Cyber Threat Advisory

JANUARY 2024

Image Source

Contents

Monthly Highlights - January

1. **Delta Dental of California Data Breach Exposed Info of 7 Million People** – Delta Dental of California and its affiliates are warning almost seven million patients that they have experienced a data breach, as personal data was exposed in a MOVEit Transfer software breach.

   The software was vulnerable to a zero-day SQL injection flaw, leading to remote code execution tracked as CVE-2023-34362. The Clop ransomware gang leveraged this vulnerability to breach thousands of organizations worldwide.

   Delta Dental of California became aware of the compromise on June 1, 2023. After 5 days of internal investigation, they confirmed that unauthorized actors had accessed and stolen data from its systems between May 27 and May 30, 2023.

2. **Google Warns How Hackers Could Abuse Calendar Service as a Covert C2 Channel** – Google has issued a warning about the emergence of a potential threat involving multiple threat actors engaging in a public proof-of-concept (PoC) exploit that manipulates its calendar service for hosting command-and-control (C2) infrastructure. The tool, known as Google Calendar RAT (GCR), utilizes Google Calendar Events for C2 purposes through a Gmail account and was initially shared on GitHub in June 2023.

   In its eighth Risk Horizons Report, Google stated that while there haven't been observed instances of the tool being utilized in real-world scenarios, its Mandiant threat intelligence unit has identified several threat actors engaging in the PoC on underground forums. The Google Calendar RAT, when operational on a compromised machine, periodically monitors the calendar event description for

new commands, executes these commands on the targeted device, and then updates the event description with the output of the executed command.

Google emphasized that the tool's exclusive reliance on legitimate infrastructure poses a significant challenge for defenders in detecting suspicious activities. This development underscores threat actors' persistent interest in exploiting cloud services to seamlessly integrate into victim environments and evade detection.

The report also highlighted the activities of an Iranian nation-state actor employing macro-laden documents to compromise users with a compact .NET backdoor named BANANAMAIL for Windows and utilizing email as a channel for C2. Google's Exploration Team took action by restricting the attacker-controlled Gmail accounts utilized by the malware for communication channels.

3. **Black Basta Ransomware Made Over $100 Million From Extortion** – The Russia-linked ransomware group Black Basta has reportedly amassed over $100 million in ransom payments from more than 90 victims since its emergence in April 2022, according to joint research conducted by Corvus Insurance and Elliptic. The cybercriminal operation employs double extortion attacks, targeting over 329 victims globally. In these attacks, the group's associates illicitly acquire sensitive data from compromised systems and then deploy ransomware payloads across the victims' networks, encrypting the compromised systems.

   To pressure victims into paying ransoms, Black Basta uses the stolen data, threatening to publish it on their dark web leak site. The investigation reveals that Black Basta has secured a minimum of $107 million in ransom payments from over 90 victims since early 2022. The highest recorded ransom payment reached $9 million, with at least 18 payments exceeding the $1 million mark. The average ransom payment, as reported by the Corvus Threat Intel team, stands at $1.2 million.

   According to data derived from Black Basta's leak site through Q3 of 2023, at least 35% of identified victims have made ransom payments. This aligns with findings from ransomware negotiation company Coveware, indicating that despite record-low ransomware payments in 2022, approximately 41% of all ransomware victims have paid a ransom.

   Black Basta initially emerged as a Ransomware-as-a-Service (RaaS) operation in April 2022, focusing on global corporate entities through double-extortion attacks. The group gained prominence following the closure of operations by the Conti ransomware gang in June 2022. The fragmentation of the cybercrime syndicate led to the emergence of Black Basta as one of its factions.

   The Department of Health and Human Services security team, in a March report, highlighted the threat group's prolific targeting of at least 20 victims in its initial two weeks of operation, indicating its expertise in ransomware and a stable source of initial access.

4. **Ten New Android Banking Trojans Targeted 985 Bank Apps in 2023** – This year has witnessed the emergence of ten new families of Android banking malware, collectively targeting 985 apps related to banks, fintech, and trading platforms across 61 countries. Banking trojans are malicious software designed to compromise online bank accounts and funds by stealing credentials and session cookies, circumventing 2FA protections, and occasionally executing transactions automatically.

   In addition to the introduction of these ten new trojans in 2023, 19 malware families from 2022 underwent modifications to incorporate new capabilities, enhancing their operational sophistication. Mobile security firm Zimperium analyzed all 29 (10 + 19) and identified several emerging trends, including:

   - **The incorporation of an automated transfer system (ATS) that captures MFA tokens, initiates transactions, and facilitates fund transfers.**
   - **The utilization of social engineering tactics, such as cybercriminals posing as customer support agents, guiding victims to download trojan payloads themselves.**
   - **The addition of live screen-sharing capability for direct remote interaction with infected devices.**
   - **Offering the malware through a subscription package to other cybercriminals at a cost of $3,000 to $7,000 per month.**

   Common features found in most examined trojans include keylogging, overlaying phishing pages, and stealing SMS messages. A concerning development is that banking trojans are evolving beyond the theft of banking credentials and funds, now extending to the targeting of social media, messaging, and personal data.

   Zimperium analyzed ten new banking trojans, comprising over 2,100 variants circulating in the wild, disguised as utilities, productivity apps, entertainment portals, photography tools, games, and educational aids. These ten new trojans are named as follows:

   1. Nexus: MaaS (malware-as-a-service) with 498 variants offering live screen-sharing, targeting 39 apps in nine countries.
   2. Godfather: MaaS with 1,171 known variants targeting 237 banking apps in 57 countries, supporting remote screen-sharing.
   3. Pixpirate: Trojan with 123 known variants powered by an ATS module, targeting ten bank apps.
   4. Saderat: Trojan with 300 variants targeting eight banking apps in 23 countries.
   5. Hook: MaaS with 14 known variants powered by live screen-sharing, targeting 468 apps in 43 countries, available for rent to cybercriminals at $7,000/month.

6. PixBankBot: Trojan with three known variants targeting four banking apps, equipped with an ATS module for on-device fraud.
7. Xenomorph v3: MaaS operation with six variants capable of ATS operations, targeting 83 bank apps in 14 countries.
8. Vultur: Trojan with nine variants targeting 122 banking apps in 15 countries.
9. BrasDex: Trojan targeting eight bank apps in Brazil.
10. GoatRat: Trojan with 52 known variants empowered by an ATS module, targeting six banking apps.

Among the malware families existing in 2022 and updated for 2023, those displaying significant activity include Teabot, Exobot, Mysterybot, Medusa, Cabossous, Anubis, and Coper.

5. **Vulnerabilities Now Top Initial Access Route for Ransomware** – Threat actors are altering their strategies for deploying ransomware, shifting towards exploiting vulnerabilities rather than relying on phishing emails, as reported by Corvus Insurance. The insurer examined claims data from this year to gain insights into threat actor behavior.

   According to security researchers, vulnerability exploitation as an initial access method surged from nearly 0% of ransomware claims in H2 2022 to almost one-third in the first half of 2023. While this data might be influenced by significant campaigns, such as the extortion attacks exploiting MOVEit and GoAnywhere file transfer software, it underscores an evolution in threat activity.

   Corvus also pointed out that exposed cryptographic keys are becoming an increasingly popular method for threat actors to compromise organizations. The insurer noted that 7% of the studied organizations had at least one exposed secret, with the most common being Google API keys, JSON web tokens, Shopify domain keys, and keys for AWS S3 buckets.

   However, not all exposures carry the same level of risk. Some provide limited information for threat actors, posing minimal concern for the exposed organizations. Yet, for approximately 1% of the studied organizations, Corvus identified exposed keys classified as 'critical' by security experts, necessitating immediate attention. These critical keys included AWS API keys, keys to cloud storage buckets (AWS S3 and Google Cloud Storage), and API keys from various non-cloud provider services such as LinkedIn, Okta, Slack, MailChimp, Facebook, New Relic, Stripe, and Sauce Labs.

   In addition, Corvus highlighted that social engineering has become a prominent cause of insurance claims, comprising nearly half of all claims as of Q3 2023. This represents a notable increase from around 35-38% a year earlier. Social engineering is now responsible for almost three times more claims than the next largest category, which involves breaches at vendors or other third parties.

   Interestingly, there were no reports of social engineering-related breaches among Google Workspace policyholders, while Microsoft accounted for the vast majority. Corvus noted that, despite Microsoft being the most prevalent business email provider used by policyholders, the absence of social engineering claims from Google Workspace organizations was unexpected, considering their prevalence.

6. **WhatsApp, Slack, Teams, and Other Messaging Platforms Face Constant Security Risks** – Messaging platforms like WhatsApp, Telegram, Slack, and Teams face persistent threats, highlighting the crucial need for robust protection. Approximately 66% of threat indicators are identified in transient messages associated with these cloud-based collaboration tools.

   WhatsApp, increasingly adopted for enterprise communication, is not without risks. Among messages flagged for security or compliance concerns, 42% originated from WhatsApp, 24% from Telegram, 17% from Slack, and 17% from Teams.

   Common messaging apps are frequent targets for social engineering attacks, with 42% of flagged messages triggering impersonation warnings. Moreover, employees are sharing files violating regulatory compliance laws, as 23% of flagged messages include attachments considered potentially sensitive and non-compliant.

   The current threat landscape, diverse and multilingual, prompts cybercriminals to target victims across various platforms. For global companies operating in multiple markets and languages, the threat is evident, with 24% of flagged messages on WhatsApp being in a language other than English.

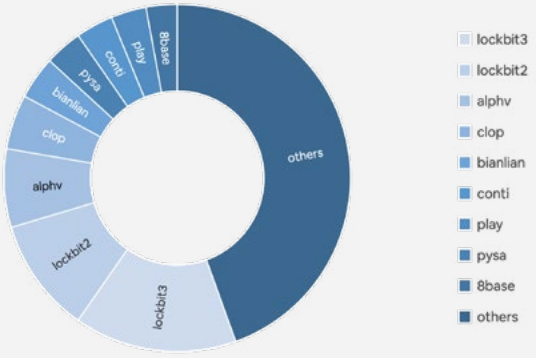
   A noticeable shift away from traditional email for business communication has been observed. Employees, accustomed to using popular messaging apps from their personal lives, bring these practices into business. Despite the productivity benefits, data indicates that the rise of these apps provides new entry points for threat actors.

   However, many enterprises lack effective security measures to monitor these instances. In such an instance, adapting security strategies aligned with human behavioral patterns and emphasizing unified visibility and contextual analysis is very important.

   The surge in cloud-based collaboration tools and the merging of personal and business usage has given rise to a new attack category known as Business Communication Compromise. Threat actors target various collaboration tools to exploit login credentials, financial reports, and proprietary data. To safeguard critical data and operations, organizations must strengthen defense by gaining greater visibility over business communication channels and leveraging machine learning (ML) and artificial intelligence (AI) for a comprehensive understanding of the business communications landscape.

Ransomware Tracker

Distribution of Post by Group (Total - 9423 in Dec)



Post by Group last 7 days

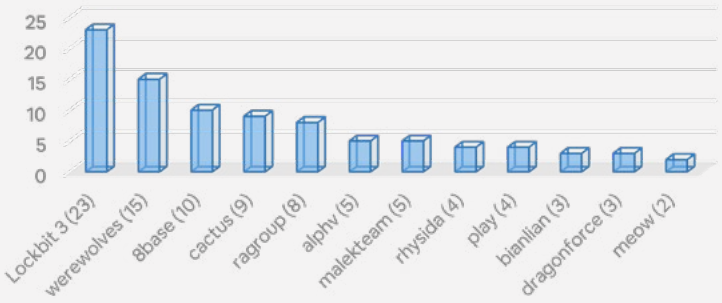


Image Source

Russian SVR aka Cozy Bear Actively Exploiting JetBrains TeamCity CVE

Software developers utilize TeamCity software for managing and automating software compilation, building, testing, and releasing processes. In the event of a compromise, unauthorized access to a TeamCity server exposes the software developer's source code, signing certificates, and the potential to manipulate software compilation and deployment processes. This access could be exploited by malicious actors to conduct supply chain operations, as witnessed in the SolarWinds compromise of 2020. Despite the TeamCity CVE being utilized by the SVR, the limited number of victims suggests a different approach compared to the SolarWinds incident. The SVR, however, leverages the initial access gained through the TeamCity CVE for privilege escalation, lateral movement, and deploying additional backdoors to ensure persistent access to compromised network environments.

Detection

Initial Access - Exploitation

The SVR initiated exploitation in late September 2023 by targeting Internet-connected JetBrains TeamCity servers using the CVE-2023-42793. This vulnerability allowed for the insecure handling of specific paths, enabling the bypassing of authorization and resulting in arbitrary code execution on the server. The observed exploitation consistently led to code execution with elevated privileges, providing the SVR with a strategic foothold in the network environment.

Host Reconnaissance

After gaining access, the SVR utilized basic built-in commands for host reconnaissance, extracting essential information such as user privileges, group memberships, domain details, active processes, network connections, and more. Additionally, the SVR leveraged PowerShell commands to query Active Directory properties, demonstrating a comprehensive effort to understand the compromised environment.

File Exfiltration

The SVR demonstrated file exfiltration capabilities, particularly targeting sensitive files related to the operating system, SQL Server, Visual Studio, and update management agents. Files were exfiltrated to gather information on system versions, SQL Server configurations, and Visual Studio details. The use of PowerShell for archiving and staging files indicates a deliberate and organized exfiltration process.

Tactics Used to Avoid Detection

To evade detection, the SVR employed various tactics, including the "Bring Your Own Vulnerable Driver" technique, using the EDRSandBlast tool. This technique was used to disable or terminate endpoint detection and response (EDR) and antivirus (AV) software. Additionally, the SVR masked its backdoors through DLL hijacking vulnerabilities in Zabbix and Webroot antivirus software, demonstrating a sophisticated approach to stealthy operations.

Privilege Escalation

The SVR facilitated privilege escalation using techniques such as modifying the NoLMHash registry key, employing the Mimikatz tool to extract cached credentials, and utilizing WinPEAS for comprehensive system analysis. These tactics aimed to elevate the SVR's access within the compromised environment, ensuring persistent control and maneuverability.

Persistence

Scheduled tasks were leveraged for persistent execution of backdoors, with executable files strategically stored in directories such as C:\Windows\temp, C:\Windows\System32, and C:\Windows\WinStore. The use of schtasks.exe facilitated the creation and management of scheduled tasks, allowing the SVR to maintain a long-term presence within the compromised network.

Sensitive Data Exfiltration

The SVR exfiltrated sensitive data, including Windows Registry hives (SYSTEM, SAM, SECURITY), using PowerShell commands and reg save functionality. Compression and staging of data into .zip archives were observed, showcasing an organized and covert approach to data exfiltration. Specific interest in SQL Server, Visual Studio, and update management agents' files underlines the SVR's focus on critical components.

Network Reconnaissance

After establishing a secure foothold, the SVR executed network reconnaissance using built-in commands and additional tools, such as port scanners and PowerSploit. PowerSploit commands were employed to gather information on network computers, groups, users, domain details, and more. This comprehensive reconnaissance phase enabled the SVR to understand the broader network landscape.

Tunneling into Compromised Environments

In selected environments, the SVR utilized the "rr.exe" tool, a modified open-source reverse socks tunneler (Rsockstun), to establish a tunnel to the command and control (C2) infrastructure. This tunneling technique provided a covert channel for communication and data exchange, enhancing the SVR's ability to operate undetected within the compromised environment.

Lateral Movement

The SVR used Windows Management Instrumentation Command Line (WMIC) for lateral movement, executing processes remotely to propagate within the network. Modification of the DisableRestrictedAdmin key enabled remote connections, demonstrating a strategic effort to extend influence beyond the initially compromised systems.

Adversary Toolset

The SVR employed custom and open-source tools, including GraphicalProton and its HTTPS variant, to facilitate data exchange and command execution. GraphicalProton, a backdoor leveraging OneDrive and Dropbox for communication, demonstrated sophistication in utilizing cloud services for covert operations. The HTTPS variant showcased the SVR's adaptability, relying on HTTP requests for communication and utilizing a re-registered expired domain to legitimize the command and control channel.

These technical details provide a deeper understanding of the SVR's tactics, techniques, and procedures, enabling organizations to enhance their detection and response capabilities against similar cyber threats.

The SVR's cyber operations, spanning since 2013, pose a persistent threat to both public and private organizations globally. While historical reports focused on spear-phishing operations, recent activities indicate a broader targeting pattern encompassing technology companies involved in future cyber operations. The SVR's exploitation of CVEs, deployment of custom malware, and targeting of specific industries, such as biomedical and energy, align with its mission to collect foreign intelligence, including economic intelligence and science and technology.

Indicators of Compromise (IOCs):

File IoCs

GraphicalProton backdoor:

- 01B5F7094DE0B2C6F8E28AA9A2DED678C166D615530E595621E692A9C0240732
- 34C8F155601A3948DDB0D60B582CFE87DE970D443CC0E05DF48B1A1AD2E42B5E
- 620D2BF14FE345EEF618FDD1DAC242B3A0BB65CCB75699FE00F7C671F2C1D869
- 773F0102720AF2957859D6930CD09693824D87DB705B3303CEF9EE794375CE13
- 7B666B978DBBE7C032CEF19A90993E8E4922B743EE839632BFA6D99314EA6C53
- 8AFB71B7CE511B0BCE642F46D6FC5DD79FAD86A58223061B684313966EFEF9C7
- 971F0CED6C42DD2B6E3EA3E6C54D0081CF9B06E79A38C2EDE3A2C5228C27A6DC

- CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC5869D85F69633E44DCF
- CD3584D61C2724F927553770924149BB51811742A461146B15B34A26C92CAD43
- EBE231C90FAD02590FC56D5840ACC63B90312B0E2FEE7DA3C7606027ED92600E
- F1B40E6E5A7CBC22F7A0BD34607B13E7E3493B8AAD7431C47F1366F0256E23EB
- C7B01242D2E15C3DA0F45B8ADEC4E6913E534849CDE16A2A6C480045E03FBEE4
- 4BF1915785D7C6E0987EB9C15857F7AC67DC365177A1707B14822131D43A6166

GraphicalProton HTTPS backdoor:

- 18101518EAE3EEC6EBE453DE4C4C380160774D7C3ED5C79E1813013AC1BB0B93
- 19F1EF66E449CF2A2B0283DBB756850CCA396114286E1485E35E6C672C9C3641
- 1E74CF0223D57FD846E171F4A58790280D4593DF1F23132044076560A5455FF8
- 219FB90D2E88A2197A9E08B0E7811E2E0BD23D59233287587CCC4642C2CF3D67
- 92C7693E82A90D08249EDEAFBCA6533FED81B62E9E056DEC34C24756E0A130A6
- B53E27C79EED8531B1E05827ACE2362603FB9F77F53CEE2E34940D570217CBF7
- C37C109171F32456BBE57B8676CC533091E387E6BA733FBAA01175C43CFB6EBD
- C40A8006A7B1F10B1B42FDD8D6D0F434BE503FB3400FB948AC9AB8DDFA5B78A0
- C832462C15C8041191F190F7A88D25089D57F78E97161C3003D68D0CC2C4BAA3
- F6194121E1540C3553273709127DFA1DAAB96B0ACFAB6E92548BFB4059913C69

Backdoored vcperf:

- D724728344FCF3812A0664A80270F7B4980B82342449A8C5A2FA510E10600443

Backdoored Zabbix installation archive:

- 4EE70128C70D646C5C2A9A17AD05949CB1FBF1043E9D671998812B2DCE75CF0F

Backdoored Webroot AV installation archive:

- 950ADBAF66AB214DE837E6F1C00921C501746616A882EA8C42F1BAD5F9B6EFF4

Modified rsockstun:

- CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC5869D85F69633E44DCF

Network IoCs

Tunnel Endpoints

- 65.20.97[.]203
- 65.21.51[.]58

Exploitation Server

- 103.76.128[.]34

GraphicalProton HTTPS C2 URL:

- hxxps://matclick[.]com/wp-query[.]php

Prevention

To mitigate the threat posed by the SVR's activities, organizations are advised to:

1. Apply patches promptly: Ensure that the CVE-2023-42793 patch issued by JetBrains TeamCity in mid-September 2023 is applied.
2. Monitor network activities: Look for evidence of encoded commands and the execution of network scanning tools.
3. Enable multi-factor authentication (MFA): Implement MFA, especially for critical systems and services, to enhance access security.
4. Keep systems updated: Regularly update operating systems, software, and firmware to maintain a secure environment.
5. Audit logs and deploy security tools: Review log files for privileged certificate access attempts and utilize security tools to identify suspicious behavior on systems.

Remediation

In the event of a potential compromise, organizations are advised to:

1. Conduct threat-hunting activities: Organizations with affected systems that did not apply patches or workarounds immediately should assume compromise and initiate threat-hunting activities.

2. Apply incident response recommendations: If potential compromise is detected, follow incident response recommendations provided in the advisory.
3. Report findings: Report key findings to the FBI and CISA for further investigation and collaboration.

These mitigations align with Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and NIST, providing a comprehensive approach to enhance cybersecurity posture.

APT28 & Exploitation of CVE-2023-23397

- Microsoft has recently detected nation-state cyber activity, backed by the Kremlin, exploiting a critical security flaw (CVE-2023-23397) in its Outlook email service.
- Attributed to the threat actor Forest Blizzard (formerly Strontium/APT28/Fancy Bear), the attack aims to gain unauthorized access to victims' accounts within Exchange servers.
- The security vulnerability, patched by Microsoft in March 2023, allows a privilege escalation that could lead to unauthorized access.
- The goal, as indicated by the Polish Cyber Command, is to compromise mailboxes of public and private entities, with subsequent malicious activities focused on modifying folder permissions for prolonged unauthorized access.

Detection

A successful exploit of CVE-2023-23397 can lead to unauthorized access to an organization's environment through a Net-NTLMv2 hash leak. Understanding the vulnerability and how threat actors leverage it is crucial for effective investigative processes.

Exploitation of CVE-2023-23397

- CVE-2023-23397 is a critical elevation of privilege vulnerability in Microsoft Outlook on Windows. It is exploited when a threat actor sends a specially crafted message to a user, triggering a Net-NTLMv2 hash leak to a server controlled by the threat actor.
- The message includes the PidLidReminderFileParameter property set to a UNC path share on a threat actor-controlled server via SMB/TCP port 445.
- Exploitation occurs when Outlook on Windows is open during the reminder trigger, sending the user's Net-NTLMv2 hash to the remote SMB server.

Post-Exploitation Activity

1. TNEF and Custom Sound Deception

   The technique leverages Transport Neutral Encapsulation Format (TNEF), a Microsoft-specific format for transmitting formatted email messages. Threat actors may set a custom sound file associated with a reminder to modify the PidLidReminderFileParameter property.

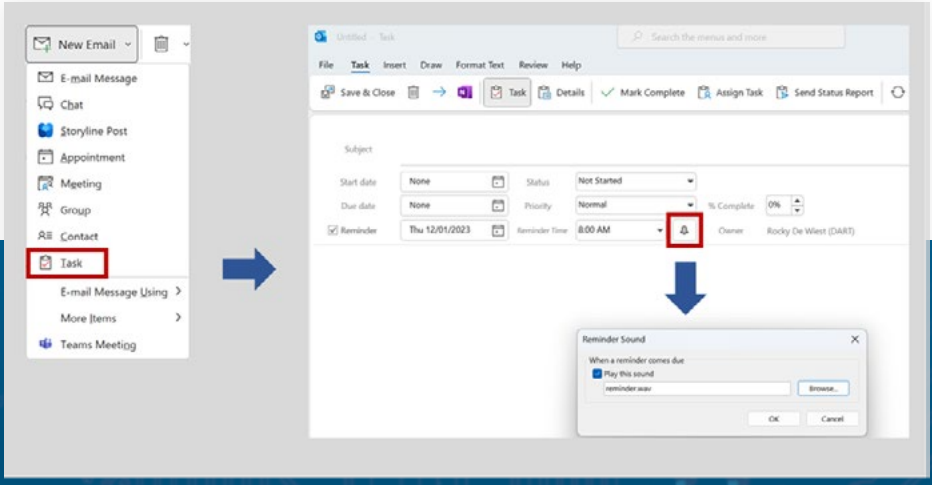


Figure 1 - Setting a custom sound to play when a reminder is triggered in Outlook on Windows client

A tool like MFCMAPI reveals extended MAPI properties associated with the mail object.

Deceptive actions include setting the PidLidReminderTime property to remain dormant and evade detection.

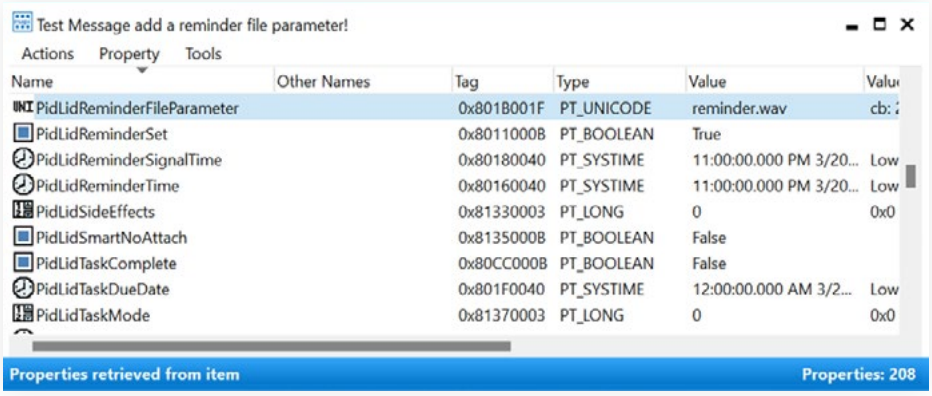


Figure 2 - Resulting extended MAPI Properties and their values as a result of customizing the sound to play when reminders are triggered as seen using MFCMAPI.

2. Net-NTLMv2 Hash Leakage

   The leaked Net-NTLMv2 hash belongs to the user signed in to the Windows device with the running Outlook client, regardless of the recipient's identity. If the reminder is not dismissed, the hash can be leaked multiple times.

3. Protocol Risks

   The vulnerability exploits the SMB protocol, not WebDAV. Interaction based on the WebDAV protocol does not risk leaking credentials to external IP addresses.

Observed Post-Exploitation Actions

Initial Access (Authentication Bypass):

- Net-NTLMv2 Relay attack against Exchange Servers.

Credential Access/Lateral Movement:

- Use of Exchange Web Services (EWS) API to send malicious messages.

Discovery/Persistence:

- Use of EWS API to enumerate folders and change mailbox folder permissions for persistent access.

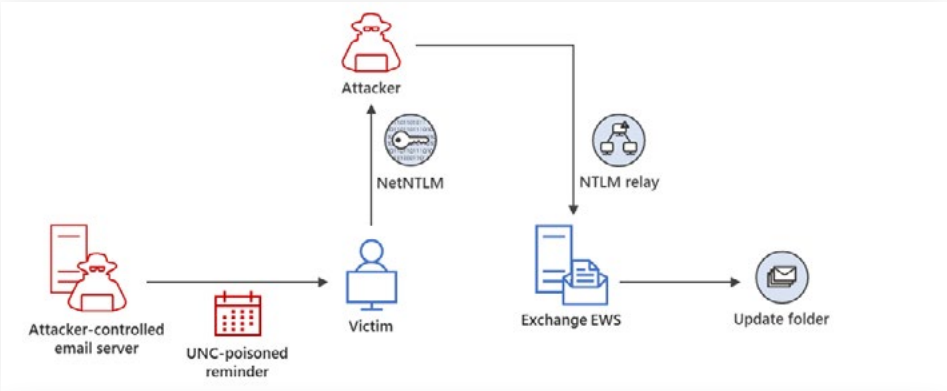


Figure 3 - Observed threat actor exploitation of CVE-2023-23397 to gain unauthorized access to Exchange Server and modify mailbox folder permissions for persistent access to the mailbox.

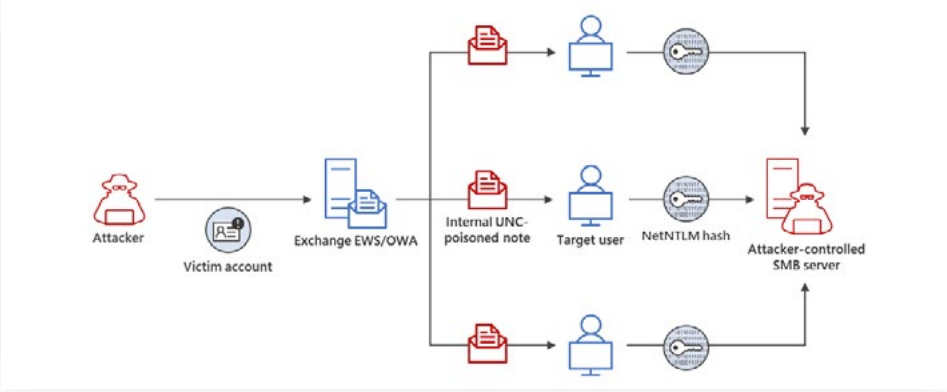


Figure 4 - Observed threat actor activity to extend their access in a compromised environment by using a compromised e-mail account to target other members of the same organization.

APT28 or Forest Blizzard, a well-resourced group associated with Russian military intelligence (GRU), has been exploiting this vulnerability in a series of campaigns targeting strategic organizations related to energy, transportation, military, and government sectors across NATO member countries.

Indicators of Compromise

- 101.255.119[.]42
- 213.32.252[.]221
- 168.205.200[.]55
- 185.132.17[.]160
- 69.162.253[.]21
- 113.160.234[.]229
- 181.209.99[.]204
- 82.196.113[.]102
- 85.195.206[.]7
- 61.14.68[.]33

Several malicious samples have been uploaded to VirusTotal.com and a signature has been created that identifies potentially malicious messages associated with exploitation of CVE-2023-23397.

VirusTotal subscribers can review those results here:

https://www.virustotal.com/gui/search/crowdsourced_yara_rule%253A000bc4a247%257CEXPL_SUSP_Outlook_CVE_2023_23397_Exfil_IP_Mar23

Prevention

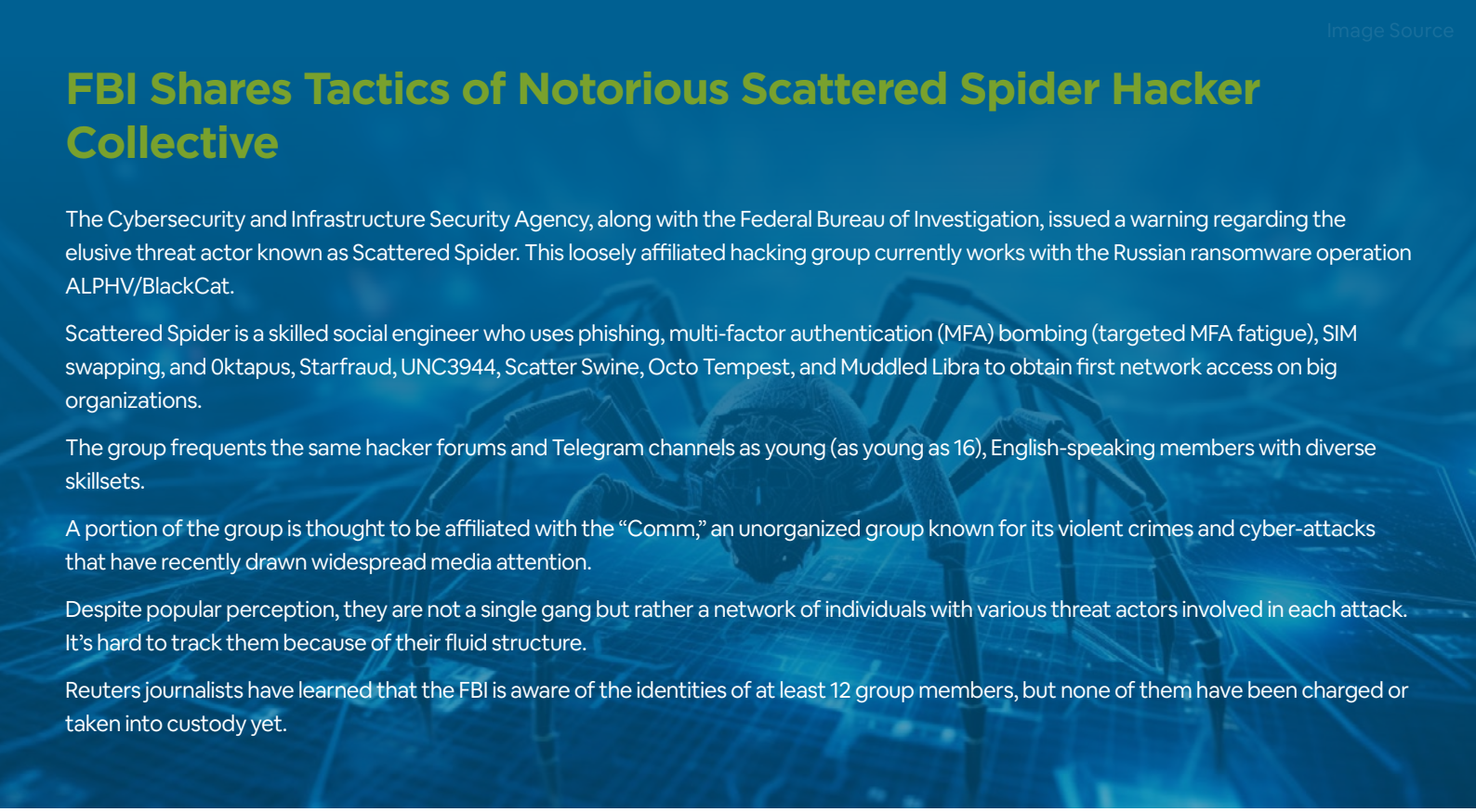
To mitigate the threat posed by the Forest Blizzard activities, organizations are advised to:

- Promptly patch the CVE-2023-23397 vulnerability in their Microsoft Outlook installations.
- Address the vulnerability and install the Outlook security update. Additional protections are provided in Outlook, Exchange Online, and Exchange Server.
- Endpoint protections should be configured to block malicious campaigns associated with Forest Blizzard.
- Ongoing monitoring of network activities for unusual patterns and implementing robust cybersecurity measures are crucial preventive measures.
- Examine reported messages, calendar items, or tasks with reminders for anomalies.
- Investigate evidence of known indicators and anomalies in NTLM authentication, WebDAV connections, SMBClient logs, firewall logs, etc.
- Leverage advanced hunting tools to align SMB connections with Net-NTLMv2 behavior. Query telemetry data for potential threats and analyzed logs for specific indicators.

Remediation

In case of compromise, remediation efforts should include the following:

1. Investigate and undo any unauthorized modifications to mailbox permissions.
2. Update Microsoft Outlook:
   - Apply the latest security updates to mitigate the vulnerability.
3. Implement Security Best Practices:
   - Add users to the Protected Users group.
   - Block TCP 445/SMB outbound.
   - Apply defense-in-depth measures on Exchange.
4. Threat Hunting and Incident Response:
   - Employ threat-hunting techniques and initiate incident response activities for compromised users.



FBI Shares Tactics of Notorious Scattered Spider Hacker Collective

The Cybersecurity and Infrastructure Security Agency, along with the Federal Bureau of Investigation, issued a warning regarding the elusive threat actor known as Scattered Spider. This loosely affiliated hacking group currently works with the Russian ransomware operation ALPHV/BlackCat.

Scattered Spider is a skilled social engineer who uses phishing, multi-factor authentication (MFA) bombing (targeted MFA fatigue), SIM swapping, and 0ktapus, Starfraud, UNC3944, Scatter Swine, Octo Tempest, and Muddled Libra to obtain first network access on big organizations.

The group frequents the same hacker forums and Telegram channels as young (as young as 16), English-speaking members with diverse skillsets.

A portion of the group is thought to be affiliated with the "Comm," an unorganized group known for its violent crimes and cyber-attacks that have recently drawn widespread media attention.

Despite popular perception, they are not a single gang but rather a network of individuals with various threat actors involved in each attack. It's hard to track them because of their fluid structure.

Reuters journalists have learned that the FBI is aware of the identities of at least 12 group members, but none of them have been charged or taken into custody yet.

Detection

Since last summer, when researchers from the cybersecurity company Group-IB published a report about a wave of attacks intended to steal 2FA codes and Okta identity credentials that began in March of the same year, Scattered Spider attacks have been documented.

The threat actor was identified by CrowdStrike in December 2022 as a financially driven organization that targets telcos and uses sophisticated social engineering techniques, defense reversal, and a wide range of software tools.

Crowdstrike discovered in January 2023 that Scattered Spider was avoiding detection from EDR (endpoint detection and response) security products by using BYOVD (Bring Your Own Vulnerable Driver) techniques.

Additionally, in September, Scattered Spider was blamed for two well-publicized attacks against Caesars Entertainment and MGM Casino, in which threat actors encrypted systems using the BlackCat/ALPHV locker.

Tactics

The FBI and CISA alert draws attention to Scattered Spider's potent initial access strategies, which involve tricking workers at a company into providing credentials or even direct network access by assuming the identity of IT or help desk personnel.

Phone calls, SMS phishing, email phishing, MFA fatigue attacks, and SIM swapping are examples of individual tactics. To appear genuine, the domains used for email and SMS phishing misuse the names of the target along with the Okta and Zoho ServiceDesk brands.

Following its establishment on the network, Scattered Spider moves laterally and conducts reconnaissance using a variety of openly accessible software tools, such as:

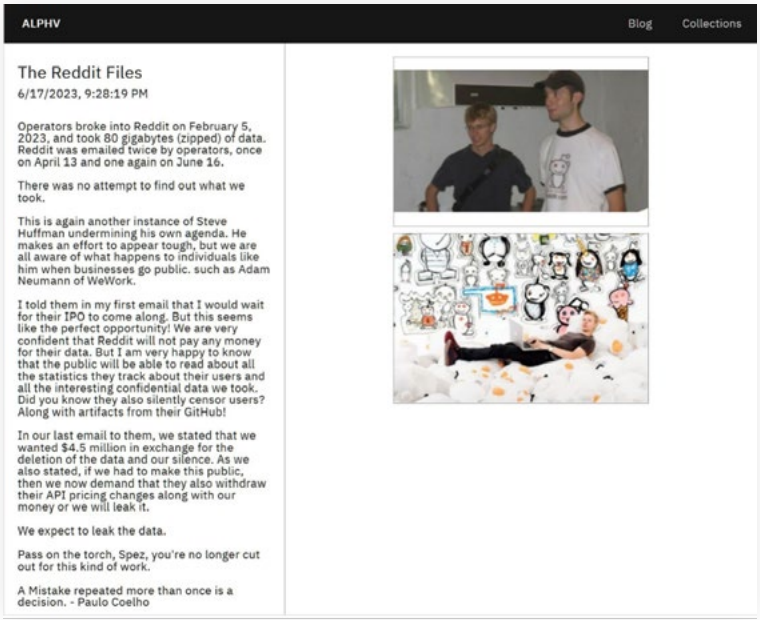
- Fleetdeck.io: Online system administration and monitoring
- Level.io: Online system administration and monitoring
- Mimikatz: Extraction of Credentials
- Ngrok: Internet tunnelling for remote web server access
- Pulseway: Remote monitoring and system management
- Screenconnect: Remote connection management for network devices
- Splashtop: Remote connection management for network devices
- Tailscale: Virtual Private Network for Safe Internet Access
- Teamviewer: Remote connection management for network devices

Scattered Spider not only uses the tools, which are legitimate tools used for malicious purposes, but also launches phishing attacks to

infect systems with malware such as the WarZone RAT, Raccoon Stealer, and Vidar Stealer. This allows the malware to steal cookies, login credentials, and other pertinent data from compromised systems.

Data exfiltration and file encryption using the ALPHV/BlackCat ransomware, followed by contact with the victims via messaging apps, email, or other secure tools to negotiate a ransom payment, is a new tactic seen in the threat group's recent attacks.

As demonstrated by their attack on Reddit, the Scattered Spider actors, who are associated with BlackCat, have a history of using the ransomware gang's data leak website as a means of extortion. Here, they either release statements or leak data.



Important resources like source code repositories, code-signing certificates, and credential storage pique the interest of Scattered Spider in particular.

Additionally, the attackers keep a careful eye on the victim's Microsoft Teams, Microsoft Exchange emails, and Slack channels for any messages that might hint that their actions have been noticed.

Prevention

- Block unknown scripts from running.
- Patch all .DLL files on production.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Do not use malicious/free VPN to access web applications or networks.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

- Use application controls with "allowlisting" to manage software execution.
- Monitor remote access tools and implement phishing-resistant multifactor authentication (MFA).
- Secure and limit Remote Desktop Protocol (RDP) usage with best practices and MFA.
- Maintain offline backups and adhere to a robust data recovery plan.
- Follow NIST standards for strong, less frequently changed passwords.
- Keep systems and software regularly updated, focusing on patching vulnerabilities.
- Implement network segmentation to control traffic and prevent ransomware spread.
- Use network monitoring and Endpoint Detection and Response (EDR) tools to detect abnormal activities.
- Enhance email security by disabling risky links and encrypting backup data.

The New APT Group DarkCasino and the Global Surge in WinRAR 0-Day Exploits

Security Researchers have exposed a massive APT attack campaign called DarkCasino and discovered a dangerous and persistent aggressive threat actor. It has also been determined that the attacker's activities are not associated with any known APT groups, confirming that it poses a high-level persistent threat. By adopting the operational name, the APT group has been assigned the name DarkCasino.

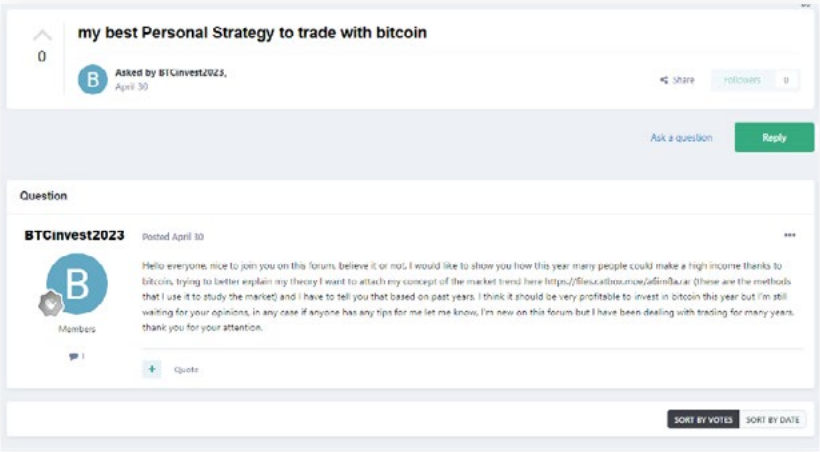
Security vendor Group-IB investigated in August 2023 and revealed DarkCasino's actions against members of cryptocurrency forums. They also discovered that the DarkCasino APT threat actor had exploited the WinRAR 0-day vulnerability CVE-2023-38831 in this attack.

Examining the exploitation of WinRAR vulnerabilities, Security Research discovered numerous attacks by both confirmed and unconfirmed APT organizations, in addition to analyzing the attack activities of the APT group DarkCasino and verifying its strategies and tactics. Multinational corporations or national governments were the targets of many of these attacks.

Detection

In this new attack pattern, DarkCasino took advantage of a WinRAR zero-day vulnerability (later discovered by security researchers and given the number CVE-2023-38831) by inserting malicious programs into specially created vulnerability zip files for phishing attacks against forum users through online trading forum posts.

DarkCasino created a variety of post content, including advice on investments and ways to make money, and tricked forum members into opening malicious files that were either attached to or linked to the posts.

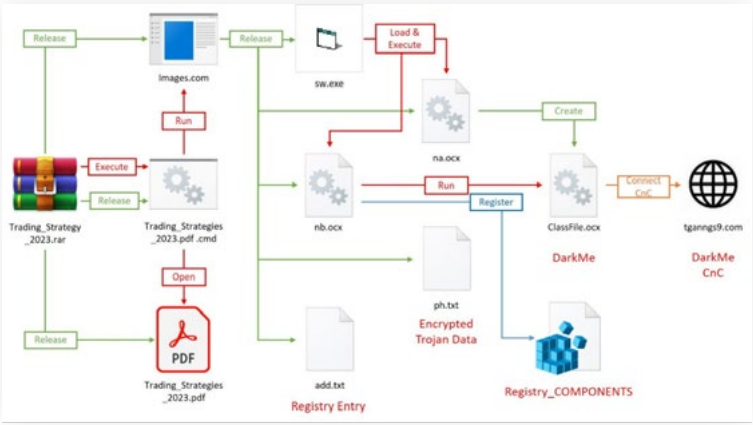


Attack Process Analysis

Security Researchers discovered that by using these vulnerabilities to compress files, DarkCasino implemented two attack processes. The primary distinction between these two attack procedures is in the way the Trojan data is stored. Otherwise, their logic is similar.

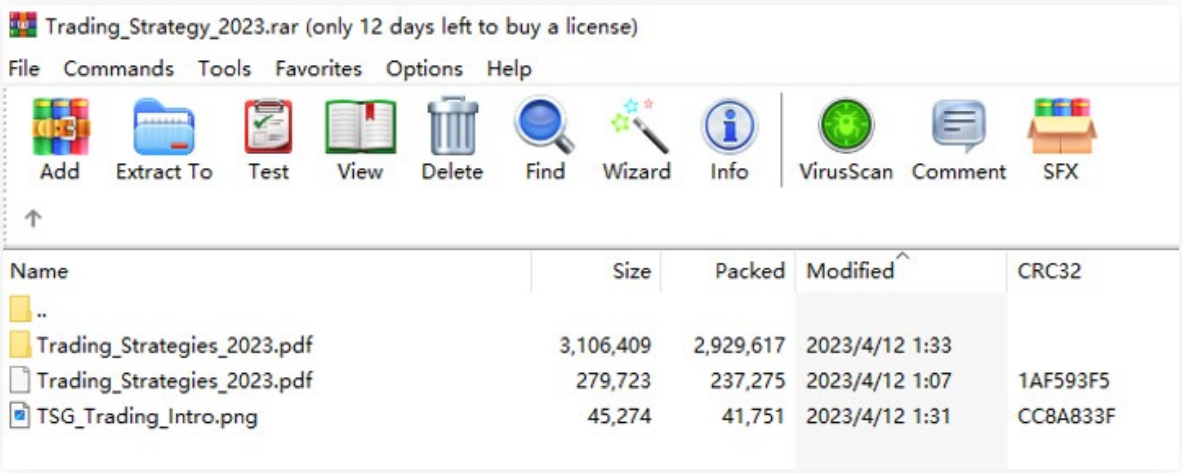
This report introduces DarkCasino's process design ideas and changes for this round of operations using the attack flow and encrypted.txt files as an example.

The following figure illustrates the main components of this attack process: the registry file, ActiveX control file, CVE-2023-38831 vulnerability exploitation file, and Cabinet archive file. Vulnerability exploitation, load release, and Trojan execution are its three phases.

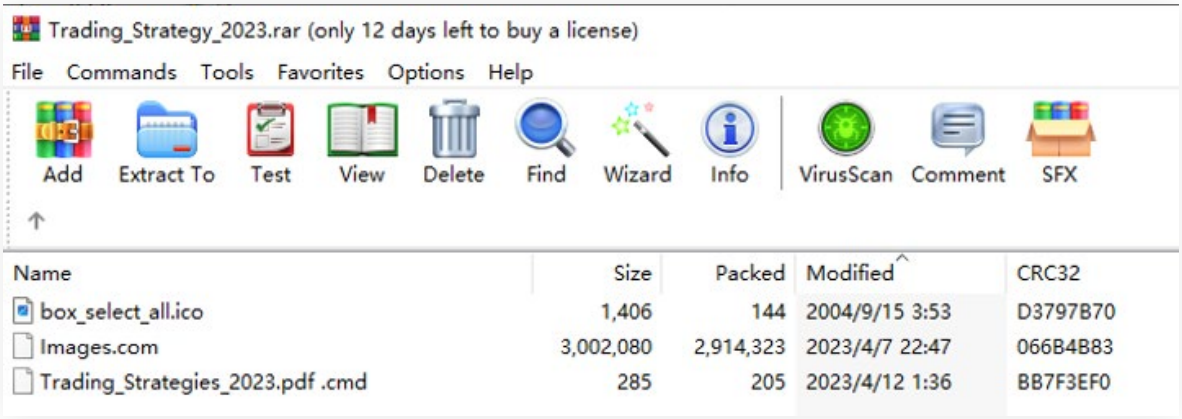


In an alternate attack flow, DarkCasino substitutes a steganographic image for the medium holding encrypted Trojan data.

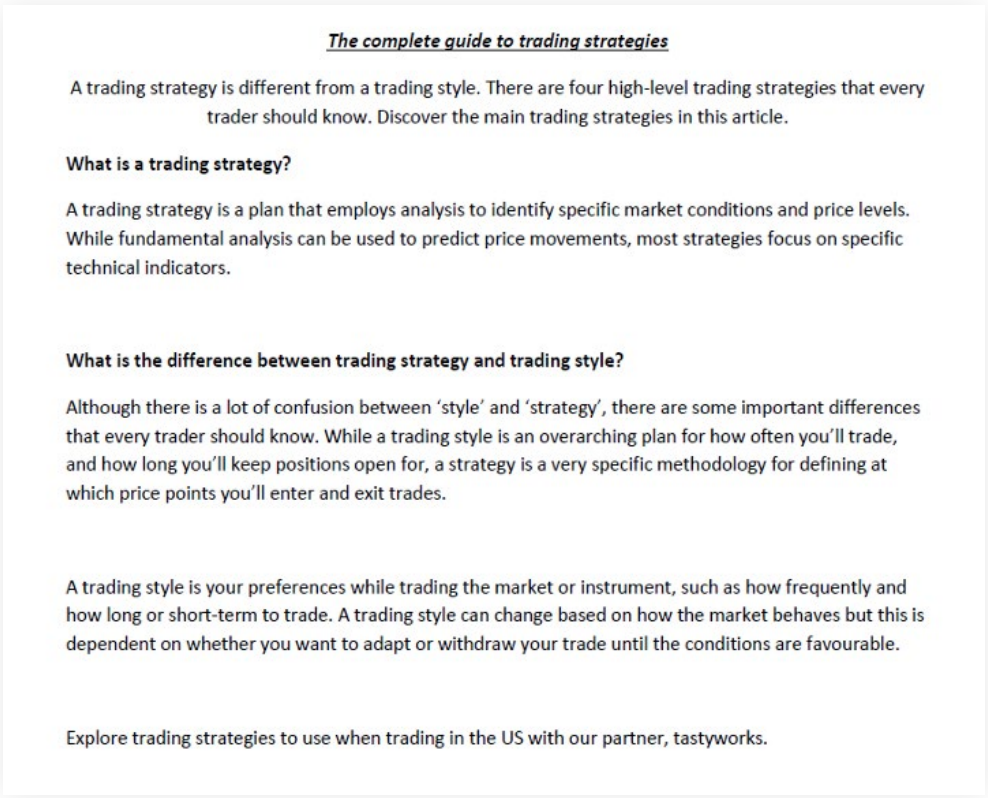
The victim will discover the following file structure in WinRAR when they open a file called “Trading_strategy_2023.rar”:



A common build pattern for vulnerabilities CVE-2023-38831 is as follows. The “Trading_Strategies_2023.pdf.cmd” batch file is executed under the same name folder when the user attempts to double-click the PDF file in the zip package.



The data contained in the original decoy PDF file in this example process are displayed below. This batch will open both the malicious Images.com file and the original decoy PDF file.



The complete guide to trading strategies

A trading strategy is different from a trading style. There are four high-level trading strategies that every trader should know. Discover the main trading strategies in this article.

What is a trading strategy?

A trading strategy is a plan that employs analysis to identify specific market conditions and price levels. While fundamental analysis can be used to predict price movements, most strategies focus on specific technical indicators.

What is the difference between trading strategy and trading style?

Although there is a lot of confusion between ‘style’ and ‘strategy’, there are some important differences that every trader should know. While a trading style is an overarching plan for how often you’ll trade, and how long you’ll keep positions open for, a strategy is a very specific methodology for defining at which price points you’ll enter and exit trades.

A trading style is your preferences while trading the market or instrument, such as how frequently and how long or short-term to trade. A trading style can change based on how the market behaves but this is dependent on whether you want to adapt or withdraw your trade until the conditions are favourable.

Explore trading strategies to use when trading in the US with our partner, tastyworks.

Load Release Stage

The loader-type Trojan created by DarkCasino that was used to execute batch files inside the Images.com file was discovered. The program, which consists of five components—sw.exe, na.ocx, nb.ocx, ph.txt, and add.txt—is a cabinet archive file that is masquerading as a.com file.

The sw.exe application will be launched by the loader Trojan to initiate the next loading execution process after it releases the five components into the TEMP directory.

Sw.exe is primarily used to load the library files na.ocx and nb.ocx; it does not itself contain any malicious functions.

The ph.txt file will be read and encrypted by na.ocx, which will then move add.txt to this directory and store the encrypted content in %APPDATA%\RarDir\ClassFile.ocx.

The primary CMD commands executed by the nb.ocx file are as follows:

command /c timeout 1&&cmd /c reg.exe import add.txt; cmd /c cd APPDATA\RarDir

cmd /c rundll32.exe /sta; cmd /c timeout 1; cmd /c cd APPDATA\RarDir Mouse_Keyboard {EA6FC2FF-7AE6-4534-9495-F688FEC7858C}

By writing to the host registry and then executing it, these cmd commands register a com component and the decrypted and saved ClassFile.ocx file mentioned above is the registered com component.

IoC

Hash	APT Group
dd9146bf793ac34de3825bdabcd9f0f3	DarkPink
5504799eb0e7c186afcb07f7f50775b2	DarkPink
c5331b30587dcaf94bfde94040d4fc89	DarkPink
ac28e93dbf337e8d1cc14a3e7352f061	DarkPink
fefe7fb2072d755b0bfdf74aa7c9013e	DarkPink
428a12518cea41ef7c57398c69458c52	Konni
7bb106966f6f8733bb4cc5bf2ab2bab4	GhostWriter
2b02523231105ff17ea07b0a7768f3fd	Actor230830
63085b0b7cc5bb00859aba105cbb40b1	Actor231003
7195be63a58eaad9fc87760c40e8d59d	Actor231004
129ccb333ff92269a8f3f0e95a0338ba	Actor231010
cd1f48df9712b984c6eee3056866209a	Actor231010
b05960a5e1c1a239b785f0a42178e1df	Actor231010
6b5d5e73926696a6671c73437cedd23c	Actor231009

Prevention

- Block unknown scripts from running.
- Do not click on the malicious link.
- Do not share your credentials on fake URLs.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connections.
- Do not install unwanted applications from untrusted sources.
- Enable limitations on administrative access or rights.

Remediation

- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving data through communication channels.
- Update your machine & servers on a monthly basis.
- Enable packet filtration through the firewall.
- Configure DLP in environment properly.
- Update the operating system (OS) and all installed programs.
- Use a paid VPN to access web applications or networks.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

TOP THREAT ACTORS

Threat Actor	IOC Reference
Cozy Bear	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a?&web_view=true
Forrest Blizzard	https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
Scattered Spider	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
Dark Casino	https://securityboulevard.com/2023/11/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/?web_view=true
Gang 8220	https://www.imperva.com/blog/imperva-detects-undocumented-8220-gang-activities/?web_view=true

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
Zero-Day Kofax Power PDF J2K File Parsing Memory Corruption Remote Code Execution Vulnerability CVE-2023-51608	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Kofax Power PDF. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://www.cybersecurity-help.cz/vdb/SB2023122207
Linux Kernel nf_tables_expr_destroy Use-After-Free Privilege Escalation Vulnerability CVE-2022-32250	Vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	https://access.redhat.com/security/cve/cve-2022-32250
D-Link G416 awsfile rm Command Injection Remote Code Execution Vulnerability CVE-2023-50217	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link G416 routers. The specific flaw exists within the HTTP service listening on TCP port 80.	https://www.cyberveille-sante.gouv.fr/alertes/d-link-cve-2023-50217-2023-12-21
Inductive Automation Ignition ModuleInvoke Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-50218	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.	https://nvd.nist.gov/vuln/detail/CVE-2023-29218
Parallels Desktop virtio-gpu Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2023-50227	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Parallels Desktop. User interaction is required to exploit this vulnerability in that the target in a guest system must visit a malicious page or open a malicious file.	https://vuldb.com/?id.248378

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
Schneider Electric EcoStruxure Power Monitoring Expert GetFilteredSinkProvider Deserialization of Untrusted Data Remote Code Execution Vulnerability CVE-2023-5391	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Schneider Electric EcoStruxure Power Monitoring Expert. The specific flaw exists within the GetFilteredSinkProvider method.	https://www.tenable.com/cve/CVE-2023-5391
Microsoft Windows win32kfull UMPDDrvCopyBits Use-After-Free Local Privilege Escalation Vulnerability CVE-2023-36804	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. The specific flaw exists within the win32kfull driver. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://www.rapid7.com/db/vulnerabilities/msft-cve-2023-36804/
Zero-Day Intel Driver & Support Assistant Link Following Local Privilege Escalation Vulnerability CVE-2023-50197	Vulnerability allows local attackers to escalate privileges on affected installations of Intel Driver & Support Assistant. The specific flaw exists within the DSA Service. By creating a symbolic link, an attacker can abuse the service to write a file.	https://www.redpacketsecurity.com/intel-driver-support-assistant-privilege-escalation-cve-2023-50197/
Microsoft Skype Cross-Site Scripting Remote Code Execution Vulnerability	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Microsoft Skype. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	https://www.zerodayinitiative.com/advisories/ZDI-23-1769/
Extreme Networks AP410C ah_webui Missing Authentication for Critical Function Remote Code Execution Vulnerability CVE-2023-46271	Vulnerability allows network-adjacent attackers to reach critical functions on affected installations of Extreme Networks AP410C routers. The specific flaw exists within the ah_webui service, which listens on TCP port 3009 by default.	https://extreme-networks.my.site.com/ExtrArticleDetail?an=000115354&q=CVE-2023-46271
SolarWinds Orion Platform VimChartInfo SQL Injection Remote Code Execution Vulnerability CVE-2023-40056	Vulnerability allows remote attackers to execute arbitrary code on affected installations of SolarWinds Orion Platform. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://www.solarwinds.com/trust-center/security-advisories/cve-2023-40056
Delta Electronics InfraSuite Device Master RunScript Exposed Dangerous Method Remote Code Execution Vulnerability CVE-2023-39226	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Delta Electronics InfraSuite Device Master. Authentication is not required to exploit this vulnerability. The specific flaw exists within the RunScript method.	https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-39226
Zero-Day Voltronic Power ViewPower Pro selectDeviceListBy SQL Injection Remote Code Execution Vulnerability CVE-2023-51595	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Voltronic Power ViewPower Pro. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries.	https://www.cybersecurity-help.cz/vdb/SB2023122218
oFono SMS Decoder Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-2794	Vulnerability allows remote attackers to execute arbitrary code on affected installations of oFono. The specific flaw exists within the parsing of SMS PDUs.	https://bugzilla.redhat.com/show_bug.cgi?id=2255387
Zero-Day Hancom Office Show PPT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-50235	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Hancom Office Show. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer.	https://www.redpacketsecurity.com/hancom-office-show-buffer-overflow-cve-2023-50235/
Zero-Day Honeywell Saia PG5 Controls Suite CAB File Parsing Directory Traversal Remote Code Execution Vulnerability CVE-2023-51603	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Honeywell Saia PG5 Controls Suite. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations.	https://www.redpacketsecurity.com/honeywell-saia-pg5-controls-suite-directory-traversal-cve-2023-51603/
NETGEAR ProSAFE Network Management System saveNodeLabel Cross-Site Scripting Privilege Escalation Vulnerability CVE-2023-50231	Vulnerability allows remote attackers to escalate privileges on affected installations of NETGEAR ProSAFE Network Management System. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script.	https://www.zerodayinitiative.com/advisories/ZDI-23-1847/
Trimble SketchUp Viewer SKP File Parsing Use-After-Free Remote Code Execution Vulnerability CVE-2023-50196	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Trimble SketchUp Viewer. The specific flaw exists within the parsing of SKP files. The issue results from the lack of validating the existence of an object prior to performing operations on the object.	https://www.kyoceradocumentsolutions.us/en/about-us/pr-and-award-certifications/press/kyocera-device-manager-cve-2023-50196-vulnerability-solution-update.html
Linux Mint Xreader CBT File Parsing Argument Injection Remote Code Execution Vulnerability CVE-2023-44452	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Linux Mint Xreader. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call.	https://vulmon.com/vulnerabilitydetails?qid=CVE-2023-44452

Security Bulletin

1. Threat Actor Targets Recruiters with Malware

Recruiters are currently facing a sophisticated threat from a financially motivated actor known as TA4557, as per security researchers. This threat actor employs malicious emails to infect targets, utilizing the More_Eggs backdoor. The More_Eggs backdoor is designed to establish persistence, profile the compromised system, and deploy additional payloads.

TA4557 initially responded to job vacancies on third-party employment platforms in 2022 and early 2023. More recently, the threat actor has shifted to contacting recruiters directly. In a novel attack chain utilizing a direct email technique, the actor replies with a URL leading to an actor-controlled website posing as a candidate's resume after the recipient responds to the initial email. Alternatively, the actor may respond with a Word or PDF attachment instructing the recipient to visit the fraudulent resume website.

In recent phishing attempts, the threat actor instructs the target to "refer to the domain name of my email address to access my portfolio," aiming to bypass security filters. Visiting the sender's website and following these instructions leads to a CAPTCHA page. Upon completion, a zip file is downloaded, containing a shortcut file (LNK).

Upon execution, the LNK file exploits valid software features in 'ie4uinit.exe' to download and execute a scriptlet from a location specified in the 'ie4uinit.inf' file. After decryption, the scriptlet deposits a DLL in the subdirectory %APPDATA%\Microsoft. Subsequently, it attempts to use Windows Management Instrumentation (WMI) to initiate a new regsrv32 process for running the DLL. If unsuccessful, it employs an alternative strategy using the ActiveX Object Run function.

These "living-off-the-land" techniques are crafted to infect the victim's computer with the More_Eggs backdoor by launching a DLL. To mitigate the threat posed by TA4557, associated with FIN6, Proofpoint recommends that recruiters update their user awareness training. The adoption of this technique by TA4557 may lull recipients into a false sense of trust, making them more susceptible to engaging with and sharing content from the threat actor.

Researchers have noted an increase in threat actors utilizing benign messages to build trust with targets before delivering malicious content. The gang's frequent modification of infrastructure, fake resume domains, and sender emails pose a challenge for automated security systems, as it becomes difficult to identify harmful information.

2. New AeroBlade Hackers Target Aerospace Sector in the U.S.

'AeroBlade,' a previously unidentified cyber espionage hacking gang, was found to be targeting US aerospace industry groups.

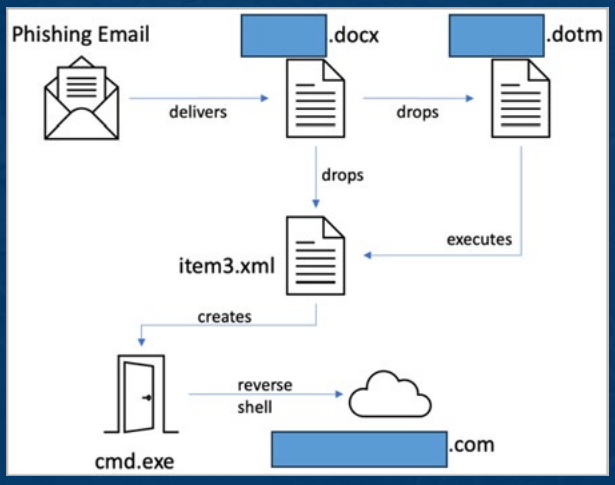
The effort was carried out in two stages: a testing phase in September 2022 and a more sophisticated attack in July 2023.

To gain initial access to corporate networks, the assaults involved spear-phishing using weaponized documents, dropping a reverse-shell payload that can be used for file listing and data theft.

The primary objective of this attack was commercial cyber espionage, with a mid to high degree of confidence, in order to obtain important data.

Campaign Details

The first attacks linked to AeroBlade happened in September 2022. The second stage DOTM file was downloaded using phishing emails with a document (docx) attachment that used remote template injection.



To establish a reverse shell on the target's system and connect it to the attacker's command and control (C2) server, the second step of the attack uses malicious macros.

"Once the victim opens the file and executes it by manually clicking the "Enable Content" lure message, the [redacted].dotm document discretely drops a new file to the system and opens it," states BlackBerry.

"The newly downloaded document is readable, leading the victim to believe that the file initially received by email is legitimate."

The reverse shell payload, a massively obfuscated DLL that specifies every directory on the stolen computer, helps its operators plan their next moves in data theft.

The DLL file incorporates anti-analysis features such as API hashing to conceal Windows function misuse, proprietary string encoding, dead code and control flow obfuscation for disassembly protection, and sandbox detection.

Additionally, the payload adds a process called "WinUpdate2" to the Windows process Scheduler to create persistence on compromised computers even after a system reboot.

Most of the evasion techniques seen in the 2023 samples, as well as the capacity to list folders and exfiltrate data, were absent from the early DLL payload samples.

This suggests that while the 2022 attempts were mostly concerned with testing the intrusion and infection chain, threat actors are still developing new tools for increasingly complex attacks.

The threat actors utilized the identical lure documents in the phishing stage of both operations, and the ultimate payload was a reverse shell connecting to the same C2 IP address.

BlackBerry has not been able to ascertain AeroBlade's source or the exact aim of the attacks.

The researchers hypothesize that the purpose of the data theft was to either sell the knowledge, give it to rival aerospace companies abroad, or use it as leverage to blackmail victims.

3. North Korea-Linked APT Group Sapphire Sleet Set Up Bogus Skills Assessment Portals in Attacks Aimed at IT Job Seekers

Sapphire Sleet, also known as APT38, BlueNoroff, CageyChameleon, and CryptoCore, is an Advanced Persistent Threat (APT) group linked to North Korea and considered a subset of the Lazarus APT organization. The group primarily targets banks, venture capital firms, and cryptocurrency exchanges in its campaigns. Microsoft researchers have issued a warning to IT job applicants about a recent social engineering campaign orchestrated by Sapphire Sleet, involving the use of fraudulent talent evaluation portals.

According to Microsoft's alerts on X, Sapphire Sleet, known for cryptocurrency theft through social engineering, has shifted its tactics in recent weeks by creating new websites posing as skills assessment portals. The APT group previously employed tools like LinkedIn to lure victims with offers related to competence evaluation. Once contact is established, the threat actors transition to other communication channels such as email or instant messaging apps.

To deceive recruiters into creating accounts, Sapphire Sleet registered multiple domains. The APT group either sent URLs to pages hosted on reputable sites like GitHub or directly transmitted malicious attachments. Microsoft specialists suspect that the group developed its own websites after uncovering Sapphire Sleet's previous strategies.

In a separate discovery, Jamf Threat Labs identified a new macOS malware strain named ObjCShellz and linked it to APT BlueNoroff, associated with North Korea. The RustBucket malware campaign, attributed to the BlueNoroff APT group, shares similarities with the ObjCShellz virus. The use of a domain resembling that of a reputable exchange suggests that threat actors targeted an organization or individual with an interest in the cryptocurrency industry, although specific targets have not been identified.

Elastic Security Labs recently disclosed the use of new KandyKorn macOS malware by the Lazarus APT group, also associated with North Korea. These attacks, directed at blockchain developers, demonstrate the ongoing and evolving threats posed by APT groups in the cybersecurity landscape.

4. Kinsing Exploits Linux Vulnerability for Cloud Credential Extraction

Threat actors associated with Kinsing are actively exploiting the Linux privilege escalation vulnerability, Looney Tunables (CVE-2023-4911), in a new experimental campaign. The attackers are demonstrating an expanded focus on cloud-native attacks by extracting credentials from Cloud Service Providers (CSP), a strategic shift from their traditional methods. Kinsing's exploitation of Looney Tunables poses a severe threat, potentially granting the attacker root privileges and compromising cloud environments.

In technical terms, the attackers leverage a Python-based exploit disclosed on X (formerly Twitter) by the researcher bl4sty to probe victim environments for the Looney Tunables vulnerability. After identification, Kinsing executes an additional PHP exploit, initially obscured but revealed to be a JavaScript code upon de-obfuscation. The JavaScript code functions as a web shell, providing backdoor access to the server, enabling file manipulation, command execution, and retrieval of system information.

Organizations are advised to monitor for unusual activities related to Linux systems, especially those indicating exploitation of the Looney Tunables vulnerability. Unexplained changes in system configurations, unauthorized access, or abnormal patterns of cloud credential usage should be thoroughly investigated.

To prevent such attacks, it is crucial to apply the latest security patches to Linux systems promptly to mitigate the risk of Looney Tunables exploitation. Enhance cloud security measures by implementing multi-factor authentication, regularly updating credentials, and monitoring CSP activity for anomalies.

In the event of a suspected compromise, organizations should conduct a thorough review of system logs, focusing on Linux systems and cloud infrastructure. Rotate and strengthen credentials associated with cloud services, limiting potential damage caused by unauthorized access.

This development marks a significant shift in Kinsing's tactics, showcasing a heightened focus on cloud environments and a diversified operational scope. Organizations are urged to bolster their defense promptly to mitigate the evolving threat landscape posed by Kinsing's latest campaign.

5. MongoDB Investigates Customer Account Data Breach

MongoDB, a leading database provider, recently faced a security incident involving unauthorized access to specific corporate systems. Lena Smart, MongoDB's Chief Information Security Officer, communicated the issue to clients via email, stating that the breach exposed contact details and metadata from consumer accounts. The incident was detected on December 13, prompting MongoDB to activate its incident response procedures.

MongoDB reassured clients that, as of the latest update, there is no evidence of security breaches involving client data stored in MongoDB Atlas. Despite the breach, the company encouraged customers to be vigilant for potential phishing attempts that may leverage the compromised account details and metadata to appear legitimate.

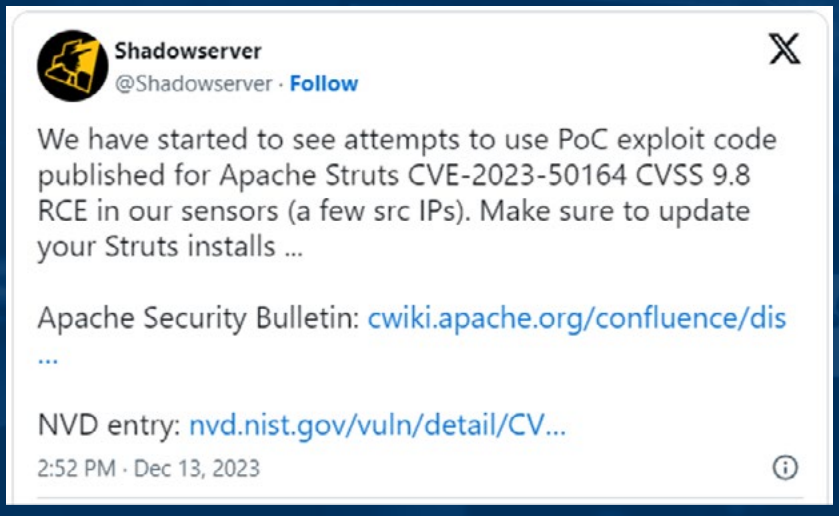
According to Smart, the unauthorized access might have occurred over an extended period before its discovery, and an ongoing active investigation is being conducted to determine the full scope of the incident. Clients were advised to implement phishing-resistant multi-factor authentication (MFA) promptly and consider changing passwords regularly.

A subsequent update from MongoDB clarified that the security breach was unrelated to the recent surge in login attempts causing issues for clients accessing Atlas and its Support Portal. While malicious hackers have historically targeted misconfigured MongoDB databases, leading to data theft and ransom demands, MongoDB hasn't experienced any significant breaches in recent times.

6. Hackers Are Exploiting Critical Apache Struts Flaw Using Public PoC

Attackers using publicly accessible proof-of-concept exploit code are trying to take advantage of a recently patched major vulnerability (CVE-2023-50164) in Apache Struts that allows for remote code execution.

The Shadowserver scanning platform's researchers saw a modest number of IP addresses involved in exploitation attempts, suggesting that threat actors are still relatively new.



With its form-based interface and powerful integration features, Apache Struts is an open-source web application framework that makes it easier to create Java EE web applications.

Because of the product's effectiveness in creating scalable, dependable, and readily maintained web applications, it is widely utilized in a variety of businesses in both the public and private sectors, including government organizations.

Versions 6.3.0.2 and 2.5.33 of Struts were made available by Apache on December 7 to fix a critical severity vulnerability that is presently known as CVE-2023-50164.

The security concern constitutes a path traversal defect that can be exploited provided specific requirements are met. An attacker may be able to use it to upload malicious files and take control of the target server's remote code execution (RCE). By taking advantage of this vulnerability, a threat actor could alter private files, steal information, interfere with essential services, or move laterally across the network.

This may result in the following: disruption of vital services; lateral movement inside compromised networks; manipulation or theft of sensitive data; and unauthorized access to web servers.

Struts versions 2.0.0 through 2.3.37 (end of life), 2.5.0 through 2.5.32, and 6.0.0 through 6.3.0 are impacted by the RCE vulnerability.

A technical write-up for CVE-2023-50164 was released on December 10 by a security researcher. It described how a threat actor may taint file upload parameters during an attack. On December 11, the publication of a second write-up included attack code for the vulnerability.

7. Cisco Possibly Impacted

Cisco stated in a security alert yesterday that it is looking into CVE-2023-50164 to find out which of its products that use Apache Struts might be impacted and how much.

The Customer Collaboration Platform, Identity Services Engine (ISE), Nexus Dashboard Fabric Controller (NDFC), Unified Communications Manager (Unified CM), Unified Contact Center Enterprise (Unified CCE), and Prime Infrastructure are among the Cisco products that are being examined.

Cisco's security bulletin contains a comprehensive list of potentially affected products; this list is subject to periodic updates with new information.

REFERENCE LINKS

- https://thehackernews.com/2023/11/kinsing-hackers-exploit-apache-activemq.html
- https://thehackernews.com/2023/11/darkgate-and-pikabot-malware-resurrect.html
- https://apnews.com/article/kansas-courts-cyberattack-hack-network-offline-097a11cfa9de552ec5a9ea49b500d3d6
- https://www.malwarebytes.com/blog/news/2023/11/windows-hello-fingerprint-authentication-can-be-bypassed-on-popular-laptops
- https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-for-investigating-attacks-using-cve-2023-23397/
- https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a?&web_view=true
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
- https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/
- https://www.malwarebytes.com/blog/news/2023/11/scattered-spider-ransomware-gang-falls-under-government-agency-scrutiny
- https://securityboulevard.com/2023/11/the-new-apt-group-darkcasino-and-the-global-surge-in-winrar-0-day-exploits/?web_view=true
- https://thehackernews.com/2023/11/experts-uncover-darkcasino-new-emerging.html
- https://thehackernews.com/2023/11/google-warns-of-hackers-absing-calendar.html?&web_view=true
- https://www.bleepingcomputer.com/news/security/delta-dental-of-california-data-breach-exposed-info-of-7-million-people/?&web_view=true
- https://www.helpnetsecurity.com/2023/12/12/messaging-platforms-security-risks/?&web_view=true
- https://www.infosecurity-magazine.com/news/vulnerabilities-initial-access/?&web_view=true
- https://www.bleepingcomputer.com/news/security/ten-new-android-banking-trojans-targeted-985-bank-apps-in-2023/?&web_view=true
- https://www.bleepingcomputer.com/news/security/black-basta-ransomware-made-over-100-million-from-extortion/?&web_view=true

About SDG

SDG is a global cybersecurity, identity governance, GRC, risk consulting and advisory firm. SDG's SaaS platform TruOps in combination with its services deliver a comprehensive range of identity, cybersecurity, risk, compliance, and cloud security solutions that enable organizations to identify and mitigate cyber risk, protect cyber assets, and manage their business securely.

To learn how SDG can help ensure the security and compliance of your technology and data infrastructure visit **www.sdgc.com** and **www.truops.com**.

SDG

75 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com