DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°013**	**Fecha: 15-01-2024**
		Página: 5 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de malware “Phemedrone Stealer” explota una vulnerabilidad crítica en Windows		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha detectado una nueva campaña de malware denominada “Phemedrone Stealer” que explota una vulnerabilidad de severidad **CRÍTICA** de tipo omisión de la función de seguridad que afecta a equipos con plataforma Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto eludir las comprobaciones de Windows Defender SmartScreen y otras indicaciones. Esta falla se puede explotar en campañas de phishing para evadir las indicaciones de los usuarios que advierten a los destinatarios sobre la apertura de un documento malicioso.

2. DETALLES:

Los investigadores de Trend Micro han descubierto una nueva campaña de malware que explota la vulnerabilidad registrada por MITRE como CVE-2023-36025 para implementar una cepa previamente desconocida del malware denominada “Phemedrone Stealer”.

Un atacante puede aprovechar esta vulnerabilidad para eludir las comprobaciones de Windows Defender SmartScreen y otras indicaciones. Esta falla se puede explotar en campañas de phishing para evadir las indicaciones de los usuarios que advierten a los destinatarios sobre la apertura de un documento malicioso.

Los investigadores indicaron que se han publicado múltiples demostraciones y códigos de prueba de concepto sobre la explotación de esta vulnerabilidad. Asimismo, se ha incrementado las campañas de malware que incluyen el exploit para esta vulnerabilidad en sus cadenas de ataque.

El malware “Phemedrone Stealer” permite a los operadores robar datos confidenciales de navegadores web, billeteras de criptomonedas y aplicaciones de mensajería como Telegram, Steam y Discord. El malware admite múltiples capacidades, incluida la toma de capturas de pantalla y la recopilación de información del sistema sobre el hardware, la ubicación y los detalles del sistema operativo.

Los datos robados se extraen a través de la plataforma de mensajería y VOIP “Telegram” o su servidor de comando y control (C2). El malware está escrito en lenguaje C# y sus autores mantienen activamente el código malicioso en GitHub y Telegram.

Una vez que se ejecuta el archivo .url malicioso que explota la vulnerabilidad CVE-2023-36025, se conecta a un servidor controlado por un atacante para descargar y ejecutar un archivo de elemento del panel de control (.cpl). en este caso Microsoft Windows Defender SmartScreen debería advertir a los usuarios con un mensaje de seguridad antes de ejecutar el archivo .url desde una fuente que no es de confianza. Sin embargo, los atacantes crean un archivo de acceso directo de Windows (.url) para evadir el mensaje de protección SmartScreen empleando un archivo .cpl como parte de un mecanismo de entrega de carga maliciosa.

Los archivos URL maliciosos que explotan la vulnerabilidad CVE-2023-36025 hacen referencia al servicio de mensajería instantánea y chat de voz VoIP “Discord” u otros servicios en la nube. Al ejecutar los archivos, se descarga y ejecuta un archivo de elemento del panel de control (.cpl). Luego llama a rundll32.exe para ejecutar una DLL maliciosa que actúa como cargador para la siguiente etapa, un script malicioso alojado en GitHub.

La siguiente etapa es un cargador ofuscado que recupera un archivo ZIP del mismo repositorio de GitHub a un directorio oculto creado utilizando la utilidad binaria de atributos de Windows (attrib.exe).

El archivo contiene los archivos para cargar la siguiente etapa y mantener la persistencia. La siguiente etapa carga la carga útil de Phemedrone Stealer.

A. Productos afectados:

- Equipos con Sistema operativo Windows.

B. Indicadores de compromiso:

SHA256

- f32964087462ba3c96a87ee8387f89de8fa605f2f5bb84cb5f754cd736683f2d.
- 5f1a027f1c1468f93671a4c7fc7b5da00a3c559a9116f5417baa6c1f89550d9f.
- c6765d92e540af845b3cbc4caa4f9e9d00d5003a36c9cb548ea79bb14c7e8f66.
- a841cd16062702462fdffdd7eef9fc3d88cde65d19c8d5a384e33066d65f9424.
- 22236e50b5f700f5606788dcd5ab1fb69ee092e8dffdd783ac3cab47f1f445ab.

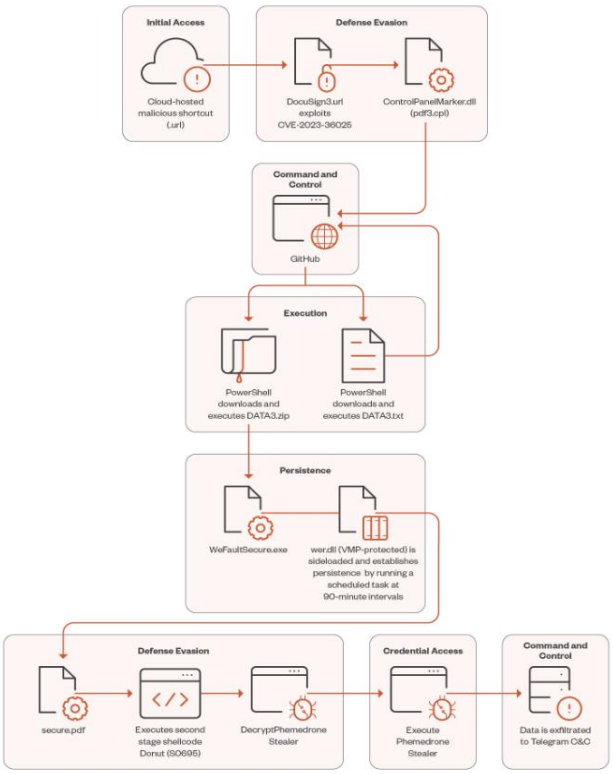
URL

- hxxps[://]raw[.]githubusercontent[.]com/nateeintanan2527/Joyce_Data/main/DATA3[.]txt.
- hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1175808264479449138/DocuSign3[.]url?ex=656c93c7&is=655a1ec7&hm=6e8b316f2112cfaf27bc8cf35089098e4a0f2d16054e8d199c13588c31b2e383&.
- hxxps[://]cdn[.]discordapp[.]com/attachments/1083311514368360519/1177255995156742144/DocuSign4[.]url?ex=6571d815&is=655f6315&hm=f9e208714ffc862f97cb6363fb887f11fda0020802a020a56a571c4195114854&.
- hxxps[://]URLcorta[.]at/ixEZ7.

IP

- 51[.]79[.]185[.]145.

Ver lista completa en los enlaces de referencia.



3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan esta vulnerabilidad. Microsoft señalo que abordó esta vulnerabilidad con el lanzamiento de las actualizaciones de seguridad del martes de parches en noviembre de 2023. Esta vulnerabilidad es un problema de omisión de la función de seguridad SmartScreen de Windows y viene siendo explotada activamente en la naturaleza.

Fuente de Información:	• hxxps://www.trendmicro.com/en_us/research/24/a/cve-2023-36025-exploited-for-defense-evasion-in-phemedrone-steal.html • hxxps://documents.trendmicro.com/images/TEx/20240111-cve-2023%E2%80%9336025-phemedrone-iocs8L7B0q0.txt