FORTINET

Outbreak Alerts
Annual Report 2023

FortiGuard Labs

START >

FortiGuard Labs

Outbreak Alerts Annual Report 2023

Table of Contents

Table of Contents

FortiGuard Labs

Outbreak Alerts Annual Report 2023

Executive Summary

In year 2023, FortiGuard Labs blocked 2.4 trillion vulnerability attempts and 3 billion malware deliveries to protect its customers from cyber threats. FortiGuard Labs escalated the significant threats through the Outbreak Alert system to raise awareness.

This annual report covers:

- The categories and timeframe of more than three-dozen Outbreak Alerts on vulnerabilities, targeted attacks, ransomware, and OT/IoT related threats
- Highlights of significant outbreaks and several prevalent vulnerabilities and malware
- Real-world telemetries compiled by FortiGuard Labs showing exploitation attempts and malware deliveries
- Context around the entire attack surface to understand the components that can aid in protection, detection and response

2.4 trillion
Vulnerability attempts blocked by FortiGuard

38 Outbreak Alerts

FortiGuard blocked 3 billion malware delivery and 90 million 0-day

Cyber Threat R&D Centers **6**

Operations Centers **3**

Cyber Consultation **11**

FortiGuard Labs

Outbreak Alerts Annual Report 2023

Outbreaks Summary

In 2023, FortiGuard Labs released numerous outbreak alerts each month, making it a notable year in terms of the frequency of significant incidents with widespread reach.

These outbreaks highlighted the various targeted and 0-day attacks, weaponized vulnerabilities, malware/ransomware campaigns, and OT/IoT threats launched last year.

This diversity emphasizes the importance of timely threat intelligence, proactive protections, and a multi-layered security approach to ensure organizations remain safe by addressing all threat vectors.

Vulnerabilities (23)

- Adobe ColdFusion Deserialization of Untrusted Data
- Apache RocketMQ RCE
- Cacti Command Injection
- CWP Control Web Panel Command Injection
- Fortra GoAnywhere MFT RCE
- Google Chromium WebP
- IBM Aspera Faspex RCE
- Ivanti Endpoint Manager Mobile Authentication Bypass
- JetBrains TeamCity Authentication Bypass
- Joomla! CMS Improper Access Check
- Microsoft Office and Windows HTML RCE
- Microsoft Outlook Elevation of Privilege
- Oracle WebLogic Server
- PaperCut MF/NG Improper Access Control
- Progress MOVEit Transfer SQL Injection
- Teclib GLPI RCE
- ThinkPHP RCE
- TP-Link Archer AX-21 Command Injection
- VMware Aria Operations for Networks Command Injection
- WooCommerce Payments Improper Authentication
- Zoho ManageEngine RCE
- Zyxel Multiple Firewall
- Zyxel Router Command Injection

Targeted Attack (8)

- 3CX Supply Chain Attack
- Apache ActiveMQ Ransomware Attack
- Cisco IOS XE Web UI Attack
- Citrix Bleed Attack
- HTTP/2 Rapid Reset Attack
- Progress Telerik UI Attack
- Realtek SDK Attack
- VMware ESXi Server Ransomware Attack

Malware (3)

- Agent Tesla Malware Attack
- Lazarus RAT Attack
- Router Malware Attack

OT/IoT (4)

- CosmicEnergy Malware
- Multiple Vendor Camera System Attack
- SolarView Compact Command Injection
- TBK DVR Authentication Bypass Attack

List of Outbreak Alerts per category

FortiGuard Labs

Outbreak Alerts Annual Report 2023

Outbreak Release Timeline

The data reveals a continuous stream of critical cyber threats throughout the 2023. There were notable increases in the number of outbreaks between March and July.

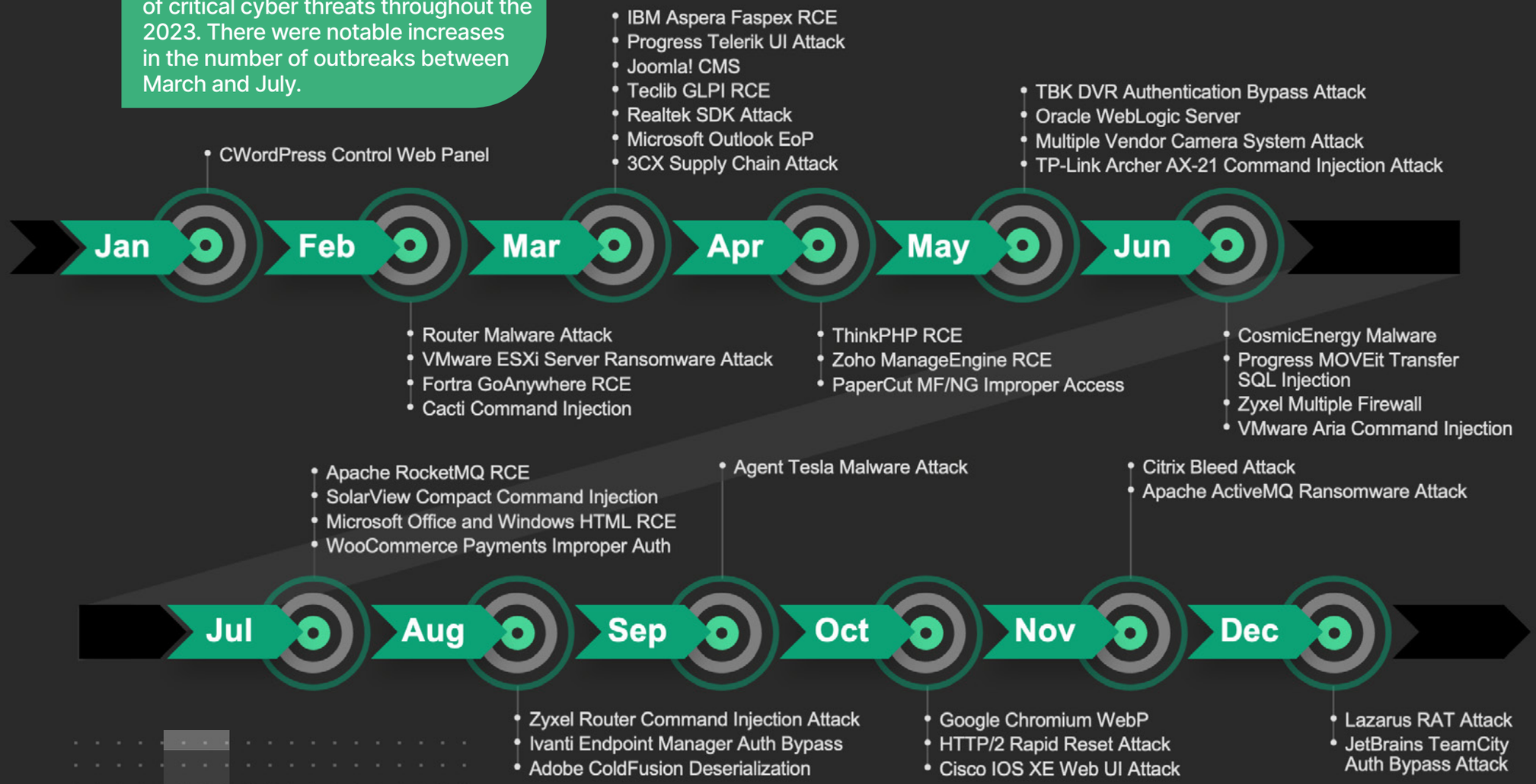


Figure 1: Outbreak Alerts timeline

Let's focus on several significant outbreaks in 2023:

3CX Supply Chain Attack

Trojanized VoIP application

(CVE-2023-29059)

APT Group(s)	Labyrinth Chollima
Darknet Activity	Yes

FortiGuard Labs observed that threat actors abused a popular business communications software produced by 3CX.

This voice and video conferencing application was trojanized to attack multiple organizations to gather sensitive information using an info stealer malware. Based on the telemetries from blocked malware, the victims' geographic spread spanned Australia, Austria, Canada, Germany, Italy, the Netherlands, South Africa, Switzerland, the United States and the United Kingdom.

For more info: Outbreak | Threat Research

Agent Tesla Malware Attack

New variant in the wild

(CVE-2018-0802, CVE-2017-11882)

APT Group(s)	Bitter, Cloud Atlas, OceanLotus, Ta413, Tonto Team
Ransomware Group(s)	REvil

In September 2023, FortiGuard Labs detected a phishing campaign that exploits Microsoft Office vulnerabilities and disseminates a new variant of Agent Tesla malware.

This malware has been seen with multiple iterations for almost a decade. In this particular campaign, it utilized a Remote Access Trojan (RAT) to initiate access and data-stealing mechanism to extract sensitive information from stored credentials, keylogging data, and screenshots from various software programs like Google Chrome, Mozilla Firefox, and Microsoft Outlook.

For more info:
Outbreak | Threat Research

Significant Outbreaks in 2023:

Fortra GoAnywhere MFT RCE

A zero-day exploited in the wild

(CVE-2023-0669)

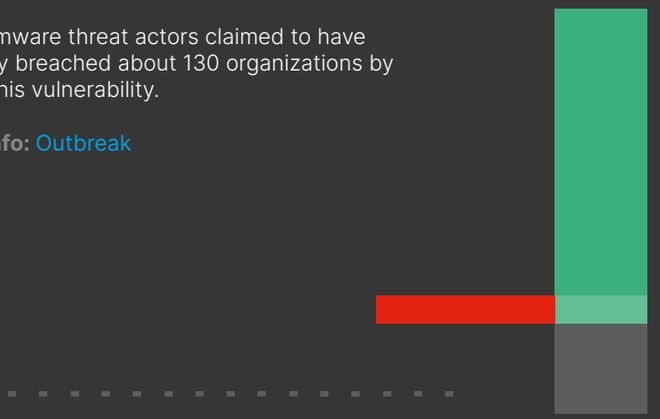
Ransomware Group(s)	Cl0p, Ta505
Exploit publicly available	Yes

Fortra GoAnywhere MFT software is a secure managed file transfer solution that streamlines the exchange of data between systems, employees, customers, and trading partners.

The security flaw tagged CVE-2023-0669 enables attackers to remotely execute code on unpatched GoAnywhere MFT.

Clop ransomware threat actors claimed to have successfully breached about 130 organizations by exploiting this vulnerability.

For more info: Outbreak



HTTP/2 Rapid Reset

Zero-day DDoS attack

(CVE-2023-44487)

Exploit publicly available	Yes
Darknet Activity	Yes

HTTP/2 protocol aims to address the limitations of HTTP/1.1 by providing a more efficient and faster web browsing experience.

It is widely adopted by modern web browsers and public cloud servers to optimize the delivery of web content. The HTTP/2 Rapid Reset is a distributed denial of service (DDoS) attack on Web servers. The attack leverages a flaw in the implementation of protocol HTTP/2 by sending high volume of HTTP requests.

Attackers can cause a significant increase in the CPU utilization on the servers that eventually can cause denial of service by resource exhaustion. In October 2023, Google posted a report that they've blocked the largest attack in history which reached up to 398 million requests per second.

For more info: Outbreak

Significant Outbreaks in 2023:

JetBrains TeamCity Authentication Bypass

Advanced Persistent Threat Groups exploiting the flaw in (CI/CD) application

(CVE-2023-42793)

APT Group(s)	Apt29, Diamond Sleet
Darknet Activity	Yes

Multiple threat actors have been seen exploiting the authentication bypass flaw in JetBrains TeamCity that led to remote code execution.

If compromised, these attackers could access a TeamCity server, gaining entry to the software developer's source code, signing certificates, and software deployment procedures. This access could also be misused to carry out attacks on supply chain operations.

For more info: Outbreak | Threat Research

Lazarus RAT Attack

APT groups exploiting Log4j2 vulnerability to deploy Remote Access Trojans (RAT)

(CVE-2021-44228)

APT Group(s)	Andariel, Dev-0270, Lazarus, Phosphorus, Teal Kurma
Ransomware Group(s)	Lockbit

In March 2023, a new campaign conducted by the Lazarus and other groups were seen employing new DLang-based Remote Access Trojans (RATs) malware in the wild.

The APT groups were targeting manufacturing, agricultural and physical security companies by exploiting the Log4j vulnerability and using it for initial access leading to a C2 (command and control) channel with the attacker.

For more info: Outbreak

Significant Outbreaks in 2023:

Progress MOVEit Transfer SQL Injection

Exploited in data theft and ransomware attacks

(CVE-2023-34362, CVE-2023-35708, CVE-2023-35036)

Ransomware Group(s)	Cl0p
Darknet Activity	Yes

MOVEit Transfer is a managed file transfer (MFT) solution developed by Ipswitch, a subsidiary of Progress Software, that allows an enterprise to securely transfer files between business partners and customers using SFTP, SCP, and HTTP based uploads.

Allegedly exploited by the Cl0p ransomware threat actor, high-profile government, finance, media, aviation, and healthcare organizations have reportedly been affected, with data exfiltrated and stolen.

The attack stemmed from multiple SQL injection vulnerability found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.

The attacker may then be able to execute malicious SQL code that can change or delete database elements.

For more info: Outbreak | Threat Research

Vulnerability Profile

The cyber actors choose vulnerabilities to exploit based on several factors including consideration of strategic goals, industry-specific targets, and evasion tactics in selecting vulnerabilities for exploitation. Understanding different vulnerability types and prioritizing the remediation are crucial to a risk based approach to security.

That brings several advantages, such as...

Risk Assessment

Identify the vulnerability types, assess their potential risks associated with specific weaknesses in systems, applications, or networks and then prioritize security efforts by focusing on vulnerabilities with higher risk levels.

Attack Surface Analysis

Understand the entry point that could be exploited by attackers to guide efforts to reduce and secure based on the vulnerability types and their attack vector.

Effective Mitigation Strategies

Implement targeted security measures, such as patching software, improving coding practices, and configuring systems securely based on vulnerability types that require distinct mitigation strategies.

Prioritization of Resources

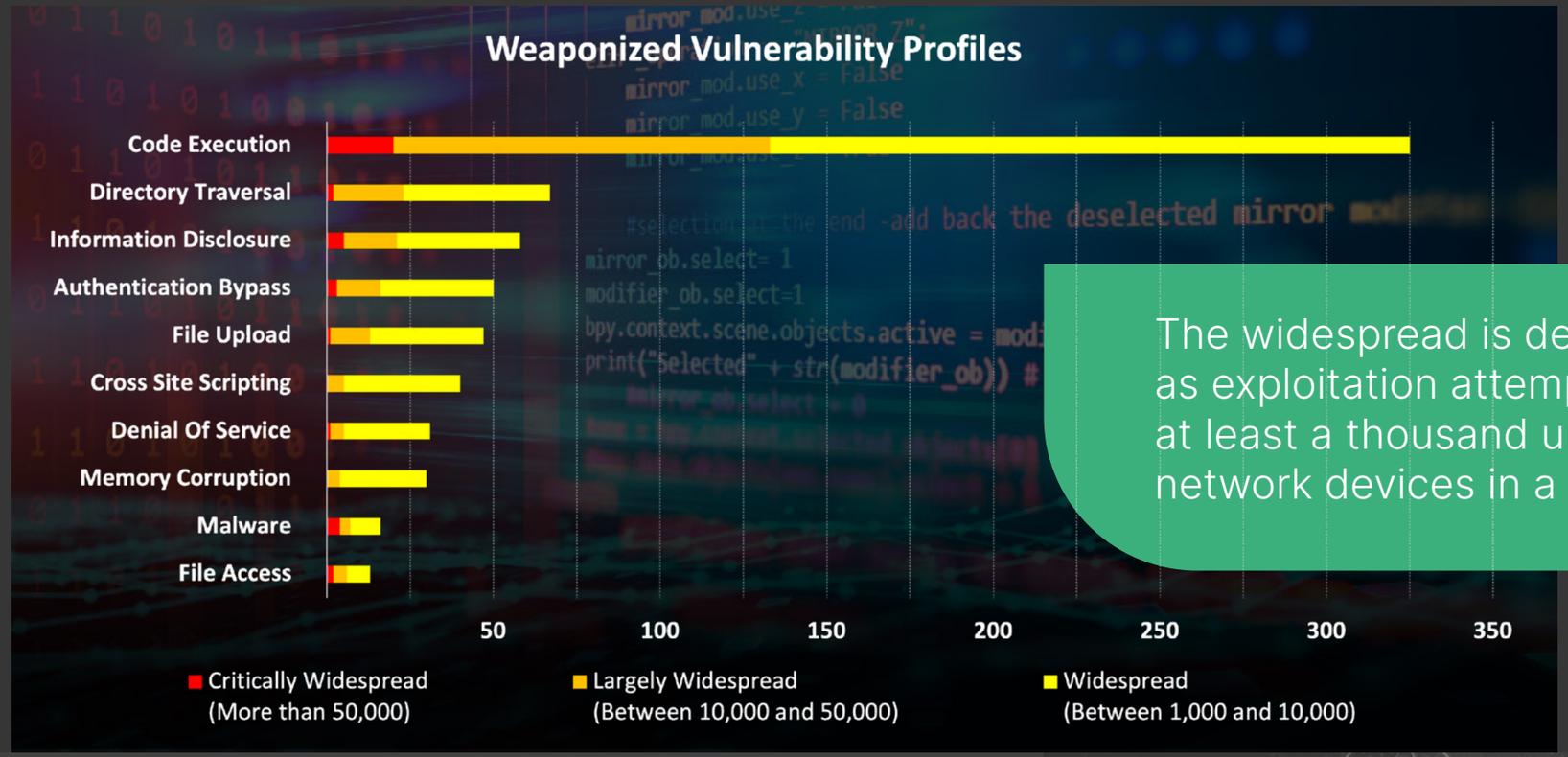
Allocate resources efficiently and focus on addressing high-priority vulnerabilities that pose the greatest risk based on the vulnerability types and their varying levels of impact and exploitability.

Weaponized Vulnerability Profiles

In 2023, the number of actively targeted vulnerabilities with widespread attack had increased by 15%.

Attackers choose vulnerabilities based on ease of exploitation, potential impact, commonly-used application, and financial incentives. Rightly so, Remote Code Execution (RCE) vulnerabilities were prevalent due to their wide impact on various systems, versatility for attackers, and potential for wormable attacks.

For instance, there were 325 weaponized and widespread remote code execution vulnerabilities. Out of those, 20 vulnerabilities had been attempted on more than 50,000 devices in a single month.



The widespread is defined as exploitation attempts of at least a thousand unique network devices in a month.

Figure 2: Vulnerability profile count categorized by widespread.

Widely Targeted Vulnerabilities

Apache Log4j Remote Code Execution

(CVE-2021-44228)

APT Group(s)	Andariel, Budworm, Cobalt Mirage, Dev-0270, Lazarus, Muddywater, Phosphorus, Teal Kurma
Ransomware Group(s)	Lockbit, Avos

On the top of chart is still the infamous remote code execution on Apache Log4j with an average of 90,000 unique devices per month.

This vulnerability was quite epidemic because it was used alongside the recent Lazarus Remote Access Trojan Attack.

For more info: Outbreak
Detection Signature: Intrusion Prevention

Figure 3: Number of network devices that blocked exploitation attempts of the Apache Log4J2 vulnerability

Widely Targeted Vulnerabilities

Cisco IOS XE Web UI

(CVE-2023-20198)

Exploit publicly available	Yes
Darknet Activity	Yes

A recent vulnerability on Cisco IOS XE Web UI was a popular target.

The detection signature was released mid-October and had already record exploit attempts on 60,000 unique devices in October 2023. The vulnerability exploits a backdoor access on a Cisco Web interface via a crafted HTTP request.

For more info: Outbreak
Detection Signature: Intrusion Prevention

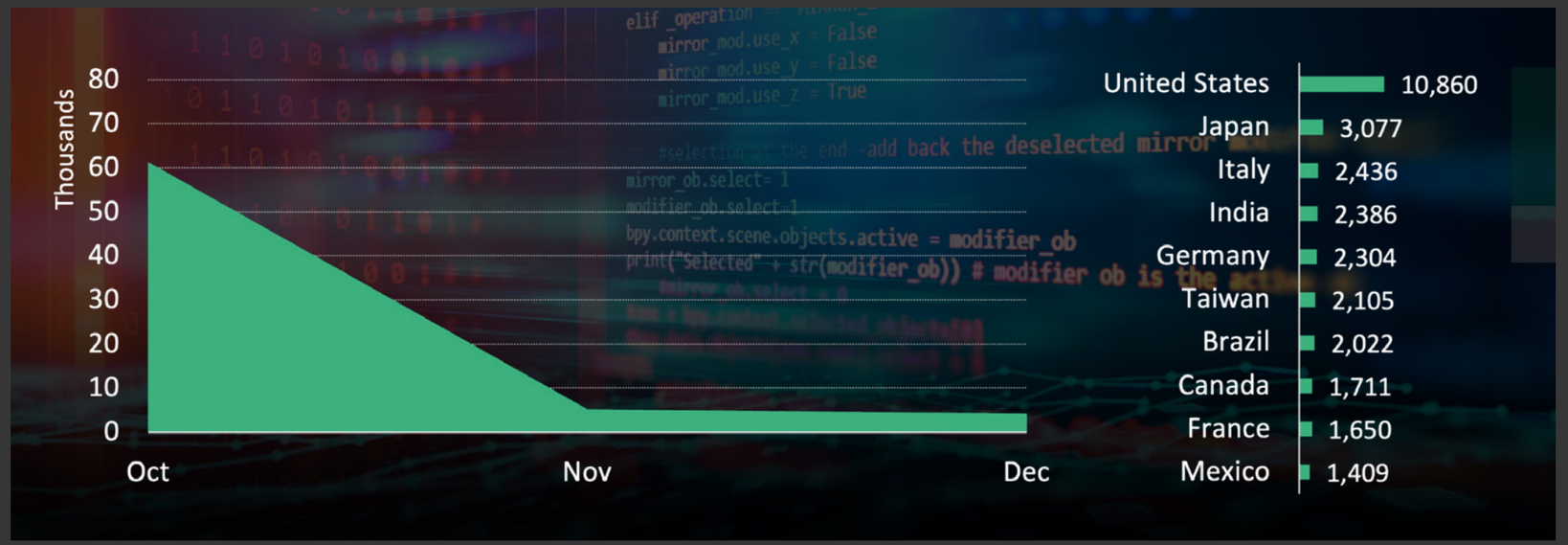


Figure 4: Number of network devices that blocked exploitation attempts of the Cisco IOS XE vulnerability.

Widely Targeted Vulnerabilities

NetLink and Zyxel Router Attacks

(CVE-2017-18368)

The vulnerabilities on NetLink and Zyxel network devices came in second and third on the top weaponized vulnerabilities with each an average of 80,000 unique devices per month.

Several malware attacks such as MooBot, Lucifer, BotenaGo, Zerobot and Enemybot had been targeting these vulnerabilities for the entire year which likely prove successful exploitation.

Detection signature for NetLink vulnerability:
Intrusion Prevention

Detection signature for Zyxel vulnerability:
Intrusion Prevention

Figure 5: Number of network devices that blocked exploitation attempts of the NetLink vulnerabilities

Figure 6: Number of network devices that blocked exploitation attempts of the Zyxel vulnerability

Malware Profile

Overall Malware and 0-day Detections

In the year 2023, FortiGuard Labs observed an average of 250 million total malware detections per month. Among those were 6 million 0-day (or unknown) malware detections per month.

The Microsoft Windows executable file type remained the most common vehicle for malware attacks followed by Microsoft Office file type.

Similar to the previous year, the top malwares were the MSOffice/CVE_2017_11882.C and MSExcel/CVE_2018_0798.BOR which are both file-based stack buffer overflow vulnerability in Microsoft Office.

The exploit can run malicious shellcode which will allow the malware to attempt to download the next malicious payload.

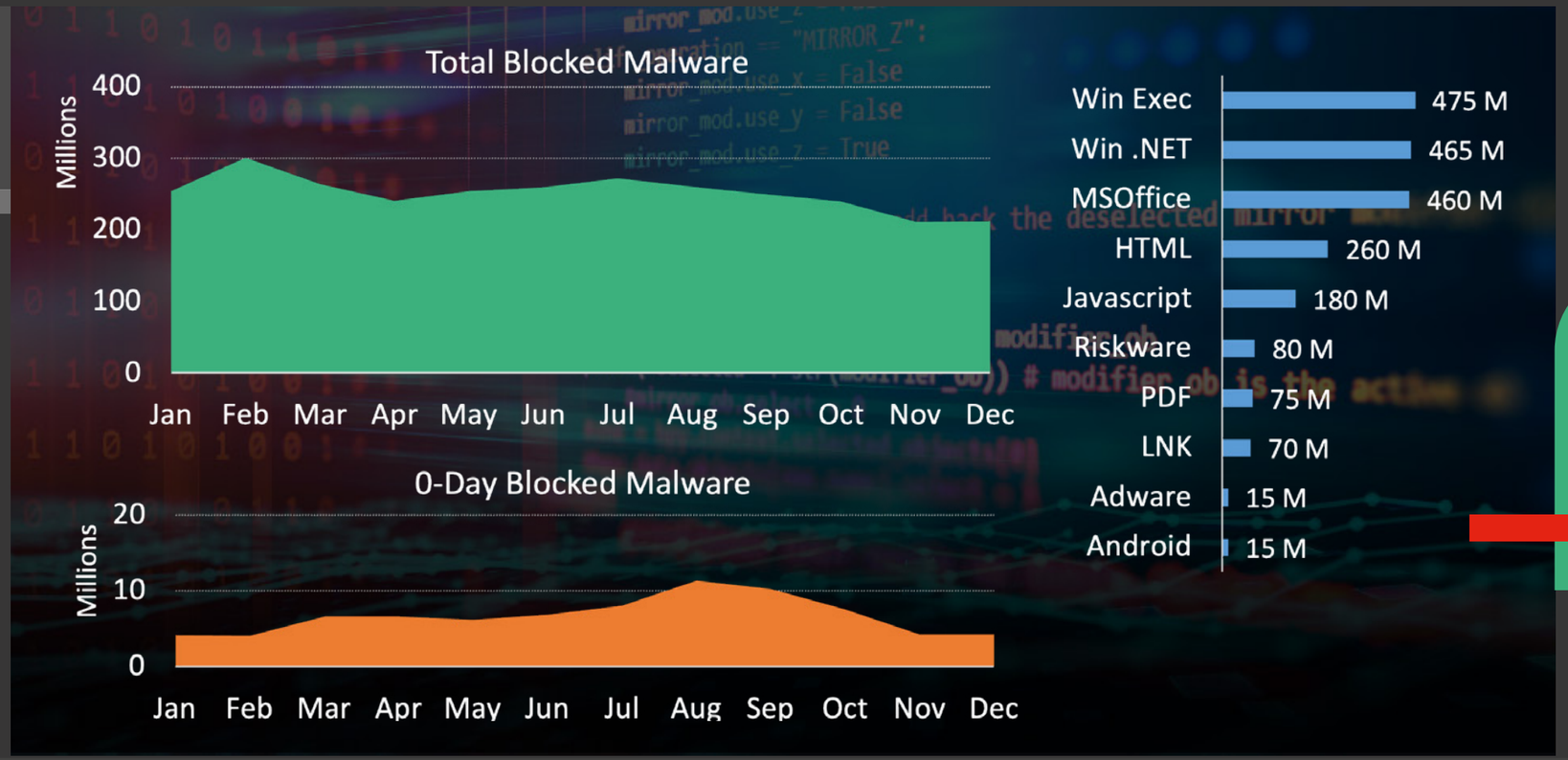


Figure 7: Monthly blocked count of Total Malware and 0-Day Detection. Total per file type.

Significant Active Malware

Ash Trojan

The Ash trojan is an installer script-based malware that incorporates numerous junk instructions to evade Antivirus programs. It was quite prevalent in European and Asian countries with million block hits per month.

This malware was quite epidemic because it was used alongside the recent Lazarus Remote Access Trojan Attack.

Detection signature for Ash Trojan: W32/Ash!tr

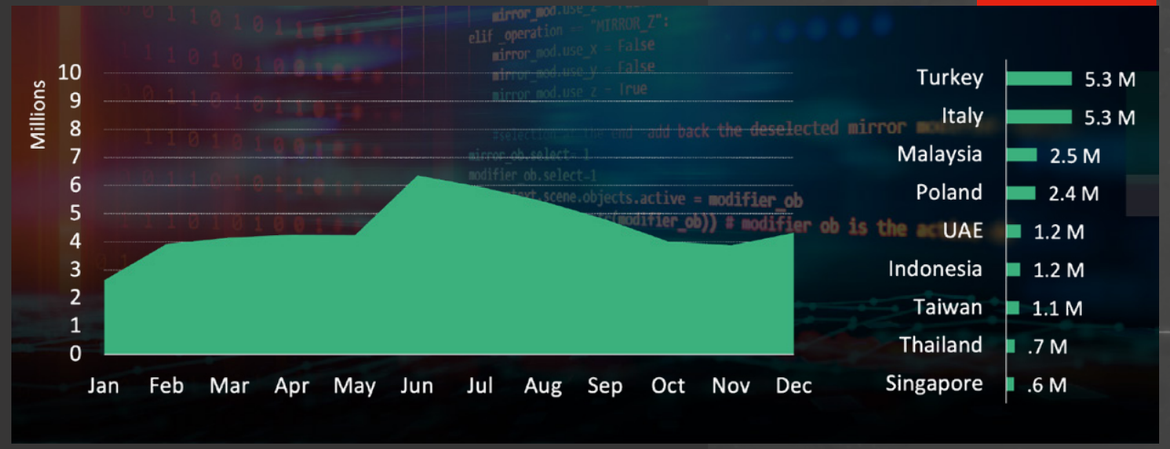


Figure 8: Monthly blocked count and total per country of Ash Trojan.

Stealer 36680 Trojan

The Stealer 36680 trojan is a .NET based Windows executable malware that hides and encrypts its malicious code specifically in the 'Resource' section.

The decrypted code is another Windows executable program that contains the payload. This malware was first discovered in May 2023 and continued to prevail with an average of 4 million blocked hits per month.

Detection signature for Stealer 36680 Trojan: MSIL/Stealer.36680!tr

Figure 9: Monthly blocked count and total per country of Stealer 36680 Trojan.

Significant Active Malware

WannaMine Trojan

The WannaMine trojan has a call home requests to *"doc.conf1g.com."*

That domain name is categorized as the command-and-control (C2) server for WannaMine which is a known malicious mining service. This malware was heavily seen in Tunisia, a country in North Africa, with a total of 11 million block hits.

Detection signature for WannaMine Trojan:
W32/Agent.EFD9!tr

Figure 10: Monthly blocked count and total per country of WannaMine Trojan.

Ransomware Observations and Highlights

Several noteworthy developments and observations regarding ransomware:

Ransomware-as-a-Service (RaaS) Model

The prevalence of the RaaS model persists as a notable trend. This model empowers less technically proficient individuals to execute ransomware attacks by utilizing pre-designed malware provided by more advanced developers, leading to the widespread dissemination of ransomware.

Targeted Attacks

While indiscriminate attacks on individuals and small businesses persist, there is an escalating trend of focused attacks on larger organizations, government entities, and critical infrastructure. Attackers conduct comprehensive reconnaissance before initiating their attacks.

Diverse Tactic

Ransomware operators continue to refine their tactics, utilizing various methods for initial access. These methods encompass phishing emails, exploiting software vulnerabilities, compromising remote desktop protocols, and even employing supply chain attacks or targeting software vendors to broaden their victim pool.

Let's focus on significant widespread ransomware.

Crysis Ransomware

Alias: Dharma
Extension: .mao, .CY3, .d0n
Detection: W32/Crysis.P!tr.ransom

CrySIS, also known as Dharma, is a type of ransomware that first appeared around 2016. Like other ransomware variants, CrySIS encrypts files on a victim's computer or network, rendering them inaccessible.

CrySIS typically spreads through phishing emails, malicious attachments, or compromised websites. Once it infiltrates a system, it begins encrypting files using a strong encryption algorithm, making it challenging to recover the files without the decryption key.

Learn more: Threat Research

Figure 11: Monthly blocked count and total devices per country of CrySIS Ransomware.

Significant Widespread Ransomware

GogaLocker Ransomware

Extension: .locked
Detection: W32/Crypren.AFFL!tr.ransom

Goga Locker is a type of ransomware that has been known to target businesses specifically Industrial OT environments.

One of the world's biggest producers of aluminum was hit by GogaLocker ransomware attack in 2019 that shut down its worldwide network and disrupted its operation.

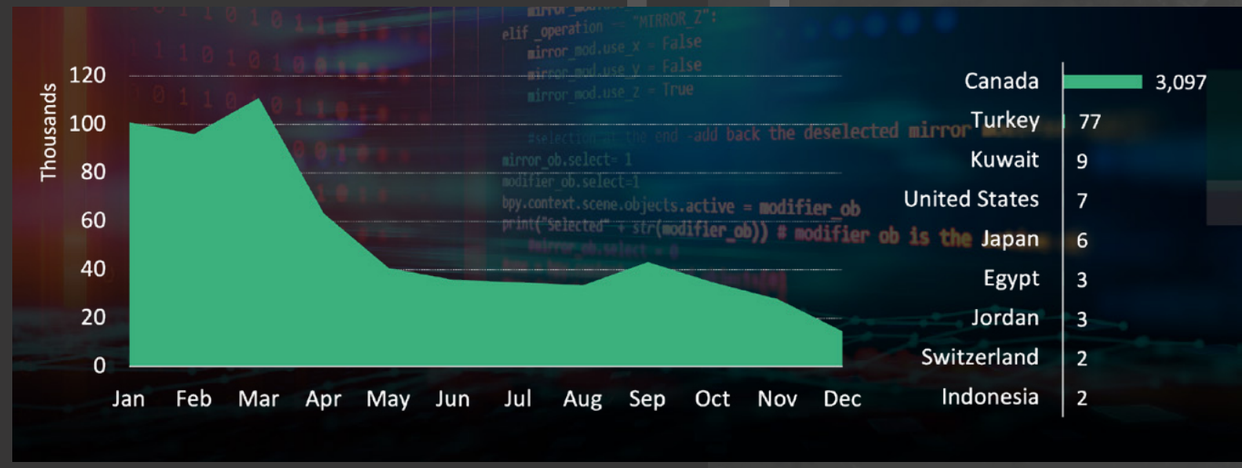


Figure 12: Monthly blocked count and total devices per country of GogaLocker Ransomware

REvil Ransomware

Alias: Sodinokibi Extension: .sodinokibi
Detection: W32/Sodinokibi!tr.ransom

REvil ransomware is infamous for targeting high-profile victims and demanding large ransom payments.

It has been involved in high-stakes attacks against businesses. REVil is often associated with a Ransomware-as-a-Service model. This means that the creators of the ransomware provide it to other criminal actors, who then use it to conduct attacks.

Ransomware attacks, including those involving REVil, have led to significant financial losses, data breaches, and disruptions in various sectors. The targets of REVil attacks have included various organizations and businesses around the world. Ransomware attacks often focus on industries with critical data, such as healthcare, finance, and government.

Figure 13: Monthly blocked count and total devices per country of Revil Ransomware.

OT/ICS Profile Summary

Operational Technology (OT) and Industrial Control Systems (ICS) face unique and critical cybersecurity threats that can have severe consequences on physical infrastructure and industrial processes.

Here is a summary of some key aspects of OT/ICS cyber threats...

Targeted Attacks on Critical Infrastructure

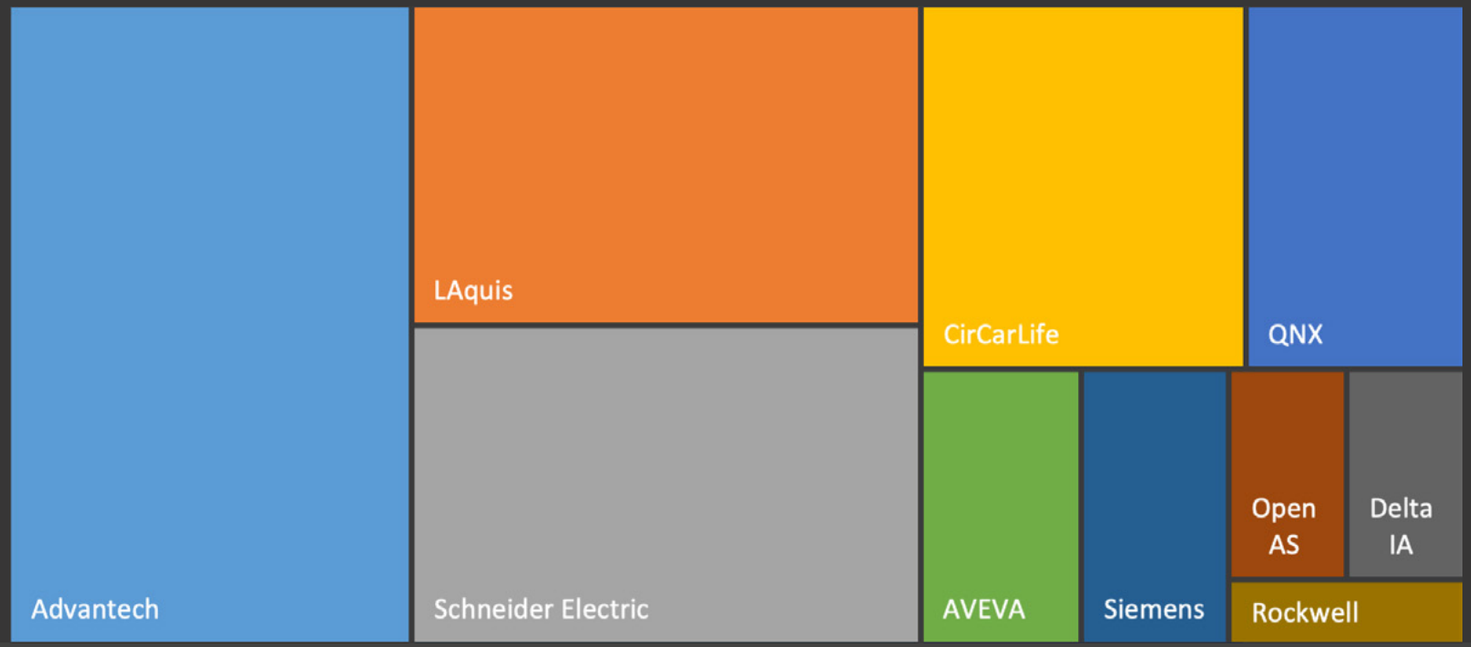
Adversaries increasingly target critical infrastructure, such as energy, water, transportation, and manufacturing sectors, aiming to disrupt operations, cause physical damage, or compromise safety systems.

Specifically Crafted Malware

Cyber threats to OT/ICS often involve specially crafted malware designed to manipulate or disrupt industrial processes. Examples include Stuxnet, Triton, and Industroyer, which target control systems and programmable logic controllers (PLCs).

Convergence of IT and OT Networks

The convergence of Information Technology (IT) and OT networks increases the attack surface. Threats that begin in IT environments may move laterally into OT networks, potentially impacting critical infrastructure.



Exploitation attempts on Advantech, LAquis and Schneider Electric comprised 60% of the top 10 OT vulnerabilities.

Figure 14: Top 10 OT vendor with unique exploit attempts per device and month.

Let's focus on some significant targeted OT/ICS vulnerabilities and threats

CosmicEnergy Malware

OT Malware designed to cause electric power disruption

The CosmicEnergy malware was observed targeting the operational technology sector.

According to the reports, the malware is specifically designed to cause electric power disruption through exploiting IEC 60870-5-104 protocol. That protocol is commonly used in electric transmission and distribution operations in Europe, the Middle East, and Asia.

Based on FortiGuard Labs, detection hits were seen in the following countries: Bulgaria, Canada, Israel, and United Kingdom. The identification of this malware exemplifies that the threat actors are actively engaged to disrupt critical infrastructure and using new design flaws to create new malware which share technical similarities with other OT malware families.

Detection Signature: OT Security Service

Ignition Authentication Bypass

CVE-2022-35871

Ignition is a software platform provided by Inductive that utilizes HMI (Human Machine Interface), SCADA (Supervisory Control and Data Acquisition), and MES (Manufacturing Execution System) functionalities.

The platform provides real-time status and control screens for monitoring and managing machines. A security vulnerability has been identified, allowing remote unauthenticated attackers to execute arbitrary code.

Based on FortiGuard Labs, detection hits were seen in the following countries: Belgium, Brazil, Canada, Spain and United States.

Detection Signature: OT Security Service

Milesight Routers Information Disclosure

CVE-2023-43261

Milesight specializes in providing intelligent IoT and video surveillance products, with a primary emphasis on IoT technologies and industrial solutions.

The Milesight router information disclosure vulnerability exposes sensitive information and enables unauthorized access to the device. This vulnerability is attributed to a misconfiguration that activates directory listing on the router systems, making log files openly accessible to the public.

Detection Signature: OT Security Service

MITRE ATT&CK TTPs Profile

Analyzing the Techniques, Tactics and Procedures (TTPs) employed by threat adversaries to conduct vulnerability and malware attacks can provide insight into the predominant ways cyber actors achieve their objectives.

This Matrix here focuses on the primary MITRE ATT&CK techniques and tactics observed in the FortiGuard Labs Outbreak Alerts in 2023.

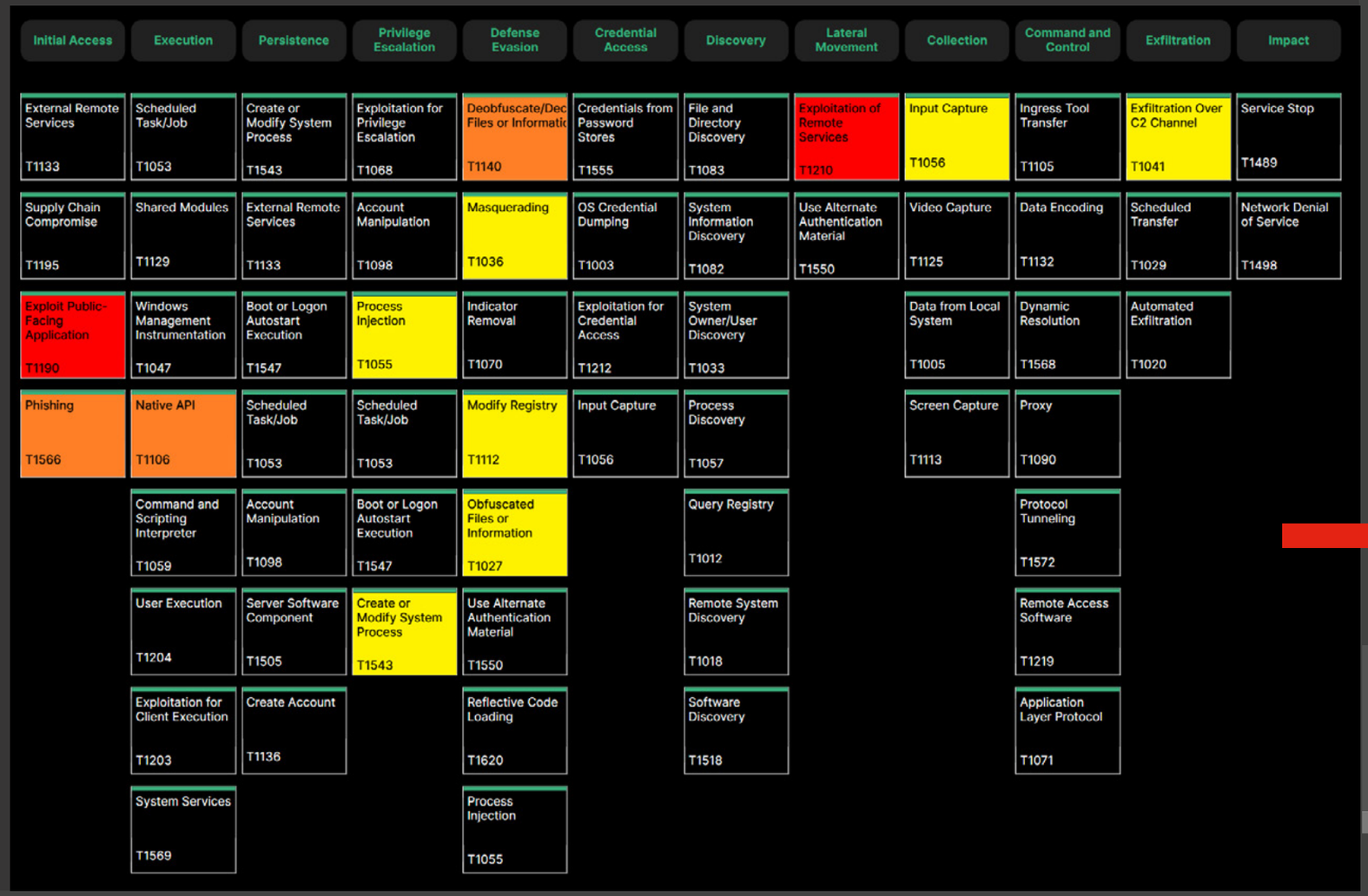


Figure 15: Primary MITRE ATT&CK techniques and tactics observed

Let's focus on the notable TTPs

Exploit Public-Facing Application (T1190)
Tactic: Initial Access

T1190 is the most frequently observed technique by the Outbreaks in 2023.

Attackers try to take advantage of weaknesses in applications accessible to the public, aiming to gain unauthorized access to systems or manipulate the behavior of the applications. Adversaries could exploit established vulnerabilities within these applications, utilize custom exploits, or employ social engineering techniques to compromise their security.

For more info: Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®

Exploitation of Remote Services (T1210)
Tactic: Lateral Movement

Technique **T1210** is highly prevalent, highlighting the importance of securing remote service protocols against unauthorized access and exploitation.

Remote services such as web servers, databases, and other networked services are common targets for exploitation. Adversaries leverage known vulnerabilities or use custom exploits to compromise these services.

For more info: Exploitation of Remote Services, Technique T1210 - Enterprise | MITRE ATT&CK®

Phishing (T1566)
Tactic: Initial Access

Adversaries use phishing to deceive individuals into providing sensitive information or executing malicious actions.

Phishing attacks commonly involve emails, but they can also use other communication channels such as instant messaging, social media, or even phone calls. Ransomware gangs often use phishing as a primary method to deliver their malicious payloads. **LockBit** is a ransomware strain that has been observed using phishing emails for initial access. **Sodinokibi**, also known as **REvil**, has been associated with phishing campaigns that leverage malicious attachments or links.

For more info: Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®

Other notable TTPs include:

Native API (T1106)
Process Injection (T1055)
Masquerading (T1036
Create or Modify System Process (T1543)
Modify Registry (T1112)
Process Injection (T1055)

Deobfuscate/Decode Files or Information (T1140)
Tactic: Defense Evasion

"Deobfuscate" or "decode" refers to the process of reversing the obfuscation or encoding applied to files or information.

Obfuscation and encoding techniques are often used by attackers to hide the true nature of malicious code, making it more challenging for security tools to detect and analyze. The Agent Tesla Malware uses an deobfuscation technique with the Rijndael symmetric encryption algorithm.

For more info: Deobfuscate/Decode Files or Information, Technique T1140 - Enterprise | MITRE ATT&CK®

The insights drawn from the data underscore the complexity and diversity of cyber threats and their applied techniques and tactics.

Challenges to the Cyber Landscape in 2024

The cybersecurity landscape is ever changing, marked by the continual emergence of new threats. Being aware of the primary challenges enables organizations to remain vigilant against evolving risks and adjust their cybersecurity strategy accordingly.

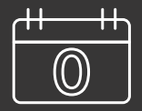
Understanding these key challenges is vital for efficient risk management, safeguarding sensitive data, ensuring uninterrupted business operations, fostering trust, and staying proactive against emerging threats.

Let's discuss what are some of the key challenges...

Some key challenges include:

Increased sophistication of attacks

Cyber attackers are becoming more sophisticated, using advanced tactics such as artificial intelligence (AI) and machine learning (ML) to enhance the effectiveness of their campaigns.



Zero-day exploits

The discovery and exploitation of previously unknown vulnerabilities, known as zero-day exploits, remain a persistent challenge, as they provide attackers with the opportunity to bypass existing security measures.

Ransomware proliferation

Ransomware attacks continue to surge, with threat actors employing advanced techniques like double extortion, targeting critical infrastructure, and demanding larger ransom payments. Some ransomware attacks involve a more hands-on, human-operated approach, allowing attackers to tailor their strategies, evade detection, and increase the effectiveness of their campaigns.

Nation-state threats

State-sponsored cyber threats pose significant challenges, with nation-states engaging in cyber-espionage, cyber warfare, and attempts to disrupt critical infrastructure.

IoT vulnerabilities

The proliferation of Internet of Things (IoT) devices introduces new security challenges, as many of these devices may have inadequate security features, making them potential targets for exploitation.

About FortiGuard Labs Outbreak Alerts

FortiGuard Labs Outbreak Alerts provide a unique analysis of the threat landscape throughout the tech ecosystem. FortiGuard Services provides solutions to cover the complete attack surface, identify outbreaks and aid SOC teams in mitigating impacts and investigating suspected compromises.

Given the volume of active threats, evolving methods for exploiting systems and increasing damage to critical business operations, today's SOC teams require automation and dynamic services to succeed.

FortiGuard Labs Outbreak Alerts provide a unique analysis of the threat landscape throughout the tech ecosystem. FortiGuard Services provide solutions to cover the complete attack surfaces, identify outbreaks and aid SOC teams to mitigate impacts and investigate suspected compromises.

Learn more about:

FortiGuard Outbreak Alerts

FortiGuard Threat Signal

Fortinet Threat Blog

Source: *The data presented in this report is based on FortiGuard Outbreak Alerts and Telemetries. These telemetries are based on the detection logs of FortiGuard Intrusion Prevention (IPS), Antivirus (AV), and Sandbox services used by Fortinet products. The IPS telemetry is mainly based on widespread activity on unique network devices instead of actual block hits to exclude multiple attempts, while, the AV and Sandbox telemetries are based on actual blocking of the known and 0-day Malware, respectively. The report is supplemented by the FortiRecon Threat Intelligence service for the threat actors, availability of PoC, and Darknet activities.*