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

Nombrado como Saint Bot, el malware apareció por primera vez 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 cobrando impulso. Se vio caer a ladrones o cargadores adicionales, pero su diseño le permite utilizarlo para distribuir cualquier tipo de malware»*, dijo Aleksandra Hasherezade Doniec, analista de inteligencia de amenazas en Malwarebytes.
>
> *«Además, Saint Bot emplea una gran variedad de técnicas que, aunque no son novedosas, indican cierto nivel de sofisticación considerando su apariencia relativamente nueva»,* agregó.

La cadena de infección analizada por la compañía de seguridad cibernética comienza con un correo electrónico de phishing que contiene un archivo ZIP incrustado («bitcoin.zip»), que dice ser una billetera bitcoin cuando, en realidad, 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.

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 visual, 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
- Desinstalarse a sí mismo de la máquina comprometida

Aunque estas capacidades parecen pequeñas, el hecho de que Saint Bot sirva como descargador de otro malware lo hace suficientemente peligroso.

Algo que llama la atención es que 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 utilizando la URL de CDN codificada por cualquier sistema, independientemente de si Discord se ha instalado, simplemente navegando a la URL de CDN donde se aloja el contenido»,* dijeron los investigadores de Cisco Talos.

> *«Saint Bot es otro pequeño descargador. No es tan maduro como SmokeLoader, pero es bastante nuevo y actualmente está desarrollado activamente. El autor parece tener algún conocimiento sobre el diseño de malware, lo cual es visible por la amplia gama de técnicas utilizadas. Sin embargo, todas las técnicas implementadas son bien conocidas y bastante estándar, y hasta ahora no muestran*

> *mucha creatividad»,* dijo Hasherezade.