**[Alerta: hay un nuevo malware que arrebata las contraseñas de los usuarios](https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html)**

09 de abril de 2021[Ravie Lakshmanan](https://thehackernews.com/p/authors.html)

[](https://thehackernews.com/images/-Q243YkfewCc/YHBJTt3qs8I/AAAAAAAACO4/AqlmsGBMNBk2Z13eapjH76z9bppY4dbkwCLcBGAsYHQ/s0/password-stealers.jpg)

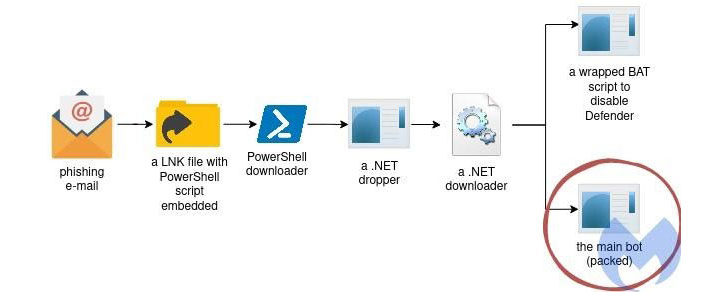
Se ha detectado un descargador de malware previamente indocumentado en ataques de phishing para implementar ladrones de credenciales y otras cargas útiles maliciosas.

Apodado " Saint Bot ", se dice que el malware apareció por primera vez en la escena en enero de 2021, con indicios de que está en desarrollo activo.

"Saint Bot es un programa de descarga que apareció recientemente, y poco a poco está ganando impulso. Se vio caer a ladrones (es decir, [Taurus](https://www.zscaler.com/blogs/security-research/taurus-new-stealer-town) Stealer) o cargadores adicionales ( [ejemplo](https://www.virustotal.com/gui/file/388d18b98704bff34ac1cb0a6603e68ba300205ee2f14e4bf482f1012d933231/detection) ), pero su diseño le permite utilizarlo para distribuir cualquier tipo de malware ", dijo Aleksandra" Hasherezade "Doniec, analista de inteligencia de amenazas en [Malwarebytes](https://blog.malwarebytes.com/threat-analysis/2021/04/a-deep-dive-into-saint-bot-downloader/" \t "_blank) .

"Además, Saint Bot emplea una amplia variedad de técnicas que, aunque no son novedosas, indican cierto nivel de sofisticación considerando su apariencia relativamente nueva".

La cadena de infección analizada por la firma de ciberseguridad comienza con un correo electrónico de phishing que contiene un archivo ZIP incrustado ("bitcoin.zip") que dice ser una billetera bitcoin cuando, de hecho, es un script de PowerShell bajo la apariencia de un archivo de acceso directo .LNK. Este script de PowerShell luego descarga el malware de la siguiente etapa, un ejecutable de WindowsUpdate.exe, que, a su vez, suelta un segundo ejecutable (InstallUtil.exe) que se encarga de descargar dos ejecutables más llamados def.exe y putty.exe.

[](https://thehackernews.com/images/-uIAVQPFuDVE/YHBFY-Ya4HI/AAAAAAAACOs/g6UIR9fcwk8aO8g52pmyo9i31-_UkywRgCLcBGAsYHQ/s0/malware-attack.jpg)

Mientras que el primero es un script por lotes responsable de deshabilitar Windows Defender, putty.exe contiene la carga útil maliciosa que finalmente se conecta a un servidor de comando y control (C2) para su posterior explotación.

La ofuscación presente en cada etapa de la infección, sumada a las técnicas de anti-análisis adoptadas por el malware, permite a los operadores de malware explotar los dispositivos en los que fueron instalados sin llamar la atención.

Además de realizar "comprobaciones de autodefensa" para verificar la presencia de un depurador o un entorno virtual, Saint Bot está diseñado para no ejecutarse en Rumania y en países seleccionados de la Comunidad de Estados Independientes (CEI), que incluye a Armenia, Bielorrusia, Kazajstán y Moldavia. , Rusia y Ucrania.

La lista de comandos admitidos por el malware incluye:

* descargar y ejecutar otras cargas útiles recuperadas del servidor C2
* actualizar el malware del bot, y
* desinstalarse a sí mismo de la máquina comprometida

Si bien estas capacidades pueden parecer muy pequeñas, el hecho de que Saint Bot sirva como descargador de otro malware lo hace lo suficientemente peligroso.

Curiosamente, las cargas útiles se obtienen de archivos alojados en Discord, una táctica que se ha vuelto cada vez más común entre los actores de amenazas, que abusan de las funciones legítimas de dichas plataformas para las comunicaciones C2, evitan la seguridad y entregan malware.

"Cuando los archivos se cargan y almacenan dentro de Discord CDN, se puede acceder a ellos usando la URL de CDN codificada por cualquier sistema, independientemente de si se ha instalado Discord, simplemente navegando a la URL de CDN donde se aloja el contenido", investigadores de Cisco Talos [reveló](https://blog.talosintelligence.com/2021/04/collab-app-abuse.html) en un análisis a principios de esta semana, convirtiendo así software como Discord y Slack en objetivos lucrativos para alojar contenido malicioso.

"Saint Bot es otro pequeño descargador", dijo Hasherezade. "[No es] tan maduro como SmokeLoader, pero es bastante nuevo y actualmente está desarrollado activamente. El autor parece tener algún conocimiento del diseño de malware, que es visible por la amplia gama de técnicas utilizadas. Sin embargo, todas las técnicas implementadas son bien conocido y bastante estándar, [y] no ha mostrado mucha creatividad hasta ahora ".

¿Qué tipo de amenaza es?

Esta amenaza es un troyano “downloader” cuyo principal objetivo es descargar e instalar otros malwares en los equipos infectados. Su diseño le permite utilizarlo para distribuir cualquier tipo de malware pero su principal objetivo es arrebatar las contraseñas de los usuarios.

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con un correo electrónico de phishing que contiene un archivo ZIP incrustado que simula ser una billetera bitcoin sin embargo, es un script de PowerShell bajo la apariencia de un archivo de acceso directo, y este luego descarga otro malware, un ejecutable de WindowsUpdate.exe que descarga otro ejecutable InstallUtil.exe que descarga dos ejecutables más, llamados def.exe y putty.exe.

¿Hay más de una amenaza aplicada?

Si, un troyano que ejecuta varios archivos y spyware que roba las contraseñas de usuarios.