	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°026	Fecha: 30-01-2024
		Página: 5 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de malware de robo de información “WhiteSnake Stealer” dirigido a equipos con sistema operativo Windows		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Investigadores de ciberseguridad de la empresa Checkmarx, han identificado múltiples paquetes maliciosos en el repositorio de Python Package Index (PyPI) que distribuyen un malware de robo de información llamado “WhiteSnake Stealer (WS)” en sistemas Windows. Un ataque exitoso podría permitir a un actor de amenazas el robo de información de navegadores web, billeteras de criptomonedas y diversas aplicaciones.

2. DETALLES:

El Python Package Index (PyPI) es un repositorio abierto de paquetes de software desarrollado por la comunidad de Python para facilitar el desarrollo o actualización rápido de aplicaciones. Aunque la mayoría de los paquetes subidos a PyPI son contribuciones de individuos dedicados que buscan apoyar a la comunidad de Python, actores de amenazas también publican regularmente paquetes infectados con malware.

Los investigadores de ciberseguridad de Checkmarx han identificado múltiples paquetes maliciosos en el repositorio de PyPI que distribuyen un malware de robo de información llamado “WhiteSnake Stealer” en equipos con sistema operativo Windows. Los paquetes identificados en esta campaña (nigpal, figflix, telerer, seGMM, fbdebug, sGMM, myGens, NewGends y TestLibs111) muestran metodologías de ataque similares a las descritas de Checkmarx hace cuatro meses, sugiriendo una posible conexión con una campaña maliciosa de principios de 2023.

Estos paquetes contienen código fuente codificado en Base64 de ejecutables PE u otros scripts de Python, y dependiendo del sistema operativo de la víctima, se ejecuta el payload malicioso al instalar estos paquetes de Python. Recientemente, identificaron a un autor de malware en PyPI, apodado «WS», que subía discretamente paquetes maliciosos. Se estima que puede haber más de 2000 víctimas solo con los paquetes mencionados.

El malware “WhiteSnake Stealer” personalizado para Windows tiene un mecanismo Anti-VM, se comunica con un servidor de comando y control (C&C) a través del protocolo Tor y puede robar información de navegadores web, billeteras de criptomonedas y diversas aplicaciones.

El actor detrás de esta campaña, identificado como “PYTA31” por la empresa Checkmarx, tiene como objetivo principal exfiltrar datos sensibles y, en particular, información de billeteras de criptomonedas de las máquinas afectadas.

Cabe indicar que algunos paquetes maliciosos también han sido observados incorporando funcionalidades de «clipper» para sobrescribir el contenido del portapapeles con direcciones de billeteras controladas por los atacantes, con el fin de realizar transacciones no autorizadas.

A. Productos afectados:

- Equipos con Sistema operativo Windows.

3. RECOMENDACIÓN:

- Ser cautelosos al utilizar paquetes de código abierto y verificar la presencia de contenido malicioso que pueda hacer que los dispositivos sean susceptibles al robo de información.

Fuente de Información:	• hxxps://unaaldia.hispasec.com/2024/01/paquetes-pypi-maliciosos-introducen-el-malware-whitesnake-infostealer-en-windows.html • hxxps://www.fortinet.com/blog/threat-research/info-stealing-packages-hidden-in-pypi • hxxps://jfrog.com/blog/new-malware-targets-python-developers-uses-tor-for-c2-communication/ • hxxps://thehackernews.com/2024/01/malicious-pypi-packages-slip-whitesnake.html