Capítulo 10:

Análisis de las cargas útiles de los correos electrónicos

El capítulo 9 está enfocado en el análisis del propio correo electrónico, mientras que este capítulo le explicará algunos aspectos básicos del análisis de archivos adjuntos y enlaces maliciosos (también denominados "cargas útiles") en los correos electrónicos. La primera parte trata de los sandboxes, una forma cómoda de analizar archivos y enlaces potencialmente maliciosos, y la segunda es una introducción al análisis manual de los archivos, aunque, como se explicará en el capítulo, esto es algo que querrá evitar si puede.

Puesto que este capítulo trata de malware, asegúrese de haber revisado de manera exhaustiva el capítulo 4.

Sandboxes

Un **sandbox** es un programa que proporciona un entorno seguro para que se ejecute un programa informático. El **sandbox de malware** es un tipo particular de sandbox, en el que el malware puede ejecutarse de forma contenida y sus acciones pueden ser analizadas.

El sandbox recomendado en este capítulo le permitirá cargar un archivo para ejecutarlo o conectarse a una URL para cargarlo en un navegador. Luego de un tiempo de análisis, el sandbox le proporcionará un informe de las actividades en la máquina, destacando a menudo cuáles de ellas, en caso de haberlas, son indicativas de un comportamiento malicioso.

Puesto que el malware suele utilizar múltiples etapas, ofuscación y otras técnicas antianálisis, utilizar un sandbox bien ejecutado es a menudo mucho más rápido que realizar un análisis manual. Además, facilita una comprensión de alto nivel del funcionamiento del malware.

Usted podría, en teoría, configurar su propio entorno sandbox mediante el uso de máquinas virtuales: usted crea una máquina virtual (o VM), normalmente ejecutando una versión reciente de Windows, y toma una instantánea, a continuación, ejecuta el malware en esa VM. Pasado un tiempo, usted observa qué ha ocurrido y vuelve a la instantánea.

Sin embargo, este enfoque tiene muchos inconvenientes:

- Si bien una VM le ayudaría a evitar cualquier daño causado por cambios en el sistema operativo, usted lo sigue ejecutando en su propia red. El malware podría encontrar formas de propagarse de una máquina a otra. También se puede conectar a Internet, y si se detectan estas conexiones, su dirección IP podría acabar en una lista de bloqueo. Algunos servicios no le permitirán acceder a ellos desde una dirección IP incluida en una lista de bloqueo.
- Tendrá que verificar manualmente todos los cambios hechos en la VM y decidir si indican un comportamiento malicioso. También tendrá que capturar de algún modo el tráfico de red y ver qué conexiones se están realizando.

- Las técnicas antianálisis a menudo buscan entornos virtuales, en cuyo caso el malware no se ejecutará si detecta alguno. Entre los ejemplos de lo que el malware podría estar buscando en una VM se encuentran las CPU que son típicas de las máquinas virtuales, una imagen de fondo que sea la predeterminada de Windows, un disco duro excesivamente pequeño o muy pocos archivos presentes en el disco duro aparte de los presentes tras la instalación.
- Algunos malware realizan una conexión con su servidor de control, que verifica si ya se ha ejecutado desde esta dirección IP concreta. Si lo ha hecho, no volverá a ejecutarse.

Algunos de estos problemas pueden solucionarse con relativa facilidad. Otros son más complicados, y la lista anterior no es, sin duda, exhaustiva.

Afortunadamente, existen sandboxes que ya están configurados para mitigar estos desafíos. Cuckoo, que es de código abierto, es uno muy popular. Si desea experimentar con la gestión de un sandbox, Cuckoo es un buen lugar para empezar. Fue originalmente desarrollado por personas vinculadas a la comunidad por la libertad en Internet, por lo que está diseñado pensando en la sociedad civil.

Sin embargo, cabe saber que el Cuckoo original, cuya última versión se publicó en 2018, no está en desarrollo activo[1] y, por lo tanto, es poco probable que pueda manejar adecuadamente las amenazas actuales. Un grupo de personas del CERT-EE, el CERT nacional de Estonia, está reescribiendo Cuckoo para Python 3; usted puede seguir su progreso en GitHub, y si se siente aventurero, instale esta versión de Cuckoo, pero debe contar con tener que solucionar bastantes problemas para que funcione.

Una opción mucho más sencilla es utilizar sandboxes basados en la nube. Hay varios disponibles, como ANY.RUN, Hybrid Analysis, Joe Sandbox, Triage e incluso una versión en línea de Cuckoo. Todos tienen versiones gratuitas que le permiten cargar malware y URL, aunque algunos requieren registro[2]. Sin embargo, una advertencia: al igual que con VirusTotal, el uso de uno de estos sandboxes esencialmente hace que el análisis esté disponible públicamente. Si parece probable que el malware haya sido dirigido específicamente a usted, señalar públicamente que lo está analizando podría permitir al atacante saber que lo está investigando.

Cada sandbox tiene sus propias características únicas, pero también comparten muchos rasgos. A continuación le ofrecemos una descripción de Triage, pero le recomendamos que pruebe también otros sandboxes y, si hay alguno que le guste especialmente, se familiarice con su funcionamiento.

Las siguientes capturas de pantalla proceden de un documento malicioso encontrado (sha256:

---

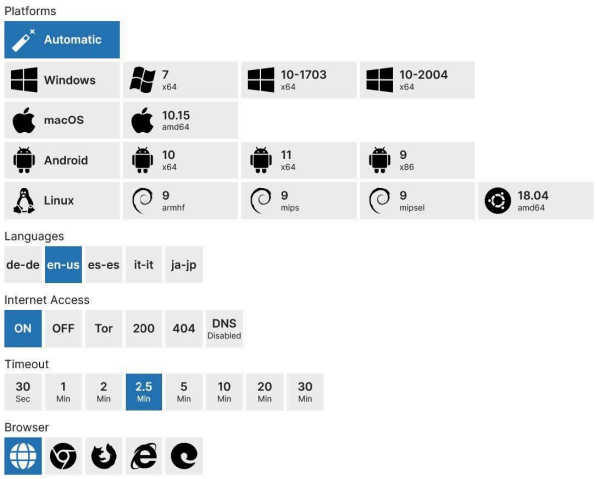
[1] Un problema es que Cuckoo fue escrito originalmente para Python 2, una versión obsoleta de Python.

[2] En el momento de escribir estas líneas, Hybrid Analysis y Cuckoo pueden utilizarse sin necesidad de registrarse, Any.run y Triage requieren un registro gratuito y Joe Sandbox exige el registro y la aprobación de la cuenta.

8404d3dc32b0555bc3b076d7fc080d2a341508b4a2c84805a1d5ffc0057e2b39) en MalwareBazaar, donde lo podrá descargar gratuitamente si lo desea. El análisis sandbox está disponible en la versión pública de Triage.

En Triage, utilice "Submit" en la esquina superior izquierda de la página para cargar un archivo. Algo muy útil es que le permite subir archivos protegidos por contraseña (la contraseña por defecto que intenta es "infected", ¡recuerde que ésta es la norma de la industria que hay que utilizar!), por lo que no tiene que preocuparse de guardar un archivo potencialmente malicioso en su computadora antes de enviarlo.

También puede enviar URL, ya sea para descargar malware directamente desde una URL y luego analizarla o para analizar una URL en un navegador.



En la siguiente página, podrá elegir varios ajustes para el sandbox. La más importante es el sistema operativo. Como puede ver, puede seleccionar varias versiones de Windows, macOS, Android o Linux. Si no elige nada aquí, puede hacer que Triage elija uno o más sistemas operativos por usted, y eso suele funcionar.

También puede elegir el idioma de la máquina. El predeterminado es en-us: Inglés de EE.UU. A veces, el malware dirigido a una región o grupo de personas en particular sólo se ejecuta en máquinas con un idioma concreto. A continuación, puede decidir si desea mantener activado (por defecto) o desactivado el acceso a Internet o conectarse a través de Tor. Una gran cantidad de malware realiza una conexión a un servidor controlado por el adversario, y si esto es una posible preocupación para usted – quizás no quiera avisar al adversario de que lo está investigando – puede intentar ejecutar el sandbox con la conexión a Internet desactivada o configurarlo para que las peticiones web emulen códigos de retorno 200 o 404. Algunos malware realizan una comprobación rápida de la presencia de algunas páginas web para ver si se ejecutan en un entorno sin conexión a Internet; esto simularía dicha conexión. Sin embargo, es posible que algunos malware no se ejecuten.

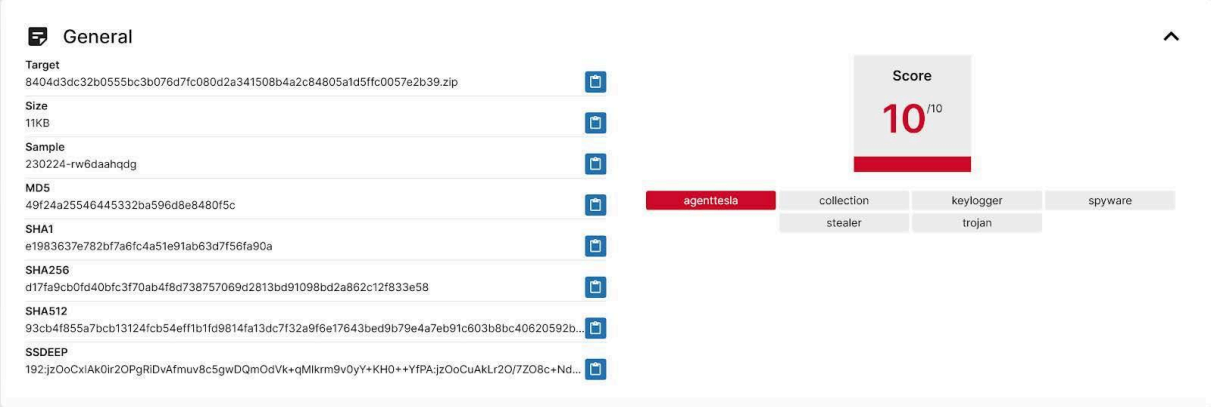
También puede establecer un tiempo de espera: la ejecución se detendrá tras un tiempo sin actividad (2,5 minutos, por defecto). Una técnica antianálisis habitual es que el malware espere algún tiempo antes de realizar cualquier actividad maliciosa, así que en algunos casos, puede que desee aumentar el tiempo de espera.

Por último, puede cambiar el navegador que utiliza el sandbox para abrir sitios web. Esto puede ser útil muy ocasionalmente en caso de que la amenaza potencial que esté analizando sólo se ejecute en un navegador concreto.

Ahora puede empezar a analizar el archivo (o URL), que se abre en el sandbox.

Algo interesante de Triage es que usted puede tanto ver lo que está ocurriendo en el sistema operativo virtual del sandbox – o sistemas operativos: ¡puede ejecutar múltiples análisis en paralelo! – como interactuar con ese sistema operativo. A veces, esto puede ser útil, por ejemplo, si el malware vigila su sistema y registra cuándo se hace clic en un botón. Sin embargo, en la mayoría de los casos, basta con que el sandbox se ejecute en segundo plano.

Cuando el sandbox haya finalizado, podrá ver el análisis. Esto es lo que más le interesa.



La página "Overview" es donde probablemente querrá mirar primero. Le proporciona un resumen del análisis del sandbox. En este caso, vemos que Triage da a nuestra muestra una puntuación de 10 sobre 10 y la etiqueta con el nombre "agenttesla". Agent Tesla es un malware común utilizado para robar información, como datos de acceso, de una máquina infectada. También observará etiquetas como "stealer", "keylogger" y "spyware" que dejan aún más claro que se trata de algo malo.

En la mayoría de los casos, esto será suficiente: usted sabe que el archivo que quería analizar es el Agent Tesla. Hay suficientes análisis del Agent Tesla disponibles en Internet como para hacerse una idea de lo que hace. Como Agent Tesla es bastante común, Triage también sabe cómo extraer la información de configuración del malware y la muestra en la sección "Malware Config".

Pregunta 10.1 Según la configuración extraída del malware, ¿cómo extrae esta variante del Agent Tesla información de una máquina infectada? (Ver la respuesta en el apéndice).

La sección "Targets" le muestra de nuevo que se trata del Agent Tesla, pero también sus actividades maliciosas. Por ejemplo, un proceso incluido en la lista de bloqueo realiza una

solicitud de red y se descarga un archivo "MZ/PE"[3]. Recuerde que el archivo que está analizando es un documento de Office. ¡Es altamente sospechoso que esté intentando descargar archivos!

Esta sección también muestra otras cosas que el malware intenta hacer, por ejemplo, acceder a archivos de configuración FTP y a datos de clientes de correo electrónico y navegadores web. Esa actividad es habitual en los malware que roban información. Incluso si estuviera intentando analizar un malware que el sandbox no reconoció, dicha actividad es altamente sospechosa.

También hay una sección para la "MITRE ATT&CK Matrix". ATT&CK es un "framework" que los analistas de amenazas utilizan como lenguaje común y más fácil de entender para describir y documentar las tácticas y técnicas utilizadas por los adversarios. En el caso que nos ocupa, esta pestaña muestra las técnicas (como la recopilación de correos electrónicos o la modificación del registro) utilizadas por este malware. ATT&CK se diseñó pensando en las empresas y se centra en las amenazas y no en muestras individuales de malware, pero no estará de más echarle un vistazo a las técnicas registradas en esta sección.

La sección "Replay Monitor" le permite reproducir lo que el malware hizo al sistema operativo, lo que es realmente útil para entender lo que ocurrió visualmente. Por último, si el malware intentó bajar algún archivo nuevo de Internet, podrá verlo en la sección "Download" y posiblemente descargarlo usted mismo para realizar un análisis adicional. Tenga en cuenta que estos archivos podrían ser maliciosos, ¡así que manipúlelos con cuidado!

Aparte de la página "Overview", también querrá echar un vistazo a las pestañas del sandbox correspondientes al comportamiento del archivo. En este caso, el archivo se ejecutó tanto en Windows 7 como en Windows 10.

Echemos un vistazo primero a Windows 7. Encontrará la información más interesante en la pestaña "Report". Parte de esto también estaba disponible en la página "Overview", pero notará alguna información extra. Por ejemplo, en la sección "Signatures", dice que el archivo ejecuta Equation Editor y que "Equation Editor es un antiguo componente de Office a menudo objetivo de exploits como CVE-2017-11882". Curiosamente, esta vulnerabilidad se explota con frecuencia para atacar a la sociedad civil wayback machine.

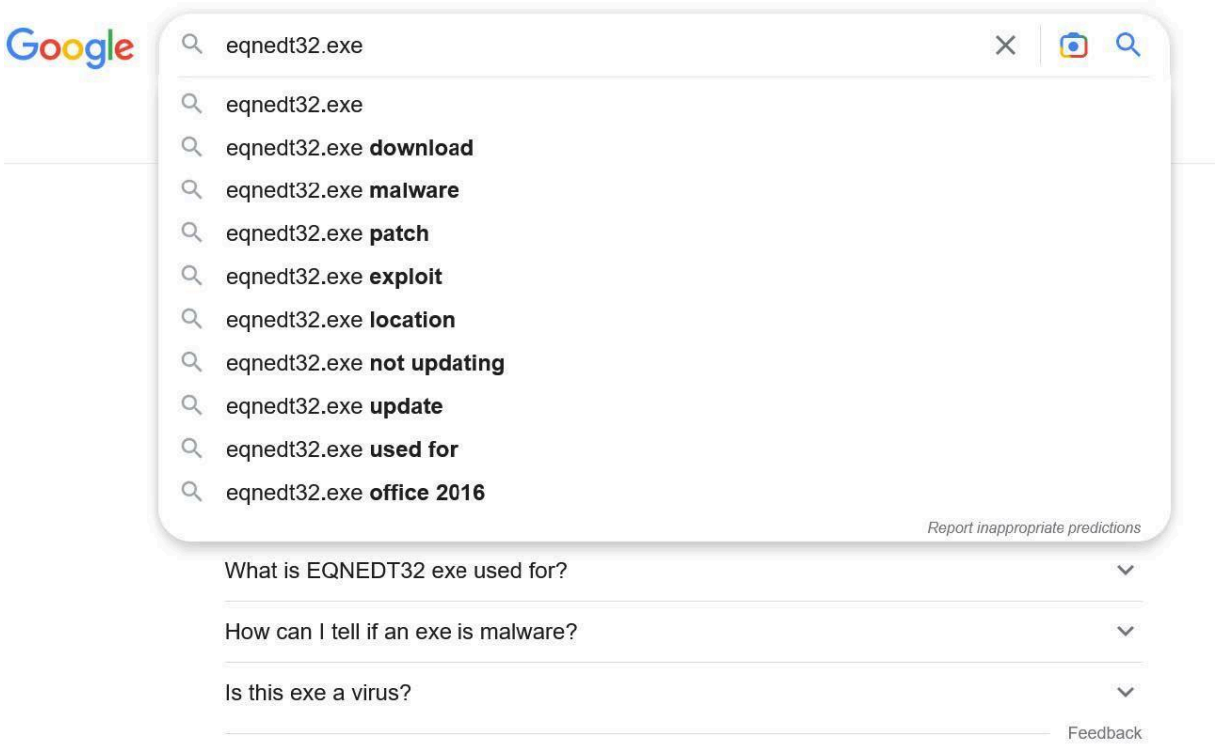
En la sección "Processes", puede ver qué procesos inició el malware después de abrir el archivo. Puede ver que se iniciaron cuatro procesos: WINWORD.EXE, splwow64.exe, EQNEDT32.EXE y arnolded4874.exe – con este último iniciado dos veces. No se espera que usted sepa lo que significa todo esto, pero estos procesos pueden ser útiles a la hora de intentar comprender lo que está ocurriendo.

Un motor de búsqueda le indicará que WINWORD.EXE es Microsoft Word, lo que tiene sentido ya que se trata de un archivo de Word: Word se ejecutaría al abrir el archivo del malware. El segundo proceso, splwow64.exe, también es un programa legítimo y está relacionado con la ejecución de programas de 32 bits en un sistema operativo de 64 bits.

---

[3] PE significa "portable executable" (ejecutable portátil), mientras que MZ son los dos primeros bytes de un archivo PE. Tanto los ejecutables .exe de Windows como las bibliotecas .dll de Windows son ejemplos de este tipo de archivos.

EQNEDT32.EXE también es legítimo, pero si echa un vistazo a las sugerencias de los motores de búsqueda para este archivo, verá que se mencionan con frecuencia "malware" y "exploit", lo que sugiere que se utiliza habitualmente para ejecutar malware. Efectivamente, se trata del anteriormente mencionado Equation Editor.



Por último, hay muy pocos resultados para arnolded4874.exe en Google: en el momento de escribir estas líneas, sólo uno, y es nuestra propia muestra en MalwareBazaar. Un archivo que inicia un proceso con un nombre único, ¡es extremadamente sospechoso!

De hecho, en la siguiente sección, "Network", observamos una solicitud HTTP que se realizó a una URL que contenía este mismo archivo. Así pues, el malware descargó este archivo de Internet y luego lo ejecutó en su sistema virtual. Incluso ignorando todas las señales de alarma anteriores, esta debería ser una muy grande para un documento de Office.

Si estas pestañas no le dieron suficiente información, puede echar un vistazo a las otras pestañas donde puede ver mucha más actividad, como toda la actividad de la red, a qué archivos se accedió y qué claves del registro se leyeron y configuraron. Las claves del registro pueden estar relacionadas con la configuración global de Windows. Hay mucha información aquí, y se necesita experiencia para entender todos los detalles, pero puede encontrar algunas pistas aquí para comprender mejor cualquier comportamiento posiblemente malicioso. Sin embargo, a menudo la pestaña "Reports" le proporciona toda la información que necesita.

Recuerde que la muestra también se ejecutó en Windows 10. Curiosamente, en ese caso no ocurre nada malicioso – observe la puntuación de 1, frente a la puntuación de 10 (sobre 10) de Windows 7.

Hay varias razones posibles para ello. La razón más plausible en este caso es que el exploit no funcionó: CVE-2017-11882 se solucionó a finales de 2017. Windows 10 es de 2020, por lo que incluye el parche que solucionó esa vulnerabilidad.

Ejercicio 10.2 Descargue la muestra

37419d3a8a50d2e5bc0eef676a37d6757ba43a64eff868edb4af5c386900235f de MalwareBazaar y ejecútelo dentro de Triage. Comparta tantos indicadores de comportamiento malicioso como pueda encontrar en la pestaña "Reports".

Ejercicio 10.3 Descargue la muestra a43e0864905fe7afd6d8dbf26bd27d898a2effd386e81cfbc08cae9cf94ed968 de MalwareBazaar y ejecútelo dentro de Triage. Busque indicadores de comportamiento malicioso. Si el análisis no le da una puntuación de 10 sobre 10, ejecútelo de nuevo, pero esta vez, interactúe con la máquina y haga clic en "Next" en la advertencia como le pide OneNote. ¿Cambia esto el comportamiento detectado por el sandbox y la puntuación?

Ejercicio 10.4 *(opcional)* Si utiliza con regularidad otro sandbox en línea, ejecute las muestras de los dos ejercicios anteriores también en ese sandbox. ¿Qué indicadores de comportamiento malicioso encuentra?

Ejercicio 10.5 *(opcional)* Busque algún malware reciente y ejecútelo en un sandbox de su elección para familiarizarse con su funcionamiento. Malware Bazaar es un excelente lugar para encontrar mucho malware nuevo, pero es aún mejor si encuentra un artículo que analice el malware y lo sube: entonces podrá comparar los resultados del sandbox con el análisis del artículo para entender los resultados de su sandbox.

Analizar manualmente los archivos adjuntos

En la sección anterior, aprendió lo útiles que son los sandboxes cuando se trata de analizar archivos adjuntos o enlaces encontrados en correos electrónicos. En la mayoría de los casos, un sandbox le proporcionará toda la información que necesita. Pero a veces, usted querrá comprender mejor un adjunto potencialmente malicioso porque le ayuda a realizar su trabajo o simplemente porque siente curiosidad. Esta sección le ayudará a comprender cómo realizar un análisis manual para explorar más a fondo.

El correo electrónico ha sido un vector habitual para propagar malware desde finales de la

década de 1990 (cuando el malware aún se denominaba virus[4]). Basta con abrir un archivo adjunto de correo electrónico para infectar su computadora, tras lo cual el malware hacía cosas nefastas y utilizaba su cuenta de correo electrónico para enviar una copia de sí mismo a todos sus contactos.

Para los autores de malware, las cosas son mucho más difíciles hoy en día. Los filtros de spam eficaces hacen que sea mucho más difícil enviar un archivo ejecutable[5] de cualquier tipo, incluido el malware[6], a un objetivo. Las computadoras también cuentan con mejores protecciones, como antivirus incorporados, contra archivos maliciosos descargados de Internet o incluidos en archivos comprimidos como los .zip.

Por ello, los creadores de malware han intentado encontrar formas de eludir esta situación. Casi todas ellas implican convencer al destinatario para que actúe, ya sea haciendo clic en un enlace, activando macros o eludiendo de otro modo las normas de seguridad que impiden la infección automática con malware.

Esto convierte la distribución de malware en un juego del gato y el ratón. Los proveedores de seguridad siguen mejorando su detección de nuevos tipos de archivo, y los proveedores de software, como Microsoft, siguen dificultando que su software pueda ser utilizado por el malware. Pero los autores de malware siguen encontrando nuevas formas de distribuir malware.

En consecuencia, su objetivo como alguien que responde a incidentes de seguridad – y el objetivo de este módulo de capacitación – no debería ser saber cómo analizar cada tipo posible de carga útil, sino más bien comprender lo básico y saber dónde buscar si encuentra un nuevo tipo de carga útil.

Los archivos adjuntos y los enlaces son dos formas diferentes en que los atacantes pueden añadir una carga útil (que puede ser maliciosa) a un correo electrónico. Sin embargo, es habitual que un archivo adjunto no contenga nada más que un enlace a la carga útil real o que un enlace descargue un archivo malicioso que es la carga útil real. A veces, un archivo adjunto contiene un enlace que descarga otro archivo más.

Documentos de Office maliciosos

Como ya se ha mencionado, los archivos de Microsoft Office, como los documentos de Word, las hojas de cálculo de Excel y las presentaciones de PowerPoint, pueden contener una o varias macros: fragmentos de código que se automatizan. Existen razones legítimas por las que las organizaciones utilizan macros en este tipo de documentos, pero las macros son populares desde hace tiempo entre los autores de malware.

---

[4] Los primeros virus informáticos se comportaban de forma similar a los virus biológicos, en el sentido de que infectaban archivos legítimos y se ejecutaban una vez que se ejecutaba el archivo "host". En la actualidad, este tipo de virus son extremadamente raros, pero el término "virus" se sigue utilizando a menudo para referirse al malware en sí.

[5] Un archivo que se ejecuta en la computadora. Esto incluiría programas legítimos pero también mucho malware. En Windows, los ejecutables suelen tener la extensión .exe.

[6] En algunos casos, el malware ni siquiera acaba en la carpeta de spam. Los filtros de spam descartan muchos correos electrónicos sin avisar al usuario, especialmente los maliciosos. También pueden eliminar automáticamente los archivos adjuntos maliciosos.

A principios de siglo, las macros se ejecutaban automáticamente al abrir un archivo. Esto dio lugar a gusanos de correos electrónicos masivos: correos con archivos adjuntos que, cuando se abría el archivo adjunto, ejecutaban una macro que enviaba por correo electrónico una copia del archivo adjunto a todas las personas de la libreta de direcciones. Comprensiblemente, Microsoft desactivó la ejecución automática de macros. Durante aproximadamente una década, el malware de macros pareció ser cosa del pasado.

Sin embargo, alrededor de 2014, los autores de malware cambiaron a una nueva táctica que utilizaba la ingeniería social para conseguir que un usuario habilitara las macros: el archivo, por ejemplo, mostraba una página borrosa, y supuestamente era necesario habilitar las macros para mostrar el contenido, a menudo diciendo algo como "por razones de seguridad". Esto se convirtió en un importante vector de infección para muchos tipos diferentes de malware.

Recientemente, Microsoft ha realizado algunos cambios que dificultan que los autores de malware consigan que los usuarios ejecuten las macros, por lo que los autores de malware las utilizan con menos frecuencia. Sin embargo, es posible que siga encontrándoselas en su trabajo.

La mejor herramienta para analizar documentos de Office es oledump.py, una herramienta escrita por el investigador de seguridad belga Didier Stevens (también escribió emldump.py, que utilizamos anteriormente). Está incluida en REMnux, que probablemente usted configuró en el capítulo 6. Si no es así, el vídeo del siguiente ejercicio explica cómo instalarlo.

Ejercicio 10.6 Vea el taller de Didier en YouTube sobre el análisis de documentos maliciosos. Como probablemente tenga instalado REMnux, puede saltarse el primer vídeo sobre la configuración de oledump, pero tenga en cuenta lo siguiente si quiere seguir lo que hace Didier:

- Si quiere ejecutar oledump en REMnux, simplemente ejecute oledump.py seguido de los argumentos, no ./oledump.py como hace Didier[7].
- Preceda los nombres de los plugins con /opt/oledump-files/ ya que se almacenan en ese directorio.
- Este es un taller largo, y le recomendamos que simplemente se siente y vea el vídeo (posiblemente a una velocidad ligeramente superior; puede ser un poco lento) y no se centre en todos los detalles. No pasa nada si no lo entiende o no lo recuerda todo. Sólo asegúrese de que al final, usted sepa:
- Cómo utilizar oledump para mostrar las distintas partes de un archivo de Office (ejercicio 1)
- Cómo utilizar oledump para mostrar las macros VBA integradas en un documento (ejercicio 6)
- Que las macros VBA maliciosas a menudo utilizan ofuscación de código (ejercicio

[7] Si ejecuta un comando en la línea de comandos, Linux busca un archivo ejecutable con ese nombre en uno de varios directorios (el `eco $PATH` le muestra cuáles). Si quiere ejecutar un archivo desde el directorio actual, tiene que añadir ese directorio y, en Linux, el directorio actual viene dado por un único punto. Esto explica por qué en el vídeo, donde oledump está instalado en el directorio local, el comando va precedido de ./

17) y cadenas/URL (ejercicio 20)

- Los comandos de Linux `less` y `head`. Éstos no se explican explícitamente en el taller; esta página web [wayback machine] es una buena introducción si no está familiarizado con ellos.

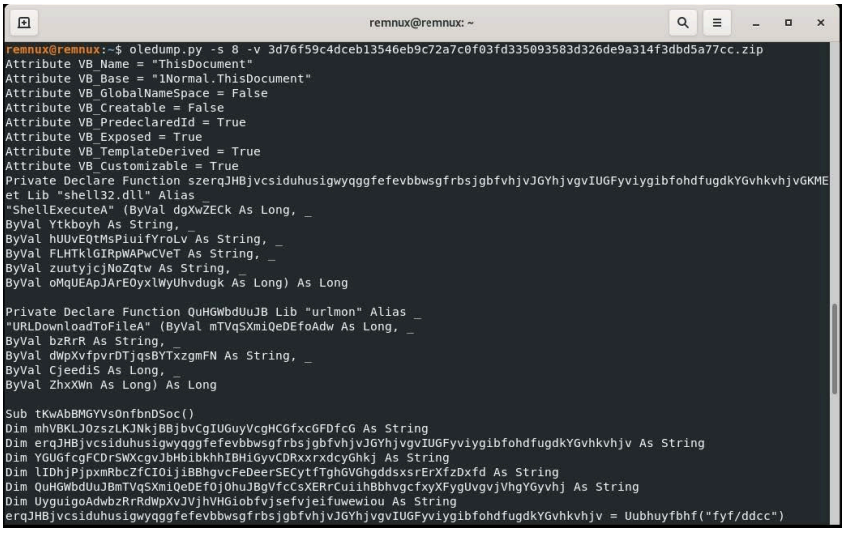
Pregunta 10.7 Didier explica por qué los descargadores suelen ser más beneficiosos para los autores de malware que los droppers. ¿Se le ocurre alguna ventaja de los droppers sobre los descargadores para los autores de malware? (Ver la respuesta en el apéndice).

Ahora, utilicemos oledump en la práctica. Lo haremos sobre el archivo con hash sha256 3d76f59c4dceb13546eb9c72a7c0f03fd335093583d326de9a314f3dbd5a77cc que fue subido a MalwareBazaar justo antes de escribir esta guía. Como es habitual, la descarga es un archivo zip protegido con la contraseña "infected".

MalwareBazaar ya proporciona mucha otra información sobre el archivo que puede ser útil si desea analizarlo. Pero supongamos que encontramos este archivo adjunto a un correo electrónico y no hay información pública disponible sobre él.

Como Didier explicó en sus vídeos, oledump funciona en el archivo zip. Podemos utilizarlo para averiguar si el archivo contiene macros VBA, cosa que hace en la parte 8:

Ahora podemos mostrar las macros:



No todas las macros caben en la pantalla. Si lo ejecuta usted mismo, puede añadir `| less`

al final del comando para ver el resultado completo. Usted puede utilizar la barra de desplazamiento a la derecha de la ventana del terminal para ver más.

Retrocedamos un momento. El creador del archivo utilizó una fuerte ofuscación y macros VBA. Incluso si usted no es programador, esto debería hacerle estar casi seguro de que este archivo es malicioso. Si está realizando su análisis sólo para comprobar si es malicioso, puede detenerse aquí y sacar sus conclusiones. Pero puede que quiera continuar con su análisis para entender más sobre este archivo.

Dado que los descargadores son más comunes que los droppers, busquemos las URL. El plugin `http_heuristics` de Didier no funciona aquí (pruébelo usted mismo para confirmarlo), y eso no es demasiado sorprendente. Si fuera tan fácil extraer una URL del documento, los productos de seguridad lo harían, y podrían cotejar el dominio o la URL con una lista de bloqueo. En consecuencia, los autores de malware ocultan bastante bien las URL y siguen encontrando nuevas formas de hacerlo.

Así pues, busquemos cadenas en el documento: cualquier cosa entre comillas dobles (`"..."`). Hay alrededor de una docena de ellas, pero la mayoría son demasiado cortas para contener una URL ofuscada. La única excepción es la cadena `fyf/higehsvj0tuofuopdeffg0npd/ujmjlufn/xxx00;tquui`.

Ahora puede hacer dos cosas. Puede observar que esta cadena es el argumento de la función Uubhuyfbhf, que se define más adelante en el código. Si entiende un poco de programación, puede deducir lo que hace esta función y observar que, efectivamente, desofusca la cadena hasta convertirla en una URL.

También puede observar la cadena con más detenimiento y notar que una URL comienza con http:// o https://, que tiene una doble t y una doble /. Al final de nuestra cadena, hay una doble u y un doble 0. Si se fija un poco más, observará que tquui deletreado al revés es iuuqt y que https se ha desplazado una letra en el alfabeto.

Si a continuación se da cuenta de que : va seguido de ; en la tabla ASCII y 0 va seguido de /, entonces ha descubierto la codificación: para descodificar la cadena, tenemos que invertirla y luego, para cada carácter, tomar el anterior en la tabla ASCII. Si sabe programar, puede escribir un breve script que haga eso, o simplemente puede desofuscar manualmente la cadena y descubrir que da[8]

`https://www.metkilit[.]com/feedcontents/iurgdfhg.exe`

De hecho, si hubiéramos buscado nuestra muestra en VirusTotal, nos habríamos dado cuenta de que sí se conecta al `www.metkilit[.]com`. Pero recuerde que, en este experimento, fingimos que no se sabía nada del archivo.

Ahora que tenemos una URL que presumiblemente es donde el malware busca descargas, podemos investigar esto más en profundidad si queremos. Más adelante en esta guía,

[8] Recuerde la buena práctica de añadir corchetes alrededor del punto final de un nombre de dominio para "neutralizarlo"; véase el capítulo 7.

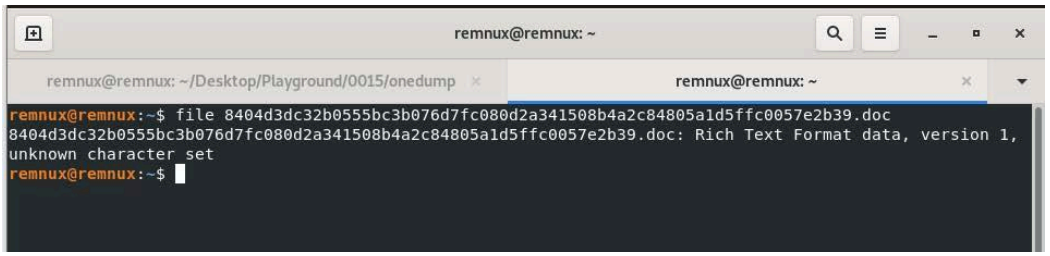
veremos brevemente cómo analizar las URL.

Una cosa es entender cómo funciona la ofuscación de URL. Otra cosa es ser capaz de encontrarla por sí mismo. Para ello se necesitan dos cosas: suerte y experiencia. Suerte porque la ofuscación, en este caso, era bastante sencilla y también porque basta con verla. Cuando se realiza un análisis como éste, siempre es beneficioso trabajar juntos: dos (o más) personas tienen muchas más probabilidades de detectar algún patrón que una sola.

Ahora echemos un vistazo a otra pieza de malware:

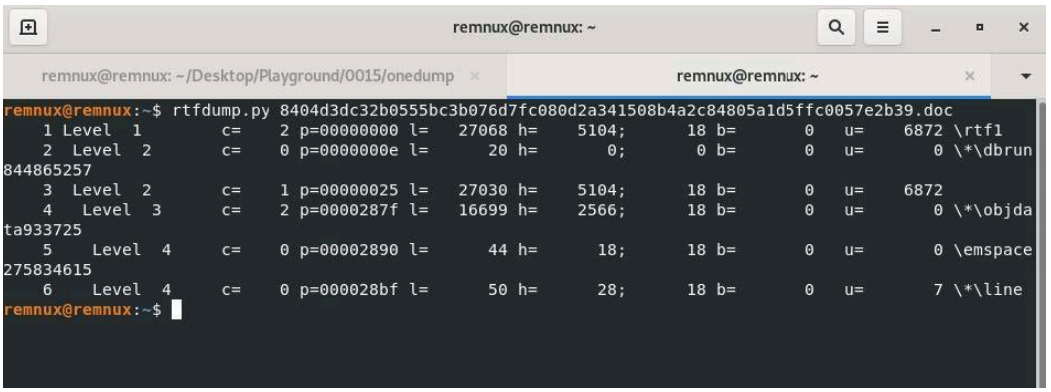
8404d3dc32b0555bc3b076d7fc080d2a341508b4a2c84805a1d5ffc0057e2b39, la muestra que analizamos en Triage más arriba. Si ejecutamos oledump en el archivo zip, obtenemos un error que indica que no es un archivo zip válido. Puede pensar que descomprimir el archivo ayuda[9], pero ejecutar oledump sobre el archivo .doc da el mismo error.

Afortunadamente, Linux dispone de un útil `archivo` de comandos que nos indica que se trata de un archivo en formato de texto enriquecido:



Dichos archivos RTF (que a menudo tienen la extensión .rtf, pero como ve, también vienen como .doc) tienen un formato diferente en comparación con los archivos ordinarios de Word. Afortunadamente, existe otra herramienta que Didier ha escrito y que también se incluye en REMnux: rtfdump.py.

Al igual que oledump, rtfdump le proporciona las distintas partes de las que consta el documento.



De forma similar a oledump, podemos volcar el contenido de cada sección. Por desgracia, a

[9] Recuerde del capítulo 7 que probablemente necesitará ejecutar `7z x [file]` en lugar de `descomprimir [file]`

partir de aquí las cosas no son tan sencillas. Cuando un documento de Office contiene macros VBA maliciosas, el malware es una característica de Office, aunque sea bastante indeseada. Pero en este caso, el malware actúa como un error. Más concretamente, utiliza una vulnerabilidad de Office denominada CVE-2017-11882. Eso hace que el malware sea más difícil de encontrar, además de las dificultades causadas por la ofuscación en el código malicioso.

Para descodificar el malware, un analista probablemente tendría que entender el funcionamiento interno de los archivos RTF y el exploit CVE-2017-11882 e incluso podría tener que adaptar la herramienta rtfdump. De hecho, Didier sigue añadiendo nuevas funciones a sus herramientas en respuesta a nuevos retos como estos.

Ser incapaz de descifrar un malware puede ser frustrante y un poco vergonzoso. Pero también es la realidad del análisis de malware. Una lección importante con este ejemplo es que pudimos analizar el archivo en Triage, lo que nos dio todo lo que necesitábamos. Esto proporciona un argumento extra para utilizar sandboxes en lugar de confiar únicamente en los análisis manuales.

Ejercicio 10.8 *(opcional)* Como referencia, aquí tiene un análisis de un archivo RTF diferente que pudo ser analizado utilizando rtfdump. ¿Puede encontrar el código malicioso dentro del documento RTF utilizando las herramientas de REMnux?

La experiencia se adquiere con la práctica y leyendo lo que hacen los demás. Es un proceso largo, e incluso así, los analistas de malware avanzados se atascan muy a menudo. No deje que eso le desanime, y no sienta que tiene que ser capaz de manejar cualquier archivo adjunto. Incluso los analistas experimentados se atascan con regularidad.

Archivos adjuntos PDF

Los PDF son otros archivos adjuntos comunes. Hubo un tiempo en el que las vulnerabilidades en Adobe Reader, el software de PDF más popular, eran muy comunes. El uso de PDF maliciosos era una forma habitual de infectar dispositivos que ejecutaban una versión ligeramente desactualizada de Reader.

Hoy en día esto es menos común, pero los PDF maliciosos siguen existiendo. A veces, llevan incrustado otro documento, como un documento de Office malicioso. Otras veces, sólo contienen un enlace que descarga la carga útil de la siguiente fase.

De nuevo, Didier Stevens ha creado varias herramientas para el análisis de PDF. También ha creado un taller en vídeo para demostrar algunas de estas herramientas. Sin embargo, este taller es de hace 11 años y se centra principalmente en el tipo de malware PDF que era común en ese momento. Si trabaja habitualmente con archivos PDF, puede que le resulte útil ver el taller, pero considérelo opcional.

La principal herramienta PDF de Didier es pdf-parse.py, que, como su nombre indica, analiza un archivo PDF.

Tomemos de nuevo una muestra descargada de MalwareBazaar:

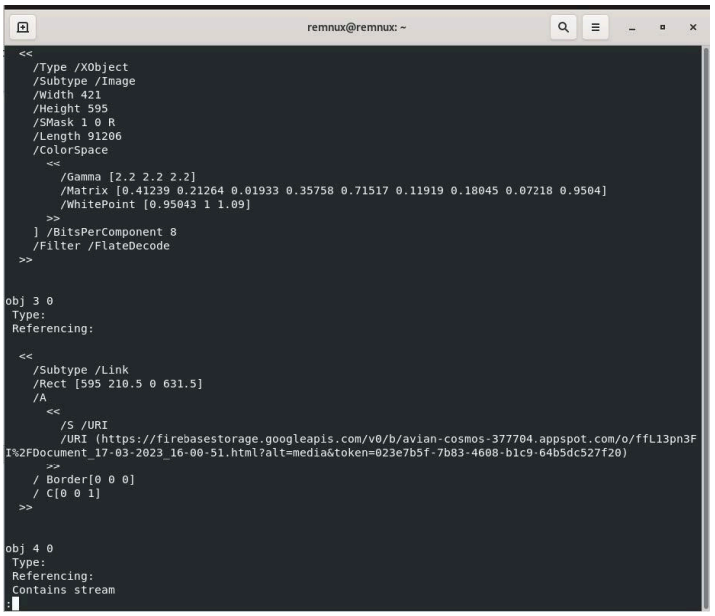
26509fa876a07966824bed8e5b0a6e0626b37d68355871fac49b2fa636d7fe6e.

Primero, ejecutamos:

```
pdf-parser.py

26509fa876a07966824bed8e5b0a6e0626b37d68355871fac49b2fa636d7fe6e.pdf |less
```

en una sola línea para navegar por los distintos componentes del archivo. Fíjese cómo un archivo PDF consta de varios objetos numerados. Si navegamos por los objetos, observamos una URL en el objeto 3, alojada en el almacenamiento Firebase de Google. Se trata de un servicio legítimo (si no lo sabía, una rápida búsqueda en Internet se lo habría dicho), pero comúnmente utilizado para alojar malware.



¡Y ya está! Hemos extraído la URL del PDF, y eso es todo lo que necesita saber. (Para estar seguro, puede comprobar los demás objetos del archivo para confirmar que no hay nada más).

Otro PDF que puede consultar es 907e75030b0e09cec6524f612f1c7439b5260b57b43d515968f81ba69278ba77.

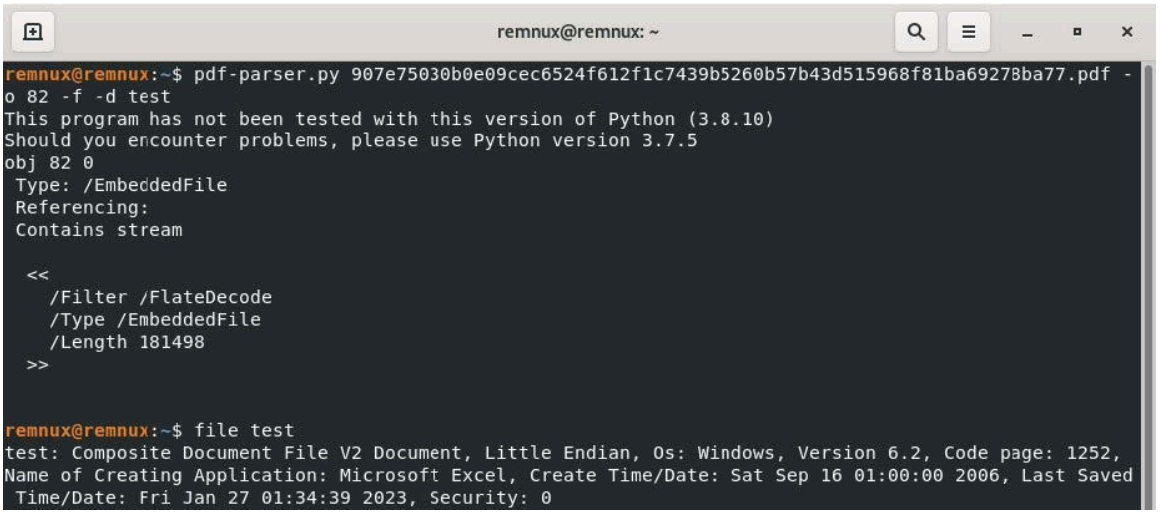
Para navegar por los distintos objetos, podemos ejecutar pdf-parser.py sobre este archivo, seguido de `| less`. Desafortunadamente, esto no produce una URL, por lo que necesitamos estudiar los objetos con más detenimiento. Puede ser útil fijarse en la longitud de los objetos: muchos tienen una longitud de 10 bytes, lo que significa que es poco probable que contengan algo malicioso.

Sí vemos algunos objetos más grandes, empezando por el objeto 61, que dice `/Subtype`

`/Image`. Como probablemente pueda adivinar, contienen imágenes integradas en el PDF. Pero luego está el objeto 82, que es un archivo integrado (`/Type /EmbeddedFile`). Añadir la opción `-o` al final del comando que acabamos de introducir nos permite mostrar sólo este objeto:

La herramienta pdf-parser nos ayuda a extraer el objeto utilizando la opción `-d` (que significa "volcar") seguida de un nombre de archivo. Como el objeto está codificado (ver `/Filter /FlateDecode`) también podemos utilizar -f para descodificarlo.

En este caso, almacenamos los datos extraídos en un archivo, `test`, y luego utilizamos el comando file para encontrar cuál es el objeto. ¡Resulta que es un documento Excel! Si quisiéramos, podríamos analizarlo más a fondo utilizando oledump.



Ejercicio 10.9 Utilice la opción `-d` en `pdfdump.py` para extraer una imagen del PDF.

Ejercicio 10.10 Utilice la herramienta pdf-parser para analizar el archivo PDF.

ad517cb885ee279ec6ca95cd7402da998ec5461461f745c2f075085ef49b4eb6.

Ejercicio 10.11 *(opcional)* Abra los dos PDF en Triage, o en otro sandbox de su elección, y

confirme lo que mostró el análisis manual.

Otros tipos de adjuntos

Existen muchos otros tipos de archivos adjuntos utilizados para propagar malware, y los actores maliciosos siguen encontrando otros nuevos que utilizar. Como se ha mencionado anteriormente, no debe esperar saber analizarlos todos. Si se encuentra con un nuevo tipo de archivo que no sabe cómo manejar, busque en Internet. Es muy probable que alguien haya escrito una herramienta y/o una guía sobre cómo analizar este tipo de archivo en particular.

Ese alguien bien puede ser Didier Stevens. Vale la pena seguir su blog y sus publicaciones en el blog Internet Storm Center. Por ejemplo, en los primeros meses de 2023, escribió cómo analizar archivos OneNote wayback machine y archivos HTA wayback machine.

Analizar enlaces

A diferencia de un documento malicioso, un enlace web (o una URL) en realidad no contiene nada; simplemente enlaza con un recurso en otro lugar. Puede tratarse de una página HTML, una pieza de malware o incluso una página que dé un error 404. Lo que el enlace devuelve a veces depende de cómo y cuándo su dispositivo realiza la solicitud. Muchas URL dejan de funcionar pasado un tiempo, lo que es especialmente cierto en el caso de las maliciosas. Sin embargo, incluso cuando éste es el caso, el análisis sigue siendo posible.

En primer lugar, está el nombre de dominio utilizado. Esto suele ser un gran indicio a la hora de decidir si el enlace es o era malicioso. Consulte el capítulo 7 para obtener un recordatorio sobre cómo utilizar VirusTotal para obtener más información sobre un nombre de dominio potencialmente malicioso.

En segundo lugar, puede fijarse en lo que se carga cuando intenta acceder al enlace. Aquí tiene que tener suerte: el recurso puede haber sido eliminado o cambiado. Incluso si el recurso sigue ahí, puede que el servidor malicioso no se lo sirva basándose en su dirección IP, navegador web o alguna otra característica. Y, por supuesto, querrá descargarlo en un entorno seguro, como REMnux. El ejercicio opcional 10.12 que aparece a continuación le orienta sobre cómo hacerlo.

Por lo general, es más seguro abrir la URL en un sandbox. Esto no le ayudará si el recurso ha sido eliminado o cambiado, pero si todavía está ahí, es mucho menos peligroso abrirlo en un sandbox. Recuerde que en Triage, la sección "Downloads" le da acceso a los archivos descargados por si desea analizarlos más a fondo.

A principios de la década de 2010, las "descargas drive-by" eran una forma habitual de infectar las computadoras. Un sitio web malicioso o infectado detectaba que su navegador o complemento de navegador (como Flash Player o Java) era vulnerable y utilizaba esa vulnerabilidad para instalar malware en su computadora. Hoy en día, los navegadores modernos funcionan para bloquear los complementos peligrosos y suelen instalar actualizaciones de seguridad automáticamente, lo que hace que estas descargas no

autorizadas sean mucho más raras. Sin embargo, siguen existiendo y, en algunos casos, aprovechan vulnerabilidades de día cero en los navegadores.

Por esta razón, abrir enlaces sospechosos en un navegador sigue sin ser una buena idea, aunque el riesgo sea mucho menor de lo que era antes.

Ejercicio 10.12 Busque una URL maliciosa reciente en URLhaus , una página web de la misma gente que también mantiene MalwareBazaar, y ábrala en Triage o en otro sandbox de su elección. Confirme que el contenido descargado es visible en la pestaña "Downloads" de Triage. Si no ocurre nada, pruebe con una URL diferente. (Este ejercicio le hace buscar deliberadamente las URL usted mismo en lugar de sugerirle una.)

Ejercicio 10.13 *(opcional)* Lea este blog wayback machine sobre el uso de `curl` para descargar el contenido de una URL potencialmente maliciosa y pruébelo con algunas URL recientes de URLhaus.

Clientes de correo electrónico vulnerables

Por último, hay un tipo diferente de correo electrónico malicioso que es poco frecuente pero que merece la pena mencionar: aquel en el que una vulnerabilidad en un cliente de correo electrónico es explotada directamente por un correo electrónico especialmente diseñado. En marzo de 2023, se descubrió wayback machine que un grupo de piratas informáticos vinculado a Rusia y conocido como Fancy Bear o APT28 (o varios nombres más) había estado utilizando una vulnerabilidad de día cero en Outlook para infectar computadoras de esta forma.

No existe una forma genérica de analizar este tipo de correos electrónicos. Los atacantes pueden utilizar diferentes tipos de vulnerabilidades. Son muy cuidadosos a la hora de utilizar los días cero; a menudo, los atacantes no quieren revelar su capacidad para explotarlos, no sea que los desarrolladores del software de correo electrónico se enteren y los parcheen. Afortunadamente, estos casos son muy raros. Pero esto pone de relieve la importancia de asegurarse de que los clientes de correo se mantienen actualizados, algo que los clientes de correo web hacen automáticamente.