Se ha descubierto una nueva variedad de malware en Internet que ya ha infectado a miles de computadoras en todo el mundo y lo más probable es que ningún antivirus pueda detectarlo.

Esto se debe a que se trata de un malware avanzado sin archivos, aparte de que aprovecha solo las utilidades legítimas del sistema incorporado y las herramientas de terceros para ampliar su funcionalidad y comprometer las computadoras, en lugar de utilizar cualquier código malicioso.

La técnica de traer sus propias herramientas legítimas es efectiva y rara vez se ha visto en la naturaleza, lo que ayuda a los hackers a combinar sus actividades maliciosas con la actividad regular de la red o las tareas de administración del sistema, dejando menos huellas.

Descubierto independientemente por investigadores de ciberseguridad en Microsoft y Cisco Talos, el malware, denominado como *«Nodersok» y «Divergent»,* se distribuye principalmente por medio de anuncios maliciosos en línea e infecta a los usuarios mediante un ataque de descarga automática.

Fue descubierto por primera vez a mediados de julio de este año, y ha sido diseñado para convertir las computadoras Windows infectadas en servidores proxy, que según Microsoft, pueden ser utilizados por los atacantes como un relevador para ocultar el tráfico malicioso, mientras que Cisco Talos cree que los proxies se utilizan para el fraude de clics para generar ingresos para los atacantes.

La infección comienza cuando los anuncios maliciosos sueltan el archivo de la aplicación HTML (HTA) en las computadoras de los usuarios, que al hacer clic, ejecuta una serie de cargas de JavaScript y scripts de PowerShell que eventualmente descargan e instalan el malware Nodersok.

> *«Todas las funcionalidades relevantes residen en scripts y códigos de shell que casi siempre se cifran, se descifran y se ejecutan solo en la memoria. Ningún ejecutable*

> *malicioso se escribe en el disco»,* explicó Microsoft.

El código JavaScript se conecta a servicios legítimos de Cloud y dominios de proyecto para descargar y ejecutar scripts de segunda etapa y componentes cifrados adicionales, que incluyen:

- Scripts de PowerShell: Intenta deshabilitar el antivirus de Windows Defender y la actualización de Windows.
- Shellcode binario: Intenta escalar privilegios utilizando la interfaz COM con elevación automática.
- Node.exe: La implementación de Windows del popular framework Node.js, que es confiable y tiene una firma digital válida, ejecuta JavaScript malicioso para operar dentro del contexto de un proceso confiable.
- WinDivert (Desvío de paquetes de Windows): Una utilidad legítima y poderosa de captura y manipulación de paquetes de red que el malware utiliza para filtrar y modificar ciertos paquetes salientes.

Finalmente, el malware deja caer la carga útil de JavaScript escrita para el marco Node.js que convierte el sistema comprometido en un proxy.

> *«Esto concluye la infección, al final de la cual el filtro de paquetes de red está activo y la máquina funciona como un posible zombie proxy. Cuando una máquina se convierte en un proxy, los atacantes de la red (sitios web, servidores de C&C, máquinas comprometidas, etc.), lo que puede permitirles realizar actividades maliciosas sigilosas»,* explicó Microsoft.

Según los expertos de Microsoft, el motor proxy basado en Node.js actualmente tiene dos propósitos principales: primero, conecta el sistema infectado de nuevo a un servidor remoto de comando y control controlado por el atacante, y segundo, recibe solicitudes HTTP para

poder volver a él.

Por otro lado, los expertos de Cisco Talos concluyen que los atacantes están utilizando este componente proxy para ordenar a los sistemas infectados que naveguen a páginas web arbitrarias con fines de monetización y fraude de clics.

Nodersok infectó a miles de usuarios de Windows

Según Microsoft, el malware Nodersok ya infectó miles de máquinas en las últimas semanas, con la mayoría de los objetivos ubicados en Estados Unidos y Europa.

Si bien el malware se enfoca principalmente en apuntar a usuarios domésticos de Windows, los investigadores han visto aproximadamente el 3% de los ataques dirigidos a organizaciones de sectores industriales, que incluyen educación, atención médica, finanzas, comercio minorista y servicios comerciales y profesionales.

Debido a que la campaña de malware emplea técnicas avanzadas sin archivos y se basa en una infraestructura de red evasiva mediante el uso de herramientas legítimas, la campaña de ataque pasó desapercibida, lo que dificulta la detección de los programas antivirus tradicionales basados en firmas.

> *«Si excluimos todos los archivos limpios y legítimos aprovechados por el ataque, todo lo que queda es el archivo HTA inicial, la carga útil final basada en Node.js y un montón de archivos encriptados. Las firmas tradicionales basadas en archivos son inadecuadas para contrarrestar sofisticadas amenazas como esta»,* dijo Microsoft.

Sin embargo, la compañía dice que el *«comportamiento del malware produjo una huella visible que se destaca claramente para cualquiera que sepa dónde buscar».*

En julio de este año, Microsoft también descubrió e informó sobre otra campaña de malware sin archivos, denominada Astaroth, que fue diseñada para robar información confidencial de

los usuarios, sin dejar caer ningún archivo ejecutable en el disco o instalar ningún software en la máquina de la víctima.

Microsoft dijo que su protección de próxima generación ATP de Windows Defender detecta estos ataques de malware sin archivos en cada etapa de infección al detectar comportamientos anómalos y maliciosos, como la ejecución de scripts y herramientas.