," https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext

19 https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

20 https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

21 https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/

22 https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

https://t.me/learningnets

Contributing Teams

https://t.me/learningnets

Contributing Teams

The data and insights in this report were provided by a diverse group of security-focused professionals, working across many different Microsoft teams. Collectively, their goal is to protect Microsoft, its customers, and the world at large from the threat of cyberattacks. We are proud to share these insights in the spirit of transparency with a common goal of making the world a safer place for everyone.

AI for Good Research Lab: Harnessing the power of data and AI to address many of the world's challenges. The lab collaborates with organizations outside Microsoft, applying AI to improve livelihoods and environments. Areas of focus include online safety (disinformation, cybersecurity, child safety), disaster response, sustainability, and AI for Health.

Azure Edge & Platform, Enterprise & OS Security: Responsible for the core OS and platform security across Windows, Azure, and other Microsoft products. The team builds industry-leading security and hardware solutions into Microsoft platforms to drive down exploit, identity, and malware compromise from chip to cloud. Creators of Microsoft's Secured-core platform across PC, Edge and Server, the Microsoft Pluton Security Processor, and more.

Azure Networking, Core: A cloud networking team focused on the Microsoft WAN, data center networks, and the software defined networking infrastructure of Azure including the DDoS platform, the network edge platform, and network security products such as Azure WAF, Azure Firewall, and Azure DDoS Protection Standard.

Cloud Security Research team: By securing the Microsoft cloud, building innovative security features and products, and conducting research, this team protects and empowers Microsoft customers to securely transform their organizations.

Customer Security and Trust (CST): A team driving continuous improvement of customer security in Microsoft products and online services. Working with engineering and security teams across the company, CST ensures compliance, enhances security, and provides more transparency to protect customers and promote global trust in Microsoft.

Customer Success: Security teams in Customer Success work directly with customers to share best practices, lessons learned, and guidance to accelerate security transformation and modernization. This team assembles and organizes best practices and lessons learned from Microsoft's journey—as well as our customers'—into reference strategies, reference architectures, reference plans, and more.

Cyber Defense Operations Center (CDOC): Microsoft's cybersecurity and defense facility is a fusion center that brings together security professionals from across the company to protect our corporate infrastructure and the cloud infrastructure to which customers have access. Incident responders sit alongside data scientists and security engineers from across Microsoft's services, products, and devices groups to help protect, detect, and respond to threats 24x7.

Democracy Forward Initiative: A Microsoft team working to preserve, protect, and advance the fundamentals of democracy by promoting a healthy information ecosystem, safeguarding open and secure democratic processes, and advocating for corporate civic responsibility.

Digital Crimes Unit (DCU): A team of attorneys, investigators, data scientists, engineers, analysts, and business professionals dedicated to fighting cybercrime at a global scale using technology, forensics, civil actions, criminal referrals, and both public and private partnerships.

Digital Diplomacy: An international team of former diplomats, policymakers, and legal experts working to advance a peaceful, stable, and secure cyberspace in the face of rising nation state conflict.

Digital Security & Resilience (DSR): An organization dedicated to enabling Microsoft to build the most trusted devices and services, while keeping our company safe, and both our company and customer data protected.

Digital Security Unit (DSU): A team of cybersecurity attorneys and analysts who provide legal, geopolitical, and technical expertise to protect Microsoft and its customers. DSU builds trust in Microsoft's enterprise security defenses against advanced cyber adversaries worldwide.

Digital Threat Analysis Center (DTAC): A team of experts who analyze and report on nation state threats, including cyberattacks and influence operations. The team combines information and cyber threat intelligence with geopolitical analysis to provide insights to our customers and to Microsoft to inform effective response and protections.

Enterprise and Security: A team focused on providing a modern, secure, and manageable platform for the intelligent cloud and intelligent edge.

Enterprise Mobility: A team that helps deliver the modern workplace and modern management to keep data secure, in the cloud and on-premises. Endpoint Manager includes the services and tools Microsoft and customers use to manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, and servers.

https://t.me/learningnets

Contributing Teams

Continued

Enterprise Risk Management: A team working across business units to prioritize risk discussions with Microsoft's senior leadership. ERM connects multiple operational risk teams, manages Microsoft's enterprise risk framework, and facilitates the company's internal security assessment using the NIST Cybersecurity Framework.

Global Cybersecurity Policy: A team working with governments, NGOs, and industry partners to promote cybersecurity public policy that empowers customers to strengthen their security and resiliency as they adopt Microsoft technology.

Identity and Network Access (IDNA) Security: A team working to protect all Microsoft customers from unauthorized access and fraud. IDNA Security is a cross-discipline team of engineers, product managers, data scientists, and security investigators.

M365 Security: Organization that develops security solutions including Microsoft Defender for Endpoint (MDE), Microsoft Defender for Identity (MDI), and others, to secure enterprise customers.

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): An advisory board at Microsoft with the mission of ensuring new technologies are developed and fielded in a responsible manner.

Microsoft Bing Search and Distribution: A team dedicated to providing a world-class internet search engine, enabling users around the world to find trusted search results and information quickly, including tracking topics and trending stories that matter to them, while giving users control of their privacy.

Microsoft Customer and Partner Solutions: Microsoft's unified commercial go-to-market organization responsible for field roles such as security and technical sales specialists and advisors.

Microsoft Defender Experts: Microsoft's largest global organization of product-focused security researchers, applied scientists, and threat intelligence analysts. Defender Experts delivers innovative detection and response capabilities in Microsoft 365 security products and Microsoft Defender Experts managed services.

Microsoft Defender for IoT: A team composed of domain-expert researchers specializing in reverse-engineering of IoT/OT malware, protocols and firmware. The team hunts for IoT/OT threats to uncover malicious trends and campaigns.

Microsoft Defender Threat Intelligence (RiskIQ): A team that produces tactical intelligence through analysis of Microsoft's extensive external telemetry collection, charting the threat landscape as it evolves to discover previously unknown threat infrastructure, and adding context to threat actors and campaigns. The team regularly publishes timely and distinctive research to deliver crucial tactical intelligence to defenders.

Microsoft Security Business Development Team: A team that leads Microsoft's cybersecurity growth strategy, partnerships, and strategic investments.

Microsoft Security Response Center (MSRC): A team engaged with security researchers working to protect Microsoft's customers and partner ecosystem. An integral part of Microsoft's Cyber Defense Operations Center (CDOC), MSRC brings together security response experts to detect and respond to threats in real time.

Microsoft Security Services for Incident Response: A team of cybersecurity experts helping customers through the entire cyberattack from investigation to successful containment and recovery related activities. Services are offered via two highly integrated teams, the Detection and Response Team (DART) with a focus on the investigation and groundwork for recovery, and the Compromise Recovery Security Practice (CRSP), which focuses on the containment and recovery aspects.

Microsoft Threat Intelligence Center (MSTIC): A team focused on identifying, tracking, and collecting intelligence related to the most sophisticated adversaries impacting Microsoft customers, including nation state threats, malware, and phishing.

One Engineering System (1ES): A team with a mission of delivering world class tools to help Microsoft developers be as productive and secure as possible. The team leads the central strategy for securing Microsoft's end-to-end software supply chain.

Operational Threat Intelligence Center (OpTIC): The team responsible for managing and disseminating cyber threat intelligence that supports the Microsoft Cyber Defense Operation Center's (CDOC) mission to protect Microsoft and our customers.

https://t.me/learningnets

Microsoft

Illuminating the threat landscape and empowering a digital defense.

- Learn more: **https://microsoft.com/mddr**
- Dive deeper: **https://blogs.microsoft.com/on-the-issues/**
- Stay connected: **@msftissues and @msftsecurity**

© 2022 Microsoft. All rights reserved.

https://t.me/learningnets