Este martes, investigadores de seguridad cibernética detallaron cuatro familias diferentes de troyanos bancarios brasileños, que fueron detectados dirigidos a instituciones financieras en Brasil, América Latina y Europa.

Denominados colectivamente como *«Tetrade»* por investigadores de Kaspersky, las familias de malware, que comprenden Guildma, Javali, Melcoz y Grandoreiro, desarrollaron sus capacidades para funcionar como una puerta trasera y adoptar una variedad de técnicas de ofuscación para ocultar sus actividades maliciosas de los antivirus.

> *«Guildma, Javali, Melcoz y Grandoreiro son ejemplos de otro grupo/operación bancaria brasileña que decidió expandir sus ataques en el extranjero, apuntando a bancos en otros países»*, dijo Kaspersky.
>
> *«Se benefician del hecho de que muchos bancos que operan en Brasil también tienen operaciones en otros lugares de América Latina y Europa, lo que facilita extender sus ataques contra los clientes de estas instituciones financieras»,* agregó.

Guildma y Javali emplean un proceso de implementación de malware de múltiples etapas, utilizando correos electrónicos de phishing como mecanismo para distribuir las cargas útiles iniciales.

Kaspersky descubrió que Guildma no solo tiene nuevas características y agregó más sigilo a sus campañas desde su origen en 2015, sino que también se expandió a nuevos objetivos más allá de Brasil para atacar a los usuarios bancarios en América Latina.

Una nueva versión del malware, por ejemplo, utiliza archivos adjuntos de correo electrónico comprimidos, como un vector de ataque para ocultar las cargas útiles maliciosas, o un archivo HTML que ejecuta un fragmento de código JavaScript para descargar el archivo y buscar otros módulos que usan una herramienta legítima de línea de comandos como BITSAdmin.

Además de esto, aprovecha los flujos de datos alternativos de NTFS para ocultar la presencia de las cargas útiles descargadas en los sistemas y aprovecha el secuestro de órdenes de búsqueda de DLL para lanzar los binarios de malware, solo si el entorno está libre de depuración y virtualización de herramientas.

> *«Para ejecutar los módulos adicionales, el malware utiliza la técnica de vaciado de procesos para ocultar la carga maliciosa dentro de un proceso en la lista blanca, como svchost.exe»*, dijo Kaspersky.

Estos módulos se descargan de un servidor controlado por el atacante, cuya información se almacena en páginas de Facebook y YouTube en un formato cifrado.

Una vez instalado, la carga útil final monitorea sitios web bancarios específicos, lo que al abrirse, desencadena una cascada de operaciones que permiten a los criminales informáticos realizar cualquier transacción financiera utilizando la computadora de la víctima.

Javali, activo desde noviembre de 2017, de forma similar, descarga las cargas útiles enviadas por correo electrónico para recuperar un malware de etapa final de un C2 remoto, que es capaz de robar información financiera y de inicio de sesión de usuarios en Brasil y México que visitan sitios web de criptomonedas como Bittrex o soluciones de pago como Mercado Pago.

## Robo de contraseñas y billeteras Bitcoin

Melcoz, una variante del RAT de acceso remoto de código abierto, se vinculó a una serie de ataques en Chile y México desde 2018, y el malware tiene la capacidad de robar contraseñas desde el portapapeles, los navegadores y las billeteras de Bitcoin, reemplazando la información original de la billetera.

Utiliza scripts VBS en los archivos del paquete de instalación (.MSI) para descargar el

malware en el sistema, y posteriormente, abusa del intérprete AutoIt y del servicio NAT de VMware para cargar la DLL maliciosa en el sistema destino.

> *«El malware permite al atacante mostrar una ventana superpuesta frente al navegador de la víctima para manipular la sesión del usuario en segundo plano. De esta forma, la transacción fraudulenta se realiza desde la máquina de la víctima, lo que dificulta la detección de soluciones antifraude al final del banco»,* dijeron los investigadores.

Además, un actor de amenazas también puede solicitar información específica que se solicita durante una transacción bancaria, como una contraseña de un solo uso, evitando de esta forma la autenticación de dos factores.

Finalmente, Grandoreiro se rastreó en una campaña extendida en Brasil, México, Portugal y España desde 2016, permite a los atacantes realizar transacciones bancarias fraudulentas utilizando las computadoras de las víctimas para eludir las medidas de seguridad utilizadas por los bancos.

El malware se aloja en páginas de Google Sites y se entrega a través de sitios web comprometidos, Google Ads o métodos de phishing, además de utilizar el Algoritmo de generación de dominio (DGA) para ocultar la dirección C2 utilizada durante el ataque.

> *«Los delincuentes brasileños están creando rápidamente un ecosistema de afiliados, reclutando cribercriminales para trabajar en otros países, adoptando MaaS (Malware como Servicio), y agregando rápidamente nuevas técnicas a su malware como una forma de mantenerlo relevante y financieramente atractivo para sus socios»*, agregó Kaspersky.

> *«Como amenaza, estas familias de troyanos bancarios intentan innovar mediante el*

> *uso de DGA, cargas útiles cifradas, vaciando procesos, secuestro de DLL, muchos LoLBins, infecciones sin archivos y otros trucos como una forma de obstruir el análisis y la detección. Creemos que estas amenazas evolucionan para apuntar a más bancos en más países*».