

Tema: Resolver los retos tipo (Machines/Sherlocks) asignados dentro de la plataforma web HackTheBox. Elaborar un informe técnico detallado que documente el desarrollo completo de las soluciones implementadas para cada reto. Incluir en el informe una lista y descripción de las aplicaciones software utilizadas en la resolución de cada uno de los CTFs.

Descripción: Completar los ejercicios asignados durante las clases (Sherlocks ElectricBreeze-1). Entregar un archivo en formato .pdf a través del Entorno Virtual de Aprendizaje (EVA), a menos que se indique lo contrario.

Practica:

1. ¿Desde cuándo ha estado activo Volt Typhoon?

Esta respuesta lo saque de la información del grupo G1017 en MITRE ATT&CK. Volt Typhoon ha sido identificado operando desde al menos 2021, enfocado en objetivos estratégicos como telecomunicaciones y transporte. Fuentes:

<https://attack.mitre.org/groups/G1017>



Task 1

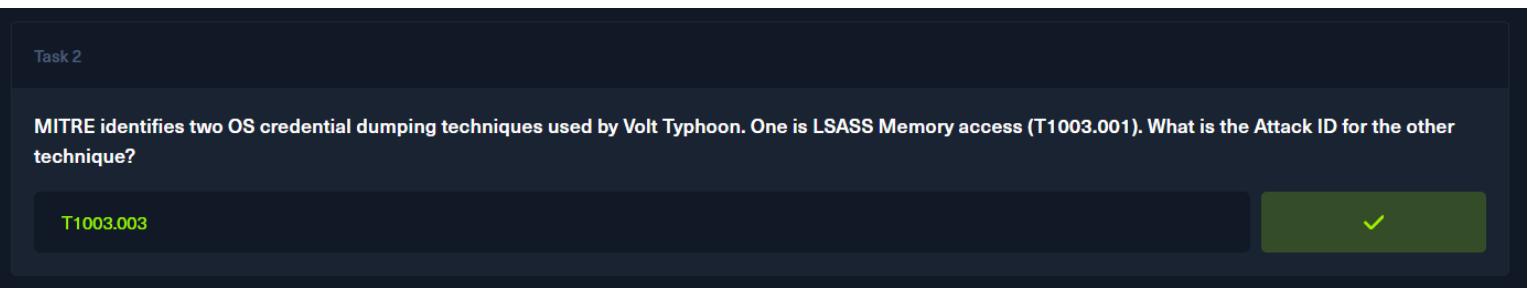
Based on MITRE's sources, since when has Volt Typhoon been active?

2021 ✓

2. MITRE identifica dos técnicas de volcado de credenciales del sistema operativo utilizadas por Volt Typhoon. Una es el acceso a memoria LSASS (T1003.001). ¿Cuál es el ID de ataque de la otra técnica?

La segunda pregunta la resolví leyendo las técnicas de Volt Typhoon, Esto aparece listado en su perfil técnico en ATT&CK. Fuentes:

<https://attack.mitre.org/techniques/T1003/003>



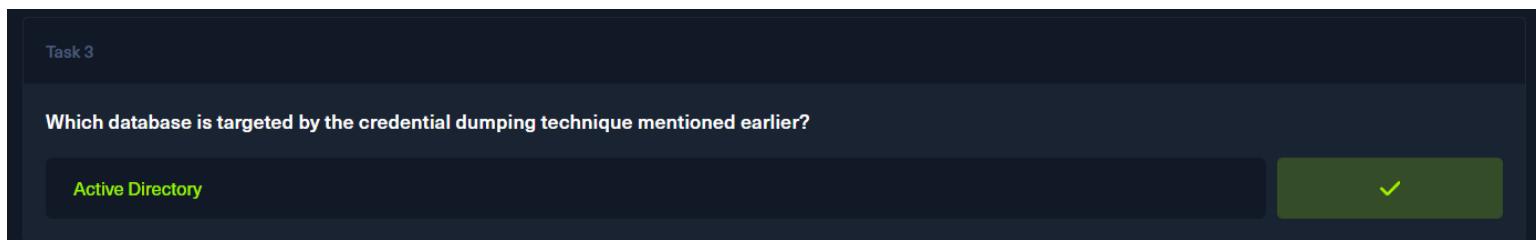
Task 2

MITRE identifies two OS credential dumping techniques used by Volt Typhoon. One is LSASS Memory access (T1003.001). What is the Attack ID for the other technique?

T1003.003 ✓

3. ¿Qué base de datos es el objetivo de la técnica de volcado de credenciales mencionada anteriormente?

La respuesta la encontré revisando donde encontré la anterior respuesta y salía muy claro la respuesta. Fuentes: <https://attack.mitre.org/techniques/T1003/003>



Task 3

Which database is targeted by the credential dumping technique mentioned earlier?

Active Directory ✓

4. ¿Qué subárbol de registro necesita el actor de amenazas para descifrar la base de datos objetivo?

La respuesta la encontré con investigación y encontré que para descifrar la base de datos Active Directory se encuentra en el hive SYSTEM del registro. Fuentes:

<https://attack.mitre.org/techniques/T1003/003>

Task 4

Which registry hive is required by the threat actor to decrypt the targeted database?

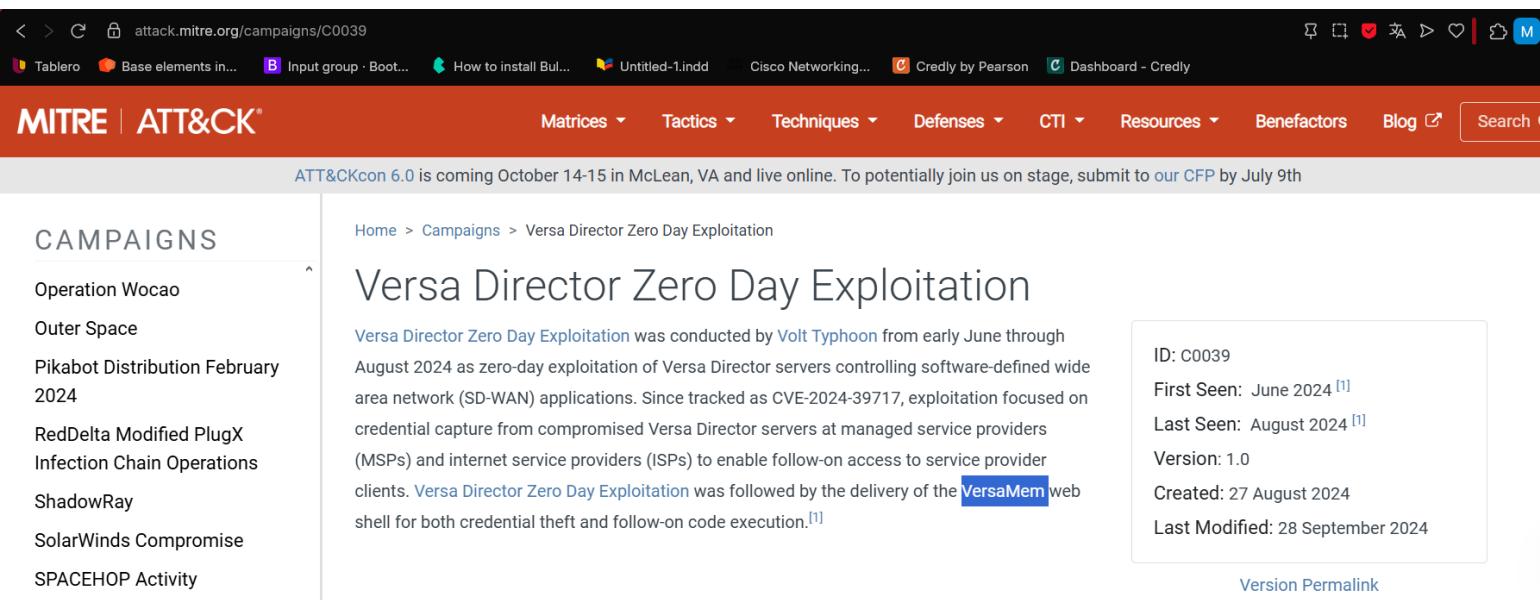
SYSTEM



5. Durante la campaña de junio de 2024, se observó que un adversario utilizaba una explotación de día cero dirigida a Versa Director. ¿Cuál es el nombre del software o malware utilizado?

Para contestar esta pregunta solo me bastó leer y la respuesta esta muy clara en la página.

Fuentes: <https://attack.mitre.org/campaigns/C0039>



The screenshot shows the MITRE ATT&CK website. At the top, there's a navigation bar with various links like 'Tablero', 'Base elements in...', 'Input group · Boot...', 'How to install Bul...', 'Untitled-1.indd', 'Cisco Networking...', 'Credly by Pearson', and 'Dashboard - Credly'. Below the navigation is the 'MITRE | ATT&CK' logo. A red banner at the top says 'ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. To potentially join us on stage, submit to our CFP by July 9th'. On the left, there's a sidebar titled 'Campañas' with a list of campaigns: Operation Wocao, Outer Space, Pikabot Distribution February 2024, RedDelta Modified PlugX, Infection Chain Operations, ShadowRay, SolarWinds Compromise, and SPACEHOP Activity. The main content area shows the details for 'Versa Director Zero Day Exploitation'. It includes a brief description: 'Versa Director Zero Day Exploitation was conducted by Volt Typhoon from early June through August 2024 as zero-day exploitation of Versa Director servers controlling software-defined wide area network (SD-WAN) applications. Since tracked as CVE-2024-39717, exploitation focused on credential capture from compromised Versa Director servers at managed service providers (MSPs) and internet service providers (ISPs) to enable follow-on access to service provider clients.' Below this is a box with metadata: ID: C0039, First Seen: June 2024 [1], Last Seen: August 2024 [1], Version: 1.0, Created: 27 August 2024, and Last Modified: 28 September 2024. At the bottom right of the main content area is a link 'Version Permalink'.

Task 5

During the June 2024 campaign, an adversary was observed using a Zero-Day Exploitation targeting Versa Director. What is the name of the Software/Malware that was used?

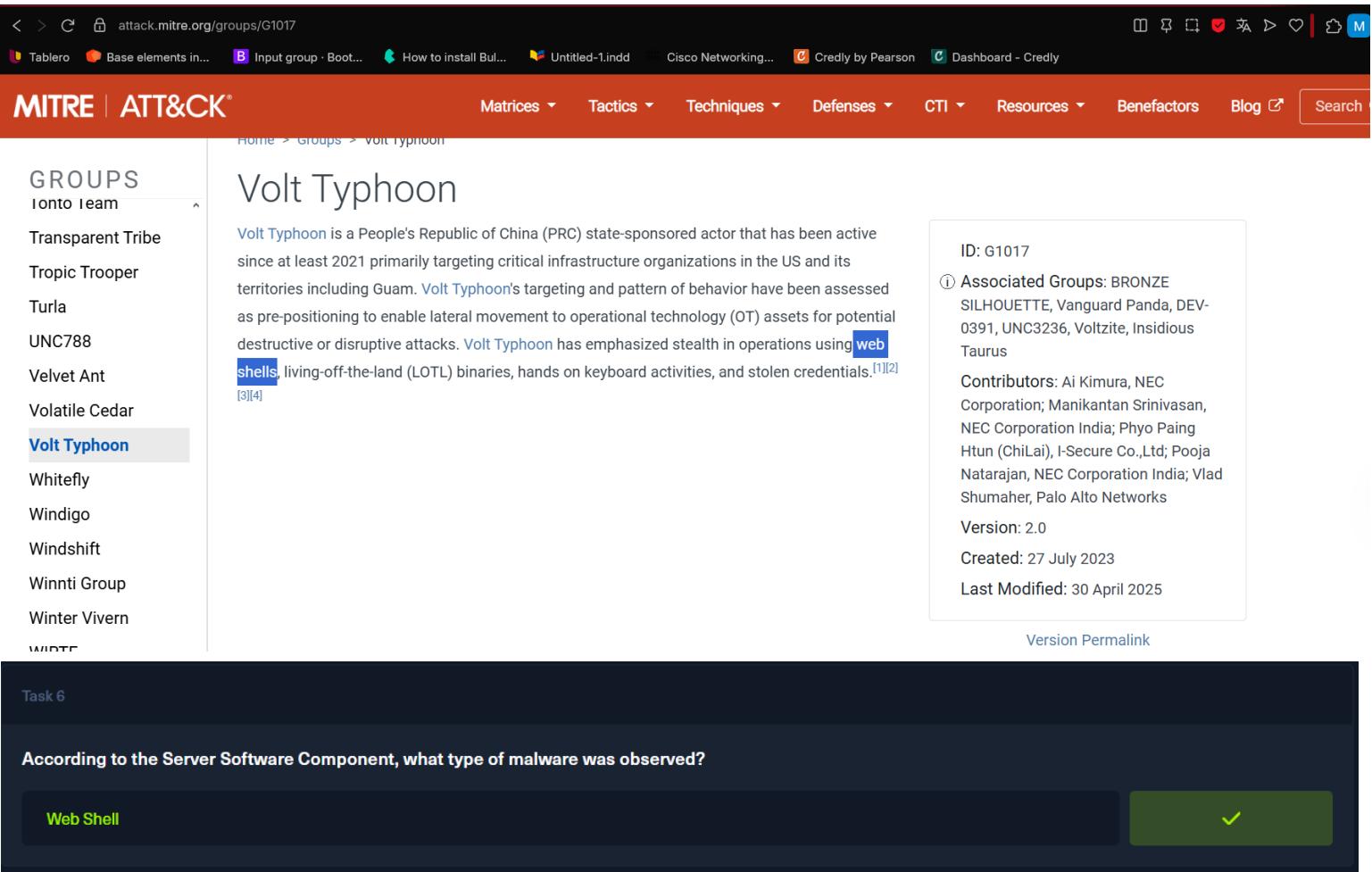
VersaMem



6. Según el componente de software del servidor, ¿qué tipo de malware se observó?

La respuesta también estuvo clara solo es de leer y nos damos cuenta del nombre.

<https://attack.mitre.org/groups/G1017>



The screenshot shows the MITRE ATT&CK Groups page for the group "Volt Typhoon". The left sidebar lists various groups, with "Volt Typhoon" highlighted. The main content area displays detailed information about Volt Typhoon, including its description as a state-sponsored actor from the PRC targeting critical infrastructure in the US and its territories, its use of web shells, and its contributors. A sidebar on the right provides a summary of the group's details. At the bottom, there is a task section asking about the observed malware type, with "Web Shell" selected as the answer.

Volt Typhoon

Description: Volt Typhoon is a People's Republic of China (PRC) state-sponsored actor that has been active since at least 2021 primarily targeting critical infrastructure organizations in the US and its territories including Guam. Volt Typhoon's targeting and pattern of behavior have been assessed as pre-positioning to enable lateral movement to operational technology (OT) assets for potential destructive or disruptive attacks. Volt Typhoon has emphasized stealth in operations using **web shells**, living-off-the-land (LOTL) binaries, hands on keyboard activities, and stolen credentials.^{[1][2]} [3][4]

Associated Groups: BRONZE SILHOUETTE, Vanguard Panda, DEV-0391, UNC3236, Voltzite, Insidious Taurus

Contributors: Ai Kimura, NEC Corporation; Manikantan Srinivasan, NEC Corporation India; Phylo Paing Htun (ChiLai), I-Secure Co.,Ltd; Pooja Natarajan, NEC Corporation India; Vlad Shumaher, Palo Alto Networks

Version: 2.0
Created: 27 July 2023
Last Modified: 30 April 2025

[Version Permalink](#)

Task 6

According to the Server Software Component, what type of malware was observed?

Web Shell ✓

7. ¿Dónde capturó el almacén de malware las credenciales?

La respuesta se presenta en la siguiente fuente, se encuentra de manera clara. Fuentes:

<https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation>

The VersaMem web shell is a sophisticated Java web shell that was uploaded to VirusShare on June 7, 2024, with the filename "VersaTest.png" and currently has zero anti-virus (AV) detections. Analysis of the web shell, which the threat actors aptly named "Director_tomcat_memShell" and Black Lotus Labs has dubbed VersaMem, identified it as a JAR archive bundled through Apache Maven on June 3, 2024.

The VersaMem shell, both in name ("Director_tomcat_memShell") and in functionality, is custom-tailored to interact with Versa Directors. On execution, the web shell attaches to the primary Apache Tomcat (Java servlet and web server) process and takes advantage of the Java Instrumentation API and Javassist (Java bytecode manipulation toolkit) to dynamically modify Java code in-memory. It serves two primary functions:

1. Capture plaintext user credentials

a. Hooks and overrides Versa's built-in authentication method "setUserPassword" to intercept plaintext credentials in-line, AES encrypt and Base64 encode those credentials, then write them to disk at "/tmp/.temp.data."

Categories

- Adaptive Networking
- Connected Security
- Hybrid Cloud
- Communications and Collaboration
- Edge Computing
- SASE

Task 7

Where did the malware store captured credentials?



8. Según la referencia de MITRE, un artículo de Lumen/Black Lotus Labs (Taking The Crossroads: The Versa Director Zero-Day Exploitaiton), ¿cuál era el nombre del archivo de la primera versión de malware escaneada en VirusTotal?

La respuesta la encontré leyendo y encontré que es una técnica muy utilizada de los actores de amenazas: disfrazar malware bajo extensiones de archivos inocentes, su formato es .png. Fuentes: <https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation>

LUMEN®

Technologies ▾ Customer Stories Insights ▾ Industries ▾ About Lumen ▾



software services.” SD-WAN is a software-defined approach to networking that aims to simplify IT infrastructure control and management by delivering a virtual WAN architecture. In essence, Versa Director servers are the centralized management for client SD-WAN network infrastructure and are predominately intended for ISP and MSP operations. This makes Versa Director a lucrative target for advanced persistent threat (APT) actors who would want to view or control network infrastructure at scale, or pivot into additional (or downstream) networks of interest.

The VersaMem web shell is a sophisticated JAR web shell that was uploaded to VirusTotal on June 7, 2024, with the filename “[VersaTest.png](#)” and currently has zero anti-virus (AV) detections. Analysis of the web shell, which the threat actors aptly named “Director_tomcat_memShell” and Black Lotus Labs has dubbed VersaMem, identified it as a JAR archive bundled through Apache Maven on June 3, 2024.

The VersaMem shell, both in name (“Director_tomcat_memShell”) and in functionality, is custom-tailored to interact with Versa Directors. On execution, the web shell attaches to the primary Apache Tomcat (Java servlet and web server) process and takes advantage of the Java Instrumentation API and Javassist (Java bytecode manipulation toolkit) to dynamically modify Java code in-memory. It serves two primary functions:

Categories

- Adaptive Networking
- Connected Security
- Hybrid Cloud
- Communications and Collaboration
- Edge Computing
- SASE

Task 8

According to MITRE's reference, a Lumen/Black Lotus Labs article(Taking The Crossroads: The Versa Director Zero-Day Exploitaiton.), what was the filename of the first malware version scanned on VirusTotal?



9. ¿Cuál es el hash SHA256 del archivo?

La respuesta se la encuentra muy rápida en la misma pagina donde saque las respuestas anteriormente. Fuentes:<https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation>



LUMEN®

Technologies Customer Stories Insights Industries About Lumen Q

Categories

Adaptive Networking
Connected Security
Hybrid Cloud
Communications and Collaboration
Edge Computing
SASE

No security vendors and no sandboxes flagged this file as malicious

4bc6dac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37
VersaTest.png
jar sets-process-name detect-debug-environment checks-cpu-name

Figure 2: Screenshot from VirusTotal for VersaTest.png (SHA256: 4bc6dac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37) showing 0 detections.

Task 9

What is the SHA256 hash of the file?

4bc6dac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37



10. Según VirusTotal, ¿cuál es el tipo de archivo del malware?

La respuesta la encontré leyendo en la misma pagina donde saque las respuestas anteriormente. Fuentes: <https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation>

LUMEN®

Tecnologías Historias de clientes Perspectivas Industrias Sobre Lumen Q

Categorías

Redes adaptativas
Seguridad conectada
Nube híbrida
Comunicaciones y Colaboración
Computación perimetral
SASE

arquitectura WAN virtual. En esencia, los servidores Versa Director son la administración centralizada de la infraestructura de red SD-WAN del cliente y están destinados predominantemente a operaciones ISP y MSP. Esto convierte a Versa Director en un objetivo lucrativo para actores avanzados de amenazas persistentes (APT) que querían ver o controlar la infraestructura de red a escala, o girar hacia redes de interés adicionales (o posteriores).

El shell web VersaMem es un sofisticado shell web JAR que se subió a VirusTotal el 7 de junio de 2024 con el nombre de archivo "VersaTest.png" y actualmente no tiene detecciones de antivirus (AV). El análisis del shell web, que los actores de amenazas acertadamente llamaron "Director_tomcat_memShell" y Black Lotus Labs denominó VersaMem, lo identificó como un archivo JAR incluido a través de Apache Maven el 3 de junio de 2024.

Task 10

According to VirusTotal, what is the file type of the malware?

JAR



11. ¿Cuál es el valor 'Creado por' en el Manifiesto del archivo según VirusTotal?

Lo encontré leyendo el mismo documento y buscando la versión que fue utilizado.

Fuentes: <https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation>

Task 11

What is the 'Created by' value in the file's Manifest according to VirusTotal?

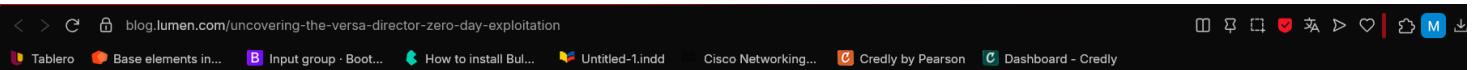
Apache Maven 3.6.0



12. ¿Cuál es el identificador CVE asociado con este malware y vulnerabilidad?

Lo encontré en la misma pagina donde encontré las demás preguntas, solo es de leer.

Fuentes: <https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation>



LUMEN®

Tecnologías ▾

Historias de clientes

Perspectivas ▾

Industrias ▾

Sobre Lumen ▾



Resumen Ejecutivo

El equipo de Black Lotus Labs en Lumen Technologies descubrió la explotación activa de una vulnerabilidad de día cero en los servidores de Versa Director, identificado como **CVE-2024-39717** y públicamente anunciado en Agosto 22, 2024. Esta vulnerabilidad se encuentra en las aplicaciones de red de área amplia (SD-WAN) definidas por software de Versa y afecta a todas las versiones de Versa Director anteriores a la 22.1.4. Director Versa los servidores administran las configuraciones de red para los clientes que ejecutan el software SD-WAN y, a menudo, son utilizados por proveedores de servicios de Internet (ISP) y proveedores de servicios administrados (MSP). Los servidores Director permiten la orquestación de la funcionalidad SD-WAN de Versa, posicionándolos como un objetivo crítico y atractivo para los actores de amenazas que buscan ampliar su alcance dentro de la gestión de redes empresariales.

Redes adaptativas

Seguridad conectada

Nube híbrida

Comunicaciones y Colaboración

Computación perimetral

SASE

Task 12

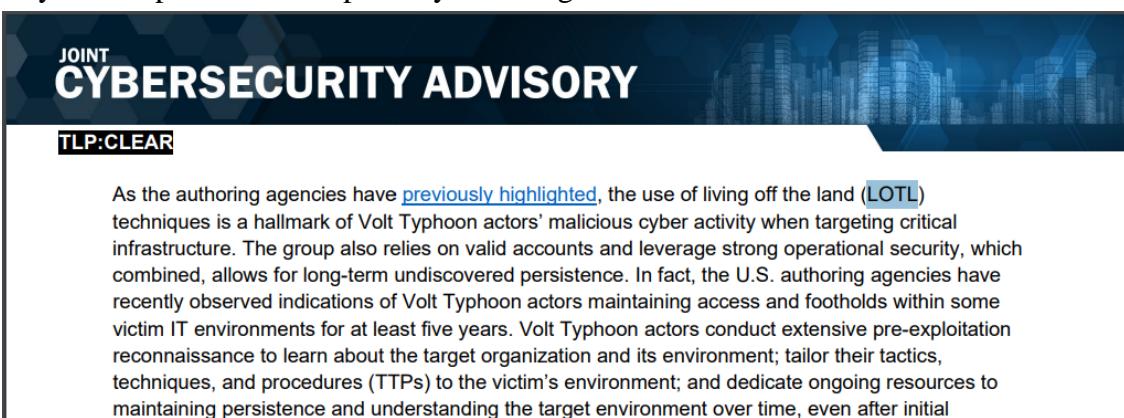
What is the CVE identifier associated with this malware and vulnerability?

CVE-2024-39717



13. Según el documento CISA (https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf) al que hace referencia MITRE, ¿cuál es la estrategia principal que utiliza Volt Typhoon para evadir la defensa?

Leyendo el pdf salió la respuesta y fue la siguiente:



JOINT CYBERSECURITY ADVISORY

TLP:CLEAR

As the authoring agencies have [previously highlighted](#), the use of living off the land (LOTL) techniques is a hallmark of Volt Typhoon actors' malicious cyber activity when targeting critical infrastructure. The group also relies on valid accounts and leverage strong operational security, which combined, allows for long-term undiscovered persistence. In fact, the U.S. authoring agencies have recently observed indications of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years. Volt Typhoon actors conduct extensive pre-exploitation reconnaissance to learn about the target organization and its environment; tailor their tactics, techniques, and procedures (TTPs) to the victim's environment; and dedicate ongoing resources to maintaining persistence and understanding the target environment over time, even after initial

Task 13

According to the CISA document(https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf) referenced by MITRE, what is the primary strategy Volt Typhoon uses for defense evasion?

LOTL



14. En el documento CISA, ¿qué nombre de archivo está asociado con el comando potencialmente utilizado para analizar patrones de inicio de sesión por Volt Typhoon?

CYBERSECURITY ADVISORY

TLP:CLEAR

Volt Typhoon uses at least the following LOTL tools and commands for system information, network service, group, and user discovery techniques:

- cmd
- certutil
- dnscmd
- ldfde
- makecab
- net user/group/use
- netsh
- nltest
- netstat
- ntdsutil
- ping
- PowerShell
- quser
- reg query/reg save
- systeminfo
- tasklist
- wevtutil
- whoami
- wmic
- xcopy

Some observed specific examples of discovery include:

- Capturing successful logon events [\[T1654\]](#).
 - Specifically, in one incident, analysis of the PowerShell console history of a domain controller indicated that security event logs were directed to a file named `user.dat`, as evidenced by the executed command `Get-EventLog security -InstanceId 4624 -after [year-month-date] | fl * | Out-File 'C:\users\public\documents\user.dat'`. This indicates the group's specific interest in capturing successful logon events (event ID 4624) to analyze user authentication patterns

Task 14

In the CISA document, which file name is associated with the command potentially used to analyze logon patterns by Volt Typhoon?

C:\users\public\documents\user.dat



Recursos Bibliográficos:

<https://labs.hackthebox.com/achievement/sherlock/2394798/881>