Una campaña activa de malware ha puesto su mira en los usuarios de Facebook y YouTube aprovechando un nuevo ladrón de información para secuestrar las cuentas y abusar de los recursos de los sistemas para extraer criptomonedas.

Bitdefender llama al malware S1deload Stealer, por su uso de técnicas de carga lateral de DLL para superar las defensas de seguridad y ejecutar sus componentes maliciosos.

> *«Una vez infectado, S1deload Stealer roba las credenciales de los usuarios, emula el comportamiento humano para aumentar artificialmente la participación de videos y otros contenidos, evalúa el valor de las cuentas individuales (como identificar a los administradores de redes sociales corporativas), extrae la criptomoneda BEAM y propaga el enlace malicioso a los seguidores de los usuarios»*, dijo el investigador de Bitdefender, Dávid ÁCS.

En otras palabras, el objetivo de la campaña es tomar el control de las cuentas de Facebook y YouTube de los usuarios y alquilar el acceso para aumentar el número de visitas y los likes de los videos y publicaciones compartidas en las plataformas.

Se estima que más de 600 usuarios únicos se vieron comprometidos durante el período de seis meses entre julio y diciembre de 2022. La mayoría de las infecciones se encuentran en Rumania, Turquía, Francia, Bangladesh, México, Perú y Canadá.

Para realizar el esquema, los usuarios son atraídos por contenido para adultos por medio de publicaciones de Facebook que contienen enlaces a archivos ZIP que, al extraerse, desencadenan una intrincada secuencia de infección que conduce a la implementación del malware.

> *«El autor del malware, por lo tanto, puede crear un ciclo de retroalimentación: cuantas más PC pueda infectar, más spam podrá generar en Facebook, más clics podrá generar para infectar más PC»*, dijo Bitdefender.

Además de ser capaz de descargar módulos adicionales en el host comprometido, el malware también es responsable de iniciar un navegador Chrome sin interfaz gráfica de usuario que usa una extensión para inflar de forma artificial las visitas de videos de YouTube.

El ladrón además captura las credenciales guardadas y las cookies de los navegadores web, realiza verificaciones del perfil de Facebook y también carga un cryptojacker que extrae criptomonedas sin el conocimiento o consentimiento de la víctima.

Bitdefender dijo que encontró superposiciones de infraestructura con un sitio web llamado upview[.]us, que anuncia opciones para comprar visitas, likes y suscriptores de YouTube, así como opciones para aumentar los likes, comentarios, seguidores y visitas de videos de publicaciones de Facebook.

> *«El ladrón S1deload tiene serias implicaciones de privacidad para la víctima infectada con él. El malware extrae las credenciales almacenadas de la víctima, incluyendo el correo electrónico, redes sociales o incluso cuentas financieras. El actor de la amenaza puede acceder a estas cuentas o venderlas en la web oscura»,* dijo la compañía rumana.