

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 a analizar a este grupo cibercriminal.

MITRE ATT&CK

ATT&CK v17 has been released! Check out the [blog post](#) for more information.

Home > Groups

Groups

Groups are activity clusters that are tracked by a common name in the security community. Analysts track these clusters using various analytic methodologies and terms such as threat groups, activity groups, and threat actors. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for an adversary activity cluster. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used and attributed Campaigns, and related techniques for each are tracked separately on their respective pages.

Groups: 170

ID	Name	Associated Groups	Description
G0001	admiral338		admiral338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as Possum, as well as some non-public backdoors.
G1030	Aghut	Pink Sandstorm, AMERCIUM, Agonizing Serpens, BlackShadow	Aghut is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East, with an emphasis on Israeli targets. Public reporting has linked Aghut to Iran's Ministry of Intelligence and Security (MOIS).
G0130	Apex Security Team	Operation Wooden Goldfish, AjaxTM, Rocket Kittens, Flying Kittens, Operation Saffron Rose	Apex Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014, Apex Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G1024	Akira	GOLD SAHARA, PUNK SPIDER, Howling Scorpions	Akira is a ransomware variant and ransomware deployment entity active since at least March 2023. Akira uses compromised credentials to access single-factor external access mechanisms such as VPNs for initial access, then various publicly available tools and techniques for lateral movement. Akira operations are associated with "double extortion" ransomware activity, where data is exfiltrated from victim environments prior to encryption, with threats to publish files if a ransom is not paid. Technical analysis of Akira ransomware indicates variants capable of targeting Windows or VMware ESXi hypervisors and multiple overlaps with Conti ransomware.
G1000	ALLANITE	Palmetto Fusion	ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States.

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

Home > Groups > Volt Typhoon

Volt Typhoon

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]}

ID: G1017

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

Contributors: Ai Kimura, NEC Corporation; Manikantan Srinivasan, NEC Corporation India; Piyu Piyu Hui (CHI), iSecure Co., Ltd; Pooja Natarajan, NEC Corporation India; Vlad Shumacher, Palo Alto Networks

Version: 2.0

Created: 27 July 2023

Last Modified: 30 April 2023

Version Permalink

Associated Group Descriptions

Name	Description
BRONZE SILHOUETTE	[1][2]
Vanguard Panda	[1]
DEV-0391	[1]
UNC3236	[1]
Voltzite	[1]
Insidious Taurus	[1]

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.exe 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][3]}
		.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][3]}
		.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]}
Enterprise	T1120	Peripheral Device Discovery	Volt Typhoon has obtained victim's screen dimension and display device information. ^[5]
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. ^[6]
		.001 Local Groups	Volt Typhoon has run <code>net localgroup administrators</code> in compromised environments to enumerate accounts. ^[5]
		.002 Domain Groups	Volt Typhoon has run <code>net group</code> in compromised environments to discover domain groups. ^[6]

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.

\$I154	VersaMem	VersaMem was used by Volt Typhoon as part of Versa Director Zero Day Exploitation. ^[9]	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.

Server Software Component: Web Shell

Other sub-techniques of Server Software Component (6) ▼

Adversaries may backdoor web servers with web shells to establish persistent access to systems. A Web shell is a Web script that is placed on an openly accessible Web server to allow an adversary to access the Web server as a gateway into a network. A Web shell may provide a set of functions to execute or a command-line interface on the system that hosts the Web server.^[1]

In addition to a server-side script, a Web shell may have a client interface program that is used to talk to the Web server (e.g. [China Chopper Web shell client](#)).^[2]

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.

Enterprise	T1074	.001	Data Staged: Local Data Staging	VersaMem staged captured credentials locally at /tmp/.temp.data . ^[1]
------------	-------	------	---------------------------------	---

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 Exploitation.), 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.

References

1. Black Lotus Labs. (2024, August 27). Taking The Crossroads: The Versa Director Zero-Day Exploitation. Retrieved August 27, 2024.

Taking The Crossroads: The Versa Director Zero-Day Exploitation

Black Lotus Labs · Posted on August 27, 2024

84.6K Views

Categories

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



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

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:

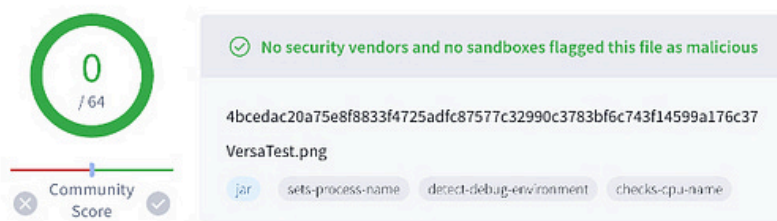


Figure 2: Screenshot from VirusTotal for **VersaTest.png** (SHA256: 4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37) showing 0 detections.

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:

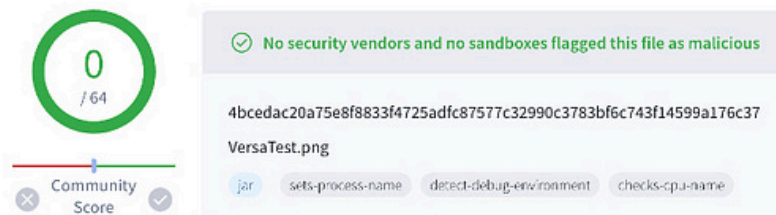


Figure 2: Screenshot from VirusTotal for VersaTest.png (SHA256:

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`:

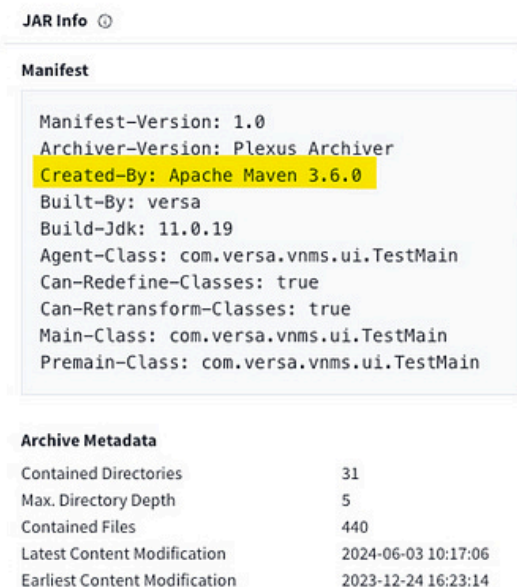


Figure 6: Screenshot from VirusTotal showing the manifest version, JDK version, built-by, agent-class, main-class and pre-main class manifest variables.

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
<code>Get-EventLog security -instanceid 4624 -after {redacted date} fl * Out-File 'C:\users\public\documents\user.dat'</code>	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!

