Capítulo 7:
Inteligencia de amenazas y VirusTotal

El presente capítulo se centra en la inteligencia de amenazas y en el uso de VirusTotal.

La **inteligencia de amenazas** (o inteligencia de ciberamenazas, a menudo abreviada como CTI) le ayuda a entender los ataques digitales y su contexto, como por ejemplo quién o qué está detrás de ellos y qué vínculos existen entre los distintos ataques.

Si, por ejemplo, está ayudando a un periodista que ha recibido un correo electrónico de phishing, probablemente no sólo querrá comprobar si se trataba efectivamente de un correo electrónico de phishing, sino también qué tipo de correo electrónico de phishing era. ¿Era un correo electrónico de phishing común y corriente enviado a miles o millones de destinatarios aleatorios? ¿O fue enviado a una persona específica y quizá a otras pocas elegidas por un actor que las tiene como objetivo? La asistencia que preste puede depender de las respuestas a estas preguntas.

Si una amenaza incluye un archivo o una aplicación maliciosa ("malware"), es posible que también desee comprender más o menos lo que hace. Esto puede ayudarle a mitigar la amenaza en el caso de que se ejecute el malware, así como a comprender cómo se puede defender contra él en el futuro.

La inteligencia de amenazas es un campo inmenso, y hay mucho más que aprender sobre él, sin duda más de lo que cabría en esta guía. Si le interesa profundizar, la analista de inteligencia de amenazas Katie Nickels ha desarrollado un plan de autoaprendizaje en dos partes (parte 1 wayback machine; parte 2 wayback machine).

VirusTotal

VirusTotal es un servicio en línea muy conocido que puede utilizarse para llevar a cabo tareas de inteligencia de amenazas básicas y, en ocasiones, más avanzadas. VirusTotal se creó en 2004 en España y fue adquirido por Google en 2012. Sin embargo, en el momento de escribir estas líneas (noviembre de 2022), el front-end no está particularmente integrado con otros servicios de Google. Por ejemplo, las cuentas de la página no están directamente vinculadas a una cuenta de Google.

Originalmente, la finalidad de VirusTotal era servir como repositorio de malware en el que los archivos podían cotejarse con numerosos productos antivirus, y probablemente esa siga siendo su característica más conocida. Puesto que personas y organizaciones le han subido millones de piezas de malware a lo largo de los años, VirusTotal es probablemente también el mayor repositorio de malware del mundo, lo que lo convierte en un lugar excelente para buscar vínculos entre distintos tipos de malware.

Además, lo que lo hace aún más útil es que VirusTotal no se centra únicamente en las muestras de malware, sino que también analiza los distintos elementos con los que interactúan las muestras. VirusTotal también escanea y agrega direcciones IP, nombres de dominio y URL y busca vínculos entre ellos. Así, usted puede subir un archivo adjunto que encontró en un correo electrónico, descubrir que se trata de malware, saber que está vinculado a un dominio que en algún momento apuntó a una dirección IP a la que se

conectó otro archivo de malware cuando se ejecutó y llegar a la conclusión de que el archivo adjunto original que subió está relacionado con este malware conocido.

Antes de que abra VirusTotal, hay dos cosas importantes que debe tener en cuenta. Primero, *no suba simplemente* archivos a VirusTotal sin entender lo que está haciendo. Y segundo, hacer conexiones de este tipo no es una ciencia exacta, y es fácil llegar a conclusiones incorrectas. Por ejemplo, las direcciones IP se reasignan frecuentemente a nuevas organizaciones, así que lo que era una dirección IP maliciosa la semana pasada podría ser inocua esta semana. Tenga cuidado con sacar conclusiones rápidas, sobre todo si estas conclusiones tienen consecuencias.

Conceptos importantes en materia de inteligencia de amenazas

Esta sección presenta algunos conceptos importantes que necesitará conocer para el resto del capítulo y los capítulos siguientes.

El presente capítulo proporciona una breve visión general de estos conceptos; sin embargo, le recomendamos que utilice su motor de búsqueda favorito para profundizar en cada tema. Los motores de búsqueda serán quizá una de las herramientas más importantes en su trabajo sobre inteligencia de amenazas. Independientemente de lo avanzados que sean sus conocimientos, siempre se encontrará con la necesidad de buscar cosas, a menudo cosas sorprendentemente básicas. Ser capaz y sentirse cómodo haciéndolo es una aptitud importante para cualquier analista de inteligencia de amenazas.

Indicadores de compromiso

El término **Indicadores de compromiso** (o IoC, por sus siglas en inglés) hace referencia a cualquier artefacto o prueba que se encuentre mientras se investiga un dispositivo o una red comprometidos. Esto suele hacer referencia a direcciones IP o dominios a los que se conecta el malware o el sistema comprometido o a cualquier archivo malicioso que el atacante deje en su sistema. En ocasiones, también se refiere a direcciones de correo electrónico, direcciones de Bitcoin, frases comunes utilizadas por el atacante o artefactos más esotéricos.

Cuando quiera publicar sobre un incidente que haya gestionado o una amenaza que haya analizado, una buena práctica es incluir un resumen por separado de los IoC que haya encontrado. Esto ayuda a otras personas a comprobar sus propios sistemas y redes, por ejemplo, comprobando los registros del sistema o del servidor en busca de pruebas de un ataque similar.

A continuación se profundiza en algunos IoC que puede encontrar.

Direcciones IP

Las **direcciones IP** son direcciones legibles por ordenador compuestas de números (y a veces letras) para cada dispositivo conectado a Internet. Contrariamente a su dirección postal o a su número de teléfono, a menudo son reasignadas rápidamente por la red para poder dar cabida a más dispositivos: por ejemplo, el Wi-Fi de su casa puede reasignar la misma dirección IP a su laptop, a su teléfono o a los dispositivos de sus amigos según la disponibilidad. Los nombres de dominio – el componente básico de las direcciones legibles por humanos que puede utilizar para visitar páginas web – también se "resuelven" o están conectados a un determinado rango de direcciones IP.

Cuando hablamos de direcciones IP, solemos referirnos a **IPv4** (direcciones IP versión 4). También existen direcciones **IPv6**, pero en la presente guía, una dirección IP será una dirección IPv4 a menos que se especifique lo contrario. No existen más direcciones IP que las versiones 4 y 6.

No tiene por qué comprender todos los detalles del funcionamiento de las direcciones IP; sin embargo, es importante que pueda hacer al menos lo siguiente:

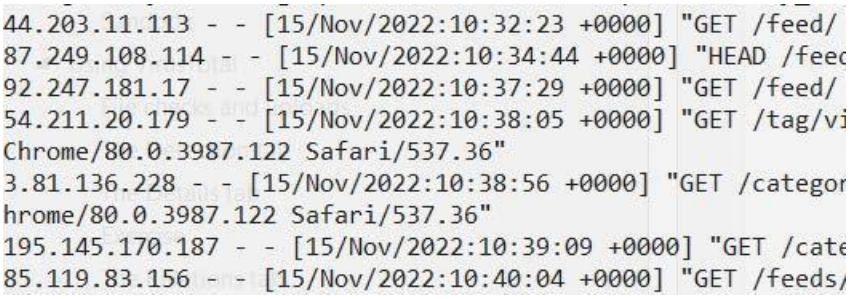
- Reconocer cómo son las direcciones IPv4 e IPv6.
- Entender qué es una dirección IP(v4) privada como `192.168.1[.]2`.[1]
- Entender qué es Tor y cómo Tor oculta la dirección IP de alguien.
- Entender qué es una VPN y cómo oculta la dirección IP de alguien.

Una de las formas en las que podría encontrar una dirección IP realizando una conexión sospechosa sería descubriendo en el registro de su página web que esa dirección IP solicitó una URL que parecía explotar una vulnerabilidad[2]. La dirección IP que vea podría ser la dirección IP pública del actor malicioso. No obstante, muchos actores malintencionados utilizan algún tipo de proxy, como Tor o una VPN, para ocultar su dirección IP. Así que, en este caso, la dirección IP puede no ser relevante para su investigación. Ahora bien, "el actor malicioso utilizaba Tor para conectarse" también puede ser un dato útil del que hacer un seguimiento o compartir.

---

[1] Ignore los corchetes por ahora; se explicarán en la sección "Neutralizar" más adelante en este capítulo.

[2] Esto es extremadamente común y la mayor parte de estas solicitudes se realizan de forma totalmente automática y no están dirigidas. No significa que el servidor presente esa vulnerabilidad en concreto, ¡ni siquiera que ejecute ese software en particular!



Direcciones IP en el registro de un servidor web

Si quiere investigar la dirección IP, la primera pregunta a la que tendrá que responder es si está:

- Totalmente controlada por el actor que ejecuta la página de phishing (su propia web, y no una página de alojamiento público, como por ejemplo imgur o YouTube). En este caso, podrá estar razonablemente seguro de que otros contenidos alojados allí están vinculados al mismo actor.
- Compartida con otros contenidos. Un gran número de direcciones IP alojan varios servicios no relacionados, como un servidor web que sirve a varias páginas web o un servidor de correo que sirve a varios dominios. Estos servicios no están necesariamente relacionados entre sí. Además, observe que a veces el contenido legítimo comparte la misma dirección IP con varios tipos de contenido malicioso. Sin otro tipo de pruebas (por ejemplo, páginas de phishing que parezcan muy similares), en este caso, no podrá vincular de forma segura el contenido alojado en la misma dirección IP al mismo actor.
- Gestionada por una entidad legítima pero comprometida de alguna manera. Por ejemplo, el actor malicioso puede haber hackeado el servidor. En este caso, debe saber cuál fue el hackeo y cuándo se produjo antes de poder sacar conclusiones basadas en la dirección IP.

  No suele ser fácil averiguar en cuál de estas tres situaciones se encuentra, pero un servicio como VirusTotal puede ayudarle con ello.

Un **nombre de dominio** corresponde a la parte de una dirección web legible por humanos que se adquiere en un registro de dominios – principalmente el dominio de nivel superior (`.com`, `.org`, `.co.uk`, `.in`, `.br`, etc.) y lo que precede inmediatamente a ese punto (`google`, `amazon`, `internews`, etc.). Un **nombre de host** se refiere a esa dirección así como a cualquier subdominio que el propietario del dominio pueda establecer dentro de su dominio. Así, internews[.]org o google.co[.]uk son nombres de dominio además de nombres de host, pero `www.internews[.]org` y `mail.google.co[.]uk` sólo son nombres de host. Los términos "nombre de dominio" y "nombre de host" suelen utilizarse indistintamente. No tiene por qué comprender todos los detalles del funcionamiento de los nombres de dominio, los nombres de host y el DNS; sin embargo, es importante que pueda hacer al menos lo siguiente:

- Distinguir entre dominios de nivel superior con código de país y otros dominios de nivel superior.
- Saber qué es un subdominio.
- Saber utilizar el comando `dig` en Linux (¡por ejemplo en su instancia REMnux!) para realizar búsquedas de DNS (ésta es una buena introducción).
- Saber qué son los registros A, AAAA y MX.

- Saber cómo encontrar la fecha de registro de un dominio utilizando el comando "whois".
- Entender qué es un registrador de nombres de dominio.

Al analizar una amenaza, si se encuentra con un nombre de host, suele ser porque en él se aloja algún contenido o porque se establece una conexión con el nombre de host. Si desea estudiar más en profundidad el nombre de dominio o de host, determine si se encuentra en una de las siguientes situaciones:

- El dominio es legítimo y no se utiliza para fines maliciosos. Es el caso, por ejemplo, de `internews[.]org`. El malware puede seguir conectándose a dominios legítimos: a veces por una razón explícita (podría, por ejemplo, utilizar una página como `whatismyipaddress[.]com` para determinar la dirección IP pública del dispositivo), a veces como señuelo.
- El dominio es legítimo pero también se utiliza para fines maliciosos. Por ejemplo, `drive.google[.]com` es claramente una página legítima, pero en ella se aloja una gran cantidad de malware.
- El dominio es legítimo pero ha sido comprometido y utilizado para fines maliciosos. El compromiso podría haber sucedido a nivel del servidor al que apunta el dominio, pero también a nivel del DNS. En este último caso, usar una página como VirusTotal le puede ayudar a comprobar el historial de DNS.
- El dominio fue registrado y configurado para fines maliciosos.

Al registrar un dominio, los actores malintencionados no dicen que van a utilizarlo como phishing o malware. Por ello, si desea saber si un dominio fue configurado con fines maliciosos, usted tendrá que hacer algunas investigaciones.

Los dominios registrados para fines maliciosos:

- Suelen haberse registrado hace relativamente poco tiempo.
- Suelen tener un aspecto muy aleatorio (por ejemplo, `vniopquiopvqr[.]com`) o parecerse a otros legítimos (por ejemplo, `internews- official[.]org`).
- Utilizan a menudo dominios de nivel superior poco habituales, como .top o .surf.
- Con frecuencia no tienen configurado un registro MX o utilizan el predeterminado del registrador.

La entidad que gestiona el dominio no puede ver las búsquedas DNS de un dominio[3], pero sí el sondeo activo de un servidor web o de correo al conectarse a ese dominio. Tome esto en consideración si no quiere que su investigación sea visible, ¡y utilice una VPN o Tor para ocultar su identidad!

Neutralizar

Cuando trate con nombres de dominio o direcciones IP potencialmente maliciosos, no deseará que alguien haga clic accidentalmente en ellos (tenga en cuenta que, muy a menudo, se convierten automáticamente en nombres). Tampoco querrá que algún software de seguridad que analice el contexto en el que se comparten los artefactos (por ejemplo, un producto de seguridad de correo electrónico) los detecte como si fueran maliciosos y emita una alerta.

[3] Ellos pueden notar una búsqueda si es para un subdominio muy específico, pero esto es un caso raro.

Por lo tanto, suele considerarse una buena práctica **neutralizar** los dominios y las direcciones IP colocando corchetes alrededor de todos los puntos o, al menos, del último. En la práctica, esta última opción es casi siempre suficiente, por lo que así se ha hecho en esta guía. Así, en lugar de `internews.org`, escribiremos `internews[.]org` y en lugar de `127.0.0.1`, escribiremos `127.0.0[.]1`.

Los artefactos incluidos en el párrafo anterior y muchos de los incluidos en esta guía no son maliciosos y podríamos, por tanto, omitir los corchetes. Sin embargo, una práctica común es simplemente eliminarlos todos.

Numerosas herramientas y servicios donde puede introducir dominios y direcciones IP, incluido VirusTotal, eliminarán los corchetes de forma automática, por lo que no tendrá que hacerlo usted antes de buscar algo.

Pregunta 7.1 ¿Por qué no es necesario neutralizar los corchetes de los nombres de archivo? (Ver la respuesta en el apéndice).

Hashes

Una **función hash criptográfica** consiste en un algoritmo matemático que toma datos de tamaño arbitrario (por ejemplo, una contraseña o el contenido de un archivo) y los convierte en un número fijo de bytes: el "**valor hash**" o simplemente "**hash**". Al tratar con muestras de malware, los hashes son muy convenientes por muchas razones.

La primera es por seguridad. Usted no quiere compartir malware de forma que pueda ejecutarse accidentalmente y causar daños. Compartir un hash de una muestra es más seguro.

La segunda tiene que ver con el tamaño. Un hash es pequeño, así que puede compartirlo en un correo electrónico, un mensaje de Signal o en las redes sociales sin tener que adjuntar el archivo original.

La tercera razón es que un hash constituye la "huella dactilar" de la muestra, lo que hace más fácil la búsqueda de otras instancias de la misma en una colección de muestras de malware. Esto puede ser muy útil. A veces, usted no querrá hacer pública más información sobre la muestra de la que ya tiene. Cuando usted comunica que ha visto un archivo adjunto de correo electrónico malicioso con un hash concreto, las personas pueden verificar su propia colección de archivos adjuntos o repositorios de muestras de malware como VirusTotal y ver si han visto el mismo archivo.

Cuando un actor malintencionado envía varios archivos de malware en el marco de una campaña, es bastante fácil que modifique cada uno de ellos ligeramente para que los hashes sean completamente diferentes. Sin embargo, en la práctica, no lo hacen muy a menudo, por lo que los hashes siguen siendo un buen modo de ayudar a la gente a identificar que están viendo los mismos archivos de malware (y, por tanto, los mismos adversarios) en una campaña de ataques.

Cabe destacar que el nombre del archivo no forma parte de los datos hash, por lo que si cambia el nombre de un archivo, el hash no cambiará. Sin embargo, si cambia un byte de un archivo, éste cambiará.

Los hashes criptográficos tienen las siguientes propiedades:

- El hash puede calcularse rápidamente, incluso para entradas muy grandes.
- Dado un valor hash, en la práctica es imposible calcular los datos originales.
- Dados unos datos, que permiten calcular su valor hash, en la práctica es imposible encontrar otros datos con el mismo valor hash.
- El más mínimo cambio en los datos da un valor hash completamente distinto.

Es importante señalar que hay otros tipos de hashes que desempeñan un papel en la inteligencia de amenazas y que no comparten esta última propiedad. A estos se les llama "fuzzy hashes". Por ejemplo, puede fijarse en SSDEEP en VirusTotal. Se trata de un "fuzzy hash".

En la práctica, existen tres funciones hash relevantes: md5, sha1 y sha256. Las dos primeras son más antiguas y algo imperfectas, aunque es poco probable que eso afecte a su trabajo. Sin embargo, si puede elegir una función hash, se recomienda elegir sha256.

Un hash sha256 consta de 32 bytes (o 256 bits; de ahí su nombre) y se escribe como 64 caracteres utilizando los dígitos del 0 al 9 y las letras de la a a la f. Dadas las propiedades anteriormente mencionadas, los caracteres particulares de un hash no importan, sin embargo: en su investigación es sólo una cadena de caracteres.

Pregunta 7.2 Usted no puede simplemente "invertir" el hash para encontrar los datos originales, dada la segunda propiedad anterior. Sin embargo, si encuentra un hash y no tiene la menor idea de lo que es, siempre puede utilizar un motor de búsqueda y tal vez tenga suerte. ¿Cuáles son los datos originales que resultaron en los siguientes hashes?

```
md5:d41d8cd98f00b204e9800998ecf8427e
sha1:da39a3ee5e6b4b0d3255bfef95601890afd80709
sha256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

(La notación de dos puntos es común para indicar qué tipo de hash es algo, pero como se puede ver, los tres hashes también tienen longitudes diferentes).

Ejercicio 7.3 En su instancia REMnux, cree un archivo de texto, escriba el texto "`hello world`" (sin comillas ni salto de línea) y guarde el archivo llamándolo `test.txt`.

1 A continuación, utilice el comando `sha256sum` para calcular el hash sha256 del archivo. Tome nota del valor del hash.

Utilice `md5sum` y `sha1sum` para calcular también los hashes md5 y sha1.

2 Ahora cambie el nombre del archivo a `newtest.txt` utilizando el comando `mv`. Calcule el hash sha256 del nuevo archivo. Confirme que es el mismo.

3 Ahora abra el nuevo archivo para editarlo y convierta la "h" en una "H" (de minúscula a mayúscula). Guárdelo y calcule el nuevo hash sha256. Confirme que es diferente y no está relacionado con el hash original.

4 Vaya a Malware Bazaar (asegúrese de hacerlo en un navegador dentro de

REMnux), busque su base de datos de malware y haga clic en cualquier archivo. Descargue la muestra y descomprímala (recuerde que es una práctica común poner malware en un archivo zip con la contraseña "infected").

Descomprimir un archivo zip funciona normalmente con el comando unzip, pero es posible que obtenga un error. Si es así, instale el comando 7z ejecutando

```
sudo apt-get install p7zip-full
```

y luego descomprima el archivo ejecutando

```
7z x [file]
```

A continuación, calcule el hash sha256 de la muestra de malware.

Si lo hace correctamente, usted notará que el hash es el mismo que el nombre del archivo. ¡Esto es bastante común entre las bases de datos de malware!

Utilizar VirusTotal

Con todo este bagaje de información, examinemos VirusTotal, en el que podrá comparar los dominios, las direcciones IP y las URL de sus archivos con los subidos por analistas de amenazas del mundo entero.

Antes de utilizar VirusTotal, tiene que entender cómo funciona esta página. Su funcionalidad principal es gratuita y ni siquiera exige registro. La creación de una cuenta gratuita le proporcionaría algunas opciones adicionales, pero no las utilizaremos en el marco de esta guía.

VirusTotal también ofrece cuentas de pago, que hacen más fácil buscar en la enorme colección de archivos determinadas propiedades, como un nombre, y descargarlos. A continuación le explicamos por qué esto es importante: vamos a suponer que sus adversarios, especialmente los más fuertes, tienen cuentas de pago y que las utilizan para buscar archivos relevantes para sus objetivos. Así que tenga cuidado a la hora de subir archivos a VirusTotal: *sólo suba archivos que no tenga problemas en hacer públicos*.

Verificaciones y subidas de archivos

Hay dos razones por las cuales puede querer subir un archivo. La primera es para comprobar su contexto y saber más sobre él: ¿es malicioso, a qué dominios se conecta, cuando se ejecuta, etc.?

La segunda es para compartirlo con la industria de la seguridad. La mayor parte de las empresas de seguridad son clientes de VirusTotal, y subir un archivo es una forma sencilla de compartirlo con ellas. Les podría ayudar a detectar el ataque específico al que usted se enfrenta y evitar que afecte a otros.

Conviene señalar aquí que la mayoría de las empresas de seguridad ven millones de muestras de malware al día, y la mayor parte del escaneado – y la adición de la detección – se produce de forma totalmente automática. A menudo esta práctica está bien, pero si por alguna razón usted desea que presten especial atención a su archivo, ¡asegúrese también

de contactarse directamente con ellas!

Cuando compruebe un archivo en VirusTotal, siga los cuatro pasos que se indican a continuación:

1. Calcule el hash sha256 del archivo tal y como se ha descrito anteriormente. Compruebe el hash en VirusTotal. Si existe, el archivo ya ha sido cargado.
2. De lo contrario, decida si desea subir el archivo. Aunque el archivo sea malicioso, es posible que haya sido diseñado específicamente para el objetivo y, por tanto, contenga alguna información personal. En el caso de un archivo con un objetivo, subirlo a VirusTotal demuestra que fue abierto y está siendo analizado. También es aceptable decidir no subir el archivo porque usted no está seguro.
3. Si desea subirlo, considere si el nombre del archivo es algo que está dispuesto a compartir. En caso negativo, o si no está seguro, cambie el nombre del archivo a `[sha256].[extension]`:, mantenga la extensión original (.exe, .docx, etc.), pero cambie la parte que precede al punto por el hash sha256. Es una buena práctica (ya lo vimos anteriormente con Malware Bazaar) y no revela nada sobre el archivo.
4. Suba el archivo utilizando la interfaz web de VirusTotal. Asegúrese de que sólo sube el archivo y no una carpeta entera o un archivo zip que lo contenga.

La pestaña "Detección"

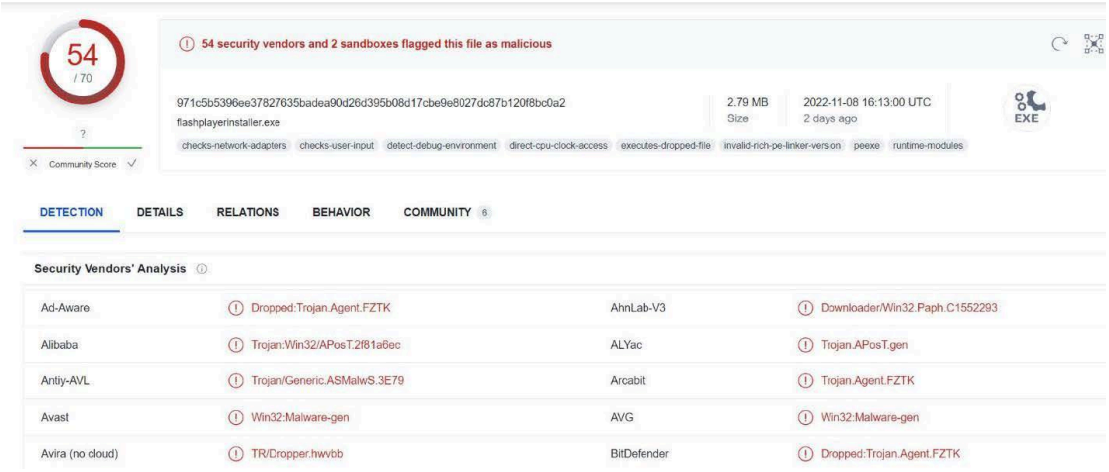
En las siguientes secciones, utilizaremos el ejemplo 971c5b5396ee37827635badea90d26d395b08d17cbe9e8027dc87b120f8bc0a2[4]. Se trata de un archivo .exe malicioso utilizado en ataques dirigidos por un actor de amenazas vinculado a Irán llamado APT42. Fue referido en un informe Wayback Machine por la empresa de seguridad Mandiant (ahora propiedad de Google).

VirusTotal presenta un encabezado con varias "pestañas" debajo. El encabezado incluye el hash sha256, el tamaño del archivo y la fecha en que fue analizado por última vez.

Debajo, la primera pestaña se llama "Detección". En ella aparecen los resultados del escaneado de docenas de motores antivirus. La palabra motor se utiliza aquí deliberadamente: normalmente, esta parte del producto sólo examina el archivo en sí y no lo que hace.

Es importante destacar que las tasas bajas de detección son bastante comunes, especialmente para archivos nuevos. Además, el número de detecciones debe interpretarse como un indicador de qué tan conocido es el archivo dentro de la comunidad de seguridad, y no como una medida de la eficacia de un producto en particular para detener la amenaza en una situación real[5].

[4] ¡Un ejemplo de referirse a un archivo por su hash!
[5] Eso se debe a que VirusTotal sólo utiliza un motor simplificado del archivo, no el producto completo. Puede compararse con un guardia de seguridad que no hubiera reconocido a un ladrón por su aspecto, pero que aun así hubiera podido impedir que robara algo.



Los falsos positivos – archivos inofensivos o legítimos detectados incorrectamente como malware – ocurren, pero no son frecuentes. En la práctica, cualquier cosa que supere unas pocas detecciones apunta a que un archivo es malicioso.

Consejo: si el archivo se escaneó por última vez hace algún tiempo, usted puede hacer clic en la flecha curva de la esquina superior izquierda para que se escanee de nuevo. La detección suele mejorar con el tiempo, lo que le ofrece una imagen más precisa.

Por último, cabe destacar dos cosas sobre los motores. Algunos son en realidad el mismo (por ejemplo, AVG fue adquirido por Avast hace algún tiempo; los productos son exactamente idénticos desde hace mucho tiempo), y sólo se enumeran por separado porque las respectivas marcas siguen existiendo. Por lo general, los nombres de las detecciones pueden ignorarse: suelen ser genéricos y, cuando no lo son, suelen ser erróneos.

Por último, fíjese en que si ha iniciado sesión en VirusTotal, verá algunas reglas de detección listadas por encima de los resultados de los antivirus. Se trata de otras reglas de detección y, al contrario que los nombres de detección de los antivirus, pueden ser útiles para saber de qué tipo de malware se trata.

La pestaña "Detalles"

La pestaña "Detalles" muestra más información sobre un archivo, como varios hashes: sha256, md5, etc. Nuestro archivo es un ejecutable de Windows (verá el tipo de archivo en la lista). En el caso de otros tipos de archivos, la información aquí es diferente; por ejemplo, para los archivos de Android, se muestran los permisos solicitados, lo que puede ser muy útil.

La pestaña "Detalles" le indica cuándo se envió por primera vez el hash a VirusTotal, lo que es un buen indicador. También le dice cuándo se creó el archivo y cuándo se vio por primera vez en la naturaleza; estos datos no son particularmente precisos, así que no les preste demasiada atención.

También notará los diferentes nombres con los que se presentaron los archivos. En ocasiones, esto le ayuda a comprender cómo se utilizó el archivo, como se ve en el siguiente ejercicio.

Pregunta 7.4 Alguien a quien usted da soporte ha recibido un archivo malicioso llamado `tax_information.docx`, y usted sospecha que un adversario le está apuntando específicamente con una campaña realizada para que parezca que proviene de la oficina tributaria local. En VirusTotal, descubre que el mismo archivo también se ha presentado como package_receipt.docx y birthday_gift.docx. ¿Cómo podría ayudarle esta información? (Ver la respuesta en el apéndice).

La pestaña "Relaciones"

La pestaña "Relaciones" muestra las relaciones entre el archivo que ha subido y otros IoC en VirusTotal: URL, dominios y direcciones IP contactadas cuando el archivo se ejecutó en un sandbox (más sobre este tema en un capítulo posterior), así como los archivos que se bajaron de Internet o que se crearon directamente cuando el archivo se ejecutó.

Puede hacer clic en estos objetos para saber más sobre ellos y posiblemente encontrar enlaces a otras amenazas; esto se denomina pivoting. Hablaremos de esto más adelante en la guía.

Ejercicio 7.5 El dominio `update-driversonline[.]bid` destaca entre los que están conectados a este archivo (recuerde que seguimos hablando de 971c5b5396ee37827635badea90d26d395b08d17cbe9e8027dc87b120f8bc0a2). Hay muchas razones por las que sospechar que esto es malicioso y algunas para pensar que no lo es. ¿Cuáles se le ocurren a usted?

La pestaña "Relaciones" también podría contener otros contextos, como las URL desde las que se descargó este archivo o los archivos (como un zip) que lo contienen. ¡Todo esto puede ser información útil para entender la amenaza!

Las pestañas "Comportamiento" y "Comunidad"

La pestaña "Comportamiento" analiza lo que hace el archivo. Para un ejecutable de Windows, esto puede ser de gran ayuda. Pero para un analista principiante, la información aquí puede ser bastante confusa. Sin una mayor comprensión de lo que hacen los archivos (para lo que podría, por ejemplo, utilizar un sandbox, del que se hablará en el capítulo 10), sea cauto a la hora de sacar conclusiones basándose únicamente en esta pestaña.

La pestaña "Comunidad" contiene comentarios sobre el archivo. Muchos comentarios son generados de forma automática y muestran más resultados del sandbox. Algunos comentarios los añaden personas; éstos son especialmente útiles. Si lo desea, puede crear una cuenta gratuita en VirusTotal y proporcionar algo de contexto sobre el archivo y tal vez incluso sugerir que se comuniquen con usted si alguien sabe más al respecto. En este último caso, tenga en cuenta que esta es una herramienta de acceso público, incluso por parte de adversarios, así que no añada nada que pueda relacionarse con usted como persona si no considera seguro hacerlo.

Otros tipos de archivos

VirusTotal puede manejar muchos tipos de archivos distintos. Las pestañas y su contenido pueden resultar algo diferentes en función del tipo de archivo.

Compruebe las pestañas de VirusTotal de los tres ejemplos siguientes y dedique unos minutos a cada uno de ellos para familiarizarse:

Un documento de Word malicioso:
2382d4957569aed12896aa8ca2cc9d2698217e53c9ab5d52799e4ea0920aa9b9

Un archivo de paquete Android (APK):
86acaac2a95d0b7ebf60e56bca3ce400ef2f9080dbc463d6b408314c265cb523

Un ejecutable de macOS:
483b2f45a06516439b1dbfedda52f135a4ccdeafd91192e64250305644e5ff48

Pregunta 7.6 En los ejemplos anteriores, observe las pestañas e intente responder a las siguientes preguntas:

1. ¿El documento de Word se conecta con algún dominio sospechoso? Si no es así, ¿realiza alguna conexión sospechosa por otros medios?
2. ¿El archivo de Android solicita permiso para acceder al micrófono?
3. Sin utilizar un motor de búsqueda que no sea VirusTotal, ¿puede encontrar algún informe sobre el ejecutable de macOS?

(Ver la respuesta en el apéndice).

Nombres de host y dominios

Ahora busque en VirusTotal el dominio `update-driversonline[.]bid` que vimos en nuestra muestra original.
También puede ir a esa muestra en VirusTotal y hacer clic en ese enlace en la pestaña "Relaciones".

Verá que VirusTotal también tiene mucha información sobre nombres de dominio. La pestaña "Detección" le resultará familiar. Sin embargo, detectar dominios es menos ciencia dura que detectar archivos, y no siempre existe una distinción clara entre dominios "buenos" y "malos" (recuerde los cuatro tipos de dominios de los que hablamos en este capítulo, en la sección Conceptos importantes en materia de inteligencia de amenazas), pero aquí también: cuantos más proveedores lo detecten como malicioso, más probable es que lo sea.

La pestaña "Detalles" contiene más información sobre el dominio, incluida la información whois, que le informa de cuándo fue registrado y, en ocasiones, por quién. Las pestañas "Comunidad" y "Relaciones" le resultarán familiares; esta última es especialmente útil. Con ella puede hacer pivoting y también encontrar subdominios.

Pregunta 7.7 El dominio fue contactado por tres archivos, incluida nuestra muestra original. ¿Cree que los tres archivos tienen relación? ¿Por qué lo cree? (Ver la respuesta en el apéndice).

Direcciones IP

VirusTotal también contiene información sobre direcciones IP. La pestaña "Relaciones" aquí es muy útil, ya que muestra que dominios han tenido su registro A apuntando a una dirección IP. Esto puede ser realmente útil a la hora de encontrar otros dominios vinculados a un dominio en particular.

Pregunta 7.8 Utilice la entrada de VirusTotal para `update-driversonline[.]bid` y busque las direcciones IP relacionadas. ¿Encuentra otros dominios que crea que se utilizaron en la misma campaña? (Ver la respuesta en el apéndice).

URL

Por último, VirusTotal también tiene páginas sobre URL, pero rara vez añaden mucho a lo que indican las correspondientes páginas de dominios o nombres de host. Dado que las URL suelen ser únicas, añadirlas a VirusTotal puede dar a un adversario información sobre usted analizándola. Por consiguiente, es mejor limitarse a buscar el nombre de host.

Comprobar un nombre de host o un nombre de dominio casi siempre está "bien": VirusTotal analiza activamente los nombres de dominio, por lo que no tiene que preocuparse de "subir" un nuevo dominio. La única situación en la que quizá deba tener un poco de cuidado es si tiene un nombre de host muy específico, como `[long string].domain`, que puede ser exclusivo de este objetivo en particular. Sin embargo, esto es poco frecuente.

Caza de amenazas

La caza de amenazas consiste en una actividad proactiva en la que se buscan amenazas en lugar de analizar las existentes. A veces, la caza de amenazas supone buscar amenazas dirigidas a una organización o comunidad específica sin ningún enfoque concreto, por ejemplo, buscando dominios recién registrados que utilicen el nombre de la organización, lo que podría significar que el autor de la amenaza los está registrando para utilizarlos en una campaña de phishing.

Más a menudo, la caza de amenazas empieza con una amenaza existente, como un archivo malicioso, y luego busca artefactos relacionados (otros archivos, dominios, etc.) para hacerse una mejor idea de la amenaza y del actor que está detrás de ella.

VirusTotal es una excelente herramienta para la caza de amenazas, y en la sección anterior lo hicimos un poco buscando archivos y dominios relacionados. Las cuentas de pago de VirusTotal resultan realmente fantásticas para esto, ya que abren muchas más posibilidades para la caza de amenazas. Puede hacer pivoting para investigar más indicadores que encuentre y también utilizar "rules YARA", un método para buscar archivos en una gran colección que resulta especialmente útil cuando se busca malware relacionado.

Puede sorprenderle lo mucho que puede conseguir con herramientas gratuitas en línea sin saber cómo realizar ingeniería inversa de malware[6] o cómo escribir reglas YARA. Pero hay

[6] La ingeniería inversa consiste en aprender lo que hace un software, a menudo malware, a partir del código de bytes compilado.

dos advertencias importantes.

Lo primero que debe hacer es desconfiar de las conclusiones audaces. Es tentador entusiasmarse mucho[7] cuando se vincula algún malware a un actor conocido, sobre todo cuando se trata de un actor avanzado vinculado a algún gobierno. A veces, estos vínculos existen efectivamente. Otras veces, no. Por ejemplo, ambos actores pueden haber compartido infraestructura de terceros, o ha habido un intento deliberado de despistar a los investigadores. Existe otra posibilidad: que los dominios utilizados por ambas amenazas acabaran apuntando al mismo sumidero (en breve hablaremos más de los sumideros).

La segunda advertencia es que no olvide el objetivo de su investigación. No tiene por qué buscar amenazas similares a cada amenaza que investigue. Si la persona que informó del suceso no abrió el adjunto malicioso o el adjunto no iba dirigido a ella o a su organización específicamente, puede cerrar la investigación y centrarse en otras cosas.

Amenazas dirigidas y no dirigidas

Las amenazas digitales como el malware y el phishing se han dividido tradicionalmente en amenazas dirigidas y no dirigidas. En el primer escenario, la amenaza está dirigida a un usuario individual o a una organización, o quizá a un número muy reducido de ellos. En el segundo escenario, cualquier usuario podría haber recibido la amenaza, y los actores que están detrás de ella sólo esperan que algunos de los que la reciban "caigan en la trampa".

En la práctica, el reto es que muchas amenazas no dirigidas pueden seguir pareciendo en cierto modo dirigidas. En primer lugar, es muy habitual que una campaña no dirigida sólo tenga como objetivo un país o una región concretos. Esto permite al actor que está detrás de ella escribir mensajes en el idioma local y añadir un contexto local que lo hace más creíble.

En segundo lugar, los actores de amenazas suelen recurrir a los datos de muchas cuentas de correo electrónico comprometidas cuando envían correos maliciosos. De este modo, pueden hacer que un correo electrónico parezca una respuesta a algo que usted había enviado previamente o que procede de uno de sus contactos. Esto haría que un correo electrónico pareciera muy dirigido, aun cuando no sea el caso: los actores son capaces de enviar automáticamente una gran cantidad de correos electrónicos, cada uno de los cuales parece bastante personal para el destinatario.

Por último, los actores de amenazas, especialmente los que se dedican a los ciberdelitos, han encontrado un híbrido entre las amenazas dirigidas y las no dirigidas, en el que una amenaza no dirigida da como resultado una cuenta comprometida, a menudo dentro de una gran organización. El acceso a esta cuenta es vendido entonces a otro actor, que lo utiliza de forma más selectiva, por ejemplo, desplegando ransomware por toda la red. Aunque esta última amenaza era muy selectiva, ¡la amenaza original no lo era!

La gran mayoría de las amenazas digitales no son selectivas, y esto es cierto incluso para las amenazas contra las que también se enfrentan amenazas muy selectivas.

---

[7] Está bien entusiasmarse con estas cosas, ¡incluso si las amenazas son serias y afectan a personas reales de maneras a menudo graves! Pero no deje que su deseo de ayudar a las personas y a los grupos se vea impulsado por las amenazas que más le emocionan. La gran mayoría de las amenazas son muy mundanas.

Pregunta 7.9 Un correo electrónico con un archivo adjunto malicioso se dirige al destinatario, un trabajador de una organización de la sociedad civil, por su nombre y apellidos y se hace pasar por otro empleado de la organización. ¿Puede dar una razón por la que se podría tratar de una amenaza automatizada y no dirigida? (Ver la respuesta en el apéndice).

Sumideros

La mayoría del malware se controla mediante un servidor o conjunto de servidores, que son controlados por el autor de la amenaza. Este servidor o conjunto de servidores se denomina mando y control (a menudo denominado C&C o C2). La mayoría del malware necesita una conexión a Internet para poder recibir órdenes de su C&C. El malware indica a su dispositivo que se conecte a uno o varios dominios que apunten a la dirección IP del servidor de C&C. Apuntar a un dominio y no a una dirección IP permite a los actores cambiar a un servidor diferente si el original dejara de estar disponible para ellos.

Para detener una operación de C&C (comando y control) y el malware que está ejecutando, una agencia de aplicación de la ley o una empresa de seguridad puede presentar a un registrador de dominios pruebas de que el dominio se utilizó con fines maliciosos y convencer al registrador para que les permita tomar el control del dominio. A continuación, pueden apuntar el dominio a un servidor que controlan (lo que a menudo se denomina "**sinkholing**" del dominio). Esto significa que cada vez que el malware trata de conectarse a su servidor de C&C, se conecta al dominio sumidero, lo que proporciona a sus operadores una buena visión de la amenaza. A veces, la agencia de aplicación de la ley o la empresa pueden entonces enviar comandos para neutralizar el malware si llegan a comprender suficientemente cómo funciona el C&C.

Algunos malware utilizan un algoritmo de generación de dominios (o DGA) para generar nuevos dominios, a menudo a diario. Este movimiento furtivo dificulta que un analista identifique que varias muestras de malware apuntan al mismo servidor de C&C, ya que no puede buscar dominios identificativos con tanta facilidad. Los autores del malware registran estos nuevos dominios mientras dura su campaña y no tienen que preocuparse demasiado por la apropiación de dominios o por que éstos sean bloqueados por los productos de seguridad. En muchos casos, el DGA está "crackeado", lo que permite a los investigadores predecir qué dominios se van a utilizar, registrarlos de forma proactiva y dirigirlos a un sumidero.

Por tanto, cuando investigue un dominio malicioso, es importante que tenga en cuenta que un dominio que vea puede haber sido sinkholed. No existe ninguna lista pública de direcciones IP de sumidero – si existiera, los autores de malware simplemente harían que el malware no se conectara a ninguna dirección IP de esa lista – y no siempre es obvio cuándo una dirección IP es un sumidero. Muchos dominios de campañas aparentemente no relacionadas que apunten a la dirección IP suelen revelar que se trata de un sumidero. Si tiene dudas, introduzca la dirección IP en un motor de búsqueda, consulte la pestaña "Comunidad" de VirusTotal o pregunte por ahí.

Pregunta 7.10 Utilizar un sumidero para enviar mandos para neutralizar infecciones de malware es algo controvertido. ¿Puede pensar en las razones por las que esto es así? (Ver

la respuesta en el apéndice).

Otras herramientas

VirusTotal es una gran herramienta para el análisis y la caza de amenazas. Sin embargo, no es la única. Quizás las herramientas más útiles de todas sean los motores de búsqueda. Ya prefiera Google o una de las muchas y excelentes alternativas, le sorprenderá lo mucho que puede encontrar a menudo buscando un nombre de dominio, una dirección IP, el hash de un archivo u otro artefacto.

Lo mismo ocurre con las redes sociales, en particular Twitter, aunque hay que señalar que en el momento de escribir este artículo (principios de diciembre de 2022), muchos investigadores de seguridad han abandonado Twitter y se han pasado a Mastodon. El intercambio de IoC era bastante común en Twitter y podría llegar a serlo en Mastodon. Una de las grandes ventajas de encontrar un IOC en las redes sociales es que usted puede responder a la persona que lo publica y hacerle preguntas o añadir sus propios comentarios.