	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268	Fecha: 09-11-2023
		Página: 6 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de Spam utiliza el portal de noticias de Windows para distribuir malware		
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:

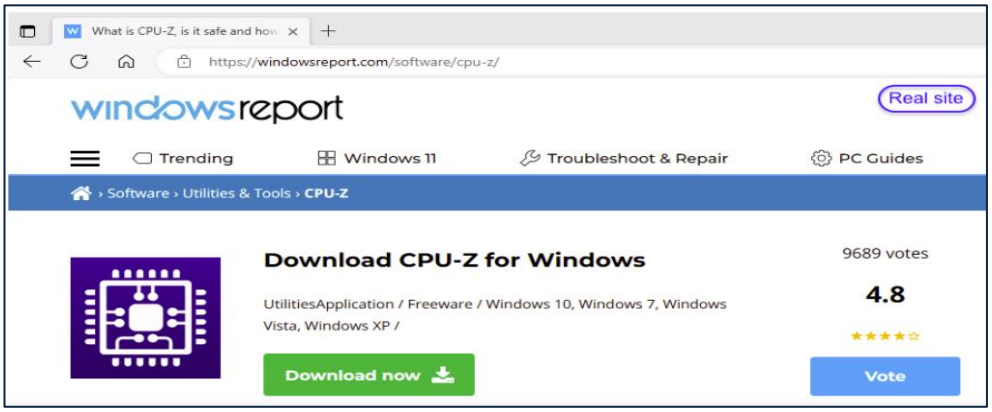
Investigadores de Inteligencia de amenazas de Malwarebytes, han informado que se ha detectado una nueva campaña de distribución de malware "RedLine Stealer", que utiliza publicidad maliciosa y se hace pasar por un portal de noticias legítimo de Windows. Un ataque exitoso podría permitir a un actor de amenazas el robo de credenciales de inicio de sesión, el robo de contraseñas, tarjetas de crédito e información confidencial, entre otros. De igual forma, un actor de amenazas también podría infectar a sus víctimas con otros tipos de malware, como ransomware, troyanos, mineros de criptomonedas y RAT.

2. DETALLES:

Los investigadores han observado una nueva campaña de publicidad maliciosa en la que los actores de amenazas copian un portal de noticias legítimo de Windows (WindowsReport.com) para distribuir un instalador malicioso de malware "RedLine Stealer", para la popular herramienta de procesador CPU-Z. Cabe señalar, que el portal de noticias de Windows nunca se vio comprometido y es legítimo, sino que los actores de amenazas copiaron su contenido para engañar a los usuarios, al suplantar el sitio oficial por otra que contiene la carga útil de malware.

"RedLine Stealer" es un programa malicioso de robo de información más destacados y utilizados en la actualidad. Según un informe de Insikt Group, es uno de los mayores proveedores de credenciales robadas para dos mercados clandestinos: Amigos Market y Russian Market. Su comercio se ha observado en mercados clandestinos a través de una serie de videos de YouTube sobre las principales tendencias globales de interés, como las NFT. Se detectó en foros de cibercriminales en febrero de 2020, como Malware-as-a-Service (MaaS).

"RedLine Stealer" es conocido por troyanizar servicios populares como Telegram (utilizando tácticas de ingeniería social como señuelos COVID-19), Signal y Discord (disfrazados de instaladores de Windows 11). También aprovecha las campañas de phishing por correo electrónico, Google Ads (para clasificar sitios web maliciosos) y experimentos con tácticas de ingeniería social dirigidas a los entusiastas de NFT.



El anuncio malicioso es para CPU-Z, una utilidad popular para usuarios de Windows que desean solucionar problemas de su procesador y otros detalles del hardware de su computadora. El anunciante aparece como Scott Cooper y probablemente sea una identidad falsa o comprometida.

Una técnica común utilizada por los actores de amenazas para evadir la detección es emplear encubrimiento. Cualquier persona que haga clic en el anuncio y que no sea la víctima prevista verá un blog estándar con varios artículos. Si la víctima que busca la aplicación CPU-Z hace clic en el anuncio, será redirigida a la página de descarga del software suplantado, donde pueden suponer erróneamente que es legítimo. Sin embargo, la URL de la barra de direcciones no coincide con la URL oficial de la aplicación.

Sin embargo, en un caso real, la víctima objetivo es redirigida a una página de descarga que contiene un instalador MSIX firmado digitalmente para evadir la detección. Una vez que el usuario hace clic en el instalador, se ejecuta en el sistema un script de PowerShell malicioso llamado "FakeBat", que descarga Redline Stealer. El script muestra el servidor de comando y control (C2) de malware, así como la carga útil remota Redline stealer. Los cargadores MSI son bastante comunes y permiten a los actores de amenazas actualizar la carga útil final simplemente intercambiando un script de PowerShell.

Según la infraestructura, los nombres de dominio y las plantillas de encubrimiento utilizadas, los investigadores creen que el incidente es parte de una campaña de publicidad maliciosa más amplia dirigida a otras utilidades como Notepad++, Citrix y VNC Viewer.

A. Indicadores de compromiso (IoC):

Dominios publicitarios:
- argenferia[.]com.
- realvnc[.]pro.
- Corporatecomf[.]online.
- cilrix-corp[.]pro.
- thecoopmodel[.]com.
- winscp-apps[.]online.
- wirehark-app[.]online.
- cilrix-corporate[.]online.
- workspace- aplicación[.]online.

URL de carga útil:
- thecoopmodel[.]com/CPU-Z-x86.msix.
- kaotickontracting[.]info/account/hdr.jpg.
- ivcgroup[.]en/temp/Citrix-x64.msix.
- robo-reclamo[.]sitio/orden/team.tar.gpg.
- argenferia[.]com/RealVNC-x64.msix.

Cargas útiles:
- 55d3ed51c3d8f56ab305a40936b446f761021abfc55e5cc8234c98a2c93e99e1.
- 9acbf1a5cd040c6dcecbe4e8e65044b380b7432f46c5fbf2ecdc97549487ca88.
- 419e06194c01ca930ed5d7484222e6827fd24520e72bfe6892cfde95573ffa16.
- cf9589665615375d1ad22d3b84e97bb686616157f2092e2047adb1a7b378cc95.

C2:
- 11234jkhfkujhs[.]site.
- 11234jkhfkujhs[.]top.
- 94.131.111[.]240.
- 81.177.136[.]179.

3. RECOMENDACIONES:

- Verificar la suma de comprobación de un archivo para asegurarse de que no haya sido manipulado comparando su suma hash SHA256 con lo que se publica en el sitio web del proveedor.
- Mantener su sistema operativo y software actualizados con los últimos parches y actualizaciones de seguridad.
- Utilizar un programa antivirus y mantenerlo siempre actualizado.
- Tener cuidado al abrir archivos adjuntos de correo electrónico o al hacer clic en enlaces de fuentes desconocidas.
- Evitar descargar software de fuentes no confiables y de sitios no oficiales.
- Utilizar contraseñas seguras y únicas para todas sus cuentas y evite guardar contraseñas en su navegador.
- Hacer una copia de seguridad periódica de sus datos importantes en un disco duro externo o en un servicio de almacenamiento en la nube.

Fuente de Información:	• hxxps://www.malwarebytes.com/blog/threat-intelligence/2023/11/malvertiser-copies-pc-news-site-to-deliver-infostealer • hxxps://cyware.com/news/threat-actors-impersonate-windows-news-portal-to-distribute-redline-stealer-7b320bfd • hxxps://cyware.com/resources/research-and-analysis/all-about-high-in-demand-information-theft-tool-redline-stealer-0df1

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°268**	**Fecha: 09-11-2023**
		Página: 10 de 14

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en 4D y 4D server 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:

Alexander Huamán Jaimes (@zanganox) ha reportado una vulnerabilidad de severidad **MEDIA** de tipo elemento de ruta de búsqueda no controlado en 4D y 4D server Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto la ejecución de código arbitrario.

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-4770 de tipo elemento de ruta de búsqueda no controlado, consiste en un secuestro de DLL, sustituyendo x64 shfolder.dll en la ruta de instalación y provocando una ejecución de código arbitrario.

Esta vulnerabilidad, utiliza una ruta de búsqueda fija o controlada para encontrar recursos, pero una o más ubicaciones en esa ruta pueden estar bajo el control de actores no deseados.

A. Productos afectados:

- Los ejecutables 4D.exe y 4D Server.exe, en sus versiones 19 R8 100218.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que el proveedor lance para abordar esta vulnerabilidad.

Fuente de Información:	• hxxps://es.4d.com/