ALERTA DE SEGURIDAD CIBERNÉTICA
MALWARE REDLINE STEALER

Una de las numerosas campañas de malware (programas maliciosos) de alta relevancia en el último tiempo es Redline Stealer, de la familia de malware troyano conocida como **stealer** o **infostealer**. Como su nombre lo indica (*steal* es robar en inglés), Redline Stealer se dedica a robar información de los usuarios, principalmente desde sus navegadores web, además de incorporar recientemente la habilidad de robar criptomonedas de varias billeteras virtuales.

- Cuidado también con otros stealers conocidos: Racoon Stealer, Taurus, AZORult y Vidar.

Algunas características de Redline Stealer:

- No existen síntomas específicos que delaten la presencia de Redline Stealer ya que se hace pasar por procesos legítimos del sistema operativo del dispositivo.
- Es del tipo "Malware as a Service", o sea, se vende por, según señalan fuentes en línea, por alrededor de US$ 100 mensuales o unos US$ 200 de por vida. Es fácil de usar, no se necesita grandes habilidades para emplearlo con fines maliciosos.
- Redline Stealer recolecta información de los navegadores web de los equipos de sus víctimas, como cookies, claves guardadas, datos de autocompletar, información de tarjetas de crédito, credenciales de inicio de sesión VPN, registros de chat.
- Versiones más recientes también roban criptomonedas.
    - Algunas de las billeteras vulnerables: Armory, AtomicWallet, BitcoinCore, Bytecoin, DashCore, Electrim, Ethereum, LitecoinCore, Monero, Exodus, Zcast y Jaxx.
- El malware también recopila datos del sistema de la víctima, dirección IP, país, ciudad, nombre de usuario, distribución de teclado, sistema operativo, entre otros. Además, verifica las configuraciones de la tarjeta de video, antivirus instalado.
- Con esa información robada, los ciberdelincuentes pueden realizar transacciones bancarias y robar cuentas en redes sociales, por ejemplo. A través del secuestro de cuentas pueden engañar a otros usuarios y difundir malware y campañas de fraude, instalar mineros de criptomonedas, ingresar a entorno corporativos a través de los accesos VPN y descargar otros archivos troyanos de acceso remoto (RAT) entre múltiples otras acciones maliciosas.
- Se sabe que RedLine Stealer ha sido difundido a través de varias fachadas:
    - Como enlaces maliciosos en videos de YouTube. Por ejemplo, una campaña usó un enlace que prometía ser una herramienta para hacer trampa en el juego Valorant.
    - En falsos sitios de criptomonedas gratis
    - En cadenas de correo electrónicos de phishing con archivos adjuntos o link
    - Anuncios emergentes en sitios web de baja reputación o anuncios pagados por ciberdelincuentes (malvertising)
    - Softwares que aparenta ser legítimos para ser instalados por los usuarios, pero en realidad son maliciosos.

- Activadores de programas como Windows, office, adobe entre otros
- Descargas archivos de redes Peer-to-peer que fueron modificados para contener malware

Recomendaciones

- Activar el segundo factor de autenticación en todas las cuentas que lo permitan.
- Tener conciencia y reforzar, entre todos los miembros de la organización, la importancia de no hacer clic en enlaces que no nos conste sean seguros (phishing).
- Evitar descargar software fuera de los sitios de los proveedores o las tiendas online de su sistema operativo (AppStore, Google Play, etc.)
- No guardar contraseñas o números de tarjetas en el navegador web.
- Eliminar cookies regularmente.
- Implementar sistemas como DKIM, DMARC y SPF en el correo institucional.
- Instalar un buen programa antivirus y antimalware desde sus propios sitios web o tiendas oficiales (como Google Play y App Store).

Fuentes:

- https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer.
- https://www.pcrisk.com/removal-guides/17280-redlinestealer-malware.
- https://socradar.io/what-is-redline-stealer-and-what-can-you-do-about-it/.
- https://muha2xmad.github.io/malware-analysis/fullredline/
- https://asec.ahnlab.com/en/29885/
- https://www.proofpoint.com/us/blog/threat-insight/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign