Se ha descubierto una nueva y poderosa operación de spyware habilitada para rootkits en la que los hackers distribuyen malware multifuncional disfrazado de software o aplicación troyana que se presenta como software legítimo, ya sean reproductores de video, controladores o incluso productos antivirus.

El rootkit, denominado como Scranos, fue descubierto por primera vez el año pasado, pero parece ser todavía un trabajo en proceso, pues evoluciona continuamente, probando nuevos componentes y mejorando regularmente los componentes antiguos, lo que lo convierte en una amenaza importante.

Scranos cuenta con un diseño modular que ha adquirido capacidades para robar credenciales de inicio de sesión y cuentas de pago de diversos servicios populares, eliminar el historial de navegación y las cookies, obtener suscriptores de YouTube, mostrar anuncios, además de descargar y ejecutar cualquier carga útil.

Bitdefender compartió un extenso informe con The Hacker News antes de su lanzamiento, el malware gana persistencia en las máquinas infectadas al instalar un controlador de rootkit firmado digitalmente.

Los investigadores creen que los atacantes obtuvieron el certificado de firma de código digital válido de forma fraudulenta, que originalmente se emitió a Yun Yu Health Management Consulting (Shangai) Co., Ltd., y no se ha revocado hasta ahora.

> *«El rootkit registra una devolución de llamada de apagado para lograr la persistencia. En el cierre, el controlador se escribe en el disco y se crea una clave de servicio de inicio en el registro»*, dicen los investigadores.

Después de la infección, el malware del rootkit inyecta un descargador en un proceso legítimo que luego se comunica con el servidor de Comando y Control (C&C) controlado por el atacante y descarga una o más cargas útiles.

Estos son algunos datos y cargas útiles del robo de contraseñas:

Robo de contraseña e historial de navegación: El dropper principal roba las cookies y las credenciales de inicio de sesión de Google Chrome, Chromium, Mozilla Firefox, Opera, Microsoft Edge, Internet Explorer, Baidu Browser y Yandex. Además, puede robar las cookies e información de inicio de sesión se las cuentas de las víctimas en Facebook, YouTube, Amazon y Airbnb.

Extensión de carga útil del instalador: Esta carga instala extensiones de adware en Chrome e inyecta anuncios maliciosos o cargados de malware en todas las páginas web que visitan los usuarios. Algunos ejemplos también encontraron la instalación de extensiones de navegador falsas, como Chrome Filter, Fierce-tips y PDF Maker.

Carga de datos de Steam Stealer: Este componente roba y envía las credenciales e información de la cuenta Steam de las víctimas, incluida la lista de aplicaciones y juegos instalados, así como la versión codificada, al servidor del atacante.

El malware interactúa en redes sociales en nombre de las víctimas

Algunas otras cargas útiles pueden interactuar con distintos sitios web en nombre de la víctima, como:

Carga útil de suscriptor de YouTube: Esta carga manipula las páginas de YouTube ejecutando Chrome en modo de depuración, e indica al navegador que realice varias acciones en una página web, como iniciar un video, silenciar un video, suscribirse a un canal y hacer clic en los anuncios.

Proceso de carga de Scranos para spam en Facebook

Carga de spam de Facebook: Mediante el uso de cookies recopiladas y otros tokens, los atacantes pueden ordenar que el malware envíe las solicitudes de amistad de Facebook a otros usuarios. También puede enviar mensajes privados a los amigos de Facebook de la

víctima con enlaces a APK de Android maliciosos.

Aplicación de software publicitario para Android: Disfrazada de la legítima aplicación «Escaneo preciso de código QR», disponible en Google Play Store, la aplicación de malware muestra agresivamente anuncios, rastrea a las víctimas infectadas y utiliza el mismo servidor de C&C que el malware de Windows.

Scranos roba información de pago de sitios web populares

Aquí está la lista de DLL contenidas en el dropper principal:

DLL de Facebook: Esta DLL extrae información sobre las cuentas de usuario de Facebook, incluidas sus cuentas de pago, su lista de amigos y si son administradores de una página.

DLL de Amazon: Esta DLL extrae información de la cuenta de Amazon del usuario. Los investigadores encontraron una versión de esta DLL que ha sido diseñada para extraer información de las cuentas de Airbnb registradas.

Según la telemetría recopilada por los investigadores de Bitdefender, Scranos está apuntando a usuarios de todo el mundo, pero *«parece ser más frecuente en India, Rumania, Brasil, Francia, Italia e Indonesia».*

La muestra más antigua de este malware se remonta a noviembre de 2018, con un pico masivo en diciembre y enero, pero en marzo de 2019, Scranos comenzó a impulsar otras cepas de malware, lo que, según los investigadores, es *«un claro indicador de que la red ahora está afiliada con terceros en esquemas de pago por instalación».*