El notorio malware TrickBot se está dirigiendo a clientes de 60 empresas financieras y tecnológicas, incluyendo empresas de criptomonedas, ubicadas principalmente en Estados Unidos, incluso cuando sus operadores han actualizado la red de bots con nuevas funciones anti análisis.

> *«TrickBot es una malware sofisticado y versátil con más de 20 módulos que se pueden descargar y ejecutar bajo demanda»,* dijeron los investigadores de Check Point, Aliaksandr Trafimchuk y Raman Ladutska en un informe.

Además de ser frecuente y persistente, TrickBot ha evolucionado continuamente sus tácticas para superar las capas de seguridad y detección. Con ese fin, el módulo de inyección web «injectDll» del malware, que es responsable de robar datos bancarios y de credenciales, aprovecha las técnicas anti-desofuscación para bloquear la página web y frustrar los intentos de examinar el código fuente.

También se implementaron barandillas contra el análisis para evitar que los investigadores de seguridad envíen solicitudes automáticas a los servidores de comando y control (C2) para recuperar nuevas inyecciones web.

Otra de las fortalezas clave de TrickBot es su capacidad de propagarse, lo que logra mediante el uso del módulo «tabDLL» para robar las credenciales de los usuarios y propagar el malware a través de la red compartida SMBv1 utilizando el exploit EternalRomance.

Un tercer módulo crucial implementado como parte de las infecciones de TrickBot es «pwgrabc», un ladrón de credenciales diseñado para desviar contraseñas de navegadores web y otras aplicaciones como Outlook, Filezilla, WinSCP, RDP, Putty, OpenSSH, OpenVPN y TeamViewer.

> *«TrickBot ataca a víctimas de alto perfil para robar las credenciales y brindar a sus operadores acceso a los portales con datos confidenciales donde pueden causar un*

> *daño mayor. Los operadores detrás de la infraestructura tienen mucha experiencia en el desarrollo de malware en un nivel alto»,* dijeron los investigadores.

Los hallazgos también se producen cuando se reveló que el grupo de TrickBot empleaba métodos de metaprogramación para su familia de malware Bazar para ocultar su código y protegerse contra la ingeniería inversa con el objetivo final de evadir la detección basada en firmas.