Campaña de malware activa dirigida a América Latina se encuentra difundiendo una variante reciente de un troyano bancario denominado BBTok, enfocándose particularmente en usuarios de Brasil y México.

> Según la investigación publicada por Check Point esta semana, *«El troyano bancario BBTok cuenta con una funcionalidad especializada que replica las interfaces de más de 40 bancos en México y Brasil, engañando a las víctimas para que ingresen su código de autenticación de dos factores (2FA) en sus cuentas bancarias o su número de tarjeta de pago».*

Las cargas útiles son generadas a través de un script personalizado de PowerShell en el servidor y son únicas para cada víctima, teniendo en cuenta su sistema operativo y país. Estas cargas se envían mediante correos electrónicos de phishing que utilizan diversos tipos de archivos.

BBTok es un malware bancario basado en Windows que surgió por primera vez en 2020. Está equipado con funciones que abarcan las capacidades típicas de un troyano, lo que le permite enumerar y finalizar procesos, emitir comandos a distancia, manipular el teclado y presentar páginas de inicio falsas para bancos que operan en estos dos países.

Las cadenas de ataque son relativamente sencillas en su ejecución, empleando enlaces fraudulentos o archivos adjuntos ZIP para implementar sigilosamente el troyano, el cual es recuperado desde un servidor remoto (216.250.251[.]196), mientras se muestra un documento señuelo al usuario.

Sin embargo, estas cadenas de ataque están diversificadas para sistemas Windows 7 y Windows 10, adoptando principalmente medidas para evitar los mecanismos de detección recién implementados, como la Interfaz de Escaneo Antimalware (AMSI) que permite escanear la máquina en busca de amenazas.

Dos métodos clave para pasar inadvertidos son el uso de binarios *«living-off-the-land»*

(LOLBins) y verificaciones de geovallado para asegurarse de que los objetivos provengan exclusivamente de Brasil o México antes de distribuir el malware mediante el script de PowerShell.

Una vez que se ejecuta, BBTok establece conexiones con un servidor remoto para recibir comandos y simular páginas de verificación de seguridad de diversos bancos.

Al suplantar las interfaces de bancos latinoamericanos, el objetivo es recopilar información de credenciales y autenticación ingresada por los usuarios para realizar apropiaciones de cuentas bancarias en línea.

> *«Lo que destaca es el enfoque cauteloso del operador: todas las actividades bancarias se ejecutan únicamente bajo el comando directo de su servidor C2 y no se realizan automáticamente en todos los sistemas infectados»,* señaló la compañía.

El análisis de Check Point sobre el malware ha revelado una mejora sustancial en su ofuscación y enfoque desde 2020, expandiéndose más allá de los bancos mexicanos. La presencia de idioma español y portugués tanto en el código fuente como en correos electrónicos de phishing da una pista sobre el origen de los atacantes.

Se estima que más de 150 usuarios han resultado infectados por BBTok, según una base de datos SQLite encontrada en el servidor que aloja el componente de generación de carga útil, y que registra el acceso a la aplicación maliciosa.

El enfoque geográfico y lingüístico apunta a que los actores de amenazas probablemente operen desde Brasil, que sigue siendo un epicentro de malware enfocado en aspectos financieros.

> *«Aunque BBTok ha logrado pasar desapercibido debido a sus técnicas evasivas y a*

> *su enfoque en víctimas de México y Brasil, está claro que aún se encuentra activo»,* advirtió Check Point.

> *«Debido a sus numerosas capacidades y su método de distribución único y creativo que implica archivos LNK, SMB y MSBuild, todavía representa una amenaza para organizaciones e individuos en la región».*

Este desarrollo coincide con la descripción por parte de la empresa de ciberseguridad israelí de una nueva campaña de phishing a gran escala que recientemente apuntó a más de 40 empresas prominentes en diversas industrias en Colombia, con el objetivo final de desplegar el troyano Remcos a través de una secuencia de infección en varias etapas.

> *«Remcos, un troyano sofisticado tipo 'Swiss Army Knife', otorga a los atacantes control total sobre la computadora infectada y puede utilizarse en una variedad de ataques. Las consecuencias comunes de una infección con Remcos incluyen el robo de datos, infecciones posteriores y apropiaciones de cuentas»,* informó Check Point.