MEMORIA

ANÁLISIS DE MALWARE

Laura Quijorna Velázquez

27 de Julio de 2023

El presente trabajo trata del análisis de un malware para el que se han empleado las herramientas Virus Total, Joe Sandbox, Tria.ge y Any.run.

A continuación, se detalla la interpretación de los datos extraídos.

DATOS GENERALES:

Se ha analizado el siguiente fichero:

- MD5: c756bd728a07726e9e92529b4be0b3ce
- SHA-1: 32bd8d19833ff2a406befa44b156148bd42f7303
- SHA-256: cb9b591fb411abb5ba554f6679775eea77df4b035618f679e5bf11cccf215574
- SSDEEP: 6144:Z8pJxC9ZBkhD5GsFNJdA6NZ+BPFMMUcMUDyu5Wp2i7UdSGZRW:GpJxVvNbp8PViUd
- TLSH: T155546C56F7A80961C4A7C17ED592A7A2EAF0B8401F2047C703518B7E5E33BF5EA39712
- Nombre: file.exe
- Tipo: PE32+ executable (GUI) x86-64, for MS Windows
- Tamaño: 292.00 KB (299008 bytes)
- Timestamp del PE: 2009-07-13 23:31:55 UTC

ANÁLISIS ESTÁTICO:

- Estructura del PE::
    - .txt
    - .data
    - .pdata
    - .rsrc (posee una entropía de 7.2 por lo que es posible que contenga un packer)
    - .reloc

      *Entropía: es un algoritmo específico que devuelve un valor entre 0 y 8 donde los valores cercanos a 8 indican que los datos son muy aleatorios, mientras que los valores cercanos a 0 indican que los datos son muy homodulos. La entropía puede ser un buen indicador para detectar el uso de empaquetado, compresión y cifrado en un archivo. Los archivos legítimos suelen tener una entropía entre 4,8 y 7,2, en

cambio, los archivos con una entropía superior a 7,2 tienden a ser maliciosos.

- **Reglas Yara:**
  Las reglas yara son una herramienta de código abierto que fue desarrollada por la plataforma VirusTotal para identificar los elementos de un malware por medio de un análisis estático automatizado.

    - Yara detected Fabookie

- **Reglas Sigma:**

  Estas reglas se pueden utilizar para detectar una amplia variedad de ataques y amenazas, incluyendo ataques de phishing, ransomware, malware, exploits de vulnerabilidades y tráfico malicioso.

    - Change PowerShell Policies to an Insecure Level - PowerShell:
      Detects use of Set-ExecutionPolicy to set insecure policies
      (El cambio es efectivo inmediatamente. No es necesario reiniciar PowerShell).

    - Suspicious Get-WmiObject (infraestructura para la gestión de datos y operaciones que permite la gestión local y remota de ordenadores personales y servidores Windows).

- **Reglas Ids**

  En algunas situaciones, el servicio de detección de intrusiones (IDS) puede detectar la comunicación entre routers u otros dispositivos de red internos como un posible ataque. Por ejemplo, puede agregar la dirección segura conocida a las direcciones excluidas de la zona del IDS para que evada el IDS.

    - Matches rule ET MALWARE Win32/Fabookie.ek CnC Request M4 (GET) at Proofpoint Emerging Threats Open.
    - Matches rule FILE-MULTIMEDIA Microsoft Windows Transport Stream Program Map Table Heap overflow attempt at Snort registered user ruleset.
    - Matches rule MALWARE-CNC Win.Trojan.Dropper outbound connection at Snort registered user ruleset.

- Matches rule PROTOCOL-ICMP Unusual PING detected at Snort registered user ruleset.
- Matches rule FILEEXT JPG file claimed at Suricata
- Matches rule PROTOCOL-ICMP PING Windows at Snort registered user ruleset
- Matches rule PROTOCOL-ICMP PING at Snort registered user ruleset
- Matches rule PROTOCOL-ICMP Echo Reply at Snort registered user ruleset
- Matches rule FILE-EXECUTABLE Portable Executable binary file magic detected at Snort registered user ruleset.

- Importación de librerías dinámicas.

  Las librerías dinámicas son archivos que contienen código ejecutable que puede ser compartido y utilizado por múltiples programas. Al importar DLLs, el malware puede aprovechar funciones y rutinas ya existentes en el sistema operativo o en otras aplicaciones para llevar a cabo sus objetivos. Se han importado las siguientes librerías:

  - VERSION.dll
  - GDI32.dll
  - ADVAPI32.dll
  - KERNEL32.dll
  - msvcrt.dll
  - OLEAUT32.dll
  - MFC42u.dll
  - SHELL32.dll
  - ntdll.dll
  - ole32.dll
  - ATL.DLL
  - USER32.dll

- Contiene 17 recursos todos en ingles US tipo:

  - RT_ICON (13) → Este recurso se utiliza para almacenar iconos en formato de mapa de bits (.bmp) en un archivo ejecutable. Los iconos son gráficos pequeños utilizados para representar visualmente una aplicación, un archivo o una carpeta. Los archivos ejecutables pueden

contener varios tamaños de iconos, y el recurso RT_ICON los almacena para que la aplicación pueda mostrar el icono correspondiente en la interfaz gráfica de usuario y en el explorador de archivos.

- RT_GROUP_ICON (1) → Este recurso se utiliza para almacenar un grupo de iconos en un archivo ejecutable. Un grupo de iconos consiste en varios tamaños y profundidades de color del mismo icono, lo que permite que la aplicación seleccione el icono más adecuado según las necesidades del sistema y la pantalla donde se ejecuta.

- REGISTRY (1) → Este recurso puede hacer referencia a configuraciones o información almacenadas en el registro del sistema. El registro es una base de datos jerárquica utilizada por el sistema operativo Windows para almacenar configuraciones, opciones, información de hardware y software, y otros datos relevantes del sistema. Un malware podría utilizar este recurso para almacenar sus propias configuraciones o información, o para manipular claves de registro existentes para mantener su persistencia o realizar acciones maliciosas.

- MUI (1) → Las siglas "MUI" significan "Multilingual User Interface" (Interfaz de usuario multilingüe). El recurso MUI se utiliza para almacenar traducciones y recursos de idiomas en aplicaciones. Con el recurso MUI, una aplicación puede tener interfaces de usuario localizadas en varios idiomas diferentes. Un malware que incluye recursos MUI podría tener capacidad para adaptarse a diferentes idiomas, lo que podría ser útil para propagarse y engañar a los usuarios en distintos países.

- RT_MANIFEST (1) → Este recurso almacena un archivo de manifiesto, que es un archivo XML que contiene información sobre la aplicación,

sus requisitos de sistema, dependencias y políticas de ejecución. El manifiesto es utilizado por el sistema operativo para asegurarse de que la aplicación se ejecute correctamente y cumpla con los requisitos de configuración. En el contexto de malware, el recurso RT_MANIFEST podría ser utilizado para indicar cómo la aplicación debe comportarse en diferentes sistemas o configuraciones, o para engañar al sistema operativo y evitar su detección.

- **Motores AV:**
    - VT: Detectado por 50/71 antivirus
    - Joe Sandbox: Detectado por 88/100 antivirus

ANÁLISIS DINÁMICO

Ejecución:

- Potencial función criptográfica detectada:

033606E8	488DAC24E0F5FFFF	lea rbp, qword ptr [rsp-00000A20h]	0x0000000000000650
033606F0	4881EC200B0000	sub rsp, 0000000000000B20h	
033606F7	4C8BF1	mov r14, rcx	
033606FA	33D2	xor edx, edx	
033606FC	41B808020000	mov r8d, 00000208h	
03360702	488D8DD0030000	lea rcx, qword ptr [rbp+000003D0h]	0x0000000000000A20
03360709	E84F58FDFF	call 0338B4D0h	target: 0338B4D0
0336070E	488D85D0030000	lea rax, qword ptr [rbp+000003D0h]	0x0000000000000A20
03360715	4889442420	mov qword ptr [rsp+20h], rax	

Esto es un indicativo de que el archivo malicioso está utilizando técnicas de cifrado o ofuscación para ocultar su código o comportamiento malicioso. Los atacantes a menudo utilizan la criptografía como una táctica para evadir la detección de soluciones de seguridad y dificultar el análisis de su malware.

- El PE contiene un checksum que no coincide con el esperado.

```
Static PE information: real checksum: 0x490c5 should be: 0x51b52
```

El checksum es un valor numérico que se utiliza para verificar la integridad de un archivo y asegurar que no ha sido modificado accidental o maliciosamente.

Cuando un archivo ejecutable se crea, se calcula un valor de checksum basado en los contenidos del archivo. Cualquier cambio en el archivo, incluso una modificación menor, cambiará el valor del checksum. Si el valor del checksum almacenado en el archivo no coincide con el valor calculado del checksum en el momento de la ejecución, se considera que el archivo ha sido alterado y puede indicar una posible manipulación o corrupción del mismo.

En este caso, el mensaje indica que el archivo ejecutable tiene un valor de checksum almacenado de 0x490c5, pero debería ser de 0x51b52 según el valor calculado. Esto significa que el archivo ha sido modificado o alterado desde su creación original, ya que el valor del checksum almacenado no coincide con el valor esperado.

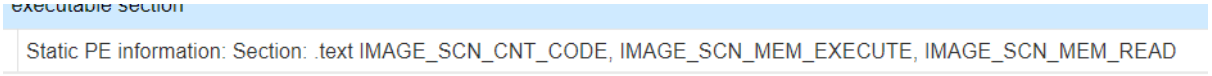
Las posibles causas de que el checksum no coincida con el valor calculado en un malware son:

- ➢ Ofuscación y modificación para cambiar el contenido del archivo sin alterar su funcionalidad principal. Estos cambios pueden incluir inserción de código malicioso, encriptación de secciones del archivo o incluso reordenamiento de instrucciones para evitar patrones de detección.
- ➢ Técnicas de polimorfismo para cambiar su código constantemente, lo que hace que cada instancia del malware sea única y difícil de detectar por las soluciones de seguridad basadas en firmas. Esto puede resultar en diferencias en el checksum cada vez que se genera una nueva variante del malware.
- ➢ Inyección de código en tiempo de ejecución para modificar el archivo ejecutable en memoria sin alterar el archivo en disco. Esto puede llevar a discrepancias en el valor del checksum almacenado en el archivo.
- ➢ Para evitar la detección, los malwares pueden cifrar o comprimir su carga útil dentro del archivo ejecutable. Cuando el malware se ejecuta, descifra o descomprime su contenido en memoria, lo que hace que el

archivo en disco tenga una estructura diferente y, por lo tanto, un valor de checksum diferente al valor esperado.

➢ Para auto-modificarse en función del entorno del sistema o del análisis de seguridad que enfrentan. Esto podría resultar en cambios en el archivo ejecutable que afecten al valor del checksum.

- El archivo PE tiene una sección .text ejecutable y ninguna otra sección ejecutable.



El formato de archivo PE es el formato de archivo ejecutable utilizado por el sistema operativo Windows. Este formato define la estructura y diseño de los archivos ejecutables, bibliotecas de enlace dinámico (DLL) y otros archivos relacionados con la ejecución de programas en Windows.

En el contexto del análisis de malware, las secciones de un archivo PE son bloques lógicos de datos que contienen diferentes tipos de información, como código ejecutable, datos, recursos, tablas de importación y exportación, entre otros. Estas secciones ayudan a organizar y estructurar el contenido del archivo ejecutable.

El hecho de que un archivo PE tenga una única sección ".text" ejecutable y ninguna otra sección ejecutable puede ser una característica sospechosa desde el punto de vista de la seguridad y el análisis de malware. A continuación, se presentan algunas consideraciones sobre lo que esto podría implicar:

- **Técnica de empaquetamiento**: Algunos malwares utilizan técnicas de empaquetamiento o compresión para ocultar su código malicioso. En estos casos, el archivo podría contener solo una sección ejecutable (generalmente llamada ".text") que contiene el código malicioso empaquetado. Esta técnica dificulta el análisis inicial del malware.
- **Técnica de inyección de código**: Algunos malwares inyectan su código malicioso en secciones legítimas ejecutables de otros archivos. En este caso, la sección ".text" podría haber sido modificada para contener el código malicioso inyectado y, por lo tanto, ser la única sección ejecutable en el archivo.
- **Intenciones ocultas**: Al tener solo una sección ejecutable, el malware puede estar tratando de evitar detecciones de seguridad o análisis de

malware, ya que las secciones ejecutables son áreas críticas y a menudo se analizan en busca de comportamientos sospechosos.

- Descifrado de cadena potencial encontrado/funciones de asignación:

Code function: String function: 032E5358 appears 68 times
Code function: String function: 032FCBD0 appears 96 times
Code function: String function: 032E557C appears 79 times
Code function: String function: 032E502C appears 43 times

- Contiene funcionalidades para llamar a funciones nativas:

Code function: 0_2_00007FF6C06F2138 RtlInitUnicodeString,NtDeleteValueKey,NtClose,
Code function: 0_2_00007FF6C06F31E0 RtlInitUnicodeString,NtOpenFile,RtlFreeHeap,RtlFreeHeap,NtClose,
Code function: 0_2_00007FF6C06F21BC RtlInitUnicodeString,NtQueryValueKey,HeapAlloc,NtQueryValueKey,HeapAlloc,memmove,NtClose,RtlFreeHeap,
Code function: 0_2_00007FF6C06F424C NtQuerySystemInformation,HeapAlloc,NtQuerySystemInformation,memmove,RtlFreeHeap,

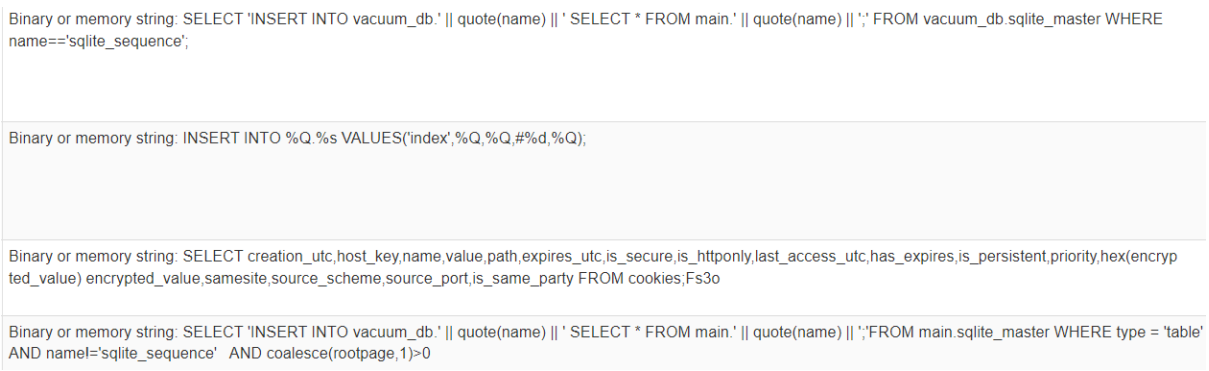
Estas funcionalidades tienen objetivos maliciosos y pueden utilizarse para:

- Realizar tareas que requieren niveles más altos de acceso, como la manipulación del registro, la comunicación a bajo nivel con hardware, el acceso a la red o la inyección de código en otros procesos.
- Ocultar sus actividades maliciosas y mezclarse con procesos y actividades legítimas del sistema. Al utilizar funciones comunes del sistema operativo, el malware puede evitar ser detectado por soluciones de seguridad que buscan comportamientos maliciosos específicos.
- Establecer persistencia en el sistema, asegurando que se ejecute cada vez que el sistema se inicie. Esto permite que el malware mantenga el control del sistema incluso después de reinicios.
- Intentar explotar vulnerabilidades en el sistema operativo o en otros programas para ganar acceso privilegiado o propagarse a otros sistemas en la red.
- Interactuar con el entorno del sistema, como leer y escribir archivos, acceder al registro, manipular procesos y servicios, entre otros. Esto

permite al malware llevar a cabo sus acciones maliciosas y realizar cambios en el sistema para su beneficio.

- Camuflarse entre procesos y actividades legítimas, dificultando su detección por parte de soluciones de seguridad que se centran en comportamientos anómalos.

- Cadenas SQL encontradas en memoria:



Los lenguajes SQL son ampliamente utilizados para interactuar con bases de datos y realizar operaciones como consultas, inserciones, actualizaciones o eliminaciones de datos. Que el malware tenga cadenas SQL en memoria, significa que puede estar utilizando consultas SQL para interactuar con bases de datos o sistemas de almacenamiento. Esto podría indicar que el malware está tratando de extraer o modificar información en bases de datos, como credenciales de usuario, datos confidenciales o información relevante para su funcionamiento.

Comportamiento:

Abuso de intérpretes de comandos y scripts para ejecutar comandos, scripts o archivos binarios.

- Cargas útiles maliciosas mediante la carga de módulos compartidos. Esto lo realiza cargando archivos DLL desde rutas locales y de red arbitrarias. Estas librerías son utilizadas para la inyección de código a través de la API de Windows.

`OpenProcessToken@ADVAPI32.dll`
`OpenProcess@KERNEL32.dll`
`VirtualAlloc@KERNEL32.dll`
`CreateThread@KERNEL32.dll`
`NtOpenProcessToken@ntdll.dll`

- Modifica servicios para ejecutar contenido malicioso y también para ejecutarlo de manera reiterada y así generar persistencia.

`OpenSCManagerW@ADVAPI32.dll`

`EnumServicesStatusW@ADVAPI32.dll`

`OpenServiceW@ADVAPI32.dll`

`ChangeServiceConfigW@ADVAPI32.dll`

`QueryServiceConfigW@ADVAPI32.dll`

- Modificación de permisos de archivos y directorios:

  Los adversarios pueden modificar los permisos/atributos de archivos o directorios para evadir las listas de control de acceso (ACL) y acceder a archivos protegidos.

- Igualmente genera persistencia vía Run a través del registro de claves. Lo que consiguen con esto es lograr la persistencia agregando un programa a una carpeta de inicio o haciendo referencia a él con una clave de ejecución del Registro. Esto hará que el archivo malicioso se ejecute automáticamente al inicio de sesión de usuario teniendo el nivel de permisos asociado de la cuenta.

  SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
  Software\Microsoft\Windows\CurrentVersion\Run
  SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- Utiliza la manipulación de Tokens de acceso para la escala de privilegios.

`OpenProcessToken@ADVAPI32.dll`
`AdjustTokenPrivileges@ADVAPI32.dll`

Los tokens de acceso son estructuras de datos que contienen información sobre la identidad y los derechos de un usuario o proceso en un sistema operativo.

Los tokens de acceso se utilizan para determinar qué recursos y acciones están permitidos para un usuario o proceso en particular. Un token de acceso contiene información como el identificador de seguridad del usuario, su grupo de pertenencia y los privilegios asignados. Los privilegios incluyen acciones como el acceso al sistema de archivos, la capacidad de modificar configuraciones, la capacidad de interactuar con ciertos servicios y más.

Al manipular los tokens de acceso, el malware intenta obtener mayores privilegios de los que inicialmente tiene para realizar acciones que normalmente no estarían permitidas. Esto es especialmente peligroso si el malware se ejecuta con privilegios limitados, como un usuario estándar, y busca elevar esos privilegios a nivel de administrador o de superusuario.

- Para obtener las credenciales de acceso realiza captura de entrada mediante el registro de teclas.

Métodos de evasión

- Enmascaramiento: Se enmascara dentro de un archivo que parece legítimo con el fin de ocultarse y evadir las defensas.

Source: C:\Users\user\Desktop\file.exe	File created: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\imagc[1].jpg

- Hace Sleep para evitar el análisis dinámico:

	Source: C:\Users\user\Desktop\file.exe TID: 7420	Thread sleep count: 57 > 30	
	Source: C:\Users\user\Desktop\file.exe TID: 7420	Thread sleep time: -17100000s >= -30000s	

- Se encontró una cadena de API evasiva (puede detener la ejecución después de acceder a las claves de registro):

Evasive API call chain: RegOpenKey,DecisionNodes,Sleep

- Desofusca/Decodifica archivos o información: Los adversarios pueden usar archivos o información ofuscados para ocultar artefactos de una intrusión del análisis.

Descifrado de cadena potencial encontrado/funciones de asignación		
Source: C:\Users\user\Desktop\file.exe	Code function: String function: 032E5358 appears 68 times	
Source: C:\Users\user\Desktop\file.exe	Code function: String function: 032FCBD0 appears 96 times	
Source: C:\Users\user\Desktop\file.exe	Code function: String function: 032E557C appears 79 times	
Source: C:\Users\user\Desktop\file.exe	Code function: String function: 032E502C appears 43 times	

- Archivos o información ofuscada: Los adversarios pueden intentar dificultar la detección o el análisis de un archivo ejecutable mediante el cifrado, la codificación o la ofuscación de su contenido en el sistema o en tránsito. Este

es un comportamiento común que se puede usar en diferentes plataformas y en la red para evadir las defensas.

Uses code obfuscation techniques (call, push, ret)	
Source: C:\Users\user\Desktop\file.exe	Code function: 0_2_0333536C push 8B44C033h; retf

PE file contains an invalid checksum	
Source: file.exe	Static PE information: real checksum: 0x490c5 should be: 0x51b52

Métodos anti-debugging (mecanismos mediante los cuales un software puede detectar si está siendo ejecutado bajo la supervisión de un depurador).

- Contiene funcionalidad para comprobar si se está ejecutando un depurador (IsDebuggerPresent).
- Contiene funcionalidad para acceder a la funcionalidad del cargador (LdrGetProcedureAddress, RtlInitUnicodeString,LdrGetDllHandle,RtlInitAnsiString).
- Contiene funcionalidad para registrar su propio controlador de excepciones (etUnhandledExceptionFilter).
- Contiene funcionalidad para determinar dinámicamente las llamadas a la API (GetModuleHandleW,GetProcAddress,LoadLibraryW,GetProcAddress,GetLastError).
- Contiene funcionalidad que puede usarse para detectar un depurador (GetProcessHeap, HeapAlloc,GetProcessHeap,HeapFree).

Acceso a Credenciales

- Intenta recolectar y robar información del navegador (historial, contraseñas, etc.)

Source: C:\Users\user\Desktop\file.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\1e941ceb871c74c91b6a6f309b6eaa19
Source: C:\Users\user\Desktop\file.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
Source: C:\Users\user\Desktop\file.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies

- Contiene funcionalidades para robar contraseñas o cookies de Chrome

Source: C:\Users\user\Desktop\file.exe	Code function: \Google\Chrome\User Data\Default\Login Data
Source: C:\Users\user\Desktop\file.exe	Code function: \Google\Chrome\User Data\Default\Login Data

- Credenciales en archivos: Los adversarios pueden buscar sistemas de archivos locales y recursos compartidos de archivos remotos en busca de archivos que contengan credenciales almacenadas de forma insegura. Estos pueden ser archivos creados por los usuarios para almacenar sus propias credenciales, almacenes de credenciales compartidas para un grupo de personas, archivos de configuración que contienen contraseñas para un sistema o servicio, o archivos binarios/de código fuente que contienen contraseñas incrustadas.

Descubrimiento

- Contiene diversas funcionalidades para extraer información:
    - ❖ Información local

Code function: EnumSystemLocalesW,
Code function: EnumSystemLocalesW,
Code function: GetLocaleInfoW,GetLocaleInfoW,GetACP,
Code function: EnumSystemLocalesW,GetUserDefaultLCID,ProcessCodePage,IsValidCodePage,IsVa
Code function: EnumSystemLocalesW,
Code function: TranslateName,TranslateName,GetACP,IsValidCodePage,GetLocaleInfoW,
Code function: GetLocaleInfoW,

    - ❖ Hora local/del sistema

```
GetSystemTimeAsFileTime,GetCurrentThreadId,GetCurrentProcessId,QueryPerformanceCounter,
```

- ❖ Zona horaria

```
_get_daylight,GetTimeZoneInformation,
```

- ❖ Información del sistema

  GetSystemInfo
  Enumerate services
  Query environment variable
  Get system information on Windows
  Get memory capacity
  Get disk information

- ❖ Enumerar procesos o subprocesos (posiblemente lo haga para saber si el sistema es virtualizado)

```
Code function: 0_2_02F406D8 SHGetFolderPathW,GetDesktopWindow,GetWindow,GetWindowThreadProcessId,CreateToolhelp32Snapshot,Module32FirstW,IsWindowVisible,SendMessageW
,CloseHandle,GetWindow,Sleep,SleepEx,
```

- Lee las políticas de software:

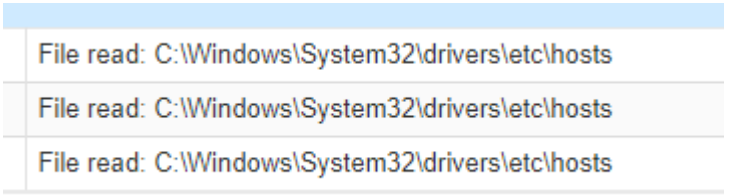
```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
```

Las políticas de software son configuraciones y directivas establecidas en el sistema que controlan el comportamiento de diferentes programas y servicios. Algunas de las razones por las que el malware puede leer las políticas de software son las siguientes:

- Evitar ser detectados y bloqueados por la seguridad del sistema identificando las configuraciones de seguridad y restricciones establecidas en el sistema.
- Buscar vulnerabilidades o debilidades en la configuración del sistema. Esto le permite explotar esas vulnerabilidades para ganar acceso privilegiado o eludir las defensas de seguridad.
- Obtención de información del sistema para adaptar sus ataques o propagarse de manera más efectiva.

- Recopilación de información sensible como credenciales almacenadas, configuraciones de red o datos de usuarios, que puedan ser útiles para sus actividades maliciosas.
- Determinar oportunidades de ataque o puntos débiles en el sistema, ya que las políticas de software pueden revelar si ciertos servicios o aplicaciones están permitidos o restringidos en el sistema.
- Establecer persistencia incluso después de reinicios y actualizaciones.

- Lee el archivo de hosts locales para descubrir las asignaciones de nombre de host a dirección IP de sistemas remotos.



El archivo de hosts es un archivo de configuración en los sistemas operativos, como Windows o Linux, que se utiliza para asociar nombres de dominio con direcciones IP específicas. Cuando un usuario intenta acceder a un sitio web, el sistema primero verifica el archivo de hosts local antes de realizar una consulta al servidor de nombres (DNS) para obtener la dirección IP correspondiente.

Al leer el archivo de hosts, un malware puede tener diferentes intenciones maliciosas:

- **Redirección de tráfico**: Modificar el archivo de hosts permite al malware redireccionar el tráfico de los usuarios a sitios web legítimos a servidores controlados por los atacantes. Esto podría utilizarse para robar información confidencial, como credenciales de inicio de sesión, o para mostrar contenido falso y engañar a los usuarios.
- **Bloqueo de sitios web**: Al agregar entradas al archivo de hosts que apunten a direcciones IP no válidas o locales, el malware puede bloquear el acceso a ciertos sitios web, incluidos sitios de seguridad y antivirus, para evitar que el usuario descargue actualizaciones o acceda a información que pueda ayudar a detectar o eliminar el malware.

- **Distribución de malware**: Al modificar el archivo de hosts, el malware puede redirigir solicitudes de actualización o descarga de software legítimo a sitios que contienen versiones maliciosas de esos programas, lo que permite la instalación de malware adicional o actualizaciones maliciosas.

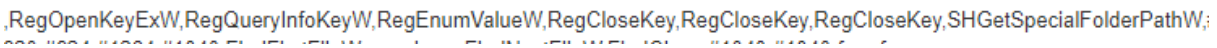
- **Bypass de seguridad**: Al agregar entradas al archivo de hosts, el malware puede evitar que el sistema realice consultas DNS legítimas a servidores de nombres, lo que podría permitir eludir ciertas medidas de seguridad que dependen de la resolución de nombres de dominio para bloquear o monitorear sitios maliciosos.

- **Camuflaje y persistencia**: Al leer y modificar el archivo de hosts, el malware puede utilizarlo para camuflar su presencia en el sistema, lo que dificulta su detección y eliminación. También puede establecer entradas persistentes en el archivo para asegurar que sus redirecciones y acciones maliciosas se mantengan incluso después de reinicios o actualizaciones del sistema.

- Descubrimiento de archivos y directorios:

  Enumeración de archivos y directorios para obtener cierta información dentro de un sistema de archivos. Con esta información los adversarios durante el descubrimiento automatizado pueden dar forma a los comportamientos de seguimiento, incluso tomar la decisión de si se infecta o no completamente al objetivo y/o intenta acciones específicas.

  ➢ Contiene funcionalidad para enumerar/listar archivos dentro de un directorio.



- Descubrimiento de la ventana de la aplicación:

  Los adversarios pueden intentar obtener una lista de las ventanas de aplicaciones abiertas, ya que éstas pueden transmitir información sobre cómo se utiliza el sistema. Por ejemplo, podría usarse para identificar datos potenciales para recopilar, así como para identificar herramientas de seguridad para evadir.

  ➢ Encuentra ventana gráfica

- Registro de consultas:
  Los adversarios pueden interactuar con el Registro de Windows para recopilar información sobre el sistema, la configuración, la seguridad y el software instalado.

Recopilación:

- Keylogging → Registra pulsaciones de teclas mediante sondeo.

  Los adversarios pueden registrar las pulsaciones de teclas del usuario para interceptar las credenciales a medida que el usuario las escribe.

Acciones registradas:

Claves de registro: crear claves de registro en el sistema pueden ser con el objetivo de asegurar su persistencia, evitar detección y realizar acciones dañinas.

- Claves de registro abiertas:

  Un malware puede abrir claves de registro por diversas razones maliciosas y podrían llevarse a cabo para fines específicos:

  - Verificar configuraciones: Al abrir claves de registro, el malware puede verificar la configuración actual del sistema y obtener información relevante sobre el hardware, software instalado y configuraciones de red. Esta información puede ser utilizada para adaptar su comportamiento y tomar decisiones sobre cómo llevar a cabo sus acciones maliciosas de la manera más efectiva.
  - Inyección de código: Al abrir ciertas claves de registro, el malware podría inyectar su propio código o cambiar los valores existentes para desviar la ejecución de programas legítimos o sistemas operativos hacia el código malicioso, permitiendo así que el malware tome el control del sistema o realice acciones indeseables.
  - Verificación de persistencia: Al abrir ciertas claves de registro, el malware puede comprobar si ya se ha establecido previamente en el sistema y si está configurado para ejecutarse automáticamente en cada inicio del sistema. Esto le permitiría asegurarse de que persistirá en el sistema incluso después de reinicios o intentos de eliminación.

- Comunicación y actualización: Al abrir claves de registro, el malware puede buscar información sobre servidores de comando y control, protocolos de comunicación o actualizaciones del propio malware. Esto facilita la comunicación con los servidores de los atacantes y permitiría que el malware reciba nuevas instrucciones o actualizaciones para mejorar su funcionalidad.
- Camuflaje: Al abrir ciertas claves de registro, el malware puede intentar camuflarse como una aplicación legítima o un servicio del sistema, ocultando así su presencia y dificultando su detección por parte de soluciones de seguridad.
- Preparación para ataques futuros: Al abrir claves de registro, el malware puede realizar cambios en la configuración del sistema para prepararse para futuros ataques o facilitar el movimiento lateral a través de la red.

HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections

HKCU\Software\iksaa23

HKCU\Software\iksaa23\it

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet\

HKLM\Software\Microsoft\Tracing

HKLM\Software\Microsoft\Tracing\hbkmrtp_RASAPI32

HKLM\Software\Microsoft\Tracing\hbkmrtp_RASMANCS

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

- Registro de conjunto de claves de registro:

  El registro de claves de un malware puede suponer para llevar a cabo una serie de acciones como mantener persistencia, ocultar su presencia, realizar configuraciones específicas, modificar configuraciones del sistema, deshabilitar servicios de seguridad, robar información y para propagarse a otros sistemas conectados y llevar a cabo ataques dirigidos.

  HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

  HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet\{A8B1B530-930D-4F5A-B04B-4C388594DD4B}

  HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

  HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable

  HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer

- Claves de registro eliminadas:

  Un malware puede eliminar claves de registro por varias razones maliciosas como: eliminar rastros, desactivar servicios de seguridad, romper funcionalidades del sistema y favorecer reinfecciones.

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass

Impacto

- Shutdown system (apagado): Los adversarios pueden apagar/reiniciar los sistemas para interrumpir el acceso o ayudar en la destrucción de esos sistemas. Los sistemas operativos pueden contener comandos para iniciar un apagado/reinicio de una máquina o dispositivo de red. En algunos casos, estos comandos también se pueden usar para iniciar un apagado/reinicio de una computadora remota o un dispositivo de red

  Esta acción también puede suponer interrumpir el acceso a los recursos informáticos para los usuarios legítimos y, al mismo tiempo, impedir la recuperación de incidentes y acelerar los efectos previstos en el sistema.

Procesos y servicios

- Árbol de procesos:

  2056 - wmiadap.exe /F /T /R

  2240 - %windir%\system32\wbem\wmiprvse.exe

  2280 - 87420f6e5c4d3abb650fae89b8d43e58.exe

  2316 - %WINDIR%\system32\ping.exe

  2320 - %WINDIR%\system32\wbem\wmiprvse.exe

2344 - %windir%\System32\svchost.exe -k WerSvcGroup

2392 - C:\tpyh\hbkmrtp.exe

2724 - %SAMPLEPATH%

2812 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}

3640 - %WINDIR%\system32\audiodg.exe

368 - %WINDIR%\system32**svchost.exe** → Proceso de servicio compartido que Windows usa para cargar archivos DLL.

3928 - %WINDIR%\system32\find.exe

3932 - %WINDIR%\system32\cmd.exe

3948 - %WINDIR%\system32\conhost.exe

3988 - %WINDIR%\system32\ipconfig.exe

4008 - %WINDIR%\system32**taskhost.exe** → Se trata de un ejecutor de diversas tareas en segundo plano (background). Es un proceso de Windows al que acuden diversas librerías DLL para iniciar tareas que de por sí solas le es imposible ejecutar.

MUTEXES

- Mutexes Creados: El malware crea un mutex con un nombre específico que actúa como un identificador único para asegurarse de que solo una instancia del malware se ejecute en el sistema. Si el mutex ya existe, el malware puede detectar que ya está en ejecución y evitar la duplicación o reinfección del sistema.

  \Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208

  \Sessions\1\BaseNamedObjects\Local\ZoneAttributeCacheCounterMutex

- Mutexes Opened: Abre mutex específico para verificar si ya se ha ejecutado previamente en el sistema. Al abrir el mutex, el malware puede determinar si hay otra instancia en ejecución o si es la primera vez que se ejecuta en el sistema. Esto puede ser utilizado para evitar la duplicación y asegurarse de que solo haya una instancia activa del malware en el sistema.

  \Sessions\1\BaseNamedObjects\Local_!MSFTHISTORY!_

  \Sessions\1\BaseNamedObjects\Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!

  \Sessions\1\BaseNamedObjects\Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!

  \Sessions\1\BaseNamedObjects\Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!

Dropped files

Los dropped files son archivos que son descargados, creados o copiados por un malware en un sistema comprometido como parte de sus actividades maliciosas. Se puede observar como el primer dropped es identificado como malicioso.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\e68b03d8843fb3c48c0037fa2610911e	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 10
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.43613063485556663
Encrypted:	false
SSDEEP:	12:TLqlUlFnGP6Gkwtwhg4FdbXGwvfhowcFOaOmzdOtssh+bgc4Jp+FxOUwa5q0u9z3:TLqlj1czkwubXYFpFNYcw+6UwcYzHr
MD5:	46076967A4692D6323BCBDAD8532DA6A
SHA1:	A2C61F0EAECF8C2D126FCF82828808B78291E582
SHA-256:	BFA77719DCA9C4C92B38BD8A23C9DD751B82DB0F21620E6937C4F97AECC5536B
SHA-512:	B4C03F075B2E4DC527AD25B5D5788BE55D4CBCCA66002884CC75528FC57AF54C494B2219C726999E9A29C5AB05C789DB1412F4A01A8AC61726E2F7B785E77691
Malicious:	true
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....[5.....g...$.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\imagc[1].jpg	
Process:	C:\Users\user\Desktop\file.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1080x1440, components 3
Category:	dropped
Size (bytes):	1506508
Entropy (8bit):	6.926989858619382
Encrypted:	false
SSDEEP:	24576:SMaEt+i3CaSEKFaGWWEfpVk3XFc8ZSK10CGWQw6tsJCetgJlfpsP45:SloigCWERVk3XsgQw6jeU2PY
MD5:	6ED71A5BC6E0C24D6BAD213EFD6D6349
SHA1:	59F252310BD9AACC4E219D3F3B374532C7176B4B
SHA-256:	EFA20F0295EDF9EA8364293CB82F4C408DC89F6F4451A5736BC021D13F449EC8
SHA-512:	1C269614B447C97E21DDC54CA3EBC98FC9D514FE6275F0C84B32CE5B961A7CD0589B37FC4579EE215939C7400CA0961CA61D3FD9B239B81062925AD5062FC3DD
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....C.....C..... .c.....!..."1A.2Q.#BRaq3br.....$4CS...c....%s.....&5DTd..'6EUet....7F.....>.....

ANÁLISIS DE RED

- Las reglas Ids identificaron que el malware hace PING a través del protocolo ICMP. Esta acción puede haberse hecho para identificar si otros dispositivos o sistemas están activos. Esto le permite descubrir otros objetivos potenciales en la red para propagarse, realizar ataques dirigidos o buscar vulnerabilidades para explotar.

- Proveedor de Internet visto en conexión con otro malware:

  ASN Name: HKKFGL-AS-APHKKwaifongGroupLimitedHK HKKFGL-AS-APHKKwaifongGroupLimitedHK

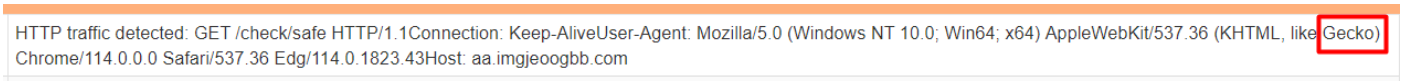
  Se conecta a un sistema de red autónomo para el intercambio de datos. Posiblemente ésta sea la conexión a la botnet.

- Dirección IP vista en conexión con otro malware.

  IP Address: 103.100.211.218 103.100.211.218

  IP Address: 103.100.211.218 103.100.211.218

- Utiliza el User Agent del navegador web Mozilla para la comunicación HTTP:



- Se detectó una o más solicitudes HTTP anómalas algunos dominios no incluidos en la lista blanca:

  PETICIONES HTTP

  - http://aa.imgjeoogbb.com/check/?sid=458556&key=6a9f4dd171076df1c4f5002fc609e90b

    HTTP Method POST
  - http://aa.imgjeoogbb.com/check/?sid=805030&key=fb5dfa7b2938d9dbd712bded5901e088

    HTTP Method POST
  - http://aa.imgjeoogbb.com/check/safe

    HTTP Method GET
  - http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt

    HTTP Method GET

    Response code 200
  - http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c

    HTTP Method GET

    Response code 200
  - http://us.imgjeoigaa.com/sts/imagc.jpg

    HTTP Method GET

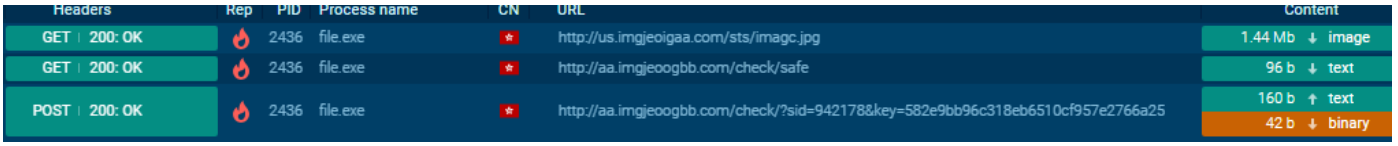
    Response code 200
  - http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt

    HTTP Method GET

    Response code 200
  - http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt

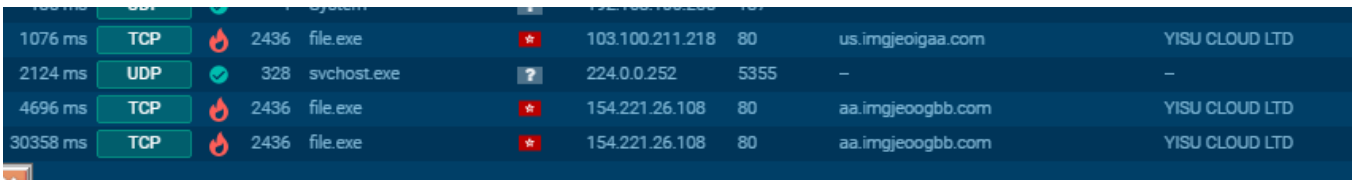
    HTTP MethoD GET

Response code 200



En esta última imagen se puede ver las peticiones http por el método GET a un servidor de nube desde donde realiza descargas probablemente maliciosas, entre ellas, un binario que seguramente sea el malware que se ejecutará en código máquina. También se puede observar como hay un POST que sube información posiblemente robada a la nube (posible botnet).

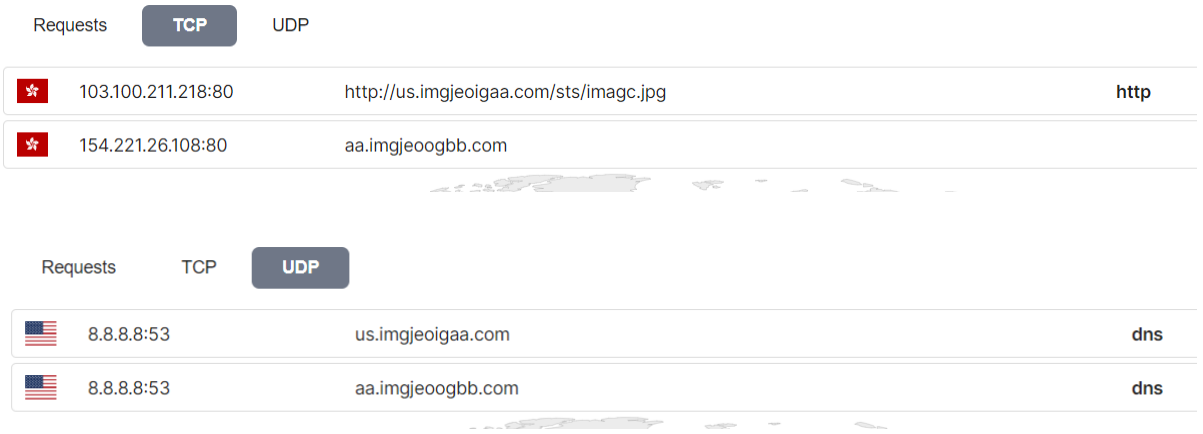
- Resoluciones DNS:
  - aa.imgjeoogbb.com → 154.221.26.108 → Posible botnet.
  - crt.sectigo.com → 104.18.14.101 → Es una autoridad de certificación que emite certificados digitales utilizados para garantizar la seguridad y privacidad de las comunicaciones en línea, ya que cifran los datos transmitidos entre el cliente (navegador) y el servidor.
  - dns.msftncsi.com → 131.107.255.255 → Dominio utilizado por Microsoft para realizar verificaciones de conectividad a Internet en sistemas operativos Windows. Hace la comprobación de conectividad a través de una solicitud DNS al dominio dns.msftncsi.com. Si la solicitud tiene éxito, el sistema asume que tiene acceso a Internet y muestra un ícono de red en la barra de tareas con el estado de conectividad "Conectado".
  - us.imgjeoigaa.com → 103.100.211.218 → Posible botnet.



En esta imagen se puede observar cómo las ips maliciosas corresponden a YISU CLOUD LTD, un proveedor de servicios en la nube. Una botnet puede utilizar una infraestructura en la nube para

llevar a cabo sus operaciones de manera más eficiente y resistente. Al alojar parte de su infraestructura en la nube, los ciberdelincuentes pueden aprovechar la escalabilidad y recursos disponibles para controlar y administrar los dispositivos infectados. Además la nube proporciona un entorno flexible y de alta disponibilidad que permite a los atacantes coordinar sus actividades maliciosas de manera más efectiva.

- TRÁFICO IP por el protocolo TCP/UDP



- Se detectan, por lo tanto, como maliciosas las siguiente ips:

  103.100.211.218:80 (TCP)

  154.221.26.108:80 (TCP)

RECOMENDACIONES

- Mantener el software actualizado: Asegúrate de que tu sistema operativo, navegadores, aplicaciones y programas estén siempre actualizados con las últimas correcciones de seguridad. Los fabricantes lanzan actualizaciones para abordar vulnerabilidades conocidas y mejorar la protección contra las amenazas.

- Utilizar un software antivirus y antimalware confiable: Instalar un software de seguridad que ofrezca protección contra troyanos y otras amenazas de malware. Es importante mantener el antivirus actualizado y ejecuta análisis periódicos del sistema.

- Ser cauteloso con los correos electrónicos y adjuntos: No abrir correos electrónicos sospechosos o no solicitados, especialmente si contienen enlaces o archivos adjuntos desconocidos. Este troyano especialmente puede propagarse a través de correos electrónicos de phishing y adjuntos maliciosos.

- Evitar hacer clic en enlaces desconocidos que lleguen a través de mensajes de correo electrónico, redes sociales o aplicaciones de mensajería.

- Descargar software solo de fuentes confiables, es decir, sitios web oficiales. Evita descargar software pirateado o de fuentes no verificadas.

- Activar el firewall del sistema ya que ayuda a proteger tu sistema al bloquear conexiones no autorizadas y controlar el tráfico de red. Asegurarse de que el firewall esté activado en el sistema operativo.

- Configurar permisos de usuario: Utilizar cuentas de usuario con privilegios limitados para el uso diario y evita utilizar cuentas de administrador para tareas cotidianas. Esto ayudará a reducir el impacto de un posible ataque.

- Habilitar el filtrado de URL: Algunos navegadores y aplicaciones de seguridad ofrecen filtros de URL que pueden bloquear el acceso a sitios web maliciosos o conocidos por propagar malware.

- Realizar copias de seguridad periódicas de los datos importantes en un dispositivo externo o en la nube. En caso de un ataque, podrás restaurar tus archivos sin pagar un rescate.

- Educar a los usuarios del equipo acerca de ciberseguridad especialmente sobre los riesgos de hacer clic en enlaces sospechosos, descargar archivos de fuentes desconocidas y abrir correos electrónicos no solicitados.

CONCLUSIONES

- El malware analizado se trata de un troyano llamado Fabookie.
- Su principal acción es el robo de datos del navegador y robo de credenciales o cookies de Chrome.
- Hace consultas a base de datos SQL malware para extraer y modificar información en bases de datos, como credenciales de usuario, datos confidenciales o información relevante para su funcionamiento.
- Busca credenciales e información comprometida en archivos del sistema.
- Utiliza métodos de evasión (sleep y enmascaramiento).
- Utiliza métodos anti-debugging (IsDebuggerPresent).
- Crea persistencia vía Run a través del registro de claves.
- Se enmascara dentro de un archivo de procedencia legítima.
- Hace registro de pulsación de teclas para obtener las credenciales del usuario.
- Utiliza el protocolo ICMP para buscar conexiones para verificar si puede comunicarse con otros hosts o servidores en la red. Con esto puede que busque expandirse e infectar otros objetivos.
- Utiliza el protocolo TCP/UDP para conectarse con ips maliciosas.