Una serie de campañas maliciosas han aprovechado instaladores falsos de aplicaciones y juegos populares como Viber, WeChat, NoxPlayer y Battlefield, como un señuelo para engañar a los usuarios para que descarguen una nueva puerta trasera y una extensión maliciosa indocumentada de Google Chrome, con el objetivo de robar credenciales y datos almacenados en los sistemas comprometidos, además de mantener un acceso remoto persistente.

Cisco Talo atribuyó las cargas útiles del malware a un actor desconocido con alias magnat, y dijo que *«estas dos familias han estado sujetas a un constante desarrollo y mejora por parte de sus autores».*

Al parecer, los ataques comenzaron a fines de 2018, con actividad intermitente observada hacia fines de 2019 y hasta principios de 2020, seguidos de nuevos picos desde abril de 2021, mientras que destacaron principalmente a los usuarios en Canadá, seguidos de Estados Unidos, Australia, Italia, España y Noruega.

Un aspecto notable de las intrusiones es el uso de publicidad maliciosa como un medio para atacar a las personas que buscan software popular en los motores de búsqueda para presentarles enlaces para descargar instaladores falsos que arrojan un ladrón de contraseñas llamado RedLine Stealer, una extensión de Chrome denominada MagnatExtension, que está programada para registrar las pulsaciones de teclas y realizar capturas de pantalla, y una puerta trasera basada en AutoIt que establece el acceso remoto a la máquina.

MagnatExtension, que se hace pasar por la navegación segura de Google, también incluye otras características que son útiles para los atacantes, incluida la capacidad de robar datos de formularios, recolectar cookies y ejecutar código JavaScript arbitrario. Los datos de telemetría analizados por Talos revelaron que la primera muestra del complemento del navegador se detectó en agosto de 2018.

Las comunicaciones de comando y control (C2) de la extensión también se destacan. Aunque la dirección C2 está codificada, el C2 actual también puede actualizarla con una lista de dominios C2 adicionales.

Pero en caso de falla, recurre a un método alternativo que implica obtener una nueva dirección C2 a partir de una búsqueda en Twitter de hashtags como *«#aquamamba2019» o «#ololo2019».*

Después, el nombre de dominio se construye a partir del texto del tweet adjunto concatenando la primera letra de cada palabra, es decir, un tweet con el contenido *«Squishy turbulent areas terminate active round engines after dank years. Industrial creepy units» y con el hashtag «#aquamamba2019»*, se traduce como *«statareadу[.]icu».*

Una vez que un servidor de comando y control activo está disponible, los datos aspirados (historial de navegador, cookies, datos de formulario, pulsaciones de teclas y capturas de pantalla) se extraen en forma de una cadena JSON cifrada en el cuerpo de una solicitud HTTP POST, el cifrado clave a la que está codificada en la función de descifrado. La clave de cifrado, a su vez, se cifra con la clave pública del servidor.

> *«Basándonos en el uso de ladrones de contraseñas y una extensión de Chrome que es similar a un troyano bancario, evaluamos que los objetivos del atacante son obtener credenciales de usuario, posiblemente para la venta o para su propio uso en una mayor explotación»*, dijo el investigador de Cisco Talos, Tiago Pereira.

> *«El motivo para la implementación de una puerta trasera RDP no está claro. Lo más probable es la venta de acceso RDP, el uso de RDP para evitar las funciones de seguridad del servicio en línea basadas en la dirección IP u otras herramientas instaladas en el punto final o el uso de RDP para más explotación en sistemas que parecen interesantes para el atacante».*