Una nueva variante del malware Snake Keylogger está siendo empleada activamente para atacar a usuarios de Windows en China, Turquía, Indonesia, Taiwán y España.

Según Fortinet FortiGuard Labs, esta versión actualizada del malware ha sido responsable de más de 280 millones de intentos de infección bloqueados a nivel global desde que comenzó el año.

> *«Por lo general, se propaga a través de correos electrónicos fraudulentos que incluyen archivos adjuntos o enlaces maliciosos. Snake Keylogger está diseñado para extraer información confidencial de navegadores web ampliamente utilizados como Chrome, Edge y Firefox. Lo hace mediante el registro de pulsaciones de teclas, la recopilación de credenciales y el monitoreo del portapapeles»*, explicó el investigador de seguridad Kevin Su.

El malware también cuenta con funcionalidades que le permiten transferir la información robada a servidores bajo el control de los atacantes. Para ello, emplea el protocolo SMTP (Simple Mail Transfer Protocol) y bots de Telegram, lo que facilita a los ciberdelincuentes el acceso a credenciales y otros datos sensibles.

Un aspecto destacable de este reciente ataque es que utiliza AutoIt, un lenguaje de scripting, para entregar y ejecutar la carga maliciosa. Específicamente, el archivo ejecutable que transporta el malware es un binario compilado en AutoIt, lo que le ayuda a evadir los métodos de detección tradicionales.

> *«El uso de AutoIt no solo complica el análisis estático al encapsular la carga en el script compilado, sino que también permite generar un comportamiento dinámico similar al de herramientas de automatización legítimas»,* agregó Su.

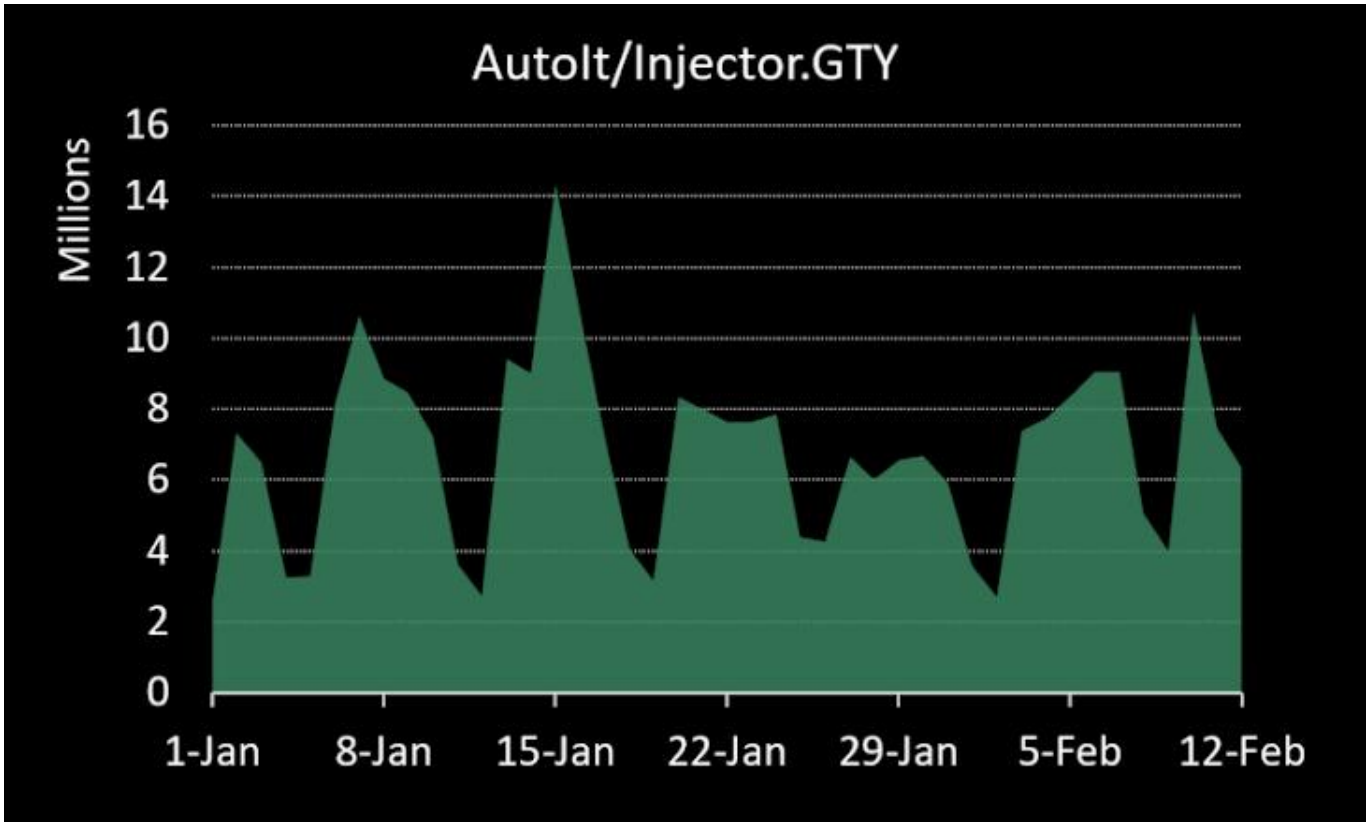
Al ejecutarse, Snake Keylogger se duplica en un archivo denominado «ageless.exe» dentro

de la carpeta «%Local_AppData%\supergroup». Además, crea un archivo adicional llamado «ageless.vbs» en la carpeta de inicio de Windows, lo que permite que el script de Visual Basic (VBS) inicie automáticamente el malware tras cada reinicio del sistema.

Gracias a este método de persistencia, Snake Keylogger puede seguir operando en el dispositivo comprometido, reactivando sus actividades maliciosas incluso si su proceso es detenido.

El ataque se completa cuando la carga principal es inyectada en un proceso legítimo de .NET, como «regsvcs.exe», mediante una técnica conocida como process hollowing. Esto permite al malware ocultarse dentro de un proceso de confianza y evitar ser detectado.

Por otro lado, se ha descubierto que Snake Keylogger captura pulsaciones de teclas y emplea sitios como «checkip.dyndns[.]org» para obtener la dirección IP y ubicación de la víctima.



> *«Para registrar las pulsaciones de teclado, el malware emplea la API SetWindowsHookEx con el parámetro WH_KEYBOARD_LL (valor 13), lo que le permite monitorear la actividad del teclado a nivel bajo. Gracias a esta técnica, los atacantes pueden interceptar datos sensibles como credenciales bancarias»*, explicó Su.

Este ataque coincide con una campaña detectada por CloudSEK, en la que ciberdelincuentes aprovechan infraestructuras vulneradas de instituciones educativas para propagar archivos LNK maliciosos disfrazados de documentos PDF, con el propósito final de instalar el malware Lumma Stealer.

La operación está dirigida a sectores como finanzas, salud, tecnología y medios de comunicación, utilizando una estrategia de ataque en varias etapas que conduce al robo de

contraseñas, datos de navegación y monederos de criptomonedas.

> *«El principal método de infección de esta campaña se basa en la distribución de accesos directos LNK maliciosos, diseñados para parecer documentos PDF legítimos»*, explicó el investigador de seguridad Mayank Sahariya. Añadió que estos archivos se alojan en un servidor WebDAV, al que las víctimas son redirigidas tras visitar ciertos sitios web.

Cuando se abre el archivo LNK, este ejecuta un comando PowerShell que se conecta a un servidor remoto para descargar el siguiente componente malicioso: un código JavaScript ofuscado que contiene otro PowerShell, el cual obtiene y ejecuta Lumma Stealer desde el mismo servidor.

Recientemente, también se ha detectado la distribución de malware tipo stealer a través de archivos JavaScript ofuscados, cuyo propósito es extraer una amplia cantidad de datos sensibles de equipos Windows comprometidos y enviarlos a un bot de Telegram controlado por los atacantes.

> *«El ataque comienza con un archivo JavaScript ofuscado, el cual obtiene cadenas codificadas desde un servicio de código abierto para ejecutar un script de PowerShell»,* indicó Cyfirma.
>
> *«Este script descarga una imagen JPG y un archivo de texto desde una dirección IP y un enlace acortado. Ambos contienen ejecutables maliciosos en formato MZ DOS, que han sido ocultos mediante técnicas de esteganografía. Una vez ejecutados, estos archivos despliegan el malware stealer».*