ESET CYBERSOC

Mekotio

Troyanos bancarios al acecho

Laboratorio de Investigación

ESET LATAM

Contenido

Mekotio (Win32/Spy.Mekotio) 3
Actividades maliciosas 4
Robo de credenciales bancarias con ventanas falsas 4
¿Cómo funciona? 4
¿Quiénes pueden ser víctimas? 4
Robo de contraseñas en buscadores 4
Reemplazo de direcciones de billeteras de bitcoin 5
Ejemplo de la dinámica 5
Etapas de la infección 7
Ingeniería social 7
Instalación 8
Downloader 8
Persistencia 8
Indicadores de compromiso 9
Persistencia 9
Archivos utilizados 9
Proceso con ícono de Autoit 9
Tráfico de red 10
Hashes, sitios web y C&C 10
Hash 10
Sitios web para almacenar contraseñas robadas 10
Servidores C&C 10
Consejos para protegerse de Mekotio 11

Mekotio (Win32/Spy.Mekotio)

En esta ocasión nos comunicamos desde el laboratorio de ESET Latinoamérica con el fin de informar sobre una amenaza de gran potencial malicioso para aquellos usuarios que utilizan servicios de online-banking y Bitcoin. Se trata del troyano bancario Mekotio, también conocido como BestaFera, que afecta a computadoras con sistema operativo Windows en sus versiones XP, 7, 8 y 10.

Desde su primera detección, en marzo de 2018, los cibercriminales detrás de esta amenaza le han ido aplicando cambios y actualizaciones. Si bien estos cambios han agregado, quitado y/o modificado funcionalidades, el objetivo se mantiene constante: hacer lo posible para obtener dinero o credenciales de acceso a portales de online banking de sus víctimas. Siguiendo esta línea, nuestros análisis han revelado que, entre todas sus variantes, el malware apunta a más de 51 instituciones bancarias.

En sus comienzos, la amenaza apuntaba mayormente hacia usuarios de Brasil. Sin embargo, con el paso del tiempo, la misma fue orientándose principalmente hacia usuarios de Chile. Actualmente, Chile es el país con mayor número de detecciones, por amplia diferencia, seguido por Brasil y México, con un nivel de detecciones medio, y luego por Perú, Colombia, Argentina, Ecuador y Bolivia, que presentan un nivel de detecciones bajo. El resto de los países latinoamericanos no presentaron un nivel de detecciones relevante.

[Nivel de detecciones de Mekotio en países latinoamericanos]

Es importante destacar que un bajo número de detecciones no implica que la amenaza no esté presente en otros países de Latinoamérica. A su vez, debe considerarse que, si los atacantes lo consideraran rentable, podría haber nuevas campañas dirigidas específicamente a los países que actualmente no son alcanzados.

Actividades maliciosas

Al tratarse de una amenaza sostenida en el tiempo y presente en múltiples países, adaptada en versiones específicas dirigidas puntualmente a cada uno de ellos, es normal encontrar cierta variabilidad en las actividades maliciosas llevadas a cabo por las diferentes muestras analizadas. Sin embargo, como hemos mencionado, hay un factor común entre todas ellas: buscan robar dinero y/o credenciales bancarias.

A continuación, describiremos los principales comportamientos maliciosos observados recientemente en estas muestras.

Robo de credenciales bancarias con ventanas falsas

¿Cómo funciona?

El malware analiza constantemente los sitios web a los cuales se accede desde el navegador. En caso de haber ingresado al sitio de alguno de los bancos de interés para los atacantes, el malware mostrará una ventana falsa de ingreso que simula ser la del sitio de la institución financiera. El objetivo es que el usuario ingrese allí sus credenciales de acceso al sistema. Una vez obtenidas, las mismas son enviadas a un servidor remoto dedicado a almacenar la información robada.

¿Quiénes pueden ser víctimas?

A diferencia de otros troyanos bancarios más genéricos, Mekotio está dirigido específicamente a usuarios de un conjunto reducido de países. Para lograr esto, los atacantes crean numerosas variantes del mismo malware; cada versión está dirigida únicamente a un país determinado. Por tal motivo, es usual encontrar muestras que solo están diseñadas para robar credenciales de los bancos presentes en un determinado país y no de los que operan en otros donde también se encuentra la amenaza. Al analizar las muestras dirigidas a Chile, se descubrió que el malware busca robar las credenciales de acceso a los portales de online banking de los 24 bancos con mayor presencia en el país. En el caso de Brasil, la misma dinámica se repite, apuntando a 27 instituciones bancarias.

Gracias a esta dinámica, el alcance de esta funcionalidad no es muy alto, ya que afecta únicamente a los usuarios que se infecten con la variante que apunta al país en el cual viven y que, a su vez, sean clientes de alguno de los bancos seleccionados.

Robo de contraseñas en buscadores

Una peculiaridad que caracteriza a numerosas variantes de Mekotio es la capacidad de robar las contraseñas almacenadas en el sistema por algunos navegadores, como Google Chrome y Opera.

Generalmente, al intentar acceder a un sitio web usando un formulario de log-in, el navegador pregunta al usuario si quiere guardar la contraseña en el equipo y, en caso de autorizarlo, procede a hacerlo. Sin embargo, el mecanismo de seguridad utilizado por estos navegadores no es efectivo en aquellos casos en que el dispositivo ya se encuentra comprometido por un malware. Esto se debe a que la función de cifrado utilizada al guardar la contraseña está diseñada para que dicha información solo pueda ser descifrada por el mismo usuario del sistema operativo que la cifró en primer lugar. Dado que el malware se ejecuta como una aplicación del usuario, puede descifrar las contraseñas fácilmente. Para más detalles sobre el mecanismo utilizado para robar las contraseñas puede dirigirse a este articulo de WeLiveSecurity.

Una vez obtenidas las contraseñas en texto plano, Mekotio las guarda en un archivo y procede a exfiltrarlas a través de un POST a un sitio web probablemente comprometido por los cibercriminales. A partir de este punto, las credenciales del usuario ya se encuentran comprometidas y en poder de los atacantes.

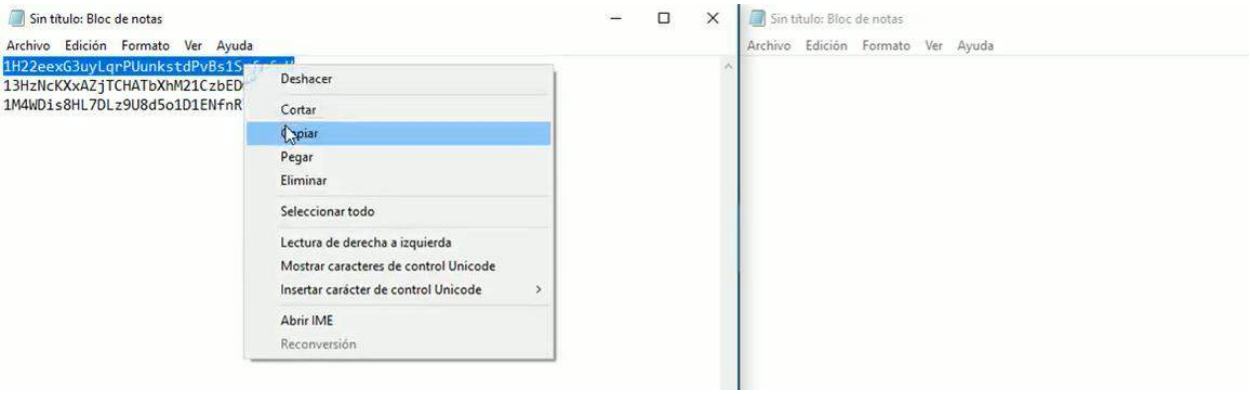
Resulta interesante destacar que estos buscadores almacenan las contraseñas cifradas en una base de datos SQLite3, con lo cual el malware debe tener la capacidad para manejar este tipo de base de datos. En función de este objetivo, Mekotio suele ser distribuido junto con la dll "SQLite3.dll", que contiene todas las instrucciones necesarias para que pueda obtener las contraseñas almacenadas allí.

Reemplazo de direcciones de billeteras de bitcoin

Esta actividad maliciosa consiste en reemplazar las direcciones de billeteras de bitcoin copiadas al portapapeles por la dirección de la billetera del atacante. De esta manera, si un usuario infectado quiere hacer una transferencia o un depósito a una dirección determinada y utiliza el comando copiar (click derecho-copiar / ctrl+c) en lugar de escribirla manualmente, al querer pegar (click derecho-pegar / ctrl+v) no se pegará la dirección a la que pretendía hacerse la transferencia, sino la dirección del atacante. Si el usuario no se percata de esta diferencia y decide continuar con la operación, acabará enviando el dinero directamente al atacante.

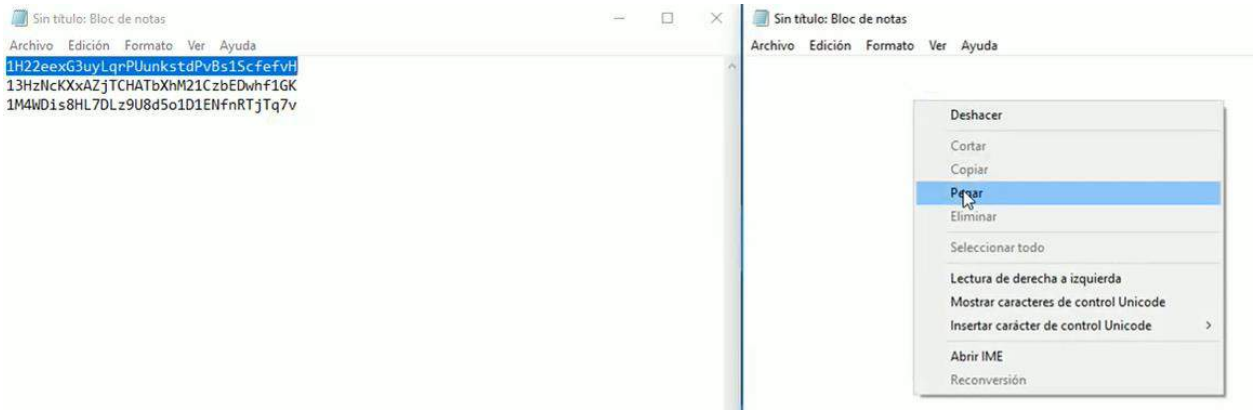
Ejemplo de la dinámica

Paso 1: Un usuario copia la dirección de una billetera de bitcoin en un equipo infectado con Mekotio.



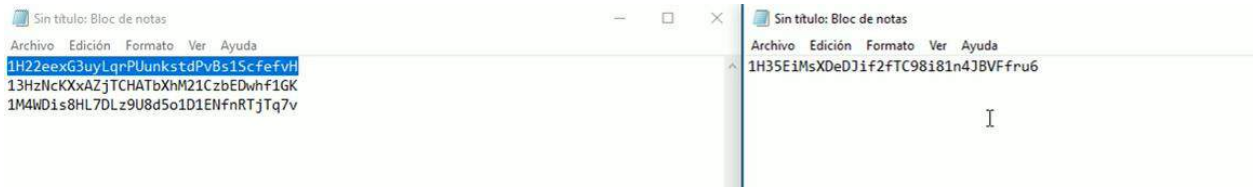
[Se copia la dirección de una billetera de Bitcoin al azar para observar cómo Mekotio la reemplaza en el portapapeles]

Paso 2: El usuario pega la dirección que copió previamente.



[Se utiliza el comando "pegar" para observar cómo Mekotio ha reemplazado la dirección en el portapapeles]

Paso 3: Puede advertirse claramente como la dirección que se pegó en el paso 2 es diferente a la dirección que se copió en el paso 1.



[Puede observarse la diferencia entre la dirección copiada inicialmente y la dirección pegada]

Si bien este mecanismo de robo es muy simple y puede ser contrarrestado fácilmente verificando la dirección a la cual se va a transferir, al revisar el historial de transferencias recibidas por las billeteras del atacante puede concluirse que muchas personas fueron víctimas de esta dinámica.

Cabe destacar que los cibercriminales detrás de Mekotio no utilizan una única billetera para recibir el dinero robado, sino que cuentan con muchas de ellas. Es común que los atacantes cambien esta dirección periódicamente, por lo cual dos muestras con hash diferente podrían contener en su código direcciones diferentes.

Etapas de la infección

[Diagrama con las principales etapas del proceso de infección de esta amenaza]

Ingeniería social

El proceso de infección comienza con una campaña de spam. Los correos enviados abordan diversas temáticas y utilizan la ingeniería social para engañar al usuario y lograr que haga clic sobre el enlace malicioso incluido en el cuerpo del mensaje.


Mon 11/25/2019 12:15 PM

Sii <subscribe@cl.jooble.org>

Sii - Servicio de impuesto internos 18226

To

<http://www.jsrepresentacoes.com/include/009097432/www/>

* <http://www.jsrepresentacoes.com/include/009097432/www/>

1. Home <http://www.jsrepresentacoes.com/include/009097432/www/> /

Estimado(a) ciudadano, Su comprobante solicitado:

<http://www.jsrepresentacoes.com/include/009097432/www/>

Descargar Comprobante <http://www.jsrepresentacoes.com/include/009097432/www/>

[Captura de uno de los emails de spam donde se puede observar la estrategia empleada por los cibercriminales para que el usuario abra el enlace]

Aquí puede observarse claramente la estrategia utilizada para engañar a la víctima: un correo que aparenta provenir de una entidad gubernamental le envía a un ciudadano el comprobante de pago de un impuesto. Esta estrategia suele ser muy efectiva para despertar la curiosidad del usuario, ya que, si éste efectivamente realizó el pago de un impuesto, probablemente esté interesado en guardar el comprobante; si no realizó tal acción, quizá tema que se le haya cobrado algo por error y tenga interés en saber más sobre el asunto. En ambos casos, si el usuario decide abrir el enlace para descargar el supuesto comprobante, ya habrá dado inicio al proceso de infección.

Instalación

Una vez abierto el enlace, comienza la descarga automática de un archivo comprimido .zip. Una vez descomprimido el archivo, nos encontramos con su contenido, un instalador .msi.

Al ejecutar el instalador se llevarán a cabo dos tareas principales:

Downloader

Descarga un archivo .zip adicional, extrae su contenido en la ruta:

> *C:\programdata\[*nombre aleatorio*]*

Este .zip contiene usualmente 4 archivos:

> **Intérprete de autoit *<.exe>***
> Se trata del intérprete oficial de autoit. Su finalidad es ejecutar las instrucciones del script que se distribuye junto a estos archivos.
> **Script de autoit *<.au3>***
> Contiene instrucciones para cargar la dll de Mekotio y ejecutar una de las funciones que esta exporta.
> **Mekotio *<.dll>***
> Esta dll contiene todo el código que llevará a cabo las actividades maliciosas previamente mencionadas.
> **SQLite3 *<.dll>***
> Contiene las instrucciones necesarias para que Mekotio pueda robar las contraseñas cifradas almacenadas por los buscadores (ataque descrito previamente).

Persistencia

Una vez descargados y extraídos los 4 archivos, existen dos opciones, según la variante de Mekotio en cuestión:

- Se escribe una entrada en alguna de las llaves de autorun del registro, añadiendo un comando para ejecutar el malware.
- Se agrega un acceso directo en la carpeta de Startup cuyo parámetro será un comando para ejecutar el malware.

De esta manera Mekotio es ejecutado automáticamente cada vez que se inicia el sistema.

> *Como puede verse, el instalador cumple la función de downloader y, adicionalmente, establece la persistencia de la amenaza en el dispositivo infectado. Un detalle no menor es que, dado que el intérprete de autoit ejecuta el script y el script carga y ejecuta a Mekotio, Mekotio se ejecutará en el contexto del intérprete. Esto es importante ya que puede ser de utilidad para identificar si nuestro equipo se encuentra infectado.*

Indicadores de compromiso

Persistencia

Buscar rastros de los mecanismos utilizados para lograr la persistencia es una de las maneras más efectivas de detectar esta infección, dado que los mismos no son muy sofisticados. Aquí hay dos opciones según la variante de Mekotio que haya infectado el sistema:

- Revisar todas las entradas del registro utilizadas para Autorun.
- Revisar accesos directos en la carpeta de startup.

Tanto el comando utilizado en el acceso directo como el escrito en las entradas de registro deberán hacer referencia a un ejecutable que se corresponderá con el intérprete de Autoit.

Archivos utilizados

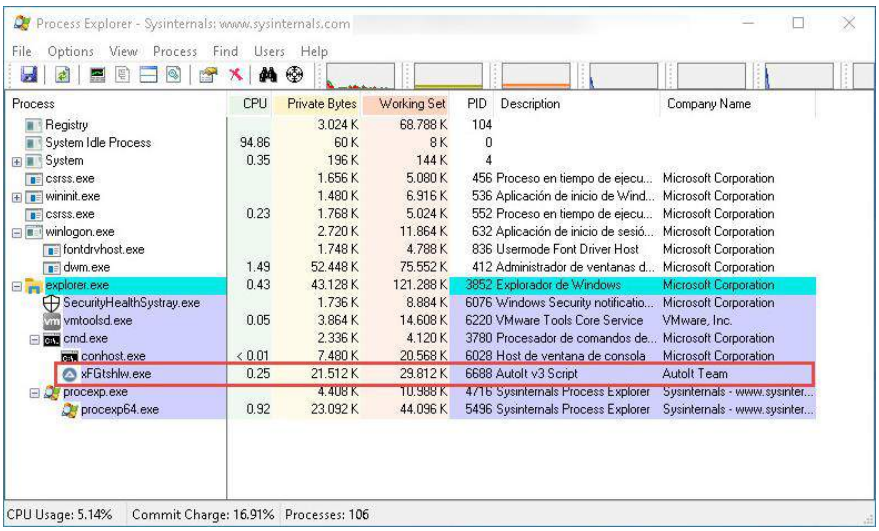
Mekotio utiliza varios archivos para almacenar las contraseñas robadas o como indicadores en base a los cuales modifica su comportamiento:

- C:\Users*nombre del usuario**nombre del interprete AI*.jkl
- C:\Users*nombre del usuario**nombre del interprete AI*.exe.jpg
- C:\Users*nombre del usuario*\Bizarro.txt
- C:\Users*nombre del usuario*\V.txt
- C:\Users*nombre del usuario*\Ok.txt
- C:\Users*nombre del usuario*\Etc

Cabe destacar que la mayoría de estos archivos no coexisten, con lo cual encontrar uno solo ya es motivo suficiente para tener sospechas de una infección y analizar el equipo en profundidad.

Proceso con ícono de Autoit

Si se encuentra un programa con el logo de Autoit y un nombre de apariencia aleatoria (letras sin sentido) siendo ejecutado en nuestro sistema, es muy probable que el equipo esté infectado. Esto puede verificarse utilizando algún software visor de procesos activos, como “Process explorer”.



[Captura de la ventana de Process Explorer, donde se listan los procesos en ejecución. Puede observarse el correspondiente a Mekotio siendo ejecutado en el contexto del intérprete de Autoit]

En líneas generales, no es posible visualizar este proceso en el administrador de tareas de Windows, ya que Mekotio utiliza mecanismos para evitar ser listado en él.

Tráfico de red

El tráfico de red entre Mekotio y su C&C implica un frecuente intercambio de mensajes que poseen una estructura muy definida:

*<|*Comando*|>*

Este formato es respetado tanto por los comandos enviados por Mekotio como por los comandos enviados por el C&C.

Algunos ejemplos de comandos utilizados por esta amenaza	
<|vhxboj|>	<|lozyw|>
<|WGSGTNU|>	<|SuaykRJ|>
<|tksN|>	<|SuaykJI|>
<|VOTM|>	<|ztUjzwtR|>
<|LSTU|>	<|IXjzwtR|>
<|Gpsxi|>	<|utypzjI|>
<|ZKXAKYWQKEHUGZJ|>	<|WGSGTNU|>

Los intercambios son iniciados por el equipo infectado. Éste envía un comando seguido de información robada sobre sistema, por ejemplo: sistema operativo, usuario, software de seguridad instalado, etc.

La característica más importante para el usuario del equipo infectado es que parte de ese tráfico viaja sin cifrar. Por lo tanto, si se observa la presencia de strings similares a estos comandos en el tráfico de nuestra red, será conveniente realizar los análisis correspondientes para descartar una infección.

Hashes, sitios web y C&C

Estos elementos suelen ser buenos identificadores de compromiso. En este caso, sin embargo, tienen una efectividad limitada, ya que los cibercriminales detrás de la amenaza se ocupan de que el período de validez de dichos elementos sea muy corto.

Hash

Las muestras distribuidas suelen contener pequeñas variaciones en su código con el objetivo de que el hash en cada una sea diferente.

Sitios web para almacenar contraseñas robadas

Si bien son utilizados en múltiples muestras, también presentan variabilidad.

Servidores C&C

La dirección IP del C&C es descargada desde un documento público en Google Docs. Los atacantes modifican este documento periódicamente, con lo cual no se utiliza el mismo C&C por periodos prolongados de tiempo.

Consejos para protegerse de Mekotio

Los usuarios que utilizan servicios de online-banking y residen en los países con mayores niveles de detecciones deben mantenerse más alertas. Esto no significa, sin embargo, que quienes se encuentran en países que aún no han sido alcanzados por estas campañas no deban tener cierta precaución; si los atacantes comienzan a enfocar sus esfuerzos en nuevas regiones, podrían pasar a ser un nuevo blanco de la amenaza.

Es recomendable entonces aplicar buenas prácticas y criterios de seguridad, medidas suficientes para evitar ser víctimas de Mekotio. Algunas de las más importantes, con relación directa a esta amenaza, son:

- No abrir enlaces contenidos en correos no deseados.
- No descargar archivos adjuntos en correos no deseados.
- En caso de que un archivo comience a descargarse automáticamente, no abrirlo.
- Ser prudentes al descargar y extraer archivos comprimidos .zip/.rar de fuentes no confiables, ya que suelen ser utilizados para ocultar malware y esquivar ciertos mecanismos de seguridad.
- Ser especialmente prudentes a la hora de descargar/ejecutar instaladores .msi o ejecutables .exe, verificando su legitimidad y sometiéndolos al análisis de un producto de seguridad.
- Contar con un producto de seguridad actualizado.
- Mantener el software de los equipos actualizados.

En cada uno de los puntos mencionados, el objetivo es cortar alguno de los pasos del proceso de infección e instalación. De lograrlo, Mekotio no llegaría a ejecutarse.

Factores	Detalles
Existencia de personal para la respuesta a incidentes	Puede estar compuesto por un equipo o ser posiciones unipersonales.
Existencia de documentación específica sobre los sistemas presentes y redes.	Permite determinar el inventario de activos y los procedimientos y ficheros de configuración.
Evaluación de la existencia de informes sobre la actividad.	Permite obtener información específica de redes y sistemas. De esta manera, es posible diferenciar la operatoria normal de la anormal, a fin de detectar actividades no deseadas.