Nro. Alerta:	AL-2024-034	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		V 1.1
Fecha:	12-dic-2024	Malware Glove Stealer	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de incidente: Malware
Nivel de riesgo: Alto

II. ALERTA

El malware Glove Stealer es una incorporación reciente al panorama de las amenazas cibernéticas, que se distingue por su capacidad de eludir el cifrado vinculado a aplicaciones (App-Bound) de Google Chrome. Identificada por primera vez por investigadores de ciberseguridad durante una investigación de una campaña de phishing, esta amenaza representa un momento crucial en la carrera armamentista entre actores maliciosos y soluciones de seguridad.

Figura 1.- *Glove Stealer* – *figura referencial*

III. INTRODUCCIÓN

Investigadores de seguridad de Gen Digital han descubierto un nuevo y sofisticado malware que roba información llamado Glove Stealer, que ataca específicamente datos del navegador, billeteras de criptomonedas y credenciales de autenticación explotando el servicio IElevator de Chrome para eludir el cifrado App-Bound.

Glove Stealer representa una evolución preocupante en el malware de robo de información, que combina tácticas de ingeniería social con sofisticación técnica para comprometer los datos de los usuarios.

Lo que hace que Glove Stealer se destaque del resto es su capacidad para eludir el cifrado vinculado a la aplicación (App-Bound), el mecanismo de protección de cookies que se introdujo en Chrome 127 para evitar su robo.

Los navegadores Chromium como Edge, Brave y el propio Chrome son susceptibles a esta maniobra, pero Glove Stealer también ataca los datos almacenados en otros navegadores, incluidos Opera, Yandex y CryptoTab.

Durante sus ataques, los actores de amenazas utilizaron tácticas de ingeniería social similares a las utilizadas en la cadena de infección de ClickFix , donde las víctimas potenciales son engañadas para instalar malware utilizando ventanas de error falsas que se muestran dentro de archivos HTML adjuntos a los correos electrónicos de phishing.

Aunque ClickFix puede adoptar muchas formas, incluida la inserción de mensajes de error falsos en sitios web comprometidos o páginas alojadas por atacantes, esta campaña comienza cuando un usuario recibió un correo electrónico de phishing. Junto con el correo electrónico, normalmente se incluye un archivo adjunto en formato HTML. Una página HTML como esta contiene motivos típicos de ClickFix, ya que muestra un mensaje de error falso que indica que no se pudo acceder correctamente a algún contenido y luego le indica al usuario cómo solucionarlo. Al seguir las instrucciones, el usuario copia un script malicioso en su portapapeles y, después de ejecutarlo en una terminal o en el indicador “Ejecutar”, infecta involuntariamente su propio sistema. Como ejemplo de página HTML de este tipo se muestra en la siguiente imagen:

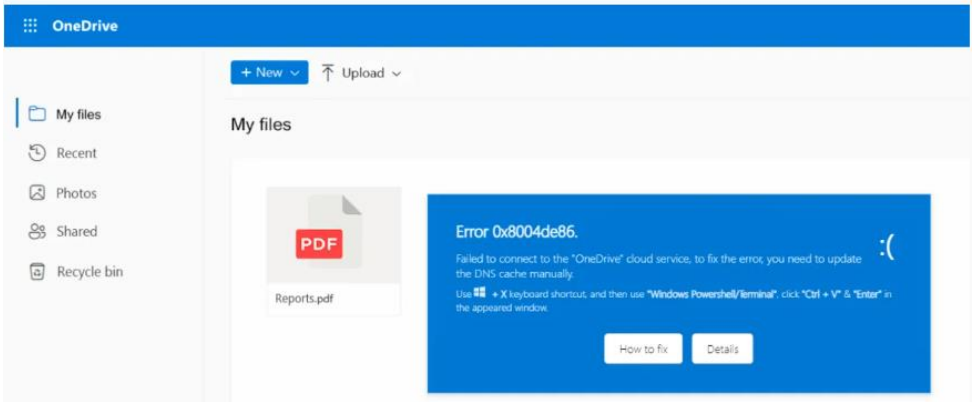

Figura 1. Ejemplo de archivo adjunto HTML de ClickFix

IV. VECTOR DE ATAQUE:

Glove Stealer, en campañas de phishing utilizan tácticas de ingeniería social, como ClickFix. En estas tácticas, los atacantes intentan engañar a los usuarios para que piensen que se están ayudando a sí mismos, cuando en realidad están infectando inadvertidamente sus dispositivos al seguir las instrucciones proporcionadas por los atacantes.

V. INDICADORES DE COMPROMISO

Guion original copiado en el portapapeles:

2bf6fab237ab58ae6cfe78f9a61ab6dcaf55f437cb7a77878e2e6aae3b208e80

Glove Stealer

56da496329d54587c31119d8878a7831a9814a92839aa6a9873ceeb91575b11a

Módulo de soporte para omitir el cifrado vinculado a la aplicación:

86ad4082e086a0b9a22dc91a16d0d9be38232975ab4d3d035224fb6d6cc7a44c

C&C

maestro.hdsjfkgsadoghdsiougds[.]espacio
master.volt-texs[.]en línea

VI. IMPACTO

Una de las características más destacadas de Glove Stealer es su capacidad para extraer datos de una amplia variedad de fuentes. El malware es experto en la recolección de:

- **Cookies del navegador:** el objetivo principal de la recopilación inicial de datos y ayuda a los atacantes a secuestrar sesiones autenticadas.
- **Carteras de criptomonedas:** extraen datos de la cartera de las extensiones del navegador, una preocupación importante para los titulares de monedas digitales.
- **Tokens 2FA:** estos tokens apuntan a sesiones de aplicaciones de autenticación como Google, Microsoft, Aegis y LastPass, poniendo en peligro una capa esencial de seguridad.
- **Datos de contraseña:** roba credenciales almacenadas en administradores de contraseñas como Bitwarden, KeePass y LastPass.
- **Correos electrónicos:** compromete a los clientes de correo, especialmente a Thunderbird, para acceder a comunicaciones confidenciales.

VII. RECOMENDACIONES:

1. Tenga cuidado con los correos electrónicos que contienen archivos adjuntos en formato HTML.
2. Nunca copie y pegue comandos de fuentes no confiables
3. Uso de métodos de autenticación fuertes para cuentas confidenciales
4. Actualizar periódicamente su sistema operativo y las aplicaciones instaladas.
5. Implementar soluciones antivirus confiables capaces de detectar y bloquear amenazas similares.
6. Supervisar periódicamente los registros del sistema y de la red para detectar actividades inusuales que indiquen un compromiso.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

https://www.kaspersky.com/about/press-releases/steelfox-exploits-foxit-pdf-editor-and-autocad-for-banking-data-theft-and-covert-crypto-mining

https://www.europapress.es/portaltic/ciberseguridad/noticia-paquete-malicioso-steelfox-combina-ransomware-tecnicas-criptomineria-dirige-ordenadores-windows-20241108121024.html

https://www.bleepingcomputer.com/news/security/new-steelfox-malware-hijacks-windows-pcs-using-vulnerable-driver/

https://cybersecsentinel.com/advanced-malware-steelfox-uses-windows-vulnerabilities-for-system-access/

https://www.ecucert.gob.ec/consejos/#

https://www.ecucert.gob.ec/alertas/