Microsoft

# Microsoft Digital Defense Report

## Building and improving cyber resilience

October 2023
Microsoft Threat Intelligence

https://t.me/learningnets

# Contents

The data, insights, and event in this report are from July 2022 through June 2023 (Microsoft fiscal year 2023), unless otherwise noted.

For easier viewing and navigating through the report on certain browsers, we suggest using Adobe Reader, which is available for free on the Adobe website.

Chapter 1
**Introduction**

Introduction 3
Sharing Microsoft's unique vantage point 5
The power of partnership in building cyber resilience 6
How can we protect against 99% of attacks? 7
Driving global progress through the Cybersecurity Tech Accord 8
About this report 9
Threat actor map 11

Chapter 2
**The State of Cybercrime**

Key developments 13
Introduction 14
How the threat landscape is evolving 15
Insights on ransomware and extortion 17
Insights on phishing 27
Insights on business email compromise 32
Insights on identity attacks 34
Insights on distributed denial of service attacks (DDoS) 38
Return on mitigation: Targeting investment to increase resilience 41

Chapter 3
**Nation State Threats**

Key developments 46
Introduction 47
Russia 54
China 60
Iran 65
North Korea 70
Palestinian threat actors 73
The emerging threat posed by cyber mercenaries 74

Chapter 4
**Critical Cybersecurity Challenges**

Key developments 76
Introduction 77
The state of IoT and OT security 78
Improving global critical infrastructure resilience 86
Innovating for supply chain resilience 90

Chapter 5
**Innovating for Security and Resilience**

Key developments 97
Introduction 98
Using the power of AI for cybersecurity 100
Working together to shape responsible AI 106

Chapter 6
**Collective Defense**

Key developments 109
Introduction 110
How the global Cybercrime Atlas will revolutionize cybercrime intelligence and collaboration 111
Collective intelligence and defense against Volt Typhoon 112
Uniting forces against cybercrime: A success story of collaboration and disruption 113
Advancing open source security together 116
Strengthening media content provenance, accountability, and transparency 117
Combining efforts to safeguard democracy 118
How we are addressing the digital talent and diversity shortage 119
The CyberPeace Institute: Uniting to empower nonprofits with cyber resilience 121
Building cybersecurity capacity through the Cyber Development Goals 122

Appendix
**Additional information**

Cybersecurity Tech Accord principles mapping index 124
Contributing teams 126
Footnotes 128

https://t.me/learningnets

# Chapter 1 Introduction

## About this report


| | |
|---|---|
| Introduction | 3 |
| Sharing Microsoft's unique vantage point | 5 |
| The power of partnership in building cyber resilience | 6 |
| Driving global progress through the Cybersecurity Tech Accord | 8 |
| About this report | 9 |
| Threat actor map | 11 |


https://t.me/learningnets

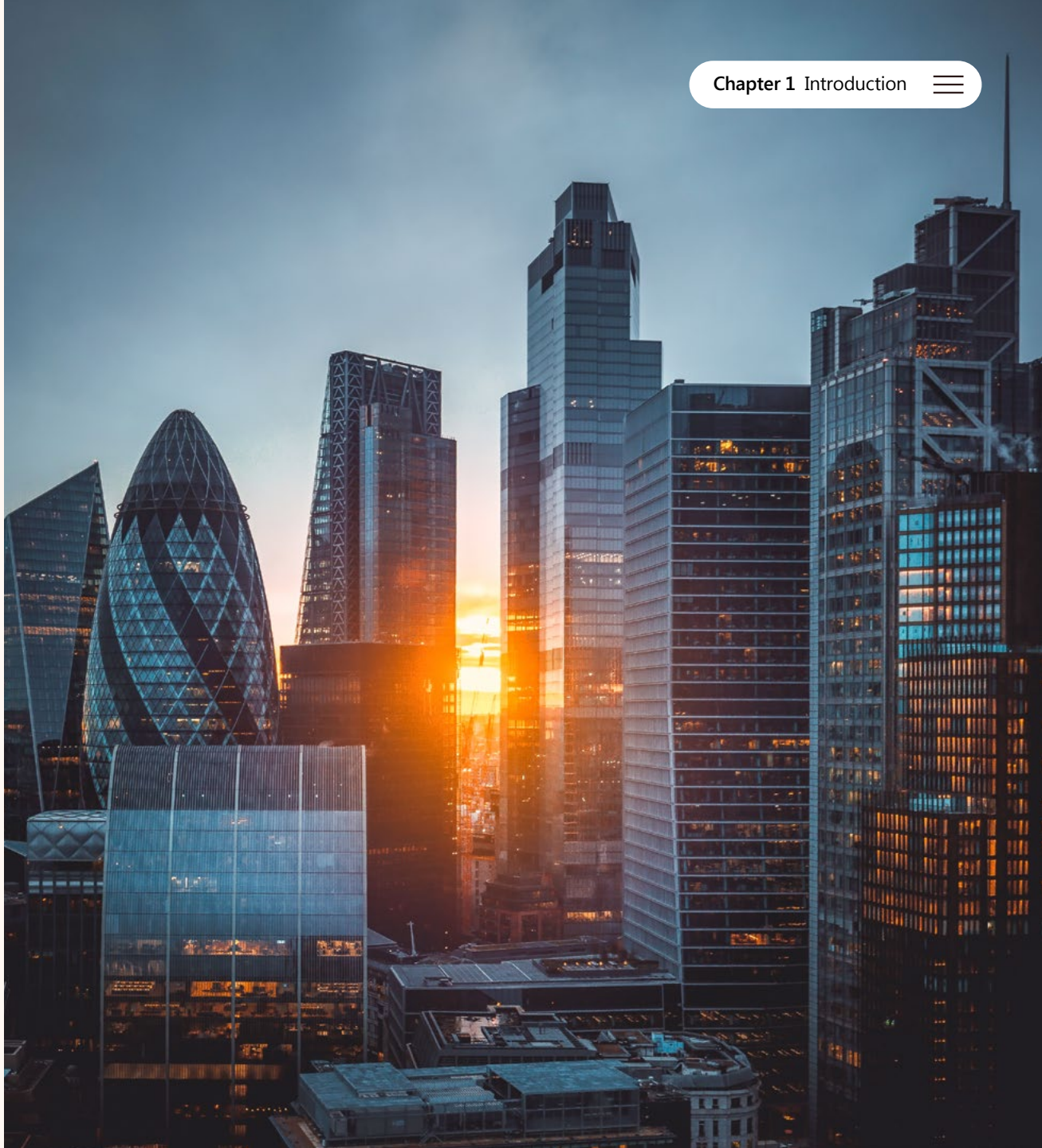
# Securing our future together

## Introduction from Tom Burt

Over the last year, threats to digital peace have reduced trust in technology and highlighted the urgent need for improved cyber defenses at all levels. Encouragingly, defenders the world over are responding to the call to improve security with the public and private sectors investing and collaborating to confront the challenges and build long-term resilience.

In this fourth annual edition of the Microsoft Digital Defense Report, we draw on our unique vantage point to share insights on how the threat landscape has evolved and discuss the shared opportunities and challenges we all face in securing a resilient online ecosystem which the world can depend on.

"Close collaboration between the public and private sectors to formulate, enforce, and harmonize these requirements is crucial to improve global cybersecurity and foster innovation."



https://t.me/learningnets

"As the digital domain faces new and more threatening challenges, defenders are being driven to innovate and collaborate more closely than ever."

As the digital domain faces new and more threatening challenges, defenders are being driven to innovate and collaborate more closely than ever. For example, Russia's use of cyberweapons as part of its hybrid war against Ukraine sparked sustained collaboration between Microsoft and Ukrainian officials to successfully defend against most of these cyberweapons.

Russia is not alone in its use of destructive malware; we have also seen increased use of cyberweapons by Iran to pressure the Albanian government and in its ongoing conflict with Israel. At the same time, nation states are becoming increasingly sophisticated and aggressive in their cyber espionage efforts, led by highly capable Chinese actors focused on the Asia Pacific region in particular.

One recent example of the troubling increase in aggression and capability involves a Chinese actor, which Microsoft calls Volt Typhoon. It used inventive tradecraft to infiltrate and pre-position malware in the networks of a range of communications companies and other critical infrastructure organizations in Guam and the United States, deploying "living off the land" techniques to evade detection.

Nation-state actors were not alone in stepping up their abuse of the digital ecosystem. Well-resourced cybercriminal syndicates also continue to grow and evolve, leveraging the cybercrime-as-a-service ecosystem we highlighted last year. Ransomware-as-a-service and phishing-as-a-service are key threats to businesses and cybercriminals have conducted business email compromise and other cybercrimes, largely undeterred by the increasing commitment of global law enforcement resources.

Many vendors are taking steps to improve the cybersecurity of their products and services, developing new tools to help customers better defend against attackers. Governments across the globe are providing the public with more information about cyber threats and how to counter them, like the effective alerts from the US Cybersecurity and Infrastructure Security Agency's (CISA) Shields Up campaign. Governments are also imposing new legal and regulatory requirements for cybersecurity. While many of these are beneficial, they can impose counterproductive conditions—such as requiring overly rapid reporting of cybersecurity incidents or establishing inconsistent or conflicting requirements across agencies or geographies. Close collaboration between the public and private sectors to formulate, enforce, and harmonize these requirements is crucial to improve global cybersecurity and foster innovation.

As we are seeing, Artificial Intelligence (AI) technologies are set to become a major focus of regulators and industry. We will undoubtedly see attackers using AI as a tool to refine phishing messages, develop malware and enable other abuses of technology. But AI will also be a critical component of successful defense. For example, in Ukraine we saw the first successful use of AI technology to help defend against Russian cyberattacks. In the coming years, innovation in AI-powered cyber defense will help reverse the tide of cyberattacks.

Advancing the promise of digital peace requires public-private collaboration to ensure we are bringing to bear the best technological and regulatory tools to combat cyber aggression. We need more and deeper alliances in the private sector and stronger partnerships between the private and public sectors. Enabling this collaboration can be challenging but, when successful, it drives meaningful impact. We must accelerate the move of critical computing workloads to the cloud, where vendors' security innovations will be most impactful, and ensure AI innovation provides defenders with the durable technological advantage over attackers that it promises.

**Tom Burt**
Corporate Vice President, Customer Security & Trust

https://t.me/learningnets

# Sharing Microsoft's unique vantage point

Cybersecurity is a defining challenge of our time. Organizations of every size across every industry around the globe feel the urgency and pressure of protecting and defending against increasingly sophisticated attacks.

While AI is transforming cybersecurity, using it to stay ahead of threats requires massive amounts of diverse data. Here at Microsoft, our more than 10,000 security experts analyze over 65 trillion signals each day with the help of AI, and Microsoft Threat Intelligence teams track hundreds of threat actor groups worldwide. The Microsoft security ecosystem includes more than 15,000 security partners with specialized solutions, while the global open community of security researchers and testers contribute to bug bounties and security challenges. This broad, deep, and diverse security ecosystem is driving some of the most influential insights in cybersecurity. Together, we can build cyber resilience through innovative action and collective defense.

**As part of our longstanding commitment to create a safer world, Microsoft's investments in security research, innovation, and the global security community include:**

## 65 trillion
signals synthesized daily

That is over 750 million signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

## 10,000+
security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

## 4,000
identity attacks blocked per second

4,000 identity authentication threats blocked per second.

## 300+
threat actors tracked

Microsoft Threat Intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

## 100,000+
domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

## 15,000+
partners in our security ecosystem

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

## 135 million
managed devices

135 million managed devices providing security and threat landscape insights.

All data is based on Microsoft fiscal year 2023 unless otherwise indicated.

https://t.me/learningnets

# The power of partnership in building cyber resilience

We believe every individual and company around the world should be empowered to meet its security needs. Achieving this will require a collective global effort as we harness the power of partnership to strengthen our defenses together.

Strength in numbers. Stronger together. Together we stand. Societies around the world recognize the benefits of collective behavior. The power of multistakeholder partnerships in cybersecurity, too, cannot be ignored as we seek to answer the question, "What we can do to ensure a more safe and secure world for everyone on the planet?"

Individual organizations are often focused on safeguarding their own data and systems and protecting their customers, constituents, and communities.

But partnerships act as a force multiplier for everyone involved in cybersecurity. Collaborative efforts among stakeholders—including government agencies, private sector entities, academia, non-profits, and other organizations—are crucial in building resilient defenses against cyber threats.

### The cyber poverty line

To understand the need for collaboration, it is useful to consider the concept of a "cyber poverty line." In the same way that governments and economists establish a social poverty line to determine a bare minimum standard of living, the cyber poverty line is the minimum level of resources required for adequate protection from cyber threats. As we ponder the implication of the existence of a cyber poverty line, important questions begin to surface. How, exactly, do we quantify the cyber poverty line? Who is below it and how can we work together to support them to rise above it? These questions underscore the imperative of partnership in cybersecurity and serve as the genesis of meaningful conversations we must have.

### Public-private partnerships, policy, and standards

The opportunities for partnership across the public and private sectors, policy organizations, and standards bodies are multi-dimensional. From ensuring the technology community is building safer, more secure technology and collaborating on threat intelligence and trends to developing common standards to take down and block the tools cybercriminals use, strong and bi-directional partnerships between organizations are crucial.

As much as any individual company's shareholders would like it to be so, no one technology company can solve or overcome every cybersecurity challenge. Partnerships across the technology community are an absolute necessity to ensure organizations of all types and sizes, in every industry and region, can protect themselves. This means working together to push the boundaries of innovation, ensuring technical integration of products in the security space and addressing the end-to-end security needs of customers.

> The concept of a cyber poverty line allows us to identify the minimum level of resources required for adequate protection from cyber threats and who we must support to rise above it.

### Non-profit, academia, and research

Non-profit, academia, and research organizations play a crucial role in advancing cybersecurity. By collaborating with industry partners, they bridge the gap between theoretical knowledge and practical application. Academic institutions contribute to cybersecurity research, develop innovative technologies, and educate the next generation of cybersecurity professionals. Collaborative research projects and initiatives between academia, non-profits, and industry promote innovation and help tackle emerging cyber threats effectively.

It is essential that stakeholders recognize their shared responsibility and actively engage in partnerships that enhance cybersecurity. History has already shown that by working together, we can build a safer digital future for individuals, organizations and nations—but there is so much more to be done.

**For more about the power of partnerships, please see the Collective Defense chapter on page 108.**

**Additional information**

Collaboration is crucial to strengthening cybersecurity | Microsoft On the Issues

https://t.me/learningnets

# How can we protect against 99% of attacks?

While we explore the many dimensions of the cyber threat landscape, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
2. **Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack 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. Allow only the privilege that is needed for access to a resource and no more.
   - Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
3. **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
4. **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.
5. **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

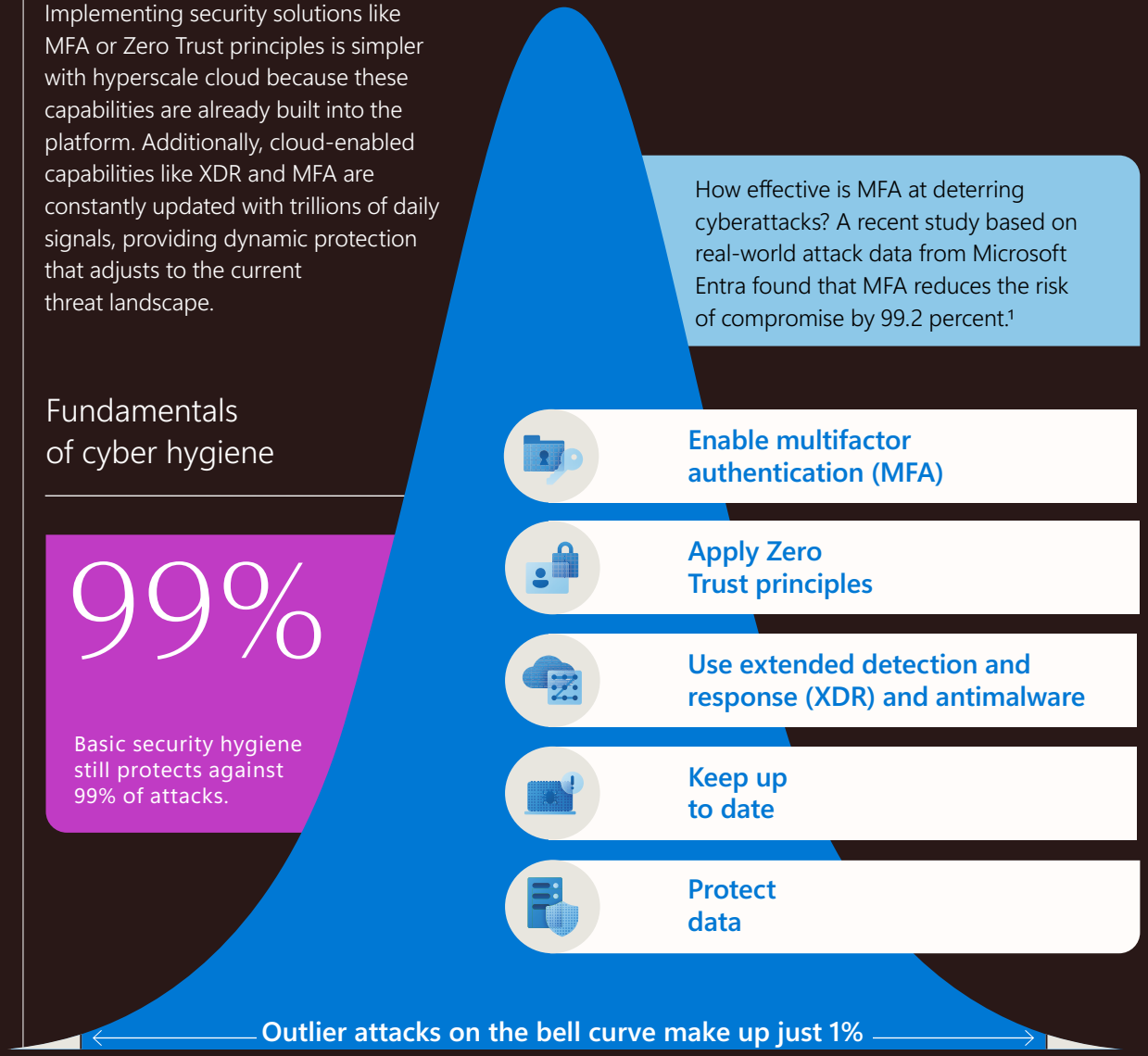
Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

## Fundamentals of cyber hygiene

**99%**

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]




https://t.me/learningnets

# Driving global progress through the Cybersecurity Tech Accord

Since its inception, the Cybersecurity Tech Accord has witnessed remarkable progress. As we mark its fifth anniversary, we celebrate a groundbreaking commitment by 156 technology and security companies from around the world to protect our customers from malicious attacks by cybercriminals and nation states.

The Cybersecurity Tech Accord has worked to be the technology industry's voice on matters of peace and security in cyberspace and to uphold a commitment to protect users and customers everywhere from evolving cyber threats. At the core of this historic initiative are four fundamental cybersecurity principles:

1. Better defense: We will protect all of our users and customers everywhere.
2. No offense: We will oppose cyberattacks on innocent citizens and enterprises from anywhere.
3. Capacity building: We will help empower users, customers, and developers to strengthen cybersecurity protection.
4. Collective action: We will partner with each other and likeminded groups to enhance cybersecurity.

The Accord has launched several initiatives, including the Internet of Things (IoT) Security Resource Hub, which aims to establish a strong global baseline for IoT security in the next generation of consumer products. Signatories and industry partners have also embraced a set of principles to combat the menace of cyber mercenaries. The group also engages in extensive consultations with governments, civil society, and private sector partners, advocating for responsible nation-state behavior and amplifying the technology industry's role in international cybersecurity.

In the past year, the Cybersecurity Tech Accord has made strides in raising awareness of the escalating threats posed by some nation-state actors. In particular, the group launched an Annual State of International Cybersecurity Thermometer, which in 2023 reached a "boiling point," largely due to the widespread and unprecedented use of cyber operations in the armed conflict in Ukraine.

The Cybersecurity Tech Accord has invested in promoting diversity, particularly empowering women in cybersecurity. Microsoft is proud to work with industry partners and non-profit organizations worldwide to broaden access and foster the careers of women working in this critical field.

**To understand how topics discussed in this report track against the Cybersecurity Tech Accord, please see page 124.**

**Additional information**

https://cybertechaccord.org

In 2023, the cyber conflict thermometer reached "the boiling point"

https://t.me/learningnets

# About this report

### Signposts

For ease of reading, we have included icons to signpost discussion that relates to specific efforts throughout this report. This relates to AI-related content, partnerships, and the Cybersecurity Tech Accord principles.

### Cybersecurity Tech Accord principles:

Icons representing the principles of the Cybersecurity Tech Accord are signposted throughout this report to serve as a visual reminder of our collective dedication to safeguarding the digital landscape. A full index is provided on page 124.

- Pr Protect Users and Customers
- Op Oppose Cyberattacks
- Em Empower Users, Customers, and Developers
- Pa Partner to Enhance Cybersecurity

**Scope:** Unless otherwise noted, this report covers the period from July 2022 through June 2023 (Microsoft fiscal year 2023).

In general, when referring to critical infrastructure sectors in this report, we are including the 16 sectors identified by the US Cybersecurity & Infrastructure Security Agency (CISA)[2]:

- Chemicals
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater

### Last year's report

The 2022 Digital Defense Report focused on illuminating the threat landscape and empowering a digital defense. Relevant discussion from last year is referenced in this report.

You can access the 2022 Microsoft Digital Defense Report in the archive section at https://aka.ms/mddr.

https://t.me/learningnets

# Threat actor descriptions and naming

Throughout this report, we refer to the five key groups that Microsoft uses to characterize threat actors:

- **Nation-state actors** are cyber operators who act on behalf of, or directed by, a nation/state-aligned program, irrespective of whether the goal is espionage, financial gain, or retribution.
- **Financially motivated actors** are cyber campaigns/groups directed by a criminal organization/person with the motivation of financial gain which have not been associated with high confidence to a known non-nation state or commercial entity.
- **Cyber mercenaries or private sector offensive actors** refer to commercial actors that are known/legitimate legal entities that create and sell cyberweapons to customers who select targets and operate the cyberweapons.
- **Influence operations** are manipulative information campaigns communicated online or offline that are intended to shift perceptions, behaviors, or decisions by target audiences to further a group or a nation's interests and objectives.
- **Groups in development** is a temporary designation given to an unknown, emerging, or developing threat activity. This allows Microsoft to track it as a discrete set of information until we can reach high confidence about the origin or identity of the actor behind the operation.

### Threat actor naming taxonomy

In April, we announced that we have shifted to a new threat actor naming taxonomy aligned to the theme of weather. The complexity, scale, and volume of threats is increasing, driving the need to reimagine not only how Microsoft talks about threats but also how we enable customers to understand those threats quickly and with clarity. With the new taxonomy, we intend to bring better context to customers and security researchers that are already confronted with an overwhelming amount of threat intelligence data. It will offer a more organized, memorable, and easy way to reference adversary groups so that organizations can better prioritize threats and protect themselves. Simply put, security professionals will instantly have an idea of the type of threat actor they are up against, just by reading the name.

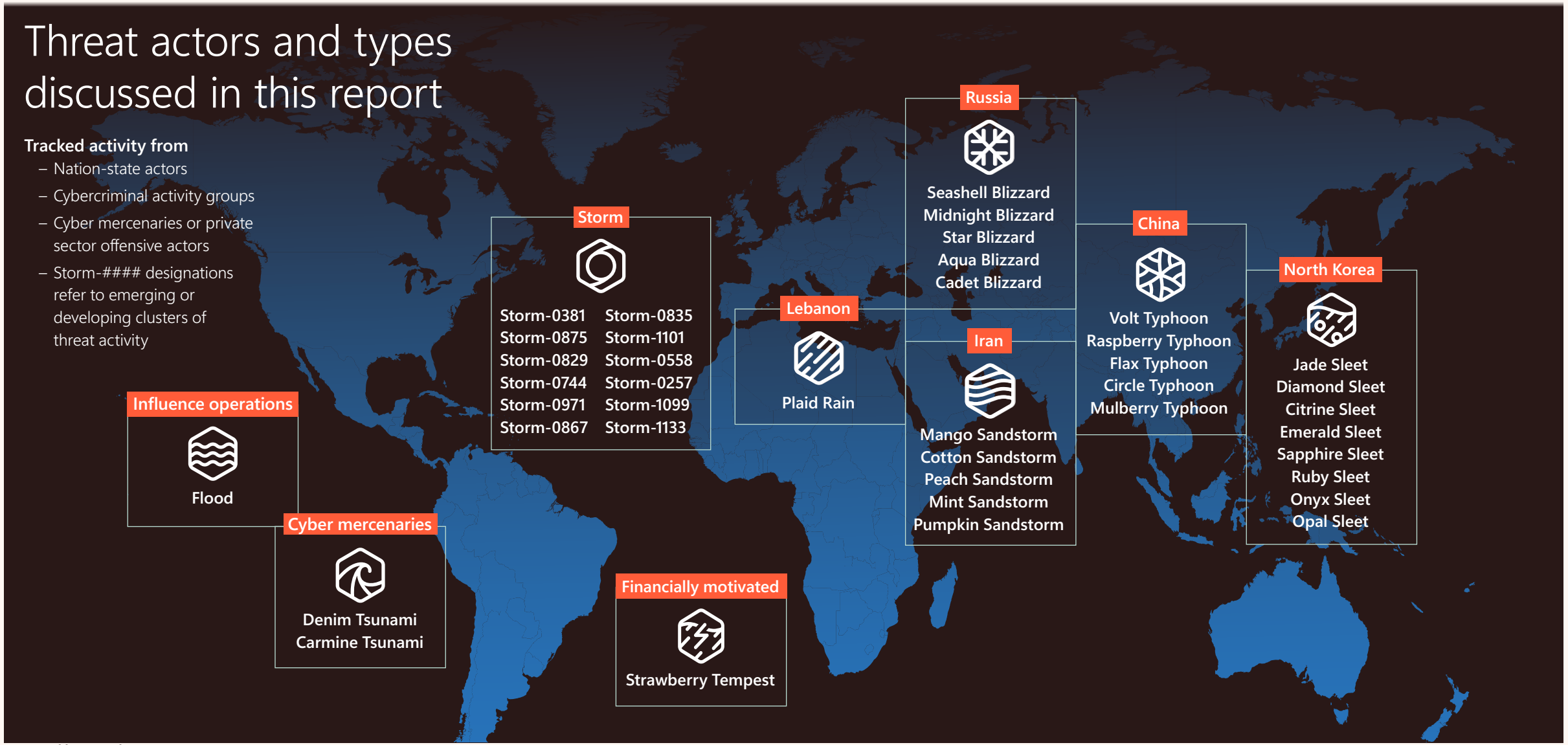
**Additional information**

How Microsoft names threat actors | Microsoft

### Other definitions:

- **Cyber-enabled influence operations:** Operations that combine offensive computer network operations with messaging and amplification in a coordinated and manipulative way to shift perceptions, behaviors, or decisions by target audiences to further a group or nation's interests and objectives.
- **NSN data:** This data is based on aggregated nation-state notifications (NSNs)—notices that we send to customers when they have been targeted or compromised by a nation-state actor that is tracked by Microsoft. Data overwhelmingly reflects activity against Office 365, followed by Outlook and Hotmail. We count NSN data by number of targeted organizations.
- **Events data:** This data covers a broader range of investigative observations of nation-state threat actor activity than NSNs. Activity captured in "events" ranges from reconnaissance and movement on network to data exfiltration or deletion.

https://t.me/learningnets



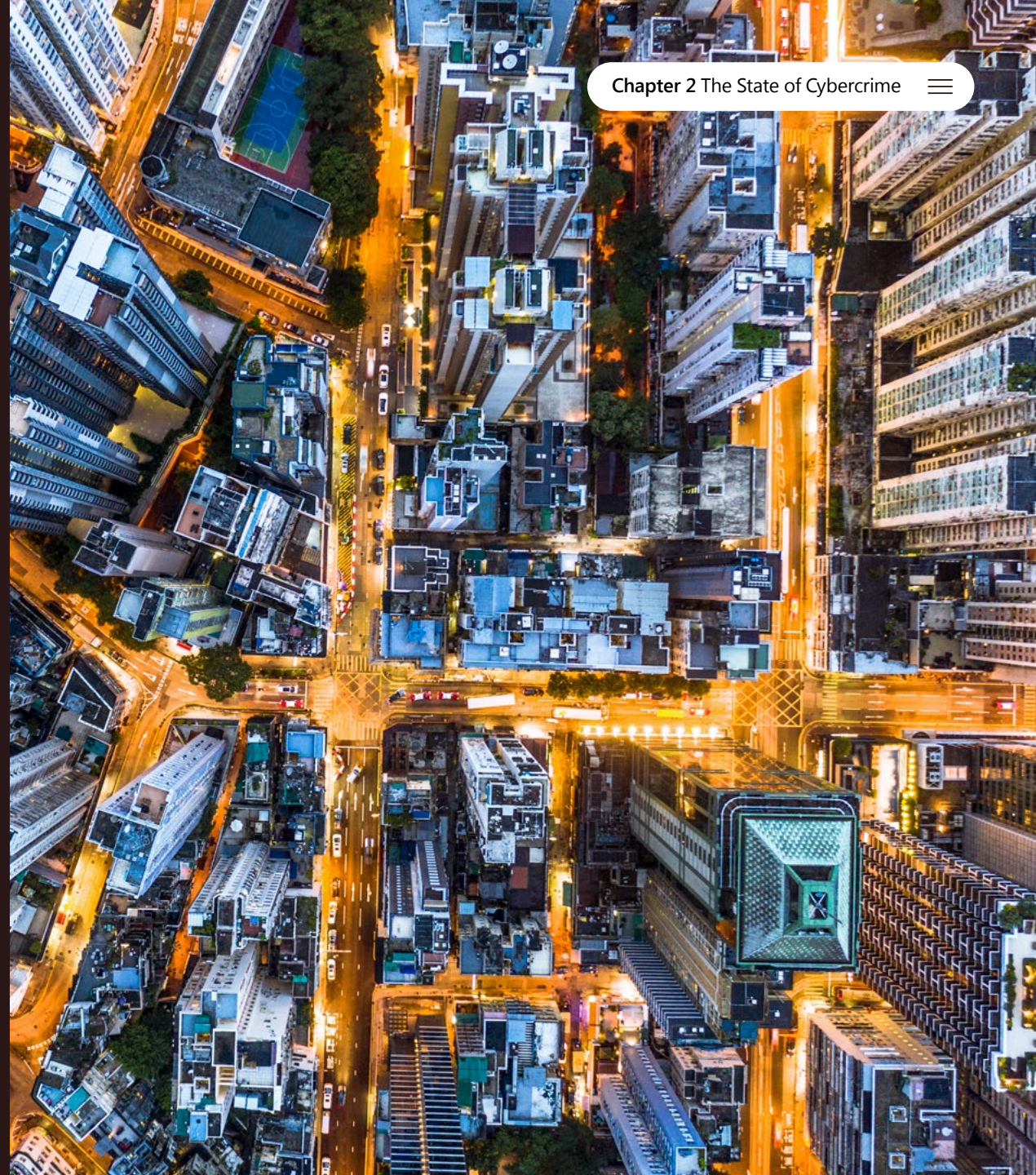

https://t.me/learningnets

# Chapter 2
# The State of Cybercrime

## What we know about cybercrime today


| | |
|---|---|
| Key developments | 13 |
| Introduction | 14 |
| How the threat landscape is evolving | 15 |
| Ransomware and extortion | 17 |
| Phishing | 27 |
| Business email compromise | 32 |
| Identity attacks | 34 |
| Distributed denial of service attacks (DDoS) | 38 |
| Return on mitigation: Targeting investment to increase resilience | 41 |


https://t.me/learningnets



The State of Cybercrime

# Key developments

Cybercriminals are leveraging the cybercrime-as-a-service ecosystem to launch phishing, identity, and distributed denial of service (DDoS) attacks at scale. Simultaneously, they are increasingly bypassing multifactor authentication and other security measures to conduct targeted attacks.

Ransomware operators are shifting heavily toward hands on keyboard attacks, using living-off-the-land techniques and remote encryption to conceal their tracks, and exfiltrating data to add pressure to their ransom demands. And cybercriminals are improving their ability to impersonate or compromise legitimate third parties, making it even harder for users to identify fraud until it's too late.

80-90%

**of all successful ransomware compromises originate through unmanaged devices.**

Find out more on page 18

**A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.**

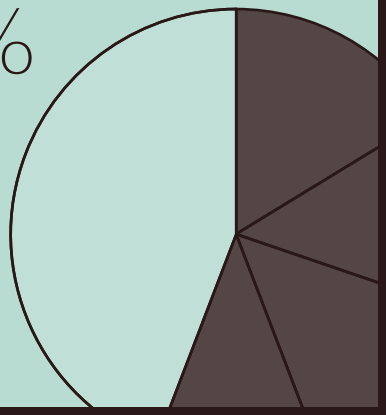
Find out more on page 41

70%

of organizations encountering human-operated ransomware had fewer than 500 employees.

Find out more on page 18

Human-operated ransomware attacks are up more than 200%



Find out more on page 17

Password based attacks spiked in 2023

Find out more on page 34

Last year marked a significant shift in cybercriminal tactics

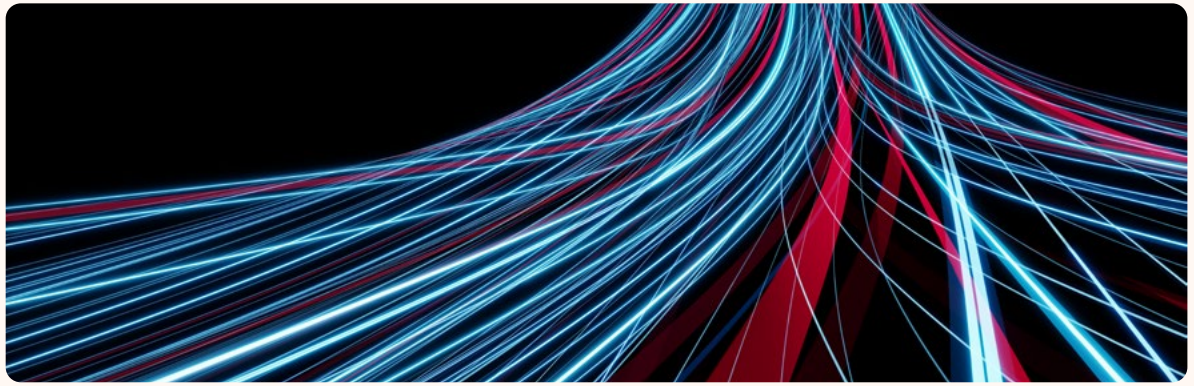
**with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.**

Find out more on page 39

https://t.me/learningnets

# Joining forces against cybercrime

## Introduction from Amy Hogan-Burney



While cybercriminals have remained hard at work, we are seeing public and private sectors come together to disrupt the technologies criminals use, hold them to account, and support the victims of cybercrime.

As cybercriminals look for new ways to generate income, they have stayed focused on exploiting weakness in humans and technology, staying ahead of security measures, and coordinating to create sophisticated global networks that sell services. To combat them, public and private sector professionals and organizations are creating strong partnerships that are disrupting criminal's technology, hold threat actors accountable, and increase resilience to attacks.

As a result, attackers are finding themselves in the crosshairs of law enforcement. Many have been outed, including the Conti ransomware operator known as "Target" whose unmasking includes a $10 million reward for additional information, indicted (Yevgeniy Polyanin) or arrested (Yaroslav Vasinskyi) alleged to have deployed the Sodinokibi/REvil ransomware to attack businesses and governments.

Governments are also looking beyond criminals to rescue victims, disrupt malicious technology, and seize and return money–as was seen in the case of the Hive ransomware. The private sector is an essential partner in these efforts, whether through criminal referrals and information sharing with law enforcement or through technical and legal action, as seen in Microsoft and Fortra's action to disrupt cracked, legacy copies of Cobalt Strike and abused Microsoft software see page 113.

Op Cybersecurity Tech Accord principles mapping index on **page 124**

The result is that cybercriminals are looking for ways to increase their anonymity and effectiveness. As human-operated ransomware attacks on small and medium businesses increase, we have seen more use of remote monitoring and management tools that leave behind less evidence. Many of these ransomware attacks attempt to compromise or gain access to unmanaged or bring-your-own devices because they typically have fewer security controls and defenses.

Attackers continue to look for the easiest method to gain unauthorized access to any system through identity attacks such as traditional brute-force attempts, sophisticated password spray attempts across multiple countries and IP addresses, and adversary-in-the middle (AiTM) attacks. Phishing is not going away, and attackers are using both malware phishing to compromise devices and AiTM phishing to steal identities that can be used in further criminal activity such as business email compromise.

As you read this report, I encourage you to look for opportunities to improve your defensive security posture, identify areas where you may need investment, and explore ways to make training programs more effective. Consider your opportunities to engage in simulated cyberattacks or tabletop exercises, invest in threat intelligence and actor tracking in the cybercrime space, share information with law enforcement, and take technical or legal disruptive actions. We all have a part to play in fighting cybercrime, and I urge you to consider what more you, your company, or your government could do to help improve cyber resilience.

**Amy Hogan-Burney**
General Manager, Associate General Counsel, Cybersecurity Policy & Protection

https://t.me/learningnets

# How the threat landscape is evolving

The cyber threat landscape is continuing to evolve toward more effective and more damaging attacks, which often take place at scale. According to our data, organizations faced an overall increase in ransomware attacks compared to the previous year, while the number of human-operated ransomware attacks almost tripled.

13%

of human-operated ransomware attacks that moved into the ransom phase included some form of data exfiltration.

This was accompanied by a sharp increase in the use of remote encryption during attacks. Using this method, an attacker encrypts a file on a different computer, and then sends the encrypted file to the original computer. This can happen if one computer on a network is hacked and has access to another computer with the compromised user account(s). No additional software is needed on the original computer, and no harmful files are left behind.

Data extortion is also on the rise. Since November 2022, we observed a doubling of potential data exfiltration instances–the theft or unauthorized removal or movement of data from a device. Thirteen percent of human-operated ransomware attacks that moved into the ransom phase had some form of data exfiltration.

The frequency of business email compromise (BEC) attacks has skyrocketed to over 156,000 daily attempts. Microsoft Entra data shows attempted password attacks increased more than tenfold in 2023, from around 3 billion per month to over 30 billion. This translates to an average of 4,000 blocked attacks per second targeting Microsoft cloud identities.

https://t.me/learningnets

# What we can learn from attack notifications

Managed extended detection and response (XDR) services, such as Microsoft Defender Experts, are invaluable resources for security operations centers to effectively detect and respond to critical incidents.

When we observe novel tactics, techniques, and procedures, human-directed attacks, or attack progression, notifications are sent to our customers to provide specific information regarding the scope, method of entry, and instructions for remediation.

Pr Cybersecurity Tech Accord principles mapping index on **page 124**

**Based on the notifications shared with customers, these are the top threats identified by Microsoft Defender Experts this year:**

1. **Successful identity attacks:** Attacks across identity included traditional brute-force attempts, sophisticated password spray attempts across multiple countries and IP addresses, and adversary-in-the middle (AiTM) attacks.

   **For more about identity attacks, see page 34**.

2. **Ransomware encounters:** These are defined in this report as any instance of ransomware activity or attempted attacks that we have detected and prevented or alerted on, throughout the various stages of a ransomware attack.

   In addition to several ransomware variants this year, we observed a unique large-scale ransomware campaign targeting both endpoints and cloud architecture of an organization. This was driven by the threat actor we named Mango Sandstorm. This campaign included both on-premises and cloud environments, and involved privilege escalation and destruction activities, including deletion of victim user resources, and persistence using OAuth applications. Attackers added a secret or certificate to an application in order to connect to Azure Active Directory (Azure AD) as the application, and perform operations (such as reading confidential data and emails, exfiltrating information through emails) leveraging the application permissions that are assigned to it.

   **For more about ransomware see page 17**.

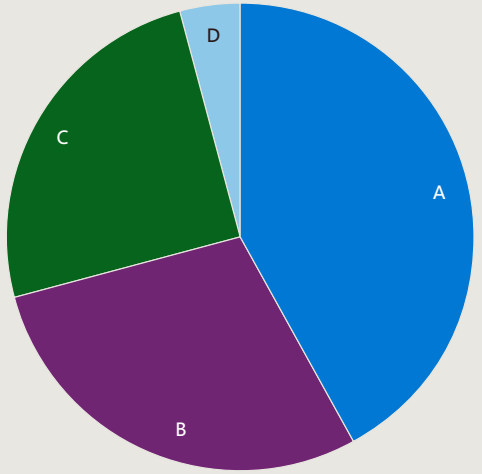
3. **Targeted phishing attempts leading to device or user compromise:** We have observed both malware phishing with intent to compromise devices, and AiTM phishing attempting to steal identities. Defense evasion techniques included phishing from compromised vendors and abuse of legitimate services.

   **For more about phishing and AiTM, see page 27**.

4. **Business email compromise (BEC):** Attackers used various methods including email conversation hijacking and mass spamming with malicious applications to commit financial fraud. They also sent phishing emails with harmful links and attachments from the victim's email address to other users within the victim's organization. Since these phishing emails were sent internally, multiple users fell victim to the attack by clicking on the links within a short period of time.

   **For more about BEC, see page 32**.

**Distribution of top four attack progression notifications**




A 42% Successful identity attacks

C 25% Successful targeted phishing attempts

B 29% Ransomware encounters

D 4% Business email compromise (BEC)

Telemetry sources: Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

**Additional information**

Detecting and mitigating a multi-stage AiTM phishing and BEC campaign | Microsoft

Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity | Microsoft

https://t.me/learningnets

# Insights on ransomware and extortion

## New tactics and trends

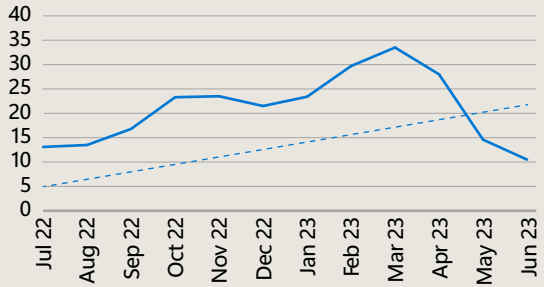
Microsoft's telemetry indicates that organizations faced an increased rate of ransomware attacks compared to last year, with the number of human-operated ransomware attacks up more than 200 percent since September 2022.

The good news is, for organizations with a strong security posture, the likelihood of an attack succeeding is very low. Typically, an attack is stopped in the pre-ransom phase, with on average 2 percent of attacks progressing to a successful ransomware deployment.

Approximately 40 percent of the ransomware encounters we detected in June were human-driven. Most of these attacks can be attributed to 123 tracked ransomware-as-a-service affiliates. The number of affiliates grew by 12 percent in the last year, setting up conditions for human-operated ransomware attacks to continue to grow in 2024.

**Ransomware breaches per month per 100,000 organizations**

We observed an overall increase in successful ransomware attacks with a sharp decrease in March-April.




Telemetry sources: Microsoft Security Graph, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

### Remote encryption

In a notable change from last year, we observed a sharp increase in the use of remote encryption during human-operated ransomware attacks. Instead of deploying malicious files on the victim device, encryption is done remotely, with the system process performing the encryption, which renders process-based remediation ineffective. On average, 60 percent of human-operated ransomware attacks used remote encryption over the past year. This is a sign of attackers evolving to further minimize their footprint.

### Initial attack vectors

The Microsoft Incident Response team responds to incidents and helps customers secure their most sensitive, critical environments. Based on findings during these engagements, the top three initial access vectors were fairly evenly split, showing criminals are consistently exploiting the same vectors: external remote services, valid accounts, and public facing applications.

We found that among external remote services, adversaries primarily leveraged unsecured remote desktop protocol (RDP) and virtual private networks (VPN). Threat actors attacking valid accounts, where the attacker somehow gained legitimate account credentials, were most often able to log in via Citrix.

Among vulnerable external facing applications, cybercriminals exploited vulnerabilities ranging from zero-day vulnerabilities to those that were two to three years old, with Zoho Java ManageEngine, Exchange, MOVEit, and PaperCut print management software among the top applications exploited.

**Actionable insights**

**To safeguard against these attacks:**

1. It is crucial to implement Zero Trust and least privilege principles.
2. The most efficient solutions are those that can instantly identify attackers by utilizing signals from devices, users, and the entire organization, and take automatic remedial measures across both managed and unmanaged devices.
3. It is essential to have a seamless method to restore encrypted files at the organizational level.

**Additional information**

How automatic attack disruption works in Microsoft 365 Defender | Microsoft

Automatically disrupt adversary-in-the-middle attacks with XDR | Microsoft

https://t.me/learningnets

# Ransomware targeting

### Unmanaged devices

Most human-operated ransomware attacks attempt to compromise or gain access to unmanaged or bring-your-own devices (personal devices used to access work-related systems and information). These typically have fewer security controls and defenses. We have observed that 80 to 90 percent of all compromises originate from unmanaged devices. Ransomware operators are also increasingly exploiting vulnerabilities in less common software, making it more difficult to predict and defend against their attacks. This reinforces the importance of a holistic security approach.

### Organization size

Despite the notoriety of high-profile attacks last year, the primary victims of ransomware attacks this year were small and medium size organizations. Between July and September 2022, around 70 percent of organizations encountering human-operated ransomware had fewer than 500 employees.

### Industries

While the critical infrastructure sectors experienced the most ransomware encounters this year, cybercriminals have broadly attacked all sectors. Attackers leveraged new techniques as pre-cursors to ransomware to establish the foothold within the victim organization before exfiltration and ransom. As seen in the distribution of pre-ransom notifications sent by Microsoft Defender Experts to our customers, education and manufacturing sectors were key targets. For example, threat actors targeted a critical remote code execution vulnerability found in PaperCut server, which is used by educational organizations.

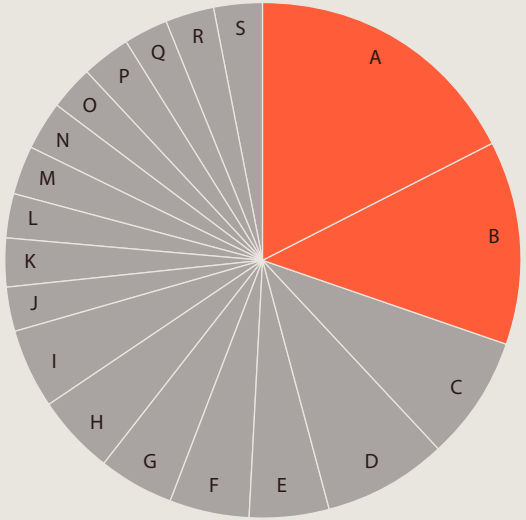
**70%**

of organizations encountering human-operated ransomware had fewer than 500 employees.

**80-90%**

of all compromises originate from unmanaged devices.

**Pre-ransom notifications by industry**




- A Discrete Manufacturing
- B Higher Education
- C Real Estate
- D Professional Services
- E Consumer Goods
- F Retailers
- G Primary & Secondary Edu/K-12
- H IT Services & Business Advisory
- I Insurance
- J Gov Ops & Infrastructure
- K Power & Utilities
- L Media & Entertainment
- M Health Provider
- N Water & Sewage
- O Automotive & Mobility
- P Capital Markets
- Q Medical Manufacturing
- R Automobile
- S Telecommunications

Source: Microsoft Defender Experts notifications

https://t.me/learningnets

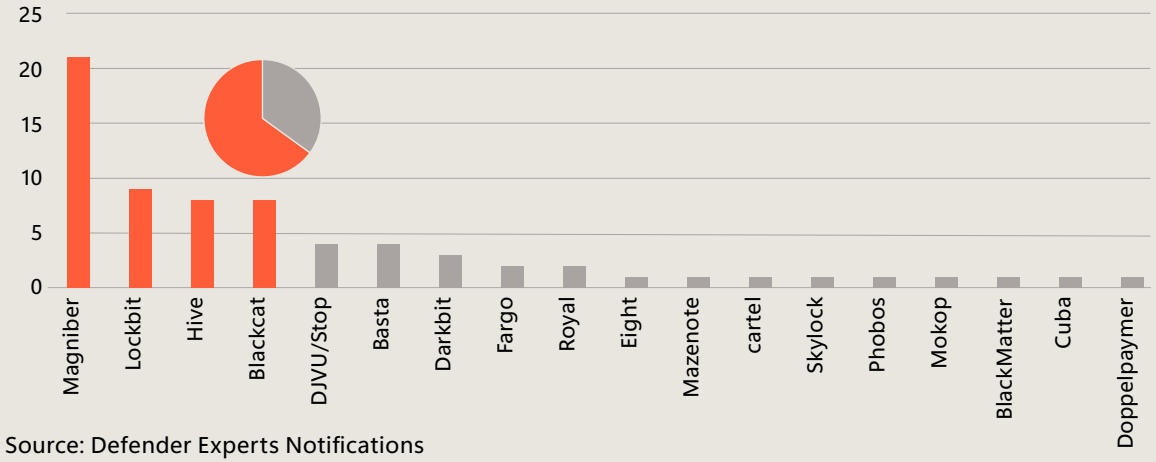
# Ransomware variants

Based on data from Microsoft Defender Experts notifications the top four malware variants—Magniber, Lockbit, Hive, and BlackCat—comprised almost two-thirds of ransomware encounters.

Magniber ransomware, which is an automated variant without human operation, has been linked to Storm-0381, which has a track record of using malvertising, the Magnitude exploit kit, and malicious payloads disguised as Windows updates to disseminate Magniber. Magniber was initially used to target countries in Asia in around 2017, but since resurfacing a few years ago it has expanded its reach to global targets.

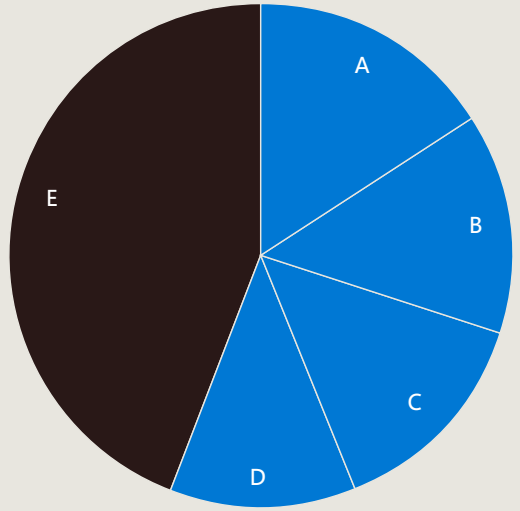
**Breakdown of ransomware by variants**

The top four variants comprised 65% of all ransomware encounters




Source: Defender Experts Notifications

**Top human-operated ransomware variants that achieved breaches**




A 16% Lockbit 3.0

B 14% BlackBasta

C 14% Blackcat

D 12% Royal

E 44% BlackByte
Hive, Play
Akira, BitLocker
Cartel, Cuba
Dagoned
Gazprom
Lorenz
Prestige
Ragnarlocker
Rorschach
Vice Society
Dharma

Source: Microsoft Incident Response

**Human-operated ransomware variants that achieved breaches**

Ransomware accounted for 31 percent of all Microsoft Incident Response customer engagements. Looking at successful breaches among our incident response findings, four human-operated ransomware variants accounted for more than half of all breaches, with Lockbit being the most observed.

https://t.me/learningnets

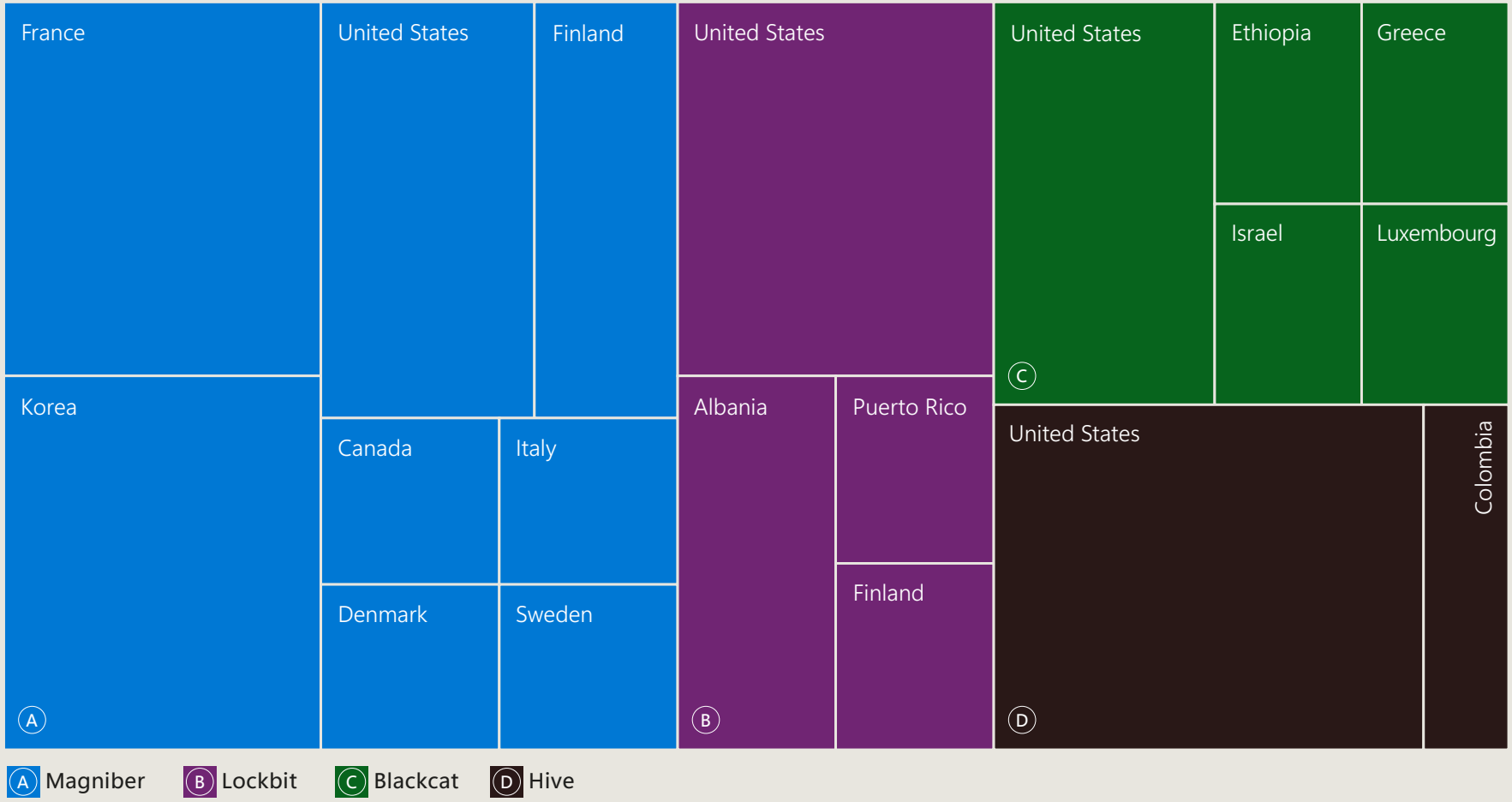
**Ransomware variants** continued

### Regional footprints

The geographical distribution of the Microsoft Defender Experts notifications reveals that the top ransomware variants had varying regional footprints. This reflects the targeted nature of attacks by their operators.

**Countries targeted by the top four ransomware variants**

The regional presence of ransomware was an indication of targeted attack and encryption by the threat actors.




Source: Microsoft Defender Experts notifications

https://t.me/learningnets

# How cybercriminals are using remote monitoring and management tools

Attackers continue to abuse legitimate remote monitoring and management (RMM) software for post-compromise activity such as information-stealing and delivering malicious payloads like ransomware. Microsoft incident responders found that 17 percent of intrusions involved known RMM tools.

**17%**

of intrusions involved known RMM tools.

In addition to providing attackers with persistent access to compromised systems, RMM software allows significant permissions that enable attackers to launch PowerShell commands or run scripts with system-level privileges. Threat actors can also abuse RMM software to copy files to a clipboard and exfiltrate data using a file transfer web service.

Because managed service providers, IT support, and system administrators use RMM software for legitimate purposes, it is often permitted by application controls. This makes automated detection of its use in an attack difficult. Its presence often blends in with common activity, buying the attacker time and complicating incident response as defenders may overlook the software. Organizations that do not use RMM software can defend against its abuse during an attack by using application control policies or perimeter network blocking rules.

**Actionable insight**

1. If your organization does not use RMM software, you can protect against its abuse during an attack by implementing application control policies or perimeter network blocking rules.

# Spotlight on cryptojacking

Cryptojacking is the unauthorized use of other people's devices to mine cryptocurrency. It generally does not trigger an incident response; rather, the criminal activity is often detected while investigating a separate incident. We observed evidence of current or past coin mining activity in 4.2 percent of all our engagements during the year. In these incidents, responders identified the presence of XMRig mining malware or the creation of virtual machines within a customer's subscription for coin mining.

Cryptojacking slows down an infected device, uses its resources, can steal information, and decreases overall performance.

Microsoft Defender Experts has identified the following Linux hosted application vulnerabilities being exploited for cryptojacking:

**Additional information**

Cryptojacking: Understanding and defending against cloud compute resource abuse | Microsoft

| Applications exploited by cryptojacking gangs | Publicly disclosed security flaws in the list of Common Vulnerabilities and Exposures (CVEs) |
|---|---|
| Teclib GLPI | CVE-2022-35914 |
| PACS (picture archiving and communication system) | Not applicable |
| Apache NiFi | Not applicable |
| Liferay portal | CVE-2020-7961 |
| Oracle WebLogic | CVE-2020-14750<br>CVE-2020-14882<br>CVE-2020-14883 |
| Confluence | CVE-2022-26134 |
| WSO2 | CVE-2022-29464 |
| GeoServer | Not applicable |

https://t.me/learningnets

# Insights on data exfiltration

Data exfiltration involves the unauthorized removal or movement of data from a device. Since November 2022, we have observed a doubling of potential data exfiltration instances after threat actors compromised an environment. This growth is consistent with the rise in double and triple extortion activity after ransomware attacks that we and the broader security community have observed in the past several years.

Not all data theft is associated with ransomware; it can also be part of credential harvesting or nation-state espionage. Stopping data exfiltration therefore requires a broader approach than focusing solely on preventing ransomware payload deployment and backup deletion.

### Infostealers

Information stealers (infostealers) are malicious software designed to steal data stored in browsers. Such data includes session tokens and cookies which can include multifactor authentication (MFA) claims, saved passwords and input form data, credit card information, user files, and cryptocurrency wallets. They can also harvest credentials for internet-facing systems and applications including VPN, RDP, virtual desktop infrastructure including Citrix, and identity providers such as Azure Active Directory and Okta.

In some instances, infostealers act as loaders for other malware.

As infostealers have become more prevalent in the last two years, they have increased as a risk to enterprise security. For example, an unmanaged device might lead to corporate compromise after an employee syncs their workplace credentials with infected home devices from browsers that are signed in.

Infostealers are advertised as a malware-as-a-service offering. The infostealer ecosystem is a multi-tiered business model usually involving three or four entities:

- The developer/operator develops the malware, operates its infrastructure, and sells the malware build to multiple distributors.
- The distributor uses the build to create infostealer payloads, deploys the infostealer in phishing or malvertising campaigns, downloads the infostealer output from the operator's centralized infrastructure, and is responsible for getting customers and developing a monetization strategy, which usually includes posting the output onto online credential marketplaces.
- The credential marketplace advertises stolen credentials for purchase. These online forums include Russian Market, Genesis Market, and Industrial Spy Market.
- The customer purchases infostealer output from the distributor or credential marketplace.

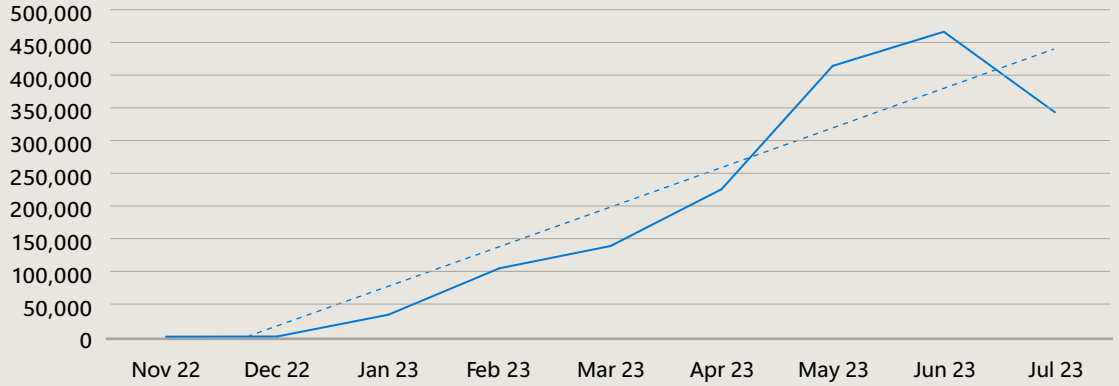
The infostealer ecosystem has enabled a new group of threat actors that leverage these tools to exfiltrate data and destroy resources. Such threat actors include Karakurt, the now-inactive Strawberry Tempest (DEV-0537, formerly LAPSUS$), Storm-0875 (0ktapus), Storm-0829 (Nwgen Team), Storm-0744, and Storm-0971.

### Data extortion

Ransomware operators have multiple opportunities to monetize their attacks, all of which are linked to data–encrypting, deleting, or publishing it. Because of the sensitivity of many organizations' data, some threat actors have turned to exfiltrating data for ransom without ever deploying an actual ransomware payload. Microsoft has observed that while approximately 16 percent of recent successful human-operated ransomware attacks involved both encryption and exfiltration, 13 percent used exfiltration only.

To exfiltrate data, attackers often leverage open-source data management and synchronization tools such as Rclone and MEGAsync. These tools are freely available for legitimate purposes and allow large volumes of data to be uploaded to remote cloud resources. Given that many RaaS programs include a suite of data extortion support offerings—including leak site hosting, payment pressure, and cryptocurrency transaction services—it is easier than ever for cybercriminals to monetize data exfiltration.

**Instances of potential exfiltration**




Sources: Microsoft Defender for Endpoint, Microsoft Purview Data Loss Prevention, Microsoft Defender for Office 365, Microsoft Defender for Cloud, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft 365 Defender, App Governance in Microsoft Defender for Cloud Apps, Microsoft Sentinel, Azure Active Directory Identity Protection.

https://t.me/learningnets

# Disrupting the financial networks of cybercriminals: a hypothetical case study

One of the best ways to deter cybercriminals is to hit them where it hurts: in their wallets. The Microsoft Digital Crimes Unit (DCU) has been doing that through a holistic strategy which places financial disruption at the core of its investigations.

Going after the financial networks of cybercriminals means leveraging advanced analytics and tools to identify bad actor assets, working with public and private sector partners, and scaling the use of traditional and new legal approaches to disrupt the financial flows of the cybercrime ecosystem. Here's what that might look like:

Microsoft identifies a suspected ransomware attack and proactively contacts the impacted customer. The customer confirms its files were encrypted and that it received a ransom demand to be paid to a cryptocurrency wallet. Microsoft works with the victim on incident response while the DCU analyzes the attacker and their virtual wallet. Using tools provided by industry partners who specialize in analyzing cryptocurrency transactions, the DCU identifies more of the threat actor's wallets and technical details of their communications.

With the victim's permission, Microsoft uses its membership in the National Cyber Forensics and Training Alliance (NCFTA)—a non-profit organization that unites industry and government partners to combat cybercrime—to share this information quickly and securely. The group confirms the actor is a known ransomware group and provides details including other wallets and infrastructure the cybercriminals use.

Op Pa Cybersecurity Tech Accord principles mapping index on **page 124**

Against the recommendation of law enforcement, the victim may determine that they must pay the ransom because of the critical nature of the encrypted data and their lack of back-ups. Based on the work of the DCU and its NCFTA partners however, the company decides to coordinate payment with law enforcement. After the victim pays, law enforcement tracks the funds and works with cryptocurrency exchanges to freeze the cryptocurrency before the ransomware group can withdraw it.

Law enforcement then returns the money to the victim through the appropriate legal process. Additional investigations may lead to the arrest and prosecution of the criminals.

Given the complexity and global nature of ransomware attacks and other cybercrime activity, this collaborative approach is necessary to disrupt the finances of criminals, at scale. Microsoft and the DCU are leading efforts with partners and will continue to develop technology and legal approaches to bring threat actors to justice.

Microsoft Digital Crimes Unit

https://t.me/learningnets

# Collaboration to disrupt the ransomware business model

One recommendation of the Ransomware Task Force (RTF), of which Microsoft is a part, is to disrupt the ransomware business model and decrease criminal profits. In pursuit of this goal, the Institute of Security and Technology (IST) mapped the ransomware payment ecosystem in 2022.

**Additional information**

Mapping the Ransomware Ecosystem | Institute for Security and Technology

The Ransomware Task Force (RTF) unites key stakeholders across industry, government, and civil society

This groundbreaking identification of the actors, processes, and information involved in the ransomware payment ecosystem illuminates how the ransom payment moves from the victim to the ransomware actor to be obfuscated, cashed out, and reinvested.

The laundering process spans cryptocurrency companies, virtual asset service providers (VASPs), peer-to-peer and cryptocurrency exchanges, mixers, merchant services, and dark net markets, among other entities. IST found that previously un-leveraged information is produced as a ransom payment moves through the chain. This information can be accessed and potentially shared by a range of entities including, but not limited to, antivirus vendors, cloud service providers, hosting providers, cryptocurrency exchanges, and tooling providers. Efforts coordinated by the RTF and NCFTA, among others, can also use this information to add friction to–and potentially disrupt–the ransomware payment ecosystem. The ultimate goal is to disincentivize the use of ransomware by making it harder for ransomware operators to successfully collect on their attacks.

# Defending against future ransomware trends

As of May 2023, 92 percent of the RTF recommendations for combatting ransomware had been actioned in some way, with 50 percent experiencing significant progress, including through legislation and policy adoption.[1] Just as defenders are innovating, however, ransomware operators are too. As a result, Microsoft is focused on understanding how ransomware activity may develop over the next few years to proactively counter it. Going forward, we expect cyber criminals will seek to leverage automation, AI, and hyperscale cloud systems to scale and to maximize the profitability of ransomware attacks. Organizations looking to minimize their vulnerabilities to these approaches must respond by modernizing their organizational skills, mindset, approach, and technology.

**Actionable insights**

1. Modernize cybersecurity skills: Use AI to augment human cyber defense skills and capabilities for organizations and for collective defense. AI can also be used to expedite the time to detect and respond to ransomware attacks.
2. Modernize mindset: Organizations should understand the benefits of innovations in the public cloud, which includes hyper-scalability cybersecurity capabilities, to protect digital platforms from cybercriminals and nation-state attackers.
3. Modernize approach: Cybersecurity can no longer be seen as a technical problem; for greater resilience it must be seen as an organizational risk by leaders in the organization and managed accordingly.
4. Modernize approach: Legacy technology and siloed standalone security products are not efficient or effective at defending against sophisticated cyber attackers. Organizations should invest in integrated cybersecurity platforms that share signals across the digital backbone to provide end-to-end visibility and inform defenders across an organization's surface attack area.

https://t.me/learningnets

# What is the Optimal Ransomware Resiliency State?

Microsoft's mission to keep ourselves and our customers safe from ransomware continually evolves and grows. A resilient defense is particularly important as ransomware operators increasingly shift toward hands-on-keyboard attacks that enable sophisticated cybercriminals to seek out and exploit vulnerabilities.

Op Cybersecurity Tech Accord principles mapping index on **page 124**

Despite developments in the ransomware space, the overall approach of our Ransomware Elimination Program remains the same: to deter or counter ransomware attacks by removing opportunities for financial gain by threat actors.

In last year's report, we introduced our two-pillar approach to ransomware, with dedicated initiatives to support our enterprise and our customers. This year, our efforts resulted in three key outcomes:

- **Continuous improvement for business continuity and recovery**: We emphasized the role of employees in our defense strategy through tabletop exercises and rigorous simulations to verify our protective capabilities, supported by training for excellence in incident response preparedness.
- **Advanced evaluation of ransomware-specific controls**: Integrating new methodologies, we developed a ransomware-specific technology evaluation program to ensure controls meet the requirements of our enterprise.
- **Improved feedback loops**: We streamlined engagement between our security operating center and the product groups that build the security tools that Microsoft and its customers rely on. This provided richer insights with more actionable data and improved our ransomware protection and detection capabilities in the products and services we used.

Over the coming year, we will continue to iterate and develop our processes to further reduce the risk of ransomware impact on our environment.

### How we can build resilience against ransomware

Our approach aims to ensure that our internal products, services, and teams—including those supporting our customers—will be best positioned to defend against ransomware attacks today and in the future.

To optimize resilience, we conducted an internal assessment using the National Institute of Standards and Technology's published framework for managing the risk of ransomware (NIST.IR.8374). Based on the results, and in conjunction with data and observations of real-world human-operated ransomware, we have established a comprehensive set of requirements across different technology domains to defend against ransomware attacks. We call this our Optimal Ransomware Resiliency State (ORRS).

Integrating what we have learned from our Zero Trust journey, ORRS consists of 40+ requirements that span myriad aspects of the security landscape, from policy and governance to infrastructure and data. The requirements are platform agnostic to ensure compatibility with any device that we mandate and include employee training, and ensuring business continuity and data accessibility.

Pr Op Em Cybersecurity Tech Accord principles mapping index on **page 124**

We believe that ransomware resiliency should be available to all organizations, regardless of size or industry. Over the coming months, we're focused on the implementation experience of ORRS with new, streamlined requirements that ensure resiliency and performance are not compromised.

### The five foundations of the ransomware elimination journey

We have identified five foundational principles which we believe every enterprise should implement to defend against ransomware. When fully implemented, the Foundational Five provide proven defenses across identity, data, and endpoints. While we make exclusive use of our first-party products, the Foundational Five are solution-agnostic if they are properly implemented and fully enabled.

### The Foundational Five

1. Modern authentication with phish-resistant credentials
2. Least Privileged Access applied to the entire technology stack
3. Threat- and risk-free environments
4. Posture management for compliance and the health of devices, services, and assets
5. Automatic cloud backup and file-syncing for user and business-critical data

Pr Em Cybersecurity Tech Accord principles mapping index on **page 124**

https://t.me/learningnets

**What is the Optimal Ransomware Resiliency State?** continued

A threat- and risk-free environment is defined as an environment protected by proactive measures—through tools and technologies—to prevent ransomware. These include malware detection, endpoint detection and response, vulnerability management, security operations center enablement, the enforced blocking of unhealthy devices, and brute-force protection for operating systems.

**Links to further information:**

Building an anti-ransomware program | Microsoft

Why Microsoft uses a playbook to guard against ransomware | Microsoft

Microsoft Security Ransomware incident response playbook framework

### Actionable insights

1. Understand your security risk relative to the Foundational Five. Ensure all features are fully turned on and active since, when combined, these make for a strong defense network.
2. Prioritize protective controls while ensuring you have the detective capabilities ready to identify new threats and risks in your environment.
3. Test and verify the effectiveness of implementations for your business needs. You may find unexpected gaps in your ransomware armor that need addressing.
4. Continuously improve your process for responding to and recovering from attacks and for practicing incident response readiness. Tabletop exercises and cross-company involvement are particularly useful.
5. If you do not already have one, consider building an incident response plan that covers specific ransomware scenarios for all major areas to ensure business continuity.
6. Consider using the hyperscale cloud as a venue where these principles are accessible quickly with low cost and low complexity.

https://t.me/learningnets



# A call to action

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

1. Focus on user identity, device health, and access control to prevent lateral movement and privilege escalation in the network.
2. Implement a Zero Trust approach to reduce the attack surface and improve resilience against cyber threats. By adopting this model, organizations can increase the cost to attackers and limit the impact of successful intrusions, thus reducing the blast radius.
3. Keep cybersecurity fundamentals up to date and leverage cloud-based tools for faster threat detection and response.
4. Establish a ransomware defense strategy to mitigate the impact of extortion attacks that are becoming more frequent and damaging. Implementing a plan should be a priority especially because of the near certainty that an organization will experience at least one attack in the next few years.

**Additional information**

Advancing Modern Strong Authentication | Microsoft

How to configure for ransomware prevention in your organization | Microsoft

Stop attack progression with automatic disruption of ransomware and BEC attacks | Microsoft

# Insights on phishing

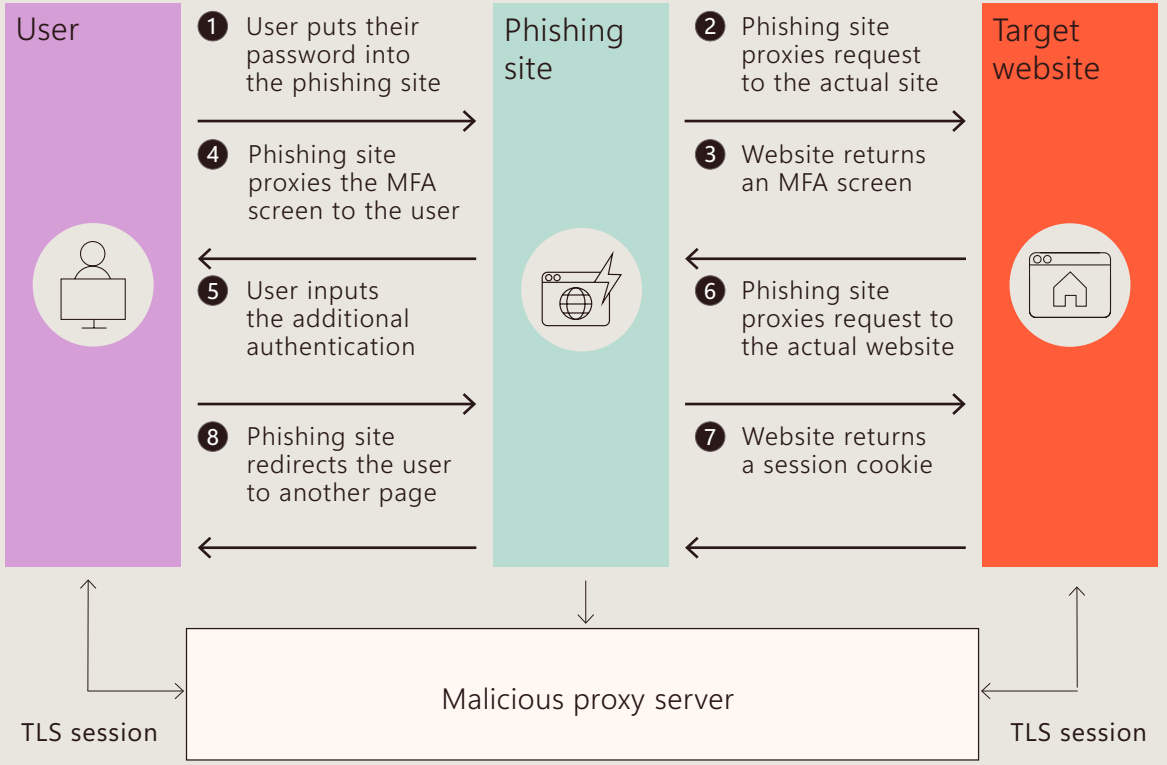
## Adversary-in-the-middle phishing attacks

Adversary-in-the-middle (AiTM) is a longstanding technique used by threat actors to obtain credentials, session cookies or personal data, or to distribute malware.

We have consistently observed a daily influx of high-volume AiTM phishing campaigns, with some instances involving millions of phishing emails sent within a 24-hour period. This trend of high-volume campaigns first appeared in September 2021 and we saw a significant surge in mid-July 2022, indicating an effort to bypass MFA on a massive scale. Unlike traditional phishing attacks, revoking and resetting user account credentials is not enough to address AiTM phishing incidents. The stolen session cookies also need to be revoked because session cookies, which are data stored in browsers, grant privileged access without repeated authentication.

During an AiTM phishing attack, a reverse proxy server is set up between the target and a legitimate login page. Reverse proxy servers sit between a client, such as a web browser, and a web server, forwarding information and requests between the client and the server. Reverse proxies are used legitimately for increasing security and performance but can also be used for malicious purposes such as AiTM attacks. The target unwittingly submits their credentials through the proxy, which triggers an MFA prompt on their mobile device. After the user inputs the authentication code, the proxy continues to deceive them by presenting subsequent MFA screens, relaying the user's input and allowing the attacker to access the account without the user's knowledge.

Anatomy of an AiTM phishing attack




https://t.me/learningnets

**Adversary-in-the-middle phishing attacks** continued

In AiTM, the target is presented a replica or imitation login page, as in traditional phishing methods. However, a separate server controlled by the threat actor or phishing service is used to submit the stolen credentials to the legitimate login service, triggering an MFA prompt. The phishing infrastructure then displays a copy of an MFA screen to the target. This is distinct from AiTM over reverse proxy, as no HTTP packets are proxied between the target and the login service.

Microsoft tracks multiple threat actor groups associated with prominent AiTM phishing kits and services and one prolific threat actor using multiple AiTM phishing services to carry out high volume phishing campaigns. These prominent kits/services are known as Caffeine (attributed to Storm-0867), EvilProxy (attributed to Storm-0835), and NakedPages (attributed to Storm-1101). We have also observed AiTM phishing campaigns linked to tracked but unidentified kits or services.

$200-$1000

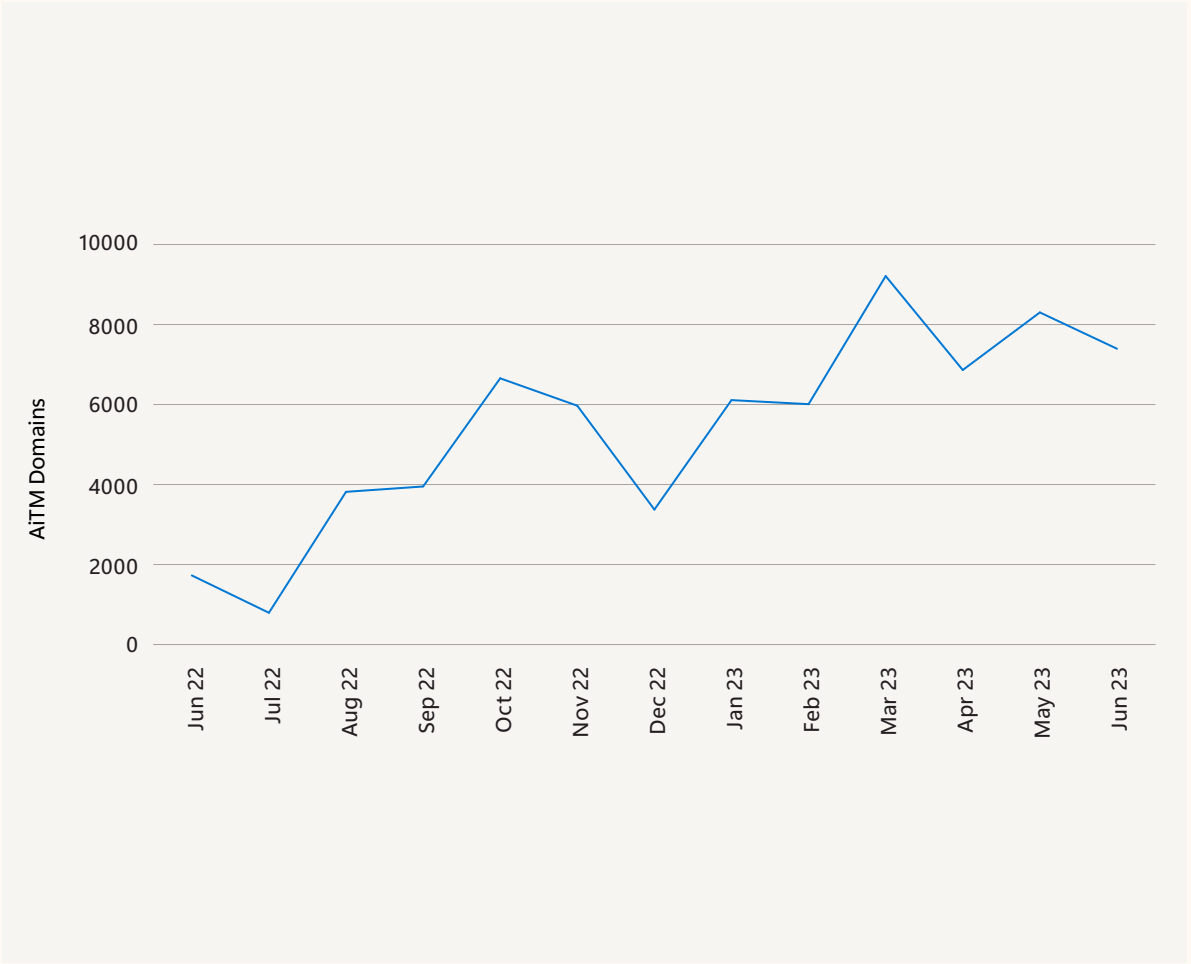
Monthly licensing fees paid by cybercriminals to carry out daily phishing campaigns.

While other kits–such as Evilginx2, Modlishka, and Muraena–have been available for free in open sources for years, they lack the service and support offered by paid-for kits. As a result, the addition of AiTM phish kits to phishing-as-a-service has supplied advanced phishing capabilities to a wider range of threat actors, reduced entry barriers, and enabled more effective attacks.

Caffeine, EvilProxy, and NakedPages each have hundreds of customers. These cyber criminals pay monthly license fees ranging from $200 to $1,000 USD and carry out daily phishing campaigns. Because so many threat actors use these services, it is impractical to attribute campaigns to specific actors. Instead, we track these phishing services, block phishing activity from them, and work to provide effective detection and defense for customers.

**AiTM domains growing as attacks become more common**

The number of domains that we tracked leading to AiTM phishing pages grew consistently throughout the last 12 months




Source: Microsoft Defender for Office 365

https://t.me/learningnets

# Evolving phish techniques

Phishing campaigns continue to improve in sophistication, including leveraging genuine services or websites and tailoring phishing links for individual users. By simulating user interaction in virtual machines, we can analyze untrusted files and URLs to assess their safety. The main goal is to deliver speedy and accurate verdicts on content.

Examples of what we're seeing in real-time analysis:

- **Emails sent from trusted third parties.** Attackers send phishing emails to all the contacts of their victims and then respond on the email thread with specially crafted messages and a malicious URL.
- **Emails with legitimate URLs.** Attackers host phishing URLs on legitimate cloud service providers such as Adobe, Dropbox, Google, and Microsoft. After multiple redirects, victims are led to the final landing page, which steals credentials or downloads malicious payloads onto their machine. Given these are popular services, it is difficult to distinguish malicious links from genuine ones.
- **OneNote malware.** Attackers abuse OneNote to execute malicious software. Phishing campaigns observed by Microsoft Defender Experts include OneNote attachments, URLs leading users to download OneNote attachments, and PDFs containing URLs that led to OneNote malware downloading.
- **OAuth device code phishing.** The attacker generates a user code, then creates a phishing email with it and a link to provide the code. This allows the attacker to sign-in on behalf of the user.
- **Other targeted phishing attempts.** Our experts also observed targeted phishing attempts in which attackers identified user-specific details through social engineering, then created tailored phishing campaigns using look-alike domains to which the users have subscribed, with contents matching the users' interests. This significantly increases the success rate of a compromise attempt.

**10,000**

In April-June 2023 we alerted users of approximately 10,000 password entries per month into malicious sites.

Source: Enhanced Phishing Protection with Microsoft Defender SmartScreen, across third-party browsers running on Windows 11

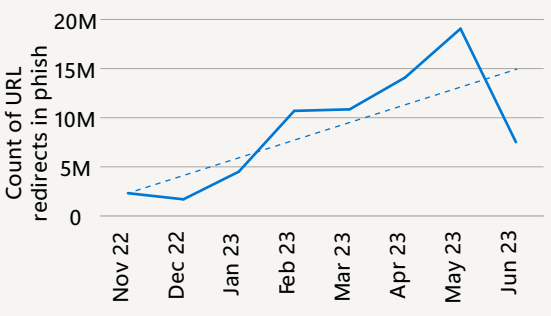
# Trends in file entities used in phish

Using data from Microsoft Defender for Office 365, we observe trends in file entities that are commonly used in phishing attacks. HTML files are often used for creating fake web pages that trick users into divulging personal information. PDF files can exploit a user's trust by embedding malicious links or using social engineering tactics to persuade users to open attachments that execute malware. URLs are commonly used to deceive users into visiting fraudulent websites.

This year, we observed major attack patterns involving URLs with open redirectors and open shorteners being dominant attack vectors.

URL open redirectors are vulnerabilities found in web applications that enable attackers to manipulate URLs to redirect unsuspecting users to malicious websites. Here, they may be victim to phishing attacks, data breaches, account takeovers, or malware infections.

### URL redirect abuse on the rise

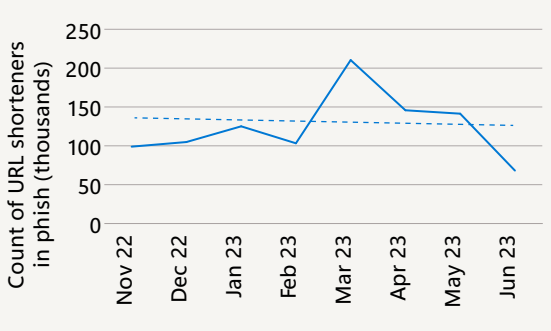



Source: Microsoft Defender for Office 365

Malicious actors can use URL shorteners in tandem with URL redirectors to send users to harmful websites or deceptive phishing pages.

Use of URL shorteners spiked in March, but remained constant overall.

### Prevalence of URL shorteners




Source: Microsoft Defender for Office 365

https://t.me/learningnets

# Analyzing click behavior in phishing simulations

Phishing campaigns continue to improve in sophistication, including leveraging genuine services or websites and tailoring phishing links for individual users. By simulating user interaction in virtual machines, we can analyze untrusted files and URLs to assess their safety. The main goal is to deliver speedy and accurate verdicts on content.

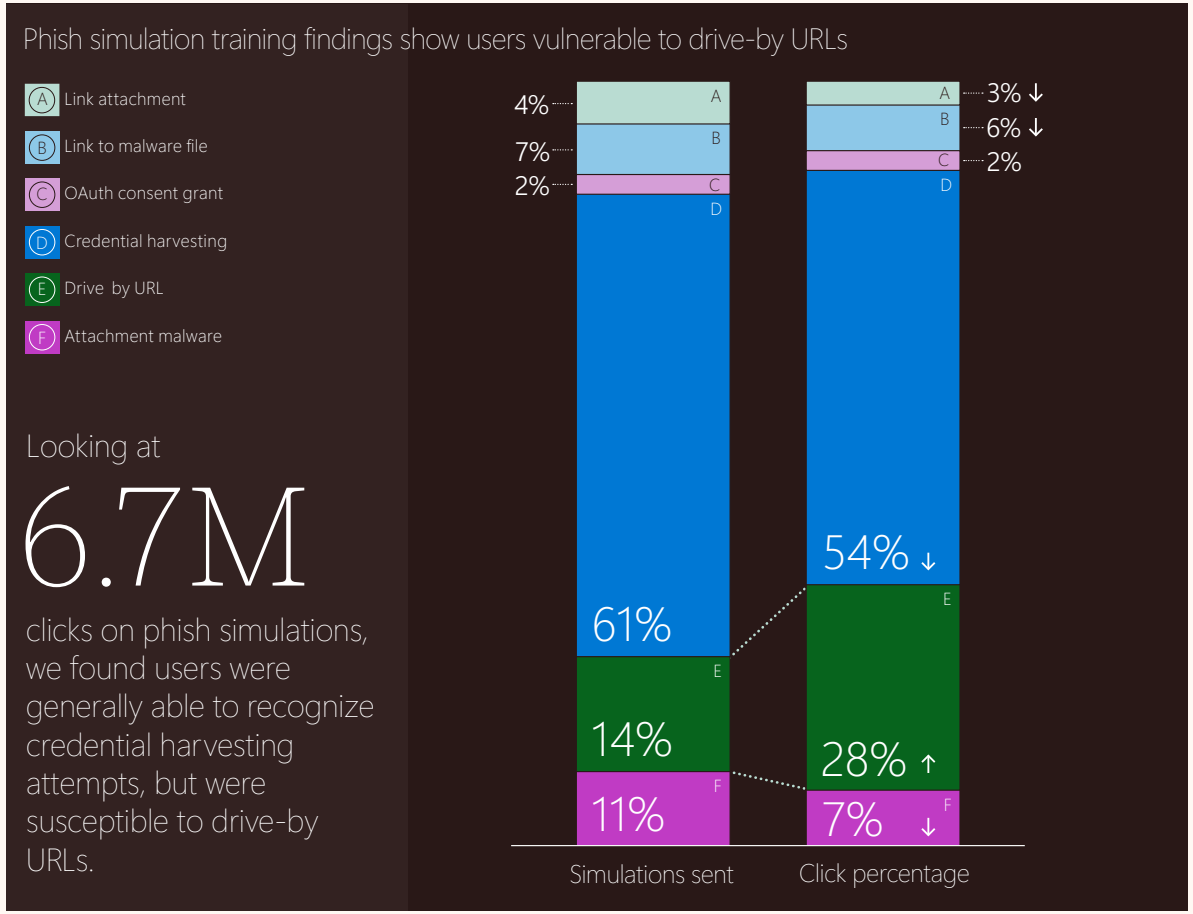
The fundamentals of phishing haven't changed over time; approximately 90 percent of phishing attacks involve social engineering. This is primarily conducted through email that leads the victim to reveal sensitive information, click a malicious link, or open a malicious file. Phishing attacks are cost-effective for attackers, adaptable to evade prevention measures, and boast high success rates. Compromise rates range from single digits to 40 percent, influenced by a wide range of variables from simulation difficulty to user type. We evaluated attack simulation training data from tens of millions of users to gain insights into the impact of phishing training.

### Why is phishing such a challenge?

Humans remain the primary risk vector in social engineering attacks. At the same time, phishing attack mechanisms are constantly evolving, and bad actors create new tactics. Users often click on links and attachments by habit and without conscious consideration of their actions, thereby opening the door to cybercrime. Three factors explain why users remain a key vulnerability:

1. As threat tactics rapidly evolve, technical systems will not be able to completely prevent social engineering attacks and human behavior will persist as a vulnerability for attackers to manipulate.
2. While security awareness programs, designed to help users identify social engineering attacks and respond appropriately have some success, often it is not the user's lack of knowledge that drives phishing susceptibility.
3. So far, users have not demonstrated the ability to consistently change their behavioral risk tendencies enough to show measurable improvement against an ever-evolving threat landscape.

Users are particularly vulnerable to drive-by URL attacks. These involve simple link-clicks that take victims to websites that collect telemetry or entice the user to a downstream attack. Whereas a credential harvest attack involves two clicks—one to get to the credential harvesting page and another to enter the credentials—a drive-by requires just one click. Drive-by URL attacks are usually less impactful, but many organizations use them to measure their click susceptibility.




Source: Microsoft Defender for Office 365, attack simulation training data

https://t.me/learningnets

### How video-based trainings alone fall short

Most enterprise phishing awareness programs prioritize meeting training compliance requirements over delivering effective behavior change programs. They operate under the misguided assumption that periodic exposure to simulated phishing attacks, accompanied by a brief educational encounter (typically in the form of a narrated video with limited interactive elements), will equip users to be able to identify and avoid advanced and evolving phishing attempts. However, these programs have proven to be fundamentally flawed.

Although tens of millions of computer users have taken phishing training, we have found that phish clicking behavior is reduced by employing video-based training by about three percent, at best. This number has remained remarkably stable over the years. Based on this data, we conclude that video-based training is not an effective way to reduce an organization's phish susceptibility.

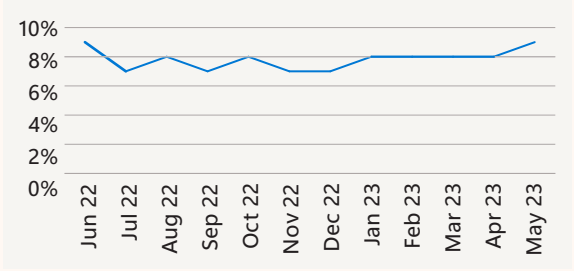
### Tailored approaches are needed

The security awareness and training industry is beginning to adopt objective behavioral measures and contextual experiences that prioritize behavior change over information delivery. This involves tailoring the approach to individual users. We believe this approach holds the greatest potential for reducing behavioral risk against modern social engineering attacks. Under this approach, organizations must embrace a new perspective regarding the involvement of their users in thwarting attacks and conduct innovative experimentation with user engagement strategies.

To truly tackle the issue of phishing, it's important to recognize that every user is unique and has their own behavioral tendencies. Our phishing awareness programs go beyond generic, one-size-fits-all training and instead provide tailored and context-aware engagement models that can be implemented at scale. We understand that each user requires a personalized learning experience based on their unique behaviors and profile, such as job function, security posture, and past actions. For example, our phish simulations are tailored to each user's performance based on telemetry from previous simulations sent. Providing personalized learning experiences based on each individual's unique behaviors and profile can enable organizations to make a real impact in reducing phish susceptibility.

### Percentage of clicks on phish simulations

Link-clicking behavior by users has remained relatively unchanged despite the widespread implementation of security awareness training programs, and increased sophistication of phish.



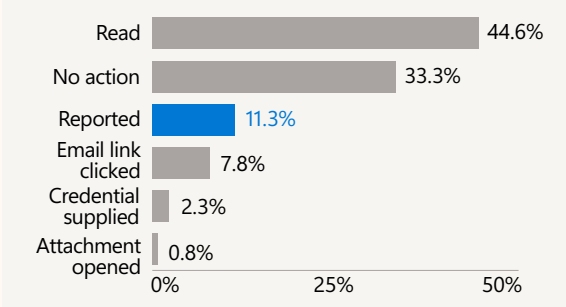

Source: Microsoft Defender for Office 365 attack simulation training data

### Inaction is better than clicking, but reporting is the best action to take.

Reporting phishing attempts is crucial to prevent cyberattacks. Users can help security teams identify and block malicious emails, websites, and other threats. However, only 11.3 percent of users who receive phishing emails report them, despite 89 percent refraining from clicking on links or opening attachments.

Administrators can use awareness campaigns, teaching guides, and rewards to raise awareness of phishing campaigns and encourage consistent reporting behavior. There is a genuine opportunity for organizations to prioritize enhancing user reporting consistency, as current rates fall short of potential.

### User responses to phish attempts still insufficient




**Over the past six months, we found users reported phishing attempts only 11.3% of the time. While no action is better than clicking, reporting phishing attempts would be best to help security teams identify incoming threats.**

Source: Microsoft Defender for Office 365 attack simulation training data

Employees must also know how to recognize and respond to evolving phishing techniques. Additionally, emphasis should be placed on strengthening organizational resiliency, such as through Zero Trust strategies which isolate and contain the potential impacts of phishing.

### Additional information

Attack Simulation Training: New insights into targeted user behavior

Simulate a phishing attack with Attack simulation training | Microsoft Learn

### Actionable insights

**To safeguard against these attacks:**

1. Shift phishing training programs away from being compliance oriented to more proactive, behavior change focused.
2. Develop tailored and context-aware education models that treat users as distinct individuals and can be implemented at scale.
3. Teach users that reporting is a gold standard behavior in protecting their enterprise.
4. Treat phishing education programs as part of a broader Zero Trust organizational resiliency strategy.

https://t.me/learningnets

# Insights on business email compromise

Business email compromise (BEC) is a sophisticated scam which targets businesses and individuals performing transfers of funds.

The scam is frequently carried out when a threat actor compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized funds transfers to accounts under their own control. The incidence of BEC attacks has skyrocketed, reaching an astonishing count of over 156,000 daily attempts between April 2022 to April 2023.[2]

In 2022, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center recorded adjusted losses of over USD 2.7 billion for 21,832 BEC complaints filed.[3]

## 156,000 daily

BEC attempts observed April 2022-April 2023

## Common BEC attack activity

**Financial fraud.** Microsoft Defender Experts have observed attackers creating domain impersonations to deceive users into thinking they are engaging with legitimate third parties for financial transactions. In some cases, attackers compromise the third party and respond on the same email thread to request money transfers. These attacks are challenging to detect as they originate from genuine third-party emails.

**Lateral movement through internal phishing.** After compromising identities with AiTM, many threat actors then launch internal phishing campaigns. Microsoft Defender Experts have witnessed large-scale internal phishing campaigns targeting over 8,000 recipients. Since these emails are internal and sent from legitimate senders, it increases the likelihood that users will be duped by the scam.

**Mass spam mailing activity.** This attack aims to disrupt users through a denial-of-service strategy. Attackers subscribe the victim user's email address to multiple lists, forums, message boards, and newsletters, resulting in the victim receiving an overwhelming number of emails, sometimes exceeding 1000 per minute. When this occurs, the victim is distracted and frustrated, often unable to notice legitimate warning or authentication messages in their overwhelmed inbox.

### How BEC is evolving

As Microsoft's cloud services continue to evolve through innovative breakthroughs, threat actors are adapting their social engineering techniques and use of technology to carry out more sophisticated and costly BEC attacks. The success of these attacks is largely due to the growing targeting of cloud-based infrastructure, exploitation of trusted business relationships, and development of more specialized skills by the threat actors. Microsoft's Digital Crimes Unit (DCU) believes that increased intelligence sharing across the public and private sectors will enable a faster and more impactful response against the threat actors behind these attacks.

### Expanded abuse of cloud-based infrastructure

The agility and power of cloud services that benefit customers have also been weaponized by cybercriminals. For instance, the DCU has observed threat actors abuse the portability of domain names and power of Microsoft 365 services (such as resiliency, orchestration, control, and scale) in multiple stages of BEC attacks, from reconnaissance to phishing to payment fraud. The use of impersonation domains, known as homoglyph domains, is also still prevalent. These allow BEC attackers to tailor email communication for social engineering. Homoglyph domains are often ported from third-party registrars and configured with M365 mail services to create mailboxes that impersonate legitimate key accounting employees.

https://t.me/learningnets

### Exploitation of trusted business relationships: Vendor email compromise

BEC attacks are evolving past simple email account compromise rooted in social engineering tactics that circumvent payment controls by exploiting supplier business relationships. A more successful type of attack is called Vendor Email Compromise (VEC). VEC occurs when a company's suppliers are targeted and exploited by threat actors who hijack email threads from the company's compromised email accounts and use them to change payment information for an upcoming transaction.

The hijacked email threads are often copied to attacker-managed mailboxes created with homoglyph domains and used in illicit communication.

### Threat actors are up-skilling

The structure of organized criminal networks perpetrating BEC attacks is also evolving, along with the skills of the threat actors who make up these organizations. BEC criminal networks predominantly originate from Africa and range from a hierarchical organization with top-down command, such as the Black Axe group,[4] to loosely organized networks managed regionally, commonly known as "zones." Many zone actors move to industrialized countries for technical education and work experience, then use their new knowledge to carry out more sophisticated attacks, such as VEC. DCU has observed some zones are organized by roles and use specialized skills to improve the efficacy of their attacks. In these instances, threat actors may be involved in one or more roles.

### Intelligence sharing builds resilience

Intelligence sharing improves our collective ability to identify and respond to BEC attacks, helping to increase resilience in the face of these threats. Mapping out malicious infrastructure and developing threat actor intelligence gives stakeholders a better understanding of the tools, techniques and procedures used by cybercriminals. This enables more holistic disruption of their supply chain and coordinated role structure. Threat intelligence also improves investigation prioritization and informs the targeting and disruption of the more advanced and prolific criminal networks.

**We are supporting the Cybercrime Atlas Initiative that brings together global leaders to fight cybercrime. For more about this initiative, please see page 111.**

### Other types of BEC attacks

- Direct Email Compromise (DEC)—compromised email accounts are used to socially engineer in-house or third-party accounting roles to wire funds to the attacker's bank account or change payment information for an existing account.
- Vendor Email Compromise (VEC)—social engineering of an existing supplier relationship by hijacking a payment-related email and impersonating company employees to convince a supplier to redirect outstanding payment to an illicit bank account.
- False Invoice Scam—a mass social engineering scam that exploits well-known business brands to convince companies to pay fake invoices.
- Attorney Impersonation—the exploitation of trusted relationships with large, well-known law firms to increase credibility with executives of small companies and start-ups to complete payment of outstanding invoices, particularly prior to significant events like initial public offerings. Payment redirection to an illicit bank account occurs once an agreement on payments terms is reached.

**Additional information**

Stop BEC attacks with XDR

### BEC threat actor roles

- Coordinator—responsible for selecting victims such as companies, suppliers and employees. The role includes building or procuring phishing capabilities to gain email access to understand payment procedures, copy invoices and hijack email threads.
- Email broker—responsible for carrying out phishing attacks to gain access to mailboxes for email collection and email forwarding rules and for covering the tracks of compromised activity.
- Infrastructure admin—responsible for procuring and configuring cloud services, managing domain names, creating mailboxes and managing licenses.
- Email operator—responsible for social engineering via email communication with the invoice fraud target, making language skills highly valued.
- Money launderer—individual or network of individuals with specialized skills or expertise in placing, moving and laundering funds. This role can include managing networks of money mules who establish fraudulent banking accounts that BEC actors use for payment fraud.

https://t.me/learningnets

# Insights on identity attacks

The first quarter of 2023 saw a dramatic surge in password-based attacks against cloud identities, especially in the education sector.

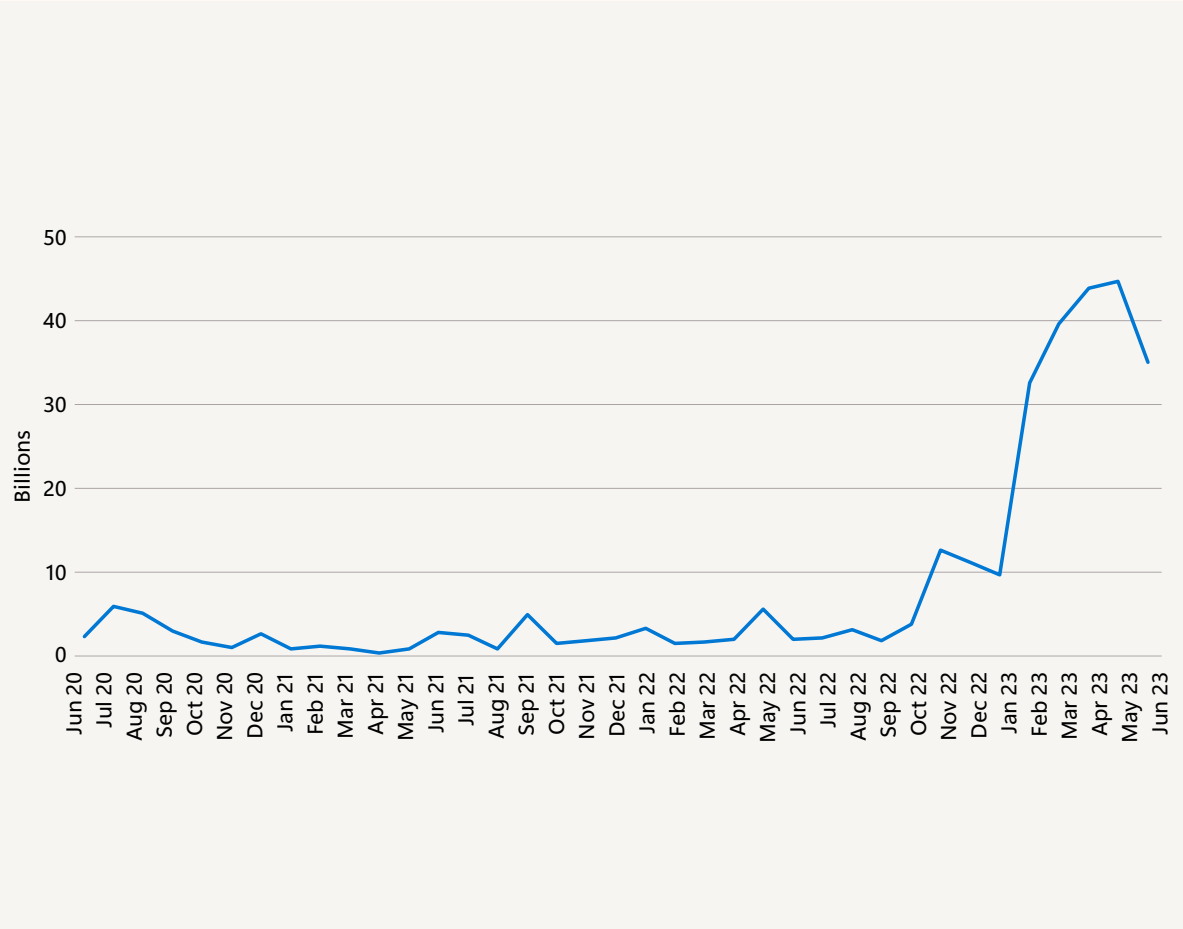
According to Microsoft Entra data, the number of attempted attacks increased more than tenfold compared to the same period in 2022, from around 3 billion per month to over 30 billion. This translates to an average of 4,000 password attacks per second targeting Microsoft cloud identities this year.

One of the main reasons password attacks are so prevalent is the low security posture of many organizations, especially in the education sector. Many of these organizations have not enabled MFA for their users, leaving them vulnerable to phishing, credential stuffing, and brute force attacks.

We blocked an average of 4,000 password attacks per second over the past year.

**Password based attacks spiked in 2023**

After a notable increase in the number of password-based attacks per month in October 2022, the number skyrocketed in 2023. In April, there were 11,000 attacks per second, a tenfold increase from the same time last year.




Source: Microsoft Entra data

https://t.me/learningnets

# Use of one-time password bots

MFA adds an extra layer of security, but cybercriminals can still find ways to bypass it. One way is by using one-time password bots (OTP bots) to gain access and perform account takeovers. OTP bots extract authentication codes from users by tricking them into providing the OTP sent to them via SMS, authentication apps, or email. The cybercriminal loads the victim's phone number into the OTP bot, which calls the victim and pretends to be a legitimate service provider. The bot tells the victim there has been suspicious activity on their account and asks them to enter the OTP for "security verification." The entered password is then sent back to the cybercriminal, granting them access to the victim's account.

While robocalls are a common method used by OTP bots, email phishing for authentication codes is also employed. The cybercriminal must act quickly once the victim enters their login credentials and OTP on the phishing web page due to the short lifespan of one-time authentication passwords.

# MFA fatigue is a threat

As MFA has gained increased importance, particularly in passwordless sign-in, attackers have adapted–trying to circumvent security protections by sending MFA or passwordless sign-in prompts to potential victims. The aim is to trick them into accidentally approving requests through what's called MFA fatigue, or MFA bombing. Once the victim does so, the attacker gains full access to customer's account and may modify the MFA settings, allowing them to sign in at any time.

Cybersecurity attacks targeting MFA authentication and passwordless sign-in are on the rise. Approximately 6,000 MFA fatigue attempts were observed per day by the end of June 2023. In response, we have developed and implemented protections against anomalous passwordless sign-in for all customers. We strongly advise customers to thoroughly review and validate MFA/passwordless sign-in prompts before approving them.

Approximately 6,000 MFA fatigue attempts were observed per day.

### Actionable insights

Despite these risks, MFA remains an effective security measure. Here are some guidelines to enhance your security while using MFA:

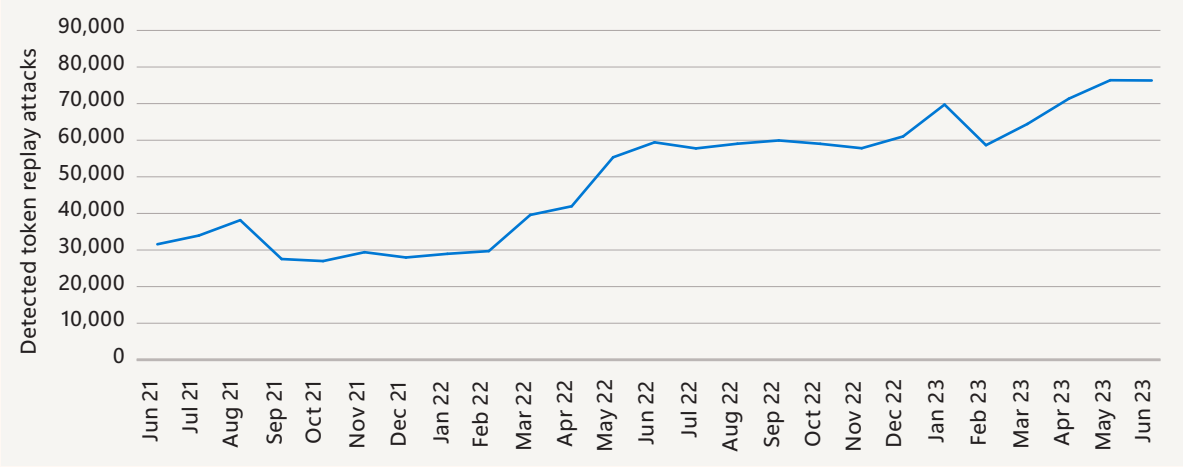
1. Use authenticator apps like Microsoft Authenticator instead of relying solely on text message codes.
2. Never share your security codes with anyone.
3. Create strong and unique passwords using password generators and use a password manager.
4. Avoid reusing passwords across multiple accounts.
5. Educate yourself and your employees about common social engineering tactics to recognize and avoid interactions with OTP bots.

https://t.me/learningnets

# Token replay remains a prevalent threat

With this technique, attackers use tokens that were originally issued to legitimate users to authenticate and authorize privileges. The attackers acquire the tokens through means such as malware, phishing, or MFA fatigue to launch additional attacks. The number of token replay attacks has doubled since last year, with an average of 11 detections per 100,000 active users in Azure Active Directory Identity Protection. Although token replay constitutes less than three percent of all identity compromises, the consistent year-on-year increase in detections indicates that cybercriminals continue to view it as an effective attack method.

**Token replay attacks consistently growing since early 2022**




Source: Azure Active Directory Identity Protection data

### Actionable insights

Relying on MFA alone does not effectively mitigate against this type of attack. We recommend the following:

1. Consider implementing risk-based and token protection policies in Conditional Access.
2. Monitor systems for signs of token replay.
3. Use non-phishable credentials which bind the token to the legitimate user's device, such as Windows Hello for Business and FIDO[5] keys.

### Additional information

What are risk detections in Azure Active Directory Identity Protection | Microsoft

# Developing immunity with phishing-resistant MFA credentials

To combat the increase in identity-based attacks targeting phishable MFA credentials, we are transitioning to use exclusively phishing-resistant credentials that are immune to various attacks. While technologies like Hello for Business and FIDO2 hardware security keys offer phishing resistance, their widespread deployment across complex environments presents challenges. Microsoft Entra ID's Conditional Access policies enforce the use of phishing-resistant credentials, including Hello for Business, FIDO2 hardware security keys, certificates, and Passkey. This is crucial for users in high-risk roles or with access to sensitive resources. This is a practical step that can increase defense against even "successful" phishing attacks.

### Additional information

Phishing-resistant authentication methods | Microsoft

Conditional Access authentication strength | Microsoft

https://t.me/learningnets

# The importance of MFA enablement on virtual private networks

For many years, VPNs have been used to enable secure remote access to company resources through encrypted tunnels. However, like any technology, ensuring compliance with an organization's security strategy requires proper configuration and alignment with a modern secure architecture, such as Zero Trust. Due to VPNs' widespread use in corporate networks and their accessibility from the internet, they have become common targets for attacks, often due to misconfigurations, such as insufficient monitoring of user accounts and devices. In a typical corporate setup, users are assigned separate VPN accounts with restricted access to the internal network.

Through our compromise recovery engagements, we found that almost half of VPN accounts lacked adequate MFA. Enabling MFA for these individual accounts is a crucial part of any VPN risk mitigation strategy. Other essential steps to secure these accounts include implementing conditional access, monitoring, and integrating security automation, if abuse of these accounts is detected.

Almost half of VPN accounts lacked adequate MFA.

In the month of June 2023 alone, we detected 158 million instances of password reuse across sites.

**Source: Enhanced Phishing Protection with Microsoft Defender SmartScreen**

**Actionable insights**

1. Use a unique password for each site.
2. Secure your devices and accounts with multifactor authentication.

**Additional information**

Create and use strong passwords | Microsoft

https://t.me/learningnets

# Insights on distributed denial of service attacks (DDoS)

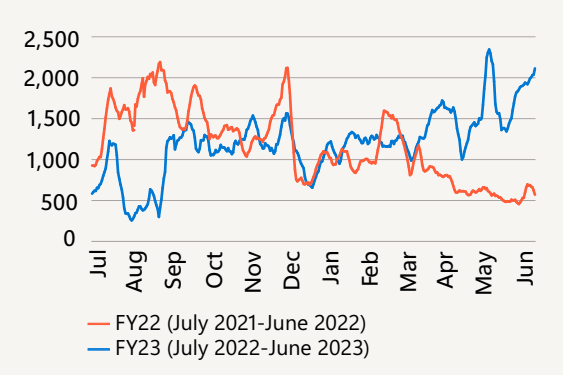
## Battling a growing threat

Not only are DDoS attacks continuing to grow, they may be poised to have an even greater impact in the future. Our global DDoS mitigation operations combatted an average of 1,700 DDoS attacks per day in the past year.

In the previous year, we amplified our globally distributed mitigation capacity to handle and neutralize DDoS attacks at rates of up to 90 Terabits of data per second (Tbps). To put this into perspective, some of the largest attacks covered by the press in last years were in the range of several Tbps.

With a mitigation scale of 90 Tbps, we can mitigate the largest recorded attacks known, as well as multiple such attacks in parallel, to protect our cloud platform, reinforcing our commitment to maintaining a secure environment for our customers.

**Comparison of DDoS attack patterns by average number of attacks**




Source: Microsoft Global DDoS Mitigation Operations

## DDoS for hire

DDoS-for-hire services—also known as booters, stressers, or ddosers–offer subscriptions to botnets for varying lengths of time, allowing users to flood target internet resources with large amounts of data.

This results in a denial of service. Since the attacks are launched from multiple networks, they are referred to as distributed denial of service attacks, or "DDoS". These services can be purchased for as little as $5 USD and are increasingly being used as a cyberweapon in human operated ransomware attacks to exploit vulnerabilities in internet resources.

These services pose a significant risk to cybersecurity, serving as a powerful tool for cybercriminals. In today's world, where we rely heavily on online services, DDoS attacks can render platforms such as business productivity and gaming inaccessible. Additionally, these attacks can be used in triple-extortion human operated ransomware attacks to force victims to make payments, potentially leading to the destruction of confidential and proprietary business data hosted on servers.

A notable achievement is the disruption by law enforcement of 48 DDoS-for-hire service platforms and legal action against six individuals involved.[6] Such intervention plays a vital role in mitigating the impact of DDoS attacks by targeting the infrastructure and individuals supporting these illicit services.

The magnitude of the struggle is reflected in the fact that despite these achievements, the number of DDoS-for-hire platforms continues to rise, with 20 percent having emerged in the past year alone. This alarming trend emphasizes the necessity for continuous monitoring, tracking, and decisive action against these platforms. The DCU has taken a proactive stance by actively tracking and monitoring 14 DDoS-for-hire sites, including one situated in the dark web, as part of its commitment to identifying potential threats and remaining ahead of cybercriminals.

The number of DDoS-for-hire platforms continues to rise, with 20 percent having emerged in the past year alone.

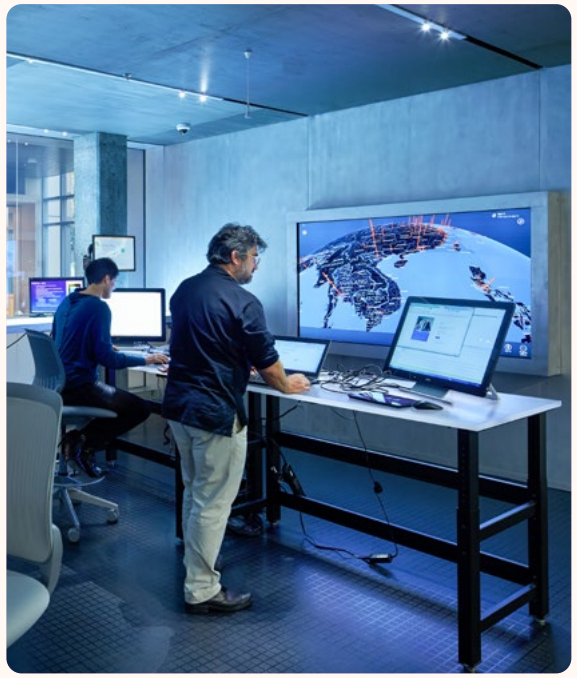
https://t.me/learningnets

# A new era of cyberattacks: the rise of the botnets at scale

Last year marked a significant shift in cybercriminal tactics, with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks.

To minimize costs, they targeted discounted Azure subscriptions across various regions, establishing and commandeering subscription accounts at every opportunity. From January 2023 onwards, we noted that compromised subscriptions were generating resources in up to 40 Azure regions monthly, demonstrating the global reach for malicious botnets holding potential for targeting assets and organizations. Among these, the US regions were the most exploited, constituting around 70 percent of the falsely spawned resources, while Europe followed at 15 percent.

As the size of DDoS attacks increases, more and more cloud computing power is needed to absorb the leading wave of the attack until patterns can be identified, spurious traffic diverted, and legitimate traffic preserved. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks. In addition, due to the global distribution of the cloud, closer proximity helps to block attacks closest to the sources.



Microsoft Digital Crimes Unit

# The healthcare sector as a target

This year, we observed an increase in daily DDoS attacks on the healthcare sector, particularly starting in January 2023. While the overall attack throughput is not very high, at around 100,000 packets per second 99 percent of the time, there was a significant spike of 14 million packets per second at its peak, with the attack intensity reaching a peak of almost 100 attacks per day in June. KillNet, a group that the US Department of Health and Human Services has assessed to be pro-Russia hacktivists, has been launching waves of DDoS attacks against western countries, including with a focus on the healthcare sector.

The US Cybersecurity and Infrastructure Security Agency has collaborated with the FBI to develop guidance for DDoS response strategies to guide government agencies in protecting themselves against DDoS attacks.

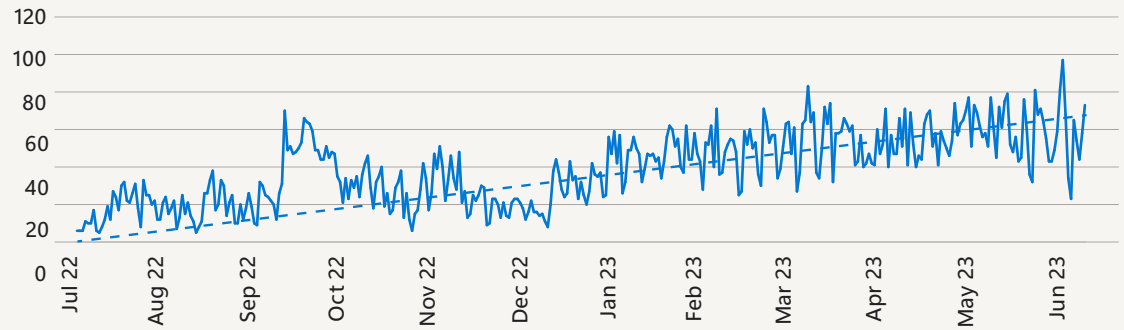
**Additional information**

KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks | Microsoft

Understanding and responding to distributed denial of service attacks | CISA

HC3 provides tips for maintaining IoT security in healthcare | Health IT Security

**Daily DDoS attack volumes on healthcare applications**




Source: Microsoft Global DDoS Mitigation Operations tracking healthcare applications in Azure

https://t.me/learningnets

# TCP attacks as the preferred vector

Transmission Control Protocol (TCP) has become the dominant attack vector, encompassing 59 percent of all DDoS attacks.

This shift toward TCP stems from the escalated activities of some hacktivist groups, who are increasingly turning their sights on web applications, bolstered by the rising adoption of DDoS-for-hire tools. In comparison, last year User Datagram Protocol (UDP) amplification and UDP flood attacks occupied most of the attack spectrum, comprising 51 percent of attacks while TCP was only 45 percent.

The predominance of UDP-led attacks in previous years, particularly targeting gaming applications, can be linked to the ripple effects of the COVID-19 pandemic. The enforced quarantines and lockdowns led to a surge in gaming's popularity, rendering these services a lucrative target for attackers.

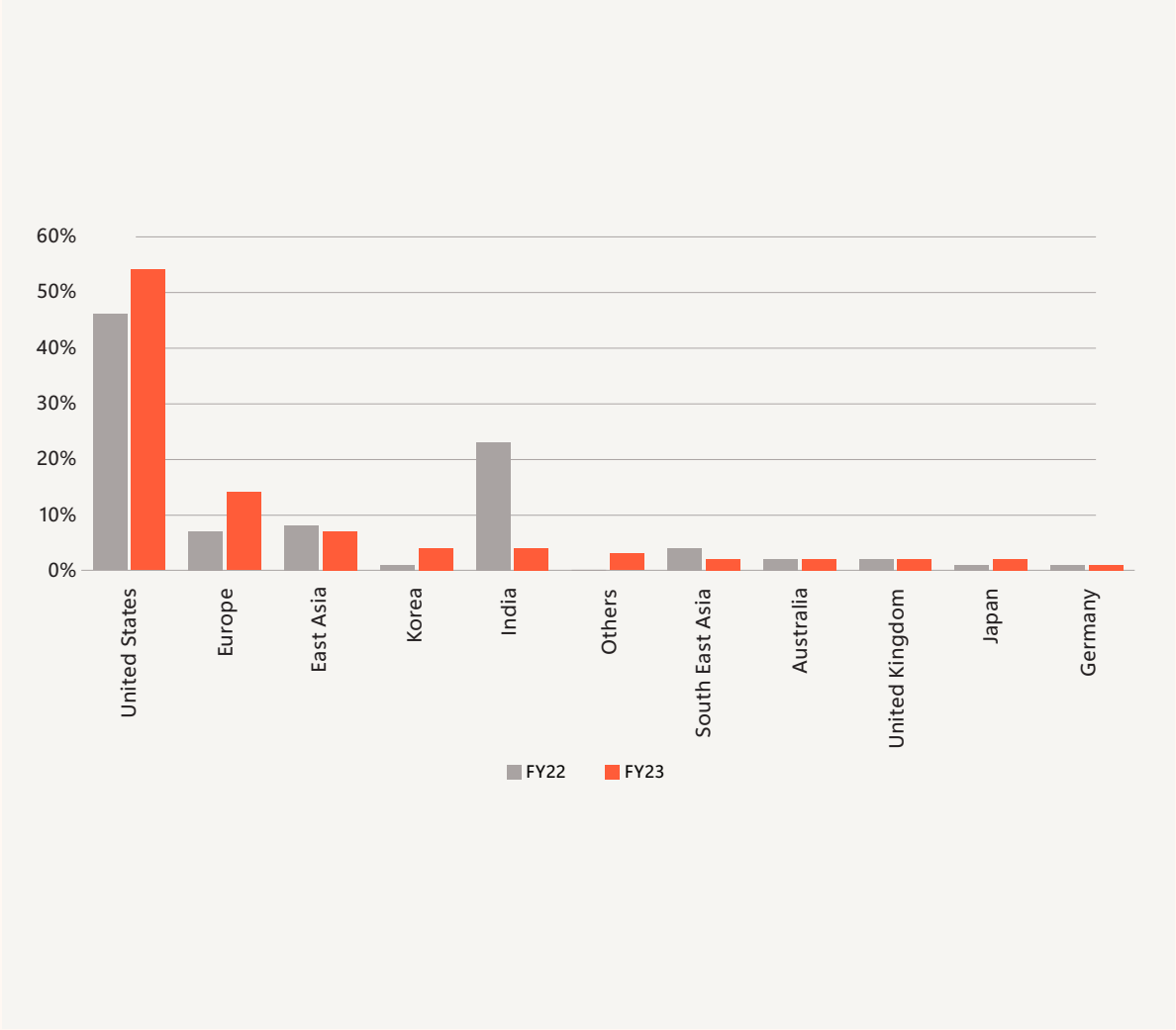
# Attacks increase in the United States and Europe, shifting away from India

US entities have continued to be primary targets for DDoS attacks, bearing the brunt of 54 percent of all attacks. However, the past year has seen Europe climb to the second highest with 14 percent of attacks, overtaking East Asia. The change is tied to geopolitical conflicts, with pro-Russian hacktivist groups intensifying their onslaught against Europe and the United States. India, the second most attacked country last year, is now fifth.

**Additional information**

What is a DDoS attack? | Microsoft Security

**Two-year comparison of top 10 most attacked regions**




Source: Microsoft Global DDoS Mitigation Operations

https://t.me/learningnets

# Return on mitigation: Targeting investment to increase resilience

During Microsoft Incident Response engagements, customer environments have been found to lack mitigations that range from the simple to the more complex.

While the goal of all mitigations is to make environments more resilient to cyberattacks, customers may not always have the resources to implement all of them, and a return on mitigation framework is helpful for prioritization. Generally speaking, the lower the resources and effort involved, the higher the return on mitigation (ROM). As an example of a high return, consider a simple solution to implement context-based MFA protection. This solution is highly effective in preventing initial access (high security value) but very simple to implement (low effort). When implemented, this solution effectively prevents initial access by providing more context around the authentication attempt, such as geographic location and the application used. The additional context can be combined with requiring the user to enter a number (number matching) to complete MFA to further improve sign-in security.

**Return on Mitigation scoring methodology**

Return on Mitigation score = (3x security value + 2x potential user impact) / Potential ease of implementation

| Return on Mitigation score | Type |
|---|---|
| 10 – 15 | Higher |
| 6 – 9 | Medium |
| 2 – 5 | Lower |

| Percentage of users potentially impacted | Score |
|---|---|
| Lower impact (<20% of users impacted) | 3 |
| Medium impact (Up to 50% users impacted) | 2 |
| Higher impact (>50% users impacted) | 1 |

| Engagement distribution (%) by major tactic | Score |
|---|---|
| 50 – 100 | 3 |
| 25 – 49 | 2 |
| 0 – 24 | 1 |

| Potential ease of implementation | Score |
|---|---|
| Easy to implement (20 hours or less) | 1 |
| Medium (20 – 40 hours) | 2 |
| Harder (40+ hours) | 3 |

We have calculated ROM values using a formula multiplying the weighted impact of the solution or mitigation by a weighted value of the solution in terms of effectiveness (security value), and factored in the effort involved in implementing the solution. The higher the ROM score, the lower the resources and effort involved in implementing the solution for the impact and value provided.

The percentage of environments missing each of the mitigations across all the environments reviewed during incident response engagements is also included.

https://t.me/learningnets

**Return on mitigation: Targeting investment to increase resilience** continued

| ROM | Issues found | % of customers with the issue |
|---|---|---|
| **Higher** | | |
| 15 | No advanced MFA protection mechanisms enabled | 37% |
| 15 | Poor user lifecycle management | 21% |
| 15 | Lack of EDR coverage | 13% |
| 15 | Lack of detection controls | 10% |
| 13 | Resource exposed to public access | 2% |
| 12 | Insufficient protections for local accounts | 60% |
| 12 | Missing security barrier between cloud and on-premise | 54% |
| 12 | Insecure Active Directory configuration | 43% |
| 12 | Insufficient device security controls | 8% |
| 11 | Legacy cloud authentication is still used | 47% |
| 11 | No advanced password protection enabled | 37% |
| 11 | Missing content based MFA protection mechanisms | 24% |
| 11 | Insecure operating system configuration | 3% |
| **Medium** | | |
| 8 | Legacy and unsecure protocols | 18% |
| 7 | Missing or inconsistent update management | 43% |
| 6 | Missing cloud application management and monitoring | 21% |
| 6 | No privileged identity management solution | 8% |
| 6 | No MFA, or MFA not mandatory for privileged accounts | 21% |
| 6 | Weak email protection against common threats | 16% |
| 6 | Legacy or unsupported operating systems | 14% |
| **Lower** | | |
| 4 | No privilege separation | 41% |
| 4 | No hardened workstations used for administration | 23% |
| 4 | Missing data classification and sharing restrictions | 5% |
| 3 | No vulnerability management | 30% |
| 2 | No adherence to the Least Privilege Principle | 63% |

### An example of a high ROM

A customer used the same local administrator password for all Windows endpoints. When an attacker gained access to one endpoint, they were able to move laterally and gain administrative privileges on all endpoints because of the shared password. This led to privilege escalation within the Active Directory Domain Services (ADDS) domain and a total domain compromise. To prevent this type of lateral movement, the customer could have used a solution called Local Administrator Password Solution (LAPS) to randomize local administrator passwords across all endpoints. By doing so, the impact could have been contained to just one endpoint, and with other mitigations for privilege escalation, a total domain compromise could have been averted.

# Recommendations

The most prevalent gaps we found during reactive incident response engagements were:

- Lack of adequate protection for local administrative accounts.
- A broken security barrier between on-premises and cloud administration.
- Lack of adherence to the least privilege model.
- Legacy authentication protocols.
- Insecure Active Directory configurations.

These gaps enable attacker tactics ranging from Initial Access to Lateral Movement and Persistence. To mitigate and protect against these tactics, we recommend randomizing local administrative account passwords, not synchronizing on-premises administrative accounts to the cloud, and having separate accounts and purpose-built hardened workstations for on-premises and cloud administration.

**For more information about return on mitigation by techniques observed, please see page 43.**

We also recommend using just-in-time and just-enough administration in the cloud and on premises, separating daily use and administrative accounts, making an inventory of all applications using legacy authentication protocols, and modernizing those applications where possible and phasing out those that cannot be modernized.

https://t.me/learningnets

## Return on mitigation: Targeting investment to increase resilience continued

Higher ROM H | Medium ROM M | Lower ROM L

### Return on mitigation by MITRE ATT&CK technique

| MITRE ATT&CK techniques observed | Reconnaissance | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Insecure Active Directory configuration | H | L | H | H | H | | L | | H | | | | |
| Unsecure legacy authentication is still leveraged | | H | L | | H | | | | | | | L | |
| Lack of detection controls | | H | | H | | | H | | | | | | |
| Lack of EDR coverage | | H | | | H | | H | | H | | | | |
| Missing context-based multifactor protection mechanisms | | H | | | H | | H | | | | | | |
| No advanced MFA protection mechanisms enabled | | H | | | H | | H | | | | | | |
| No advanced password protection enabled | | H | | | | | H | | H | | | | |
| Poor user lifecycle management | | H | | | | | H | | | | | | |
| Insecure operating system configuration | | H | | | | | H | | | | | | |
| Resource exposed to public access | | H | | | | | | | | | | | |
| Missing or inconsistent update management | | M | M | | | | M | | | | | | |
| Legacy and unsecure protocols | | M | | | M | | M | | | | | | |
| Insufficient device security controls | | L | M | H | H | | | | | L | | | M |
| Legacy or unsupported operating systems | | L | L | | | | | | | | | | |
| Weak email protection against common threats | | L | | | | | | | L | | | L | |
| No MFA or MFA not mandatory for privileged accounts | | L | | | | | | | | | | | |
| No vulnerability management | | | L | L | | L | | | | | L | | |
| Missing cloud application management and monitoring | | | | L | | | | | | L | | L | |
| Missing security barrier between the cloud and on-premise | | | | | H | | | | H | | | | |
| No privilege separation | | | | | L | | L | | L | | | | |
| No hardened device used for high privileged accounts | | | | | L | | | | L | | | | |
| No privileged identity management solution | | | | | L | | | | L | | | | |
| Not adhering the Least Privilege Principle | | | | | L | | | | | | | | |
| Insufficient protections for local accounts | | | | | | | | | H | | | | |
| Missing data classification and sharing configuration | | | | | | | | | | L | | L | |

https://t.me/learningnets

**Return on mitigation: Targeting investment to increase resilience** continued

### Summary of actionable steps

Based on the most prevalent gaps found during our reactive incident response engagements, here is a summary of actionable steps to take for greater cyber resiliency:

| Problem | Actionable steps |
|---|---|
| **Insecure configuration of identity platform**<br>Misconfigurations and exposure of identity platforms and their components are common vectors for attackers to gain unauthorized high-privilege access. | Adhere to security configuration baselines and best practices when deploying and maintaining identity systems, such as Active Directory (AD) and Azure AD infrastructure. Enforce access restrictions by implementing segregation of privileges and least privilege access and utilize privileged access workstations (PAWs) to manage identity systems. |
| **Insufficient privilege access and lateral movement controls**<br>Administrators have excessive permissions across the digital environment and often expose administrative credentials on workstations subject to internet and productivity risks. | To enhance resilience and limit the scope of an attack, secure and restrict administrative access. Utilize Privileged Access Management controls, such as just-in-time access and just-enough administration. Avoid synchronizing on-premises administrative accounts with the cloud and vice versa. |
| **Low maturity security operations**<br>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. |
| **Limited adoption of modern security frameworks**<br>Identity is now the security perimeter, granting access to various digital services and computing environments. By integrating Zero Trust principles, application security, and other modern cyber frameworks, organizations can proactively manage risks that may be difficult to anticipate. | 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. |
| **No multifactor authentication (MFA) or lack of modern MFA mechanisms**<br>Today's attackers do not break in; they log in. | MFA is a critical and fundamental user access control that all organizations should enable. Coupled with conditional access and modern MFA mechanisms, MFA can be invaluable in fighting cyber threats. |
| **Lack of information protection control**<br>Organizations struggle to implement comprehensive information protection controls that cover all data locations, remain effective throughout the information lifecycle, and align with the criticality of business data. | Identify your critical business data and where it is located. Review information lifecycle processes and enforce data protection while ensuring business continuity. |

**Additional information**
Windows LAPS overview | Microsoft Learn

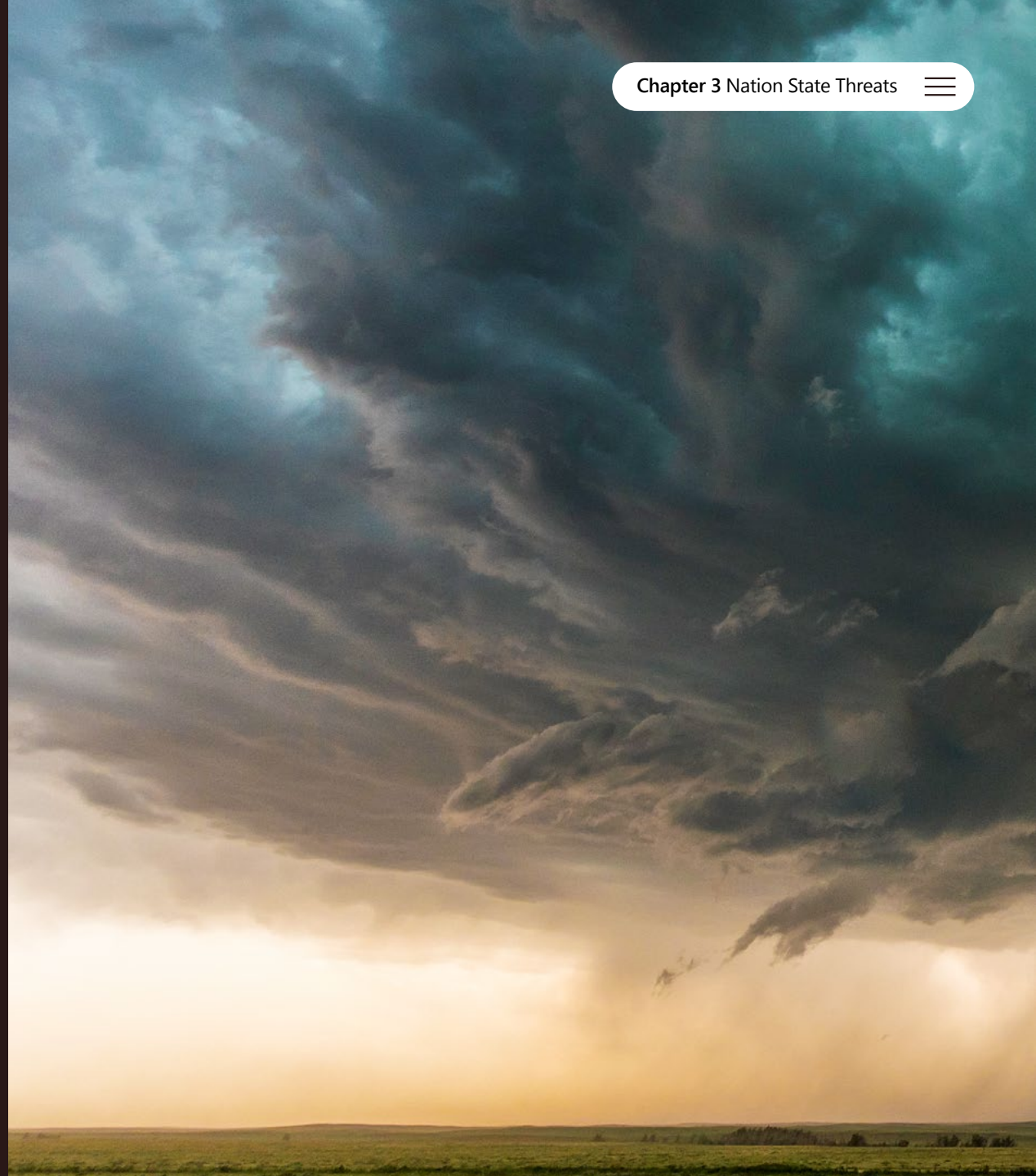
https://t.me/learningnets

# Chapter 3
# Nation State Threats

## How has the threat landscape changed?


| | |
|---|---|
| Key developments | 46 |
| Introduction | 47 |
| Russia | 54 |
| China | 60 |
| Iran | 65 |
| North Korea | 70 |
| Palestinian threat actors | 73 |
| The emerging threat posed by cyber mercenaries | 74 |


https://t.me/learningnets



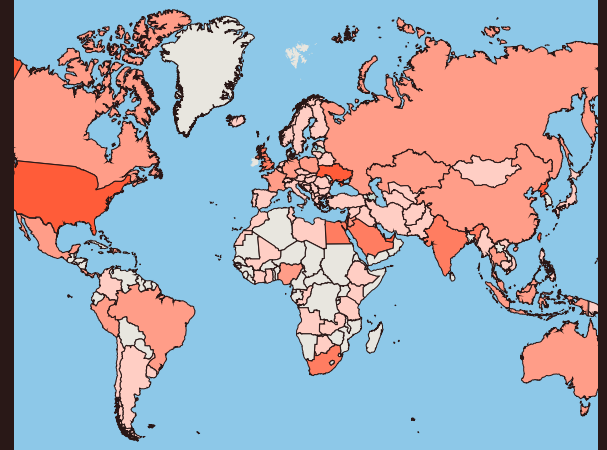
Nation State Threats

# Key developments

After last year's flurry of high-profile cyberattacks, nation-state cyber actors this year pivoted away from high-volume destructive attacks and instead directed the bulk of their activity toward cyber espionage.

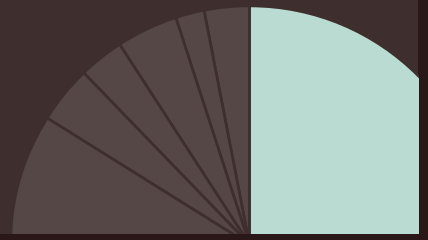
As nation-state threat actors continue to grow in sophistication, they have been increasingly used by governments to understand the plans of other nations, transnational bodies, and non-governmental organizations. Critical infrastructure also remains a popular target, with threat actors employing stealthier techniques to establish persistence and evade detection, as is the education sector. At the same time, some governments have used cyber-enabled influence campaigns to manipulate public opinion at home and abroad. Cyber operations are expanding globally, with increased activity in Latin America, sub-Saharan Africa, and the Middle East due to heightened Iranian activity.

**Nation-state and state-affiliated threat actor activities pivoted away from high volume destructive attacks in favor of espionage campaigns.**



Find out more on page 48

## Russian state-sponsored threat actors used diverse means to access devices and networks in NATO member states.



Find out more on page 54

## Chinese cyber threat groups carried out sophisticated worldwide intelligence collection campaigns.

**At the same time, China's cyber influence campaigns continue to operate at an unmatched scale.**

Find out more on page 60

## The unchecked expansion of the cyber mercenary marketplace threatens to destabilize the broader online environment.

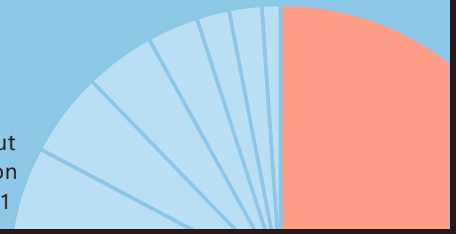
Find out more on page 74

## Iranian state actors are using increasingly sophisticated tradecraft

including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster.

Find out more on page 66

## North Korean actors conducted a supply chain attack using an existing supply chain compromise.



Find out more on page 71

https://t.me/learningnets

# Navigating evolving threats

## Introduction from John Lambert

Nation-state actors are showing increased investment and use of cyber operations as a tool to achieve their geopolitical goals. This is driving many organizations to invest in layered security to defend against sophisticated threats. It is also bringing the technology industry and governments together to increase resilience against attempts to undermine the security of the online environment.

Cyberattacks continue to rise in sophistication and frequency. As the threat landscape evolves, we are seeing a blurring of lines between cyber operations, espionage, influence campaigns, and destructive attacks. Cyber operations have also become more public, often gaining more media attention, with the ongoing use of influence narratives to manipulate global and national opinion.

We have seen a broader number of threat actors, both nation-state and criminal, exploit newly released vulnerabilities more quickly, enhance their operations in cloud environments, and continue to use techniques to "live off the land" and evade detection. Looking to destructive cyber operations, the pace of Russian state-sponsored destructive cyberattacks declined while the variety of attacks increased.

We detected limited destructive attacks leveraging rudimentary file wipers through Summer 2023 and some isolated ransomware-style attacks in late 2022. By contrast, North Korean cyber operations increased in sophistication over the past year, with Citrine Sleet being the first activity group Microsoft observed capitalizing on a prior supply chain compromise to conduct the 3CX supply chain attack in March 2023.

We saw a China-based actor which Microsoft is tracking as Storm-0558 gain access to email accounts affecting approximately 25 organizations using forged authentication tokens to access user email using an acquired inactive Microsoft account (MSA) consumer signing key. Microsoft mitigated this attack for all customers. Iranian state actors conducted a GoldenSAML attack, a technique which was previously used by the highly sophisticated Russian group Midnight Blizzard.

Op Cybersecurity Tech Accord principles mapping index on **page 124**

The rising complexity, scale, and volume of threats is driving the need to reimagine how we talk about threats and enable customers to understand threats quickly and with clarity. This year, we shifted to a new naming taxonomy for threat actors aligned with the theme of weather. The new taxonomy will bring better clarity to customers and security researchers with a more organized and easy to use reference system for threat actors.

"As the threat landscape evolves, we are seeing a blurring of lines between cyber operations, espionage, influence campaigns, and destructive attacks."

Organizations can reduce and prevent vulnerability exploits and compromised user credentials by continuing to harden the attack surface. We must also continue to combine cyber threat intelligence, geopolitical intelligence, and technical research to understand the whole adversary, achieve a more complete picture of the ever-changing threat landscape, and improve collective resilience.

**John Lambert**
Corporate Vice President, Distinguished Engineer, Microsoft Security Research

https://t.me/learningnets

# Espionage operations increase and destructive operations decline

Nation-state and state-affiliated threat actor activities in the past year pivoted away from high-volume destructive attacks in favor of espionage campaigns. While the impact of destructive attacks is felt more immediately, persistent and stealthy espionage operations pose a long-term threat to the integrity of government, private industry, and critical sector networks.

Russian and Iranian state-sponsored actors that employed destructive attacks most frequently, changed the frequency of their destructive operations over the past year. At the same time, threat actors globally acted to increase their collection capacity against foreign and defense policy organizations, technology firms, and critical infrastructure organizations.

The high-volume of destructive attacks that dominated the early stages of Russia's invasion of Ukraine tapered off. Nearly 50 percent of destructive Russian attacks we observed against Ukrainian networks occurred in the first six weeks of the war.

**Please see 'About this Report' on page 9 for relevant definitions used in this chapter.**

50%

of destructive Russian attacks we observed against Ukrainian networks occurred in the first six weeks of the war.

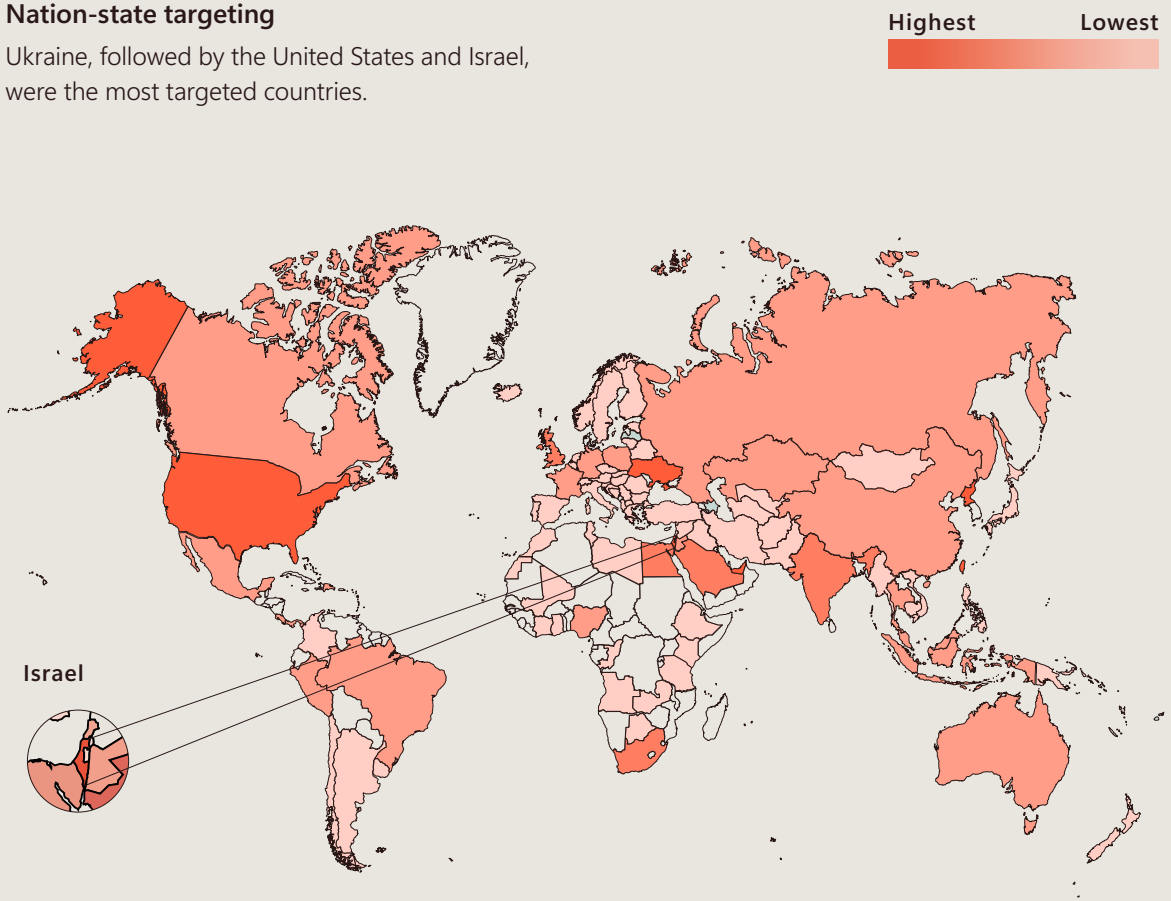
Later, in October and November 2022, Russian state actor Seashell Blizzard added destructive ransomware to its toolkit, deploying Prestige ransomware against a Polish entity, and Prestige and Sullivan ransomware against Ukrainian organizations.[1] The actor demonstrated consistent testing and development of the Sullivan payload, but Microsoft has not observed subsequent ransomware-style attacks from this threat actor.[2]

What Microsoft observed most often from Seashell Blizzard and other Russia-affiliate threat actors were phishing and password spray campaigns, credential theft, lateral movement through networks, data exfiltration, and other actions associated with gaining and retaining access to targets for intelligence collection.

**For more about Russian state actors' activity, see page 54.[5]**

**Nation-state targeting**

Ukraine, followed by the United States and Israel, were the most targeted countries.




Microsoft Threat Intelligence observed state-sponsored cyber threat activity against organizations in more than 120 countries and territories this year. Data destruction represented a small fraction of the observed activity, which was predominantly reconnaissance, initial access and various other actions on network, and data exfiltration.

https://t.me/learningnets

**Navigating evolving threats** continued

Actors associated with the Iranian government have also conducted fewer destructive cyberattacks. Groups like Cotton Sandstorm adopted a new tactic of cyber-enabled influence operations (see page 68), often using less time- and resource-intensive disruptive defacements and DDoS attacks. Since June 2022, we have observed an increased pace in Iran's use of these types of influence operations, focused on manipulative messaging and amplification with an underlying influence narrative.[3] The rise of these operations corresponded with a decline in what was previously a spike in Iranian destructive cyberattacks using ransomware as a guise from 2020 to mid-2022.

Critical infrastructure targeting remains robust across the board, increasing again in the last year, with threat actors employing stealthier techniques to establish persistence and evade detection in these sensitive networks.

Volt Typhoon, a Chinese state-affiliated actor, has targeted critical infrastructure organizations in Guam and elsewhere in the United States. Active since mid-2021, the group conducted a campaign to infiltrate networks within US critical infrastructure organizations including in the communications, utility, transportation, government, and information technology sectors.[4] To evade detection, it used legitimate accounts, living-off-the-land binaries, and SOHO routers for network communications. Meanwhile, Russian state actor Forest Blizzard exploited a zero-day vulnerability in Outlook to steal data from defense industrial base and transportation sector organizations within NATO member states.[5]

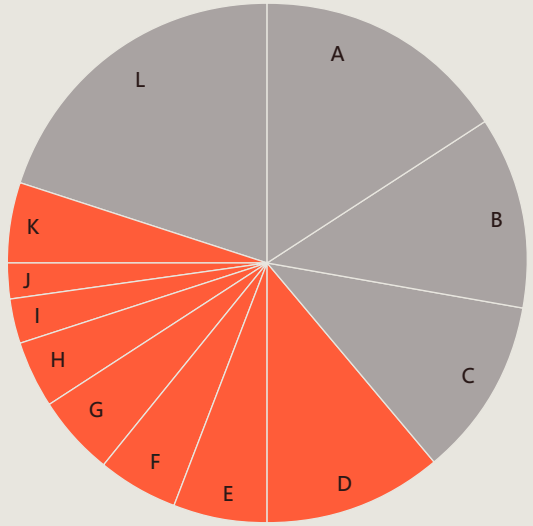
Diamond Sleet, a North Korean threat actor known for its destructive attack targeting Sony Pictures in 2014, was observed targeting and compromising nuclear energy organizations globally in the spring of 2023. In the fall of 2022, Diamond Sleet was also observed compromising maritime entities, with a focus on submarine technologies. Diamond Sleet is known to conduct persistent and stealthy espionage operations likely to collect information of high importance to the North Korean regime.

**41%**

of the threat notifications Microsoft sent to online services customers between July 2022 and June 2023 went to critical infrastructure organizations.

### Most targeted sectors globally

State-sponsored threat groups target broadly as part of their intelligence collection. Critical infrastructure sectors (highlighted) comprised 41% of the NSNs sent in FY2023.




- A 16% Education
- B 12% Government
- C 11% Think tanks and NGOs
- D 11% IT
- E 6% Communications
- F 5% Finance
- G 5% Transportation
- H 4% Defense Industry
- I 3% Energy
- J 2% Manufacturing Infrastructure
- K 5% Other Critical Infrastructure
- L 20% Other

Source: Microsoft Threat Intelligence NSN data.

### Actionable insights

1. Organizations should look at their attack surface through the lens of the attacker, prioritizing their security response based on the organization's external attack surface. Identify and protect high-value data targets and 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.
3. Use the strongest form of FIDO compliant multifactor authentication (MFA) combined with hardening the attack surface around tokens.
4. 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.
5. 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.
6. Enable MFA for all accounts (including service accounts) and ensure MFA is enforced for all remote connectivity.
7. Use passwordless solutions to secure accounts.

https://t.me/learningnets

# Increased sophistication enhances threat actors' capabilities

Iranian and North Korean state actors are demonstrating increased sophistication in their cyber operations, in some cases starting to close the gap with nation-state cyber actors such as Russia and China.

- **Iran:** Iranian state actors have increasingly migrated their cyber targeting and operations to focus on attacks that allow them to move from on-premises into cloud environments, representing a tangible increase in the maturity of their capabilities. In March, one group conducted a GoldenSAML attack, a technique only previously seen used by the highly sophisticated Russian group Midnight Blizzard, enabling Iranian operators to move from an on-premises site to a cloud environment. In February, another Iranian state actor moved laterally from an on-premises location to a cloud environment where it later conducted a destructive attack.

**For more about Iranian state actor activity, see page 65.**

- **North Korea:** In early 2023, Ruby Sleet showed increasing sophistication by utilizing a stolen legitimate certificate of an IT security solutions provider to sign malicious files used to target organizations. In March, Citrine Sleet conducted a supply chain compromise leveraging a prior supply chain compromise, marking the first time Microsoft observed such an attack.[6]

**For more about North Korean cyber operations, see page 70.**

- **Other adversarial cyber advancements:** Iranian partners and proxies also demonstrated consistent improvements in cyber operations since 2022, as highlighted in our 2022 report's disclosure of Plaid Rain's (POLONIUM) abuse of cloud services for command and control (C2) across most of its victims. In 2023, a Palestinian group delivered backdoors configured to enable rotation of C2 domains likely to evade detections.

**For more about Palestinian threat actor activity, see page 73.**

**Additional information**

Please see our mitigation and protection guidance in this article published in May 2023:
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft Security Blog

CSA Living off the Land.PDF | defense.gov

https://t.me/learningnets

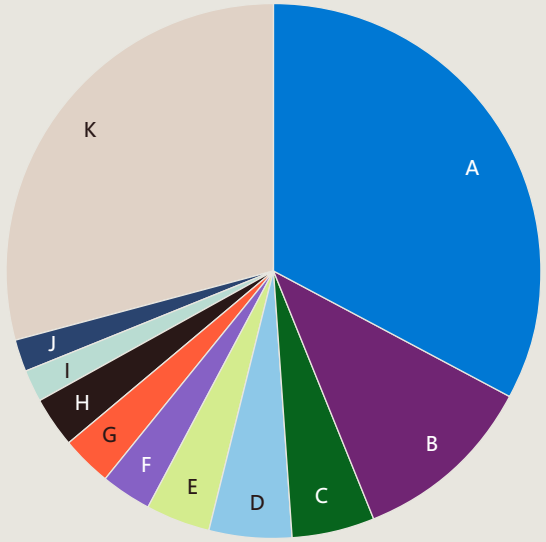
# Threat actors are expanding their global target set

Nation-state actors' cyber operations grew increasingly global in scope this past year, particularly expanding in the Global South to more parts of Latin America and sub-Saharan Africa. While cyber operations remained most pronounced against the US, Ukraine, and Israel, and pervasive throughout Europe, operations increased in the Middle East owing to Iranian actors. Organizations involved in the policymaking and implementation ecosystem were among the most targeted, in line with many groups' espionage-focused remits.

## Most targeted regions

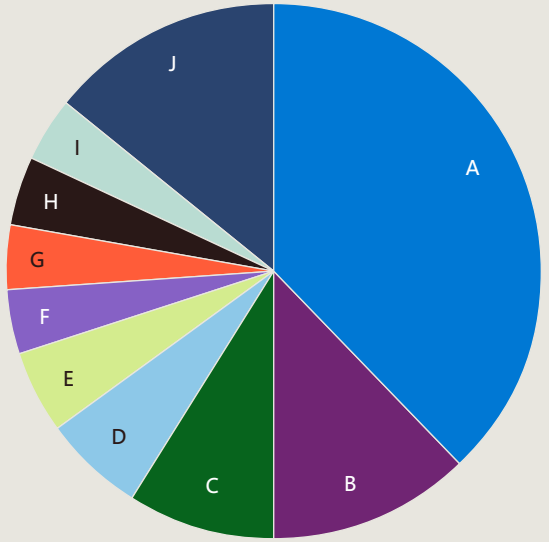
A breakdown of operations by region reflects the priority targets of the threat actors. Ukraine is the top European target per volume of observed activity, driven by Russian state actors' invasion-related operations. Israel remains by far the most-targeted country in the Middle East and North Africa region as a result of Iran's extensive focus there. North Korean and Chinese state actors drove South Korea and Taiwan to the first and second most targeted geographies in the Asia-Pacific.

### Europe



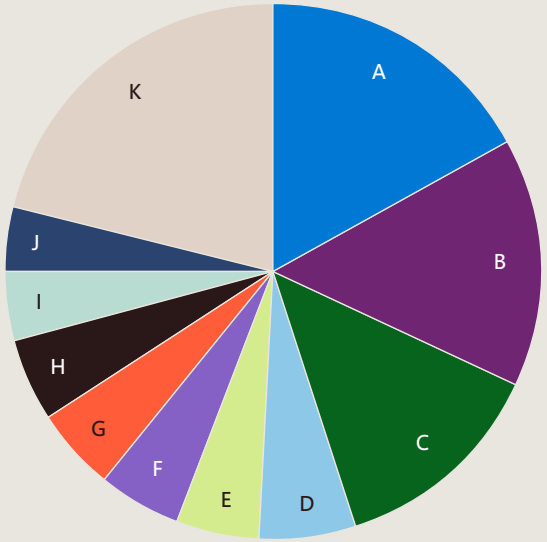

- A 33% Ukraine
- B 11% United Kingdom
- C 5% France
- D 5% Poland
- E 4% Italy
- F 3% Germany
- G 3% Switzerland
- H 3% Netherlands
- I 2% Azerbaijan
- J 2% Albania
- K 29% Other

### Middle East and North Africa




- A 38% Israel
- B 12% United Arab Emirates
- C 9% Saudi Arabia
- D 6% Jordan
- E 5% Iraq
- F 4% Bahrain
- G 4% Lebanon
- H 4% Egypt
- I 4% Turkiye
- J 14% Other

### Asia-Pacific




- A 17% Korea
- B 15% Taiwan
- C 13% India
- D 6% Malaysia
- E 5% Japan
- F 5% Australia
- G 5% Thailand
- H 5% Indonesia
- I 4% Pakistan
- J 4% Philippines
- K 21% Other

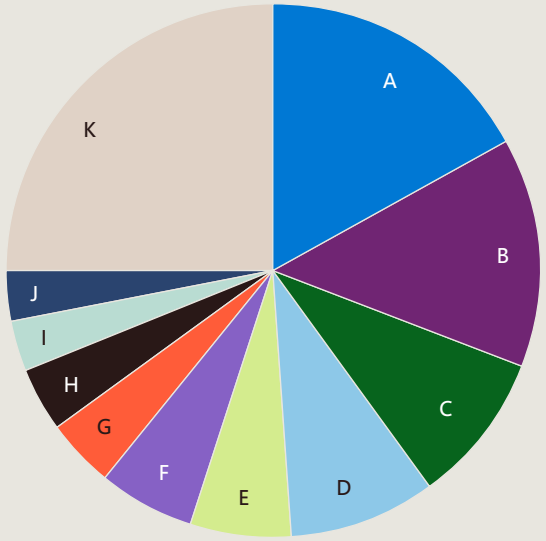
**Source: Microsoft Threat Intelligence events data**

https://t.me/learningnets

## Most targeted sectors by region

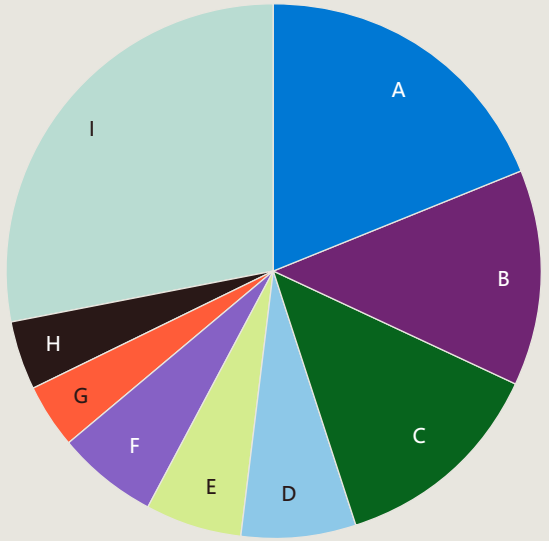
Nation-state cyber operations targeted various sectors across the globe. Perceived soft targets—such as think tanks, NGOs, and universities—remained top targets like last year, as threat actors likely view them as easier initial access vectors to gain insights into a country's policy or science and technology communities. At the same time, targeting of traditionally more hardened targets, such as government agencies and the defense industry, rose as geopolitical tensions rose surrounding the Ukraine War, the Taiwan Straits, and Iran and North Korea's nuclear programs. Increased sophistication by actors also likely enabled actors to have increased access to harder targets.

### Europe



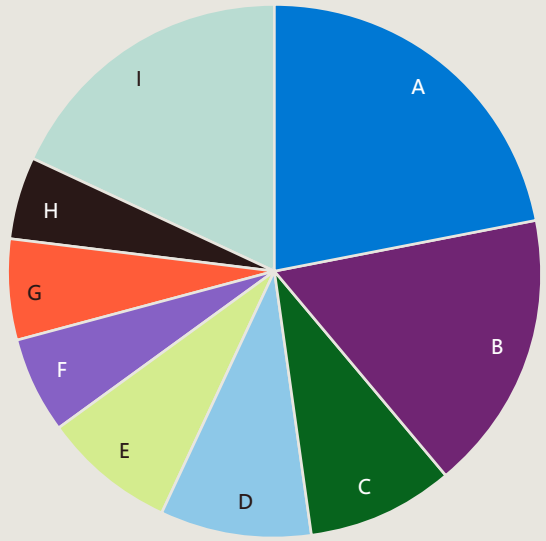

- A 17% Think tanks/NGOs
- B 14% Government
- C 9% Education
- D 9% IT
- E 6% Communications
- F 6% Intergovernmental Organizations
- G 4% Transportation
- H 4% Finance
- I 3% Defense Industry
- J 3% Energy
- K 25% Other

### Middle East and North Africa




- A 19% Education
- B 13% Government
- C 13% IT
- D 7% Communications
- E 6% Transportation
- F 6% Finance
- G 4% Energy
- H 4% Defense Industry
- I 28% Other

### Asia-Pacific




- A 22% Education
- B 17% IT
- C 9% Transportation
- D 9% Government
- E 8% Communication
- F 6% Media
- G 6% Think tanks/NGOs
- H 5% Finance
- I 18% Other

**Source: Microsoft Threat Intelligence nation state notifications**

https://t.me/learningnets

# The growing threat of influence operations

Nation state actors are more frequently employing influence operations alongside cyber operations to spread favored propaganda narratives. Such narratives aim to manipulate global and national opinion and undermine the democratic institutions within perceived adversary nations. Influence operations which occur in the context of national elections or armed conflict are especially dangerous.

In the online environment, cyber influence operations often make use of coordinated inauthentic behavior–such as the deployment of automated bots and web assets run by troll farms to generate, spread, and amplify content, often with false or misleading information. Offline, state actors undertake influence activity like staging provocations, traditional media engagement, and funding or supporting political groups or candidates. Such actions—whether online or offline—may be done overtly, for example through state-controlled media organs, or covertly. Often, they seek to exploit existing fault lines or divisions in societies to manipulate public opinion in support of a nation's objectives.

Although the tactics, techniques, and procedures (TTPs) employed in influence operations vary across campaigns, one noteworthy trend that has emerged across actors is the overlap and, in some cases, synchronization between traditional influence operations and cyber actions. In the wake of its 2022 full-scale invasion of Ukraine, Russia has consistently timed its influence activities to coincide with cyber and kinetic attacks. Similarly, Iran has intensified its use of cyber-enabled influence operations to achieve greater impact. In July and September 2022, Iranian state actors that we assess are linked to Iran's Ministry of Intelligence and Security, conducted destructive attacks against the Albanian government.[7] The attacks were followed by a coordinated influence operation by a cyber persona called Homeland Justice that has lasted up until the time of this writing. Homeland Justice's narratives aligned with the messaging in the cyberattacks, calling on Albania to stop harboring members of the Mujahedin-e Khalq, an Iranian dissident group that seeks the overthrow of the Iranian government.

Finally, some influence actors have increasingly employed AI-generated content in their influence operations targeting democracies.

While AI-generated profile pictures have long been a feature of state-sponsored influence operations, the use of more sophisticated AI tools to create more striking multimedia content is a trend we expect to persist with the wider availability of such technologies.

**For more about influence operations, please see the sections on Russia, China, and Iran in this chapter.**

https://t.me/learningnets

# Russia

**Threat actor naming taxonomy: Blizzard**

Russian state actors expanded the scope of their Ukraine war-related cyber and influence operations to target Kyiv's allies. This was in addition to the numerous destructive wiper and cyberespionage operations targeting Ukrainian government and critical civilian infrastructure that we have publicly reported over the last year.[8]

**For more information on threat actor naming taxonomy, see pages 10-11.**

**Ukraine-focused reporting released since July 2022**

Is Russia regrouping for renewed cyberwar? | Mar 15, 2023

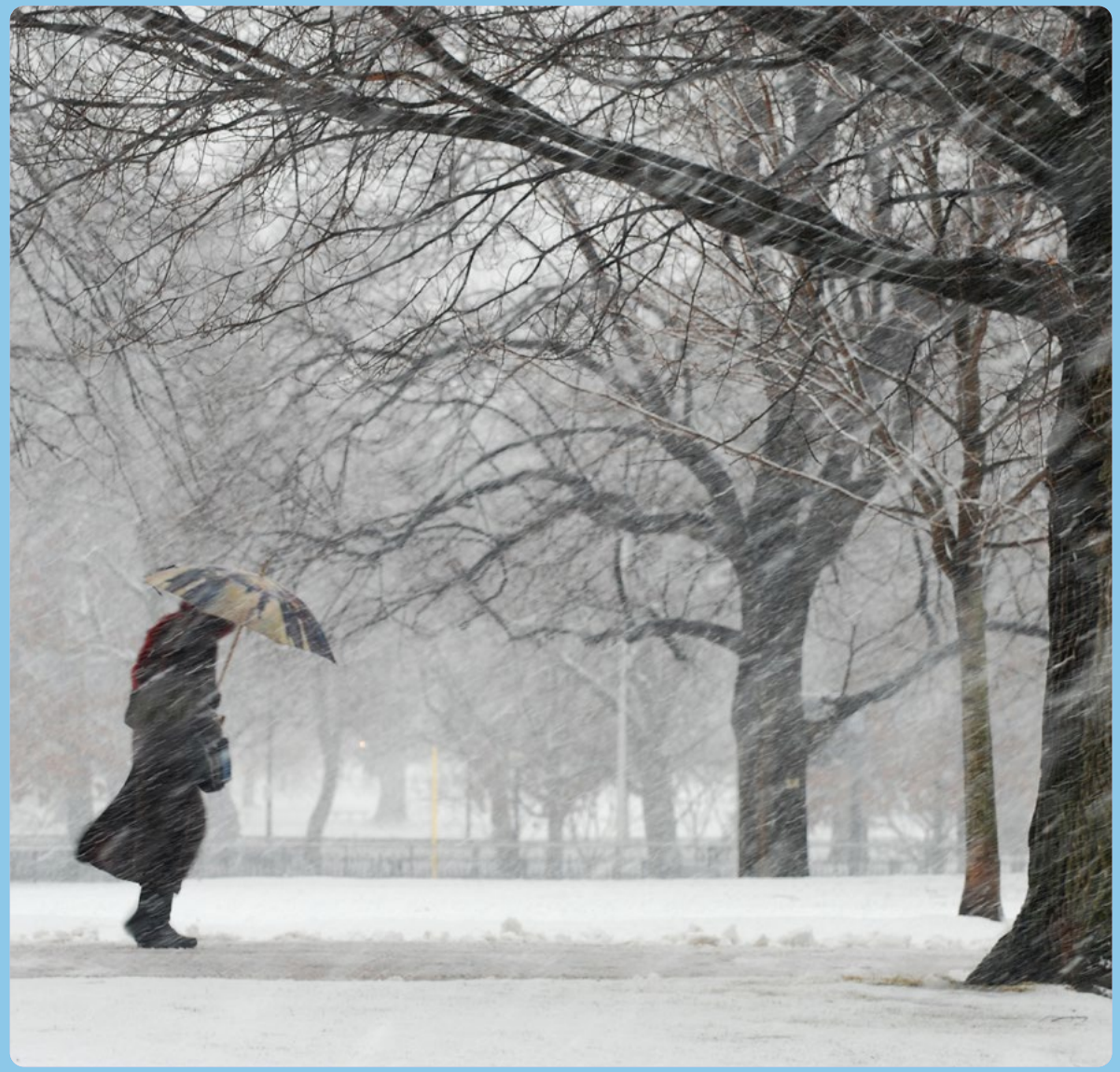
Preparing for a Russian cyber offensive against Ukraine this winter | Dec 3, 2022

Given the body of Ukraine-focused reporting we have released since July 2022, this section provides an opportunity to dive deeper into Russian state cyber operations outside of the active military conflict zone.

Russian state-sponsored threat actors used diverse means—from phishing campaigns to zero-days—to gain initial access to devices and networks in industries across NATO member states, while malign influence actors sought to intimidate the Ukrainian diaspora and encourage protest movements across Europe. The expansion of Russia's war-related targeting suggests that any government, policy, or critical infrastructure organization located within a country that provides Ukraine with political, military, or humanitarian support is at risk of compromise.

## Actionable insights

1. Protect user identities with MFA protection tools and reinforcing least privilege access.
2. Keep systems up to date; patch early and often.
3. Deploy antimalware, endpoint detection and response, and identity protection solutions.
4. Enable investigations and recovery with backups, logging, and an incident response plan.



https://t.me/learningnets

**Russia** continued

# NATO members' diplomatic, defense, and transport sectors are under threat

Russian state cyber actors from civilian and military intelligence services conducted operations against NATO member states, targeting government organizations, transportation, energy sector, and other networks almost certainly to facilitate intelligence collection.

In April and May this year, Microsoft observed a spike in activity against Western organizations, at which time roughly 46 percent of observed network intrusions were directed against organizations within NATO member states, particularly the United States, United Kingdom, and Poland.

Although most Russian state and state-affiliated intrusions since July 2022 were directed against Ukrainian organizations (48 percent), more than a third were directed against organizations in NATO member countries.

### Additional information

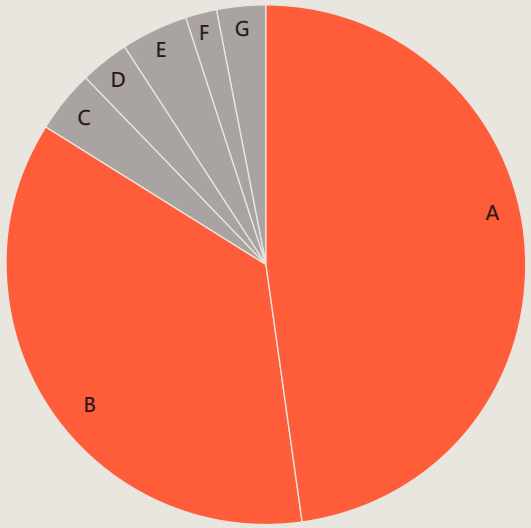
Require compliant, hybrid joined devices, or MFA – Microsoft Entra | Microsoft Learn

Learn about Windows security baselines you can deploy with Microsoft Intune | Microsoft Learn

### Actionable insights

1. Pilot and deploy phishing-resistant authentication methods. See page 36.
2. Require phishing-resistant authentication for critical apps.
3. Educate users about social engineering and credential phishing attacks, including refraining from entering MFA codes sent via any form of unsolicited messages.
4. Educate Microsoft Teams users to verify external communication attempts, be cautious about what they share, and never share their account information or authorize sign-in requests over chat.
5. Allow only known devices that adhere to Microsoft's recommended security baselines.

### Most targeted regions



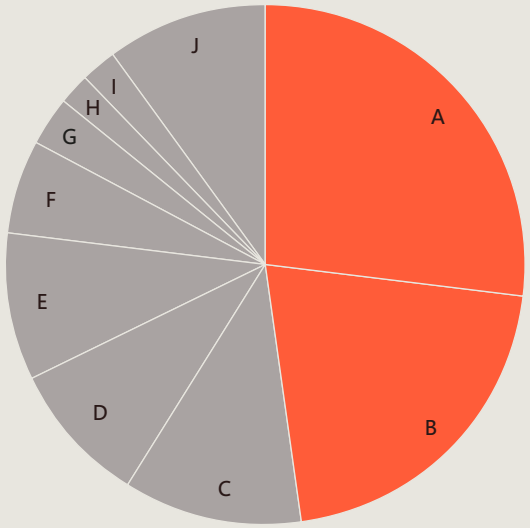

- A 48% Ukraine
- B 36% NATO Member states
- C 4% Europe
- D 3% MENA
- E 4% Latin America
- F 2% Africa
- G 3% Asia

36%

of observed network intrusions were directed against organizations within NATO member states, particularly the United States, United Kingdom, and Poland.

Source: Microsoft Threat Intelligence

### Most targeted sectors




- A 27% Government
- B 21% Think tanks/NGOs
- C 11% Education
- D 9% IT
- E 9% Intergovernmental organizations
- F 6% Defense Industry
- G 3% Energy
- H 2% Health
- I 2% Transportation
- J 10% Other

Source: Microsoft Threat Intelligence nation state notifications

https://t.me/learningnets

**Russia** continued

### Threat actors are phishing for insights

Russian state actors including Midnight Blizzard, Star Blizzard, and Aqua Blizzard launched phishing campaigns posing as Western diplomats and Ukrainian officials to gain access to accounts that might contain insights into Western foreign policy on Ukraine, defense plans and intentions, or war crimes investigations. Aqua Blizzard actors also masqueraded as Ukrainian defense and legal officials to target Western and Ukrainian humanitarian and judicial organizations, then used the html smuggling technique to bypass email detections and evade automated defenses.

Midnight Blizzard operators posed as UNICEF's Kyiv office to phish Ukraine-based diplomatic organizations representing at least 20 countries in May.

Star Blizzard impersonated a high-level former US official to send mails to US diplomatic personnel that formerly served in Ukraine. In May, Midnight Blizzard sent emails from Poland-themed email addresses to dozens of accounts at 12 international organizations including NATO, as well as diplomatic representatives of several NATO member states. This campaign was one of many that the threat actor conducted this year targeting diplomatic entities involved in Ukraine policy.

### Forest Blizzard using zero-day vulnerabilities to target sensitive sectors

Main Intelligence Directorate (GRU)-affiliated actor, Forest Blizzard's compromise of operational and strategic level targets likely represents a means by which Russian leadership can gain situational awareness supporting a range of military and foreign policy objectives.

In addition to conducting phishing campaigns, Forest Blizzard has used an Outlook zero-day vulnerability, CVE-2023-23397, throughout 2022 and into 2023 to access government organizations in Ukraine, as well as NATO member-states' defense industrial base, transportation, and education sectors. Following exposure of the vulnerability, Microsoft Threat Intelligence observed an uptick in Forest Blizzard's use of it over a two-week period, indicating the actor's increasing high-risk tolerance for conducting intrusions that could easily expose its operations.[9]

Separately, Forest Blizzard exploited Exchange Web Services in cloud and hybrid environments to steal data from email accounts at energy, defense, and air transportation organizations based in countries that provide logistics or tactical support to Ukraine. Employing advanced post-compromise techniques, the actors positioned themselves to access any account of interest in a targeted environment. They used Exchange PowerShell to obtain persistent access to targeted mail items of interest by modifying folder permissions for a mailbox. The operators also configured users' application impersonation roles to gain access to any item in a folder or to perform additional actions while authenticating as a different user.

Aqua Blizzard actors masqueraded as Ukrainian defense and legal officials to target Western and Ukrainian humanitarian and judicial organizations.

### Actionable insights

1. Track changes made to a mailbox by a user.
2. Monitor and alert on suspicious permissions changes made by users and administrators.
3. Apply patches when they become available to protect devices from targeting.
4. Add users to the Protected Users group, which provides additional credential protections beyond disabling NTLM and should be used for high-value accounts, such as domain administrators, when possible.

### Additional information

Mailbox auditing | Microsoft

Administrator audit logging | Microsoft

Protected users group | Microsoft

https://t.me/learningnets

# Cyber and influence operations continue to converge

The scope and intensity of cyber-enabled influence campaigns between state actors and hacktivist groups has matured over the course of Russia's war in Ukraine, as the dates between the attacks and public leaks have condensed from a few days to nearly same-day operations.

Microsoft has observed instances of convergence between Russia-affiliated cyber operations and pro-Russian "hacktivist" attacks in Ukraine that probably serve to obscure Russian state involvement. Seashell Blizzard, Cadet Blizzard, and other suspected Russian actors all conducted operations that at times shared victimology and close temporal proximity with hacktivist groups that leaked sensitive stolen data or claimed to have conducted cyberattacks against named organizations.[10] Cyber-enabled influence campaigns involving purported hacktivist groups Cyber Army of Russia, Free Civilian, and others almost certainly served to discredit the victim organizations, while the public claims of responsibility likely aimed to amplify the effects of cyberattacks on victims' networks.

**Russian advanced persistent threat (APT) activities overlap with influence operations campaigns**

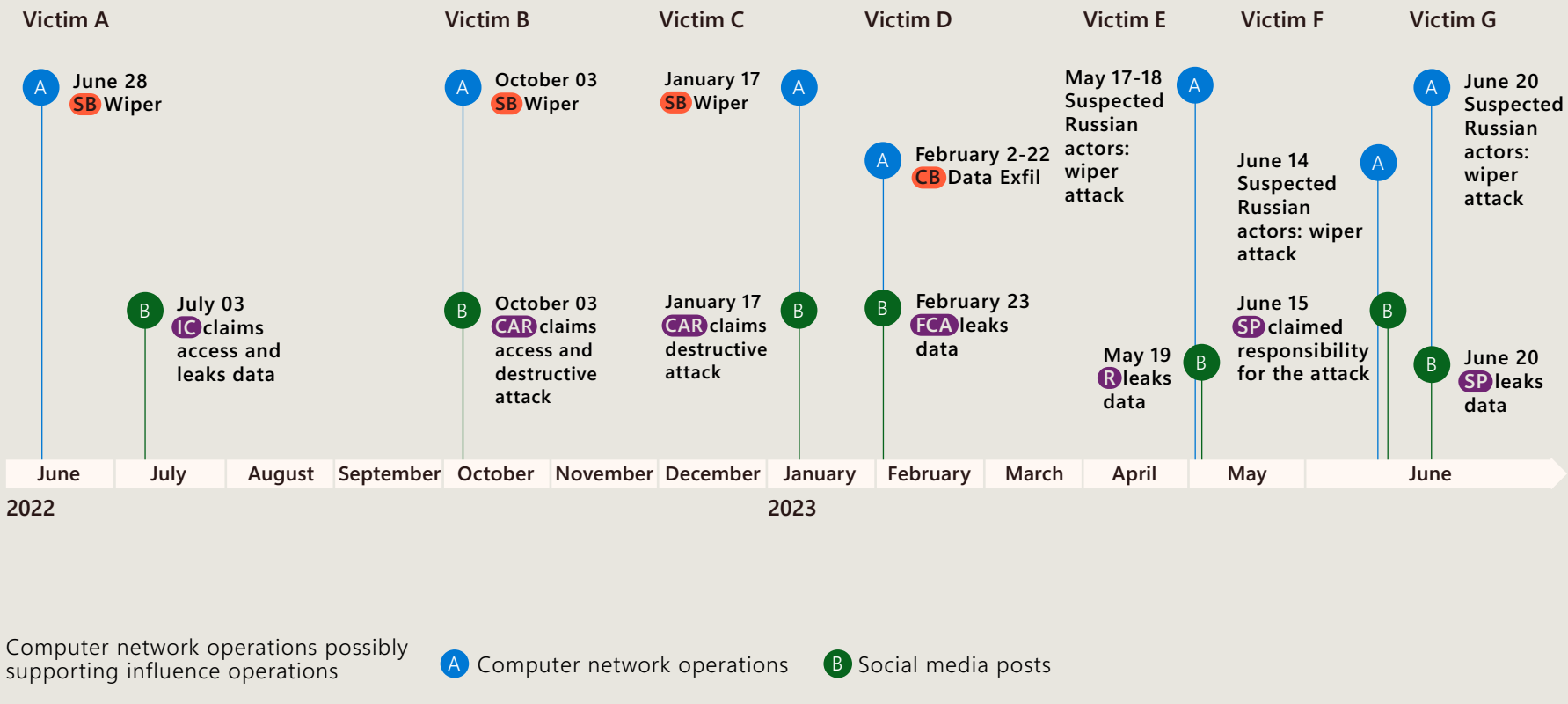
Many of the overlapping data theft, deletion, and leak operations detailed in the timeline were focused on Ukrainian media, transportation, and civilian services organizations. The messaging from the malign influence campaigns often highlighted the alleged involvement of the targeted civilian organizations in supporting Ukrainian military operations.

**Hacktivist personas:**

- IC Info Center
- SP Solntsepek
- R Readovka
- FCA Free Civilian Army
- CAR Cyber Army of Russia

**State actors:**

- SB Seashell Blizzard
- CB Cadet Blizzard




https://t.me/learningnets

**Russia** continued

# Cyber-enabled influence activity targets Ukraine, Poland, and Baltic states

Russia-affiliated threat groups engaging in influence campaigns continue to try to sow distrust between Ukrainian populations and European partners who support Kyiv—both governmental and civilian.

One of the more prominent cyber-enabled influence campaigns targeting populations outside of Ukraine involved a series of operations showing similar TTPs as those used by Storm-0257 (a threat group Microsoft assesses as most similar to Ghostwriter and UNC1151). The campaign appeared aimed at diminishing trust between the Ukrainian diaspora and refugees, Polish, Lithuanian, and Latvian populations, and their governments.

The campaign, which was first observed around mid-January 2023, leveraged email dissemination and inauthentic documents to spread a narrative that government officials may seek forced repatriation of Ukrainians or conscript European citizens for the war in Ukraine. Populations in NATO member states Poland, Latvia, and Lithuania were the primary targets.

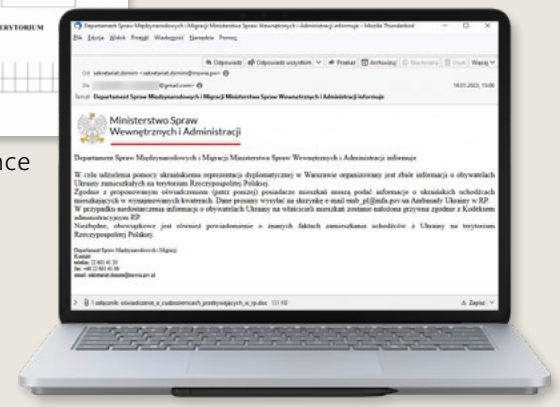
Microsoft's investigation uncovered that one of the documents distributed via email was also tied to a physical flyer posted in Poland, demonstrating that the campaign bridged the digital and physical worlds. The Polish-language, pro-Russia website Dziennik Polityczny, Belarusian state television, and a network of sockpuppet accounts posing as Lithuanian citizens on social media served to further amplify the messages.

### Dissemination tactics in Poland

Real world and digital campaigns converged on Poland, where fliers with a QR code posted throughout Polish cities and attachments in mass email campaigns led to the same document demanding the PII of Ukrainian refugees. Polish civilians received the same message from multiple angles, which likely reinforced its perception as legitimate.

Real world messaging

Real world convergence




Digital world messaging

Source: Microsoft Threat Analysis Center investigations

https://t.me/learningnets

# Influence operations aim to stoke antiwar sentiment in Europe

Source: Microsoft Threat Intelligence Center investigations

As Russia seeks to turn support for Ukraine into a point of conflict between Western populations and their governments, protests are a useful instrument by virtue of their dual role as a tactic to exert influence and a desired result of influence operations.

Russian state-sponsored influence actors, organizations, and outlets have helped amplify, support, and even organize pro-Russian, antiwar protests across Europe. For example, Russia's ruling party, United Russia, has nurtured ties with figures and groups within Italy's pro-Russia, anti-Ukraine war movement,[11] while the Kremlin has tried to influence and steer protests in Germany and forge an antiwar political coalition.[12]

Pro-Russian influence operators have specifically aimed to disrupt Western military support to Ukraine by encouraging European citizens to demonstrate against military assistance.

We assess with moderate confidence that a protest initiative out of Western Europe called "Stop Killing Donbass" is a continuation of an earlier protest initiative known as the "Map of Truth." Both initiatives tried to convince Europeans that Western military aid to Ukraine helps Kyiv kill innocent noncombatants, particularly children, and the two share striking similarities in TTPs, intended audience, involved individuals, and connections to a cluster of obscure websites.

Russian state-sponsored influence actors helped organize pro-Russian, antiwar protests across Europe.

"Map of Truth" was an on-the-ground operation connected to Storm-1099, a large-scale and ongoing network of inauthentic digital activity that was first disrupted by a US social media company in September 2022.[13]

The transition from Map of Truth to Stop Killing Donbass underscores the persistence and flexibility of these influence campaigns, despite repeated Western attempts to obstruct and dismantle such activities and their online assets.

### Additional information

Russia's African coup strategy | Microsoft On the Issues

Extending our vital technology support for Ukraine | Microsoft On the Issues

Preparing for a Russian cyber offensive against Ukraine this winter | Microsoft On the IssuesOn the Issues

Cadet Blizzard emerges as a novel and distinct Russian threat actor | Microsoft Security Blog

Ongoing Russian cyberattacks targeting Ukraine | Microsoft On the Issues

https://t.me/learningnets

# China

**Threat actor naming taxonomy: Typhoon**

Chinese state-sponsored campaigns reflect the Chinese Communist Party's (CCP) dual pursuit of global influence and intelligence collection.

Cyber threat groups continue to carry out sophisticated worldwide campaigns targeting US defense and critical infrastructure, nations bordering the South China Sea, and even China's strategic partners. Some Chinese cyber activity may also indicate possible avenues of response in the event of a future geopolitical crisis. CCP influence operations targeted global Chinese-speaking diaspora populations, leveraged coordinated inauthentic behavior on social media to denigrate US institutions, and promoted a positive image of China through multilingual lifestyle influencers.

**For more information on threat actor naming, see pages 10-11.**

## Cyberespionage targeting the South China Sea

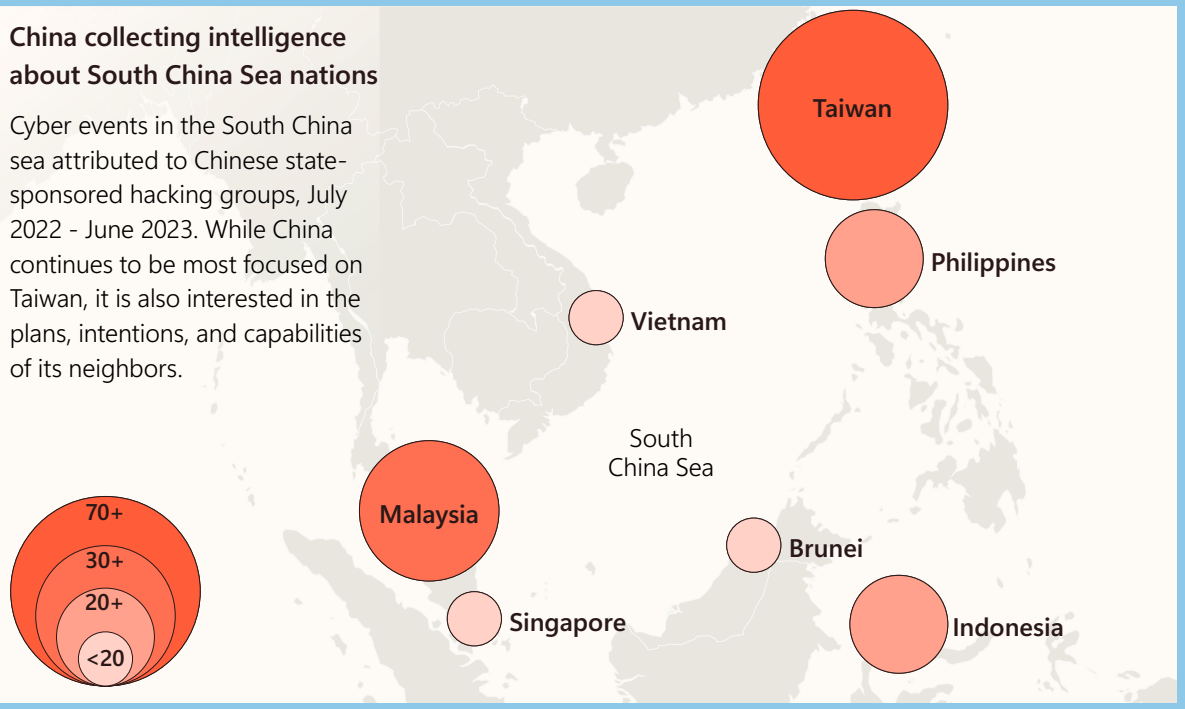
Chinese state-sponsored cyber activity around the South China Sea reflects Beijing's strategic goals in the region and heightened tensions around Taiwan. Much of the targeting appears to be for intelligence collection purposes. The primary Chinese threat groups in the region are Raspberry Typhoon and Flax Typhoon. Raspberry Typhoon targets Association of Southeast Asian Nations government ministries, military entities, and corporate entities associated with critical infrastructure, particularly telecommunications.

Raspberry Typhoon conducts intelligence collection using sophisticated spear-phishing campaigns to land its malware. Since January, the group has persistently targeted ministry-level entities relating to trade, intelligence, and finance.

Flax Typhoon targets Taiwanese critical infrastructure including IT and medical related entities, its defense sector, including contractors that work with the US government, and media entities. Flax Typhoon frequently gathers information about its targets, finds vulnerabilities, and then leverages a custom VPN solution to gain access and maintain persistence in victim networks. These attacks are likely for intelligence collection.

**China collecting intelligence about South China Sea nations**

Cyber events in the South China sea attributed to Chinese state-sponsored hacking groups, July 2022 - June 2023. While China continues to be most focused on Taiwan, it is also interested in the plans, intentions, and capabilities of its neighbors.




Source: Microsoft Threat Analysis Center investigations

### Actionable insights

1. Harden credential storage and processes on devices.
2. Restrict admin mode for remote desktop protocol.
3. Remove PowerShell from systems when not needed. If needed, consider restricting PowerShell execution policy to administrators only.
4. To protect systems against certain malware infections that use scheduled tasks, mark scheduled tasks that start programs in the system's temporary folder %TEMP% as unsafe.

https://t.me/learningnets

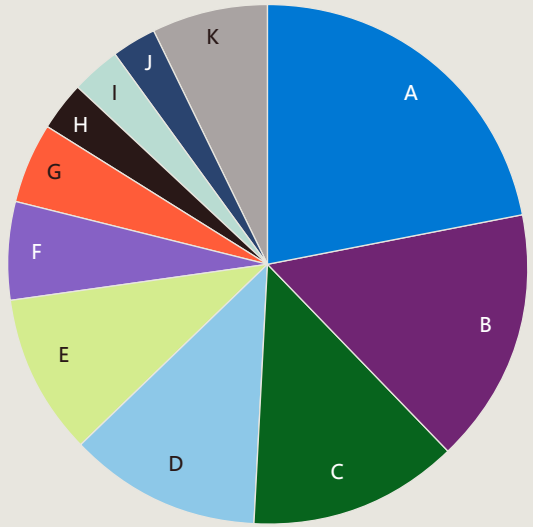
**China** continued

# US defense industrial base and critical infrastructure targeted

Multiple Chinese threat groups including Circle Typhoon, Volt Typhoon, and Mulberry Typhoon targeted the US defense industrial base with different infrastructure and capabilities. Communications infrastructure and defense contractors were among the most frequent targets. These threat groups demonstrated capabilities in resource development, data collection, initial access, and credential access. Circle Typhoon primarily targeted IT entities and US-based defense contractors with VPN appliances, while Mulberry Typhoon targeted a zero-day exploit in US DIB devices for CVE-2022-27518.[14]

**Chinese targeting of US sectors**

Chinese state-sponsored threat actors were broadly interested in US military capabilities and its policymaking during this reporting period.




Source: Microsoft Threat Intelligence

US critical infrastructure saw substantial targeting by Chinese threat actors. The most active of these, Volt Typhoon, targeted communications infrastructure on Guam, likely because it is a key strategic and logistical hub for US military operations in the Pacific and houses a US Navy and Air Force base.[15]

Microsoft has tracked Volt Typhoon conducting critical infrastructure targeting since 2021, including against transportation, utilities, medical infrastructure, and telecommunications infrastructure. These attacks, which often use unobtrusive techniques and originate from compromised Fortinet devices, include many critical infrastructure targets that do not have obvious intelligence collection benefits, such as utilities and transportation entities. These campaigns may be intended to provide China with the capability to disrupt critical infrastructure and communication between the United States and Asia during a geopolitical crisis.

## Actionable insights

1. Detecting activity that uses normal sign-in channels and system binaries requires behavioral monitoring.
2. Enforce strong multifactor authentication (MFA) policies using hardware security keys or Microsoft Authenticator.
3. To prevent unauthorized access, use passwordless sign-in, set expiration dates for passwords, and deactivate unused accounts.
4. Learn more about securing operational technology and industrial control systems beginning on page 103.

https://t.me/learningnets

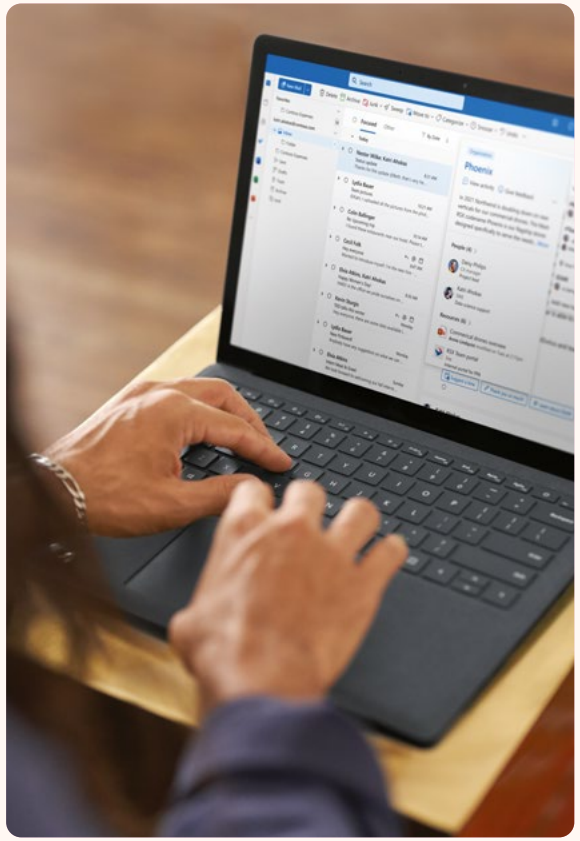
**China** continued

# China-based threat group targets approximately 25 organizations, including US government entities

Beginning May 15, Storm-0558, a China-based threat actor, used forged authentication tokens to access Microsoft customer email accounts of approximately 25 organizations including US and European government entities. Microsoft has successfully blocked this campaign. The objective of the attack was to obtain unauthorized access to email accounts for espionage purposes. In the past, Storm-0558 has targeted US and European diplomatic entities as well as individuals and organizations related to Taiwan and Uyghur geopolitical interests.

**Additional information**

Analysis of Storm-0558 techniques for unauthorized email access | Microsoft Security Blog

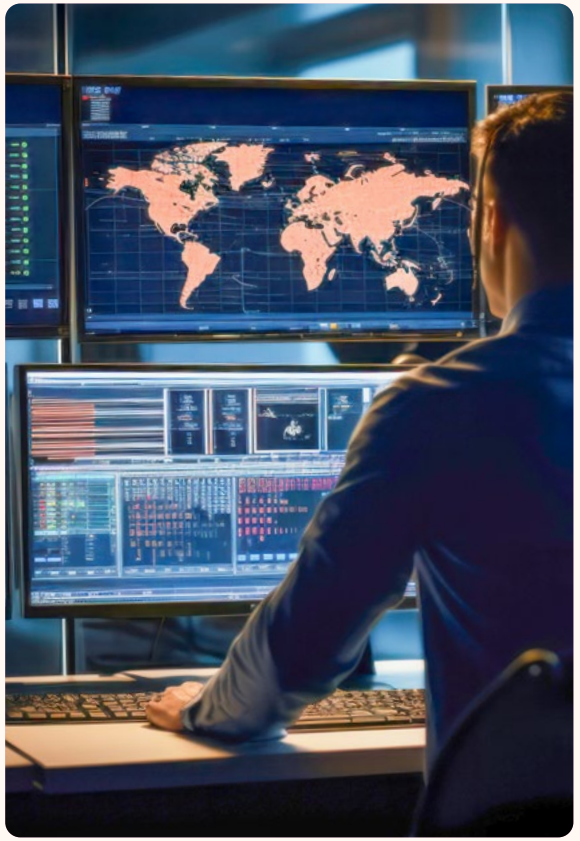


# China's strategic partners are also targets

China also targeted its strategic partners. As China has expanded its global influence through the Belt and Road Initiative (BRI), Chinese cyber threat actors have simultaneously levied cyber operations against private and public entities globally. They often target countries aligned with the CCP's BRI strategy—including Malaysia, Indonesia, and Kazakhstan—and foreign ministries across Europe, Latin America, and Asia to pursue economic espionage or intelligence collection.

**Additional information**

China, North Korea pursue new targets while honing cyber capabilities | Microsoft On the Issues



https://t.me/learningnets

**China** continued

# Influence operations expand their global reach

China continues to improve its influence campaigns, operating at a scale unmatched by other malign influence actors. Chinese-affiliated covert propaganda campaigns deploy thousands of accounts across dozens of websites spreading memes, videos, and articles in multiple languages.

In 2023, Chinese influence operations targeted additional audiences by using new languages and branching out to new platforms. Covert or obfuscated social media accounts launder and amplify the CCP's preferred narratives. One such campaign targeted a Spain-based NGO and deployed over 1,800 accounts with messaging in new languages such as Dutch, Greek, Indonesian, Swedish, and Turkish, and posting on new platforms like Fandango, Rotten Tomatoes, Medium, and Chess.com. This campaign was first observed in January 2022 and is still active.

In online news media, another digital media campaign comprises over 50 Chinese-language news websites that support the CCP's stated goal of being the authoritative voice of Chinese media worldwide. Based on technical indicators, website registration information, duplicate articles, and promoted narratives, these websites bear the hallmarks of a United Front Work Department (UFWD) media strategy targeting the Chinese diaspora globally. More than 30 sites leverage the same application programming interface (API) and content management system, developed by a "wholly-owned subsidiary" of China News Service, the UFWD's media agency.[16] Records from China's Ministry of Industry and Information Technology reveal that this UFWD-affiliated tech company and another have registered at least 14 news sites in this network.[17]

Purporting to be independent news providers, these websites frequently re-publish the same Chinese state media articles, often claiming to be the original source of the content. While the sites broadly cover international news and publish generic Chinese state media-sourced coverage, politically sensitive subjects—such as COVID-19 and Chinese dissidents—overwhelmingly align with the CCP's preferred narratives.

**Map of websites targeting the global Chinese diaspora that are assessed to be part of this media strategy.**

Source: Microsoft Threat Analysis Center investigations

CCP-aligned influence operations have been detected on many platforms and many languages. Content samples from a February 2023 campaign discussing the Nord Stream pipeline explosions reposted identical articles in multiple languages across many websites.

**Platforms**

**Languages**

| | |
|---|---|
| Croatian | Mandarin |
| Dutch | Norwegian |
| English | Slovakian |
| French | Spanish |
| German | Swedish |
| Greek | Thai |
| Indonesian | Turkish |
| Italian | Uyghur |

https://t.me/learningnets

**China** continued

# New techniques are being used to engage audiences

Although Chinese-affiliated actors have long relied on mass-volume, they are becoming increasingly effective at engaging target audiences using evolving techniques. In the lead up to the 2022 US mid-term elections, Microsoft and industry partners detected CCP-affiliated social media accounts impersonating US voters—an unprecedented move in CCP influence operations tactics.[18]

These accounts pretended to be politically conservative or liberal Americans and actively interacted with target audiences by responding to comments made by likely authentic users.

Part of an image shared by Chinese-affiliated actors that bears signs of AI generation, including distorted faces and fingers.

As part of a broad campaign focused on politically divisive topics in the United States, we have observed Chinese-affiliated actors leveraging AI-generated visual media, most likely produced by diffusion-powered image generators. While we have previously seen comics, digital drawings, collages, and stock photos being used, AI-generated images have been more successful in driving audience engagement. Audiences frequently repost these visuals despite common indicators of AI-generation—for example, more than five fingers on a person's hand.

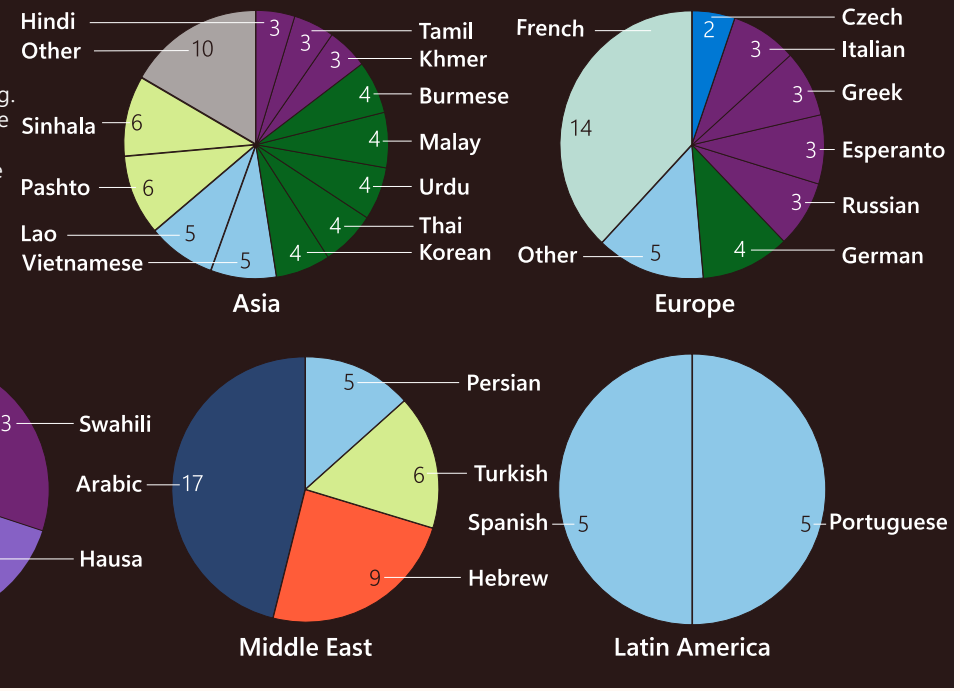
In a separate campaign, the CCP has poured resources into state-backed "multilingual internet celebrity studios" (多语种网红工作室) in recent years.[19] Comprising over 230 state media employees who masquerade as social media influencers, this effort leverages the power of authentic voices and video content.

Recruited, trained, promoted, and funded by China Radio International and other Chinese state media outfits, influencers spread localized CCP talking points that achieve meaningful engagement with target audiences around the world, reaching a combined following of at least 103 million people

**Chinese state media influencers breakdown by language grouping**

Social media influencers target seven audience spaces (language groupings) worldwide that are separated into geographic regions. No charts shown for English or Chinese-language audience spaces.

These charts show numbers of influencer profiles by language grouping. Each influencer profile features real people employed by Chinese state media to tell China's story on social media.




Source: Microsoft Threat Analysis Center investigations

across multiple platforms and speaking at least 40 languages.[20] Influencers speaking Asian languages other than Chinese—such as Hindi, Sinhala, Pashto, Lao, Korean, Malay, and Vietnamese—comprise the largest group, while English-speakers make up the second-largest. The geographic distribution of languages spoken by these state-affiliated influencers represents China's growing global influence and regional prioritization.

https://t.me/learningnets

# Iran

**Threat actor naming taxonomy: Sandstorm**

Some Iranian state actors have enhanced their offensive cyber capabilities, while others combine low sophistication attacks with multi-pronged influence operations for greater geopolitical effect. Iranian cyber and influence operations have turned firmly against the West and what it perceives as efforts by Western powers to foment unrest inside Iran. At the same time, Tehran has continued its pivot towards the East, including in the coordination of influence operations with Russia.

**For more information on threat actor naming, see pages 10-11.**

We detected increasingly global targeting by Iranian groups, particularly in the Global South. Iranian cyber operations increased across the board, with greater persistence against countries of most interest to Tehran and expanding into enterprises in Southeast Asian, African, Latin American, and European countries, particularly in Eastern and Southern Europe.

**Chart 1 – Iranian targeting July 2021-June 2022**

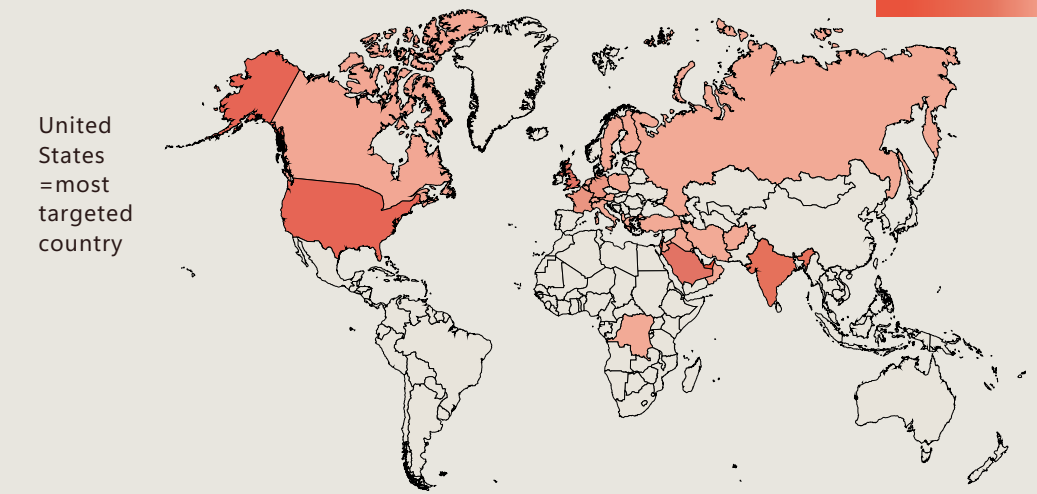
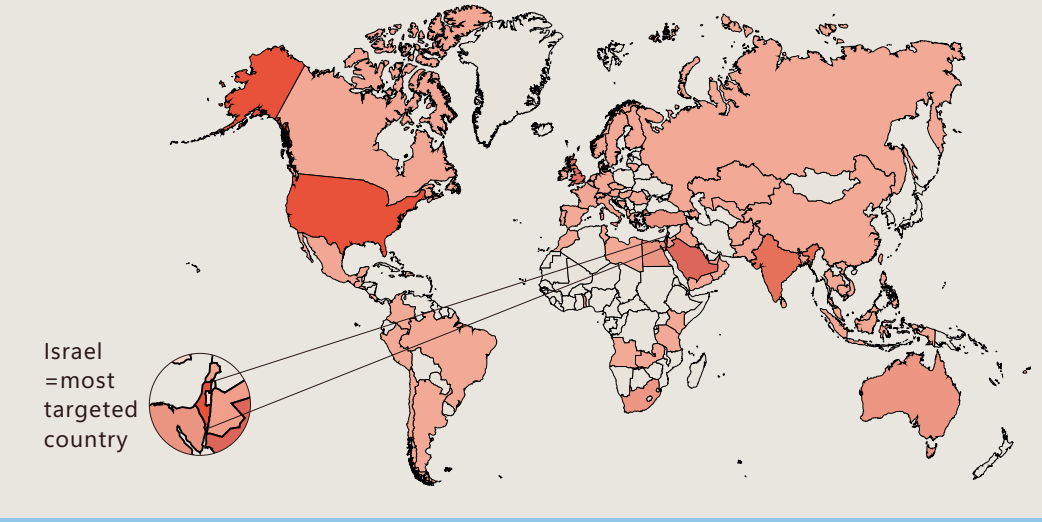



**Chart 2 – Iranian targeting July 2022-June 2023**




https://t.me/learningnets

**Iran** continued

# Advancing offensive cyber capabilities

Iranian state actors used increasingly sophisticated tradecraft, enhancing operations in cloud environments, rolling out an increasing number of custom implants, and becoming faster at exploiting newly released vulnerabilities.

### Migrating components of targeting and operations to the cloud

We have observed multiple Iranian state actors migrating components of their targeting and operations to the cloud.

- In February, destructive operations enabled by Mango Sandstorm, a group linked to Iran's Ministry of Intelligence and Security, impacted both on-premises and cloud environments. Prior to the attack, Iranian state actors moved laterally from an on-premises to a cloud environment by manipulating the Azure Active Directory Connect agent using stolen credentials of highly privileged accounts.[21]
- In March, Islamic Revolutionary Guard Corps (IRGC)-linked Peach Sandstorm conducted a GoldenSAML attack to leverage a compromise of an on-premises network to pivot to the victim's cloud environment to exfiltrate data.
- In separate intrusions early in 2023, Peach Sandstorm maintained persistence using Azure Arc—a platform that allows users to manage resources deployed both within and outside of Azure through the same control plane.
- The TTPs observed in Peach Sandstorm's intrusions represent a significant increase in the maturity of its capabilities, growth that is especially notable following a two-year period during which we observed very little activity linked to these operators.

### Regular use of custom tooling

We observed Iranian state actors regularly using custom tools in their operations. These tools provided capabilities in establishing persistence, evading detection, and credential theft. The use of previously unseen malware helps threat actors stay a step ahead of defenders, requiring defenders to identify new tools, develop and deploy corresponding signatures or detections, and keep pace with actors' evolving arsenal of options.

- Between late 2022 and June 2023, we observed Mint Sandstorm using MischiefTut, a custom backdoor implemented in PowerShell with a set of basic capabilities.[23] MischiefTut can run reconnaissance commands, write outputs to a text file, and download additional tools on a compromised system.
- In early 2023, Mango Sandstorm sent phishing emails to employees of telecommunications and government organizations in, or with ties to, countries in the Middle East. The group used remote monitoring and management tools to retain access to compromised environments. In at least one case, they used a custom credential stealer to siphon users' credentials.
- In June, Pumpkin Sandstorm used the custom dropper BellaCiao to deliver tools to organizations. Because BellaCiao can be used to deliver various tools, post-compromise activity varies based on the operators' decisions. In at least one intrusion, we observed operators stealing credentials from an infected system. We assess that known BellaCiao samples have been specifically configured to target specific organizations located in Afghanistan, Austria, Azerbaijan, Canada, Egypt, France, Greece, India, Italy, Lebanon, the Philippines, and the United Kingdom.

### GoldenSAML attack chain

In a golden SAML attack, an adversary will steal private keys from a target's on-premises Active Directory Federated Services (ADFS) server to mint a Security Assertion Markup Language (SAML) token trusted by a target's Office 365 environment.[22]

Source: Microsoft Threat Analysis Center investigations

https://t.me/learningnets

**Iran** continued

### Exploiting new vulnerabilities more rapidly

We increasingly observed a subgroup of an Iranian state actor, Mint Sandstorm, rapidly weaponizing N-day vulnerabilities in common enterprise applications.[24] An N-day vulnerability is a flaw in software for which an official patch or security update has been released. Until 2023, this subgroup—which we assess is linked to the intelligence arm of the IRGC—was slow to adopt exploits for recently-disclosed vulnerabilities with publicly reported proof of concept (POC) code, often taking several weeks to successfully weaponize exploits for vulnerabilities like Proxyshell and Log4Shell. Beginning this year, we observed a notable decrease in the time it took to adopt and incorporate public POCs. Mint Sandstorm operators exploited vulnerabilities in applications such as Zoho ManageEngine, Aspera Faspex, and Adobe ColdFusion within days of their initial disclosure.

### Additional information

Microsoft Defender External Attack Surface Management | Microsoft

Move Active Directory Federation Services apps to Azure AD | Microsoft

### Actionable insights

1. Harden internet-facing assets and identify and secure perimeter systems that attackers might use to access your network.
2. Secure internet-facing remote desktop protocol services behind a multifactor authentication gateway. If you don't have an MFA gateway, enable network-level authentication and ensure that server machines have strong, randomized local admin passwords.
3. Keep backups so you can recover data affected by destructive attacks.
4. Treat identity servers as critical infrastructure, protecting them with the same protections you would apply to a domain controller or other critical security infrastructure.

## Preferring cyber-enabled influence operations

While some Iranian state actors were honing the sophistication of their tradecraft on network, other state-sponsored groups supplemented basic cyberattacks with a new playbook: leveraging cyber-enabled influence operations to fuel geopolitical change in alignment with Tehran's objectives.

In the second half of 2022, Iranian groups increased the pace of operations in which they amplify low sophistication cyberattacks with multi-pronged influence operations. Iranian groups' use of a repeatable playbook and low-effort cyberattacks—requiring little to no access to a victim network-enabled them to quickly replicate their operations, shifting from one victim to the next.

Iran's cyber-enabled influence operations have pushed narratives that seek to bolster Palestinian resistance, sow panic among Israeli citizens, foment Shi'ite unrest in Gulf Arab countries, and counter the normalization of Arab-Israeli ties.

While specific narratives varied, the underlying goal was often the same. Tehran likely sought to retaliate against what it perceived were efforts by foreign actors to foment unrest in Iran, including highly sophisticated cyberattacks in 2021 and 2022 by a group called Predatory Sparrow against Iran's steel factories, state broadcasts, gas stations, and trains.[25]

https://t.me/learningnets

**Iran** continued

# Firmly turning against the West

While Iran's most common targets—the United States and Israel—remain at the top of its list, Iran has broadened its targeting of the West, particularly its cyber-enabled influence operations to target European NATO member states.

In France, a cyber persona calling itself "Holy Souls," assessed to be linked to Iranian state actor Cotton Sandstorm, targeted French satirical magazine Charlie Hebdo in January.[26]

The cyber-enabled influence operations against Albania marked Iran's first destructive attack directly targeting a NATO-member government.

It posted for sale on a leak site a trove of data reportedly containing the names and addresses of 230,000 Charlie Hebdo customers, likely in retaliation for Charlie Hebdo publishing cartoons that ridiculed Iranian Supreme Leader Ali Khamenei.

The previously mentioned cyber-enabled influence operations against Albania[27] marked Iran's first destructive attack directly targeting a NATO-member government. The persona has continued to leak tranches of emails from several high-profile Albanian government organizations, including the Ministry of Foreign Affairs in May.

Following the outbreak of nationwide anti-government protests in Iran in September 2022, Tehran likely directed its security services to work against the same Iranian expatriates that Iranian state cyber actors set their sights on following the election of hardline President Ebrahim Raisi in 2021.

# Targeting journalists and political activists

In the weeks after the outbreak of protests in 2022, Mint Sandstorm sent protest-themed emails to individuals and groups the actor likely perceived were linked or sympathetic to protests. Previously, since mid-2021, Mint Sandstorm has targeted Iranian expatriate human rights and women's rights activists, scholars, and journalists, often through spear-phishing campaigns masquerading as researchers soliciting input or commentary on a recent geopolitical event or development.

At the same time, since September 2022 Iran has also likely waged a cyber-enabled influence campaign to target and harass prominent Iranian oppositionists who shed light on protests and sought to counter Iran's state-controlled attempts to manipulate the narrative and suppress protests. Iran likely sought to undercut the momentum of nationwide protests by leaking information intended to embarrass prominent regime opposition figures or to expose their "corrupt" relationships.

A cyber persona we assess operates on Iran's behalf, "Adll Ali" (عدل علی), began its first influence campaign seeking to counter the narrative surrounding Mahsa Amini's death, which sparked nationwide protests. It attempted to pin the blame on the Komala Party, an Iranian Kurdish separatist group that Iran considers a terrorist group, through documents it claimed to have acquired from a cyber operation against the group. Adll Ali later sought to expose hypocritical or salacious activities of Iranian opposition figures. For example, it leaked embarrassing videos and pictures of Reza Pahlavi, the eldest son of Iran's former monarch, and his family.

https://t.me/learningnets

**Iran** continued

# Pivoting towards the East

Iranian and Russian state media outlets have a history of cooperation, including multiple formal memorandums of understanding and media cooperation agreements. Coordination between Iranian and Russian state media increased after the Russian invasion of Ukraine, leading to a convergence of narratives relating to the invasion and Iranian protest movements in 2022.

In October 2022, a leak of thousands of emails from Iran's English-language news outlet, PressTV,[28] revealed Iranian state media executives' travel to Moscow in 2019 to establish media cooperation agreements. It also revealed correspondence between Russian and Iranian state media officials to coordinate messaging in September 2020, and sharing of content and correspondents since at least 2020.

These agreements enable the two countries to support each other on controversial issues. For example, while Iran has declared its "neutrality" regarding the conflict in Ukraine, Iranian state media has largely defended Russia's position, including the verbatim use of Russian disinformation such as accusations of the United States establishing offensive biolabs in Ukraine. Additionally, PressTV has embedded a reporter with Russian troops in the Russian-occupied Donetsk region of Ukraine. Multiple Iranian Islamic Republic of Iran Broadcasting media officials contribute to Russian state media, including Sputnik's Persian language website.

Coordination between Iranian and Russian state media increased after the Russian invasion of Ukraine.

# Outsourcing influence operations to engage international audiences

Iran has increasingly outsourced influence operations to proxy outlets and journalists who present themselves as independent. In addition to operating numerous state-run outlets targeting foreign audiences in English, Arabic, and other languages, Tehran heavily supports pro-Iranian media outlets abroad that can more easily connect to international audiences.

Iran also uses its militant proxy and partner organizations like Hezbollah in Lebanon and the Iraqi Popular Mobilization Units (PMUs) to disseminate Iran-aligned propaganda via their affiliated outlets. For example, Al-Mayadeen, a popular Lebanon-based multilingual news outlet, claims to be funded by independent businessmen; however, the outlet maintains close leadership and business ties to Iranian and Hezbollah figures.

Sabereen News, which posts primarily on Telegram to an Iraqi audience, is another Iran-backed outlet run from abroad. The outlet is run by Iraq's Iran-backed PMUs and was reportedly created by Iran's Islamic Radios and Televisions Union—the "propaganda arm" of Iran's IRGC Quds Force. The outlet largely focuses on local Iraqi issues but has also promoted Russian propaganda and has claimed to conduct cyber operations against foreign and domestic targets.

https://t.me/learningnets

# North Korea

**Threat actor naming taxonomy: Sleet**

We observed an increase in the sophistication of North Korean cyber operations and targeting overlaps among North Korean threat actors.

**For more information on threat actor naming, see pages 10-11.**

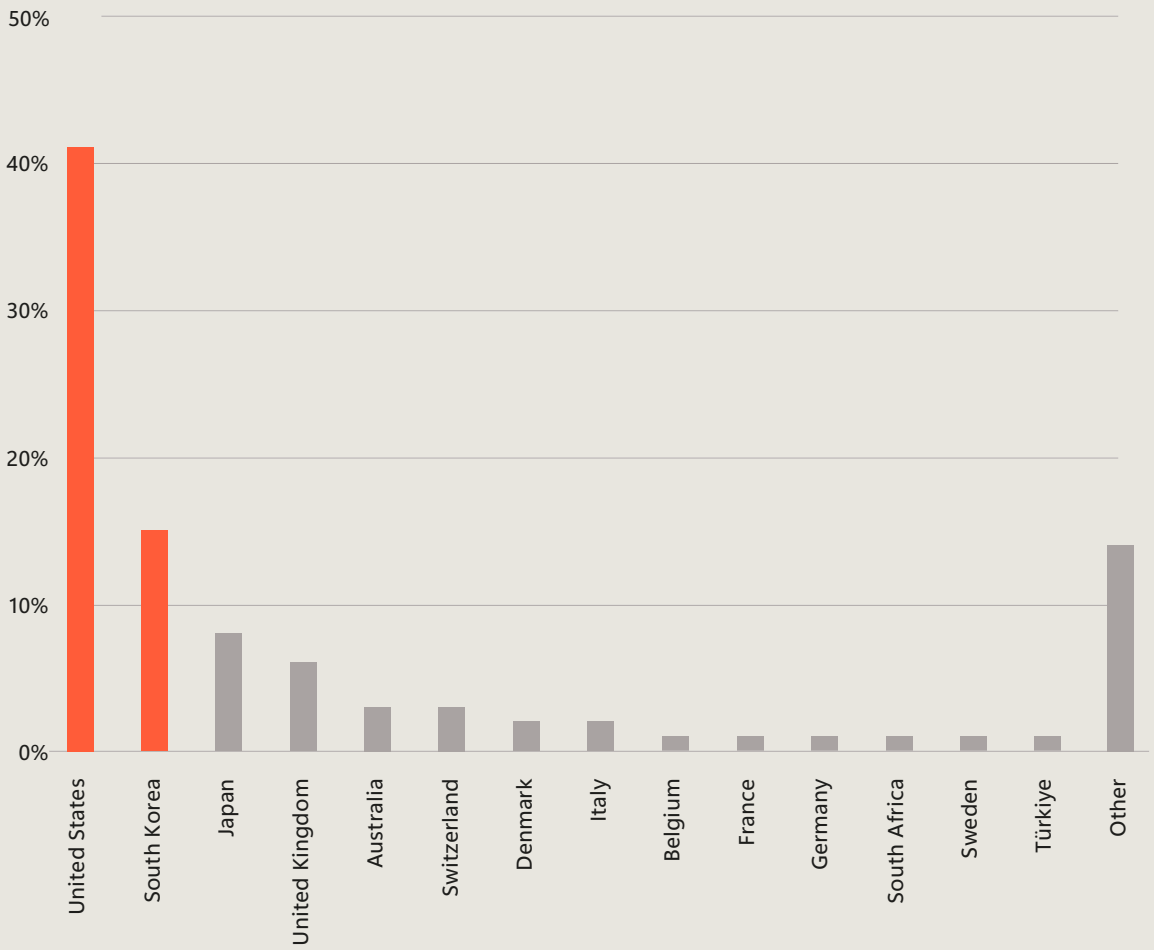
## Cyber actors help fund North Korea's nuclear and missile program

North Korean leader Kim Jong Un's main priorities include expanding the country's weapons arsenal and countering the state's perceived adversaries: the United States, South Korea, and Japan.[29] North Korea test-launched a record number of missiles in 2022. As the US government estimates cyber operations now fund approximately half of North Korea's weapons program, that means Pyongyang's hackers are working harder than ever to cover growing military expenditures.[30]

In support of its goals, North Korean cyber threat actors pursue cyber operations to collect intelligence on the policy plans of these adversaries, gather intelligence about other countries' military capabilities to improve their own, and steal cryptocurrency to fund the state.

**Countries most targeted by North Korean state-sponsored threat actors**

Unsurprisingly, the US and South Korea comprise over 50 percent of North Korea's cyber focus.



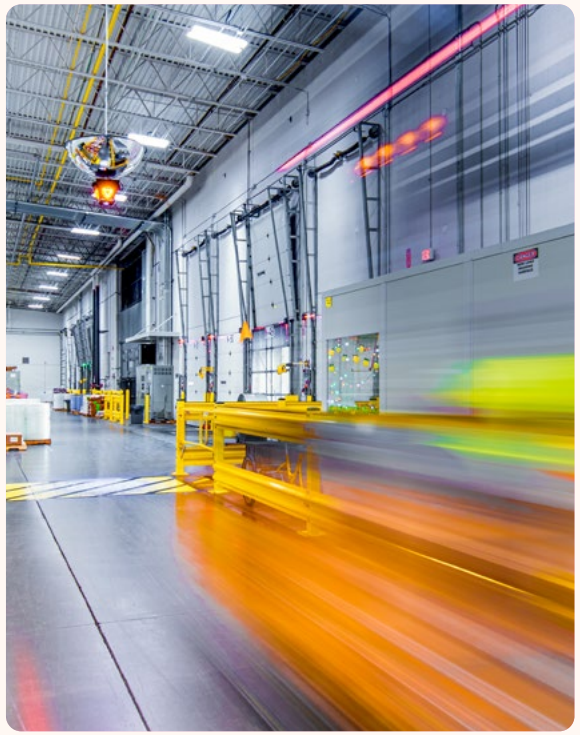

Source: Microsoft Threat Intelligence events data

https://t.me/learningnets

**North Korea** continued

# More sophisticated cryptocurrency theft and supply chain attacks

North Korean actors continued to steal cryptocurrency with greater sophistication, and conducted the first supply chain attack Microsoft has observed among these groups. In January 2023, the Federal Bureau of Investigation (FBI) publicly attributed the June 2022 heist of $100 million in cryptocurrency from Harmony's Horizon Bridge to North Korean cyber actors. Microsoft attributed this activity to Jade Sleet, which we estimate has stolen approximately $1 billion in cryptocurrency so far.[31] As mentioned earlier in the chapter (see page 47), Microsoft attributed the March 2023 3CX supply chain attack—which leveraged a prior supply chain compromise of a US-based financial technology company in 2022—to Citrine Sleet. This was the first time we have observed an activity group using an existing supply chain compromise to conduct another supply chain attack.[32]



### Actionable insights

1. Patch vulnerabilities as early as possible.
2. Block the malicious C2 domains in your environment and investigate for any connections to them.
3. Encourage end users to practice good credential hygiene.

# Weaponizing open-source software and impersonating legitimate institutions

North Korean actors are employing new techniques to exploit victims. Diamond Sleet weaponized legitimate open-source software including PDF readers and Virtual Network Computing (VNC) clients to conduct attacks.[33] After Microsoft Threat Intelligence published a blog revealing these TTPs in September 2022, it shifted to develop new malware approaches in its weaponized software malware.

Emerald Sleet continues to send frequent spear-phishing emails to Korean Peninsula experts around the world for intelligence collection. In many instances, we found that Emerald Sleet impersonates reputable academic institutions and NGOs to lure victims into replying with insights and commentary about foreign policies related to North Korea rather than deploying malicious files or links to malicious websites.

In addition to email, North Korean actors conduct phishing via social media on platforms like LinkedIn. Sapphire Sleet created fake LinkedIn profiles masquerading as financial investors to lure blockchain-related targets to other platforms like Telegram, where it then delivered malicious files. Ruby Sleet also operated fake LinkedIn profiles to heavily target a defense company and cybersecurity company in Israel. Microsoft Threat Intelligence partnered with LinkedIn Threat Prevention & Defense to restrict the profiles associated with these malicious activities.

### Actionable insights

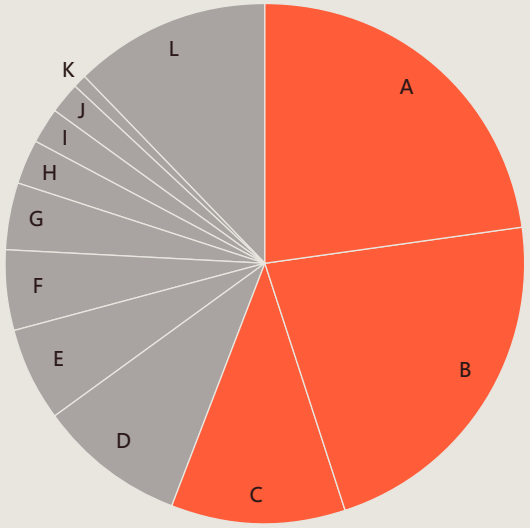
1. Educate end users about preventing malware infections, such as ignoring or deleting unsolicited and unexpected emails or attachments sent through instant messaging applications or social networks.
2. Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.
3. Educate end users about protecting personal and business information in social media, filtering unsolicited communication, identifying lures in spear-phishing email and watering holes, and reporting reconnaissance attempts and other suspicious activity.

https://t.me/learningnets

**North Korea** continued

**Most targeted sectors by North Korea**

North Korea is particularly interested in spying on institutions and individuals that study North Korea itself.




- A 23% Think tanks/ NGOs
- B 22% Education
- C 11% Government
- D 9% Finance
- E 6% Inter-Government Organization
- F 5% IT
- G 4% Media
- H 3% Defense Industry
- I 2% Manufacturing
- J 2% Transportation
- K 1% Food, Agriculture
- L 12% Other

Source: Microsoft Threat Intelligence nation state notifications

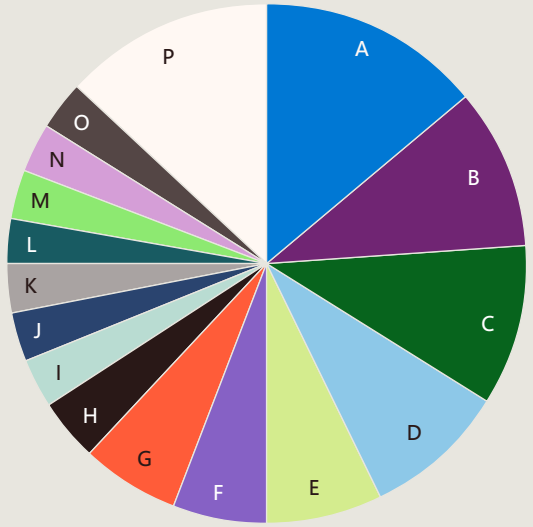
# Targeting defense companies, especially in Europe

We observed greater overlaps in the industries targeted by North Korean threat actors. Three North Korean threat actors—Ruby Sleet, Diamond Sleet, and Sapphire Sleet—targeted organizations in the maritime and shipbuilding sector from November 2022 to January 2023.

Ruby Sleet and Diamond Sleet even targeted the same organizations within these sectors. We had not previously observed this level of industry and targeting overlaps, suggesting maritime technology research was a high collection priority for the North Korean government.

We observed a second instance of shared targeting when Ruby Sleet and Diamond Sleet compromised two arms manufacturing companies based in Germany and Israel from November 2022 to January 2023. This suggests the North Korean government is assigning multiple cyber groups to meet high-priority collection requirements to improve the country's military capabilities. Since January 2023, Diamond Sleet has also compromised defense firms in Brazil, Czechia, Finland, Italy, Norway, and Poland.

**North Korea targeting of national defense industries**




- A 14% Russia
- B 10% United States
- C 10% Israel
- D 9% Germany
- E 7% India
- F 6% Africa
- G 6% South Korea
- H 4% Türkiye
- I 3% Brazil
- J 3% Czechia
- K 3% Finland
- L 3% France
- M 3% Italy
- N 3% Poland
- O 3% Norway
- P 13% Other

Source: Microsoft Threat Intelligence nation state notifications

# Targeting Russian entities for intelligence collection

While North Korea provides materiel support for Russia's war in Ukraine in exchange for food, North Korean cyber actors are also targeting Russian nuclear energy, defense industry, and government entities, likely for intelligence collection.[34] In May 2023, Diamond Sleet used a trojanized VNC client to compromise a Russian nuclear energy organization. In March 2023, Ruby Sleet compromised a Russian aerospace research institute, while Onyx Sleet compromised a device belonging to a Russian university, and an attacker account likely attributed to Opal Sleet sent phishing emails to accounts belonging to Russian diplomatic government entities. North Korean threat actors may be capitalizing on the opportunity to conduct intelligence collection on Russian entities while Russia is distracted by the war.

https://t.me/learningnets

# Palestinian threat actors

In early 2023, we observed a wave of activity from a Gaza-based group that we track as Storm-1133 targeting Israeli private sector energy, defense, and telecommunications organizations.

We assess this group works to further the interests of Hamas, a Sunni militant group that is the de facto governing authority in the Gaza Strip,[35] as activity attributed to it has largely affected organizations perceived as hostile to Hamas.

Targets have included organizations in the Israeli energy and defense sectors and entities loyal to Fatah, the dominant Palestinian political faction in the West Bank,[36] which were historically targets of Hamas cyberattacks.[37]

**For more information on threat actor naming, see pages 10-11.**

We observed Storm-1133 attempting to compromise third party organizations with public ties to Israeli targets of interest. Storm-1133 demonstrated new techniques to evade detection while continuing to send tailored phishing messages on social media. Throughout 2023, we observed Storm-1133 attempting to deliver backdoors, including a configuration that allows the group to dynamically update the C2 infrastructure hosted on Google Drive. This technique enables operators to stay a step ahead of certain static network-based defenses. Storm-1133 also used newly created LinkedIn profiles—masquerading as Israeli human resources managers, project coordinators, and software developers to conduct reconnaissance, contact and send malware to employees at Israeli defense, space, and technology organizations throughout 2023.

https://t.me/learningnets

# The emerging threat posed by cyber mercenaries

Cyberspace is an increasingly contested area for conflict and strategic rivalries among states. However, the development and maintenance of offensive cyber capabilities is costly and labor-intensive, demanding skills many countries lack or cannot maintain.

This has led to the emergence of cyber mercenaries or private sector offensive actors—commercial actors that are known/legitimate legal entities that create and sell cyberweapons to customers, often but not always governments, who select targets and operate the cyberweapons.

While the employment of cyber mercenaries may seem attractive to some countries as a means of adding to their arsenal, the unchecked expansion of the mercenary marketplace threatens to severely destabilize the broader online environment. The Carnegie Endowment for International Peace has identified at least 74 governments that have contracted firms to gain spyware and digital forensics technology.[38] The explosive growth of this market poses a real threat to democracy and the overall stability and security of the online environment.

**150+**

companies partnering to collectively push back on the cyber mercenary market

Microsoft tracks cyber mercenary actors located all over the globe. An important goal in Microsoft publicly discussing our research is to have a material impact on the cyber mercenary landscape, and there have been several notable recent developments. We publicly identified a threat actor we refer to as Carmine Tsunami and which we believe was an Israeli company, QuaDream. Together with security researchers from CitizenLab, we tracked the software suite it sold that consisted of exploits, malware, and infrastructure designed to exfiltrate data from mobile devices. CitizenLab identified at least five civil society victims, including journalists, political opposition figures, and a non-government organization (NGO) worker, in North America, Central Asia, Southeast Asia, Europe, and the Middle East.[39] Furthermore, it was able to identify operator locations for QuaDream systems around the world, including: Bulgaria, Czechia, Hungary, Ghana, Israel, Mexico, Romania, Singapore, the United Arab Emirates, and Uzbekistan. As a result of Microsoft and Citizen Lab's reports, QuaDream shut down and stopped its operations in 2023. DSIRF, an Austrian cyber mercenary tracked by Microsoft as Denim Tsunami, has also recently shut down.

We believe it is critical to work with others to address this emerging threat. Others in the technology industry have seen additional actors, employed by these and other governments, try to undermine the security of the online environment. This is why we have partnered with the over 150 companies that make up the Cybersecurity Tech Accord, as well as Google and Apple, to collectively push back on the cyber mercenary market by committing to a set of industry principles[40] aimed at limiting the threats posed by these groups (see page 124).

As the technology industry builds and maintains the majority of what we consider "cyberspace," we as an industry have a responsibility to curb the harm caused by cyber mercenaries. At a high level, signatories commit to:

- Take steps to counter cyber mercenaries' use of products and services to harm people.
- Identify ways to actively counter the cyber mercenary market.
- Invest in cybersecurity awareness of customers, users and the general public.
- Protect customers and users by maintaining the integrity and security of products and services.
- Develop processes for handling valid legal requests for information.

Progress can happen only through strong multistakeholder partnerships with governments—the primary users of these types of groups—that prioritize cybersecurity by committing to rules that restrict the use of cyber mercenaries and increase accountability and oversight for both providers and their clients. We were pleased to see the Biden Administration take first steps with its Executive Order to Prohibit US Government Use of Commercial Spyware that Poses Risks to National Security and the follow-on Guiding Principles on Government Use of Surveillance Technologies supported by 44 Summit for Democracy participating states. Similarly, in Europe, comprehensive investigations and set of recommendations by the European Parliament should be heeded.

### Additional information

Britain sounds alarm on spyware, mercenary hacking market | Reuters

Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security | The White House

Guiding Principles on Government Use of Surveillance Technologies | US Department of State

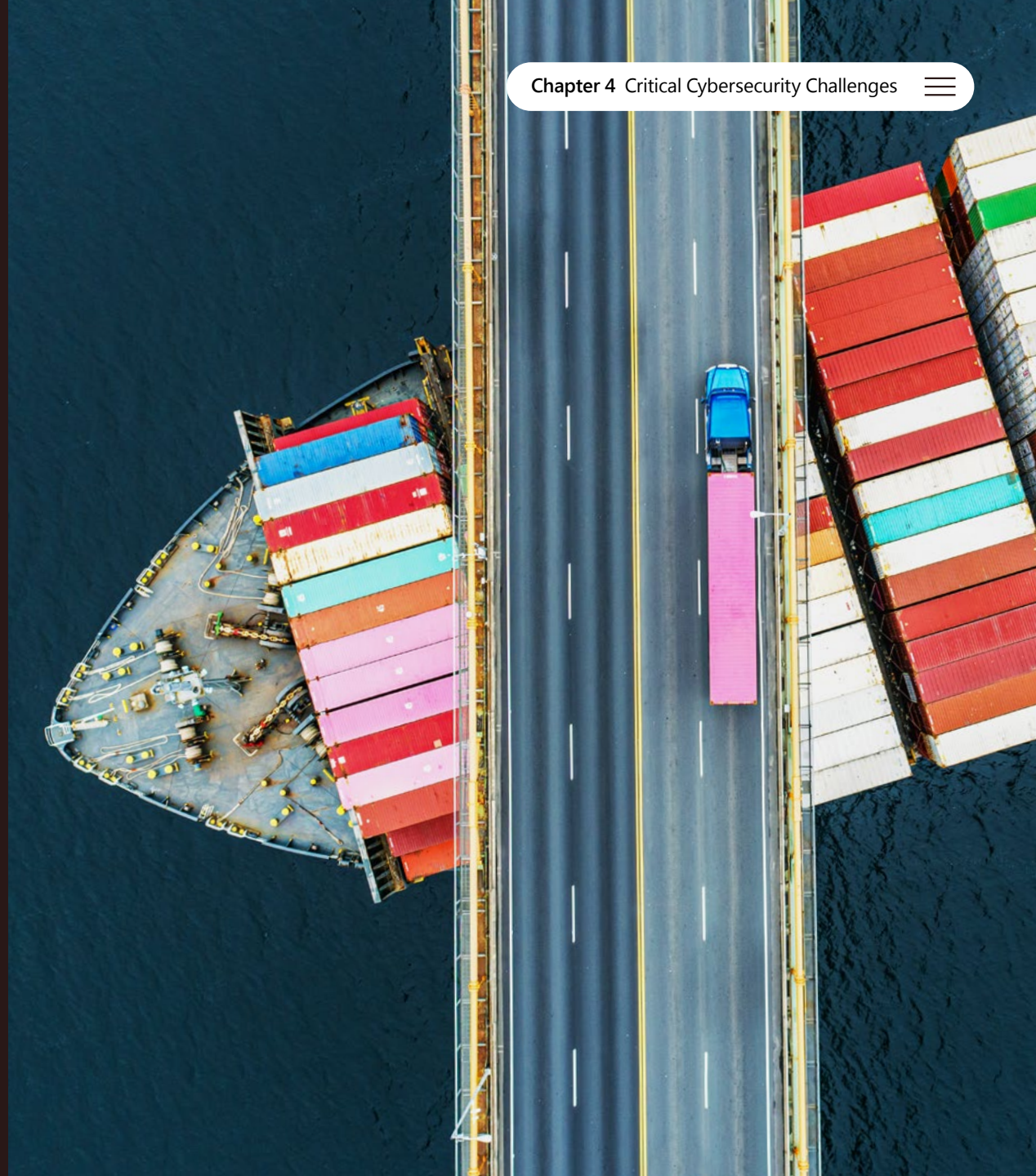
Spyware: MEPs sound alarm on threat to democracy and demand reforms | European Parliament

https://t.me/learningnets

# Chapter 4
# Critical Cybersecurity Challenges

## Charting a path forward


| | |
|---|---|
| Key developments | 76 |
| Introduction | 77 |
| The state of IoT and OT security | 78 |
| Improving global critical infrastructure resilience | 86 |
| Innovating for supply chain resilience | 90 |



https://t.me/learningnets

Critical Cybersecurity Challenges

# Key developments

Growing attacks on the highly vulnerable intersection of information technology and operational technology (IT-OT) emphasize the importance of a comprehensive defense strategy that covers the entire business ecosystem.

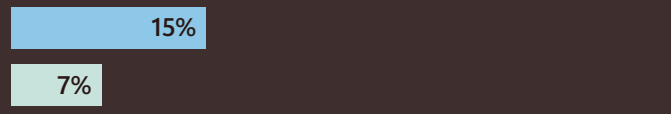
While nation-state actors were previously the main perpetrators of critical infrastructure attacks, the ease of entry for malicious actors has led to a surge in threats to OT. This calls for a more comprehensive security approach. Unmanaged devices in critical infrastructure pose a significant vulnerability, making it crucial to address the problem of unsupported operating systems in OT devices.

46%

Of the 78% of IoT devices with known vulnerabilities on customer networks, 46% cannot be patched.

25%

of OT devices on customer networks use unsupported systems.




Find out more on page 79

15

We discovered 15 new zero-day vulnerabilities in the CODESYS runtime,

**highlighting the significant risks associated with not addressing supply chain vulnerabilities to ensure the security of critical infrastructure and systems.**

Find out more on page 84

Attacks targeting open source software have grown on average

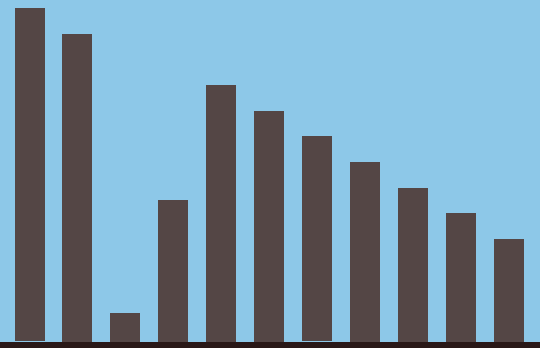
742%

since 2019.[7]

Find out more on page 93

57%

of devices on legacy firmware are exploitable to a high number of CVEs (>10).



Find out more on page 81

https://t.me/learningnets

# The imperative for holistic security strategies

## Introduction from Michal Braverman-Blumenstyk

As we navigate the ever-changing landscape of cybersecurity threats, it is clear that a new approach to defense is imperative for ensuring resilience.

Gone are the days when organizations can rely on isolated efforts at defense within their own environments. Today's attacks on the intersection of information technology and operational technology (IT-OT) emphasize the importance of a comprehensive defense strategy that covers the entire business ecosystem.

To achieve this, organizations must ensure interoperability between their IT and OT security systems, connecting telemetry and insights from all areas of the business to gain a comprehensive security view. A holistic security strategy is crucial to safeguard against threats to the internet of things (IoT), supply chains, and critical infrastructure. In the quest for a stronger defense, AI can be a valuable co-pilot–particularly in areas requiring specialized expertise like IoT/OT security. AI can bridge knowledge and resource gaps, significantly enhancing an organization's security posture and enabling it to effectively thwart attacks.

The stakes are high when it comes to critical infrastructure. In recent years, threats targeting these networks have increased, as have their far-reaching consequences, which include disruptive events, financial losses, and even danger to human lives. Defending against these attacks presents a complex challenge due to the intricate nature of OT networks, which often consist of legacy systems and encompasses diverse protocols, devices, and architectures, making them inherently challenging to secure and monitor effectively.

Past attacks on critical infrastructure were predominantly attributed to nation-state actors, given the complexity involved and limited commercial knowledge in this domain. However, we are seeing a notable shift as the accessibility of OT test beds and protocols lowers the entry barrier for malicious actors, resulting in an increase in off-the-shelf malware targeting IoT/OT devices. This has effectively opened the door for new threats to critical infrastructure.

The increasing interconnectivity between IoT/OT networks, critical infrastructure, and the outside world is fueled by digital transformation trends and the potential advantages they offer to businesses. However, this trend, coupled with the absence of secure design principles and device security in current OT networks, as well as the lack of robust supply chain security in some supply chains (which may involve the use of open-source and insecure components), presents significant risks to businesses.

Despite the challenges, organizations are improving their cybersecurity by investing in advanced technologies like AI and machine learning to augment their security teams. They're also collaborating with industry partners to share information and raise awareness of emerging threats. By working together and taking a comprehensive approach to cybersecurity, organizations can better safeguard their operations and ensure resilience against evolving threats.

**Michal Braverman-Blumenstyk**
Corporate Vice President, Chief Technology Officer, Microsoft Security

https://t.me/learningnets

# The state of IoT and OT security

IoT/OT security has undergone significant changes. Initially, systems were air-gapped, specialized, and isolated, which made them less attractive targets for attacks. However, as industrial systems started to connect with enterprise IT systems, the approach shifted towards greater network connectivity.

This transformation brought about new security guidelines, heavily influenced by the Purdue model aimed at mitigating the risks associated with increased interconnectedness.[1]

In recent years, there has been a notable move towards centralized security in response to the growing complexity and diversity of assets within organizations.

This shift in approach acknowledges that OT is just one component of a broader ecosystem of unmanaged devices, encompassing IoT, OT, building management systems, and internet of medical things device technologies.

This recognition has paved the way for the development of new categories of IoT/OT security solutions such as deception, supply chain security, firmware analysis, and managed security services.

These emerging solutions aim to address the evolving challenges and threats posed by the interconnected nature of these devices, ensuring comprehensive protection across the entire ecosystem.

### The expanding role of Chief Information Security Officer

The role of Chief Information Security Officer (CISO) has undergone a remarkable transformation as it expands beyond the traditional focus on securing information and users. Today, CISOs are entrusted with protecting all aspects of the connected business, including digital assets and cyber-physical and operational domains. The CISO's responsibility extends to safeguarding critical infrastructure, IoT/OT systems, and ensuring the continuity of operational processes. This expanded role reflects the growing recognition that cybersecurity must address the holistic protection of the entire business. In an era where the convergence of the digital and physical realms demands comprehensive security strategies and a deep understanding of the cyber-physical landscape, the CISO plays a pivotal role in the organization's resilience and success.

https://t.me/learningnets

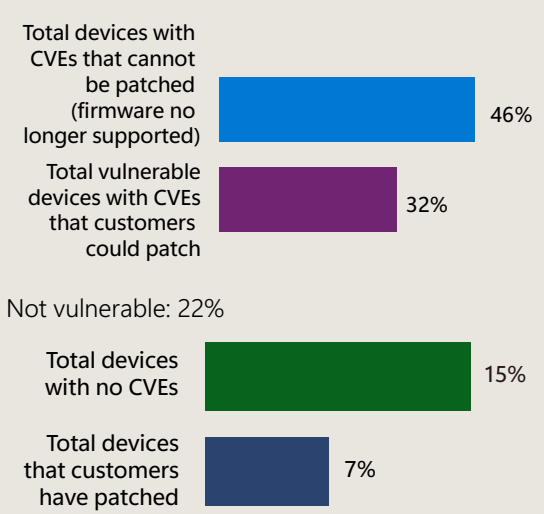
# Vulnerable devices susceptible to compromise

OT and industrial control system devices are frequently left unpatched and exposed, making them easy targets for hackers. Patching these systems can be challenging for organizations, as updates may need to be postponed to avoid disrupting operations.

Additionally, some OT devices lack patches for vulnerabilities, often due to discontinued support. Hackers can exploit vulnerable OT devices by using internet search tools to find ports used for remote management and gain unauthorized access, often using default credentials.

It is vitally important to know the status of your devices and to take steps to protect them from potential attacks.

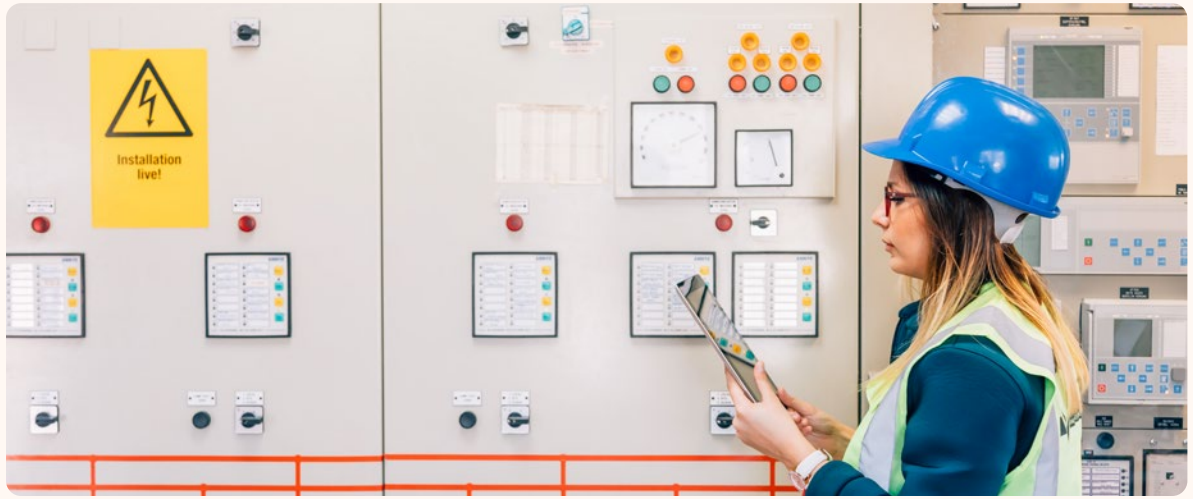
**Device vulnerabilities in industrial control networks**




Source: Microsoft Defender for IoT sensors

25%

of OT devices on customer networks use unsupported operating systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats.




Microsoft Defender for IoT actively monitors critical infrastructure device security to stay ahead of emerging threats. However, recent data reveals that 78% of devices on customer networks have known vulnerabilities that threat actors can exploit, and 46% of these devices cannot be patched.

Some OT devices still use unsupported operating systems, such as Windows 2000, which are no longer receiving security patches from Microsoft. Twenty-five percent of OT devices on customer networks use unsupported systems, making them more susceptible to cyberattacks due to a lack of essential updates and protection against evolving threats. This allows threat actors to exploit known vulnerabilities in unsupported OT devices, posing significant risks to critical infrastructure and industrial processes.

Pr Cybersecurity Tech Accord principles mapping index **page 124**

**Actionable insights**

1. Gain deeper visibility into IoT/OT devices and prioritize them based on their risk to the enterprise if compromised.
2. Reduce the attack surface by eliminating unnecessary internet connections, open ports, and restricting remote access using VPN services.
3. Ensure devices are robust by applying patches, changing default passwords, and modifying default SSH ports.

https://t.me/learningnets

# Missing security patch deployment leaves systems vulnerable

Balancing robust cyber hygiene with uninterrupted operations in industrial and critical infrastructure environments is complex. One of the key challenges lies in effectively managing timely patch updates while maintaining peak system performance. This delicate equilibrium demands careful consideration, as overlooking the importance of cyber hygiene can leave vital systems vulnerable to malicious actors seeking to exploit weaknesses.

To examine how this balance is managed across a variety of programmable logic controllers (PLCs), we started by using Defender for IoT's on-premises network sensors to identify OT assets on a network, including vendor, model, and firmware version. Our focus was on a collection of widely used PLCs within the Defender for IoT customer base to determine the distribution of firmware versions deployed on the devices. To investigate device vulnerabilities, we partnered aDolus Technology, a supply chain security company that uses machine learning algorithms to analyze manufacturer and industry disclosures and identify CVEs (publicly disclosed cybersecurity vulnerabilities) present in firmware.[2]

We found a significant lag between the availability of security fixes in firmware and their deployment onto the OT network. Although many of the PLC models showed a marked reduction in high confidence exploitable CVEs from older versions to the newest versions, over 60 percent of devices were still running older versions of the firmware with eight or more exploitable CVEs. If the latest version of the firmware available for these PLC models were to be deployed, the number of devices with no known exploitable CVEs would increase from four to 40 percent.

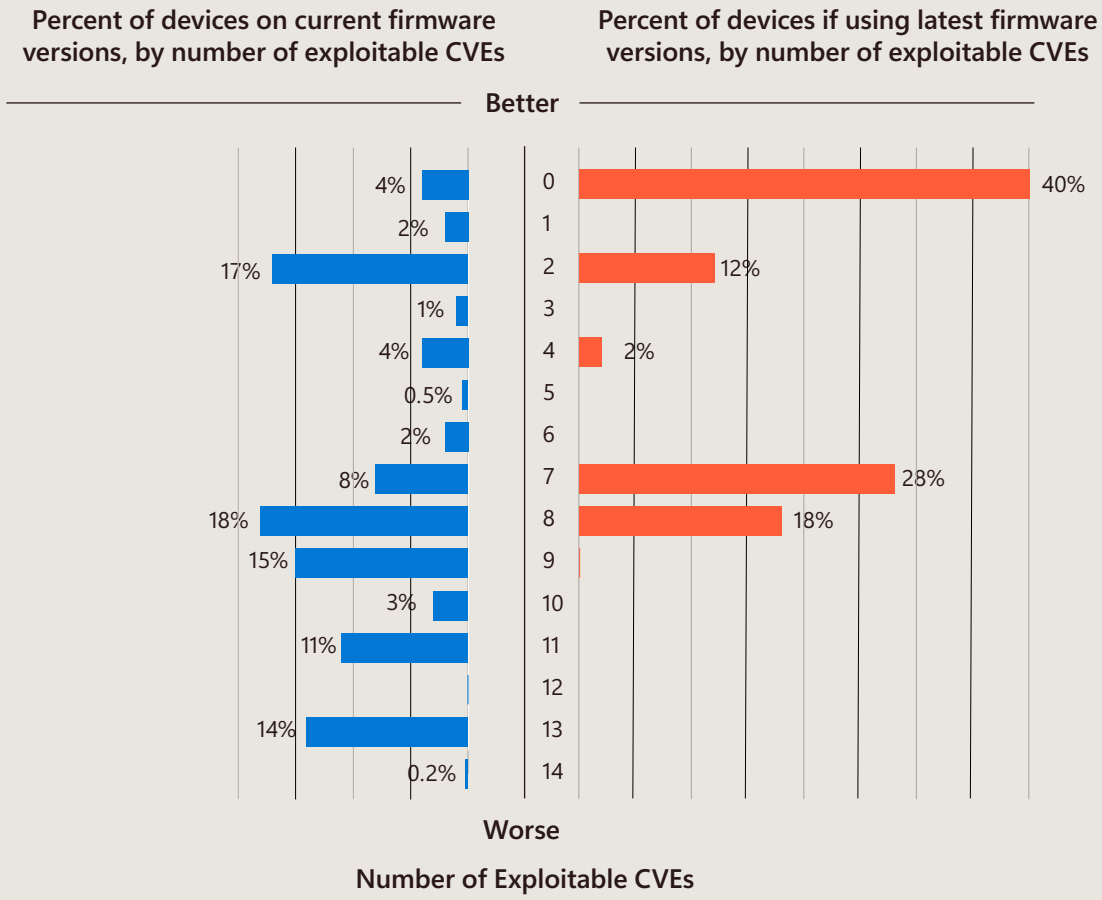
There are valid reasons for the delay in some devices receiving patches. Unlike traditional IT devices with regular "patch Tuesday" updates, OT devices have years-long patch cycles. It is not as simple as rebooting a PLC on the spot, especially when it manages a process that requires high availability. However, most facilities typically have annual or bi-annual maintenance outage windows that will allow for patching.

Deploying the latest firmware versions available for these PLC models could increase the percentage of devices with no known exploitable CVEs from

**4-40%**

**OT common vulnerabilities and exposures (CVEs)**

More than 60 percent of devices are on firmware versions that expose the devices to eight or more exploitable CVEs, even when some patches have been available for over five years.




Source: Microsoft Defender for IoT and aDolus Technology

https://t.me/learningnets

**The state of IoT and OT security** continued

Another problem may be that a patch is limited because only specific versions of firmware have the necessary certifications. As an example, SIL2 Safety Certification can be legally required when a PLC is used to control a hazardous process, but not every firmware release for a given model has SIL2 certification.

Considering these limitations, we looked at how long security patches have been available. Many were released years ago, including patched versions that were fully safety certified. A significant number of devices running vulnerable firmware have had patches available for more than eight years. Even with the unique constraints of the OT environment, these delays underscore the need for industry to decrease the time between security patch release and deployment.

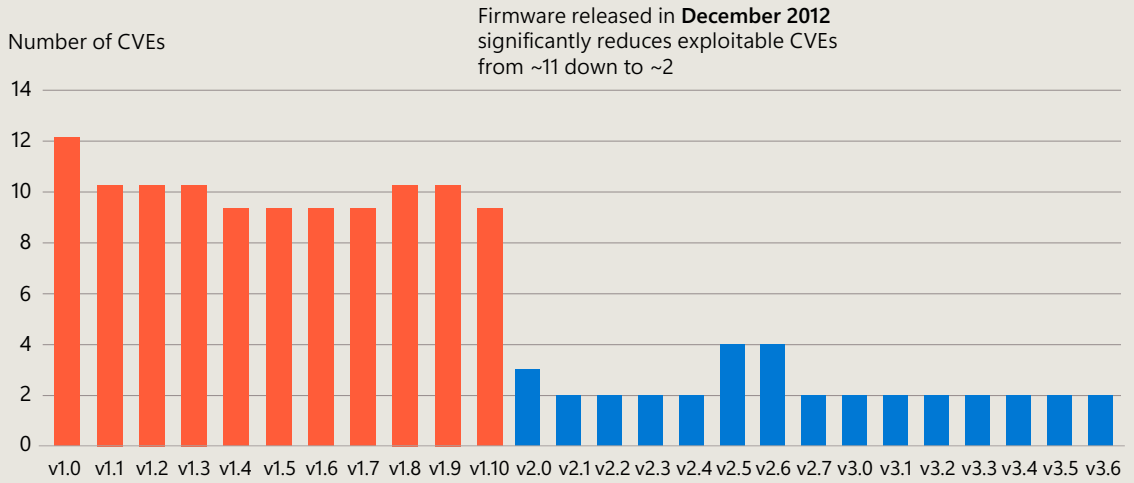
### Actionable insights

1. Implement robust network monitoring within OT environments, paying attention to abnormal behavior that may indicate malicious activity.
2. Use firmware scanning tools to identify and mitigate potential security weaknesses in high-risk devices.
3. Adopt IoT management in the cloud to benefit from standard governance models, reliable patching, broad monitoring, and continued security investment.

More than 50 percent of devices use firmware versions exposing them to more than 10 CVEs even though firmware significantly reducing exploitable CVEs has been available for **more than 10 years**

57%

of devices on legacy firmware are **exploitable to a high number of CVEs** (>10)




### Additional examples

| Device | Percent of devices on legacy firmware exploitable to a high number of CVEs (>10) | Last firmware release date significantly reducing exploitable CVEs (<3) | Delay in firmware update |
|---|---|---|---|
| Device A | 56% | December 2012 | ~10.5 years |
| Device B | 48% | December 2012 | ~10.5 years |
| Device C | 55% | August 2014 | ~8.7 years |

Source: Microsoft Defender for IoT and aDolus Technology

## Call to action

**The significance of maintaining a comprehensive OT patch management system cannot be overstated.** While strides have been made to identify and address vulnerabilities within devices powering manufacturing lines and critical infrastructure, this is insufficient. Achieving true resilience necessitates the implementation of a holistic approach to OT risk management which encompasses asset visibility, patch levels, vulnerability monitoring, and the availability of updates.

Though the prospect of interrupting essential processes or requiring recertification may be daunting, the potential consequences of leaving exploitable vulnerabilities unchecked pose a far greater risk, potentially jeopardizing lives and wreaking havoc on critical systems. Organizations must recognize the imperative nature of a robust OT patch management system as an essential component of their overall cybersecurity strategy.

https://t.me/learningnets

**The state of IoT and OT security** continued

# Defending and strengthening air gapped networks

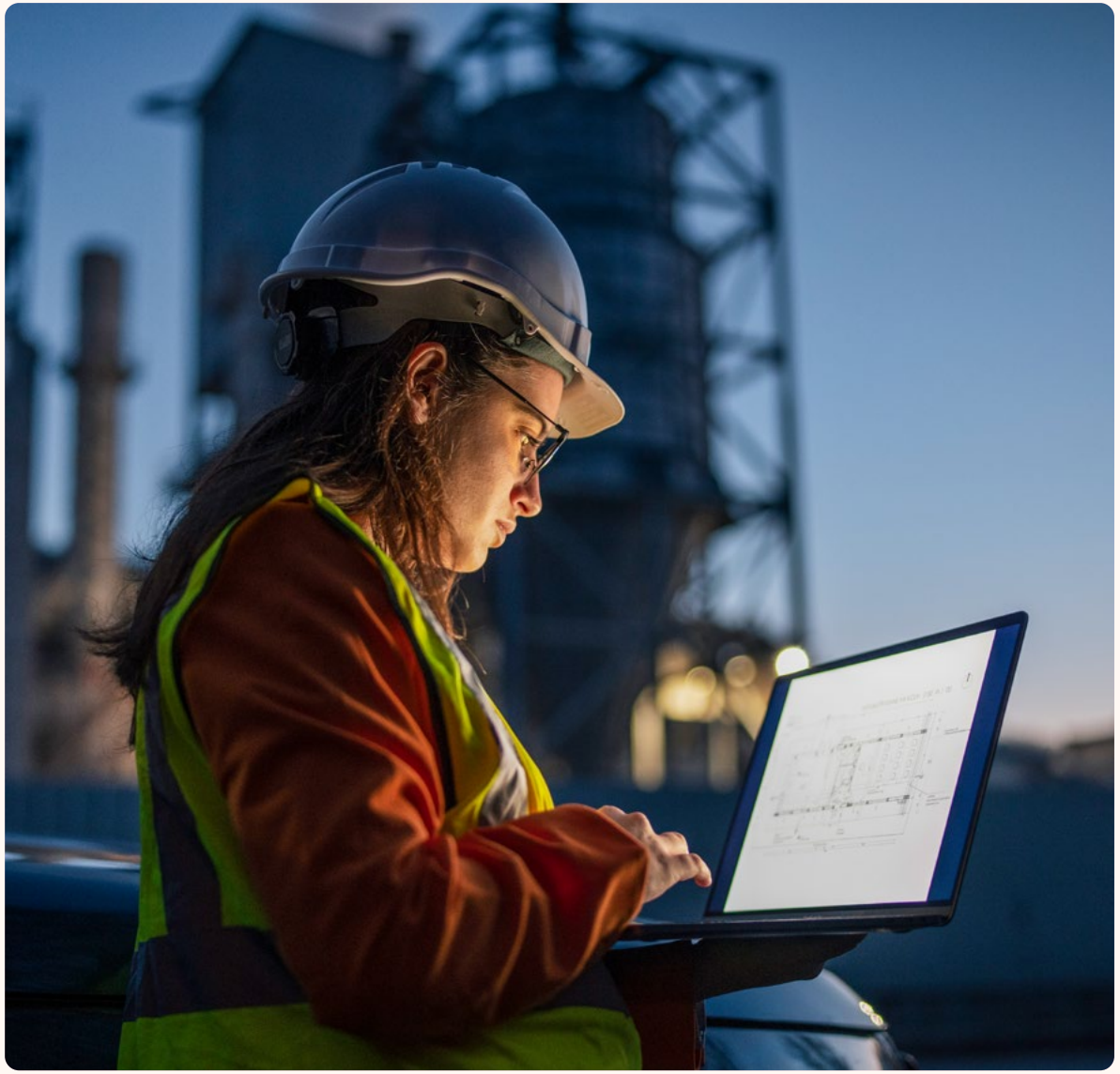
As organizations implement digital transformation programs, it's crucial to monitor and discover inventory in networks that were previously thought to be air gapped.

This is because air gaps are no longer enough to protect networks from malicious attacks, as attackers can use various methods to gain access. Therefore, organizations must extend their monitoring and inventory discovery beyond air-gapped networks to ensure their networks are secure and up to date with the latest technologies and security protocols.

Business critical systems consist of numerous assets, some of which are unknown or unmanaged by operations and security teams. With the increasing attack surface of networks, it's essential for organizations to detect and manage these unknown and unmanaged assets. This helps ensure that networks remain secure and up to date, reducing the risk of malicious attacks. Asset profiling enables end-to-end discovery of assets by analyzing network signals to identify and categorize network assets, the information collected about them, and the types of assets they represent.

A vast collection of classifiers allows for high-fidelity categorization in the cloud, including servers, workstations, mobile devices, and embedded IoT/OT devices.

Properly classifying assets enables organizations to monitor and analyze potential security risks. Any vulnerability or misconfiguration in an asset can create an entry point for attackers, making it critical to protect an organization's networks.



https://t.me/learningnets

# Supply chain risks posed by embedded software

Vulnerabilities can occur at any stage of a device's lifecycle, from design to distribution, and can have serious consequences for critical infrastructure. As organizations increasingly rely on devices to manage processes, streamline operations, and provide infrastructure, potentially insecure supply chains pose a significant risk.

One of the biggest concerns with device supply chain risks is the use of third-party components within the deployed software and hardware in OT and industrial control system (ICS) networks. These components may not be visible to organizations and can pose a significant threat to networks, particularly those that have not properly isolated devices according to best practice guidelines.

Outdated software development kits (SDKs) and system-on-a-chip (SoC) components in devices present a significant risk. SoCs are used to manage a variety of computational processes and are often operated by outdated SDKs that implement essential processes. These components can be hidden from network administrators and pose a serious threat to networks when left unpatched. Updating the firmware of IoT devices does not always fix vulnerabilities in these components, and it is often difficult to determine if they can even be updated.

### Boa web server highlights the risks

In November 2022, Microsoft researchers identified the Boa web server as a component on indicators of compromise in an attack on critical infrastructure. Despite being discontinued in 2005, it is still widely used in many IoT devices and popular SDKs.

We found over one million internet-exposed Boa web servers worldwide during our investigation. Our research revealed that 10 percent of similar incidents were related to critical industries, such as the petroleum industry and associated fleet services. Many of the IP addresses were associated with IoT devices that had additional unpatched critical vulnerabilities, making them an accessible attack vector for malware operators. Attackers can exploit vulnerabilities in the Boa web server to gain access to networks and collect sensitive information from files before moving laterally in the network or initiating additional attacks on a device.

The vulnerabilities in the Boa web server are well-known and documented, and academic training modules even teach individuals how to exploit them, lowering the barrier for a successful attack. However, many people are unaware that their devices use the outdated server or that the server is built into their network devices and shipped directly from vendors. Firmware updates and patches may not address the issue as the update may need to be issued by a chain of vendors that may not have visibility into its inclusion.

It is crucial to apply available patches as soon as available, and isolate IoT devices from networks with OT and ICS.

https://t.me/learningnets

**The state of IoT and OT security** continued

### CODESYS vulnerabilities affect hundreds of vendors

Last year, we reported on the Incontroller framework, a modular attack toolkit that can penetrate OT networks and attack devices. This highly customizable framework applies to popular PLC protocols, reducing the attacker's research lead time to attack OT and critical infrastructure. The toolkit can issue commands to change configurations, manipulate outputs, implant backdoors, issue vulnerabilities, upload ladder logic, and initiate DoS attacks.

Our research on the Incontroller framework found a module that could crash a specific vendor's PLC. We also discovered 15 new zero-day vulnerabilities in the CODESYS runtime during our extensive CODESYS SDK research.[3] CODESYS is a platform-independent software framework used for programming PLCs, and its widespread use across various industries highlights significant risks associated with supply chain vulnerabilities in the OT industry. With over 500 manufacturers supporting architectures spread across millions of devices worldwide, the potential impact of these vulnerabilities is significant.

OT networks often lack key security measures and are directly connected to the network, making them an easy target for attackers. This can lead to significant disruption of critical infrastructure, as even one disconnected component can impact manufacturing lines and operations managed by PLCs. A vulnerable version of CODESYS could enable threat actors to shut down operations of critical infrastructure through a denial-of-service attack. Remote code execution could create a backdoor for devices, allowing attackers to tamper with operations, cause a controller to run dangerously, or steal critical information.

500+

manufacturers supporting architectures spread across millions of devices worldwide

#### Actionable insights

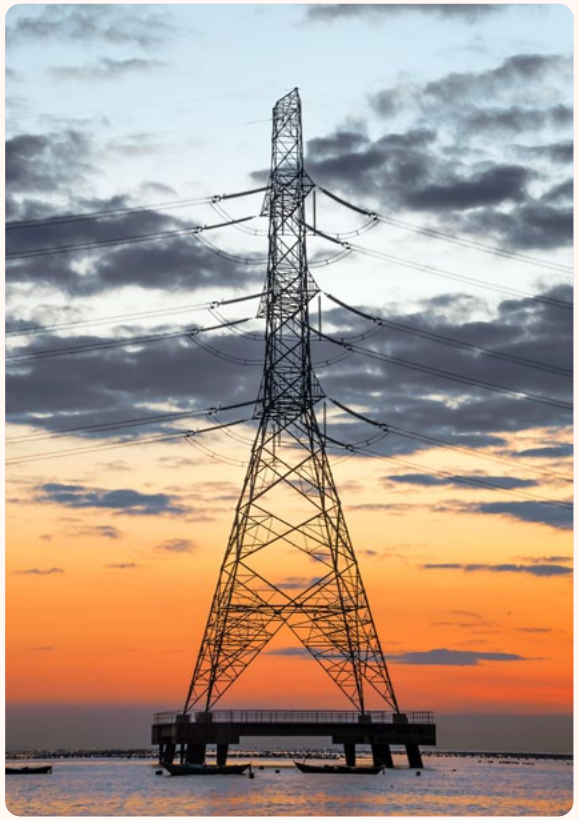
1. Proactively assess ICS infrastructure and implement high-security segmentation for critical infrastructure.
2. Segment networks to limit lateral movement and isolate IoT devices and OT networks from corporate IT networks using firewalls.
3. Protect engineering stations by implementing endpoint detection and response (EDR) solutions.
4. Proactively conduct incident response measures for OT networks.
5. Influence IoT/OT device security by requiring vendors to adopt secure development lifecycle best practices. A software bill of materials (SBOM) is a way that vendors can provide more information about the third-party components contained in their software and hardware.

#### Additional information

Multiple high severity vulnerabilities in CODESYS V3 SDK could lead to RCE or DoS | Microsoft Security Blog

Analyze IoT/OT device firmware with Microsoft Defender for IoT | Microsoft

Firmware analysis for device builders – Microsoft Defender for IoT | Microsoft



https://t.me/learningnets

**The state of IoT and OT security** continued

# Creating a unified front

Bringing OT and IT security teams together creates a unified front against evolving threats, maximizing resources while pinpointing vulnerabilities.

A converged security operations center (SOC) combines the strengths of two teams, resulting in a streamlined, cost-effective approach to enterprise security. OT and IT security teams can work together to build cohesion through tabletop exercises that establish common goals and performance indicators.

In the last year, customer security teams have made great strides in developing tools and strategies to share knowledge between defenders. These advancements have enhanced teams' preparedness and effectiveness in responding to security threats.

**Additional information**

Better together webinar with Microsoft Sentinel and Microsoft Defender for IoT | Microsoft

**Some examples of implementation are:**

- Tools for tracking security events and sharing data.
- Platforms enabling real-time communication and collaboration.
- Processes and frameworks such as incident response playbooks and knowledge sharing protocols.

**Converged SOCs offer these benefits:**

1. **Improved collaboration:** Develop your team's ability to identify and respond to threats using both IT and OT skills, allowing you to gain a deeper understanding of their potential impacts.
2. **Greater visibility:** You can gain an understanding of your organization's vulnerabilities on both the business and industrial side. Afterward, take proactive steps to prevent a breach.
3. **Streamlined response:** Reduce response times by eliminating incidents being transferred between IT and OT teams. A quick and effective response to security incidents will minimize the potential damage.
4. **Strengthened compliance:** Make sure all areas of the business comply with industry regulations and standards by sharing knowledge and expertise easily.

https://t.me/learningnets

# Improving global critical infrastructure resilience

Digital transformation is driving economic growth and prosperity across all sectors, delivering better services at lower costs and powering critical infrastructure such as electricity, finance, and transportation. But as we have seen, the digitalization of our world has brought new risks as sophisticated, dangerous cyber actors seek to exploit key vulnerabilities.

The US Intelligence Community has warned that China and Russia are both capable of disrupting critical infrastructure services,[4] and Microsoft has identified campaigns that support these goals. In May, we warned that Chinese hackers were trying to gain access to US critical infrastructure as part of prepositioning an ability to disrupt communication in case of a future geopolitical crisis.[5]

**To learn more, see page 112.**

In November, we assessed that Russian state actors were likely behind the Prestige ransomware attacks on transportation and logistics companies in Ukraine and Poland.[6]

**For more about these attacks, see page 48.**

As governments work to protect their digital ecosystem, it is of paramount importance to share security signals and threat intelligence across government and critical infrastructure organizations within a country to ensure resilience.

This facilitation can be done through implementation of a National SOC, which would act as the central orchestration entity providing an early warning system against nation-state and cybercriminal campaigns targeting a country's critical government and critical infrastructure entities.

It is of paramount importance to share security signals and threat intelligence across government and critical infrastructure organizations within a country to ensure resilience.

Pa Op Cybersecurity Tech Accord principles mapping index on **page 124**

https://t.me/learningnets

**Improving global infrastructure resilience** continued

# How regulatory initiatives can strengthen critical infrastructure

In response to these threats, governments around the world are taking steps to improve the security and resilience of their critical infrastructure through laws and regulations.

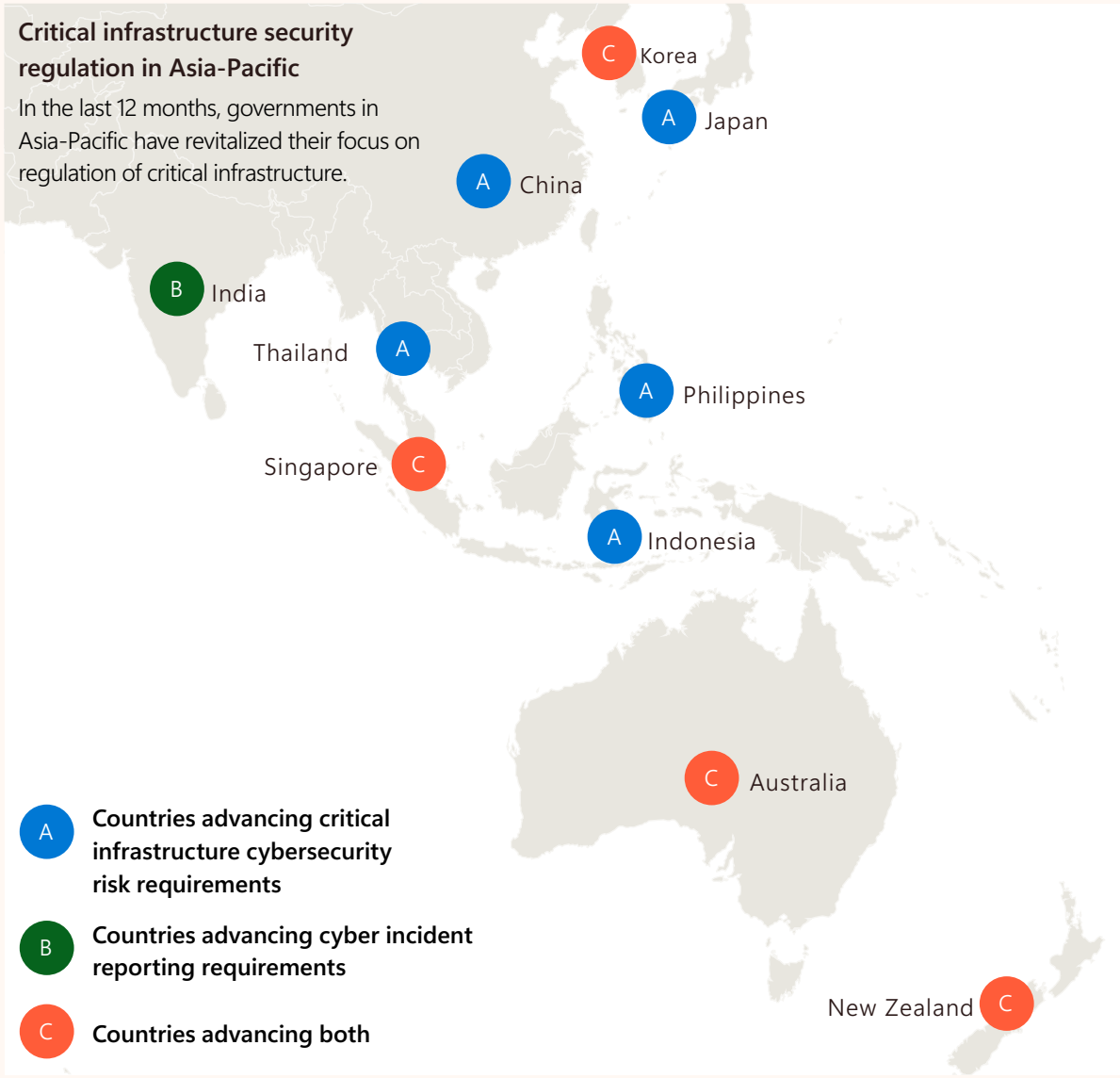
These actions have the potential to raise cyber defenses, but also increase the risk of overlapping or inconsistent requirements across different jurisdictions that increase complexity and costs and decrease security investments.

Governments should seek to establish requirements that drive iterative learning and improvements and support global, cross-sector interoperability. These requirements should maximize the ability to adopt cloud services to take advantage of their cybersecurity benefits.

While each country's approach to regulating critical infrastructure varies, we have noticed three main themes:

1. **Governments** are raising the bar for cybersecurity in critical infrastructure entities and making sure executives and boards are aware of the importance of digital security and resilience.
2. **Governments** are increasingly identifying cloud services as critical infrastructure.
3. **Regulators** are implementing new incident response and reporting requirements. Some nations are requiring notification as early as six hours after an incident, an unrealistic timeframe which is inconsistent with global norms of between 24 and 72 hours.

Governments in Asia-Pacific have revitalized their focus on regulating critical infrastructure because of supply chain disruptions caused by the pandemic, tensions between the United States and China, and lessons learned from Russia's cyberattacks on Ukraine's critical infrastructure.




https://t.me/learningnets

**Improving global infrastructure resilience** continued

The European Union, Japan, Mexico, and the United States each engaged in notable activity during the past year to advance cross-sector or sector-specific initiatives to improve critical infrastructure cybersecurity. While the various initiatives are in different development stages and their implementation varies across jurisdictions, they are all broadly intended to identify critical infrastructure and levy requirements for cybersecurity risk management.

### Actionable insights

1. Use iterative approaches to regulations for cybersecurity risk management that are risk-based and outcome- or process-oriented.
2. Focus on harmonizing regulations and enabling interoperability across sectors, regions, and policy areas.
3. Implement a National Security Operations Center to provide an early warning system against cyber threats.

### Additional information

Regulation (EU) 2022/2554 Digital Operational Resilience Act | European Parliament

### Some exemplars of actions taken worldwide during this reporting period:

**September 2022**

**US**

CISA issued a request for information from the public seeking data to inform its development of cyber incident reporting regulations, its first regulatory step toward implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022. CISA will most likely next issue a notice of proposed rulemaking that will outline its proposed regulatory requirements for cyber incident reporting and solicit public feedback on its proposal.

**October**

**US**

The Transportation Security Agency (TSA) increased cybersecurity requirements for the transportation sector. A security directive mandated passenger and freight railroad carriers to develop network segmentation controls, implement access control measures, use continuous monitoring and detection, and apply security patches promptly to ensure safe operation of operational technology systems in case of IT system incidents.

**January 2023**

**EU**

The EU implemented NIS2, CER, and DORA to enhance critical infrastructure resilience against cyber and physical threats. NIS2 mandates incident response, crisis management, cybersecurity risk management, hygiene, and training. CER strengthens critical infrastructure resilience to various threats. DORA requires financial entities to report incidents, conduct testing, and monitor third-party risks. It also oversees "critical" ICT third-party service providers. EU member states must transpose NIS2 and CER by October 2024 and apply DORA by January 2025.

**March**

**US**

TSA further increased cybersecurity requirements, including TSA-regulated airports and aircraft operators. In July, TSA revised and reissued its cybersecurity requirements for oil and natural gas pipelines starting in 2022.

**April**

**Japan**

Japan approved the General Policy for the Protection of Critical Infrastructure. The General Policy provides guidance to ministries responsible for critical infrastructure industries for designating systems as critical infrastructure and regulating their cybersecurity risk management practices. The policy and corresponding standards for each of the critical infrastructure sectors are not expected to come into effect until 2024.

**Mexico**

Mexico's Federal Congress introduced a bill for a new Federal Law on Cybersecurity. The law aims to establish a regulatory framework for critical information infrastructures (CII) and would create a national cybersecurity agency supporting risk analysis, collaboration with CII operators, maintaining a national CII catalog, monitoring security policies, and defining standardized security measures. CII operators must implement cybersecurity risk management, report incidents, and conduct reviews and exercises to improve their protections.

**July**

**US**

The Security Exchange Commission (SEC) adopted a rule to require publicly traded companies to disclose material cyber incidents within four days and describe their nature, scope, timing and impact. The rule also requires a company to describe its processes for assessing, identifying, and managing material risks from cybersecurity threats and describe its board of director's oversight of cybersecurity risks.

https://t.me/learningnets

**Improving global infrastructure resilience** continued

# Improving IoT/OT device security for critical infrastructure resilience

**Additional information**

The UK Product Security and Telecommunications Infrastructure | Product Security | UK Government

Commission strengthens cybersecurity of wireless devices and products | European Commission

Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers | The White House

IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products | NIST

National Cybersecurity Strategy Implementation Plan | The White House

Adopting guidance from the US National Cybersecurity Strategy to secure the Internet of Things | Microsoft

New EU cybersecurity rules ensure more secure hardware and software products | European Commission

To address IoT and OT security threats, governments and industry are advancing multiple standards and policy initiatives. As the market is changing, governments are moving toward mandatory requirements, where noncompliance could result in losing access to a market segment or financial penalties.

These requirements will create significant market pressure on IoT and OT device manufacturers to adopt cybersecurity best practices.

In the United States, the Biden administration announced a voluntary cyber labeling program for smart devices to protect American consumers intended to be "up and running" in 2024. The program will evaluate products against criteria NIST develops, such as the consumer IoT core baseline profile NIST IR 8425 published in September 2022 and requirements for consumer grade routers to be completed by the end of 2023. The US National Cybersecurity Strategy Implementation Plan set a completion date prior to November 2023 for the Federal Acquisition Regulatory Council to propose Federal Acquisition Regulation requirements for procurement of IoT devices by US federal agencies.

The UK Product Security and Telecommunications Infrastructure Bill empowers government ministers to specify security requirements for consumer connectable products with which businesses involved in making the products available to UK consumers must comply. Draft security requirements for connectable products have been published, and the UK's consumer connectable products security regime will come into effect on April 29, 2024. The security requirements mandate that manufacturers stop using default passwords in products, establish a vulnerability disclosure policy, and provide transparency about the minimum length of time that the product will receive security updates. While US and UK efforts are focused on consumer products, we believe they will drive improved security in the OT market as well.

The EU delegated act to the Radio Equipment Directive will enforce mandatory security requirements in mid-2024 for wireless devices with the goals of improving network resilience, protecting consumers' privacy, and reducing the risk of monetary fraud. Cybersecurity requirements in the Radio Equipment Directive are likely to be overshadowed by the proposed EU Cyber Resilience Act (CRA), anticipated to be finalized in 2024. Microsoft believes the CRA could have serious implications for product cybersecurity, similar to how the EU General Data Protection Regulation promulgated privacy requirements. The CRA envisions mandatory essential cybersecurity requirements for nearly all connected products with digital elements to be sold in the European Union, including hardware, standalone software, and associated remote data processing. Requirements are structured to improve security throughout the lifecycle of products, including design, development, and support. The CRA includes conformity assessment and product security labeling through the application of the European CE marking system.

https://t.me/learningnets

# Innovating for supply chain resilience

## Managing supply chain risk at the speed of regulation

Since 2020, software supply chain security attacks—such as Solarwinds, Log4j, Codecov and Kaseya—have affected over 490 million known customers and exposed over 100,000 malicious open source packages. With an average yearly increase of 742 percent in attacks since 2019, this number will only continue to rise.[7]

Microsoft has taken proactive and collaborative measures such as supplier audits to address the top three supply chain threats: ransomware, phishing, and malware. By working together with suppliers and investing in education and awareness training, our goal is to prevent future attacks and ensure swift recovery in case of a breach.

In collaboration with international partners, we are exploring the use of emerging technologies in AI to revolutionize the security landscape.

**For more about using modern AI to strengthen supply chain security see page 95.**

We also work internationally to lobby for rules and norms that would prohibit nation states from engaging in indiscriminate supply chain attacks that put millions of customers at risk.

Innovation for securing the software supply chain is crucial for keeping businesses and networks safe. Recent cybersecurity incidents highlight the software supply chain's extensive attack surface, which includes source code, developer machines, source control systems, dependencies, build servers, and the release pipeline. As government mandates and industry regulations emerge to address these risks, software producers and engineers play a pivotal role in tackling the compliance challenge while maintaining their efficiency. Leveraging automation presents an opportunity to fulfill these obligations at a reduced cost and lower impact on engineers.

Em Pa Op Cybersecurity Tech Accord principles mapping index on **page 124**

## Microsoft's secure-by-design supply chain

### Celebrating 20 years of the Security Development Lifecycle (SDL)

We prioritize security in every aspect of our products and services to ensure resilience. The Microsoft Security Development Lifecycle (SDL), introduced in 2004, is designed to identify and minimize risks throughout the product lifecycle, meet compliance requirements, and deliver reliable solutions to our customers.[8]

We have evolved the SDL to adapt to cloud computing, AI/ML advancements, the changing threat landscape, and regulatory demands like US Executive Order 14028 ("Improving the Nation's Cybersecurity"). Our latest SDL updates focus on simplicity, automation, and providing developers with further guidance and guardrails.

We leverage enforcement mechanisms within our development and cloud platforms to impose SDL requirements early in the development lifecycle. For example, we scan code for potential exposure of sensitive information before it is committed to version control and ensure that code is reviewed by someone other than the author before being committed.

We also invest in finding vulnerable code across our products and services. CodeQL is a powerful static analysis tool which we use to identify security issues and potential vulnerabilities in programming languages. We centrally store source code snapshots generated at build time in CodeQL Central and run predefined rules or ad hoc queries against them. These rules help identify known vulnerable code patterns, capture evidence of secure coding practices, and highlight areas affected by emerging requirements like Post-Quantum Cryptography (PQC).

Our approach has significantly reduced the feedback loop when new vulnerabilities are discovered, providing actionable results to developers within hours. When these CodeQL rules mature or require urgent release, as in the case of Solorigate,[9] we open-source them and incorporate them into the CodeQL product to benefit all users.

While automation plays a vital role, we also prioritize developer security training, threat modelling, and specialized reviews in areas like AI/ML and cryptography. These efforts provide knowledge which feeds back into our SDL guidance and automation, allowing us to scale while ensuring security. We also share knowledge externally through published guidance, open-sourced tools, and new features in our developer and cloud platforms to foster a more collaborative and resilient environment for all.

Pr Em Cybersecurity Tech Accord principles mapping index on **page 124**

https://t.me/learningnets

**Innovating for supply chain resilience** continued

### Securing the development infrastructure

We built a threat model of our end-to-end DevOps environment in 2023 to identify potential threats and prioritize security investments to reduce risk within the engineering ecosystem. It includes the Continuous Integration/Continuous Deployment (CI/CD) platform, developer identities, and all connected services used by our developers (such as Microsoft Dev Box and GitHub Codespaces). The model was informed by real-world threat reports and calculated risk scores. Based on the results, we made several security investments: adopting secure boot for our build machines, improving inventory and update processes for build tools, and validating the integrity of our software bills of materials (SBOMs) at release time.

Our security measures go beyond just identity, devices, and access. We follow Zero Trust principles to secure our developers. This includes using phish-resistant MFA, requiring managed healthy devices to access DevOps web apps, replacing personal access tokens (PAT) bearer tokens with managed identities, and applying the least privilege access principle to managing version control and build configuration. We also perform periodic user access reviews to ensure privileges are only granted to those with a business need and use just-in-time (JIT) permission controls for administration tasks.

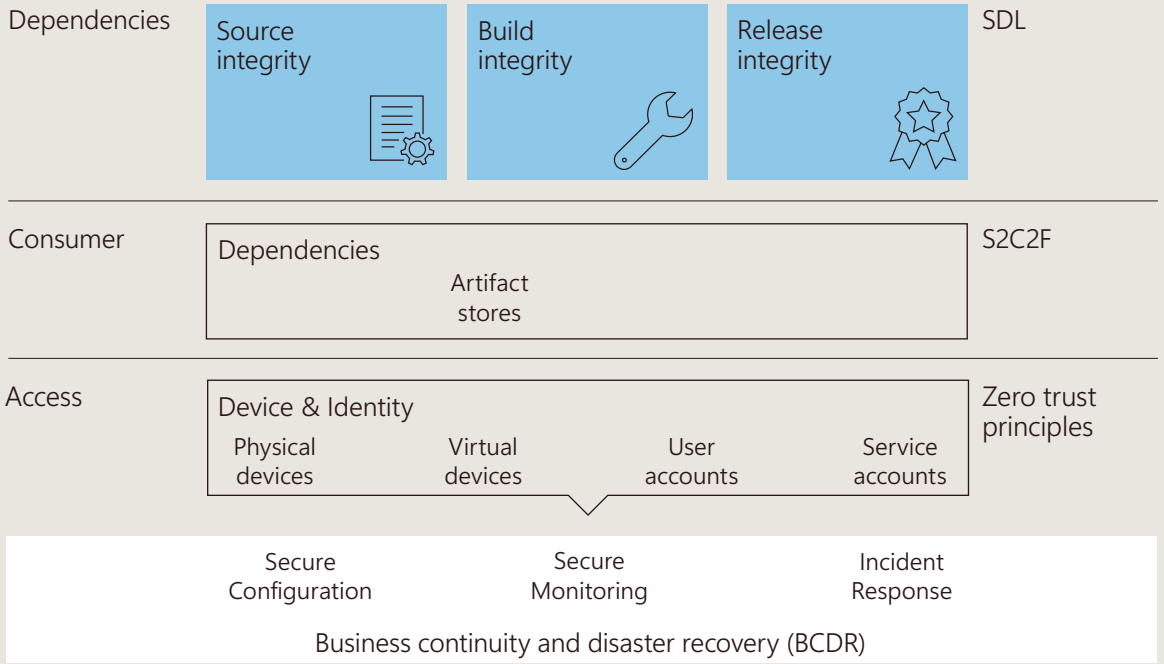
**Additional information**

Embrace proactive security with Zero Trust | Microsoft

Managed identities for Azure resources | Microsoft

### How our SDL and development infrastructure security come together

**Producing trustworthy software requires trustworthy development infrastructure.**




### Our approach to open-source governance

Microsoft relies heavily on open source in its supply chain, with over 83,000 unique packages used more than 13 million times in our products. To encourage collaboration, we have created an environment that allows developers to choose the best open source for their needs, without outdated pre-approved lists or manual reviews.

It is crucial to ensure we use open source safely and efficiently. We have invested in an internal tool that continuously inventories open source, flags license concerns, and alerts developers to vulnerabilities.

This tool is available to customers on Azure DevOps through GitHub Advanced Security for Azure DevOps.[10]

Pr Em Cybersecurity Tech Accord principles mapping index on **page 124**

83,000

unique packages used more than 13 million times in our products

https://t.me/learningnets

**Innovating for supply chain resilience** continued

### Software bills of materials

Microsoft is an advocate for software bills of materials (SBOMs), which provide software transparency to customers. SBOMs enable organizations to manage their supply chain risk for the software that's deployed across their enterprise.

Since 2019, we have contributed to cross-industry working groups, international standards, and open-source tools aiming to advance SBOM generation, sharing, and consumption.

Our SBOM generation tool detects dependencies across numerous ecosystems and is available as open source. We generate SBOMs using the Linux Foundation's Software Package Data eXchange (SPDX) 2.x JSON format. Microsoft Defender for IoT firmware analysis allows customers to generate an SBOM and identify potential security vulnerabilities.

NuGet plans to support SBOM generation natively within its ecosystem so that every future NuGet package would have an SBOM,[11] and GitHub now allows exporting SBOMs from repositories.

Organizations should prepare now for consuming and managing SBOMs from their suppliers. Most, if not all, Software Composition Analysis (SCA) tools can produce SBOMs today, so commercial software suppliers should have the capability to produce and share SBOMs. When the next incident such as Log4j occurs, having an SBOM for the software deployed across your enterprise enables you to answer the questions "Am I affected?" and "What is affected?" This empowers organizations to understand where the vulnerability is within their environment so they can understand their level of exposure, as well as prepare for deploying emergency patches if applicable.

**Additional information**

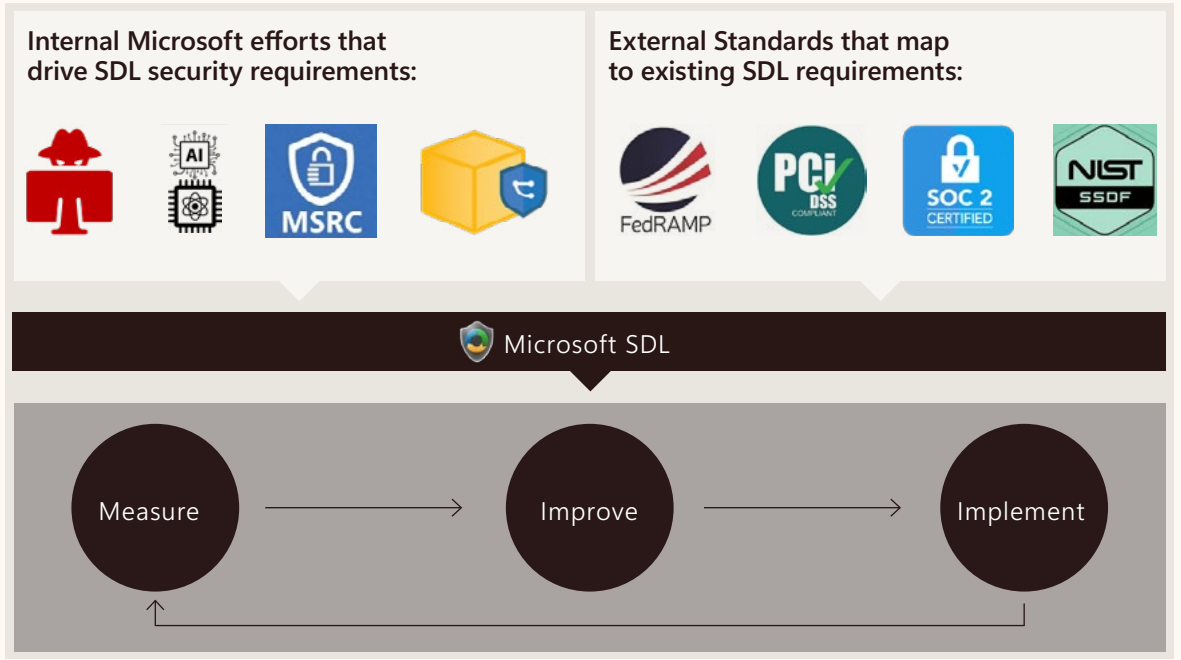
Introducing self-service SBOMs | GitHub Code Security

### Tracking conformance with standards and regulations

Industry collaboration and public-private partnerships are crucial for advancing global supply chain cybersecurity. We are committed to meeting international standards, certifications, and technology sector regulations, and we keep a close eye on our compliance by investing in automated tracking and monitoring tools.

To make sure our products meet diverse and at times conflicting requirements, we align them with our SDL framework.

This drives us to continuously evaluate our security posture through our SDL continuous assurance approach rather than assessing compliance at a single point in time like other audits. We employ automated tools like static analyzers, web scanners, and open-source scanners to assess our code and development infrastructure and use manual attestations for non-automated requirements. By analyzing assessment results from different perspectives, we can identify trends and intervene when necessary. This approach helps us prepare for new requirements by introducing draft requirements that generate reports without alerting developers.




https://t.me/learningnets

**Innovating for supply chain resilience** continued

# How we are empowering the ecosystem

### Sharing guidance through partnerships

As a co-founding member of the Open Source Security Foundation (OpenSSF), Microsoft is investing in initiatives to enhance the security of the entire open-source ecosystem. OpenSSF Alpha-Omega began in February 2022 and is funded by Microsoft, Google, and Amazon Web Services. It aims to safeguard society by engaging directly with open-source maintainers and conducting expert analysis to improve the security of open-source software.

Em Pa Cybersecurity Tech Accord principles mapping index on **page 124**

Through the "Alpha" component, we provide tailored funding to critical open-source projects, including the Eclipse Foundation, the Python Software Foundation, the Rust Foundation, Node.js, jQuery, ISRG, and OpenSSL. These engagements often include the appointment of a security champion to drive improvements within the organization's projects and embed security in their culture and processes.

The "Omega" aspect leverages technology and security experts to scale vulnerability detection across the top 10,000 critical open-source projects. We use static analysis tools like CodeQL to identify and efficiently triage critical vulnerabilities. Responsible disclosure, often accompanied by fixes, is then shared with the maintainers.

### Bringing S2C2F to OpenSSF

When combined with the fact that attacks targeting open source software (OSS) have grown 742 percent on average, securing how developers consume OSS is arguably the most important aspect of any organization's software supply chain.

We recently published and contributed the Secure Supply Chain Consumption Framework (S2C2F) to the OpenSSF, making it available for any development team or organization to adopt. It is a set of requirements focused on improving the security around how developers consume OSS into the developer workflow.

Due to the fact that OSS makes up 70-90 percent of the code base used by developers,[12] and is present in 96 percent of modern applications,[13] it has become a crucial dependency in the software industry.

Microsoft had been operating its OSS security and governance program for many years as part of the Microsoft SDL, but expanded its scope to include a holistic view of supply chain security in 2019, now called the S2C2F.

We continue to maintain the framework within the Supply Chain Integrity working group in collaboration with the OpenSSF community. Since the S2C2F is a consumption-focused framework, it can be used in addition to existing secure development practices. The S2C2F requirements have also been organized into a maturity model, enabling organizations to prioritize what requirements they should implement first. We encourage you to consider incorporating the S2C2F requirements into your organization's security strategy.

Em Cybersecurity Tech Accord principles mapping index on **page 125**

96%

of software contains some open-source components.

https://t.me/learningnets

**Innovating for supply chain resilience** continued

### Securing software at the (open) source

GitHub is the home of OSS and hosts a community of more than 100 million users. With the rise of open-source vulnerabilities like Log4Shell, it has become clear that a vulnerability anywhere can become a vulnerability everywhere, and increasing resilience needs to be a collective goal. To combat this, GitHub puts advanced security capabilities into the hands of developers to keep vulnerabilities, private keys and other secrets, and malicious code from impacting the software that powers the modern world.

While developers want to focus on writing code, security testing and remediation tasks can disrupt their workflow and make the software development lifecycle less predictable and more expensive. GitHub's solution is to make supply chain security tools easy and convenient for developers to use as they code, building best practices into the daily workflow. In addition to our commercial GitHub Advanced Security offerings, we make these capabilities available free of charge to open-source developers, because OSS is a part of everyone's supply chain.

Em Cybersecurity Tech Accord principles mapping index on **page 125**

**24m**

vulnerabilities remediated by developers[14]

**94%**

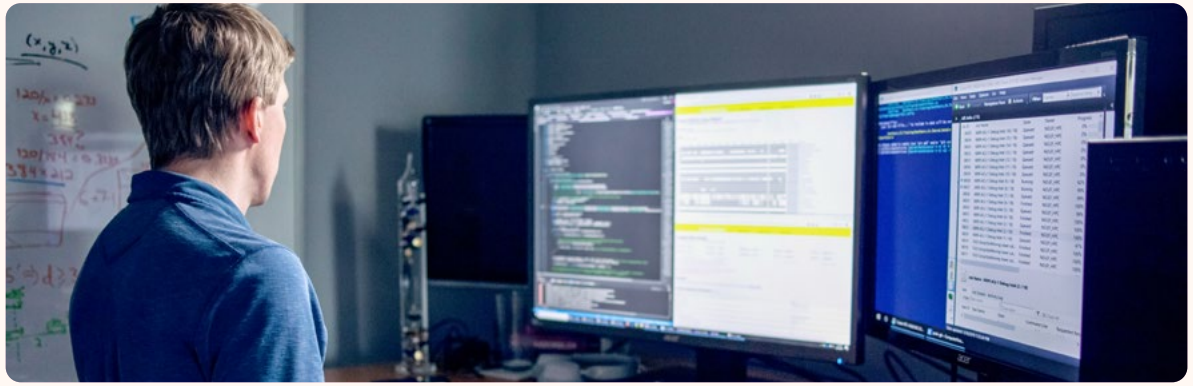
businesses in the United States use open-source components[15]

**61%**

of businesses have been impacted by supply chain attacks in the past year[16]

**12,404**

expert-reviewed security advisories[17]



### How GitHub secures the software supply chain

**Code Scanning:** Powered by the CodeQL static analysis engine and CredScan, GitHub Code Scanning helps developers quickly identify and fix insecure code patterns that are associated with security vulnerabilities.

**Secret Scanning:** Keep tokens, private keys, and other secrets from leaking into the open-source software ecosystem. GitHub provides free secret scanning and push protection features for public repositories.

**Dependabot:** GitHub's dependency management tool alerts developers to vulnerable and out-of-date dependencies and suggests remediation steps so developers can quickly fix issues and get back to coding.

**SBOMs:** GitHub helps development teams comply with regulatory and customer requirements with native tools to ingest, generate, and export SBOMs. Comprehensive and up to date SBOMs help organizations comply with regulations, meet RFI/RFP requirements, and satisfy software supply chain concerns to address customer objections and close business.

**Advisory Database:** As the industry's biggest issuer of open source software CVEs, GitHub maintains a comprehensive Advisory Database with knowledge about vulnerabilities and malware drawn from security advisories reported on GitHub, the National Vulnerability Database, and contributions from GitHub's 100 million community members. A team of security experts reviews advisories for validity and provides the contextual information needed for remediation.

**Platform Security:** Developers can protect against unauthorized access to repositories and packages with two-factor authentication (2FA) for both GitHub and npm user accounts.

https://t.me/learningnets

**Innovating for supply chain resilience** continued

### Strengthening the supply chain security landscape using AI and large language models

Protecting supply chains depends on strong partnerships between suppliers and their customers. We have been investing in strengthening our digital supply chains by incorporating controls to mitigate evolving AI and privacy risks into our supplier governance processes and providing our suppliers with security awareness training. These controls and training help ensure that our suppliers make the same commitment to safe, secure, and trustworthy AI systems and supply chains that Microsoft has.

In addition, we have announced Copilot capabilities for Microsoft Supply Chain Center, which uses AI and ML to help customers predict and act on supply chain disruptions and uses Azure OpenAI to generate contextual emails to suppliers to help minimize these disruptions in real-time. These technologies will enhance human decision-making and analysis and revolutionize how organizations manage supply chain risks, but they also have their own digital supply chain that needs to be made safe, secure, and trustworthy.

Inventory and provenance is fundamental to supply chain management, and this is also true for the digital supply chain underlying AI. Understanding the provenance of the data in our various supply chains, including how it was generated, allows Microsoft to manage supply chain risks, and to provide appropriate transparency to our customers. Microsoft has been investing in provenance standards and technologies, such as the C2PA specification SBOMs, to support the sharing and authentication of provenance information.

In May 2023, we released our report, Governing AI: A Blueprint for the Future, followed by our Voluntary Commitments to Advance Responsible AI Innovation, which outline the governance structures, data protection policies, and model validation and improvement processes we believe are needed for this transformational technology to be adopted safely and in compliance with existing and evolving laws and regulations. Protecting AI's digital supply chain builds on decades of experience and investment in protecting the supply chains of its fundamental components, which include data, software, hardware, and infrastructure.

Pa Cybersecurity Tech Accord principles mapping index on **page 125**

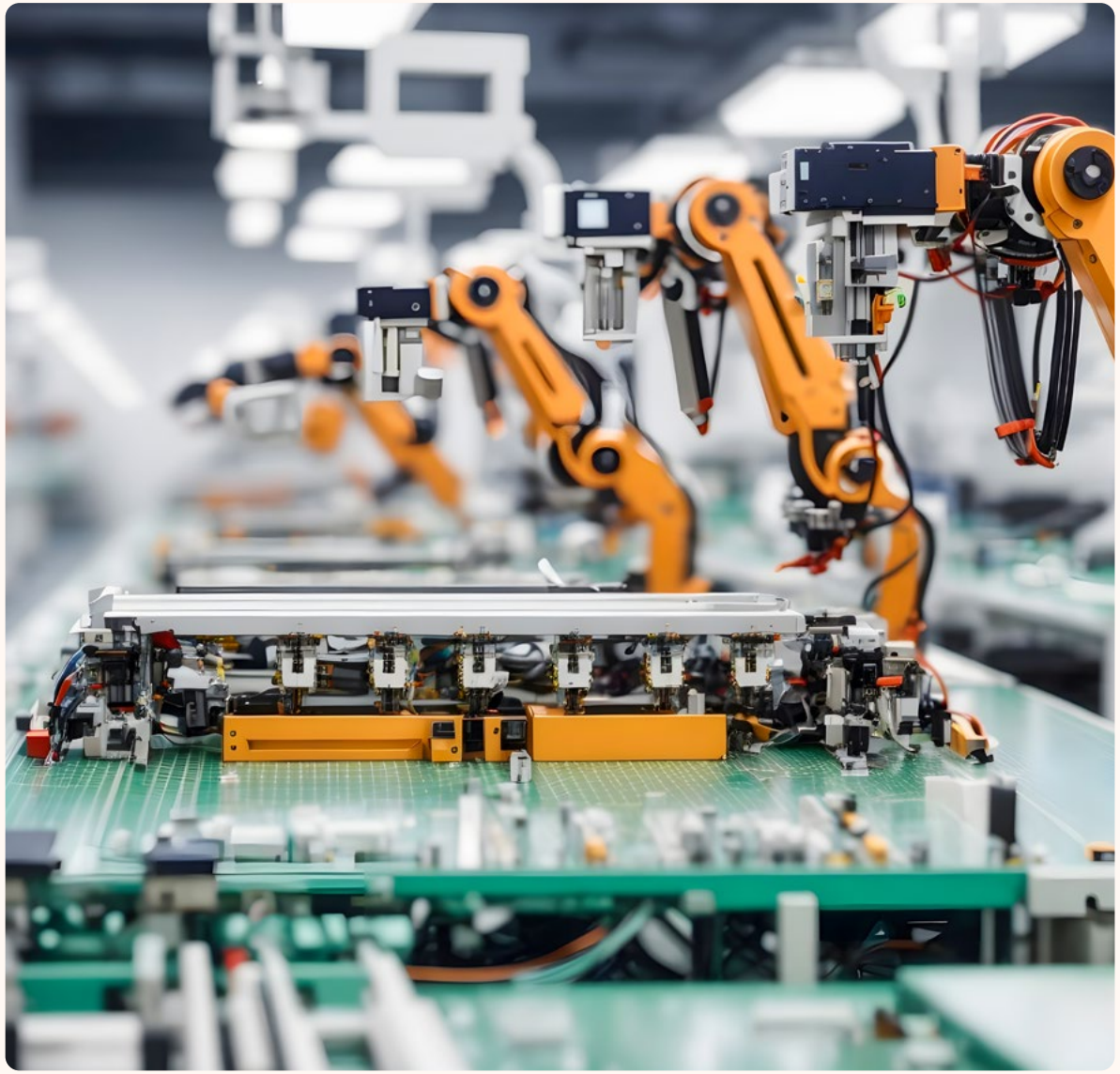
**To learn more about the use of LLMs and AI breakthroughs in cybersecurity, please see pages 100-105 of this report.**

**Additional information**

Introducing Microsoft Dynamics 365 Copilot | Microsoft

Governing AI: A Blueprint for the Future | Microsoft

Our commitments to advance safe, secure, and trustworthy AI | Microsoft

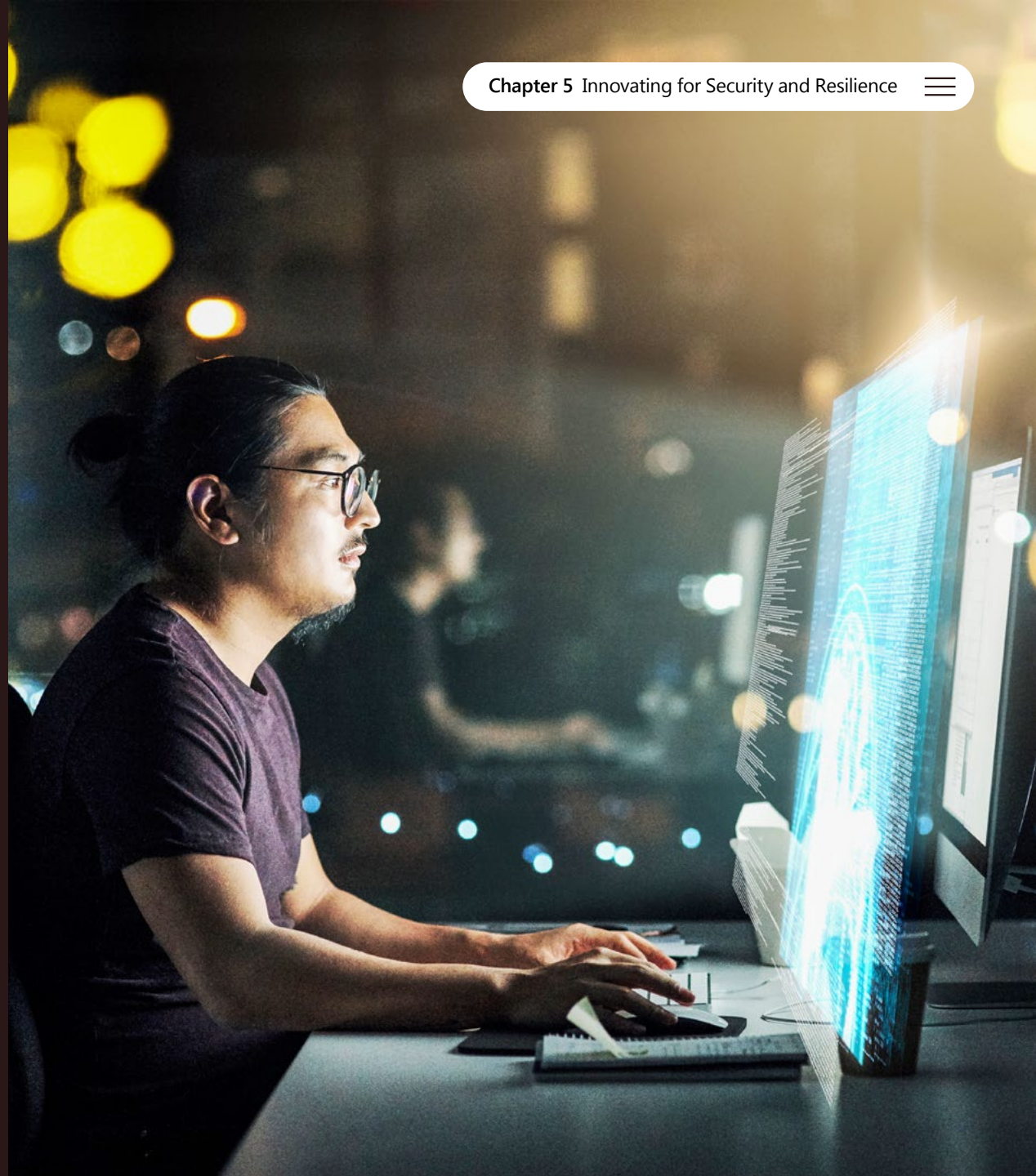


https://t.me/learningnets

# Chapter 5
# Innovating for Security and Resilience

## Defending with AI


| | |
|---|---|
| Key developments | 97 |
| Introduction | 98 |
| Using the power of AI for cybersecurity | 100 |
| Working together to shape responsible AI | 106 |

https://t.me/learningnets

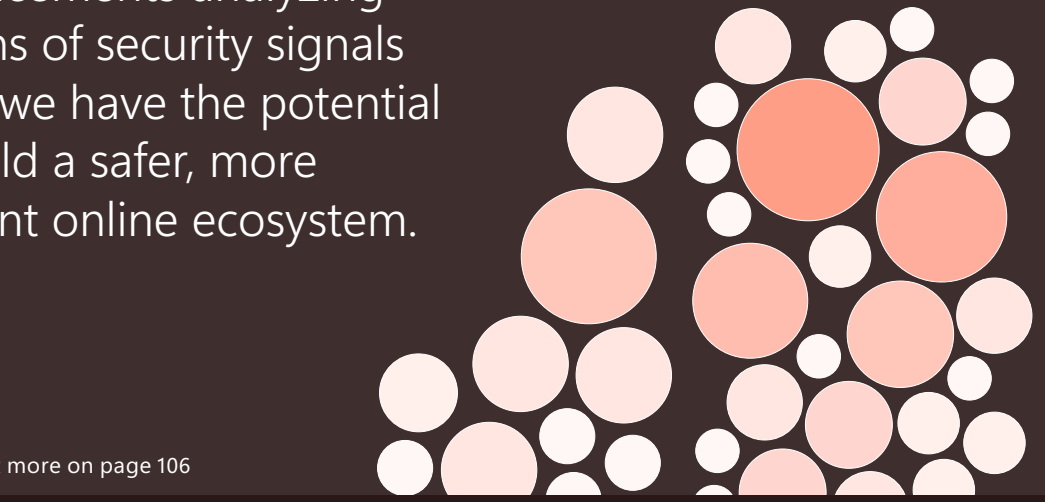
Innovating for Security and Resilience

# Key developments

Against an ever more complex cyber ecosystem, AI offers the potential to change the security landscape by augmenting the skill, speed, and knowledge of defenders.

Since Microsoft has the largest and most diverse set of products in the industry, we are continuously seeking out and eliminating vulnerabilities before threat actors can exploit them. One way that we are confronting cybercrime is by leveraging AI and large language models (LLMs). LLMs can automate and augment many aspects of cybersecurity, including: threat intelligence; incident response and recovery; monitoring and detection; testing and validation; education; and security governance, risk, and compliance.

With modern AI advancements analyzing trillions of security signals daily, we have the potential to build a safer, more resilient online ecosystem.



Find out more on page 106

Our approach for the next year will focus on bringing to bear AI in combating threats while also embracing the three SDL principles of Secure by Design, Secure by Default, and Secure in Deployment (SD3).

Find out more on page 99

LLMs have the potential to transform cyber defense for next-gen cybersecurity.

**Microsoft's researchers and applied scientists are exploring many scenarios for LLM application in cyber defense.**

Find out more on page 101

Many modern apps will become LLM-based in time.

**This will increase the threat surface, making them vulnerable to both inadvertent and deliberate misalignments. As LLM-based apps bring new and unique threats, we adapt our security measures and protocols to address them.**

Find out more on page 104

https://t.me/learningnets

# Responding with breakthrough innovation

## Introduction from Bret Arsenault

In the last few months, the world has witnessed a wave of innovation as organizations apply advanced AI to new technologies and use cases. Our industry is facing a paradigm shift and taking a massive leap forward as technology advances incredibly quickly and makes daily headlines.

The security industry has been focused on managing increased risks and innovating to adapt to the fast pace of change. We continue to hear from our peers, partners, and customers that security has never been more critical to the resilience of business and society.

There has been significant growth in the threat landscape as more attackers use increasingly sophisticated techniques to compromise an ever-growing footprint of services, devices, and users. All combined, this creates a larger attack surface and threat potential than we have ever dealt with before. At Microsoft, we have seen a 23 percent annual rise in the cases processed by the Microsoft Security Response Center and Security Operations Center teams.

While human ingenuity and expertise will always be a precious and irreplaceable component of cyber defense, technology has the potential to augment these unique capabilities with the skill sets, processing speeds, and rapid learning of modern AI. Technology can work alongside us, detect hidden patterns and behaviors, and inform a response at machine speed with the latest and most advanced security practices.

https://t.me/learningnets

**Responding with breakthrough innovation** continued

Experiences based on large language models, like ChatGPT, have taken the world by storm in the last year. This is in part because they can draw upon a vast store of data, leveraging the massive computing power available today in the cloud. But what I think is more exciting is the real, tangible impact that technology like this can drive. AI, together with the power of cloud and machine learning, has enormous potential. Much like we led the charge on password spray detection, two-factor authentication enforcement, and managed device health, we have an opportunity to demonstrate how responsible AI has the potential to positively transform the security landscape.

At Microsoft, we are developing first- and third-party solutions for our ever-increasing number of enterprise, government, and consumer customers and partners. We have seen developer activity double in the last three years, and it is up by over 31 percent in the last year alone. This trend will accelerate as developers adopt AI powered development tools like GitHub Copilot. This will require a commensurate increase in threat models, code reviews, compliance attestations, and app/infrastructure assurance to secure resilience.

An important contribution we can make is to continue to evolve our Security Development Lifecycle (SDL) rules and engineering compliance. This will ensure continued focus on secure engineering practices.

We recently simplified, updated, and automated our SDL and Operational Security Assurance requirements into a single standard. We will increase our compliance with the modernized SDL through enhanced training, automation, and reporting.

We will also deploy Security CoPilot—our new AI powered incident response assistant—across our incident response teams, so that we can both gain the benefit of AI in addressing security incidents, and so we can improve this valuable new capability by providing our development teams with feedback based on our real-world experience.

Based on actions needed to meet the growing threat landscape, our approach for the next year will focus on bringing to bear AI in combating threats while also embracing the three SDL principles of Secure by Design, Secure by Default, and Secure in Deployment (SD3). While it may sound simple, this will require all of us to prioritize and collaborate to successfully execute across everything we do, every day.

**Bret Arsenault**
Chief Information Security Officer

We have defined three priority areas in which we will invest to ensure that we embed SD3.

**Be Secure by Design and address the technical debt.** Bring systems up to current standards and levels of inspection and security. Address the need for security training for developers, threat modeling for all services, complete Code QL and Network Security.

**Create efficiency in current systems.** Unify critical tools and systems, including the numerous Identity systems, SOC/IR, case management, and risk management. Create common tooling and mechanisms to ensure compliance with Secure by Default and Secure in Deployment.

**Future-proof the company, focusing on AI.** We need to invest resources in how we identify the new risks (Secure by Design) and operate the environments (Secure by Default and Secure in Deployment). We will leverage AI to improve security operations and define the standards to ensure we build trust and transparency across all the customer facing implementations as well.

23%

annual rise in the cases processed by the Microsoft Security Response Center and Security Operations Center teams.

https://t.me/learningnets

# Using the power of AI for cybersecurity

The cost of cybercrime is projected to hit an annual $10.5 trillion by 2025.[1] By the same token, Gartner analysts predict that over the next two years, 45 percent of global organizations will be impacted in some way by a supply chain attack.[2] This challenge has been made more difficult for organizations due to the 3.5 million job talent gap in cybersecurity worldwide.

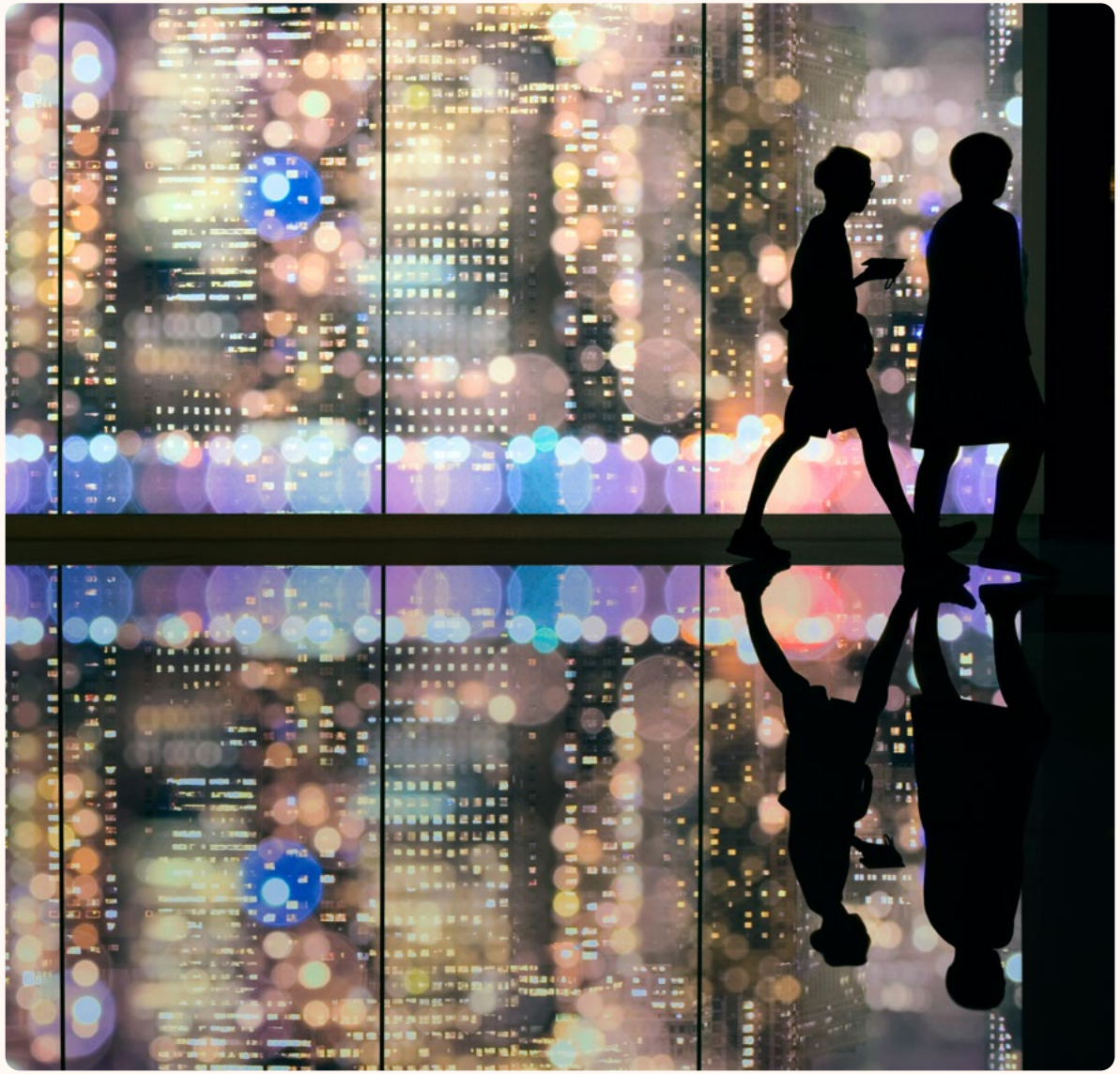
To combat this challenge, cybersecurity professionals must leverage the latest technologies and innovations to stay ahead of the curve. AI is one of the most promising technologies that can enhance cybersecurity and provide a competitive edge.

AI can help by automating and augmenting many aspects of cybersecurity, such as threat detection, response, analysis, and prediction. AI can also enable new capabilities and opportunities, such as using LLMs to generate natural language insights and recommendations from complex data, helping make junior analysts more effective and giving them new opportunities to learn.

In this section of the report, we explore some of the AI breakthroughs that are transforming cybersecurity and how they can help us achieve a more secure and resilient digital future. We also discuss some risks associated with AI and LLMs. As we integrate these technologies into our business processes, we must remain vigilant to protect privacy and security.

**$10.5 trillion**

The cost of cybercrime is projected to hit an annual $10.5 trillion by 2025.[1]



https://t.me/learningnets

**Using the power of AI for cybersecurity** continued

# Harnessing large language models for cyber defense

LLMs have the potential to greatly enhance several aspects of cyber defense. Across Microsoft, researchers and applied scientists are experimenting with and exploring the following scenarios:

**Threat intelligence and analysis:** LLMs can help cyber defenders gather and analyze data to find patterns and trends in cyber threats. They use this information to provide recommendations and alerts. LLMs also add context to threat intelligence by using information from different sources. Additionally, they perform technical tasks like reverse engineering and malware analysis.

**Security incident response and recovery**: LLMs can help cyber defenders support and automate security incident response and recovery activities such as incident triage, containment, eradication, analysis, and recovery. They can summarize incidents and generate response automation scripts, coordinate teams, and document and communicate the incident details and actions. LLMs can also help us learn from incidents and provide improvement suggestions for prevention and mitigation.

**Security monitoring and detection**: LLMs can help cyber defenders monitor and detect security events and incidents across networks, systems, applications, and data. They can analyze data from multiple sources, generate prioritized alerts, and provide contextual information for investigation and response. LLMs can also be valuable in analyzing the posture of multicloud environments where they can create comprehensive maps of resources, estimate potential impacts, and offer risk mitigation suggestions. LLMs can also be useful for phish detection by analyzing email content and identifying textual patterns, anomalies, or suspicious language indicative of phishing attempts.

**Security testing and validation**: LLMs can automate and enhance security testing and validation activities such as penetration testing, vulnerability scanning, code analysis, and configuration auditing. They generate and execute test cases, evaluate and report results, and offer remediation suggestions. LLMs can create custom apps and tools for specific scenarios, automate repetitive tasks, and handle occasional or ad hoc tasks that require manual intervention.

**Security awareness and education**: LLMs can help cyber defenders create engaging and personalized content and scenarios for security awareness and education programs. They assess the level of security knowledge and skills of the target audience, provide feedback and guidance, and generate realistic and adaptive cyber exercises and simulations for training and testing.

**Security governance, risk, and compliance (GRC)**: LLMs can assist in automating security governance, risk, and compliance (GRC) activities including policy development and enforcement, risk assessment/management, audit and assurance, and compliance and reporting. They align GRC activities with business goals and provide security metrics and dashboards for performance measurement. They can also identify gaps and issues and offer recommendations to improve the organization's security posture, prioritize vulnerabilities, and identify remediation suggestions.

Pr Cybersecurity Tech Accord principles mapping index on page 125.

https://t.me/learningnets

**Using the power of AI for cybersecurity** continued

# Lowering the entry bar for using new innovations

While LLM-based solutions show great potential for cybersecurity, they are not a replacement for human cybersecurity experts. Having the right expertise is key when it comes to combining LLMs and cybersecurity. One solution is to bring together the skills of AI professionals and cybersecurity experts to enhance productivity.

Fortunately, the use of LLMs in cybersecurity operations is not limited to large organizations with abundant resources. These models have been trained on vast amounts of data, giving them a pre-existing understanding of cybersecurity.

However, relying solely on LLMs to tackle cybersecurity challenges has its limits, and a data-oriented approach that considers enterprise-specific data and the evolving threat landscape is necessary.

Without additional finetuning, LLMs are not cognizant of the latest cybersecurity threats. Therefore, they need to be augmented with complementary modules, also called RAG (Retrieval Augmented Generation), that interface with relevant data sources, tailored analytics, and various threat intelligence enrichments. Investing in a solution to enable the adequate and flexible orchestration of the RAG will be necessary to fully take advantage of LLMs for security challenges.

With a robust LLM-powered solution, cybersecurity analysts can increase productivity with automated scans and anomaly detection, pattern identification, and root cause evidence discovery. LLMs excel at synthesizing complex information and presenting it in clear, concise language—helping analysts select the best cyber analytics for different scenarios. As the threat landscape evolves and analysis techniques expand, even experienced analysts can struggle to keep up, and LLMs can act as personal assistants, suggesting analysis and mitigation options.

Organizations should assess their current cybersecurity capabilities, identify areas where LLMs can be most effective, and invest in the necessary expertise and technology to integrate LLMs into their existing cybersecurity infrastructure to enhance their cybersecurity posture and stay ahead of evolving threats.

Em Cybersecurity Tech Accord principles mapping index on page 125.

**Additional information**

Retrieval Augmented Generation using Azure Machine Learning prompt flow | Microsoft

https://t.me/learningnets

# How Microsoft is using large language models to improve operations

Modern AI is particularly effective at processing large amounts of data and reasoning over the results to complete complex tasks. With trillions of security signals being analyzed daily, we can use these advancements to build a safer, more resilient online ecosystem.

To demonstrate the potential of this technology in addressing complex challenges and driving innovation, here are some examples to show how we've chosen to use LLMs internally to improve security and efficiency in various areas of our operations:

### Intelligent reports

We are using AI to create intelligent reports that provide decision makers with timely and accurate insights into open-source intelligence findings. Traditional reports that rely on manual analysis of multiple information sources are slow, costly, and often outdated by the time they reach their audience. This approach hinders organizations' ability to seize opportunities, mitigate risks, and adapt to changing situations. We solved this problem by applying the latest Azure OpenAI models to revolutionize report generation and delivery. These models use natural language processing to scan, synthesize, and summarize relevant data from various sources, including social media and news blogs. This capability enables us to produce concise reports based on intelligence information from multiple sources and can generate high-quality reports in minutes or hours—instead of days or weeks—highlighting key trends, patterns, and implications for decision makers. Additionally, using the latest Azure OpenAI LLMs enables us to update reports dynamically as new information becomes available, ensuring that insights are always fresh and reliable.

### Chatbot for developer support

We have created a chatbot to support Microsoft's developers in accessing compliance information and guidelines for security standards and regulations. This helps them integrate security into their code early on, reducing delays, vulnerabilities, and costs in the development process. Our chatbot uses our data sources and combines Azure Cognitive Search with Azure OpenAI models, making it easy and reliable for developers to find the relevant compliance data. This also reduces the workload and overhead of compliance program teams.

### Natural language interface with your security data

We created a natural language interface that uses Azure OpenAI models to help security teams analyze and query large amounts of data from logs, alerts, events, incidents, and threat intelligence. Traditional methods, like structured query language or scripting, can be difficult and time-consuming and it may not always provide accurate results. Our interface allows users to ask questions in plain English and receive quick answers without needing to write code or learn syntax.

### LLMs for cloud datacenter security

Industrial control systems (ICS) are crucial for ensuring security and efficiency in cloud datacenters. They are used to automate and optimize processes, reduce human error, and improve overall efficiency. However, ICS can be vulnerable to security threats and require prompt identification and resolution. The traditional method of analyzing verbose vulnerability advisories and implementing mitigations is time-consuming and inefficient. To address this issue, we have developed an LLM-based solution that automatically detects affected industrial IoT devices and their locations within Azure datacenters. This solution generates actionable Agile and DevOps items that technicians can execute in seconds, resulting in improved security and reliability while reducing operational costs and risks.

Pr Em Cybersecurity Tech Accord principles mapping index on page 125.

**Additional information**

Governing AI: A Blueprint for the Future | Microsoft

https://t.me/learningnets

# Defending the increasing threat surface

We expect many modern apps to become LLM-based in time. These apps will have an increased threat surface, meaning they will be vulnerable to both inadvertent and deliberate misalignments, such as command injection attacks. As LLM-based apps bring new and unique types of threats, we must ensure that our security measures and protocols are updated and adapted to address these new threats.

The challenges will be further complicated by the fact that, in the future, it is likely there will be more than one platform and multiple paradigms, such as Microsoft's Semantic Kernel, LangChain, and AutoGPT. This will require organizations to include new protection capabilities built intrinsically in the LLM-based apps that are agnostic to the platform, like an LLM-based app firewall.

We are at the early stage in the journey and new challenges are constantly emerging. We need to expand app discovery and inventory to address unsanctioned/unmanaged LLM-based apps and their plug-ins, and the need to manage enterprise boundaries due to emerging LLM-based solutions like personal assistants that mix private and corporate data access. The growth of autonomous apps that combine LLMs with low- or no-code platforms also significantly increases the security risk for organizations.

To build collective resilience against these emerging threats and to safeguard our ecosystem, it is crucial for organizations to collaborate, innovate, and share knowledge and best practices.

https://t.me/learningnets

**To take a multidisciplinary approach to addressing the rapidly growing LLM-level attack surface and unique threats:**

1. **Educate security teams about the novel threats that AI systems introduce**, particularly prompt injection.
2. **Consider the LLM-based app security throughout the lifecycle**. Expand risk management investments to include end-to-end visibility of LLM-based app risks and mitigation, tightening DevSecOps security controls for development and operation.
3. **Review security practices for AI-integrated products holistically, including all components**. Assessing only the AI component of a system makes it difficult to quantify risks and provides limited mitigation options. However, reviewing the entire system provides the full context and more mitigation opportunities at different points, making the risks more quantifiable.
4. **Multidisciplinary security reviews are crucial for AI systems**. Involve data scientists, engineering systems people and experts in content moderation, digital safety, and privacy. LLM systems require defenders with expertise in these areas because prompt injection attacks often involve elements from each discipline.
5. **Zero trust model investments can help the defense of LLMs**. Implement continuous monitoring and detection of anomalies and LLM models behavioral changes. Limit the LLM components' access to minimum resources required for its scope.

**Using the power of AI for cybersecurity** continued

# Insights on emerging security trends in large language models

Vulnerability reports submitted to Microsoft provide valuable insights into emerging security trends, especially in fast-changing areas like AI. Focusing specifically on LLMs, some of our key learnings from recent vulnerability reports include:

- Attacks against LLMs may look significantly different from typical software security attacks. For instance, when the attacker can control the text that is fed into the LLM, the process of developing attacks usually involves searching for a well-crafted natural language sentence to input into the model.
- The main classes of reported vulnerabilities involving LLMs have included attempts to extract the model's system prompt (prompt extraction) and attempts to cause the model to deviate from its intended behavior (command injection), such as "jailbreaks."
- In prompt extraction attacks, it may be difficult for the attacker to distinguish whether the model has output the real system prompt or just a convincing artificially-generated example prompt.
- Command injection attacks are a central concern, especially in cases where these could affect other users of the system. Comprehensive detection and prevention of command injection vulnerabilities remains an open research and development question.

Em Cybersecurity Tech Accord principles mapping index on page 125.

# Red teaming AI systems to test resilience

In the security community, red teaming is a technique used to test the effectiveness of how an organization would respond to a genuine cyberattack. It is a double-blind exercise in which dedicated security operators role-play as real-world adversaries to attain a specific goal via scoped tactics, techniques, and procedures (TTPs). The point of the exercise is to provide a realistic assessment of an organization's ability to prevent, detect, and respond to a particular group of attacker TTPs.

Red teaming as an essential practice in the responsible development of Microsoft's systems and features using LLMs. Red teaming with AI systems is a little different from traditional cybersecurity red teaming.[3] The set-up is similar; in the AI context, the red team emulates real world adversaries or their behaviors to find security-specific flaws in products and platforms. Because of the broad range of AI used in multiple domains, the AI community uses red teaming to find failures in cybersecurity and in areas beyond. For instance, can the AI system be induced to change personalities? Does it reveal sensitive information or harm the security and privacy promises made to customers overall? With LLMs, both benign and adversarial usage can produce potentially harmful outputs. This can take many forms, including harmful content such as hate speech, incitement or glorification of violence, or code with vulnerabilities.

In the new era of AI, Microsoft has routinely used red teaming to find failures in production systems before deploying them in products like Bing Chat and Azure OpenAI service.

Pr Cybersecurity Tech Accord principles mapping index on page 125.

**Please see the section about Responsible AI on page 106.**

**Additional information**

Microsoft AI Red Team building future of safer AI | Microsoft

Introduction to red teaming large language models | Microsoft

Failure Modes in Machine Learning—Security documentation | Microsoft

https://t.me/learningnets

# Working together to shape responsible AI

As transformative AI technology promises to reshape many aspects of society, we must work towards a future of responsible AI by design. Responsible AI practices are crucial for maintaining user trust and privacy, and for creating long-term benefits to society.

At the same time, the evolution of AI technology, such as generative AI models, requires us to also evolve cybersecurity practices and threat models to address new challenges. Generative AI models can create realistic content—including text, images, video, and audio—which can be used by threat actors to spread misinformation or create malicious code. To stay ahead of emerging security threats, we must invest in research and development too. Microsoft is committed to ensuring that all our AI products and services are developed and used in a manner that upholds our AI principles.

Simultaneously, we are working with industry partners to develop standards and technologies that enable transparent and verifiable information about the origin and authenticity of digital content to enhance trust online. This includes using advanced detection mechanisms to identify and mitigate potential risks associated with malicious content generation.

Across the globe, the appetite for regulatory guidance on the responsible development and use of AI is growing, with many countries drafting documentation offering guidance for managing emerging risks associated with AI technologies. Previous iterations of AI roadmaps and risk management frameworks include the European Union AI Act and the United States National Institute of Standards and Technology AI Risk Management Framework.

These were primarily focused on responsible development and use of AI and provided important but general definitions and considerations regarding AI threats, vulnerabilities, and responsible use. We now need policies which more specifically address AI security risks at the US federal level. The use of generative AI to enhance cyber exploits is under review at CISA as policymakers consider the need for additional guardrails to prevent abuse of AI.

Pr Pa Em Cybersecurity Tech Accord principles mapping index on page 125.

**For more about AI in cybersecurity, please see pages 100–105.**

## Additional information

AI in Europe: Meeting the opportunity across the EU | Microsoft

The Coalition for Content Provenance and Authenticity – an overview | C2PA

How UNESCO and Microsoft are partnering to advance responsible AI | UNESCO

Meta and Microsoft join the Framework for Collective Action on Synthetic Media | Partnership on AI

How Microsoft Build brings AI tools to the forefront for developers | Microsoft

Commitments to advance safe, secure, and trustworthy AI | Microsoft

How do we best govern AI? | Microsoft

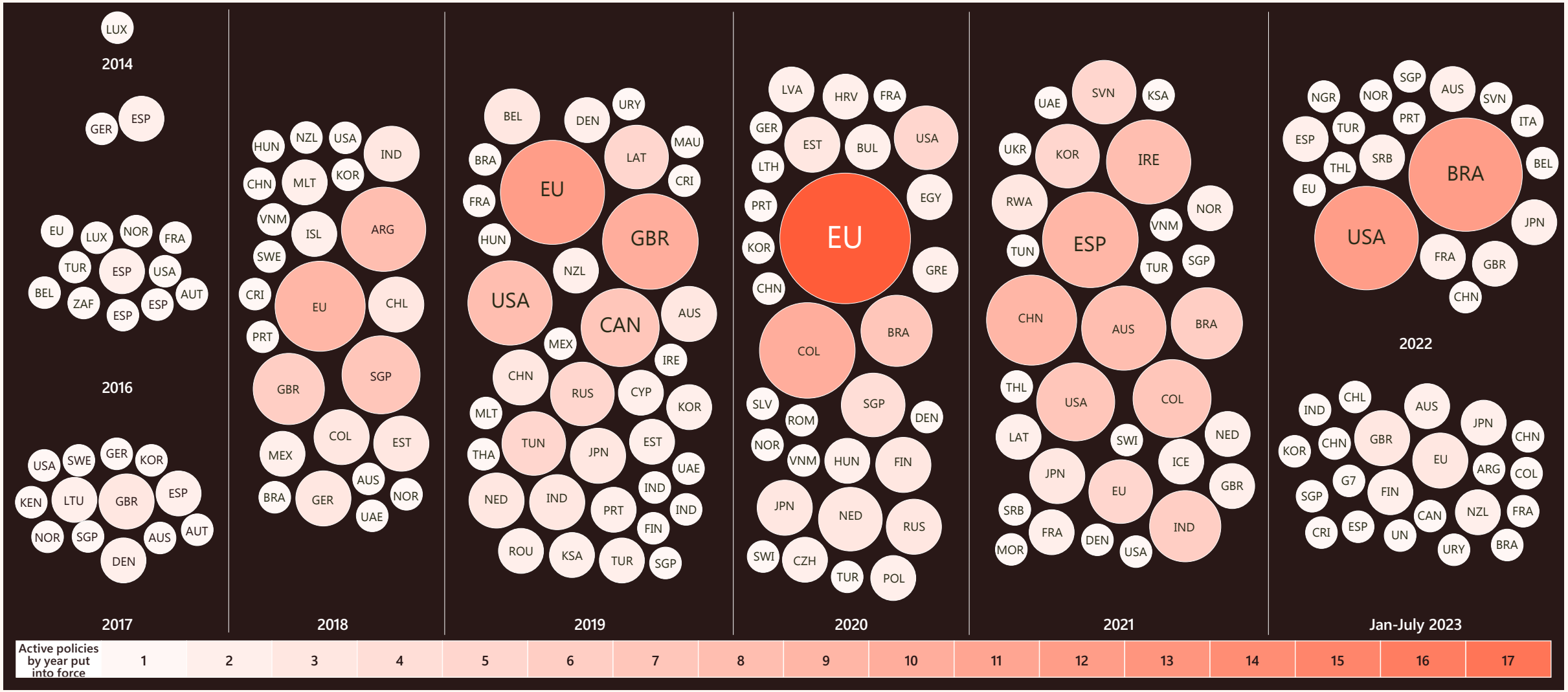
National AI strategies and policies | OECD

Launch of the Frontier Model Forum | Microsoft

https://t.me/learningnets

**Working together to shape responsible AI** continued

# 10 years of global AI policy: active policies




Active policies by country and year of implementation. Source: OECD AI Policy Observatory (OECD.AI) and Microsoft internal tracking for 2023, January-June.

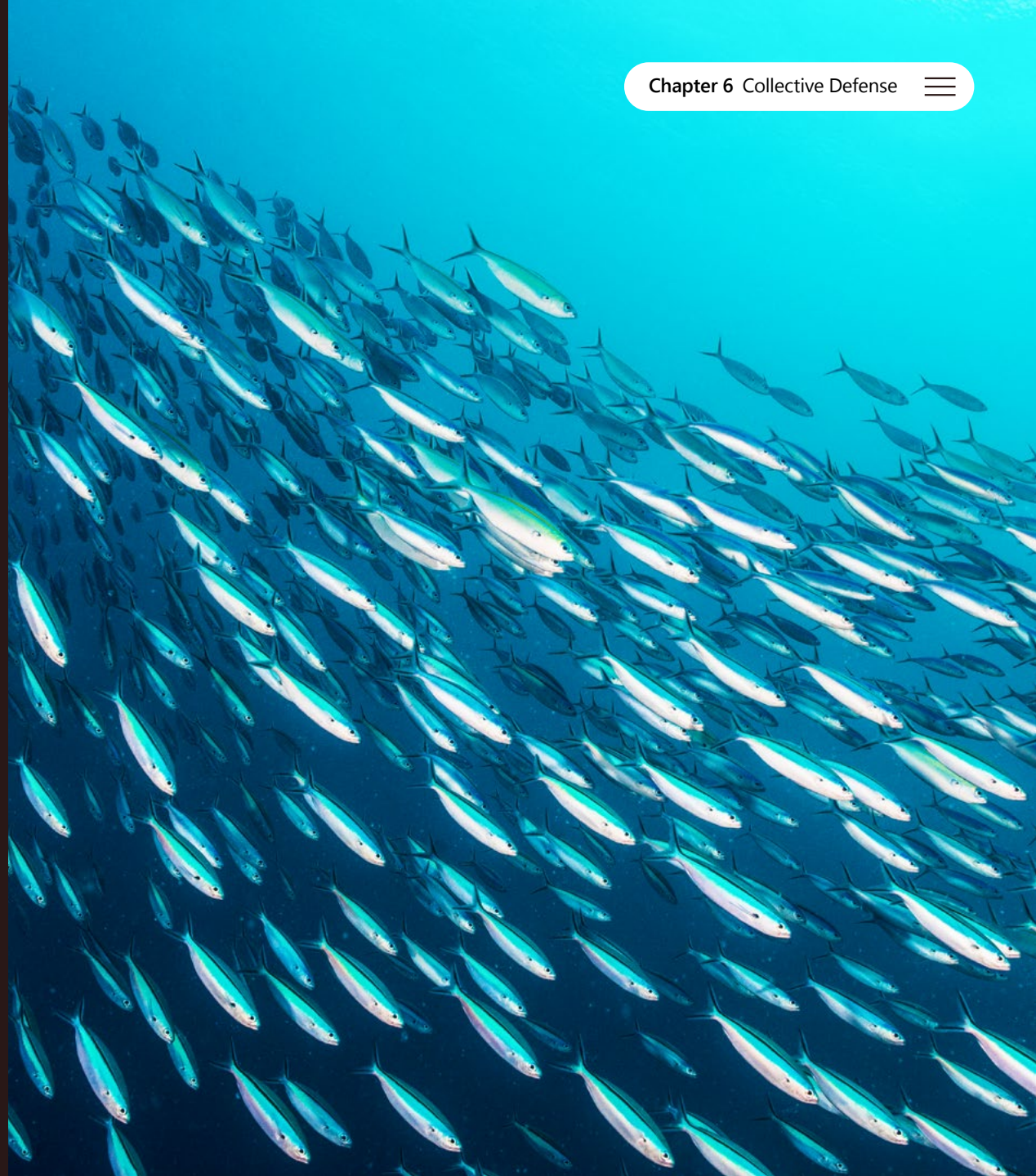
https://t.me/learningnets

# Chapter 6
# Collective Defense

## Mobilizing the power of collaboration


| | |
|---|---|
| Key developments | 109 |
| Introduction | 110 |
| How the global Cybercrime Atlas will revolutionize cybercrime intelligence and collaboration | 111 |
| Collective intelligence and defense against Volt Typhoon | 112 |
| Uniting forces against cybercrime: A success story of collaboration and disruption | 113 |
| Advancing open source security together | 116 |
| Strengthening media content provenance, accountability, and transparency | 117 |
| Combining efforts to safeguard democracy | 118 |
| How we are addressing the digital talent and diversity shortage | 119 |
| The CyberPeace Institute: Uniting to empower nonprofits with cyber resilience | 121 |
| Building cybersecurity capacity through the Cyber Development Goals | 122 |


https://t.me/learningnets



Collective Defense

# Key developments

By forging strong partnerships that transcend borders, industries, and the public-private divide, we are creating a united front against cybercrime.

As cyberthreats evolve, productive relationships across a spectrum of stakeholders will be essential to improve threat intelligence, drive resilience, and contribute to mitigation guidance.

The fragmented cybersecurity landscape means we are not making the most of the vast amount of threat intelligence and data that is available.

**The new Cybercrime Atlas will maximize global data collection while ensuring intelligence is thoroughly cleansed, enriched, and vetted by experts from diverse industries.**

Find out more on page 111

Fewer than

15%

of NGOs have cybersecurity experts on their staff.

**The CyberPeace Institute is providing critical support and assistance to humanitarian organizations.**

Find out more on page 121

**A ground-breaking lawsuit aimed at ending the illicit use of Cobalt Strike shows the power of uniting efforts to identify and take down criminal infrastructure.**

Find out more on page 113

75%

of eligible citizens in democratic nations have the opportunity to vote in the next year and a half. We must ensure that strong cyber defenses keep elections safe.

Find out more on page 118

https://t.me/learningnets

# Empowering a secure future with innovation and collaboration

## Introduction from Teresa Hutson

As technology continues to play an increasingly important role in our lives, it brings both great opportunities and significant risks to our fundamental rights and ability to engage in society.

When we develop technology, we must be thoughtful, champion access to critical services, and build equity into our solutions. At Microsoft, as we work to create a future for everyone, we have a responsibility to support people's digital safety and defend against the challenges presented by technologically enabled bad actors. We also need to uphold human rights, close divides, and partner on collaborative initiatives protecting people and systems' digital security.

Across the globe, Microsoft works closely with our customers and partners to provide security guidance and tools to improve cyber resilience and protect the integrity of digital services, especially in the face of ever-evolving threats. For example, the Microsoft Threat Analysis Center released a report highlighting the increase in Russia's espionage attacks and their development of new forms of ransomware in March 2023, and Microsoft announced its investigation of an Iranian cyberattack against Albania's government in September 2022. Cybercriminals and threat actors are constantly innovating their strategies to leverage technological advancements—but so are we. Working together and providing industry-leading solutions are core to our collective defense efforts.

In this chapter, we offer insights into our collective defense strategies, including support for the World Economic Forum's Cybercrime Atlas initiative and engagement in the Open Source Security Foundation. We also highlight strategic partnerships with threat intelligence organizations to overcome attacks like Volt Typhoon and combat the illicit use of tools like Cobalt Strike. From our role as a founding member of the Coalition for Content Provenance and Authenticity (C2PA) to our partnership with TruePic to create Project Providence, we show how we're working together in new ways to bolster our customers' digital defense capabilities, reduce their cyber risks, and further collaborative projects, such as documenting evidence of cultural heritage site destruction in Ukraine. As part of our commitment to defending democracy, Microsoft's non-partisan election protection efforts extend globally through work with organizations like the International Foundation for Election Systems, to help weave far-reaching networks that enable the sharing of best practices. Our partnerships to protect elections span work with nonprofits including the National Democratic Institute, International Republican Institute, and Freedom House. These are just a few of the many ways in which Microsoft is working cooperatively with leading organizations on innovative solutions to best meet the challenges facing our world today. We are proud to collaborate with other leading technology companies and cross-sector partners to advance open-source security, curb cybercrime, safeguard democracy, and strengthen media content.

Microsoft remains committed to supporting a healthy information ecosystem and addressing evolving threats within the digital spaces in which we operate. Core to this work are diverse strategic partnerships and trained cybersecurity professionals.

The shortage of cybersecurity professionals and the need for AI skills, as discussed in depth later in this chapter, pose significant challenges in today's rapidly changing digital landscape. Robust partnerships with educational institutions, nonprofit organizations, governments, and other businesses are central to our collective defense efforts and skill-building resources that can enable people to adapt amidst constantly shifting challenges. As the threat landscape evolves, we look forward to continuing these and other collective defense engagements with valued partners.

**Teresa Hutson**
Corporate Vice President, Technology for Fundamental Rights

Pr Em Cybersecurity Tech Accord principles mapping index on **page 125.**

Though threats to the information ecosystem have always existed, the tactics adversaries deploy in the digital age are constantly evolving. As a founding member of the Coalition for Content Provenance and Authenticity, Microsoft has helped develop technical standards for certifying the source and history of media content to help combat deepfakes and increase public trust in the media they see.

https://t.me/learningnets

# How the global Cybercrime Atlas will revolutionize cybercrime intelligence and collaboration

There is a vast amount of threat intelligence and data available, but the current fragmented cybersecurity landscape means we are not making the most of it. That is all about to change with the Cybercrime Atlas. It is leveraging open-source intelligence and a global collaboration to shape action, policy, and regulation.

The current landscape of cybercrime intelligence is made up of a patchwork of research efforts. It is complicated by limited cooperation among stakeholders, and by cross-border complexities and challenges posed by different jurisdictions.

As cybercriminals make use of complex, global infrastructure, they produce a vast amount of data that provides surface-level threat information. But the current state of cybercrime intelligence makes it hard to generate meaningful, actionable reports that make use of that data.

The World Economic Forum (WEF) has launched the Cybercrime Atlas initiative with support from companies such as Microsoft, Fortinet, PayPal, and Santander Group. It brings together a diverse community of over 40 private and public sector members to centralize knowledge sharing, collaboration, and research on cybercrime.

Pa **Cybersecurity Tech Accord principles mapping index on page 125.**

The Cybercrime Atlas focuses on cyber-enabled and cyber-dependent crimes of many types, including business email compromise, credit card fraud, malware, and ransomware. It leverages open-source intelligence and adopts a global collaborative approach to gather human-vetted intelligence from sectors such as finance, technology, telecommunications, cybersecurity, and cloud providers.

The goal is to disrupt cybercriminals by providing intelligence that facilitates actions by law enforcement and the private sector, leading to arrests and the dismantling of criminal infrastructures. The initiative creates additional value by offering evidence-based recommendations for policy and regulation changes.

Although still a new initiative, the Cybercrime Atlas will create a standardized and scalable model for open-source intelligence research. It maximizes data collection while ensuring intelligence is thoroughly cleansed, enriched, and vetted by experts from diverse industries. Contextualized intelligence collection facilitates analysis of links to enable the identification of connections between cybercriminals, groups, and shared infrastructure. It also uncovers infrastructure that is used to facilitate large scale criminal activity beyond individual domains or internal protocols (IPs). Some examples are money mule organizers (recruited by fraudsters to assist in moving and transferring illegally obtained funds), "bulletproof" hosting providers (internet hosting services that are resilient to complaints of illicit activities), cryptocurrency wallets, bank accounts, and communication channels.

Microsoft is proud to be supporting the Cybercrime Atlas initiative. We look forward to working with the WEF on driving intelligence collection, facilitating sharing processes, and supporting operations and disruptions. Disrupting global cybercriminals requires a global effort with robust, trusted relationships and collaboration across public and private organizations and industries, and we encourage companies around the world to consider joining the Cybercrime Atlas.

**Additional information**
Forum-hosted Cybercrime Initiative to Boost Coordination between Private Sector and Law Enforcement | World Economic Forum

https://t.me/learningnets

# Collective intelligence and defense against Volt Typhoon

Collaboration between the cybersecurity industry and government research organizations is crucial to understand and overcome common adversaries. As cyberthreats evolve, trusted relationships improve collective knowledge, drive resilience, and inform mitigation guidance across the security ecosystem on a global scale.

Microsoft's unparalleled visibility of the threat landscape provides us with unique insight. To extend this visibility, we have developed a community of strategic partnerships with threat intelligence organizations as we aim to more fully understand and defend against common adversaries. These partnerships which span across the security industry and government research organizations from around the world have become a crucial part of our threat hunting process. The mutual benefit to both parties adds unique value that improves our ability to protect our shared customers.

As part of our analysis of Volt Typhoon attacks against organizations in Guam and the United States, these partnerships helped us expand and analyze more deeply the telemetry we were seeing within our customer environments. Working across private industry to share our research and extending this visibility to government partners then allowed us to rapidly understand the real and potential impact of Volt Typhoon activity and craft a collective response. The outcome of this and many other collaborations have resulted in better protections across the security ecosystem, more comprehensive mitigation guidance, and deeper relationships that help us respond to evolving threats on a global scale.

Op Em Pa Cybersecurity Tech Accord principles mapping index on page 125.

**Additional information**
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques | Microsoft

https://t.me/learningnets

# Uniting forces against cybercrime: A success story of collaboration and disruption

A ground-breaking lawsuit aimed at ending the illicit use of Cobalt Strike shows the power of uniting efforts to identify and take down criminal infrastructure. This collaborative legal action aims to deny criminal infrastructure by leveraging the power of intellectual property right protections.

Microsoft, in collaboration with Fortra LLC and Health-ISAC, has filed a lawsuit in the United States targeting the illicit use of Cobalt Strike—a popular, legitimate penetration testing tool—in connection with malware and ransomware attacks. The lawsuit aims to disrupt infrastructure and malware using cracked versions of Cobalt Strike or violating Microsoft's terms of use regarding malicious use of its copyrighted APIs.

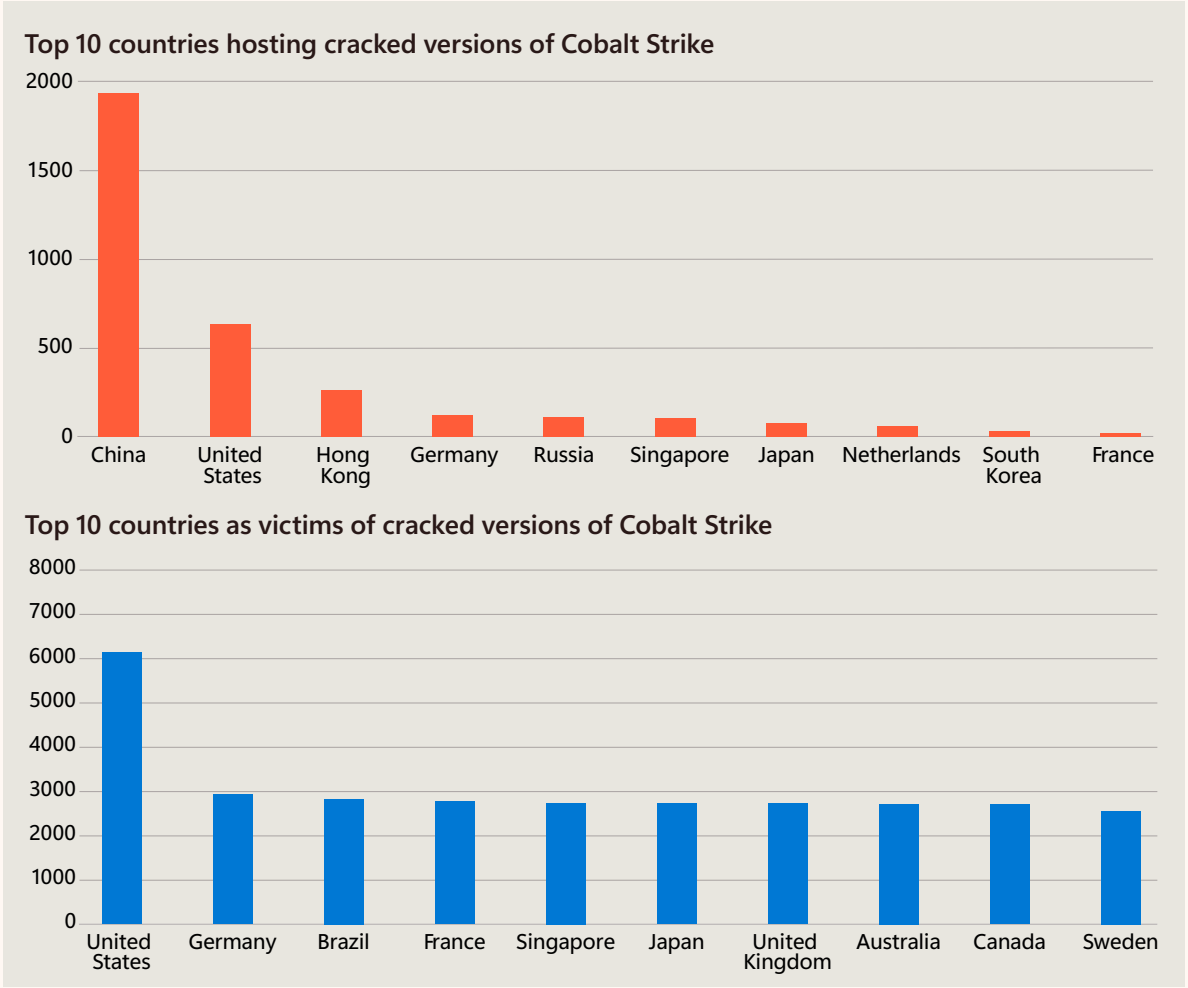
Pr Op Pa Cybersecurity Tech Accord principles mapping index on **page 125**.

https://t.me/learningnets

# Determining cracked versions of Cobalt Strike

Our extensive threat research revealed how widespread the use of cracked versions of Cobalt Strike is in ransomware attacks. Cracked software generally involves circumventing licensing and usage restrictions on commercial software by illegal methods such as modifying code. The cracked version of Cobalt Strike can be used as a post-exploitation tool, enabling cybercriminals to elevate and enumerate access after compromising a victim's system. Numerous cybercrime groups have incorporated cracked Cobalt Strike into their attack chains.

To disrupt these activities, Microsoft's Digital Crimes Unit (DCU) tracked the command and control (C2) infrastructure of Cobalt Strike team servers associated with malware campaigns. We collaborated with Fortra, the owner and licensor of Cobalt Strike, to identify cracked versions of the tool. Fortra licenses Cobalt Strike individually to its customers, each with a unique product key or watermark.




Through infrastructure tracking, we were able to analyze configuration information associated with a validated list of compromised watermarks provided by Fortra. Once identified, that infrastructure was earmarked for legal disruption. Investigators also analyzed specific families of ransomware whose operators use cracked Cobalt Strike, such as Lockbit.

# Leveraging civil laws for disruption

A lawsuit filed in the Eastern District of New York by Microsoft, Fortra, and Health-ISAC accused a sophisticated group of cybercriminals—referred to as John Does 1-16—of violations of the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and common law claims. In a novel application, the Racketeer Influenced and Corrupt Organization Act was also invoked.

The plaintiffs asserted that the cybercriminals leveraged cracked Cobalt Strike as part of a ransomware-as-a-service enterprise. After the court granted injunctive relief, Microsoft, Fortra, and Health-ISAC took down the cracked Cobalt Strike infrastructure by seizing domain names and blocking IP addresses associated with the threat actors' activities.

https://t.me/learningnets

# Impact and victim remediation

While cybercriminals continuously reconfigure their infrastructure, the DCU's development of an automated email notification system tailored to specific regions has shown promising results. At the start of the operation, we were tracking approximately 1,000 active cracked Cobalt Strike servers per day. As of July 2023, there has been a 25 percent reduction globally and a 50 percent reduction in the United States of these servers.

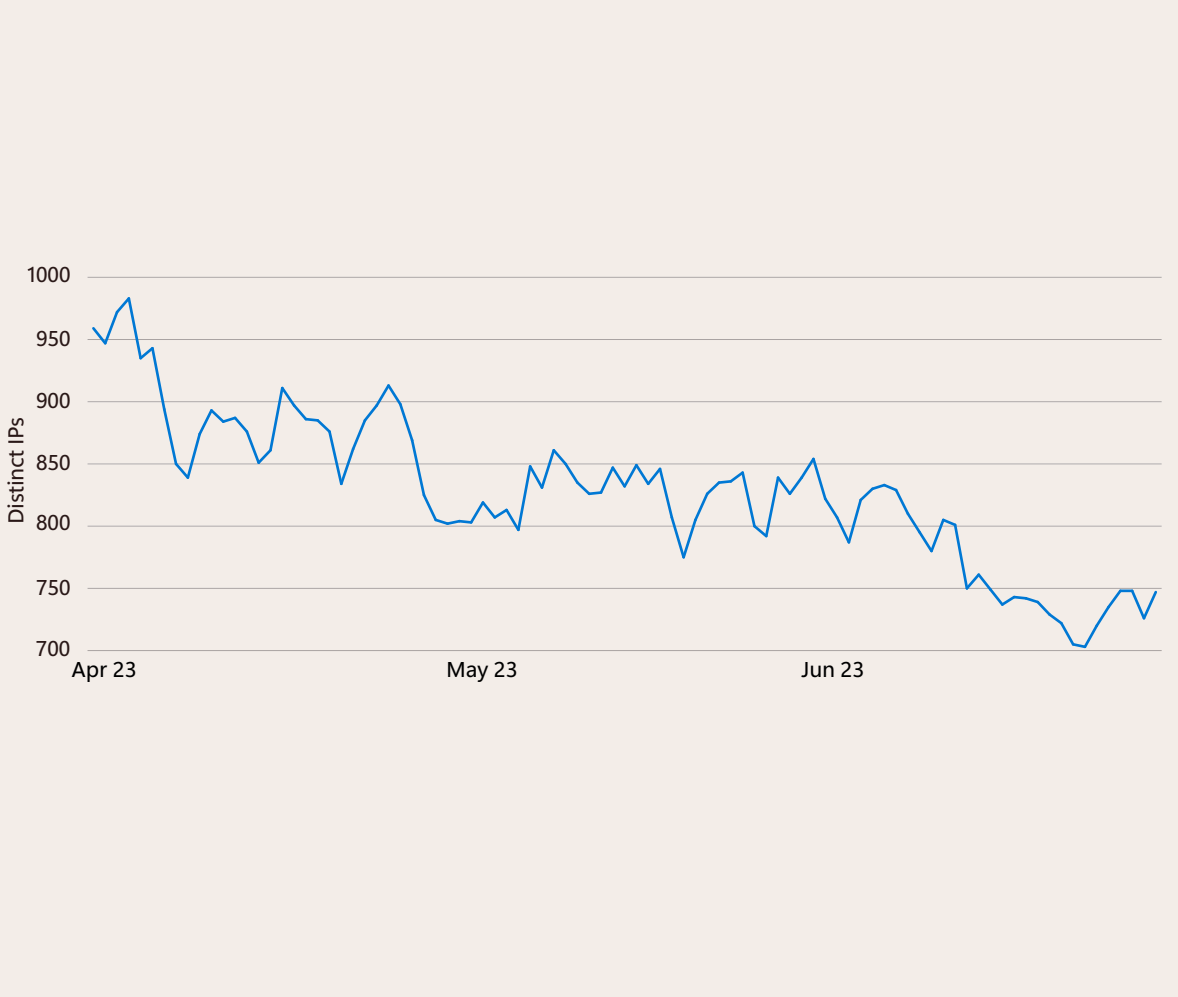
Looking ahead, disrupting the globally hosted cracked Cobalt Strike infrastructure will require collaboration with international partners due to varying legal frameworks. We are working closely with counterparts worldwide to identify local laws and regulations that could facilitate the disabling of malicious C2 infrastructure outside the US.

Op Pa Cybersecurity Tech Accord principles mapping index on **page 125**.

**Additional information**
Stopping cybercriminals from abusing security tools | Microsoft

**Active cracked Cobalt Strike C2s**

Decline in distinct IPs showing the impact of the disruption




Source: Digital Crimes Unit investigations

50%

reduction in the United States of active cracked Cobalt Strike servers.

https://t.me/learningnets

# Advancing open source security together

Leading technology companies collaborate to advance open-source security and fight cybercrime, leveraging the power of open-source communities to create change on a larger scale.

Companies such as Microsoft, Google, Amazon, and IBM are not just competitors, but also peers and partners in the fight against cybercrime. We recognize the importance of ensuring the safety and security of our customers, and have joined forces to advance open-source security, which is crucial for constructing and upholding the digital infrastructure that underpins society. It is essential that we collaborate, pool resources, and channel our collective efforts towards this goal.

While individual contributions to open-source projects are valuable, the power of open-source communities lies in their ability to create change on a much larger scale. This is evident in the crowdsourcing of project development and in building partnerships for supply chain security tools, specifications, and features. By designing projects together, gaining customer buy-in, and inviting contributions from customers and partners, we can continuously improve the project and develop additional paid-for features, products, services, and controls. Industry partners and developers who contribute to the project are incentivized to become evangelists in promoting its benefits.

Open-source collaboration also drives innovation and enhances skills through shared tools and techniques, leveraging the inclusivity and diversity of a community. This is vital for understanding the current supply chain threat landscape and scaling mitigation efforts against emerging threats.

Pr Em Pa Cybersecurity Tech Accord principles mapping index on page 125.

At a macro level this is seen through the establishment of the Open Source Security Foundation (OpenSSF) by Microsoft and Google. This cross-industry organization brings together a community of individuals and companies to help solve current and emerging challenges. An example of this is in security and compliance frameworks, where Google originated Supply Chain Levels for Software Artifacts (SLSA) and Microsoft originated the Secure Supply Chain Consumption Framework (S2C2F). Both were donated to the OpenSSF and are being worked on side by side under the OpenSSF Supply Chain Integrity Working Group.

Together, SLSA and S2C2F provide an end-to-end tool for engineers to better address the nuances of their respective threat landscapes using relevant, scalable mitigation techniques.

**Additional information**
Shaping Europe's digital future: Cyber Resilience Act | European Commission

https://t.me/learningnets

# Strengthening media content provenance, accountability, and transparency

Partnerships are crucial to secure the integrity and accountability of media content by advancing content provenance and authenticity. One example is promoting awareness of crimes committed during wartime.

Microsoft is committed to promoting content provenance and authenticity and implementing technical safeguards to combat malicious manipulation of media. As a founding member of the Coalition for Content Provenance and Authenticity (C2PA) along with Adobe, Arm, the BBC, Intel, Sony, and TruePic, Microsoft has been developing technical standards for certifying the source and history of media content to help combat deepfakes and increase public trust in the media they see.

Pr Pa Cybersecurity Tech Accord principles mapping index on page 125.

We partnered with TruePic to create Project Providence,[1] an interoperable application that utilizes TruePic's authenticating camera SDK and the Microsoft Azure cloud platform. By leveraging the open standard established by C2PA, Project Providence enables seamless interoperability throughout the entire process of capturing, storing, and displaying visual documentation.

"Documenting damage in Ukraine with transparency and authenticity will be critical to pursuing reparations and restoring the demolished objects."

Anti-Corruption Headquarters, Ukraine

During the 2023 Biden Summit for Democracy, Microsoft and TruePic showcased a pilot project aimed at documenting and protecting evidence of cultural heritage site destruction in Ukraine. This initiative—coordinated by an NGO called Pact and executed by the implementing partner Anti-Corruption Headquarters (ACHQ)—involves the documentation and photography of destruction and recovery efforts in eight major cities across Ukraine. The images captured are instrumental to promoting public accountability through ACHQ's Map of Destruction website.[2]

In the first six months following the project's launch, ACHQ documented over 1,000 instances of cultural heritage site destruction. A subset of images has been accepted as evidence in ongoing criminal investigations led by District Prosecutor offices in Ukraine, addressing violations of Customary Law and the Law of War. We are honored to have played a role in supporting ACHQ's mission of increasing accountability for crimes committed during wartime.

**Additional information**

The Coalition for Content Provenance and Authenticity | C2PA

Microsoft invests in the viability of newsrooms globally | Microsoft

https://t.me/learningnets

# Combining efforts to safeguard democracy

Cybersecurity is a keystone of secure election management systems and robust democratic processes. Safeguarding the cyber election space, engaging voters, and teaming up with nonprofits to secure election management systems all help to protect the integrity and resilience of democratic processes globally.

Over 75 percent of eligible citizens living in democratic nations within the next year and a half will have the opportunity to vote.

Elections are on the horizon for many democracies, including in New Zealand, the United Kingdom, the European Union, India, and the United States. Microsoft proactively engages in efforts to support and safeguard its partners in the election space. Additionally, we provide reactive support—both technical and otherwise—for elections commissions, political parties, and related vendors during a pre-defined election period.

In preparation for the 2024 US presidential election, our Democracy Forward team is leading an internal initiative to survey customers in the election management sector, including election management bodies, political entities, and service providers. The aim is to connect them with Microsoft's free offerings designed to enhance the sector's resilience and security. We will prioritize cloud and productivity workloads, providing special support during critical election periods.

The Democracy Forward team leverages Microsoft's extensive network of properties to protect US elections by engaging customers. During the 2022 US midterm elections, we helped register over 50,000 new voters and assisted over 130,000 existing voters in checking their registrations and signing up for election reminders in partnership with Democracy Works' TurboVote program and by utilizing platforms such as Bing, Start, Spotlight, Xbox, and more. Encouraging direct civic involvement, Microsoft and LinkedIn also recruited nearly 1,000 individuals to be poll workers in their communities.

**50,000**

new voters Microsoft helped to register during the 2022 US midterm elections

**130,000**

existing voters assisted in registration checking and election sign up reminders

**1,000**

individuals recruited by Microsoft and LinkedIn to be poll workers in their communities

We extend our election protection efforts globally, collaborating with organizations like the International Foundation for Election Systems on efforts to establish the Election Cyber Readiness Network. This network brings together election management bodies from across Europe and major tech companies in the United States to share best practices, technical knowledge, and threat analysis. We also partner with nonprofits including the National Democratic Institute, International Republican Institute, Carter Center, and Freedom House to protect elections and build societal resilience in areas critical to democratic processes.

Pr Op Pa Cybersecurity Tech Accord principles mapping index on **page 125**.

**Additional information**

The next frontier in elections: Microsoft supports the Council of State Governments' Election Technology Initiative | Microsoft On the Issues

Democracy Forward: Our approach to protecting democracy | Microsoft CSR

In the digital age, democracy depends on information literacy | Microsoft On the Issues

https://t.me/learningnets

# How we are addressing the digital talent and diversity shortage

The scarcity of skilled cybersecurity professionals is a pressing concern for safeguarding critical public and private infrastructure. Insufficient training and certification programs contribute to the deficit of skilled individuals worldwide. According to Cybersecurity Ventures, the demand for cybersecurity jobs is projected to reach 3.5 million by 2025, a staggering 350 percent increase over eight years. The lack of diversity within the current global cybersecurity workforce exacerbates the challenge.[3] With women comprising only 25 percent of the workforce, promoting inclusivity is crucial.

To tackle the talent shortage and promote diversity, Microsoft has expanded its cybersecurity skills initiative to 28 countries, with a special focus on empowering women. Strategic partnerships with organizations like Women in Cybersecurity and the Kosciuszko Institute in Poland are instrumental in training women and directing them toward employment opportunities.

Em Pa Cybersecurity Tech Accord principles mapping index on page 125.

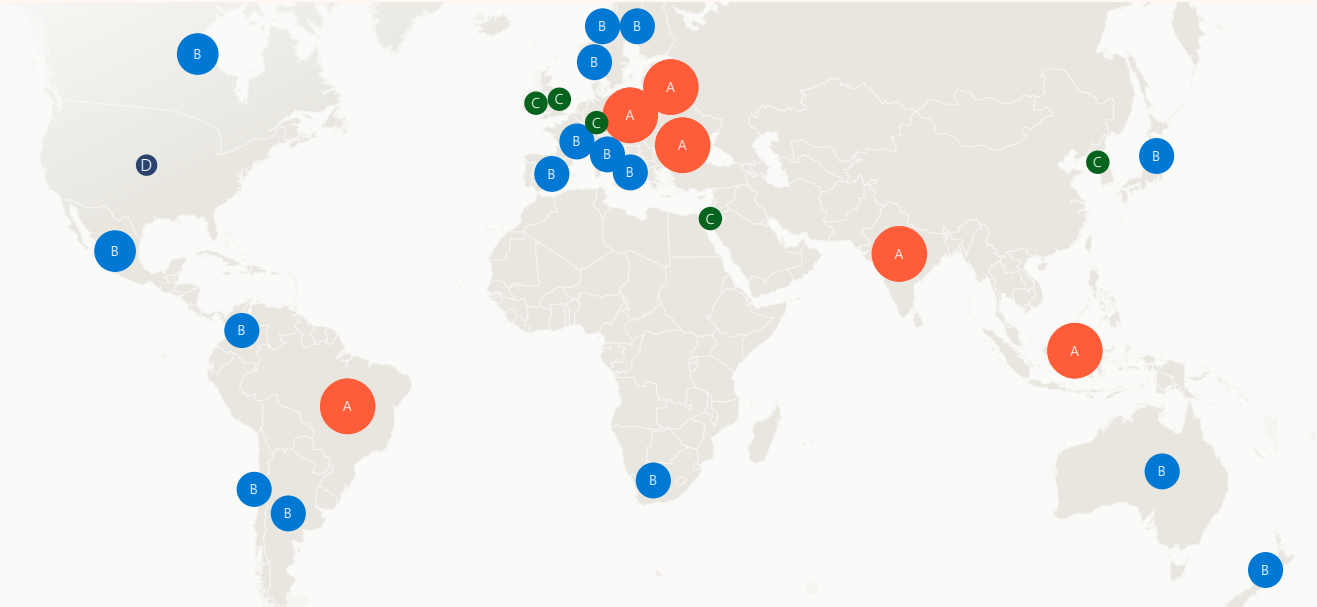
The global shortage of cybersecurity professionals and the need for AI skills pose significant challenges in today's rapidly evolving digital landscape. Strategic partnerships with educational institutions, nonprofit organizations, governments, and businesses are crucial to develop localized cybersecurity and AI skills programs that address market needs.

**The world needs cybersecurity experts**

35%

increase in demand for cybersecurity experts over the past year

**Past year growth by country**



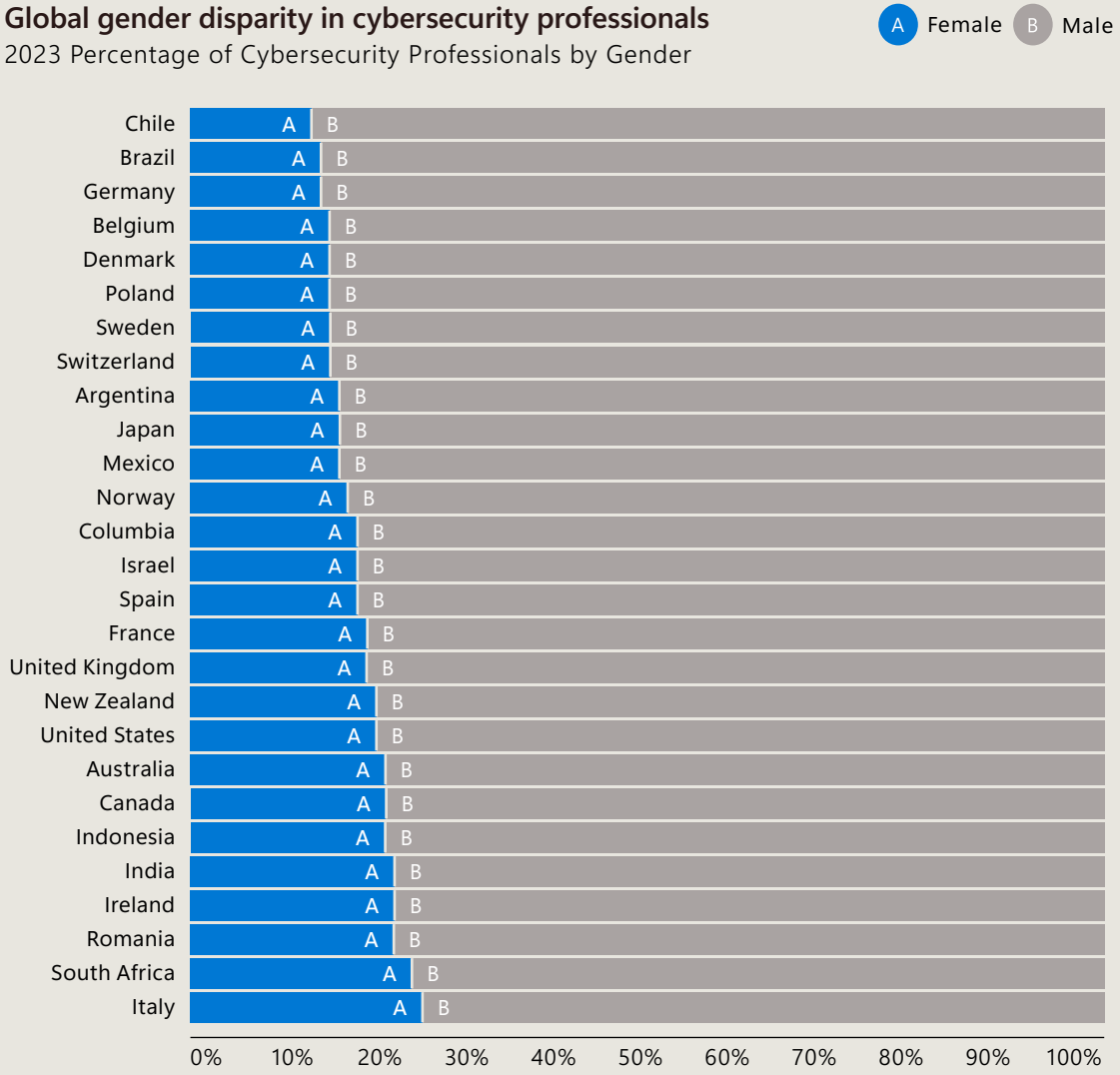

Source: LinkedIn

https://t.me/learningnets

**How we are addressing the digital talent and diversity shortage** continued

## Global gender disparity in cybersecurity professionals

2023 Percentage of Cybersecurity Professionals by Gender




Note: Gender disparity data unavailable for South Korea – Source: LinkedIn

In collaboration with over 20 nonprofit organizations, we have already trained over 400,000 individuals in cybersecurity skills worldwide. Leveraging platforms like Microsoft Learn and LinkedIn Learning, participants have earned valuable security training certificates in courses covering various topics, including systems administration and network security. Meanwhile, the rise of AI presents immense potential for empowering workers globally.

To fully harness AI's potential, however, it is essential to ensure individuals possess the necessary AI skills. According to the Organisation for Economic Cooperation and Development (OECD), there is a significant gender disparity in the field of AI, with women representing four percent of AI professionals globally.[4] The WEF names AI skills as a top priority for companies' training strategies.

To address these issues, Microsoft has launched the AI Skills Initiative aimed at providing people and communities worldwide with the tools to leverage the power of AI effectively.

The Microsoft AI Skills Initiative includes new, free coursework developed in collaboration with LinkedIn. Notably, we introduced the first Professional Certificate on Generative AI in the online learning market. This coursework enables workers to learn introductory AI concepts, including responsible AI frameworks, and receive a Career Essentials certificate upon completion. The Generative AI Skills Grant Challenge, conducted in partnership with data.org, the Microsoft AI for Good Lab, and GitHub, supports organizations in training and empowering the workforce to use generative AI. The program prioritizes fair and community-led implementations of generative AI, particularly with historically marginalized populations.

Em Pa Cybersecurity Tech Accord principles mapping index on **page 125**.

As part of the Skills for Jobs program, Microsoft is committed to bringing digital skills to people worldwide, ensuring their active participation in the digital economy. This new effort in AI skills training represents the next step in that campaign, building on technology innovation and addressing emerging skill gaps.

**28** countries in which Microsoft has expanded its cybersecurity skills initiative

**20** nonprofit collaborators

**400,000** individuals trained worldwide

### Additional information

AI Skills Challenge | Microsoft

The world needs cybersecurity experts | Microsoft

Closing the cybersecurity skills gap | Microsoft

2.5 million-plus cybersecurity jobs are open and women can fill them | Microsoft

Demographics of AI professionals by gender (The Organisation for Economic Co-operation and Development)

https://t.me/learningnets

# The CyberPeace Institute: Uniting to empower nonprofits with cyber resilience

Humanitarian organizations play an essential role in aiding those who need help most and often do the impossible with extremely limited resources. As a result, those resources often do not stretch to cybersecurity. Research shows that fewer than 15 percent of NGOs have cybersecurity experts as staff and that the vast majority do not implement critical cyber hygiene practices, such as multifactor authentication.

In a world where cyberattacks target organizations helping persons fleeing war, data of survivors of violence are sold online, and humanitarian actors are targeted for surveillance. This is an unsustainable position. There is an urgent need to help NGOs protect themselves from cyber threats.

We are therefore extremely proud to support initiatives such as the Humanitarian Cybersecurity Center, launched by the CyberPeace Institute. The Humanitarian Cybersecurity Center provides expert support and practical, free cybersecurity assistance to humanitarian organizations located anywhere in the world, tailored to their needs.

However, it goes beyond working to strengthen the cybersecurity posture of the affected organizations. The CyberPeace Institute investigates and analyzes cyberattacks against NGOs and then creates actionable threat intelligence that can be shared with the community and helps scale protections beyond a single entity.

Over the past year, Microsoft has significantly expanded our engagement with the Institute's volunteer program, CyberPeace Builders. Over 50 Microsoft volunteers are actively engaged in this effort, working to protect nonprofits around the world. To further strengthen this program, we augmented our existing security program for non-profits by providing the CyberPeace Institute with additional threat intelligence tailored to the unique needs of this community.

50+

Microsoft volunteers are actively engaged in our CyberPeace Builders volunteer program.

**Additional information**

Cyber attacks in times of conflict | CyberPeace Institute

Humanitarian Cybersecurity Center | CyberPeace Institute

Cybersecurity Volunteering | CyberPeace Institute

The imperative for digital development and public private partnerships in Least Developed Countries | Microsoft On the Issues

Pr Op Em Cybersecurity Tech Accord principles mapping index on **page 125.**

https://t.me/learningnets

# Building cybersecurity capacity through the Cyber Development Goals

This report highlights the latest cyberthreat trends and showcases the innovative technologies that are being used to address them. But to secure long-term resilience, defenses must be leveraged across the globe, particularly in low- and middle-income countries that lack sufficient cybersecurity. To achieve this, we must integrate cybersecurity capacity building into global sustainable development efforts.

While the role of technology is prioritized in international discussions around sustainable development, cybersecurity is often overlooked, despite its crucial role in maintaining a safe and secure digital ecosystem. Microsoft has partnered with the Swedish Ministry for Foreign Affairs, the Global Forum on Cyber Expertise, and the International Telecommunication Union in a project that aims to secure the adoption of universal cybersecurity goals and targets—the Cyber Development Goals. Inspired by the United Nations Sustainable Development Goals (SDGs), the objective is to establish essential technical, legal, and policy frameworks to help all countries implement global cybersecurity norms.

Em Pa Cybersecurity Tech Accord principles mapping index on page 125.

The project will mobilize global resources and facilitate international cooperation to strengthen cybersecurity capacity building efforts.

Throughout 2023, we convened experts to create a multistakeholder community dedicated to promoting cybersecurity capacity building for a safe and secure digital transformation worldwide. Key initiatives include supporting the development of national cybersecurity strategies, establishing computer security incident response teams or emergency response teams, building technical and forensic expertise, enhancing critical infrastructure resilience, and developing frameworks for incident response.

Microsoft is investing in concrete efforts to improve global cybersecurity resilience. We have launched several initiatives focused on raising awareness, fostering information and expertise exchange on effective policies and approaches to cybersecurity. One example is our partnership with the Swedish Ministry for Foreign Affairs in Africa, which seeks to improve the overall cybersecurity posture of the continent. This sharing of information is crucial among different countries and regions, as well as between and across the public and private sectors.

https://t.me/learningnets

# Appendix
# Additional information


| | |
|---|---|
| Cybersecurity Tech Accord principles mapping index | 124 |
| Contributing teams | 126 |
| Footnotes | 128 |

https://t.me/learningnets

# Cybersecurity Tech Accord

## Principles mapping index

**Pr** **We will protect all of our users and customers everywhere.**

We will strive to protect all our users and customers from cyberattacks—whether an individual, organization or government irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.

We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.

**Op** **We will oppose cyberattacks on innocent citizens and enterprises from anywhere.**

We will protect against tampering with and exploitation of technology products and services during their development, design, distribution, and use.

We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.

**Em** **We will help empower users, customers and developers to strengthen cybersecurity protection.**

We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.

We will support civil society, governments, and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.

**Pa** **We will partner with each other and with likeminded groups to enhance cybersecurity.**

We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open-source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.

We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.

For more on our principles mapping, see pages 8-9.

https://t.me/learningnets

### Chapter 2

| Page | Principle | Explanation |
|---|---|---|
| 14 | Op | Microsoft partnered with Fortra to disrupt a criminal infrastructure that was based on abuse of legitimate software. |
| 16 | Pr | Microsoft Defender Experts send attack progression notifications to customers along with instructions for remediation. |
| 23 | Op Pa | Microsoft and the DCU are leading efforts with partners and will continue to develop technology and legal approaches to bring threat actors to justice. |
| 25 | Op | The approach of our Ransomware Elimination Program is to deter or counter ransomware attacks by removing opportunities for financial gain by threat actors. |
| 25 | Pr Op Em | Integrating what we have learned from our Zero Trust journey, we introduce the "Optimal Ransomware Resiliency State" consisting of 40+ requirements that span myriad aspects of the security landscape. |
| 25 | Pr Em | We identified five foundational principles which we believe every enterprise should implement to defend against ransomware. The Foundational Five are solution-agnostic. |

### Chapter 3

| Page | Principle | Explanation |
|---|---|---|
| 47 | Op | Microsoft mitigated an attack by China-based actor Storm-0558. |
| 79 | Pr | Microsoft Defender for IoT actively monitors critical infrastructure device security to stay ahead of emerging threats. |

### Chapter 4

| Page | Principle | Explanation |
|---|---|---|
| 86 | Pa Op | In May, we warned that Chinese hackers were trying to gain access to US critical infrastructure as part of prepositioning an ability to disrupt communication in case of a future geopolitical crisis. |
| 90 | Em Pa Op | 1. By working together with suppliers and investing in education and awareness training, our goal is to prevent future attacks and ensure swift recovery in case of a breach.<br>2. In collaboration with international partners, we are exploring the use of emerging technologies in AI to revolutionize the security landscape.<br>3. We also work internationally to lobby for rules and norms that would prohibit nation states from engaging in indiscriminate supply chain attacks that put millions of customers at risk. |
| 90 | Pr Em | The Microsoft Security Development Lifecycle (SDL), introduced in 2004, is designed to identify and minimize risks throughout the product lifecycle, meet compliance requirements, and deliver reliable solutions to our customers |
| 91 | Pr Em | To encourage collaboration, Microsoft has created an environment that allows developers to choose the best open source for their needs, without outdated pre-approved lists or manual reviews. |
| 93 | Em Pa | As a co-founding member of the Open Source Security Foundation (OpenSSF), Microsoft is investing in initiatives to enhance the security of the entire open-source ecosystem. |

## Cyber Tech Accord principles mapping index continued

| | | |
|---|---|---|
| 93 | Em | Microsoft recently published and contributed the Secure Supply Chain Consumption Framework (S2C2F) to the OpenSSF, making it available for any development team or organization to adopt. |
| 94 | Em | Microsoft makes supply chain security tools available at no charge to open-source developers. |
| 95 | Pa | In May 2023, we released our Voluntary Commitments to Advance Responsible AI Innovation. |

### Chapter 5

| Page | Principle | Explanation |
|---|---|---|
| 101 | Pr | Across Microsoft, researchers and applied scientists are experimenting with and exploring scenarios to enhance cyber defense. |
| 102 | Em | With a robust LLM-powered solution, cybersecurity analysts can increase productivity with automated scans and anomaly detection, pattern identification, and root cause evidence discovery. |
| 103 | Pr Em | To demonstrate the potential of modern AI in addressing complex challenges and driving innovation, we share some examples of how we've chosen to use LLMs internally to improve security and efficiency. |
| 105 | Em | We share key findings from vulnerability reports with insights into emerging security trends in AI. |
| 105 | Pr | In the new era of AI, Microsoft has routinely used red teaming to find failures in production systems before deploying them in products like Bing Chat and Azure OpenAI service. |
| 106 | Pr Pa Em | 1. Microsoft is committed to ensuring that all our AI products and services are developed and used in a manner that upholds our AI principles.<br>2. We are working with industry partners to develop standards and technologies that enable transparent and verifiable information about the origin and authenticity of digital content to enhance trust online. |

### Chapter 6

| Page | Principle | Explanation |
|---|---|---|
| 110 | Pr Em | Microsoft works closely with our customers and partners to provide security guidance and tools to improve cyber resilience and protect the integrity of digital services. |
| 111 | Pa | The World Economic Forum (WEF) has launched the Cybercrime Atlas initiative with support from companies such as Microsoft, Fortinet, PayPal, and Santander Group. |
| 112 | Op Em Pa | We have developed a community of strategic partnerships with threat intelligence organizations as we aim to more fully understand and defend against common adversaries. |
| 113 | Pr Op Pa | Microsoft, in collaboration with Fortra LLC and Health-ISAC, has filed a lawsuit in the United States aiming to disrupt infrastructure and malware using cracked versions of Cobalt Strike or violating Microsoft's terms of use regarding malicious use of its copyrighted APIs. |
| 115 | Op Pa | We are working closely with counterparts worldwide to identify local laws and regulations that could facilitate the disabling of malicious C2 infrastructure. |
| 116 | Pr Em Pa | We recognize the importance of ensuring the safety and security of our customers, and have joined forces to advance open-source security, which is crucial for constructing and upholding the digital infrastructure that underpins society. |
| 117 | Pr Pa | As a founding member of the Coalition for Content Provenance and Authenticity (C2PA) Microsoft has been developing technical standards for certifying the source and history of media content to help combat deepfakes and increase public trust in the media they see. |
| 118 | Pr Op Pa | 1. Microsoft proactively engages in efforts to support and safeguard its partners in the election space.<br>2. Microsoft extends its election protection efforts globally, collaborating with a network of partners. |
| 119 | Em Pa | 1. To tackle the talent shortage and promote diversity, Microsoft has expanded its cybersecurity skills initiative to 28 countries, with a special focus on empowering women.<br>2. Strategic partnerships with organizations like Women in Cybersecurity and the Kosciuszko Institute in Poland are instrumental in training women and directing them toward employment opportunities. |
| 120 | Em Pa | 1. In collaboration with over 20 nonprofit organizations, we have already trained over 400,000 individuals in cybersecurity skills worldwide.<br>2. The Microsoft AI Skills Initiative includes new, free coursework developed in collaboration with LinkedIn. |
| 121 | Pr Op Em | We augmented our existing security program for nonprofits by providing the CyberPeace Institute with additional threat intelligence tailored to the unique needs of this community. |
| 122 | Em Pa | Microsoft has partnered with the Swedish Ministry for Foreign Affairs, the Global Forum on Cyber Expertise, and the International Telecommunication Union in a project that aims to secure the adoption of universal cybersecurity goals and targets—the Cyber Development Goals. |

https://t.me/learningnets

# Contributing teams

The data and insights presented in this report have been contributed by a diverse group of security-focused professionals from various Microsoft teams. Their shared objective 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 fostering a safer environment for everyone.

### Cloud + AI

**Azure Edge + Platform** is responsible for Microsoft's operating systems, IoT and edge products, engineering systems, and health platforms from the chip level to the cloud. E+P is the platform team for the company and the foundation upon which virtually every Microsoft product and service is built.

**Enterprise & Security** provides platform technologies and solutions to manage and harden platforms against attacks. The team also empowers company-wide security initiatives in Zero Trust, secure identity, secure devices, secure supply chain, and scale management from cloud.

**First-party Tools (aka One Engineering System)** is dedicated to solutions for Microsoft engineering teams to drive consistency and security compliance at scale while managing huge code repositories. The team leads the central strategy for securing Microsoft's end-to-end software supply chain engineering.

**Microsoft Offensive Research & Security Engineering** is a team of elite hackers responsible for securing the operating systems, platforms, and devices built and supported by Microsoft, using red-, blue-, and green-team approaches to simulate attacks and reinforce security and prevention.

**Open-Source Ecosystem** is a team responsible for empowering every person and every organization to contribute and consume open-source software with high quality, good governance, and assurances of compliance and security.

### Corporate, External, and Legal Affairs

**AI for Good Research Lab** harnesses the power of data and AI to address the world's great challenges. The lab collaborates with organizations outside Microsoft in applying AI to improving livelihoods and environments. Areas of focus for the lab include online safety, disaster response, sustainability, and AI for Health.

**Customer Security and Trust** drives continuous improvement of customer security in Microsoft products and online services. Working with engineering and security teams across the company, the team ensures compliance, enhances security, and drives transparency to protect customers and the global ecosystem.

**Digital Crimes Unit (DCU)** is a team of technical, legal, and business experts that have been fighting cybercrime since 2008. Their investigations have disrupted malware infrastructure, seized thousands of domains, and led to hundreds of arrests.

**Digital Diplomacy** is an international team of former diplomats, policy makers, and legal experts working to advance a peaceful, stable, and secure cyberspace in the face of rising nation-state conflict.

**Global Cybersecurity Policy** is 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.

**Microsoft Threat Analysis Center** is a team of experts who analyze nation-state threats, including cyberattacks and influence operations, by combining cyber threat intelligence with geopolitical analysis, and provide insights to customers and Microsoft for effective response and protection.

**Democracy Forward** is a 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.

https://t.me/learningnets

**Contributing teams** continued

### Experiences + Devices

**Devices Supply Chain Security** teams drive and implements end-to-end security across the Microsoft Devices supply chain lifecycle.

### Microsoft Customer and Partner Solutions

**Customer Success** security teams collaborate with customers to expedite security transformation and modernization by sharing best practices, lessons learned, and guidance. They compile and structure Microsoft's and customers' best practices and lessons learned into reference strategies, architectures, plans, and more to facilitate the process.

**Enterprise Mobility** is a team that facilitates the delivery of modern workplace and management solutions to ensure data security across cloud and on-premises environments. Endpoint Manager offers a range of services and tools for managing and monitoring mobile devices, desktop computers, virtual machines, embedded devices, and servers, utilized by both Microsoft and customers.

**Security Service Line (SSL)** is an organization of security experts with deep technical and industry skills who provide incident response, threat intelligence, and cyber resilience services to customers. The SSL maintains strategic partnerships with security organizations, governments, and many internal Microsoft groups.

### Microsoft Security

**Azure Security** is responsible for continuously improving the built-in security posture of Azure at all layers: the datacenter, physical infrastructure, and cloud products and services.

**Customer Ready Intelligence Team** includes specialized analysts responsible for producing and publishing readable threat intelligence content and detections on the threats that most impact customers.

**Cyber Physical Systems Research** consists of domain-expert researchers who specialize in reverse-engineering of IoT/OT malware, protocols and firmware. The team hunts for IoT/OT threats to uncover malicious trends and campaigns.

**Cyber Defense Operations Center (CDOC)** is a fusion center that brings together incident responders, data scientists, and security engineers from across services, products, and devices groups to provide around-the-clock protection against threats to our corporate infrastructure and the cloud infrastructure that customers use.

**Customer Security Policy and Assurance** is a team driving continuous improvement of customer security in Microsoft products and online services, working with engineering and security teams to ensure compliance and transparency.

**Digital Security & Resilience** is the organization led by our Microsoft CISO, and is dedicated to enabling Microsoft to build the most trusted devices and services, while keeping our company and customers protected.

**Identity and Network Access** safeguards Microsoft Entra ID and Microsoft consumer accounts from unauthorized access, account takeover, and abuse. The team delivers Microsoft Entra ID Protection, Conditional Access, multifactor authentication, and the Microsoft Authenticator app, as well as a host of enterprise and consumer account defense systems. They also ensure security and defense of the identity platforms.

**Microsoft Defender Experts** is Microsoft's largest global organization of product-focused security researchers, applied scientists, and threat intelligence analysts.

**Microsoft Defender Threat Intelligence** 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 actor activity and campaigns.

**Microsoft Security Response Center (MSRC) and Identity and Security Operations** are dedicated to creating a secure, defensible environment to protect Microsoft's most valuable assets while simultaneously maximizing the abilities of our users to design, build, and deliver great services.

**Microsoft Threat Intelligence Center (MSTIC)** is a team dedicated to identifying, tracking, and collecting intelligence related to the most sophisticated adversaries impacting Microsoft customers, including nation-state threats, malware, and phishing.

**Strategic Intelligence and Investigation** delivers vital threat analysis on demand. Seasoned analysts use diverse data sets to provide strategic insights to empower timely decision-making about cyberthreats.

### Office of the Chief Financial Officer

**Enterprise Risk Management** works across business units to prioritize risk discussions with Microsoft's senior leadership, and connects multiple operational risk teams, manages our enterprise risk framework, and facilitates internal security assessment using the NIST Cybersecurity Framework.

### Office of the Chief Technology Officer

**Microsoft AI, Ethics and Effects in Engineering and Research** is an advisory board at Microsoft with the mission of ensuring new technologies are developed and fielded in a responsible manner.

### Strategy and Ventures

**Microsoft Security Business Development Team:** A team that oversees and drives Microsoft's long-term investment, partnership, and growth strategy for security, compliance, identity, management, and privacy.

https://t.me/learningnets

# Footnotes

## Chapter 1

| Page | Footnote | |
|---|---|---|
| 7 | 1 | https://arxiv.org/abs/2305.00945 |
| 9 | 2 | https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience |

## Chapter 2

| Page | Footnote | |
|---|---|---|
| 24 | 1 | Ransomware Task Force Gaining Ground—May 2023 Progress Report (securityandtechnology.org) |
| 32 | 2 | Microsoft Threat Intelligence Cyber Signals report, May 2023 |
| 32 | 3 | https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf |
| 33 | 4 | https://www.bbc.com/news/world-africa-59614595 |
| 36 | 5 | FIDO Alliance—Open Authentication Standards More Secure than Passwords |
| 38 | 6 | FBI seized domains linked to 48 DDoS-for-hire service platforms (bleepingcomputer.com) |

## Chapter 3

| Page | Footnote | |
|---|---|---|
| 48 | 1 | https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/ ; https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/ |
| 48 | 2 | https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC |
| 49 | 3 | https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW13xRJ |
| 49 | 4 | https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/ |
| 49 | 5 | https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/ |
| 50 | 6 | www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise |
| 53 | 7 | Microsoft Threat Intelligence, "Iran turning to cyber-enabled influence operations for greater effect," query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW13xRJ; Microsoft Threat Intelligence, "Microsoft investigates Iranian attacks against the Albanian government." |
| 54 | 8 | https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/ |
| 56 | 9 | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397 |
| 57 | 10 | https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/ |
| 59 | 11 | https://pagellapolitica.it/articoli/amedeo-avondet-fratelli-italia-russia |
| 59 | 12 | https://www.washingtonpost.com/world/2023/04/21/germany-russia-interference-afd-wagenknecht/ |
| 59 | 13 | https://apnews.com/article/russia-ukraine-technology-social-media-misinformation-05d147b128c48bfa23705409448b7bbc |
| 61 | 14 | https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518 |
| 61 | 15 | https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/ |
| 63 | 16 | https://archive.ph/GWW0D/image |
| 63 | 17 | https://archive.ph/oAn4j |
| 64 | 18 | https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/ |
| 64 | 19 | https://archive.ph/QXvtw |
| 64 | 20 | miburo.substack.com/p/csm-influencer-ops-1; miburo.substack.com/p/chinese-state-medias-global-influencer; These statistics reflect data as of April 2023. |
| 66 | 21 | https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/ |
| 66 | 22 | https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps |
| 66 | 23 | Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets \| Microsoft Security Blog |
| 67 | 24 | https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/ |
| 67 | 25 | https://www.reuters.com/world/middle-east/hackers-breach-iran-rail-network-disrupt-service-2021-07-09/ |
| 68 | 26 | https://blogs.microsoft.com/on-the-issues/2023/02/03/dtac-charlie-hebdo-hack-iran-neptunium/ |
| 68 | 27 | https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ |
| 69 | 28 | We conducted an in-depth review of the reports, which did not reveal signs of inauthentic material and we were able to verify the authenticity of some of the leaked details. |
| 70 | 29 | https://www.theguardian.com/world/2023/jan/01/kim-jong-un-north-korea-exponentially-increase-nuclear-warhead-production<br>https://en.yna.co.kr/view/AEN20230406000800325?section=nk/nk |
| 70 | 30 | nknews.org/pro/cybercrime-funds-half-of-north-koreas-missile-program-us-official-says |
| 71 | 31 | https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft |
| 71 | 32 | https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise |
| 71 | 33 | https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/ |
| 72 | 34 | https://apnews.com/article/russia-ukraine-business-north-korea-e6a068d91bc9828ecadfb67c929a4162<br>https://www.nknews.org/2023/05/russia-sent-over-1k-tons-of-wheat-flour-to-north-korea-state-agency-says/ |

https://t.me/learningnets

**Footnotes** continued

| | | |
|---|---|---|
| 73 | 35 | www.clearskysec.com/iec/; www.cfr.org/backgrounder/what-hamas; www.cia.gov/the-world-factbook/countries/gaza-strip/. |
| 73 | 36 | https://www.cia.gov/the-world-factbook/countries/west-bank/ |
| 73 | 37 | www.timesofisrael.com/hamas-secretly-operating-cyber-counterintelligence-hq-in-turkey-report/; www.thetimes.co.uk/article/hamas-running-secret-cyberwar-hq-in-turkey-29mz50sxs. |
| 74 | 38 | https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229 |
| 74 | 39 | https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/ |
| 74 | 40 | https://cybertechaccord.org/new-industry-principles-to-curb-cyber-mercenaries/ |

## Chapter 4

| Page | Footnote | |
|---|---|---|
| 78 | 1 | Microsoft Defender for IoT and your network architecture—Microsoft Defender for IoT \| Microsoft Learn |
| 80 | 2 | https://adolus.com/ |
| 84 | 3 | https://www.microsoft.com/en-us/security/blog/2023/08/10/multiple-high-severity-vulnerabilities-in-codesys-v3-sdk-could-lead-to-rce-or-dos/ |
| 86 | 4 | 2023 Annual Threat Assessment of the U.S. Intelligence Community (odni.gov) |
| 86 | 5 | Volt Typhoon targets US critical infrastructure with living-off-the-land techniques \| Microsoft Security Blog |
| 86 | 6 | New "Prestige" ransomware impacts organizations in Ukraine and Poland \| Microsoft Security Blog |
| 90 | 7 | https://www.sonatype.com/state-of-the-software-supply-chain/introduction |
| 90 | 8 | https://www.microsoft.com/en-us/securityengineering/sdl/ |
| 90 | 9 | https://www.microsoft.com/en-us/security/blog/2021/02/25/microsoft-open-sources-codeql-queries-used-to-hunt-for-solorigate-activity/ |
| 91 | 10 | https://azure.microsoft.com/en-us/products/devops/github-advanced-security |
| 92 | 11 | https://github.com/NuGet/Home/issues/12407 |
| 93 | 12 | A Summary of Census II: Open Source Software Application Libraries the World Depends On—Linux Foundation |
| 93 | 13 | Open Source Security and Risk Analysis Report \| Synopsys |
| 94 | 14 | https://octoverse.github.com/2022/developer-community |
| 94 | 15 | https://www.infosecurity-magazine.com/news/software-supply-chain-attacks-hit/ |
| 94 | 16 | https://www.infosecurity-magazine.com/news/software-supply-chain-attacks-hit/ |
| 94 | 17 | https://github.com/advisories, 31 May 2023 |

## Chapter 5

| Page | Footnote | |
|---|---|---|
| 100 | 1 | Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com) |
| 100 | 2 | Gartner Top Security and Risk Trends in 2022 |
| 105 | 3 | https://blogs.microsoft.com/on-the-issues/2023/05/25/how-do-we-best-govern-ai/ |

## Chapter 6

| Page | Footnote | |
|---|---|---|
| 117 | 1 | https://www.globenewswire.com/news-release/2023/03/27/2634708/0/en/Truepic-and-Microsoft-Pilot-New-Provenance-Platform-to-Authenticate-Images.html |
| 117 | 2 | https://shtab.net/en/news/view/antikorupcijnij-shtab-zapustiv-novij-instrument-ka/ |
| 119 | 3 | Source: https://cybersecurityventures.com/jobs/ |
| 120 | 4 | Source: OECD.AI (2023), visualisations powered by Tableau using data from Stackoverflow, accessed on www.oecd.ai. Supported by the Patrick J. McGovern foundation. |

https://t.me/learningnets

Microsoft

# Microsoft Digital Defense Report

## Building and improving cyber resilience

**Learn more:** https://microsoft.com/mddr

**Dive deeper:** https://blogs.microsoft.com/on-the-issues/

**Stay connected:** @msftissues and @msftsecurity

October 2023
Microsoft Threat Intelligence

https://t.me/learningnets