Hack the Box — Sherlock ElectricBreeze-1

Sherlock ElectricBreeze-1

- **Perfil**: Blue Team - Cyber Threat Intelligence
- **Sección**: Threat Intelligence
- **Dificultad**: Muy fácil

En este laboratorio vamos a estar resolviendo un ejercicio correspondiente a la plataforma especializada en ejercicios de ciberseguridad y hacking, Hack the Box, dentro del apartado de sus sherlocks, que son labs de blue team.

Para este ejercicio utilizaremos la herramienta de **MITRE ATT&CK** para la inteligencia de amenazas.

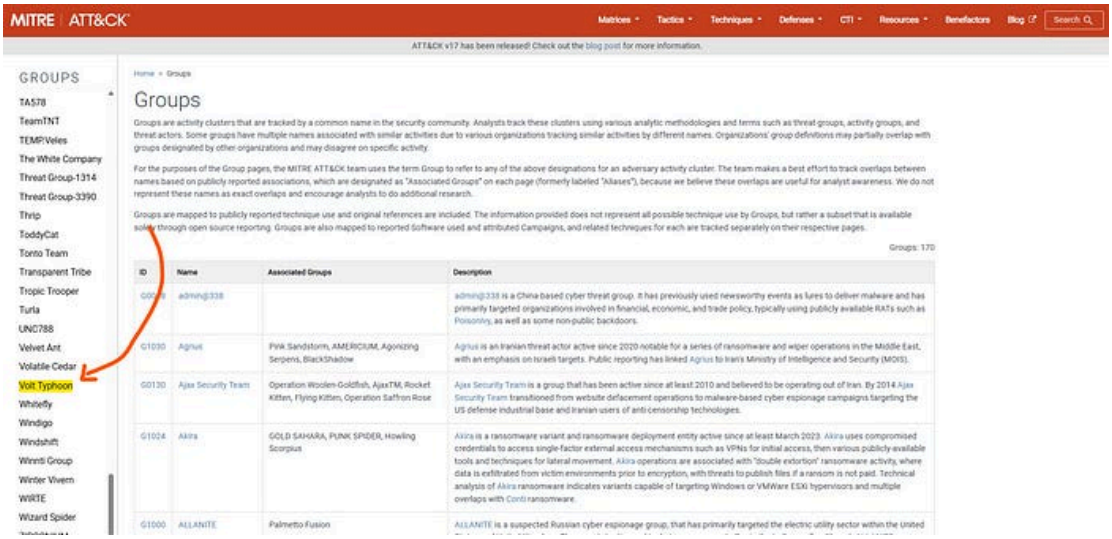
Enunciado: *"Su equipo de seguridad debe estar siempre al día y ser consciente de las amenazas que se ciernen sobre las organizaciones de su sector. Al comenzar su andadura como becario de Inteligencia de Amenazas, equipado con cierta experiencia en SOC, su jefe le ha asignado una tarea para poner a prueba sus habilidades de investigación y la eficacia con la que puede aprovechar el marco ATT&CK de MITRE. Llevar a cabo una investigación exhaustiva sobre Volt Typhoon. Utilice el marco ATT&CK de MITRE para convertir el comportamiento y las tácticas del adversario en información práctica. Impresione a su jefe con su evaluación, demostrando su pasión por la inteligencia de amenazas".*

ELECTRICBREEZE-1—SOLUCIÓN

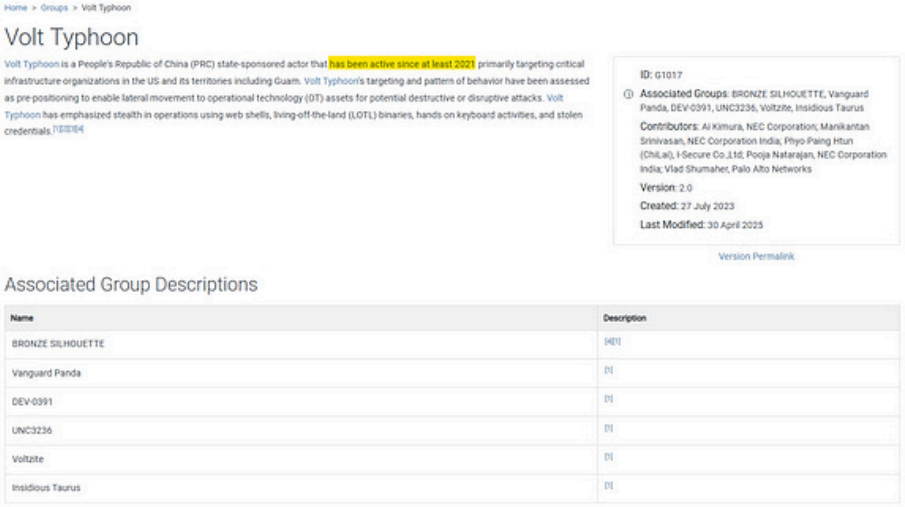
Task 1:

> Based on MITRE's sources, since when has Volt Typhoon been active?
>
> ***2021***

Lo primero que haremos será ingresar a la plataforma de MITRE ATT&CK para poner analizar a este grupo cibercriminal.



Vamos a hacer clic en el grupo, donde hallaremos la información solicitada.



Vemos que este grupo patrocinado por China ha estado activado desde, al menos, **2021**, atentando contra infraestructuras críticas de Estados Unidos y otros territorios.

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***

Vamos a movernos ahora hacia las técnicas utilizadas por estos atacantes, concretamente a las de dumping de credenciales.

Enterprise	T1571		Non-Standard Port	KV Botnet Activity generates a random port number greater than 30,000 to serve as the listener for subsequent command and control activity.[3]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Volt Typhoon has used the Ultimate Packer for Executables (UPX) to obfuscate the FRP client files BrightmetricAgent.exe and SMSvcService.ex) and the port scanning utility ScanLine.[1]
Enterprise	T1588	.002	Obtain Capabilities: Tool	Volt Typhoon has used legitimate network and forensic tools and customized versions of open-source tools for C2.[2][1]
		.006	Obtain Capabilities: Vulnerabilities	Volt Typhoon has used publicly available exploit code for initial access.[1]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	Volt Typhoon has attempted to access hashed credentials from the LSASS process memory space.[2][1]
		.003	OS Credential Dumping: NTDS	Volt Typhoon has used ntds.util to create domain controller installation media containing usernames and password hashes.[2][3][4][1]
Enterprise	T1120		Peripheral Device Discovery	Volt Typhoon has obtained victim's screen dimension and display device information.[1]
Enterprise	T1069		Permission Groups Discovery	Volt Typhoon has used commercial tools, LOTL utilities, and appliances already present on the system for group and user discovery.[1]
		.001	Local Groups	Volt Typhoon has run `net localgroup administrators` in compromised environments to enumerate accounts.[3]
		.002	Domain Groups	Volt Typhoon has run `net group` in compromised environments to discover domain groups.[4]

Mientras una de las técnicas está relacionada a acceder a credenciales hasheadas en el espacio de memoria LSASS, la otra es sobre el robo de credenciales desde NTDS, una herramienta de línea de comandos de Windows Server utilizada principalmente para administrar Active Directory (AD), la cual tiene la ID **T1003.003**.

Task 3:

> Which database is targeted by the credential dumping technique mentioned earlier?
>
> ***Active Directory***

Se nos pregunta a qué base de datos se apunta para el dumpeo de credenciales que se mencionó en la pregunta anterior.

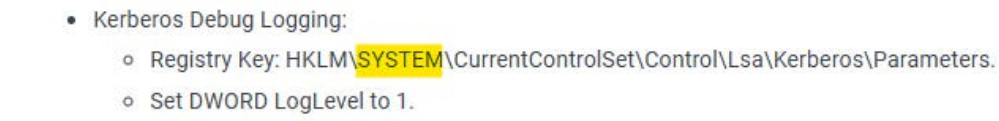
Como dijimos antes, al aprovecharse de la herramienta ntds.util, está apuntando a **Active Directory**.

Task 4:

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

Esta pregunta está relacionada con qué clave de registro es requerida por el actor malicioso para descifrar Active Directory.

Vamos a movernos hacia la sección de directorio activo para observar la clave de registro completa.

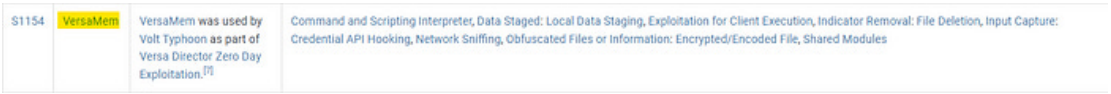

- Kerberos Debug Logging:
  - Registry Key: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters.
  - Set DWORD LogLevel to 1.

La ruta del registro HKLM**SYSTEM**\CurrentControlSet\Control\Lsa\Kerberos\Parameters pertenece a la rama HKEY_LOCAL_MACHINE\SYSTEM, la cual contiene configuraciones esenciales del sistema operativo en ejecución. Esta estructura es fundamental para el arranque y funcionamiento de Windows. En particular, la subclave Kerberos\Parameters permite ajustar el comportamiento del protocolo Kerberos, responsable de la autenticación en entornos de Active Directory.

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***

Para responder esto, podemos dirigirnos a la sección de software utilizados por los ciberdelincuentes.



S1154	VersaMem	VersaMem was used by Volt Typhoon as part of Versa Director Zero Day Exploitation.[7]	Command and Scripting Interpreter, Data Staged: Local Data Staging, Exploitation for Client Execution, Indicator Removal: File Deletion, Input Capture: Credential API Hooking, Network Sniffing, Obfuscated Files or Information: Encrypted/Encoded File, Shared Modules

Como se nos menciona allí, **VersaMem** fue utilizado como parte de una explotación de día cero contra Versa Director.

Task 6:

> According to the Server Software Component, what type of malware was observed?
>
> ***Web Shell***

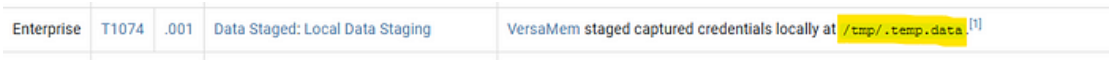
Server Software Component, al abusarse, permite generar persistencia en el acceso a sistemas. Se puede aprovechar de varios modos, mediante SQL o DLL, pero tener una reverse shell, concretamente una **web shell** para crear un backdoor, se ha vuelto popular.

Task 7:

> Where did the malware store captured credentials?
>
> ***/tmp/.temp.data***

El malware de este grupo (VersaMem) guardó las credenciales capturadas en algún sitio del sistema.

La respuesta la encontraremos dentro de las técnicas utilizadas por este software malicioso.



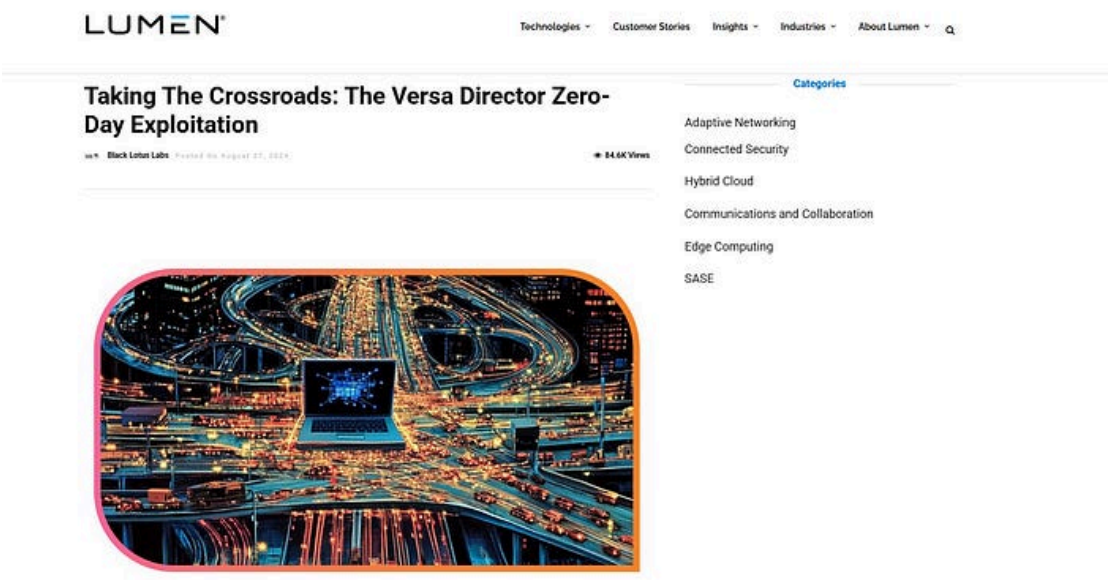
Como se observa, el virus almacenó las credenciales capturadas localmente en **/tmp/.temp.data**.

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?
>
> ***VersaTest.png***

Este artículo nos habla sobre el nombre de la primera versión de este malware cuando se escaneó en VirusTotal.

Dicho texto lo encontraremos como una referencia dentro del apartado de VersaMem.



Bajando un poco, en la sección del análisis del malware, encontraremos la respuesta.

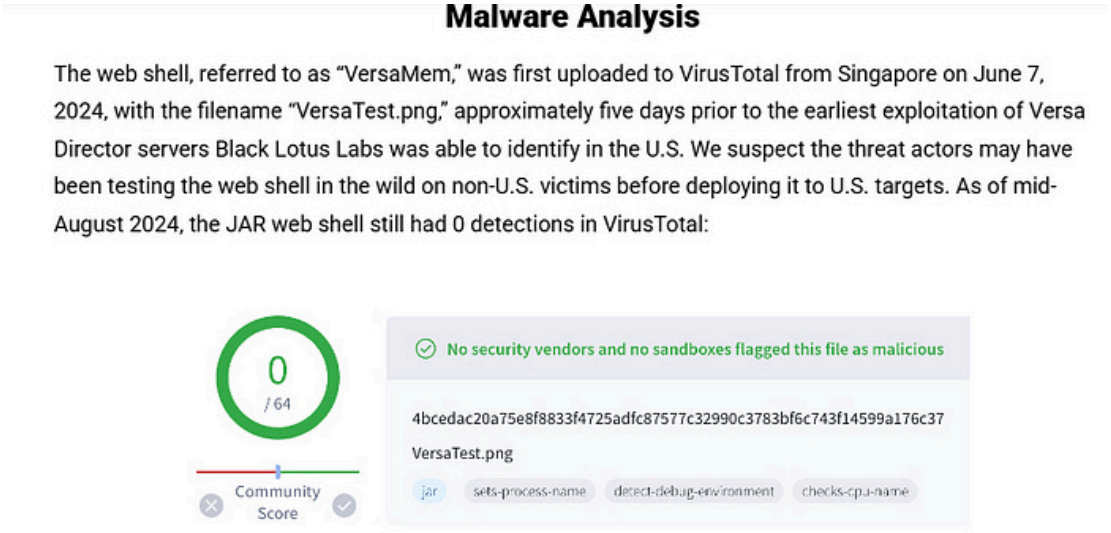


Figure 2: Screenshot from VirusTotal for VersaTest.png (SHA256: 4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37) showing 0 detections.

Como vemos, **VersaTest.png**, fue el primer nombre, y como dato curioso, lo detectaba como legítimo.

Task 9:

> What is the SHA256 hash of the file?
>
> ***4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37***

Malware Analysis

The web shell, referred to as "VersaMem," was first uploaded to VirusTotal from Singapore on June 7, 2024, with the filename "VersaTest.png," approximately five days prior to the earliest exploitation of Versa Director servers Black Lotus Labs was able to identify in the U.S. We suspect the threat actors may have been testing the web shell in the wild on non-U.S. victims before deploying it to U.S. targets. As of mid-August 2024, the JAR web shell still had 0 detections in VirusTotal:

Figure 2: Screenshot from VirusTotal for VersaTest.png (SHA256: 4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37) showing 0 detections.

Task 10:

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

Malware Analysis

The web shell, referred to as "VersaMem," was first uploaded to VirusTotal from Singapore on June 7, 2024, with the filename "VersaTest.png," approximately five days prior to the earliest exploitation of Versa Director servers Black Lotus Labs was able to identify in the U.S. We suspect the threat actors may have been testing the web shell in the wild on non-U.S. victims before deploying it to U.S. targets. As of mid-August 2024, the JAR web shell still had 0 detections in VirusTotal:

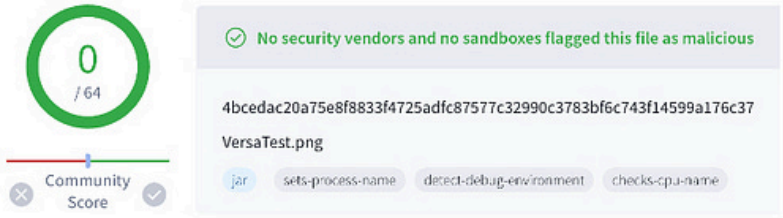


Figure 2: Screenshot from VirusTotal for VersaTest.png (SHA256: 4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37) showing 0 detections.

Task 11:

> What is the 'Created by' value in the file's Manifest according to VirusTotal?
>
> ***Apache Maven 3.6.0***

Si bajamos un poco en el análisis, vamos a encontrar el manifiesto dentro de la información del JAR.

The manifest file contents (MANIFEST.MF) identify the entry point for the main class as com.versa.vnms.ui.TestMain:

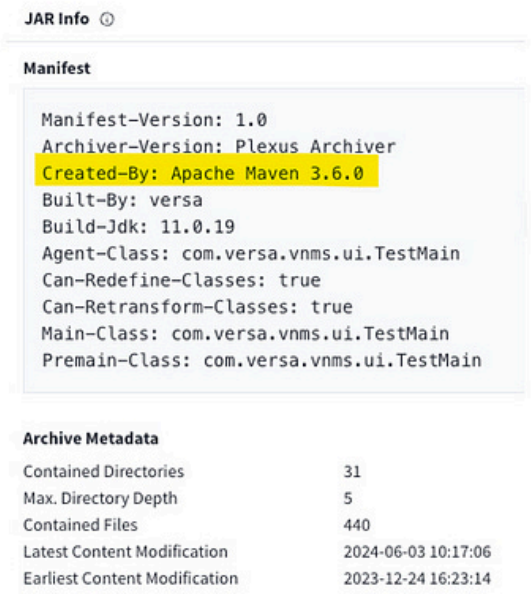


Figure 6: Screenshot from VirusTotal showing the manifest version, JDK version, built-by, agent-class, main-class and pre-main class manifest variables.

Task 12:

> What is the CVE identifier associated with this malware and vulnerability?
>
> ***CVE-2024–39717***

Dentro del resumen, al comienzo del artículo, encontraremos el identificador de CVE.

Executive Summary

The Black Lotus Labs team at Lumen Technologies discovered active exploitation of a zero-day vulnerability in Versa Director servers, identified as CVE-2024-39717 and publicly announced on August 22, 2024. This vulnerability is found in Versa software-defined wide area network (SD-WAN) applications and affects all Versa Director versions prior to 22.1.4. Versa Director servers manage the network configurations for clients running the SD-WAN software and are often used by internet service providers (ISPs) and managed service providers (MSPs). Director servers enable the orchestration of Versa's SD-WAN functionality, positioning them as a critical and attractive target for threat actors seeking to extend their reach within enterprise network management.

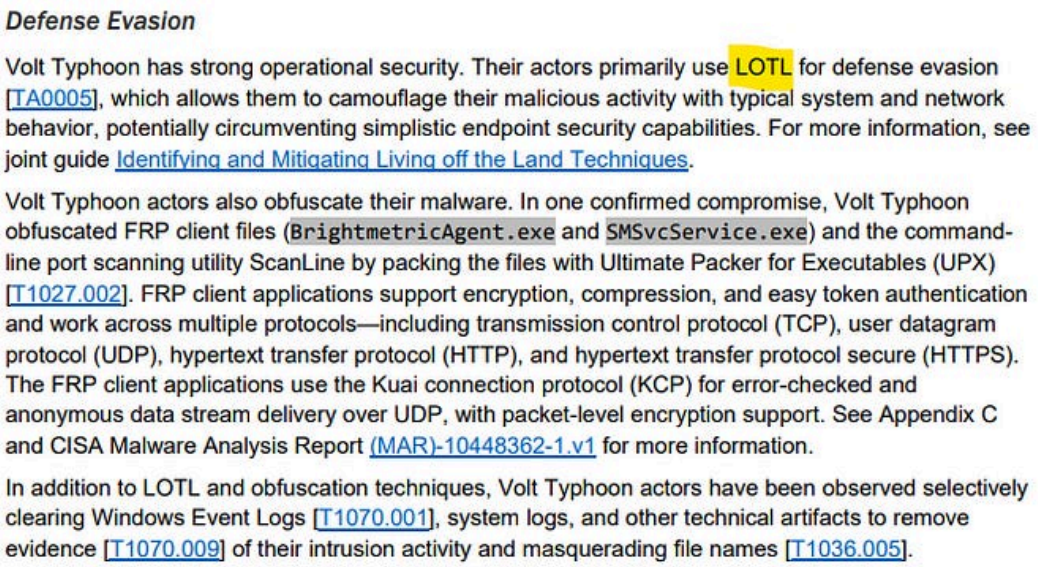
Task 13:

> According to the CISA document referenced by MITRE, what is the primary strategy Volt Typhoon uses for defense evasion?
>
> ***LOTL***

Este documento del CISA nos muestra un análisis detallado del grupo Volt Typhoon.

Debemos determinar la estrategia principal para evadir defensas perpetrada por los ciberdelincuentes chinos.

Para ahorrar tiempo, podemos visualizar el índice y dirigirnos hacia las técnicas de Defense Evasion.



Defense Evasion

Volt Typhoon has strong operational security. Their actors primarily use LOTL for defense evasion [TA0005], which allows them to camouflage their malicious activity with typical system and network behavior, potentially circumventing simplistic endpoint security capabilities. For more information, see joint guide Identifying and Mitigating Living off the Land Techniques.

Volt Typhoon actors also obfuscate their malware. In one confirmed compromise, Volt Typhoon obfuscated FRP client files (`BrightmetricAgent.exe` and `SMSvcService.exe`) and the command-line port scanning utility ScanLine by packing the files with Ultimate Packer for Executables (UPX) [T1027.002]. FRP client applications support encryption, compression, and easy token authentication and work across multiple protocols—including transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), and hypertext transfer protocol secure (HTTPS). The FRP client applications use the Kuai connection protocol (KCP) for error-checked and anonymous data stream delivery over UDP, with packet-level encryption support. See Appendix C and CISA Malware Analysis Report (MAR)-10448362-1.v1 for more information.

In addition to LOTL and obfuscation techniques, Volt Typhoon actors have been observed selectively clearing Windows Event Logs [T1070.001], system logs, and other technical artifacts to remove evidence [T1070.009] of their intrusion activity and masquerading file names [T1036.005].

LOTL se refiere a *Living Off The Land*, una técnica en la que los atacantes utilizan herramientas y funciones ya integradas en el sistema operativo o en el entorno objetivo (como Windows, Linux, o aplicaciones comunes) para llevar a cabo sus ataques, sin necesidad de cargar malware externo. Esto está directamente relacionado con el concepto de Fileless Malware.

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***

Vamos a irnos hacia los comandos utilizados para la actividad de LOTL.

APPENDIX A: VOLT TYPHOON OBSERVED COMMANDS / LOTL ACTIVITY

See Table 2 and Table 3 for Volt Typhoon commands and PowerShell scripts observed by the U.S. authoring agencies during incident response activities. For additional commands used by Volt Typhoon, see joint advisory People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.

Table 2: Volt Typhoon Observed Commands in PowerShell Console History

Command/Script	Description/Use
Get-EventLog security -instanceid 4624 -after {redacted date} | fl * | Out-File 'C:\users\public\documents\user.dat'	PowerShell command extracts security log entries with the Event ID `4624` after a specified date. The output is formatted (`fl *`) and saved to `user.dat`. Potentially used to analyze logon patterns and identify potential targets for lateral movement.

¡Ejercicio completado!