Un framework conocido por entregar un troyano bancario ha recibido nuevas actualizaciones para implementar una gama más amplia de malware, incluyendo cargas útiles de ransomware.

> *«La familia de malware Gootkit ha sido de al rededor de más de la mitad de una década un maduro troyano con funcionalidad centrado en torno al robo de credenciales de banca»,* dijeron los investigadores de Sophos, Gabor Szappanos y Andrew Brandt.
>
> *«En los últimos años, se ha dedicado casi tanto esfuerzo a la mejora de su método de entrega como al propio malware basado en NodeJS».*

Nombrado como Gootloader, el sistema de entrega de malware ampliado se produce en medio de un aumento en el número de infecciones dirigidas a usuarios en Francia, Alemania, Corea del Sur y Estados Unidos.

Documentado por primera vez en 2014, Gootkit es una plataforma de malware basada en Javascript capaz de realizar una serie de actividades encubiertas, como la inyección web, captura de pulsaciones de teclas, toma de capturas de pantalla, grabación de videos, además del robo de correo electrónico y contraseñas.

A lo largo de los años, la herramienta de ciberdelincuencia ha evolucionado para obtener nuevas funciones de robo de información, con el cargador Gootkit reutilizado en combinación con las infecciones de ransomware REvil/Sodinokibi informadas el año pasado.

Aunque la campañas que utilizan trucos de ingeniería social para entregar cargas útiles maliciosas cuestan diez centavos por docena, Gootloader lo lleva a otro nivel.

La cadena de infección recurre a técnicas sofisticadas que implican el alojamiento de archivos ZIP maliciosos en sitios web pertenecientes a empresas legítimas que han sido

engañadas para aparecer en los primeros resultados de una consulta de búsqueda mediante métodos manipulados de optimización de motores de búsqueda (SEO).

Además, los resultados del motor de búsqueda apuntan a sitios web que no tienen una conexión *«lógica»* con la consulta de búsqueda, lo que implica que los atacantes deben estar en posesión de una vasta red de sitios web pirateados. En un caso descubierto por los investigadores, un consejo para un acuerdo de bienes raíces surgió como primer resultado de una práctica médica neonatal incumplida con sede en Canadá.

> *«Para garantizar que se capturen los objetivos de las geografías correctas, los adversarios reescriben el código del sitio web sobre la marcha, para que los visitantes del sitio web que se encuentran fuera de los países deseados vean contenido web benigno, mientras que a los de la ubicación correcta se les muestra una página con un foro de discusión sobre el tema que han consultado»,* dijeron los investigadores.

Cuando se hace clic en el resultado de la búsqueda, el usuario accede a una página similar a un tablero de mensajes falso, que no solo coincide con los términos de búsqueda utilizados en la consulta inicial, sino que también incluye un enlace al archivo ZIP, que contiene un archivo Javascript muy ofuscado que inicia la siguiente etapa de compromiso para inyectar el malware sin archivos obtenido de un servidor remoto en la memoria.

Esto toma la forma de un enfoque evasivo de múltiples etapas que comienza con un cargador .NET, que comprende un malware cargador basado en Delphi, que a su vez, contiene la carga útil final en forma cifrada.

Además de entregar el ransomware REvil y el troyano Gootkit, se han detectado varias campañas que actualmente aprovechan el marco Gootloader para entregar el malware financiero Kronos en Alemania de forma sigilosa, y la herramienta de pos-explotación Cobalt Strike en Estados Unidos.

Aún no está claro cómo los operadores obtienen acceso a los sitios web para atender las inyecciones maliciosas, pero los investigadores sospechan que los atacantes pueden haber obtenido las contraseñas instalando el malware Gootkit o comprando credenciales robadas en mercados clandestinos, o aprovechando fallas de seguridad actualmente en los complementos actualizados junto con el software del sistema de gestión de contenidos (CMS).

> *«Los desarrolladores detrás de Gootkit parecen haber cambiado los recursos y la energía de entregar solo su propio malware financiero a crear una plataforma de entrega compleja y sigilosa para todo tipo de cargas útiles, incluido el ransomware REvil»,* dijo Gabor Szappanos, director de investigación de amenazas de Sophos.
>
> *«Esto muestra que los delincuentes tienen a reutilizar sus soluciones probadas en lugar de desarrollar nuevos mecanismos de entrega. Además, en lugar de atacar activamente las herramientas de endpoint como lo hacen algunos distribuidores de malware, los creadores de Gooloader han optado por complicadas técnicas evasivas que ocultan el resultado final»,* agregó.