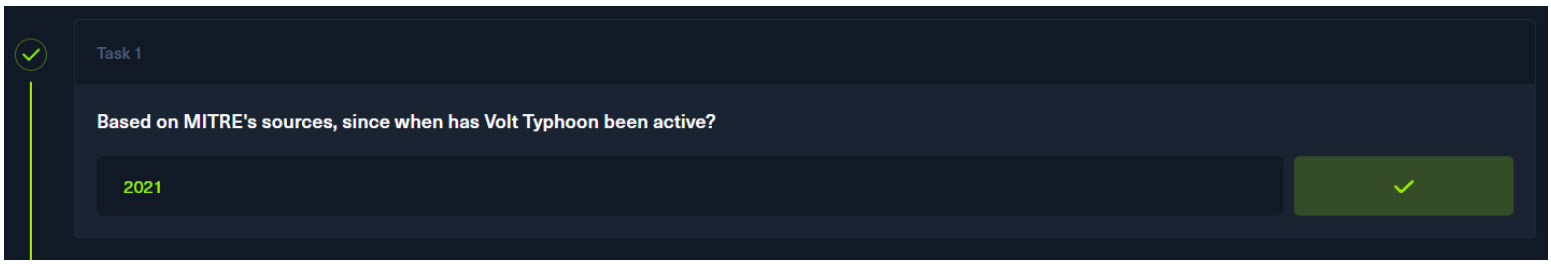
Tema: Resolver los retos tipo (Machines/Sherlocks) asignados dentro de la plataforma web HackTheBox. Elaborar un informe técnico detallado que documente el desarrolle completo de las soluciones implementadas para cada reto. Incluir en el informe una lista y descripción de las aplicaciones software utilizadas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

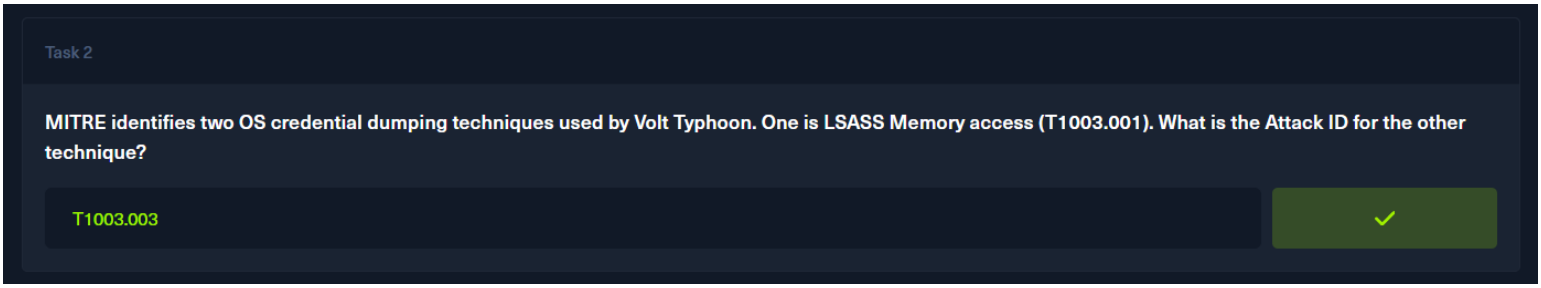
1. **¿Desde cuándo ha estado activo Volt Typhoon?**

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



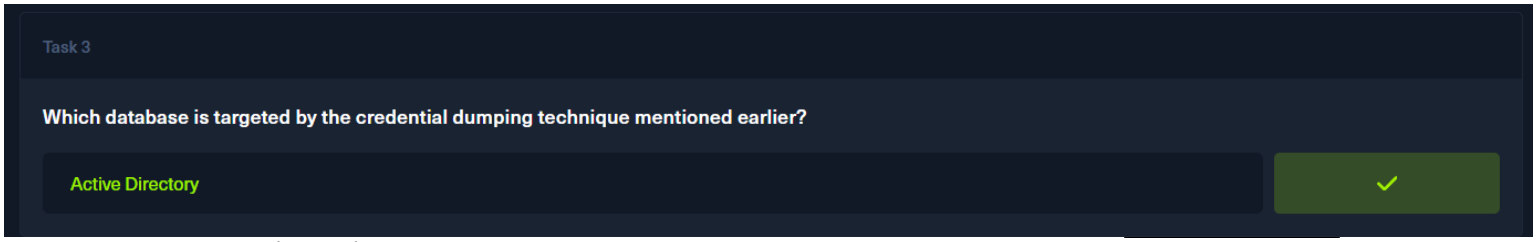
2. **MITRE identifica dos técnicas de volcado de credenciales del sistema operativo utilizadas por Volt Typhoon. Una es el acceso a memoria LSASS (T1003.001). ¿Cuál es el ID de ataque de la otra técnica?**

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



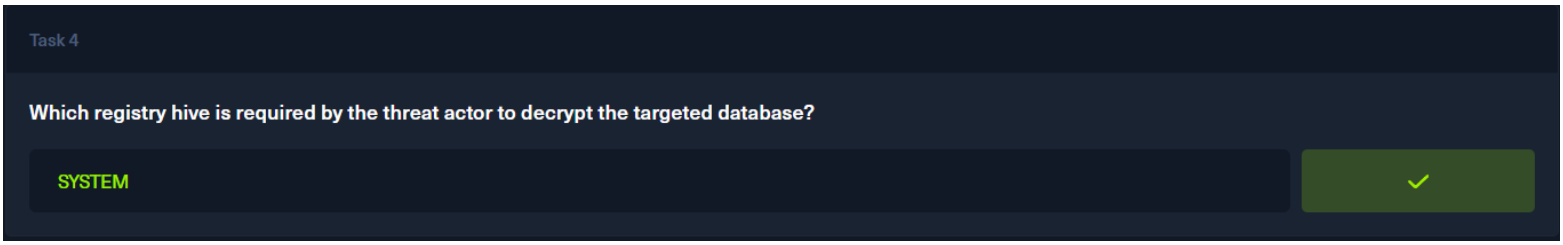
3. **¿Qué base de datos es el objetivo de la técnica de volcado de credenciales mencionada anteriormente?**

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



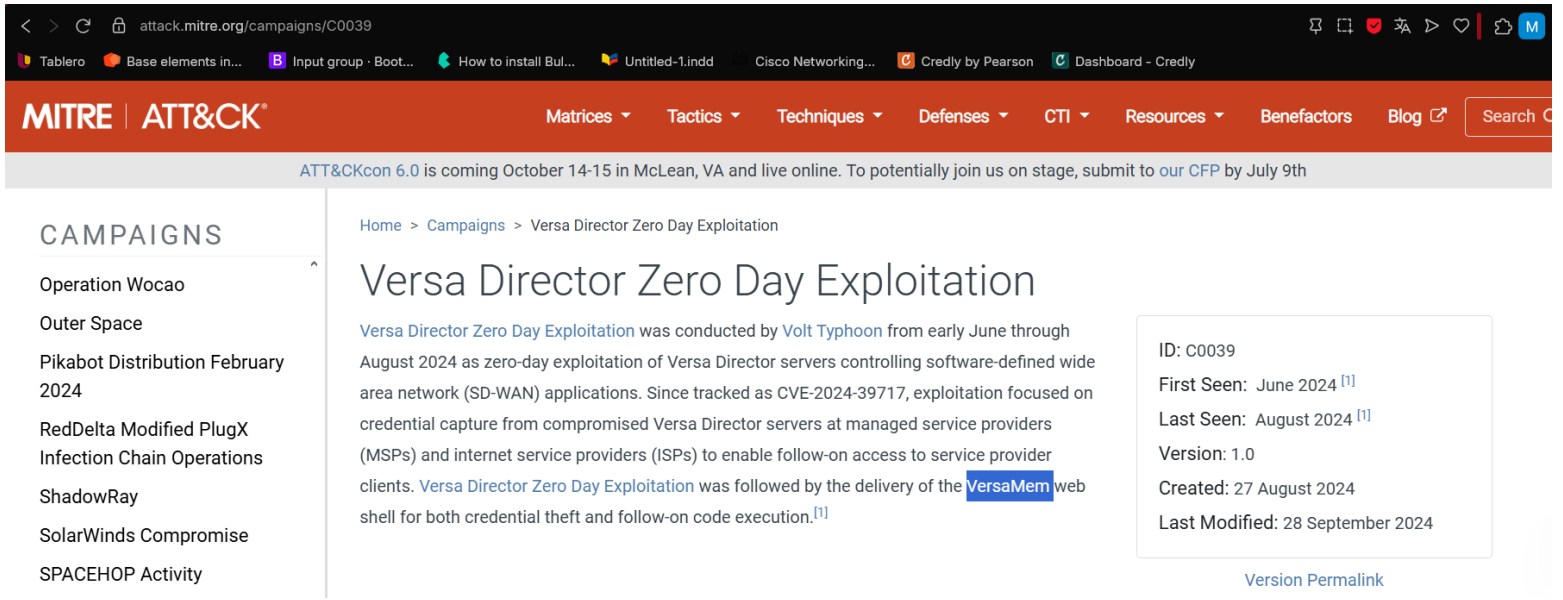
4. **¿Qué subárbol de registro necesita el actor de amenazas para descifrar la base de datos objetivo?**

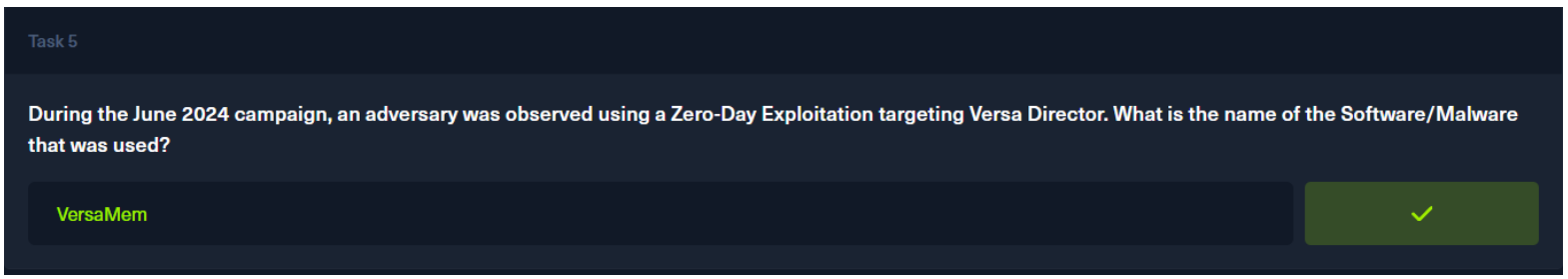
La respuesta la encontré con investigación y encontré que para descifrar la base de datos Active Directory se encuentra en el hive SYSTEM del registro. Fuentes: https://attack.mitre.org/techniques/T1003/003



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?**

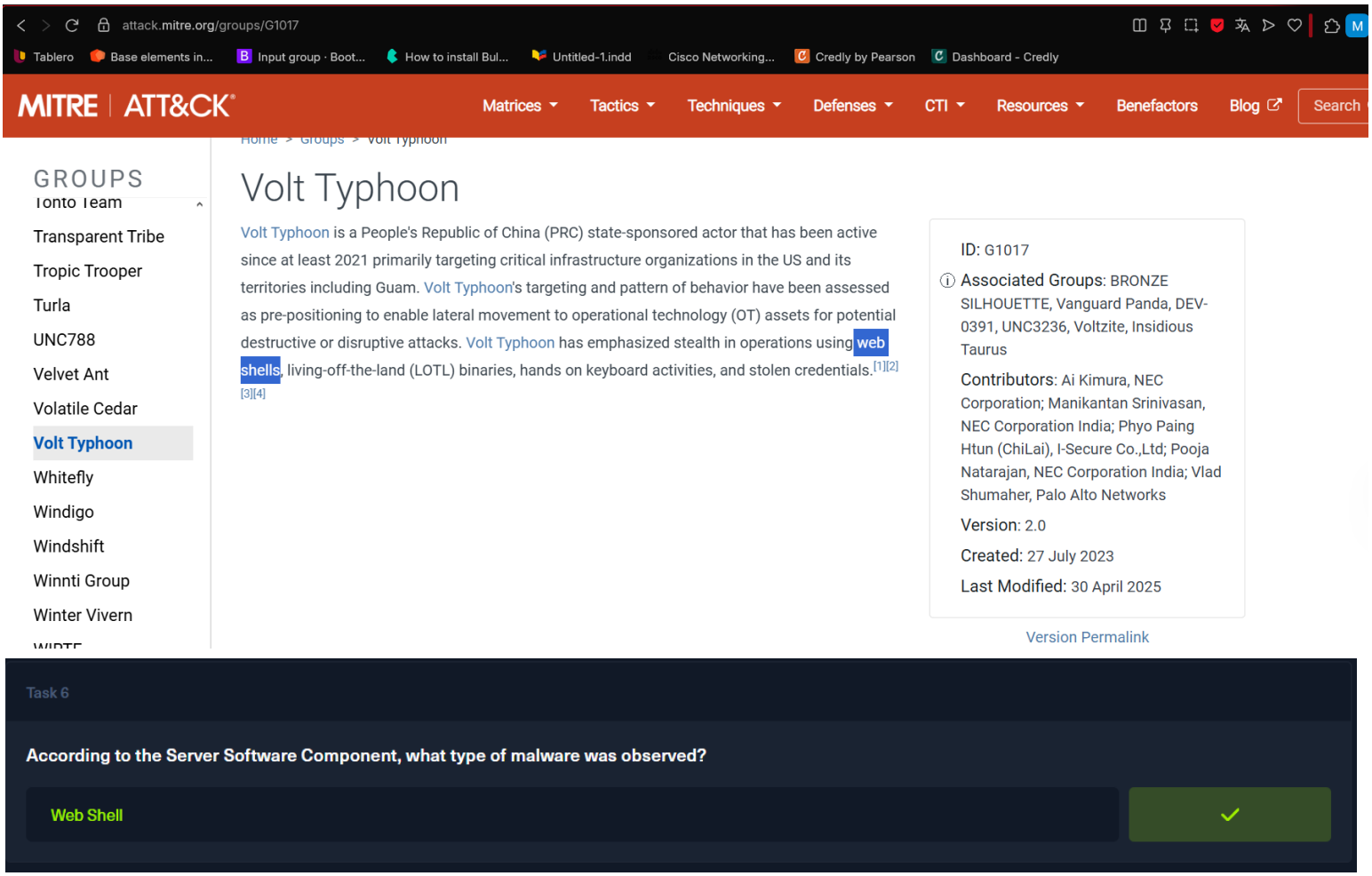
Para contestar esta pregunta solo me bastó leer y la repuesta esta muy clara en la página. Fuentes: https://attack.mitre.org/campaigns/C0039





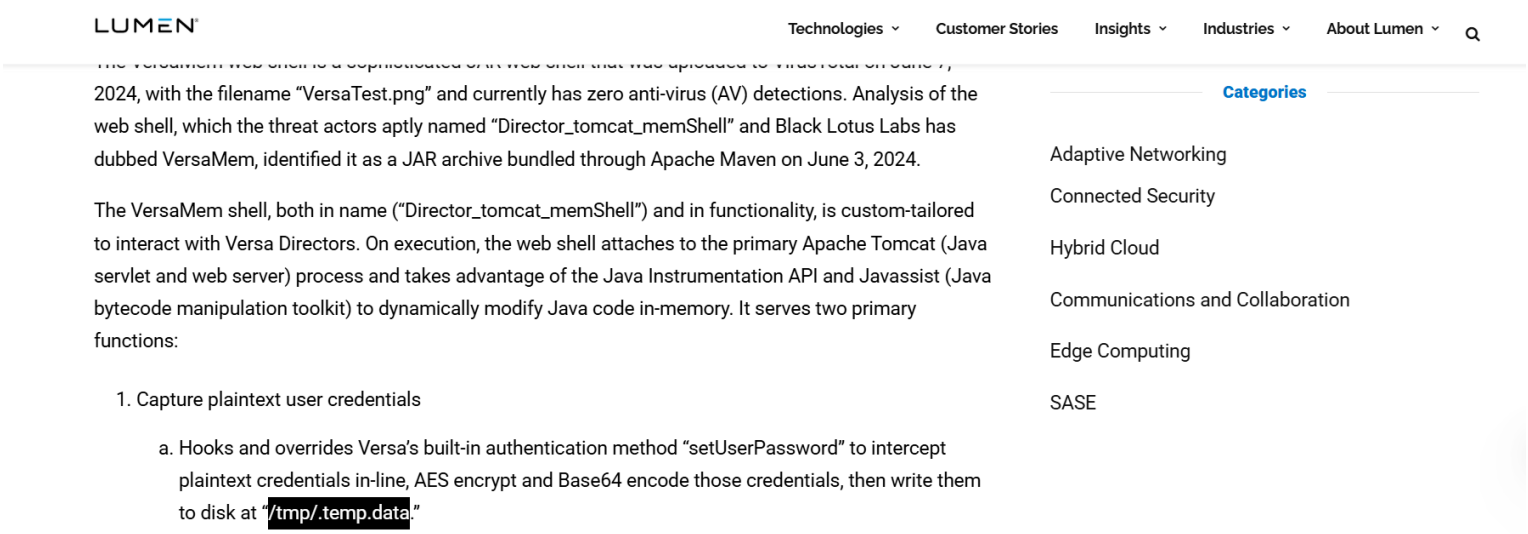
6. Según el componente de software del servidor, ¿qué tipo de malware se observó?

La respuesta también estuvo clara solo es de leer y nos damos cuenta del nombre.
https://attack.mitre.org/groups/G1017



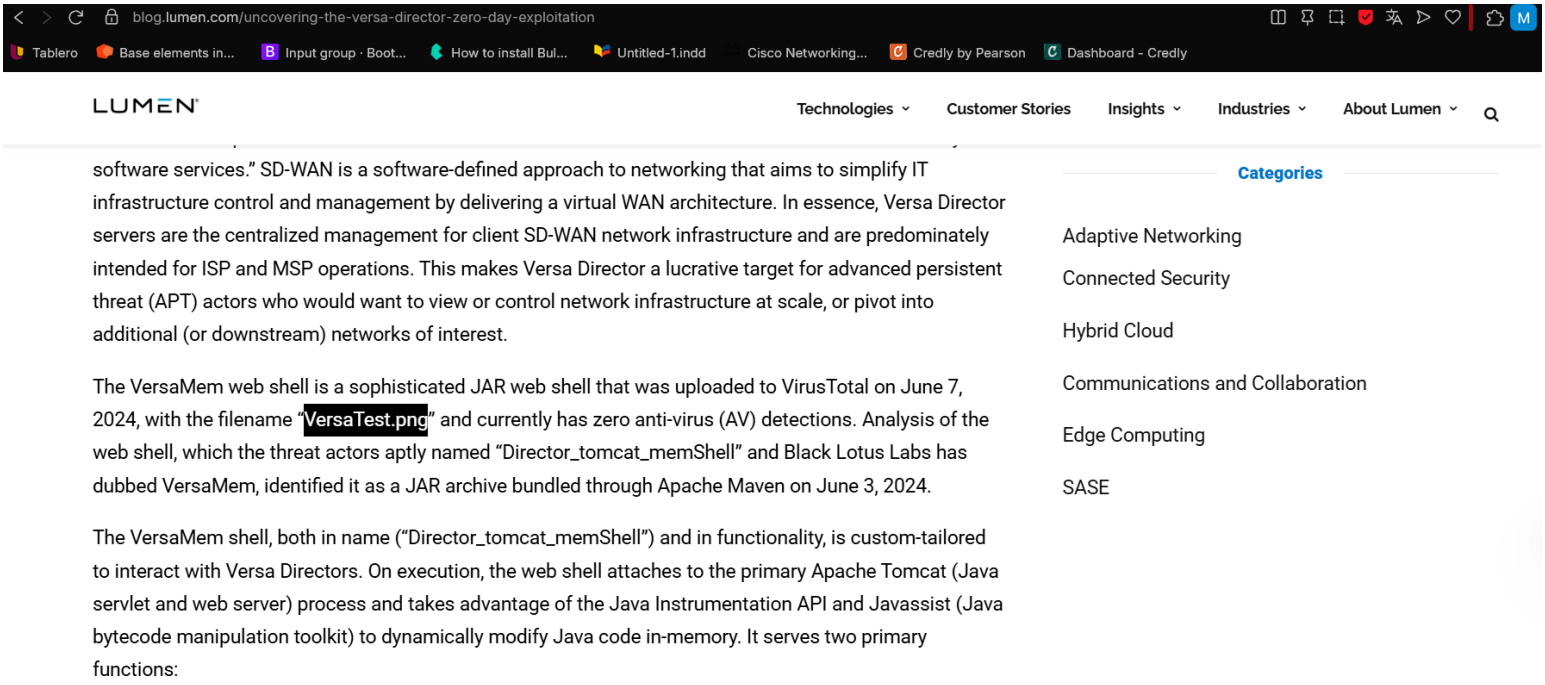
7. ¿Dónde capturó el almacén de malware las credenciales?

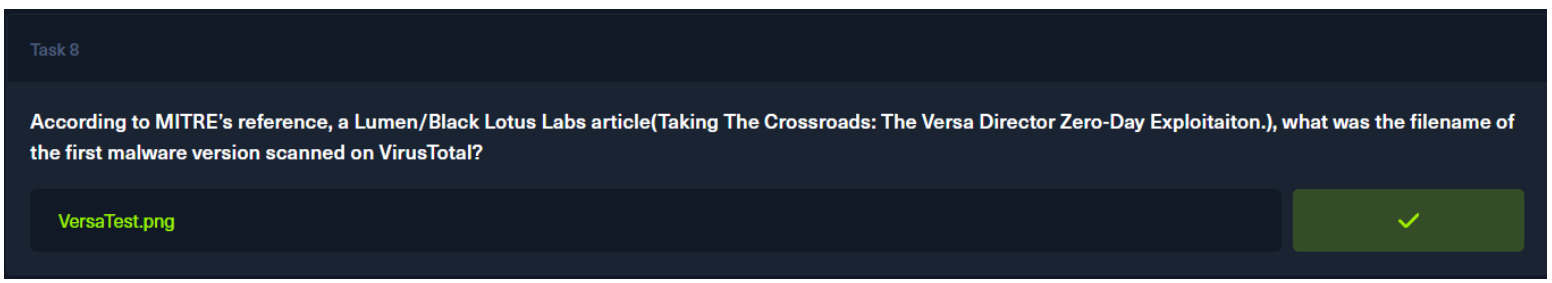
La respuesta se presenta en la siguiente fuente, se encuentra de manera clara. Fuentes:
https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation



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





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

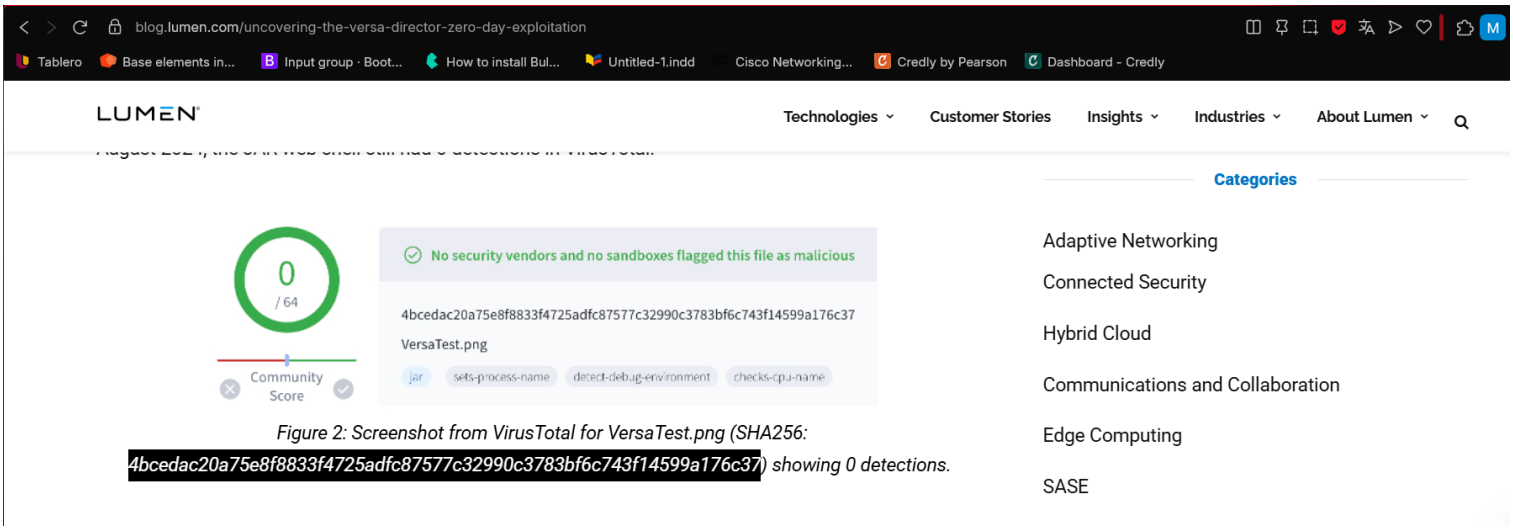
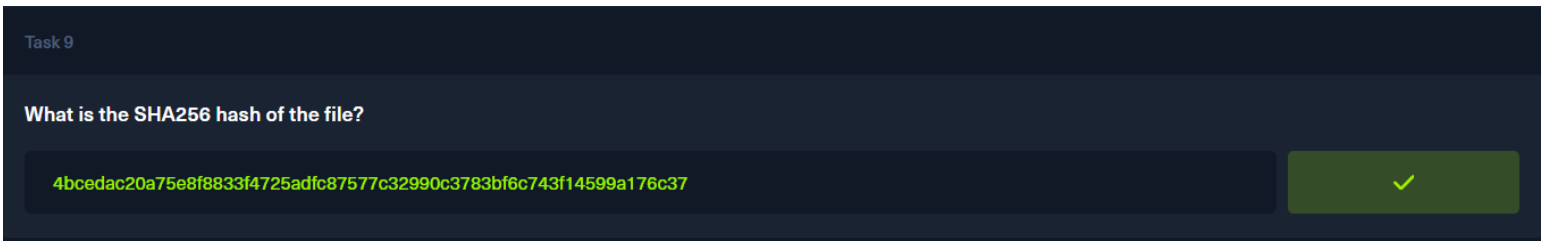


Figure 2: Screenshot from VirusTotal for VersaTest.png (SHA256: 4bcedac20a75e8f8833f4725adfc87577c32990c3783bf6c743f14599a176c37) showing 0 detections.

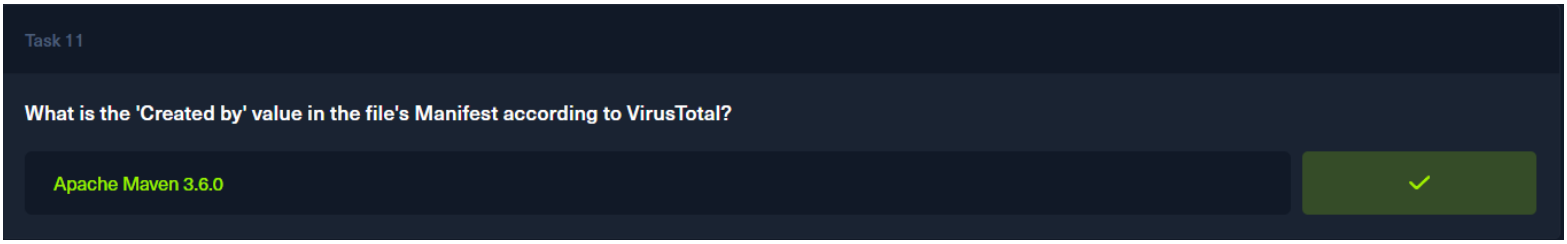


10. Según VirusTotal, ¿cuál es el tipo de archivo del malware?

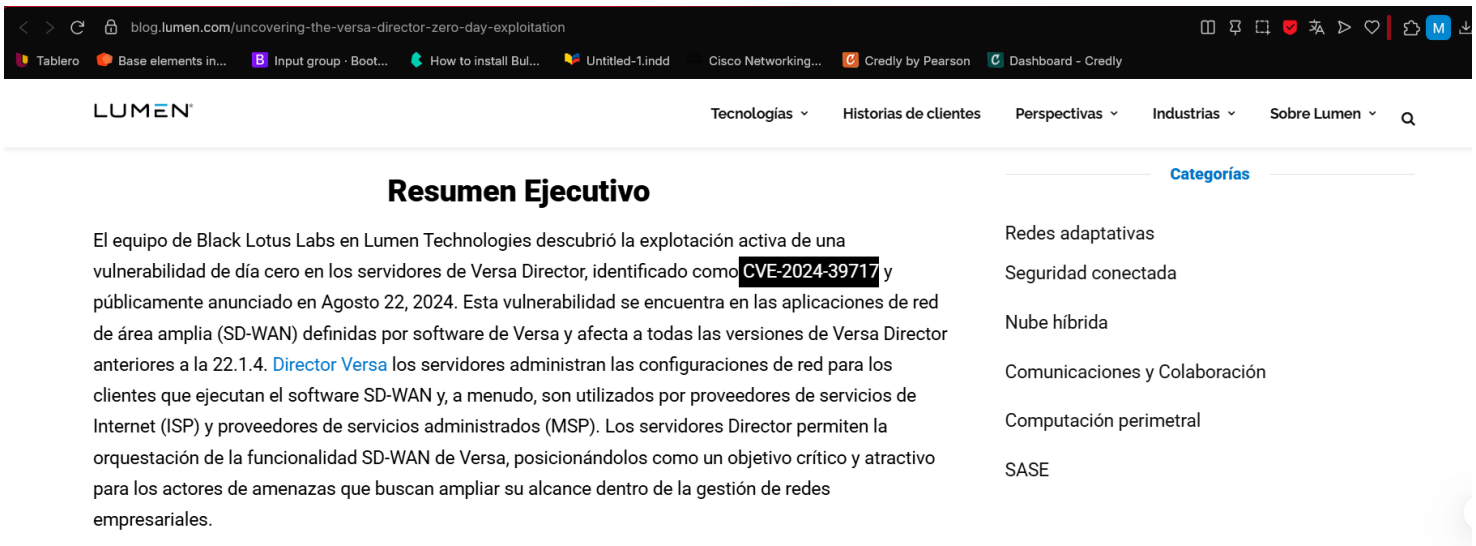
La respuesta la encontré leyendo en la misma pagina donde saque las respuestas anteriormente. Fuentes: https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation

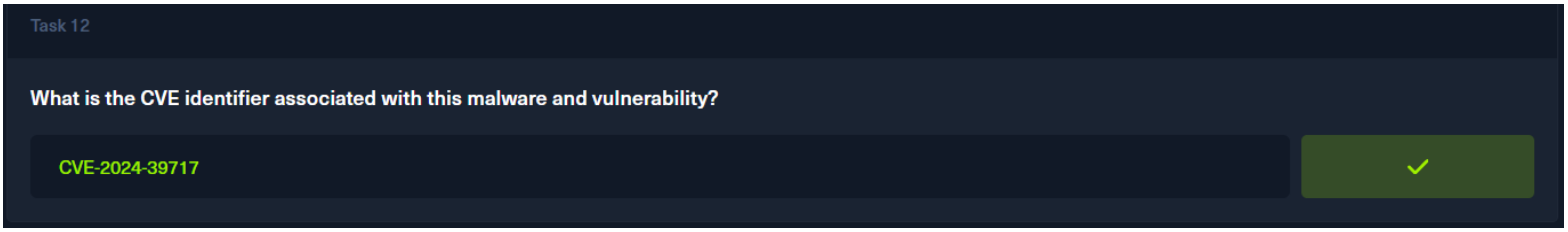
Mateo Castillo
Seguridad del Sistema de Información
Facultad de Ciencias Técnicas
Ingeniería en Tecnologías de la Información

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

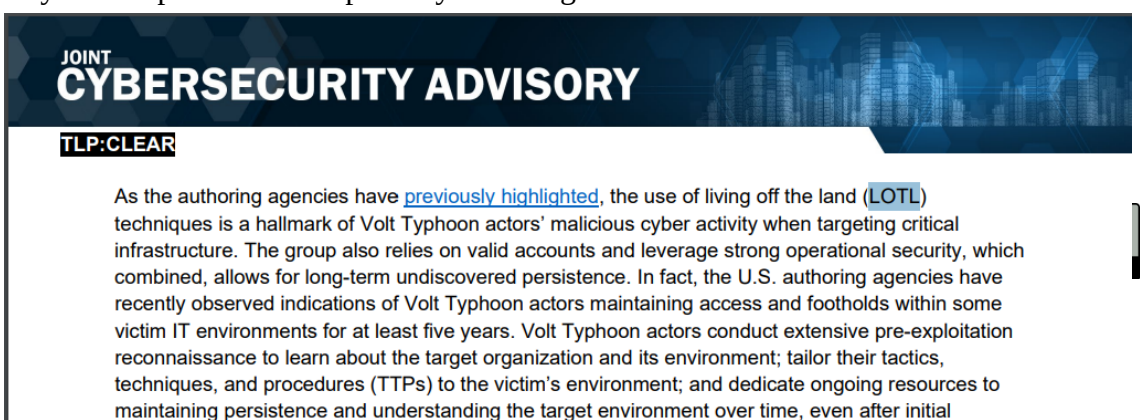


12. ¿Cuál es el identificador CVE asociado con este malware y vulnerabilidad?
Lo encontré en la misma pagina donde encontré las demás preguntas, solo es de leer.
Fuentes: https://blog.lumen.com/uncovering-the-versa-director-zero-day-exploitation

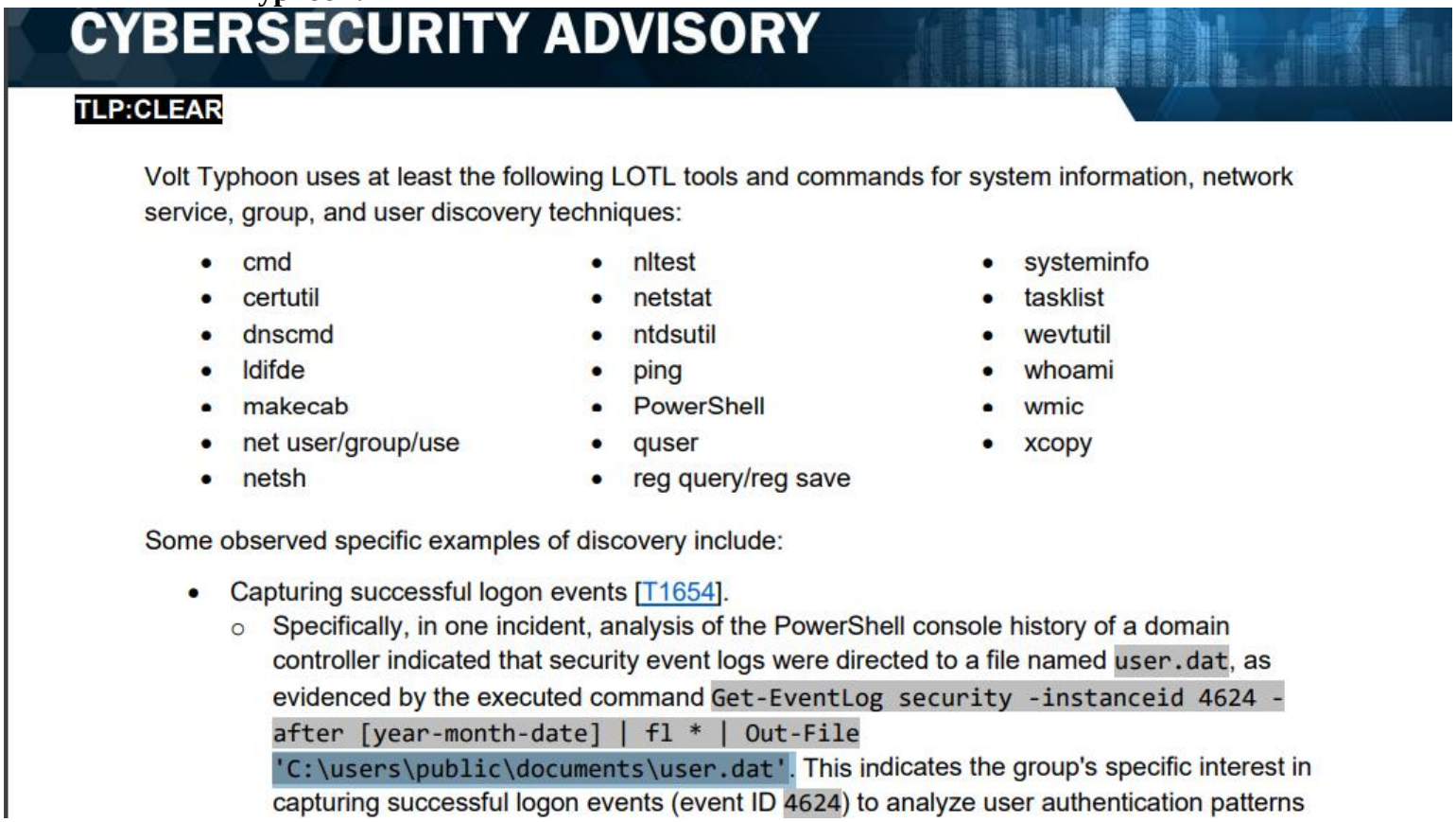


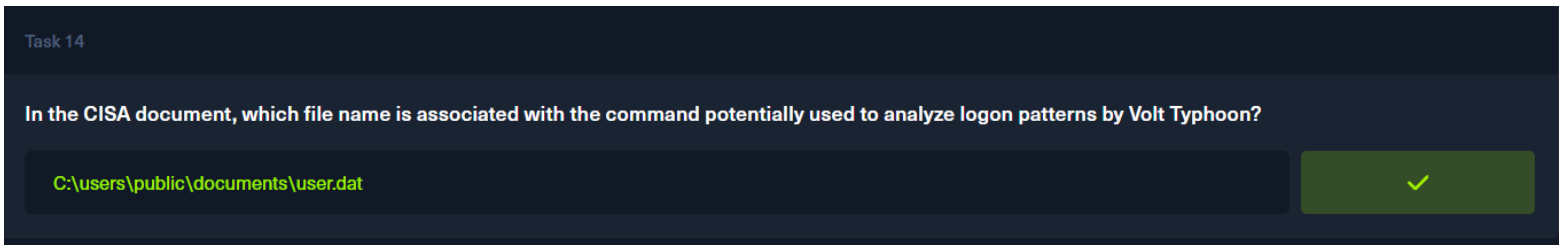


13. Según el documento CISA (https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf) al que hace referencia MITRE, ¿cuál es la estrategia principal que utiliza Volt Typhoon para evadir la defensa?
Leyendo el pdf salió la respuesta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



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?





Recursos Bibliográficos:
https://labs.hackthebox.com/achievement/sherlock/2394798/881