| | | | |
|---|---|---|---|
| Nro. Alerta: | AL-2024-032 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br><br>**ALERTAS DE SEGURIDAD** | ecucert |
| TLP: | TLP:CLEAR | | V 1.1 |
| Fecha: | 21-nov-2024 | Malware SteelFox | Pág.: **1** of **5** |

## I. DATOS GENERALES:

**Clase de alerta:** Incidente

**Tipo de incidente:** Malware

**Nivel de riesgo:** Alto

## II. ALERTA

El equipo de investigación y análisis global de Kaspersky ha descubierto una nueva campaña maliciosa que explota software popular, como Foxit PDF Editor, AutoCAD y JetBrains. Los atacantes emplean malware ladrón para capturar la información de las tarjetas de crédito de las víctimas y detalles sobre sus dispositivos infectados, al mismo tiempo que operan como mineros de criptomonedas y utilizan en secreto el poder de las computadoras infectadas para extraer criptomonedas.

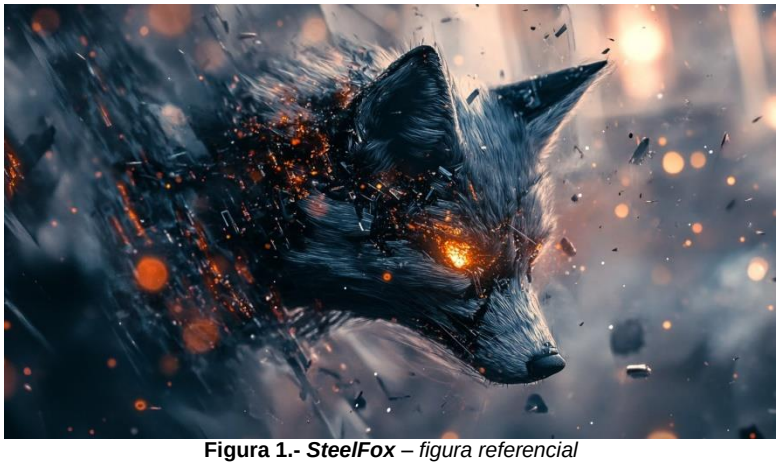

**Figura 1.- *SteelFox*** – *figura referencial*

## III. INTRODUCCIÓN

SteelFox es una sofisticada campaña de malware que combina capacidades de robo de información con minería de criptomonedas. Disfrazada como cracks de software para aplicaciones populares como Foxit PDF Editor, AutoCAD y

JetBrains, se dirige a los usuarios que buscan activaciones de software no autorizadas, para luego ejecutar ransomware en ordenadores Windows.

Así, una vez obtienen derechos de administrador, SteelFox crea un servicio que ejecuta un controlador **WinRingO.sys**, que se puede explotar para obtener diferentes privilegios a nivel del sistema (**NT/System**), lo que permite al actor malicioso acceder a procesos o recursos sin ningún tipo de restricción.

La campaña de malware consta de dos componentes principales: el módulo ladrón y un minero de criptomonedas. SteelFox recopila información extensa de las computadoras de las víctimas, incluidos datos del navegador, credenciales de cuenta, información de tarjetas de crédito y detalles sobre el software instalado y las soluciones antivirus. También puede capturar contraseñas de Wi-Fi, información del sistema y datos de zona horaria.

Además, los atacantes utilizan una versión modificada de XMRig, un minero de código abierto, para aprovechar la potencia de los dispositivos infectados para la minería de criptomonedas, probablemente apuntando a Monero.

El equipo de Análisis e Investigación Global (GReAT) de Kaspersky ha advertido que esta campaña maliciosa está activa al menos desde febrero de 2023, y al momento sigue representando una gran amenaza a pesar de que los ciberdelincuentes detrás de la campaña SteelFox no cambiaron significativamente su funcionalidad, pero trabajaron para modificar sus técnicas y código para evadir la detección.

Además, los investigadores sospechan que los actores maliciosos comenzarán a distribuir su malware bajo la apariencia de otros productos más populares a fin de afectar a más usuarios con SteelFox.

## IV. VECTOR DE ATAQUE:

SteelFox se propaga a través de publicaciones y torrents maliciosos que anuncian herramientas de activación gratuitas para software popular. Al ejecutarse, el dropper solicita privilegios de administrador, que luego se explotan para instalar un controlador vulnerable (WinRing0.sys).

Este controlador, susceptible a CVE-2020-14979 y CVE-2021-41285, permite que el malware escale privilegios al nivel de sistema.

Con privilegios elevados, SteelFox instala sus componentes, incluido el ladrón de información y el criptominero, y establece una comunicación persistente con sus servidores de comando y control.

## V. INDICADORES DE COMPROMISO

| MD5 |
|---|
| fb94950342360aa1656805f6dc23a1a0 |
| 5029b1db994cd17f2669e73ce0a0b71a |
| 69a74c90d0298d2db34b48fa6c51e77d |
| 84b29b171541c8251651cabe1364b7b6 |
| 015595d7f868e249bbc1914be26ae81f |
| 040dede78bc1999ea62d1d044ea5e763 |
| 051269b1573f72a2355867a65979b485 |
| 08fa6ebc263001658473f6a968d8785b |
| d5290ba0cd8529032849ae567faba1ce |
| d715507131bbf4ca1fe7bc4a5ddfeb19 |
| dc8c18e4b729fdbf746252b2fc1decc5 |
| dc9d42902bda8d63e5858b2a062aecc1 |
| 9dff2cdb371334619b15372aa3f6085c |
| c20e1226782abdb120e814ee592bff1a |
| c6e7c8c76c7fb05776a0b64699cdf6e7 |

| SHA-256 |
|---|
| 8d9abb726799da54909ebd7a9c356b990fd68175945e6c05e64de18ca7d1d3d8 |
| 3e52c0b97f67287c212e5bc779b0e7dd843fb0df2ef11b74e1891898d492782c |
| 9954fd4e914f2427c25ba0a4b3d305819a71d648b05fc94d108c0459795f077d |
| d625bc9ea13d56825bd3c63698743e329564ca384d51f24d417a7171df498992 |

| SHA-1 |
|---|
| 287e09c8ad36b93588e7eeb678a8d9e76c293cbb |
| ea651af34bfe2052668e37bcd3f60696ebaffa1c |
| 993d944aa84e851c48f960cf018e4abe18ec5cd9 |
| f608cc545f3dbeed9822186e3ab11f7069543d1f |
| **Direcciones IP** |
| ankjdans.xyz |

| URL maliciosas |
|---|
| hxxps://github[.]com/DavidNguyen67/CrackJetbrains |
| hxxps://github[.]com/TrungGa123/Active-all-app-Jetbrains/ |
| hxxps://www[.]cloudstaymoon[.]com/2024/05/06/tools-1 |
| hxxps://squarecircle[.]ru/Intelij/jetbrains-activator.exe |
| hxxps://drive.google[.]com/file/d/1bhDBVMywFg2551oMmPO3_5VaeYnj7pe5/view?usp=sharing |

## VI. RECOMENDACIONES:

1. Descargar aplicaciones sólo de fuentes oficiales.
2. Actualizar periódicamente su sistema operativo y las aplicaciones instaladas.
3. Implementar soluciones antivirus confiables capaces de detectar y bloquear SteelFox y amenazas similares.
4. Supervisar periódicamente los registros del sistema y de la red para detectar actividades inusuales que indiquen un compromiso.
5. Concientizar a los usuarios de los riesgos de descargar e instalar “cracks” de software no autorizado.

## VII. 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.

## VIII. 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/