



THREAT INSIGHTS 2023

TRENDS, VULNERABILITIES,
AND IMPACTS

VOLUME I

TABLE OF CONTENTS.

Executive Summary	3
Ransomware Trends	4
Ransomware Access Techniques	5
Ransomware Groups	6
Initial Access Trends	9
Global Impacts	10
Vulnerability Summary	11
Recommendations	14
About Adlumin	18

AUTHORS

ADLUMIN'S THREAT RESEARCH TEAM

Adlumin's Threat Research Team is the innovator behind Adlumin's comprehensive threat hunting to improve visibility, reduce complexity, and manage risk. The Team proactively searches for cyber threats lurking undetected in your network environment. They dig deep to identify non-remediated threats and other malicious activities to reinforce your security defenses.

EXECUTIVE SUMMARY

This report provides an overview of the current threat landscape, with a focus on trends in ransomware attacks, global impacts, and a summary of the most pressing vulnerabilities discovered in the first quarter of 2023. Below is a list of main findings.



The first quarter of 2023 saw a **5.5 percent quarter-over-quarter increase** in reported vulnerabilities, with 7,772 CVEs reported to the National Vulnerability Database.



Attackers have been increasingly **targeting professional services, manufacturing, construction, and technology sectors**, and ransomware gangs such as Lockbit, BlackCat/ALPHV, and Medusa have been particularly active.



Double extortion remains a successful scheme, with the initial access broker industry (IABs) and their changes in tactics continuing to evolve. Attackers have employed malicious OneNote documents, fake PDF shortcut files, and wscript execution to access victim networks.



The Russia-Ukraine **War is still a key driver in the global cyber landscape**, with Russian cyberattacks still hitting Ukraine. Russian tactics include the use of bots and state-run media to spread misinformation. In early March, the United States and Ukraine signed a Memorandum of Cooperation to strengthen collaboration on shared cybersecurity priorities.



High-profile and potentially critical or severe vulnerabilities during the first quarter of 2023 included those that **had an exceptional number of affected systems**, offered critical access, had no immediate patch, and/or had been seen in-the-wild (ITW) and were being actively exploited by attackers.



Microsoft Windows focused vulnerabilities included a browser sandbox escape vulnerability, a privilege escalation vulnerability in Outlook, a privilege escalation vulnerability in the Windows Common Log File System driver, a remote code execution vulnerability in the Windows Graphics Component, and a Publisher Security Features bypass vulnerability.



Other software platforms and **systems impacted by attacks or exploits** included Adobe ColdFusion, macOS, SugarCRM, GoAnywhere MFT, and the Linux kernel.

RANSOMWARE TRENDS



The first quarter of 2023 saw **ransomware as one of the top active threats** to organizations.



Almost **900 ransomware attacks were reported** from January to March, with notable victims like the City of Oakland, DISH Network Corporation, The Royal Mail, and Five Guys.



Double extortion is a growing threat within ransomware schemes. This occurs when threat actors **holding your data for ransom also threaten to release the data** to the public if their demands are not met.

The success attackers are having with double extortion is validated by the ever-growing initial access broker industry and their notable changes in tactics, which have moved to include increased reconnaissance of the target's environment.



Five Guys was able to recover from the attack easily. However, DISH Network has experienced a **slow drop in the share price of its stock** due to waning investor confidence as DISH and SlingTV customers were unable to access customer service and billing functions for multiple days.



Even a month after the DISH Network attack, customer service **response times were reported to take up to 14 hours¹**.



A January 2023 Lockbit attack against the publicly traded British postal and courier service, Royal Mail, **caused stoppages in international shipping**. It took the company about six weeks to restore the exportation of international shipments



As late as early April, the City of Oakland is still recovering from a February attack where services were shut down, **forcing government buildings to close**, and employee personal information to be leaked online.

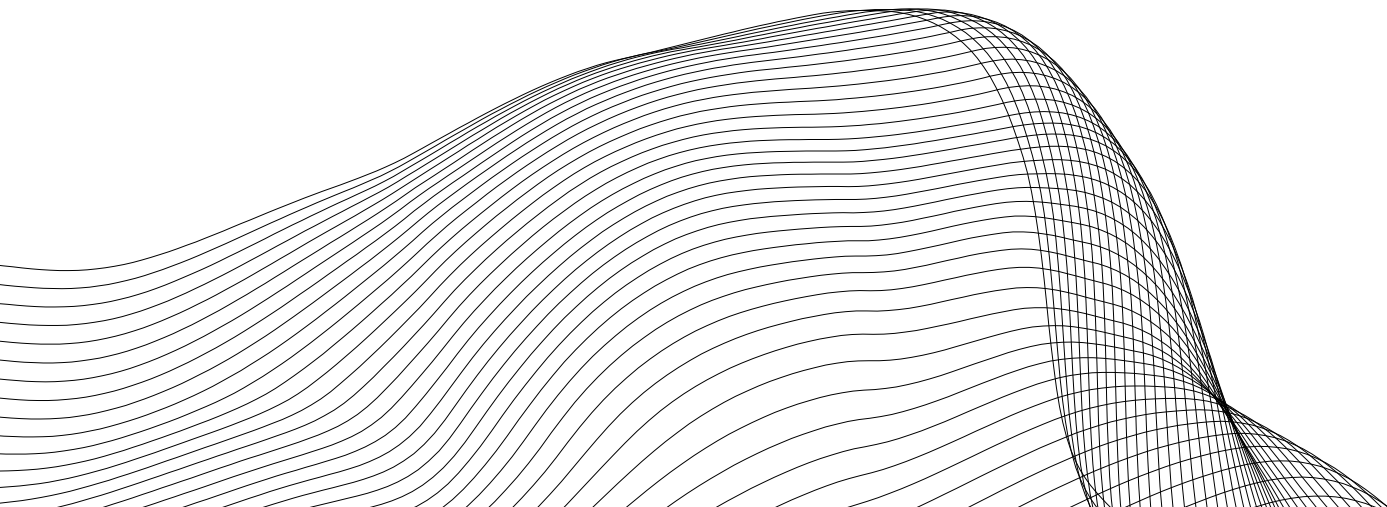


RANSOMWARE ACCESS TECHNIQUES

We are continuing to see the ramifications of Microsoft Office blocking macros by default, as threat actors continue to produce new techniques to gain execution against business targets. Retirement of this often-exploited pathway has led to attackers shifting to new methods of email attachment-based access techniques which require development of new mitigation, detections, and patches.

The techniques that we've seen develop this past quarter include malicious notebook documents, a return to fake PDF .exe documents and .lnk files, and continued evolution of wscript execution techniques on Windows systems.

Of the many threat actor groups that were active this past quarter, we have chosen three to highlight due to their activity in sectors most relevant to our clients.



RANSOMWARE GROUPS

LOCKBIT

Lockbit was the most prolific ransomware gang of the past quarter, with over 200 extortion victims reported². Lockbit is technically Ransomware-as-a-Service, where multiple “affiliates” gain access to victims and install Lockbit ransomware which then spreads across the shared infrastructure³.

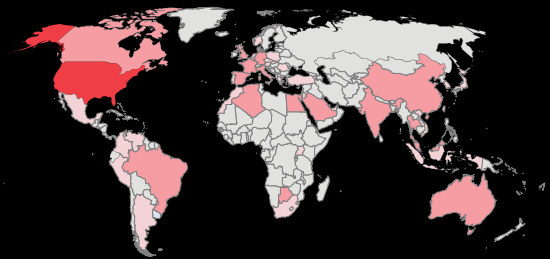
This past quarter, Lockbit heavily targeted organizations in professional services, including manufacturing, construction, and technology, but its focus on these industries was not exclusive.

Most of Lockbit’s victims were small to medium in terms of company size and notoriety, most likely due to ease of access. They did, however, also manage to infect computers at the Royal Mail and the City of Juarez government networks, in Mexico.

The overwhelming majority of Lockbit victims were in the United States, but the gang behind it targeted victims across all of North and South America. There is no discernable pattern to the regional targeting besides hitting primarily wealthy nations.



Q1 2023 LOCKBIT VICTIMS*



Q1 2023 LOCKBIT VICTIMS BY SECTOR



BLACKCAT/ALPHV

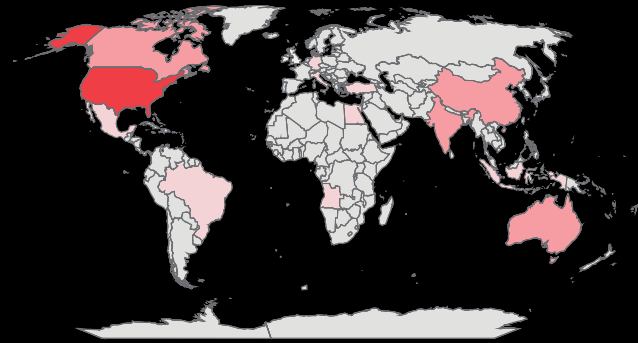
Another group that has been active this quarter, with high-profile victims in the U.S., is BlackCat, or ALPHV.

BlackCat had around 80 published victims this past quarter, with some high-profile victims in the healthcare and education sectors. Included in the list are Five Guys, Lehigh Valley Health Network, and Ring.

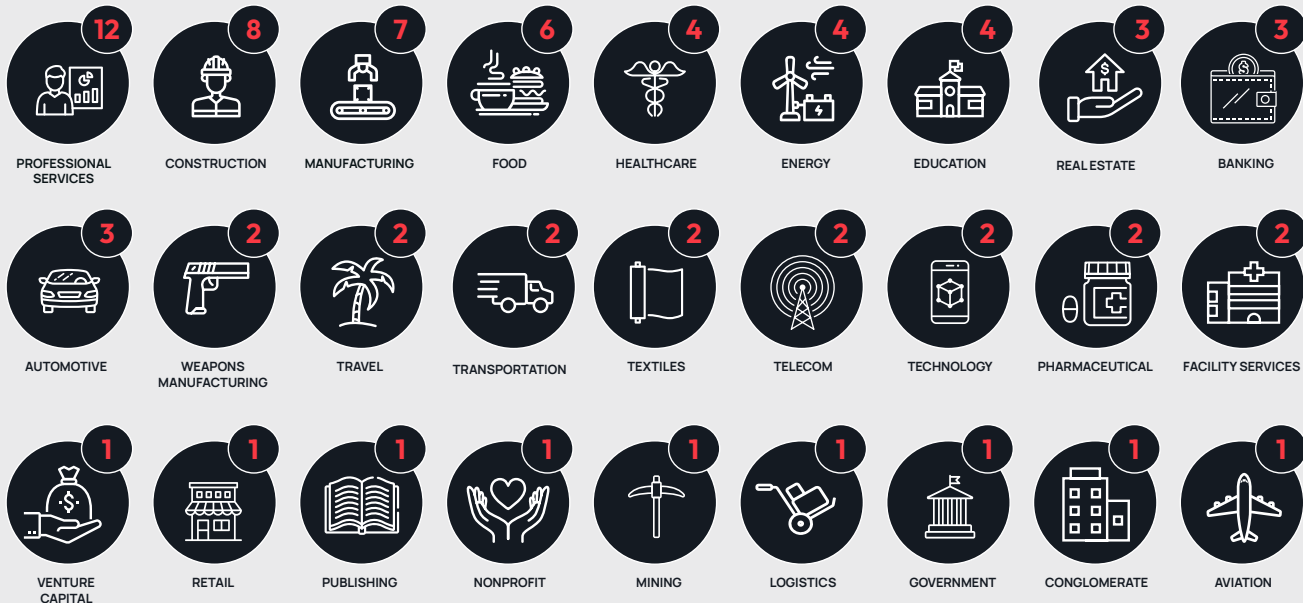
BlackCat's targets are distributed like Lockbit's in terms of both region and sector and they are both categorized as Ransomware-as-a-Service providers. It is likely that initial access methods are similar, and the sectors being targeted are highly susceptible to those methods. Again, wealthier countries are the most targeted by BlackCat.



Q1 2023 BLACKCAT/ALPHV VICTIMS**



Q1 2023 BLACKCAT/ALPHV VICTIMS BY SECTOR:



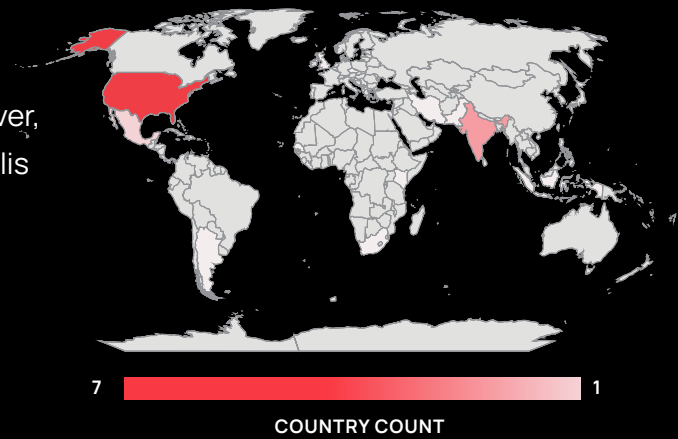
MEDUSA

Medusa is a newer ransomware gang that seems to have made a big splash this quarter. The name is unfortunately generic in this space, not to be confused with other attack groups from the past few years such as MedusaLocker, the Distributed Denial of Service (DDoS) botnet, or the Medusa password cracker tool.

Medusa had fewer victims this quarter than the other two actors we highlighted on this list, so we cannot necessarily derive any targeting trends from their data. They had, however, a high-profile victim in the education sector – the Minneapolis Public Schools District.



Q1 2023 MEDUSA VICTIMS



Q1 2023 MEDUSA VICTIMS BY SECTOR:



INITIAL ACCESS TRENDS

Malicious OneNote Documents

Attackers pivoted to embedding malicious attachments in OneNote files. OneNote is Microsoft’s note-taking app. The attackers send infected files in untargeted mass spam campaigns as well as in targeted emails and attempt to trick victims into clicking a button inside the OneNote file. When clicked, the file executes the malicious attachment embedded therein.

In order to mitigate this problem, Microsoft will be blocking embedded attachments in OneNote files by default, starting sometime in Q2 2023. You can get a head start on blocking OneNote embedded attachments with group policy settings to restrict the launching of accepted embedded attachment file types⁴.

Fake PDF Shortcut Files

Many attackers have gone back to the tactic of faking file extensions by using two of them. This is a very classic technique, but the old “document.pdf.exe” trick does not work all that well with SmartScreen (the reminder window that appears when you run a new .exe in Windows).

Now, attackers are using .lnk shortcut files instead. These shortcut files are usually contained in a .zip file that the victim is manipulated to download and open. They then execute a command, typically running a Windows script that is contained in the .zip file.

Wscript Execution

Fake PDF shortcut files lead to executing wscript—the Windows script host. Wscript is a Windows command that executes a script in a scripting language more complex than batch script – typically a variant of JavaScript (VBScript or JScript). The script will download and execute the malware.

These techniques are all used by ransomware actors to gain initial access to the victim’s network. The .lnk file to wscript execution has become the typical access vector for Qakbot, Emotet, and IcedID— three common banking trojans that end up being used as the initial stage of a ransomware intrusion.



GLOBAL IMPACTS

War in Ukraine: How the World's First Hybrid War Has Shaped the Global Cyber Landscape

The Russia-Ukraine War has garnered global attention. While it is not the first “cyber war,” it is one of the first truly “hybrid” wars, with boots on the ground and on keyboards in the cloud.

The Birth of Hybrid Warfare

Russian cyberattacks hit Ukraine well before any shots were fired, ramping up activity shortly before the invasion. In fact, the Center for Security and International Studies has suggested that Russian cyber actions forewarned Ukraine of the conflict as early as 2014.⁵

In the initial weeks of the conflict, numerous phishing attempts were made, eight different families of malware were deployed⁶, and brute force attacks targeted Ukrainian government websites, utility providers, and financial institutions to disrupt services, and undermine the Ukrainian government.

As the war gained global visibility and Ukraine gained more international support, the Russian cyber campaign extended to North Atlantic Treaty Organization (NATO) members and allies as they rushed to claim the upper hand in both the physical invasion and the global narrative.

Many cyber security experts believed the war would result in an escalation of global cyberattacks

targeting critical infrastructure beyond the borders of Ukraine and an increase in attacks on the United States and other allies. However, recent statistics show that the war has had the opposite affect – attacks on businesses within countries outside of Ukraine has slowed to a crawl.

Don't Mis(information) Dis(information)

Russian tactics have also included those that were more discrete and less newsworthy to help generate support for the war domestically and fracture international support for Ukraine.

Russia has relied heavily on bots and state-run media (often referred to as “trolls”) to spread misinformation. Russia's hacking tools remain important pieces in the spread of disinformation and pervasive state-sponsored propaganda.

International Relations

Prior to the February 2022 military invasion, the Civilian Research and Development Foundation (CRDF) Global, an independent nonprofit established by the National Science Foundation to promote safety, security, and sustainability, had been working with leading cybersecurity experts to create Ukraine's first national Cybersecurity Strategy.

As the conflict gained speed, CRDF created the Cyber Defense Assistance Collaborative (CDAC) for Ukraine, bringing in operational cyber defense

assistance from private companies to help meet an urgent and immediate need to defend critical Ukrainian infrastructure.

In July of 2022, the United States Cybersecurity and Infrastructure Agency (CISA) and the Ukrainian State Service of Special Communications and

Information Protection of Ukraine (SSSCIP), signed a Memorandum of Cooperation to strengthen collaboration on shared cybersecurity priorities, including information exchanges and sharing of best practices on cyber incidents; technical exchanges on critical infrastructure security, and joint exercises and trainings on cybersecurity.

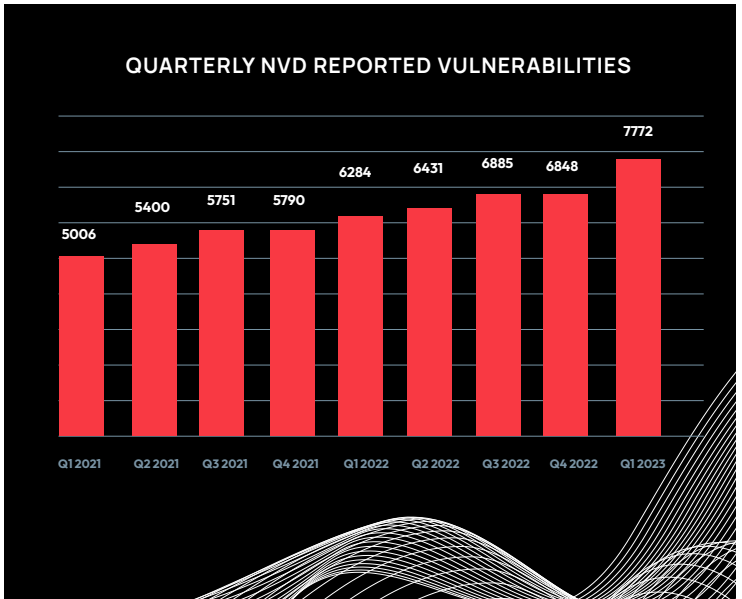
VULNERABILITY SUMMARY Q1 2023

During the first quarter of 2023, there were 7,772 CVEs Common Vulnerabilities and Exposures (CVEs) added to the official NIST (National Institute of Standards and Technology) NVD (National Vulnerability Database).⁷

The number of CVEs is in line with previous quarters and continues a quarter over quarter increase in vulnerabilities reported by 5.5 percent.

During Q1, there were high-profile and potentially critical or otherwise severe vulnerabilities. The below trending vulnerabilities for Q1 2023 include those that had an exceptional number of affected systems, offered critical access, had no immediate patch, and/or had been seen in-the-wild (ITW) and being actively exploited by attackers.

Additionally, Adlumin pays close attention to Department of Homeland Security (DHS)/(CISA) Known Exploited Vulnerabilities.



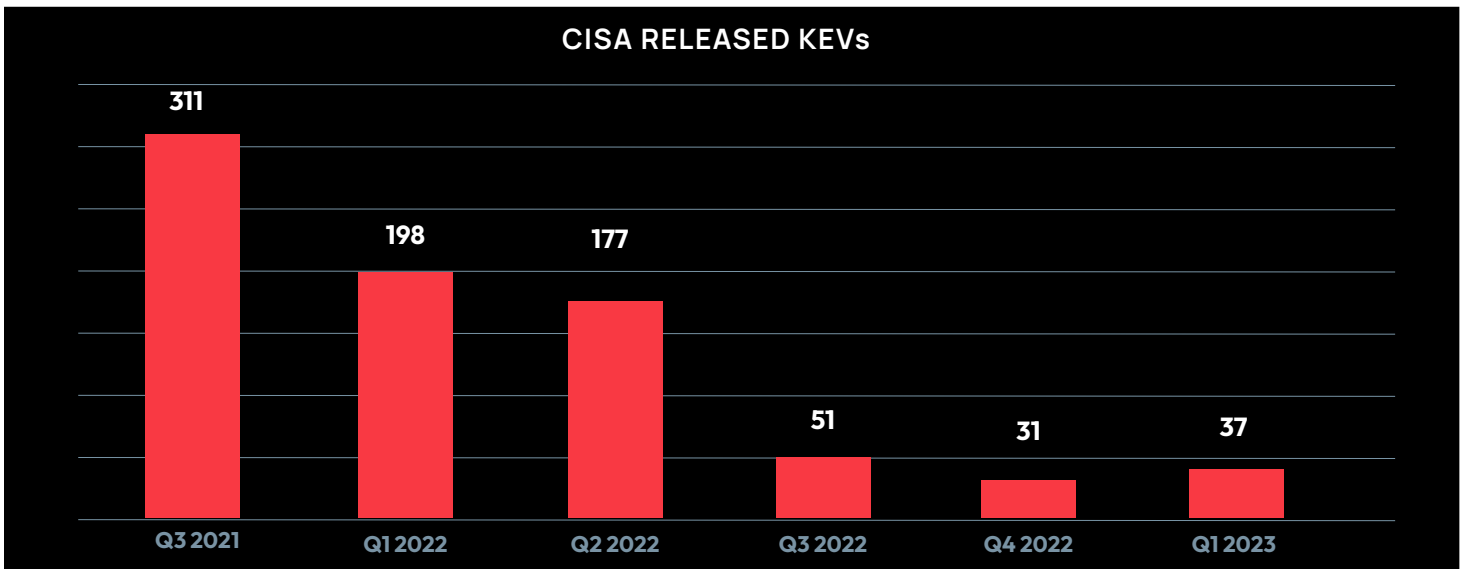
The data is not normalized based on the number of non-published submissions or the number of reporting entities but does show a clear, continuing trend of increasing discovered vulnerabilities available for use in an attacker's potential arsenal.

During Q1, there were high-profile and potentially critical or otherwise severe vulnerabilities. The below trending vulnerabilities for Q1 2023 include those that had an exceptional number of affected systems, offered critical access, had no immediate patch, and/or had been seen in-the-wild (ITW) and being actively exploited by attackers.

Additionally, Adlumin pays close attention to DHS / CISA Known Exploited Vulnerabilities (KEV). KEVs are typically those vulnerabilities which CISA has identified as being exploited in-the-wild.

CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.⁸

Q1 2023 saw a total of 37 additional KEVs: five in January, 13 in February, and 18 in March. This is in line with the addition of 51 and 31 KEVs in Q3 and Q4 of 2022 – a significant step down from the initial flood of KEVs since the program started November 2021.^{9,10}



Microsoft Windows Focused Vulnerabilities

CVE-2023-21549 (CVSS 8.8)

On 10 January 2023, Microsoft released a patch for a browser sandbox escape vulnerability in Windows. This vulnerability could allow an attacker to execute malicious code outside of the safe sandbox created by the browser¹¹

CVE-2023-23397 (CVSS 9.8)

A privilege escalation vulnerability in Outlook allows an attacker to perform an NTLM Relay attack. This attack works by sending a calendar invite to the targeted user. When the reminder for a calendar item appears, NTLM negotiation will begin with the attacker's host server, allowing the attacker to receive NTLM credentials. As this attack does not require any actions from the user,

this should be patched as soon as possible. A fix for this issue was implemented on 14 February 2022.

CVE-2023-28252 (CVSS 7.8)

A privilege escalation vulnerability was discovered by Microsoft in the Windows Common Log FileSystem driver which would allow an attacker to gain SYSTEM privileges on an affected machine. No further data has been released by Microsoft as to the methods. This issue was patched in the Windows update released the February 14, 2023.¹²

CVE-2023-21823 (CVSS 7.8)

A Remote Code Execution vulnerability in Windows Graphics Component was patched by Microsoft on February 14 of this year. This vulnerability could allow an attacker to execute arbitrary code on the system.³

CVE-2023-21715 (CVSS 5.0)

A Publisher Security Features bypass vulnerability was patched by Microsoft on the 14 of February of this year. This attack would allow an authenticated attacker to bypass Office macro policies, allowing further exploitation.¹⁴

Other Platforms, Software, Products

CVE-2023-26360 (CVSS 9.8)

Adobe ColdFusion version 2018 and 2021 allow Remote Code Execution. Adobe has stated that this attack has been seen in the wild. Updating to version 2018 Update 16, or version 2021 Update 6, will prevent this issue.¹⁵

CVE-2023-23514 (CVSS 7.8)

A use-after-free vulnerability was discovered in macOS, which could allow an attacker to execute arbitrary code. This has been fixed by Apple.¹⁶

CVE-2023-22952 (CVSS 8.8)

A PHP code-injection vulnerability was found and patched in SugarCRM, a popular customer relationship management system¹⁷. This vulnerability would allow a remote attacker to execute arbitrary code on the system. A Metasploit module has been created for this use-case.¹⁸

CVE-2023-0669 (CVSS 7.2)

A pre-authentication command injection vulnerability was discovered in GoAnywhere MFT (Managed File Transfer), a secure file transfer system produced by Fortra.¹⁹ An exploit for this vulnerability has been released publicly, as well as a module for Metasploit.^{20,21} This vulnerability has been seen being abused in-the-wild, as threat actors have used it to steal files from users, with the Clop ransomware group claiming to be responsible^{22,23}

CVE-2023-0266 (CVSS 7.8)

A use-after-free vulnerability was found in the Linux kernel which would allow an attacker to gain administrative privileges on the machine, which was addressed in more recent code commits.²⁴ This attack has been recorded by Google to be part of an attack-chain used to drop spyware onto Samsung cellphones.²⁵

RECOMMENDATIONS



Follow [CISA's Stop Ransomware Guidelines](#), newsroom, and alerts.



Financial institutions should [implement a comprehensive phishing awareness training](#) program for employees, customers, and third-party vendors.



[Multi-factor authentication should be implemented](#) where possible to prevent unauthorized access if credentials are stolen.



Email filtering technologies should be used to [detect and block malicious emails](#), and Domain-based Message Authentication, Reporting & Conformance (DMARC) should be implemented to prevent email spoofing.



[Incident response plans](#) should be in place to detect, respond to, and remediate phishing attacks quickly and effectively.



[Third-party risk management programs should be implemented](#) to assess and monitor the security of vendors and suppliers, and to ensure they are adhering to the same security standards as the financial institution.



ADLUMIN THREAT RESEARCH IN THE NEWS


Adlumin's Threat Research team has discovered a new malicious PowerShell script called "PowerDrop" that has set its sights on the U.S. aerospace industry. This novel malware combines elements of off-the-shelf threats and tactics used by Advanced Persistent Threat Groups (APTs) and uses advanced techniques to evade detection such as deception, encoding, and encryption.

Read more: [Bleeping Computer Article](#)

[Dark Reading Article](#)

REFERENCES

1. <https://www.nbcnews.com/news/us-news/frustrated-dish-customers-still-spending-hours-hold-weeks-ransomware-a-rcna76181>
2. <https://www.ransomlook.io/groups#Lockbit>
3. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a>
4. <https://www.bleepingcomputer.com/news/security/how-to-prevent-microsoft-onenote-files-from-infecting-windows-with-malware/>
5. <https://www.csis.org/analysis/cyber-war-and-ukraine>
6. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>
7. https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&isCpeNameSearch=false&pub_start_date=01%2F01%2F2023&pub_end_date=03%2F31%2F2023
8. Reducing the Significant Risk of Known Exploited Vulnerabilities | CISA
9. 9 missing ?
10. https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
11. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21674>
12. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376>
13. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21823>
14. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715>
15. <https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html>
16. <https://support.apple.com/en-us/HT213633>
17. <https://nvd.nist.gov/vuln/detail/CVE-2023-22952>
18. <https://packetstormsecurity.com/files/171320/SugarCRM-12.x-Remote-Code-Execution-Shell-Upload.html>
19. <https://nvd.nist.gov/vuln/detail/CVE-2023-0669>
20. <https://frycos.github.io/vulns4free/2023/02/06/goanywhere-forgotten.html>
21. <https://packetstormsecurity.com/files/170940/Fortra-GoAnywhere-MFT-Unsafe-Deserialization-Remote-Code-Execution.html>
22. 22 missing?
23. <https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/>
24. <https://nvd.nist.gov/vuln/detail/CVE-2023-0266>
25. <https://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/>



ILLUMINATE THREATS AND ELIMINATE RISKS

Learn more about how Adlumin's Managed Detection and Response Services and Security Operations Platform can empower your team to illuminate threats, eliminate cyber risk, and command authority; contact us today or schedule a demo at www.adlumin.com.



About Adlumin

Adlumin Inc. provides the enterprise-grade security operations platform and managed detection and response (MDR) services that keep mid-market organizations secure. With one license and one platform, its patented technology gives organizations and solution providers everything they need for effective threat hunting, incident response, vulnerability management, darknet exposure monitoring, compliance support and much more.

The Adlumin platform is feature-rich enough for organizations to operate on their own, yet built specifically to amplify the skills and capabilities of managed service providers who use it to deliver cutting-edge security that can scale to meet the needs of any operating environment. With full access to the platform regardless of whether they are running it themselves or relying on Adlumin's MDR services or expert partners, Adlumin gives organizations unparalleled visibility into their security posture through access to alerts, investigation data, threat intelligence, compliance reporting and everything else – all in real time.