Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	El troyano bancario Mispadu aprovecha el fallo SmartScreen de Windows		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

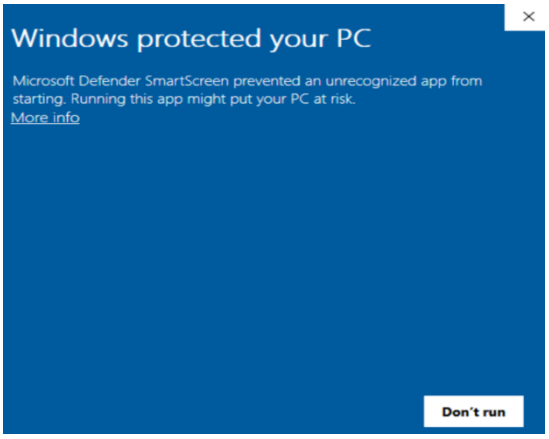
1. **ANTECEDENTES**:

Los investigadores han identificado una nueva variante del ladrón Mispadu, que se dirige específicamente a víctimas en México. Esta variante del ladrón Mispadu utiliza la vulnerabilidad CVE-2023-36025 de Windows SmartScreen para descargar y ejecutar cargas útiles maliciosas en el sistema.

El ladrón Mispadu está escrito en Delphi y fue identificado por primera vez en noviembre de 2019. Se difunde a través de correos electrónicos de phishing y se sabe que infecta principalmente a víctimas en la región de América Latina (LATAM) como Brasil y México. Metabase Q reveló en marzo de 2023 que, desde agosto de 2022, las campañas de spam de Mispadu han obtenido un mínimo de 90.000 credenciales de cuentas bancarias.

2. **DETALLES:**

Según los informes compartidos con Cyber Security News, la función Windows SmartScreen está diseñada para mostrar una advertencia a los usuarios para protegerlos contra visitas a sitios web dañinos. Sin embargo, la función se puede omitir mediante un archivo URL especialmente diseñado.



Este archivo URL o un hipervínculo contendrá un enlace al recurso compartido de red de los atacantes para descargar un binario de un sitio web dañino, que pasa por alto la advertencia de Windows SmartScreen al abusar de un parámetro que se refiere a un recurso compartido de red en lugar de una URL.

Una vez activado, Mispadu expone sus verdaderas intenciones atacando selectivamente a las víctimas en función de su ubicación geográfica (es decir, América o Europa Occidental) y la configuración del sistema.

El malware utiliza el algoritmo de cifrado AES para varios descifrados a través de la biblioteca bcrypt.dll. Además, identifica el directorio %TEMP% para almacenar ciertos archivos que se utilizarán durante la ejecución del malware.

Para establecer la comunicación C2, el malware realiza una solicitud GET HTTP o HTTPS, según la versión de Microsoft Windows que se ejecuta en el sistema.

Una vez establecida la comunicación C2, el malware utiliza SQLite para recopilar bases de datos históricas de los navegadores Microsoft Edge y Google Chrome y las almacena en el directorio %TEMP%. Después de esto, el malware extrae las URL bajo ciertas condiciones y las compara con una lista específica.

Todas las URL de destino tendrán el (.) cambiado a (,), agrupadas y codificadas para evitar la fuerza bruta del algoritmo. Luego, toda esta información se envía al C2 y podría utilizarse para futuras actividades ciberdelincuentes.

Indicadores De Archivos:

- 8e1d354dccc3c689899dc4e75fdbdd0ab076ac457de7fb83645fb735a46ad4ea
- bc25f7836c273763827e1680856ec6d53bd73bbc4a03e9f743eddfc53cf68789
- fb3995289bac897e881141e281c18c606a772a53356cc81caf38e5c6296641d4

- 46d20fa82c936c5784f86106838697ab79a1f6dc243ae6721b42f0da467eaf52
- 03bdae4d40d3eb2db3c12d27b76ee170c4813f616fec5257cf25a068c46ba15f
- 1b7dc569508387401f1c5d40eb448dc20d6fb794e97ae3d1da43b571ed0486a0
- e136717630164116c2b68de31a439231dc468ddcbee9f74cca511df1036a22ea

Indicadores De Red:

- plinqok[.]com
- trilivok[.]com
- xalticainvest[.]com
- moscovatech[.]com
- hxxp://trilivok[.]com/4g3031ar0/cb6y1dh/it.php
- hxxps://plinqok[.]com/3dzy14ebg/buhumo0/it.php
- 24.199.98[.]128/expediente38/8869881268/8594605066.exe
- 24.199.98[.]128/verificacion58/6504926283/3072491614.exe
- 24.199.98[.]128/impresion73/5464893028/8024251449.exe

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.
- Implementar sistemas sólidos de detección de intrusiones.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://gbhackers.com/mispadu-malware-exploits-windows/ • hxxps://hackarizona.org/es/el-troyano-bancario-mispadu-aprovecha-el-fallo-smartscreen-de-windows/