Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°224	Fecha: 22-09-2023
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Nueva variante del troyano bancario BBTok ataca a más de 40 bancos latinoamericanos		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Una campaña activa de malware dirigida a América Latina está distribuyendo una nueva variante de un troyano bancario llamado BBTok, particularmente a usuarios de Brasil y México.

BBTok es un malware bancario basado en Windows que apareció por primera vez en 2020. Utiliza una variedad de técnicas para ocultar su actividad y dificultar la detección por parte de los motores antivirus. Está equipado con funciones que ejecutan la gama troyana típica, lo que le permite enumerar y eliminar procesos, emitir comandos remotos, manipular el teclado y ofrecer páginas de inicio de sesión falsas para los bancos que operan en los dos países.

El troyano utiliza un mecanismo de puerta trasera (backdoor) que permite a quien lo controla ejecutar distintos comandos de manera remota. BBTok tiene la capacidad de evadir algunos de los principales softwares antivirus disponibles en el mercado: Avast, Windows Defender y Panda Antivirus, entre otros.

Con esta intrusión, el ciberdelincuente puede simular instrucciones del teclado, abrir y cerrar ventanas, grabar las pulsaciones del teclado durante un periodo determinado y también enviar alertas relacionadas con la seguridad de los servicios y las aplicaciones de la mayoría de los grandes bancos en México.

Los piratas informáticos también pueden optar por simular diferentes interfaces de verificación de seguridad falsa bancaria a través de comandos de control de puerta trasera y robar credenciales de inicio de sesión de usuario para Santander, BanBajio, ScotiaBank, AFIRME, Banregio, Banco Azteca, Multiva, Inbursa, HSBC, Banorte, CitiBanamex, BBVA, etc.

2. DETALLES:

"El banquero BBTok tiene una funcionalidad dedicada que replica las interfaces de más de 40 bancos mexicanos y brasileños, y engaña a las víctimas para que ingresen su código 2FA en sus cuentas bancarias o para que ingresen su número de tarjeta de pago", dijo Check Point en una investigación publicada esta semana.

Las cargas útiles se generan mediante un script de PowerShell personalizado del lado del servidor y son únicas para cada víctima según el sistema operativo y el país, y se envían a través de correos electrónicos de phishing que aprovechan una variedad de tipos de archivos.

Las cadenas de ataque en sí son bastante sencillas y emplean enlaces falsos o archivos adjuntos ZIP para implementar sigilosamente el banquero recuperado de un servidor remoto (216.250.251[.]196) mientras se muestra un documento señuelo a la víctima.

Una vez iniciado, BBTok establece conexiones con un servidor remoto para recibir comandos para simular las páginas de verificación de seguridad de varios bancos.

Al suplantar las interfaces de los 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 es notable es el enfoque cauteloso del operador: todas las actividades bancarias sólo se ejecutan mediante orden directa desde su servidor C2 y no se llevan a cabo automáticamente en cada sistema infectado", dijo la compañía.

El análisis del malware realizado por Check Point ha revelado una mejora significativa en su ofuscación y orientación desde 2020, expandiéndose más allá de los bancos mexicanos. La presencia de los idiomas español y portugués en el código fuente, así como en los correos electrónicos de phishing, ofrece una pista sobre el origen de los atacantes.

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

El objetivo y el lenguaje apuntan a que los actores de amenazas probablemente operen desde Brasil, que sigue siendo el epicentro de un potente malware centrado en las finanzas .

"Debido a sus muchas capacidades y su método de entrega único y creativo que involucra archivos LNK, SMB y MSBuild, todavía representa un peligro para las organizaciones e individuos de la región".

3. RECOMENDACIONES:

- Capacitar a los empleados sobre las mejores prácticas de ciberseguridad.
- No hacer clic en enlaces o archivos adjuntos incluidos en correos electrónicos que se reciben de manera inesperada.
- Utiliza una solución antivirus licenciada con protección en tiempo real y que te permita eliminar troyanos
- Instalar herramientas de seguridad en los equipos que contemplen soluciones antispam y detecten programas maliciosos de cara a evitar su instalación.
- Configura cuentas en la nube utilizando direcciones de correo electrónico que ofrezcan soporte de recuperación de cuentas.
- Segmentar las redes para proteger mejor los sistemas críticos.
- Evaluar el uso de una red privada virtual (VPN) para prevenir la vulnerabilidad de servicios expuestos.
- Utilizar la política del mínimo privilegio para limitar el número de personas que tienen acceso a un área determinada.

Fuente de Información:	• hxxps://thehackernews.com/2023/09/new-variant-of-banking-trojan-bbtok.html • hxxps://www.eleconomista.com.mx/sectorfinanciero/BBTok-el-malware-que-apunta-a-los-usuarios-de-BBVA-Banorte-Banco-Azteca-y-otros-bancos-en-Mexico--20201126-0038.html