Informe de Malware-*SmokeLoader*

Módulo de Análisis de Malware

Bootcamp Ciberseguridad VII

Indice:

Perspectiva General

-En este informe muestro una evaluación exhaustiva del malware “Smokeloader” clasificado como backdoor que a lo largo del tiempo ha ido incrementado la dificultad de su detección y es capaz de realizar diversas acciones maliciosas.

-La entrada que he creado en MISP tiene el ID: 17 y está creada por el alumno07

- El malware se distribuye de varias formas, los ciberatacantes propagan SmokeLoader usando correos basura (con adjuntos maliciosos). Con frecuencia, el malware intenta ocultar su actividad de command and control generando solicitudes a sitios legítimos como microsoft.com, bing.com, adobe.com, entre otros. Normalmente, la descarga real devuelve un error HTTP 404 pero en realidad aún contiene datos en el Cuerpo de la Respuesta HTTP.

-El análisis realizado consta de varios apartados desarrollados a partir del uso de múltiples herramientas. Para un análisis profundo inicial hice uso de CAPEv2, una herramienta de análisis de malware de código abierto la cual proporciona capacidades para extraer, analizar y clasificar configuraciones y cargas útiles de muestras de malware.

-Para un análisis más detallado utilicé herramientas en la red como LevelBlue/Labs y vmray (entre otras) para obtener distintas configuraciones del malware o una monitorización de los procesos más precisa.

-En cuanto al análisis de red he contado con varias fuentes las cuales proporcionan información importante a través de su comunidad ya que existen múltiples formar de propagación del virus y victimas de él. Entre ellas destacar VirusTotal, AbuseIPDB y Tria.ge.

-Además de este informe, toda la información relevante recogida a cerca del malware ha sido registrada en MISP (Malware Information Sharing Platform). Una plataforma de inteligencia contra amenazas la cual compañías asociadas pueden compartir descubrimientos sobre diferentes muestras de malware, con el fin de agregar dicha información a sus motores antivirus y, de este modo, aumentar la capacidad de detección.

-Mencionar además el estudio sobre MITRE ATT&CK el cual nos ayuda a entender y categorizar las tácticas y técnicas utilizadas por el malware smokeloader. La clasificación de varias observaciones del comportamiento del malware nos permite entender una manera “rápida y sencilla” como actúa en el equipo infectado.

Herramientas y fuentes

Herramientas y Fuentes	**Descripción breve**
Joesandbox	Plataforma de análisis de malware en línea.
AlienVault	Plataforma de seguridad que proporciona inteligencia sobre amenazas.
Any.Run	Entorno de sandboxing interactivo para analizar y ejecutar malware.
VMRay	Plataforma de análisis de malware automatizada.
CAPEv2	Herramienta de análisis de malware de código abierto.
VirusTotal	Servicio en línea que analiza archivos y URLs para detectar malware.
AbuseDB	Base de datos de direcciones IP asociadas con actividad maliciosa.
Tria.ge	Plataforma de inteligencia de amenazas y análisis de malware.

Análisis Estático

-El análisis nos ha permitido obtener varios HASHES:

MD5

- e0e783bba2f8e3f0d2da2bded27eceed
- 33a60439e95f0dfc10016075f97aeb0c
- fc5e9ebe857d45fa5f578593342ede53

SHA1

- a723dea176c400de9bdd169b703eb283032ed2cb
- fb3595f8a5f9c243e5ad108ff11bc5cb2400ec2b
- 6604067c66d1ef3e30c4563d0a8a8b41b9f9ea5c

SHA256

- 076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239
- 0f6db13c0239ca113c19ebeaec8f3243572fd365c3396eff1777115bc08849a1
- 82d763b6cd97ca240a291c90b8de517232b92cbbe5b593549a61547a30eebf19

-Además he análizado 3 Payload, aquí adjunto información al respecto:

Payloads

B65B:

Process: B65B.exe

Path: C:\Users\ama\AppData\Local\Temp\B65B.exe

SHA256:

- 5431d15fdcfaa2c448738b87b3eb11d6f738d023ed28c2ffb36620624c906b61

Eebagga:

Process: eebagga

Path: C:\Users\ama\AppData\Roaming\eebagga

SHA256:

- ddb73e01457127ccdd7a37042989e98a48afb611339dd6170bc22e504fd1188e
- 19ea40154cdc80fe9f0c7fb2a99515005feb732d41eafd798a0abe8191d46494
- 7888187822bc0b570dd0819d318318e2a2a6f628ac90144c9529960b0b26d1a7

288D:

Process: 288D.exe

Path: C:\Users\ama\AppData\Local\Temp\288D.exe

SHA256:

- e4bd90d785cf7073a7318f206603d5fa614e705c6c534c90be3bd0c79e5c5aa6

Comportamiento del malware

El análisis de "SmokeLoader" revela un comportamiento complejo y sofisticado, diseñado para evadir detecciones y realizar múltiples actividades maliciosas. A continuación, se detallan las principales características y funciones identificadas durante el análisis:

Carga y Ejecución de Bibliotecas DLL

El malware utiliza varias bibliotecas dinámicas (DLL) del sistema, esenciales para sus operaciones. Entre las DLLs empleadas se encuentran:

- **KERNEL32.dll**
- **USER32.dll**
- **msimg32.dll**
- **mscoree.dll**

- **ADVAPI32.dll**

Estas bibliotecas permiten al malware interactuar con funciones críticas del sistema operativo, asegurando su persistencia y eficacia.

Archivos Ejecutables Asociados

El análisis identificó varios ejecutables maliciosos asociados con "SmokeLoader", incluyendo:

- **Lameros.exe**
- **Bastard.exe**
- **B65B.exe**

Estos archivos ejecutables son responsables de la carga inicial del malware y la ejecución de sus componentes maliciosos.

Funciones del Sistema

"SmokeLoader" emplea una variedad de funciones del sistema para llevar a cabo sus operaciones. Algunas de las funciones más relevantes incluyen:

- **EncodePointer**
- **GetCPInfo**
- **GetCurrentProcess**
- **GetCurrentProcessId**
- **GetTickCount**
- **GetTimeZoneInformation**
- **GetWindowsDirectoryW**
- **InitializeCriticalSectionAndSpinCount**
- **SetDefaultCommConfigW**
- **SetLocaleInfoA**

Estas funciones permiten al malware recopilar información del sistema, gestionar procesos y configurar el entorno del sistema operativo para su beneficio.

Funciones de Consola

El malware utiliza varias funciones de consola para interactuar con la terminal y manipular el entorno de ejecución:

- **FlushFileBuffers**
- **FreeEnvironmentStringsW**
- **GetCommandLineA**
- **GetConsoleCP**
- **GetConsoleMode**

- **GetConsoleScreenBufferInfo**
- **GetEnvironmentStringsW**
- **GetLocaleInfoA**
- **GetNumberFormatW**
- **GetPrivateProfileStringA**
- **GetStartupInfoW**
- **PeekConsoleInputW**
- **SetConsoleCP**
- **SetFileApisToOEM**
- **TlsFree**
- **TlsSetValue**
- **WriteConsoleInputW**

Estas funciones permiten al malware realizar diversas operaciones en la consola, desde obtener información del entorno hasta manipular entradas y salidas.

Funciones de Memoria

Para gestionar la memoria de manera eficiente, "SmokeLoader" utiliza funciones específicas como:

- **HeapAlloc (memoria)**
- **HeapCreate**
- **HeapFree**
- **HeapSetInformation**

Estas funciones permiten al malware asignar, liberar y gestionar bloques de memoria durante su ejecución.

Funciones de Ventana y Usuario

El malware interactúa con el sistema de ventanas y el entorno del usuario utilizando funciones como:

- **GetActiveWindow**
- **GetUserObjectInformationW**
- **OpenWaitableTimerA**
- **VerLanguageNameW**

Estas funciones facilitan la interacción del malware con el sistema operativo y el entorno del usuario, permitiéndole ejecutar sus operaciones de manera más efectiva.

Otras Funciones

El malware también emplea una serie de funciones adicionales para realizar operaciones específicas:

- **DeleteVolumeMountPointA**
    - Probablemente una función de la API de Windows utilizada para eliminar un punto de montaje de volumen.
- **EnumSystemLocalesA**
    - Otra función de la API de Windows, utilizada para enumerar los locales del sistema en un sistema Windows.
- **InternalName**
    - Posiblemente un recurso o metadato interno de un archivo ejecutable que especifica el nombre interno del archivo.
- **StringFileInfo**
    - Un recurso utilizado en archivos ejecutables de Windows para almacenar información de cadena, como nombres de productos y versiones.
- **english-caribbean**
    - Probablemente un identificador de localización o una etiqueta que indica la variedad del idioma inglés
- **C:\sir64_riyexofavubix-puzadidizopoga25-wowurugibuher\78\b.pdb**
    - Una ruta de archivo que parece ser una ubicación específica en el sistema de archivos de Windows, posiblemente haciendo referencia a un archivo de depuración (PDB) generado durante la compilación de un programa.

Estas funciones permiten al malware llevar a cabo una variedad de operaciones adicionales, desde la manipulación de archivos hasta la gestión de configuraciones regionales y del sistema.

Comunicación y Persistencia

"SmokeLoader" también demuestra capacidades de comunicación y persistencia avanzadas, utilizando direcciones IP y técnicas de ofuscación para mantenerse en el sistema y evitar su detección.

Marco de Mitre

Análisis de la Matriz de MITRE ATT&CK

A continuación, presento un análisis y conclusión para cada apartado de la matriz de MITRE ATT&CK basada en las técnicas y observaciones proporcionadas por Capev2:

1. Discovery (Descubrimiento)

- **T1082 - System Information Discovery**
    - **Observación**: **antivm_generic_diskreg**

    - **Conclusión**: El malware realiza descubrimientos de información del sistema para identificar características del entorno, como información del disco y el registro, probablemente para verificar si está en un entorno virtual o sandbox.

- **T1057 - Process Discovery**
    - **Observaciones**: **enumerates_running_processes**, **antivm_generic_diskreg**, **process_needed**, **process_interest**
    - **Conclusión**: El malware enumera los procesos en ejecución para obtener una visión general de las aplicaciones y servicios activos. Esto le permite identificar procesos críticos, detectar entornos virtuales, y decidir si es seguro ejecutar el código malicioso.
- **T1012 - Query Registry**
    - **Observación**: **antivm_generic_diskreg**
    - **Conclusión**: Consulta el registro del sistema para recopilar información clave y detectar indicadores de entornos virtuales o sandboxes, ayudando a evadir la detección y adaptar su comportamiento según el entorno.

2. Command and Control (Comando y Control)

- **T1071 - Application Layer Protocol**
    - **Observaciones**: **injection_network_traffic**, **procmem_yara**, **explorer_http**, **network_http**
    - **Conclusión**: El malware utiliza protocolos de capa de aplicación, como HTTP, para comunicar y controlar sistemas comprometidos. Esto incluye inyectar tráfico de red, utilizando procesos legítimos (**explorer.exe**) para establecer conexiones y enviar datos, evadiendo así la detección mediante tráfico aparentemente normal.

3. Defense Evasion (Evasión de Defensas)

- **T1036 - Masquerading**
    - **Observaciones**: **explorer_http**, **accesses_public_folder**
    - **Conclusión**: El malware se “disfraza” o se oculta utilizando nombres y ubicaciones de archivos que parecen legítimos, como accesos a carpetas públicas y la suplantación de **explorer.exe**, para evitar ser detectado por los usuarios y las soluciones de seguridad.
- **T1055 - Process Injection**
    - **Observaciones**: **explorer_http**
    - **Conclusión**: Inyecta código malicioso en procesos legítimos para ocultar su presencia y ejecutar su payload con los privilegios del proceso inyectado, dificultando la detección por parte de herramientas de seguridad.
- **T1497 - Virtualization/Sandbox Evasion**

- **Observación**: **antivm_generic_diskreg**
- **Conclusión**: Implementa técnicas para detectar si está ejecutándose en un entorno virtualizado o sandbox, y si se detecta tal entorno, ajusta su comportamiento o se desactiva para evadir el análisis y la detección.

4. Privilege Escalation (Escalamiento de Privilegios)

- **T1548 - Abuse Elevation Control Mechanism**
  - **Observación**: **accesses_public_folder**
  - **Conclusión**: Abusa de mecanismos de control de elevación de privilegios para obtener permisos más altos, permitiendo al malware ejecutar acciones que requieren privilegios administrativos y realizar cambios significativos en el sistema comprometido.

Análisis Dinámico

El análisis dinámico de "SmokeLoader" revela un malware sofisticado que emplea diversas técnicas avanzadas para llevar a cabo sus actividades maliciosas. Durante su ejecución, "SmokeLoader" intenta establecer una conexión a una IP inactiva (190.218.32.77:80) en un único intento, posiblemente buscando contactar con un servidor de comando y control (C2). Además, realiza solicitudes HTTP a la URL "http://humydrole.com/tmp/index.php" mediante el método POST, estableciendo conexiones HTTP desde el proceso "explorer.exe" hacia el dominio humydrole.com:80. Esto sugiere una posible exfiltración de datos o comunicación con un servidor C2.

En su interacción con el sistema de archivos, "SmokeLoader" accede al archivo "C:\Users\Public\Desktop\Acrobat Reader DC.lnk" en la carpeta Pública, lo que podría indicar una manipulación de archivos o actividades de reconocimiento dentro del sistema. Para evadir la detección y dificultar su análisis, el malware utiliza la API "SetUnhandledExceptionFilter" para manejar excepciones no controladas, una técnica común de anti-depuración. Además, verifica las direcciones de los adaptadores de red mediante la API "GetAdaptersAddresses" para detectar interfaces de red virtuales, empleando así técnicas de anti-virtualización.

"SmokeLoader" también demuestra su capacidad para detectar la presencia de software de seguridad y entornos de sandbox, identificando Avast Antivirus y Sandboxie a través de librerías específicas. Realiza una verificación de las unidades de disco en el registro, posiblemente para identificar entornos virtualizados, lo que refuerza su capacidad de evasión.

En cuanto a la manipulación de procesos, el malware enumera los procesos en ejecución, incluyendo "lsass.exe", "svchost.exe" (en múltiples instancias), "winlogon.exe", "services.exe", "explorer.exe", "csrss.exe", "smss.exe" y "wininit.exe". Muestra un interés particular en el proceso "svchost.exe", lo que sugiere un posible intento de inyección de código o manipulación. Utiliza la API "VirtualProtectEx" para crear secciones de memoria con permisos de lectura, escritura y ejecución (RWX), una técnica común para ejecutar código inyectado. Además, se observa que un proceso del sistema genera tráfico de red, probablemente debido a la inyección de procesos mediante la API "WSASend".

Para asegurar su persistencia y ocultar su presencia, "SmokeLoader" elimina su binario original del disco y trata de eliminar cualquier evidencia de que un archivo fue descargado de Internet. Esta estrategia de limpieza subraya su capacidad para evadir la detección post-infección.

Durante el análisis, varias reglas Yara fueron desencadenadas, confirmando comportamientos y patrones asociados con "SmokeLoader". Estas reglas incluyen "shellcode_get_eip", "SmokeLoader", "shellcode_patterns" y "embedded_pe". Finalmente, el análisis realizado por CAPE Sandbox identificó y confirmó la presencia de "SmokeLoader" basándose en firmas específicas de Yara, reforzando la evidencia de las actividades maliciosas del malware.

Análisis de red

El análisis de la muestra de malware, revela que el malware establece varias conexiones con la intención de evitar la detección, lo que añade una capa adicional de complejidad al seguimiento de sus actividades.

Gracias a las herramientas previamente mencionadas y tras indagar a cerca de “smokeloader” a fondo obtuve una relación con las botnet AUTM y PUB1, lo que facilita la comprensión del comportamiento y las estrategias utilizadas por los ciberatacantes. La relación entre SmokeLoader y las botnets AUTM y PUB1 sugiere que este malware no solo se utiliza para infecciones individuales, sino que también puede formar parte de una red más amplia y coordinada de dispositivos comprometidos.

Durante el análisis de red del malware, se han identificado varias direcciones IP que revelan información crítica sobre las posibles actividades maliciosas y la infraestructura utilizada por los atacantes. Cada dirección IP analizada ofrece una perspectiva única sobre los métodos y objetivos del malware.

La dirección IP 192.168.122.6 fue la primera en ser examinada. Tanto VirusTotal (VT) como AbuseIPDB no encontraron ninguna actividad sospechosa o reportes asociados con esta IP, lo que sugiere que puede ser una IP local o interna utilizada durante las pruebas o configuraciones iniciales del malware. Además, es posible que esta IP haya sido utilizada para despistar a los analistas, ya que CAPEv2 había detectado múltiples IPs durante la ejecución del malware, indicando una estrategia para confundir y dificultar la trazabilidad de sus actividades.

En contraste, la IP 192.36.38.33 mostró señales de alerta en dos plataformas diferentes. VT reportó dos avisos, específicamente de "Criminal IP" y "Webroot", indicando actividades criminales y maliciosas. Además, AbuseIPDB registró tres reportes, uno de los cuales menciona que la operadora ferroviaria PT KAI recibió un ataque desde esta IP. Estos hallazgos sugieren que 192.36.38.33 ha estado implicada en actividades hostiles, incluyendo ataques dirigidos.

La dirección IP 178.20.55.16 presentó un perfil aún más preocupante. Con 14 avisos en VT, se vinculó con actividades maliciosas relacionadas con el backdoor Socks5Systemz y ataques de credenciales SSH. AbuseIPDB confirmó que esta IP es un nodo de salida de Tor y ha sido utilizada para abusar del Secure Shell (SSH), con reportes de ataques de fuerza bruta y intentos de acceso a través de RADIUS Login Brute Force Attempt. Esta IP claramente forma parte de una infraestructura de ataque sofisticada y oculta, aprovechando la red Tor para enmascarar sus actividades.

La IP 165.227.174.150 también mostró un comportamiento malicioso significativo. VT listó múltiples alertas de diversas fuentes, incluyendo Xcitium Verdict Cloud, Webroot, SOCRadar, Antiy-AVL, Criminal IP y Abusix, todas etiquetando esta IP como maliciosa, relacionada con phishing y otras actividades dañinas. Sin embargo, AbuseIPDB no encontró reportes asociados con esta IP, lo que podría indicar una falta de reportes de la comunidad o una actividad reciente no suficientemente documentada.

La IP 185.164.14.6 fue otra dirección destacada en el análisis. VT indicó que esta IP estaba involucrada en ataques de fuerza bruta SSH. AbuseIPDB proporcionó un contexto más detallado, señalando que esta IP, perteneciente al rango 185.164.14.0 - 185.164.15.255, estaba relacionada con múltiples tipos de ataques, incluyendo phishing, correos electrónicos no deseados, intentos de acceso no autorizados a servidores y suplantación de identidad. El dominio asociado, mx1.pub.mailpod2-cph3.one.com, fue identificado en estos reportes, resaltando la versatilidad y la naturaleza persistente de las amenazas vinculadas a esta IP.

Finalmente, la IP 93.184.220.29 mostró una actividad maliciosa considerable. Xcitium Verdict Cloud detectó posibles actividades de phishing, y la comunidad de VT la asoció con el troyano Remcos RAT y la botnet Qakbot. Un seguimiento de indicadores de alerta en OTX de AlienVault relacionó esta IP con actividades maliciosas de Qakbot. AbuseIPDB reveló sospechas de muchos usuarios sobre posibles ataques de ransomware y phishing de credenciales de Microsoft, confirmando la reputación maliciosa de esta dirección.

Mitigaciones y recomendaciones

Para protegerse de estas situaciones, es fundamental navegar por internet con precaución y ser meticuloso al descargar, instalar y actualizar software. Examinar cuidadosamente cada adjunto en los correos electrónicos. Si recibimos un correo de una dirección sospechosa o desconocida y el archivo o enlace no tiene relevancia aparente, no es nada aconsejable abrirlo. Es importante tener en cuenta que los anuncios intrusivos suelen parecer legítimos porque los desarrolladores invierten muchos recursos en su diseño. Sin embargo, al hacer clic en ellos, a menudo redirigen a sitios peligrosos como páginas de apuestas, citas de adultos o pornografía. Estos anuncios suelen ser generados por programas publicitarios no deseados.

Para mitigar eficazmente las tácticas y técnicas utilizadas por el malware SmokeLoader, se puede implementar una serie de medidas de seguridad globales que fortalezcan la postura de seguridad del sistema y la red. A continuación, se describe un enfoque integrado y narrativo para abordar las observaciones de descubrimiento, comando y control, evasión de defensas y escalamiento de privilegios:

Estrategia de Mitigación Global contra SmokeLoader

En el complejo y peligroso mundo de la ciberseguridad, la historia de la lucha contra el malware como SmokeLoader se construye sobre la implementación de una defensa en profundidad que abarca múltiples capas de seguridad. Imaginemos un bastión fortificado, cada muro y torre de vigilancia diseñados para anticipar y neutralizar las tácticas del enemigo. Este bastión no solo resiste ataques, sino que también detecta y responde rápidamente a cualquier intrusión.

Primero, nuestro bastión debe conocer su entorno. Para prevenir los descubrimientos maliciosos de información del sistema, es esencial desplegar agentes de monitorización que vigilen constantemente el comportamiento del sistema. Estos agentes actuarán como

centinelas, identificando cualquier intento de recopilar información sobre el hardware, los procesos en ejecución o el registro del sistema. Con alertas en tiempo real, el equipo de seguridad puede responder rápidamente a cualquier actividad sospechosa, asegurando que los atacantes no obtengan la información necesaria para llevar a cabo sus planes.

El siguiente paso en nuestra defensa es proteger las comunicaciones. SmokeLoader utiliza protocolos de capa de aplicación, como HTTP, para establecer comunicaciones de comando y control. Para interceptar estas señales enemigas, se implementan soluciones de inspección profunda de paquetes (DPI) y sistemas de prevención de intrusiones (IPS). Estos sistemas analizan el tráfico de red en busca de patrones anómalos y bloquean cualquier comunicación maliciosa. Además, la segmentación de la red asegura que, incluso si el enemigo logra infiltrarse, sus movimientos estén confinados a una pequeña parte del sistema, limitando el daño potencial.

La evasión de defensas es otro campo de batalla crítico. SmokeLoader se disfraza y oculta su presencia utilizando técnicas de masquerading (estrategias utilizadas por los atacantes para hacer que sus actividades maliciosas parezcan legítimas) e inyección de procesos. Para contrarrestar esto, se utilizan herramientas de monitoreo de integridad de archivos y sistemas de detección basados en comportamiento (Como Wazuh o AIDE). Estas herramientas funcionan como perros guardianes, alertando sobre cualquier cambio inesperado en archivos críticos o comportamientos sospechosos de los procesos. Además, la educación y concienciación de los usuarios es fundamental; al enseñar a los usuarios a reconocer y reportar actividades inusuales, se agrega una capa humana de defensa que es difícil de burlar.

Finalmente, la protección contra el escalamiento de privilegios asegura que incluso si un atacante logra infiltrarse, no podrá obtener el control total del sistema. Mediante la implementación de controles de acceso, solo los usuarios y procesos estrictamente necesarios tienen privilegios elevados. Las soluciones de monitorización detectan y alertan sobre cualquier intento de abuso de estos privilegios. Este enfoque, combinado con la regular actualización y parcheo de sistemas y aplicaciones, fortalece las defensas contra las tácticas de escalamiento de privilegios.