Guía de búsqueda de amenazas

Introducción

Esta Guía de búsqueda de amenazas ha sido creada para enseñarle cómo detectar los ataques de manera sencilla y eficaz antes de que se produzcan utilizando los datos de red de Corelight. Este documento (organizado en torno al marco MITRE ATT&CK®) está diseñado para ayudarle a desarrollar una teoría para la búsqueda de amenazas y establecer un orden de prioridad.

MITRE ATT&CK es una base de conocimientos de acceso global sobre las tácticas y técnicas de los adversarios basada en observaciones del mundo real. Se utiliza como base para modelos y metodologías de amenazas específicas en los sectores privado, público y de la ciberseguridad. Con la creación de ATT&CK, MITRE cumple su misión de resolver problemas para un mundo más seguro, reuniendo a las comunidades para que desarrollen una ciberseguridad más eficaz. ATT&CK está abierta y disponible para su uso para cualquier persona u organización de manera gratuita.[1]

¿Qué es la búsqueda de amenazas?

A grandes rasgos, la búsqueda de amenazas (*Threat hunting*) consiste en buscar activamente adversarios en su red *cuando no sabe si están dentro*. Se diferencia de la coincidencia de indicadores (*indicator matching*), en que esta solo busca señales conocidas de los atacantes, por ejemplo, direcciones IP o hash de archivos. Por lo general, llevar a cabo una búsqueda de amenazas implica investigar una teoría, o una sospecha, y luego analizar los datos en busca de algo *interesante*. Los objetos *interesantes* pueden adoptar muchas formas, por ejemplo, en *El huevo del cuco*, de Clifford Stoll, un error contable inició la búsqueda.

> ***"Dave entró en mi despacho mascullando algo sobre un pequeño contratiempo en el sistema de contabilidad del Unix. Alguien debe haber utilizado unos segundos de tiempo de computación sin pagar por ello. Los libros informatizados no acababan de cuadrar; las facturas del mes pasado, de 2.387 dólares, mostraban un déficit de 75 centavos."***

Esta diferencia de 75 centavos fue el indicador que llevó a descubrir que múltiples corporaciones y sistemas gubernamentales estaban en peligro. El término "interesante" se utiliza a lo largo de esta guía y su significado lo dejamos a su entera discreción.

¿Por qué realizar una búsqueda de amenazas?

La mayoría de los sistemas de detección basados en el host o en la red se basan en las coincidencias, también conocidas como firmas, para generar alertas que indiquen a los defensores que hay algo no deseado en la red. Sin embargo, los atacantes están en constante evolución para evitar ser detectados, y no se desarrolla una firma hasta que el artefacto ha sido descubierto en otra red. Entonces, si no está buscando artefactos en su entorno, ¿cómo puede detectar que hay atacantes evadiendo sus defensas actuales?

La búsqueda tiene varios resultados positivos. El primero es que podría encontrar artefactos de un intruso activo que sus defensas actuales han pasado por alto. Aunque algunos puedan pensar que esto es una tragedia, puede suponer una gran victoria, especialmente si el intruso no ha completado sus objetivos. En todas las búsquedas, siempre hay *algo* que encontrar.

Puede descubrir configuraciones erróneas de la red o del software que supongan una amenaza, ya sea porque reduzcan el rendimiento de la red o introduzcan una vulnerabilidad. A continuación, la búsqueda podría detectar infecciones corrientes, como el adware, u otro malware latente que no está dirigido directamente a su organización, pero que sigue siendo una amenaza. Por último, el abuso de recursos y la TI en la sombra (los programas no aprobados por el departamento de TI), pueden introducir riesgos a través de la disminución del rendimiento de la red o de nuevos vectores de ataque de adversarios. Cada búsqueda le enseñará algo nuevo sobre la red que le ayudará en su próxima investigación.

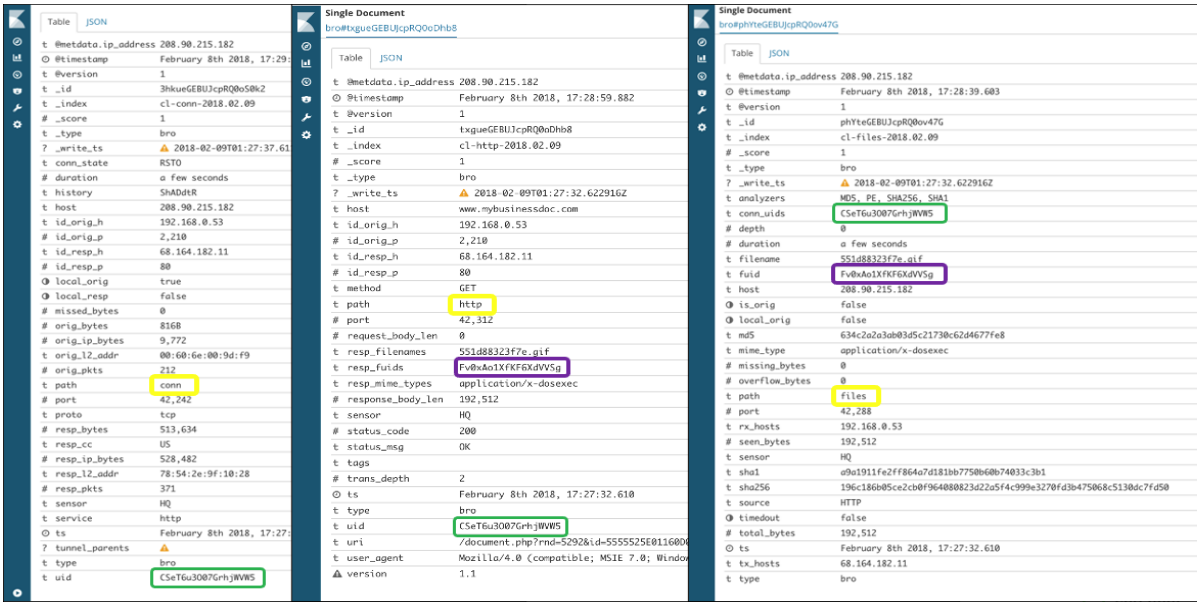
¿Por qué buscar con datos de red?
Los paquetes no mienten.

Así de simple. Si un intruso residente en la red está activo en ella, habrá artefactos de red. En los artefactos hay pistas de lo que está sucediendo, o mejor aún, un historial exacto momento a momento de lo que sucedió. Por ejemplo, si un canal de mando y control utiliza DNS como mecanismo de transporte, habrá consultas y respuestas DNS. Además, las direcciones IP que están en los extremos de una conexión TCP deben ser auténticas, no pueden ser falsificadas si se intercambian datos. Todos los ataques atraviesan la red, a menos que estén aislados en un solo host, por lo que habrá paquetes.

Nomenclatura de los registros Corelight

Corelight proporciona soluciones centradas en los datos que analizan el tráfico de la red y mejoran las herramientas de automatización transformando el tráfico de la red en registros vinculados y extrayendo archivos. El registro central es el registro *conn*, que documenta la información general sobre todas las sesiones de red.

El registro *conn* registra información sobre cada terminal de la red y el servicio (aplicación) y también asigna un UID (identificador único). El UID vincula el registro *conn* con los registros de protocolo relacionados, donde se recoge información específica de la sesión. Por ejemplo, el registro *conn* puede registrar http como el servicio, y usando el UID se puede pivotar al registro *http* para obtener información de protocolo específica sobre la sesión. El UID separa las soluciones Corelight de otras herramientas de seguridad. Este campo enlaza información que de otro modo sería dispar en registros fácilmente digeribles. El UID es fundamental para llevar a cabo el análisis de enlaces y un campo de importancia crítica que facilita el *pivoting* o la unión de varios registros.



La información sobre cada terminal de la red se resume en el campo *id,* que suele representarse en cuatro campos distintos:

- *id.orig_h*
- *id.orig_p*
- *id.resp_h*
- *id.resp_p*

Esta nomenclatura puede parecer extraña, ya que el personal de redes se refiere tradicionalmente a las sesiones utilizando el cliente y el servidor; sin embargo, el uso de orig (originador) y resp (respondedor) permite al personal de seguridad describir con precisión la conexión. Piense en el host de origen (orig_h) como la fuente, o cliente, y el host de respuesta (resp_h) como el destino, o servidor. Los campos *id.orig_p* e *id.resp_p* se rellenarán con los números de puerto correspondientes.

Muchos de los campos restantes dentro del registro *conn* y otros registros de protocolo son autodescriptivos, pero si se queda atascado, consulte la documentación de Zeek en https://docs.zeek.org/en/current/ para obtener información más detallada o visite el canal de Slack de la comunidad en http://corelightcommunity.slack.com/.

Identificación de usuarios y dispositivos

Cuando se identifican los dispositivos de una red, se suelen utilizar las direcciones IP o MAC para crear la "identidad". La dirección IP del dispositivo se utiliza más a menudo para la identidad remota de un dispositivo porque sobrevive a los límites del router. Cuando está dentro de un segmento de red, se prefiere la dirección MAC para la identificación porque puede ser un identificador fiable de un equipo específico. Cada identificador tiene sus pros y sus contras, y la capacidad de Corelight de captar ambos ayuda al personal del Centro de operaciones de seguridad a la hora de investigar los sucesos.

Mientras que las direcciones IP son duraderas[2] para investigaciones internas, a menudo son transitorias dentro de una red dado que la mayoría de las redes funcionan con DHCP (Protocolo de configuración dinámica de host, por sus siglas en inglés). Las IP transitorias resultan problemáticas para los defensores cuando la alerta del IDS (Sistema de detección de intrusiones, por sus siglas en inglés) identifica la sesión mediante las direcciones IP. Esas direcciones IP solo están relacionadas con la alerta *en el momento en que esta se generó.*

Puede utilizar herramientas de código abierto cuando realice una investigación (por ejemplo, nslookup), para proporcionar información de DNS para IP remotas. Sin embargo, se trata de una información puntual *en el momento de la investigación, no cuando se produjo el suceso.* Una técnica mejor es utilizar los registros creados en el momento de la alerta para capturar la IP y el FQDN (nombre de dominio completo, por sus siglas en inglés) del dispositivo remoto. Para localizar el dispositivo interno, puede minar los registros DHCP para identificarlo. Hay múltiples formas de identificar un host y Corelight proporciona estos datos en múltiples registros que cuentan cada uno un aspecto diferente de la historia. Ejerza la creatividad y siga todas las pistas.

Dónde se pueden encontrar los nombres de host:

- **dhcp.log:** los campos *host_name* y *domain* representan el nombre de host y el dominio comunicados por un host cuando solicita una dirección IP a través de DHCP, y el campo *assigned_addr* es la dirección IP que se asignó a ese host.
- **dns.log:** si hay una IP en el campo *answers*, entonces el campo *query* contiene el nombre de host que el servidor DNS registró (en ese momento) para la dirección IP.
- **ntlm.log:** server_dns_computer_name y server_nb_computer_name se refieren a los nombres DNS y Netbios del equipo con la dirección IP en el campo *id.resp_h*. El campo *hostname* es el nombre de host del equipo con la dirección IP en el campo *id.orig_h*.
- **kerberos.log:** en un entorno Windows, para los dispositivos unidos a un dominio, las solicitudes de kerberos en las que el campo *client* contiene un nombre que termina en $, el campo *client* es el nombre del *host* y el campo *id.orig_h* es la dirección IP de ese host. El campo *client* suele estructurarse como HOSTNAME$/EXAMPLEDOMAIN.COM, donde HOSTNAME es el nombre del host y EXAMPLEDOMAIN.COM es el nombre del dominio de Windows y el nombre del reino de Kerberos.
- **http.log:** el campo host contiene el nombre de host, el nombre de dominio o la dirección IP del cliente que ha solicitado datos al servidor HTTP. A veces este campo indica la identidad del servidor, el dispositivo con la dirección IP en el campo *id.resp_h*.
- **ssl.log:** el campo *server_name* se extrae del campo *Server Name Indication* (SNI o Indicador del nombre del servidor) en la negociación TLS/SSL, y se utiliza de forma similar al campo *host* del registro *http*. Además, el campo *subject* se extrae del asunto del certificado del servidor, y la parte del nombre canónico (CN) del asunto puede proporcionar pistas para identificar un servidor.

A la hora de identificar a los usuarios, hay varios registros que proporcionan información valiosa:

- **rdp.log:** dependiendo de la versión del protocolo RDP, el valor del campo *cookie* es el nombre de usuario declarado por el cliente, y la IP del cliente está en el campo *id.orig_h*.[3]
- **ftp.log:** el campo *user* contiene el nombre de usuario declarado por el cliente, y la dirección IP del cliente estará en el campo *id.orig_h*.
- **irc.log:** el campo *user* contiene el nombre de usuario declarado por el cliente, y la dirección IP del cliente estará en el campo **id.orig_h**.
- **socks.log:** el campo *user* contiene el nombre de usuario declarado por el cliente, y la dirección IP del cliente estará en el campo *id.orig_h*.
- **http.log:** el campo *username* contiene el nombre de usuario declarado por el cliente, y la dirección IP del cliente estará en el campo *id.orig_h*, o puede indicarse en el campo *proxied* si la conexión se hizo con proxy. Si se hizo con proxy, el campo *id.orig_h* contendrá la dirección IP del proxy.
- **ntlm.log:** el campo *username* contiene el nombre de usuario declarado por el cliente, y la dirección IP del cliente estará en el campo *id.orig_h*.
- **kerberos.log:** en un entorno Windows, las solicitudes de kerberos contienen el nombre de usuario en el campo *client* (excepto las solicitudes en las que el campo *client* contiene un nombre que termina en $, lo que significa que la identidad declarada es un dispositivo, y el campo *id.orig_h* es la dirección IP del dispositivo de origen. El campo *client* suele estructurarse como USERNAME/EXAMPLEDOMAIN.COM donde USERNAME es el nombre de usuario y EXAMPLEDOMAIN.COM es el nombre del dominio de Windows y el nombre del reino de Kerberos.

Unas palabras de advertencia sobre la extracción de conclusiones sobre la identidad de un equipo o el usuario de un dispositivo: conozca sus límites (y los límites de los datos). El hecho de que se haya registrado un nombre de usuario en el tráfico de la red no significa que la persona real con ese nombre sea la responsable, tan solo es una pista. Debería comprobar si el usuario se autenticó con éxito, ya que los ciberespías y saboteadores patrocinados por el Estado han experimentado cada vez más con la plantación de banderas falsas.[4] El nombre de usuario podría haber sido *declarado*, pero si la autenticación falló, entonces no es un indicador claro de que el usuario estaba involucrado. No olvide que los dispositivos y el software pueden almacenar en caché las credenciales, por lo que la cuenta de usuario puede estar activa, pero la persona real podría seguir siendo inocente. Debe seguir recopilando información antes de poder confirmar un comportamiento malicioso.

Por ejemplo:

- Un usuario se va a comer y deja su dispositivo desbloqueado
- Un dispositivo está siendo atacado con un Troyano de acceso remoto (RAT, por sus siglas en inglés) y un usuario al otro lado del mundo está asumiendo la identidad de nuestra víctima de manera encubierta, *mientras que el usuario original también está utilizando el dispositivo simultáneamente para llevar a cabo su actividad habitual.*
- Un usuario malintencionado dentro de la organización ha escuchado a un compañero de trabajo decir su contraseña en voz alta en una conversación, y ahora está tratando de utilizar esas credenciales para iniciar sesión en otros sistemas

Además, asegúrese de entender qué información controlan y declaran los clientes o servidores, y considere quién controla cada uno de ellos. Si un adversario está dentro de su red, determinar qué información es fiable es primordial a la hora de preparar el plan de respuesta. Por ejemplo, un intruso podría desactivar el DHCP y asignar estáticamente una dirección IP y utilizarla para navegar por la red, dificultando la identificación, ya que los registros del servidor DHCP proporcionarían información contradictoria. Además, cuando un cliente solicita una dirección DHCP, un intruso podría proporcionar una dirección MAC falsa. De ahí la importancia de capturar registros pasivos en el momento en que se produce el evento.

Cómo buscar TTP específicos

Acceso inicial

El acceso inicial es el momento en que los intrusos establecen su punto de apoyo inicial.

Ataque drive-by

Un ataque drive-by (oculta) suele producirse cuando se descarga un archivo de manera encubierta desde un sitio web que está siendo atacado. Cuando se buscan signos de ataques drive-by en los datos de Corelight, el objetivo principal son las descargas de sitios web externos.

Comience la búsqueda con el registro *http* y busque señales de ejecutables descargados:

1. Comience con los registros http donde *resp_fuids* no está vacío. Esto significa que el respondedor devolvió un archivo.
2. Si el volumen de datos es demasiado grande, filtre los respondedores locales (en la red). Puede filtrar uniendo los resultados al registro *conn* en el UID, y luego filtrando cualquier registro en el que *local_resp* sea "*true*" en el registro conn.
3. Revise los *resp_mime_types* del registro *http* y filtre los resultados no interesantes (por ejemplo, imágenes, texto, respuestas OCSP y certificados). A menudo los resultados más interesantes son los ejecutables, los dlls y los archivos/contenedores
4. Agrupe los resultados por los campos host y *resp_mime_types* para facilitar el análisis.

Examine los resultados y busque cualquier cosa interesante o extraña, como descargas de archivos ejecutables, o la extensión del archivo y la falta de coincidencia de tipo MIME.

A medida que más atacantes pasen a utilizar TLS para cifrar los intercambios entre clientes atacados y los sitios web que controlan, menos visibilidad habrá a través del registro *http*. Para recuperar esta visibilidad, considere la posibilidad de utilizar una solución de descifrado SSL empresarial y pasar el tráfico HTTP descifrado a su sensor Corelight.

Servicios remotos externos

Los servicios remotos externos son utilizados por los adversarios para conectarse a los recursos de la red interna, y la búsqueda del uso indebido de los servicios remotos suele implicar dos pasos: la detección y

el análisis. En primer lugar, debe detectar qué servicios remotos están en uso. En primer lugar, debería recopilarse la información sobre el inventario de activos y servicios, pero suele ser insuficiente. A menudo, se produce un "desvío" natural, ya que los equipos de TI realizan cambios en la infraestructura y se esfuerzan por mantener actualizada la documentación de los activos. Los usuarios empoderados lo dificultan al configurar activos y servicios sin involucrar o informar al departamento de TI, un proceso conocido como "TI en la sombra"

Servicios a distancia tradicionales, por ejemplo: RDP, VNC (*framebuffer* remoto) y SSH (*secure shell*) contienen un componente servidor y un componente cliente. Si tiene un servicio remoto alojado en su entorno, los atacantes pueden explotarlo externamente para atacar los equipos dentro de la red. Para identificar estos servicios, busque las entradas del registro *conn* en las que el campo *service* contenga rfb, rdp o ssh, y en las que *local_orig* sea *false* y *local_resp* sea *true*, o en las que la IP de origen (*id.orig_h*) sea externa y la IP de respuesta (*id.resp_h*) esté en la red de la organización. Tome nota de cualquier servidor RFP/VNC, RDP o SSH que esté aceptando conexiones desde internet.

Algunos servicios remotos funcionan a la inversa, es decir, se instala un agente en el dispositivo local, y este llega *desde* el interior de la red a un conjunto de servidores externos, por ejemplo, GoToMyPC y TeamViewer. Esta configuración está diseñada para ayudar a los usuarios (principalmente a los usuarios domésticos) que no controlan el NAT o el cortafuegos o no poseen los conocimientos necesarios para poder gestionar el reenvío de puertos o la gestión de reglas del cortafuegos.

Para descubrir si estos servicios remotos están en uso en su entorno, busque señales de conexiones salientes a los servicios. Por ejemplo, TeamViewer utiliza el puerto TCP 5938 para comunicarse con los servidores de TeamViewer, así que simplemente revise los registros *conn* donde id.resp_p es 5938, local_orig es *true* y local_resp es *false*. TeamViewer también utiliza SSL, y el nombre de dominio de las conexiones debe ser *.teamviewer.com, por lo que adicionalmente puede buscar entradas en el registro ssl en las que el nombre_del_servidor contenga, o mejor aún, termine en "teamviewer.com" (Nota: como esta sesión funciona a la inversa, el *id.orig_h* es el dispositivo de su red que tiene instalado el cliente TeamViewer) En nuestro segundo ejemplo, GoToMyPC, intenta contactar con poll.gotomypc.com. Examine el campo *host* del registro *http* para poll.gotomypc.com, o las entradas en el registro ssl en las que *server_name* sea *poll.gotomypc.com*. Para cada paquete de software de cliente, la lista de puertos y nombres de dominio varía.

Ahora que hemos hablado de la detección de servicios remotos, debería comparar los datos de Corelight con una lista de todos los servicios remotos que ofrece el departamento de TI, como, por ejemplo:

- Puertas de enlace RDP
- Puertas de enlace VDI (infraestructura de escritorio virtual, por sus siglas en inglés)
- Puertas de enlace VPN (red privada virtual, por sus siglas en inglés)
- Servidores SSH

Para cada servicio expuesto a Internet, agregue una lista de conexiones a ese servicio desde el registro *conn*, e incluya los siguientes campos:

- *id.orig_h*: Dirección IP de origen (cliente)
- *id.resp_h*: Dirección IP de respuesta (servidor)
- *id.resp_p*: Puerto de respuesta
- *service*: el protocolo de aplicación que Zeek detectó
- *history*: el historial de la conexión, por ejemplo, qué tipos de indicadores TCP se vieron
- *orig_cc*: El código de país de origen

Al filtrar los registros, asegúrese de que el campo *hystory* empieza por "Sh". En el caso de las conexiones TCP, esto significa que el originador envió un SYN y el respondedor respondió con un SYNACK (apretón de manos). Esta comprobación elimina las conexiones en las que el servidor no está escuchando, o hay un cortafuegos que bloquea la conexión.

Una vez que haya reunido todos los datos, comience a examinar los registros en busca de algo interesante, como una conexión de un país que no se espera. Utilice el UID del registro *conn* para hacer un seguimiento de los registros de Zeek específicos de la aplicación (rdp, rfb, ssh). Por ejemplo, el registro rdp contiene más detalles sobre la conexión, como el campo *cookie* que puede contener el nombre de usuario del usuario que se autentica. El último paso es comprobar con el usuario si estaba utilizando activamente el sistema en ese momento.

Los clientes de Corelight tienen acceso a la Colección de Tráfico Cifrado (ETC, por sus siglas en inglés) que genera inferencias, o conocimientos, sobre el tráfico cifrado. El registro ssh contiene información interesante inferida sobre la conexión SSH, como, por ejemplo:

- KS para las conexiones que parecen contener pulsaciones de teclas del cliente
- FU y FD para las conexiones que parecen contener una carga o descarga de archivos, respectivamente
- ABP para las conexiones que parecen no contener ninguna autenticación, pero que aun así tienen éxito ("salto de autenticación")
- SV o SC para los clientes que parecen estar explorando la versión o la capacidad, respectivamente

Si desea obtener más información sobre Corelight ETC, póngase en contacto con nuestro equipo de ventas en el teléfono (510) 281-0760

Adjunto de spearphishing

Como método de entrada en una organización, un adversario puede enviar un archivo adjunto malicioso bien elaborado a una persona o a un pequeño grupo en una campaña de spearphishing. El archivo adjunto puede ser un documento que ordena al usuario realizar alguna acción, como hacer clic en un enlace o iniciar sesión en un portal; o puede ser un archivo creado para explotar una vulnerabilidad en el software utilizado para abrirlo, como Adobe Acrobat o Microsoft Word.

El registro smtp de Corelight contiene registros en el campo *fuids* si hubo algún archivo adjunto a un mensaje entregado por SMTP. Este campo se puede utilizar para pivotar al registro de archivos que

contiene información detallada sobre el archivo, incluyendo el nombre del archivo, los hashes y la fuente. Por ejemplo:

```
path: smtp
from: Tu amigo <Jeremy.Rigeur@gmail.com>
    fuids: [ Fh5GBc1wdVp3x9MKxc ]
    mailfrom: attacker@fake-mail.com
    rcptto: [ victim@corp-mail.com ]
subject: Definitivamente esto no es spearphish
    to: [ victim@corp-mail.com ]
    uid: CzKseq1Y3zo2qsTYH5
    user_agent: Apple Mail (2.3608.80.23.2.2)

    path: archivos
    conn_uids: [ CzKseq1Y3zo2qsTYH5 ]
    filename: WIRE_FRAUD.pdf
    fuid: Fh5GBc1wdVp3x9MKxc
    md5: e71c36cddd2aa42670d89d63e653d1da
    mime_type: application/pdf
sha1: bb24829550c0ca17db73d80a1d2f969e3b06ff5f
source: SMTP
```

Para buscar posibles intentos de spearphishing, puede buscar en el registro de archivos:

1. El valor del campo *source* es SMTP.
2. Filtre los valores de *mime_type* o *filename* que no sean interesantes, como se ha mencionado anteriormente.
3. Utilice el hash (MD5, SHA1 o SHA256) con un servicio de archivos de reputación (como Virustotal) para buscar archivos maliciosos conocidos.

Además, puede comenzar desde el registro de smtp:

1. Para reducir los datos busque las entradas en las que el campo *fuids* no esté vacío.
2. Filtre las combinaciones buenas conocidas de los valores *mailfrom* y *from*.
3. Filtre los valores *subject* que no son interesantes.
4. Considere la posibilidad de utilizar el valor *fuid* de los registros restantes para pivotar al registro de archivos para obtener más información sobre el archivo.

Corelight puede realizar una extracción de archivos a alta velocidad y puede filtrar en función del tipo MIME, de modo que cualquier archivo interesante, como los ejecutables, los documentos de Office y los PDF, están disponibles para un mayor escrutinio si se desea.

Gran parte del correo que cruza internet hoy en día está cifrado a través de STARTTLS sobre el protocolo SMTP, y esto dificulta la visibilidad. Para lograr una mejor visibilidad sin sacrificar la privacidad y la

seguridad de sus usuarios, es una buena práctica aceptar el SMTP entrante en un sistema que soporte STARTTLS, y luego enviar el correo por proxy al sistema de correo interno, para que Corelight pueda generar los registros correspondientes.

Enlace de spearphishing

En lugar de enviar archivos a una organización donde puedan ser examinados por un filtro de correo corporativo, algunos adversarios envían correos electrónicos que solo contienen enlaces. Estos enlaces conducen a sitios web controlados por el atacante, e intentan engañar al usuario:

- Pidiéndoles que introduzcan credenciales que los atacantes recopilan
- Explotando una vulnerabilidad en el navegador del usuario
- Descargando un archivo para explotar otra aplicación en el dispositivo del usuario

Los sensores de Corelight tienen un paquete[5] que puede registrar los enlaces de los mensajes SMTP en un registro separado, el registro smtp_links. Este registro contiene un campo *fuid*, que enlaza el registro smtp_links con el registro smtp. Puede pivotar rápidamente al registro smtp con los detalles sobre el mensaje que contenía el enlace malicioso.

Por ejemplo:

path: smtp_links
fuid: FhahXA1eJ32gHvNP27
id.orig_h: 172.16.0.10
id.orig_p: 62345
id.resp_h: 10.0.1.10
id.resp_p: 25,
link: http://www.hamsterwaffle.com/dl.php?id=jimmydean37
uid: C62txO1FHoJFJpsgP1

path: smtp
from: Tu amigo <Jeremy.Rigeur@gmail.com>
fuids: [FhahXA1eJ32gHvNP27]
mailfrom: attacker@fake-mail.com
rcptto: [victim@corp-mail.com]
subject: Haga clic en este enlace
to: [victim@corp-mail.com]
uid: C62txO1FHoJFJpsgP1
user_agent: Apple Mail (2.3608.80.23.2.2)

Para buscar enlaces de spearphishing, comience con el registro smtp_links y revise el campo *link*, filtrando los dominios inofensivos hasta encontrar resultados interesantes. Otra opción es unir el registro smtp_links al registro smtp a través del campo *fuids* o *uid*, y filtrar las combinaciones benignas de los campos *mailfrom* y *from* para buscar mensajes de remitentes únicos.

Gran parte del correo que cruza internet hoy en día está cifrado a través de STARTTLS sobre SMTP. Para lograr una mejor visibilidad sin sacrificar la privacidad y la seguridad de sus usuarios, es una buena práctica aceptar el SMTP entrante en un sistema que soporte STARTTLS, y luego enviar el correo por proxy al sistema de correo interno, para que una solución Corelight pueda generar los registros correspondientes.

Ejecución

El adversario está tratando de ejecutar un código malicioso.

Interfaz de línea de comandos, PowerShell

Los scripts de la interfaz de línea de comandos se han utilizado durante mucho tiempo para gestionar los sistemas basados en *nix, y la capacidad de construir y ejecutar scripts es a menudo explotada por los atacantes. Durante años no hubo un equivalente disponible en Windows, y a principios de la década de 2000 Microsoft comenzó a desarrollar un nuevo enfoque para la gestión de la línea de comandos. Poco después se creó PowerShell (PS) 1.0. PS, en sus diversas iteraciones, es una herramienta integrada basada en el marco .NET que se utiliza para automatizar las tareas de administración del sistema. Proporciona una interfaz para que los usuarios accedan a los servicios del sistema operativo Windows.

Aunque ciertos comandos de PS están restringidos por defecto, hay muchos comandos disponibles para obtener información del sistema sin un archivo ejecutable. Puede utilizar las extensiones LNK para saltarse las protecciones y ejecutar un script PS. Los archivos LNK suelen verse como accesos directos, que generalmente se encuentran en el Escritorio y el Menú de inicio de los usuarios.

Los archivos LNK maliciosos suelen estar incrustados dentro de lo que parecen ser documentos o imágenes legítimas. Una vez abierto, el LNK ejecuta una aplicación legítima de Windows CMD.exe o MSHTA.exe para eludir la configuración de seguridad.

Las capacidades de extracción de archivos de Corelight y su integración con varias plataformas de inteligencia proporcionan información sobre el malware oculto por tipo de archivo. Utilizando el filtrado integrado de Corelight, puede ajustar los parámetros de extracción de archivos para dirigirse a tipos MIME específicos que se utilizan habitualmente para la distribución de malware, entre ellos:

- Archivos comprimidos
- Microsoft Office (Word, PowerPoint, etc.)
- Archivos PDF
- Archivos TXT (powershell, vbs)

Persistencia

La persistencia es el intento del adversario de mantener su punto de apoyo.

Trabajos de BITS

El Servicio de Transferencia Inteligente en Segundo Plano (BITS) de Microsoft fue creado en 2001 como un mecanismo para gestionar las transferencias de archivos que minimizan las interrupciones para el

usuario final. BITS se utiliza habitualmente para descargar las actualizaciones de Windows y de otros programas de los principales proveedores.

Los atacantes tienen dos métodos para hacer un mal uso de BITS:

- Lo más común es crear un trabajo de transferencia de BITS directamente en un host, lo que permite una descarga de cargas útiles secundarias a través de un servicio de Windows incorporado que suele eludir los cortafuegos y otros controles de seguridad.
- Otra alternativa es exfiltrar datos a través de un trabajo de carga de BITS. Las cargas deben conectarse a un servidor IIS para que BITS funcione correctamente, pero este requisito es trivial que los autores de malware pueden eludir.

Las transferencias de datos mediante el servicio BITS pueden realizarse a través de HTTP, SSL y SMB. Cuando BITS utiliza el tráfico HTTP, hay una cadena Usuario-Agente distintiva de "Microsoft BITS/7.5" (o 7.8 en versiones posteriores). Lamentablemente, no hay características distintivas del tráfico de red BITS SSL y SMB. Por lo tanto, la presencia del tráfico de red de BITS no es necesariamente sospechosa, porque está presente en cualquier lugar en que haya equipos de Windows conectados a Internet. Los analistas aún pueden utilizar los datos de Corelight para evaluar si el tráfico de BITS es legítimo, analizando los sistemas remotos que se utilizan para las transferencias de datos de BITS. Si están fuera de las redes de CDN o de los principales proveedores de software, todas las cargas de BITS deben ser investigadas hasta que se demuestre que son benignas, ya que este caso de uso es especialmente raro entre los proveedores de software legítimos.

El ejemplo de código que se muestra a continuación es un registro *http* que muestra el aspecto de los datos de BITS si es a través de HTTP.

path: http,
uid: Ca9LrF3xl5kVCxe2K4,
id.orig_h: 10.10.199.31,
id.orig_p: 49987,
id.resp_h: 151.205.0.135,
id.resp_p: 80,
trans_depth: 1,
method: GET,host:151.205.0.135,
uri:/pdata/0731497c8fa1dce5/download.windowsupdate.com/d/msdownload/update/software/secu/2018/05/windows10.0-kb4103723-x64_0722ab30824410046f954417ada8556d2ac308a6.cab,
version: 1.1,
user_agent: Microsoft BITS/7.8,
request_body_len: 0,
response_body_len: 1333068983,
status_code: 200,
status_msg: OK,
resp_fuids: FD283F3hrZH8yzYmb8,
resp_filenames: windows10.0-kb4103723-x64_0722ab30824410046f954417ada8556d2ac308a6.cab,
resp_mime_types: [application/vnd.ms-cab-compressed],
accept_encoding: identity,
accept: */*

Servicios remotos externos

- Véase *Acceso inicial: Servicios remotos externos*

Golpeo de puertos

El golpeo de puertos es una técnica para conseguir que un sistema remoto permita el acceso a un puerto que de otro modo estaría cerrado. Suele consistir en una secuencia predefinida de conexiones a otros puertos (a menudo cerrados), a veces con señales especiales a nivel de protocolo, cadenas de banners de capa 7, etc.

Zeek resume cada conexión TCP, UDP e ICMP en el registro *conn*. Este registro detallado proporciona estadísticas útiles sobre las conexiones. Los campos *history*, *conn_state* y *network tuple* (src/dest ip/port) proporcionan la información necesaria para ver los golpes de puerto. Es importante señalar que detectar los golpes de puerto sin una pista adicional puede ser una tarea desalentadora, ya que es fácil ocultar las secuencias intencionales de conexiones entre el ruido de una red típica.

Componente de software del servidor: Web shell

Un web shell es un comando web ejecutado a través de internet. Un web shell es generalmente una página web maliciosa o un fragmento de código introducido en un servidor web o aplicación existente para proporcionar un acceso no autorizado. Este acceso puede ser un shell CLI real, una herramienta de gestión de archivos o de acceso a bases de datos. Se trata de una táctica común porque el tráfico malicioso se combina con el tráfico inofensivo hacia/desde el servidor web, y puede ser difícil de identificar a través de las firmas IDS porque los detalles del web shell se cambian fácilmente.

Cuando se ejecuta un web shell, se ejecuta con permisos de usuario del software del servidor web, que deben ser limitados. Los atacantes utilizan los web shells para intentar ataques de escalada de privilegios explotando las vulnerabilidades locales del sistema para asumir privilegios de root.

La detección de web shells en la red mediante detecciones basadas en firmas es relativamente sencilla: los web shells tienen rutas de archivos específicas, métodos de comunicación u otros comportamientos que pueden activar una alerta. Como la mayoría de los indicadores de ataque "atómicos", son fáciles de evadir porque identifican comportamientos específicos que pueden cambiarse fácilmente. Siempre que sea posible, debe complementar la detección de firmas con un programa de búsqueda de amenazas para encontrar comportamientos más generales de actividad anómala.

Los web shells intentan ocultar la actividad maliciosa en el tráfico HTTP normal, por lo que el http.log es una excelente fuente de datos para investigar la actividad de los web shells. Algunos ejemplos de hipótesis de búsqueda apoyadas por los datos HTTP de Corelight son:

- Actividad inusual de HTTP POST. Esto puede ser tan sencillo como que aparezcan HTTP POST inesperados en el campo *method* del http.log donde se esperan GET (si el sitio afectado está sirviendo principalmente contenido).

El tráfico web "normal" se dirige a una lista corta de páginas comunes, con navegación a través de un hipervínculo interno. Un web shell va directamente a la página oculta y aparece como una solicitud HTTP sin página de referencia. Además, el tráfico web muestra una variedad de IP solicitantes, cadenas de usuario-agente, JA3, etc. Un web shell puede tener un grupo de usuarios más homogéneo.

- Detectar inicios de sesión sospechosos que se originan en subredes internas hacia servidores DMZ y viceversa.

Este tipo de análisis de búsqueda y detección de anomalías es una forma eficaz de identificar la actividad maliciosa (o sospechosa), pero las redes modernas son lugares ruidosos y caóticos. Como en la mayoría de las búsquedas, hay que saber qué aspecto tienen los datos "normales" para poder filtrarlos con éxito.
(https://github.com/nsacyber/Mitigating-Web-Shells)

Evasión de defensas

La evasión de defensas consiste en técnicas que los adversarios utilizan para evitar la detección a lo largo de su ataque.

Trabajos de BITS

- Véase *Persistencia: Trabajos de BITS*

Golpeo de puertos

- Véase *Persistencia: Golpeo de puertos*

Instalación del certificado raíz

Los certificados públicos se utilizan para establecer comunicaciones seguras TLS/SSL. Los certificados raíz se utilizan para identificar a la autoridad certificadora raíz (AC). Los certificados raíz son autofirmados y constituyen una base de confianza para el cifrado de clave pública. Por ejemplo, cuando se instala un certificado raíz, el sistema o la aplicación confiará en los certificados de la cadena de confianza de la raíz. Aunque ningún dispositivo a nivel de red (por ejemplo, routers y switches) puede mostrar la cadena de certificados instalada en un sistema cliente, el objetivo de instalar un certificado raíz malicioso es eludir la validación de confianza.

Utilizando los datos de Corelight, puede observar todos los aspectos de la sesión TLS/SSL utilizando los registros ssl y x509. Estos dos registros permiten a los analistas identificar los certificados que parecen sospechosos:

1. Buscando en el registro ssl cualquier entrada en la que el campo *validation_status* no tenga el valor *ok*.
2. Revisando los registros en los que el campo *validation_status* tiene un certificado autofirmado o contiene un certificado autofirmado en la cadena de certificados.
3. Revisando los campos *subject* y *server_name* para determinar la probable organización o sitio web que controla el servidor.
4. Filtrando los resultados cuando hay certificados legítimos autofirmados en uso, como en las comunicaciones entre los dispositivos IOT y la infraestructura de la nube de apoyo.
5. Investigando la dirección IP *id.resp_h* para ver a qué Sistema Autónomo pertenece la sesión y si es una organización de AS razonable (como la organización que coincide con la información del servidor, o un proveedor de alojamiento en la nube de uso común).
6. Para las conexiones restantes, utilice los valores de *cert_chain_fuids* para pivotar a los certificados en el registro x509 y revisar los detalles del certificado.

Centre sus investigaciones inspeccionando la autoridad local de certificados raíz en el terminal.

Acceso a las credenciales

El acceso a las credenciales se produce cuando el adversario intenta robar nombres de cuentas y contraseñas.

Fuerza bruta

Un adversario intenta obtener acceso no autorizado adivinando sistemáticamente la contraseña de un usuario mediante un mecanismo repetitivo o iterativo. A veces un ataque de fuerza bruta se origina a partir de una lista de información conocida, lo que aumenta la probabilidad de éxito.

Por ejemplo, un atacante que intente adivinar la contraseña de una cuenta de Active Directory, probablemente se conecte a un Controlador de dominio en el puerto LDAP (389 o 636). Un atacante que intenta descubrir URL API en un sistema de comercio electrónico genera muchas más conexiones al servidor web que otros clientes en un periodo de tiempo similar y crea más códigos de estado HTTP en el rango 400 y 500 (errores) en comparación con otros clientes.

Para buscar un ataque de fuerza bruta:

1. En el registro *conn*, agregue por *id.orig_h*, *id.resp_h*, *id.resp_p*, *proto* y (opcionalmente) servicio.
2. Añada un recuento para el número de operaciones y ordene por los recuentos más altos.
3. Elija un periodo de tiempo que tenga sentido, basado en el tamaño de la red/conjunto de datos, comenzando con poco y aumentando gradualmente.
4. Filtre los registros que son obviamente permisibles, como los contactos repetidos de los sistemas de supervisión del rendimiento de la red o de las aplicaciones, los sistemas de gestión de la vulnerabilidad o las aplicaciones empresariales.
5. Para los registros desconocidos o sospechosos, realice una investigación más profunda sobre ese comportamiento. Por ejemplo, busque otras conexiones originadas en la dirección IP remota.
6. En el caso de los protocolos que pueden mantener las conexiones a lo largo de múltiples transacciones o intentos, busque conexiones de larga duración. Estas conexiones de larga duración también pueden indicar un comportamiento repetitivo.

Los sensores de Corelight incluyen un script que registra las conexiones que se mantienen durante más tiempo que un conjunto de umbrales, empezando por diez minutos y continuando hasta tres días. Si no es cliente de Corelight, pero utiliza Zeek de código abierto, este script está disponible a través de la página GitHub de Corelight.

Para buscar conexiones largas con el paquete *Long Connections* instalado:

1. Examine el registro de avisos.
2. Revise las entradas en las que la nota es "LongConnection::found",
3. Revise cada conjunto de *id.orig_h*, *id.resp_h, id.resp_p* para entender si estos dispositivos deben tener conexiones largas.

Para buscar conexiones largas si nel paquete *Long Connections* instalado:

1. Examine el registro *conn*.
2. Recopile una lista de todas las conexiones con los siguientes campos para cada una: *id.orig_h*, *id.resp_h*, *id.resp_p*, *proto*, *service* y *duration*. Esto solo incluye las conexiones que se completaron, ya sea correctamente o a través de un tiempo de espera. Las conexiones abiertas actualmente no están representadas en los resultados.

3. Ordene los resultados por duración, colocando en primer lugar las conexiones más largas.
4. Analice cada resultado para determinar si es un comportamiento legítimo o esperado.
5. Filtre los comportamientos esperados e investigue a fondo todo lo que parezca sospechoso.

Corelight también le ofrece ETC (Recopilación de tráfico cifrado), que busca automáticamente los intentos de adivinar la contraseña por fuerza bruta contra los servidores SSH dentro de una única conexión.

Autenticación forzada

Algunos protocolos autentican automáticamente cuando un usuario accede a un recurso sin comprobar primero si el recurso al que se accede es de confianza. Por ejemplo, un atacante puede incrustar una referencia en un documento de Microsoft Office a un archivo que está alojado en una ruta UNC controlada por el atacante (\servername\sharename\path\to\file). Cuando el usuario abre el archivo, el equipo intenta acceder al recurso. El servidor controlado por el atacante desafía entonces al equipo para que se autentique y, en la mayoría de las circunstancias, el equipo víctima proporciona automáticamente las credenciales almacenadas en caché, normalmente en forma de un hash NTLM. El atacante puede entonces intentar utilizar las credenciales para un acceso no autorizado, normalmente invirtiendo el hash para obtener la contraseña, o reutilizando el hash en un ataque de "pasar el hash".

Este método requiere que el atacante controle la infraestructura del servidor. En consecuencia, el vector de ataque más probable es el spearphishing. El atacante suplanta a un usuario en la red, y el equipo víctima se comunica con el servidor controlado por el atacante a través de internet. Para buscar este comportamiento, busque la autenticación a través de internet:

1. Busque en el registro ntlm cualquier signo de autenticación NTLM en el que la IP de destino esté en la red externa.
2. Busque entradas en el registro *conn* en las que el campo *service* contenga smb (o ntlm), y *local_resp* sea *false*.

En el envenenamiento LLMNR o NBT-NS, un atacante escucha las emisiones locales de LLMNR o NBT-NS pidiendo un recurso concreto por su nombre. El atacante responde entonces al cliente consultante falseando el recurso real. Si el recurso es de los que requiere autenticación normalmente, entonces el atacante puede solicitar al cliente que se autentique. Cuando el cliente se autentica, normalmente con un hash de contraseña, el atacante utiliza las credenciales para hacerse pasar por el cliente y acceder a los recursos.

Se pueden buscar eficazmente estos ataques con los datos de Corelight, pero el sensor tiene que estar dentro del dominio de difusión porque el tráfico de difusión no suele atravesar los routers. Normalmente se necesita extender o reflejar VLAN enteras, o reenviar el tráfico LLMNR o NBT-NS de subredes de clientes y VLAN, a lugares de la red que Corelight está monitorizando.

Busque los registros dns en los que *id.resp*_p=5355 (LLMNR) o *id.resp_p*=137 (NBT-NS), y filtre los registros en los que el campo *answers* no esté vacío. A continuación, cuente el número de campos *query* distintos por *id.resp_h*. Esta búsqueda arroja IP que responden a más de un nombre.

Rastreo de la red

No se puede detectar a un intruso que está rastreando el tráfico de su red utilizando los registros de red porque la acción es invisible; sin embargo, se *puede detectar a un intruso rastreando en su propia red* porque su adversario no puede verlo.

Los sensores Corelight le permiten desplegar una red de sensores fuera de banda que genera registros vinculados. Estos registros aceleran la observación y la detección fiables, y ayudan a evitar el escollo de la dependencia de la prevención, al tiempo que proporcionan el contexto para un análisis histórico más profundo y preciso. Como dijo Rob Joyce, jefe de la división de Operaciones de Acceso a Medida de la NSA, en su charla de USENIX de 2016: "Estamos haciendo explotación de estados-nación... ¿qué puedes hacer para defenderte y hacerme la vida imposible?"

Detección

El adversario está tratando de conocer su entorno.

Exploración de servicios de red

Para determinar qué dispositivos de una red son explotables, y los servicios disponibles en esos dispositivos, un intruso puede emplear la exploración activa. Los métodos de exploración activa incluyen:

- Exploración horizontal: Enviar solicitudes de conexión a un puerto específico a través de muchas IP para ver qué IP responden. Por ejemplo, la exploración de muchos dispositivos en el puerto TCP/22 suele revelar los dispositivos que utilizan un servidor SSH. La exploración de muchos dispositivos en el puerto TCP/445 puede enumerar eficazmente la infraestructura de Windows.
- Exploración vertical: Enviar solicitudes de conexión a una única dirección IP a través de muchos puertos para ver qué puertos responden. Este método permite a los atacantes inferir los servicios disponibles desde esa dirección IP.

Cada uno de estos métodos se puede llevar a cabo utilizando un escáner de vulnerabilidades gratuito o disponible en el mercado. Estos productos suelen añadir otra lógica para comprobar la disponibilidad del servicio, la información de la versión y si los servicios son vulnerables a técnicas de explotación conocidas.

Si un intruso utiliza uno o más de los métodos anteriores para intentar detectar el servicio, el resultado es una conexión *fallida* o *rechazada*. En los datos de Corelight, estos se registran en el registro *conn* como conexiones con un *conn_state* de S0 (iniciadas e ignoradas) o REJ (iniciadas y rechazadas), y suelen tener un campo *history* en el que no hay ninguna "D" (datos posteriores a la sincronización del iniciador). Para buscar la exploración del servicio de red interna de la red:

1. Busque entradas en el registro *conn* donde *conn_state* sea S0 REJ.
2. Filtre los registros donde *local_orig=true* y *local_resp=true*.
3. Agrupe y cuente los resultados por el *id.orig_h*, y el número de *id.resp_p* únicos, para evaluar la horizontalidad/verticalidad de la exploración.
4. Inspeccione la lista, empezando por los registros que tienen el mayor número de *id.resp_h* o *id.resp_p*.
5. Identifique al originador (*id.orig_h*) y revise la lista de respondedores (*id.resp_h*) y puertos (*id.resp_p*).
6. Determine si el comportamiento es aceptable basándose en la identidad de la fuente, los puertos implicados y los destinos.

No todos los elementos de la lista son maliciosos. Los servidores DHCP, por ejemplo, suelen estar configurados para hacer ping a una dirección IP para confirmar si la dirección está en uso antes de asignarla desde el pool. Los servidores de impresión con un gran número de colas de impresión intentan servicios de impresión SNMP o de red a las impresoras, incluso si esas impresoras están desconectadas. Por este motivo, los servidores de impresión pueden provocar un gran número de conexiones S0. Por supuesto, un programa que explore legítimamente, como un escáner de vulnerabilidades aprobado por la empresa o un sistema de gestión de inventario, podría aparecer en la lista. Por último, los ingenieros de red realizan una exploración de la red ad hoc para la resolución de

problemas. Si se encuentra con la exploración de red, modifique la consulta original para omitir los registros que se sabe que son inofensivos, y luego reanude la búsqueda.

Detección de red compartida

El protocolo para compartir red al que más recurren los atacantes es SMB, el estándar para compartir archivos de Windows. Todos los sistemas operativos modernos admiten SMB. Los documentos de alto valor que almacenan información personal, secretos comerciales, diagramas de red y otros datos sensibles, normalmente residen en recursos compartidos SMB en empresas de todos los tamaños.

La búsqueda y detección de recursos compartidos en un servidor SMB se realiza normalmente mediante un comando DCE/RPC en el puerto TCP 445. En concreto, una conexión a la tubería "srvsvc" (que aparece en los registros *dce_rpc* como un terminal con el mismo nombre) va seguida de una llamada a las funciones NetShareEnumAll o NetShareEnum (llamadas "operaciones" en el registro de Zeek). Estas llamadas a funciones se utilizan para fines legítimos de intercambio de archivos, y por sí solas no son indicadores suficientes de una intención maliciosa. Sin embargo, en combinación con otros indicadores de movimiento lateral, ilustran cómo un atacante se movió lateralmente dentro de una red. Los objetivos principales para una mayor investigación son aquellos que generan un gran número de llamadas a funciones DCE_RPC a través de un gran número de hosts en un periodo corto.

Rastreo de la red (referencia X)

- Véase Acceso a las credenciales: Rastreo de la red

Detección de sistema remoto

Los mismos principios para detectar la Exploración de servicios de red se aplican a la detección de sistemas remotos. Consulte este apartado para obtener más información.

Movimiento lateral

El movimiento lateral es lo que utilizan los adversarios para entrar y controlar sistemas remotos en una red.

Protocolo de escritorio remoto

El Protocolo de Escritorio Remoto de Microsoft (RDP) se utiliza para controlar remotamente un terminal de Windows. Este protocolo puede ser utilizado por un atacante para obtener acceso no autorizado a su red (véase Acceso inicial: Servicios remotos externos). Una vez que un intruso está dentro, puede utilizar RDP para moverse lateralmente entre los dispositivos.

RDP es uno de los muchos protocolos analizados por Corelight. Para algunos entornos, la presencia de RDP, o su presencia en sistemas específicos, es suficiente para desencadenar una investigación. Para las redes en las que se permite RDP, el registro RDP de Zeek contiene mucha información que ayuda a establecer si una conexión es legítima, por ejemplo, registrando datos como la disposición del teclado, los niveles de cifrado o el nombre del cliente para una conexión.

Cuando haga una búsqueda con el registro rdp:

1. Céntrese en los campos *id.orig_h*, *id.resp_h*, *id.resp_p*, y cookie. El campo *cookie* puede contener cualquier valor arbitrario enviado por el cliente RDP al servidor, pero a menudo contiene el nombre de usuario enviado por el cliente RDP.
2. Agregue los registros basándose en estos cuatro campos y muestre un recuento para cada conjunto único.
3. Recorra el conjunto e identifique el origen y el destino de cada conexión (por ejemplo, puede utilizar los registros DNS y DHCP).
4. Algunas conexiones RDP utilizarán una disposición de teclado no estándar. Para detectarlo, examine el campo *keyboard_layout*. Cuente el número de instancias de cada valor y aplique el apilamiento de datos para buscar los valores marginales o poco frecuentes.
5. Identifique el origen y el destino y determine si se espera la disposición de teclado no estándar, por ejemplo, si se sabe que el usuario de origen tiene un idioma distinto del inglés como idioma principal, y ese idioma es el solicitado en la conexión RDP.

Una vez tenga esta información, hágase varias preguntas:

- ¿Coincide el valor de la cookie con el usuario esperado en el equipo de origen o de destino?
- ¿Existe una razón legítima para que el emisor utilice RDP?
- ¿Hay algún usuario que utilice RDP y que no se pueda esperar por su función?

Servicios remotos

La explotación de una vulnerabilidad de software se produce cuando un adversario se aprovecha de un error de programación para ejecutar un código controlado por el adversario. Esta explotación puede ocurrir en un programa, servicio o dentro del propio software del sistema operativo o kernel. Un objetivo común para la explotación de servicios remotos después de un ataque es el movimiento lateral.

Dada la complejidad de las redes empresariales actuales, a menudo se utilizan diversos servicios externos y de terceros. Estos servicios permiten a los atacantes obtener un acceso inicial o moverse lateralmente. Todas las conexiones se registran en *conn.log*, sin embargo, puede haber más detalles en los registros específicos del protocolo dependiendo de la naturaleza del servicio remoto atacado. Por ejemplo, puede supervisar el archivo *http.log* en busca de solicitudes HTTP sospechosas e inesperadas (como las solicitudes OPTIONS).

Path: http,
uid: CEeVS92Ljnr9jbW2J5,
id.orig_h: 54.235.163.229,
id.orig_p: 41855,
id.resp_h: 192.168.0.2,
id.resp_p: 80,
trans_depth: 1,
method: OPTIONS,
host: host-90-236-3-35.mobileonline.telia.com,
uri: *,

version: 1.1,

Además, Corelight extrae información sobre el software observado en la red en *software.log*. Este archivo proporciona a los defensores datos valiosos para vigilar los servidores inesperados o no autorizados, los servicios vulnerables o no actualizados y el software de cliente sin parches.

path: software,

host: 192.168.0.53,
software_type: SMTP::MAIL_CLIENT,
name: Microsoft Outlook Express,
version.major: 6,
version.minor: 0,
version.minor2: 2900,
version.minor3: 5512,
unparsed_version: Microsoft Outlook Express 6.00.2900.5512

Recursos compartidos de administrador de Windows

Los sistemas Windows tienen recursos compartidos de red ocultos a los que solo pueden acceder los administradores y que permiten copiar archivos de forma remota y realizar otras funciones administrativas. Algunos ejemplos de recursos compartidos de red son C$, ADMIN$ e IPC$.

Los atacantes suelen utilizar SMB para conectarse a recursos compartidos de administrador en estaciones de trabajo y servidores de Microsoft Windows. Es posible que quieran saber más sobre el objetivo, extraer archivos confidenciales, subir cargas útiles maliciosas o autenticarse para poder proceder con otras herramientas y ataques. Corelight supervisa el tráfico SMB, incluidos los intentos de autenticación, lo que permite a los defensores registrar y advertir patrones de intentos de autenticación administrativa, así como supervisar el tráfico SMB para extraer los archivos transferidos. El siguiente ejemplo demuestra la ejecución de la acción FILE_OPEN utilizando el recurso compartido oculto del administrador, e incluye la información de MAC. Corelight registra la acción realizada, incluyendo Abrir/Renombrar/Borrar/Escribir.

path: smb_files,
uid: CB3Ezw2X3tYKtxunq,
id.orig_h: 10.10.199.101,
id.orig_p: 49710,
id.resp_h: 10.10.199.31,
id.resp_p: 445,
action: SMB::FILE_OPEN,
path: \\\\10.10.199.31\\admin$,
name: <share_root>,
size: 24576,

times.modified: 2020-04-07T21:17:30.244159Z,
times.accessed: 2020-04-07T21:17:30.244159Z,
times.created: 2016-07-16T06:04:24.770745Z,
times.changed: 2020-04-07T21:17:30.244159Z

Recopilación

El adversario está tratando de reunir datos para lograr su objetivo.

Datos recopilados de archivo

Para ocultar los datos, los atacantes pueden consolidar los datos en archivos comprimidos, como archivos Zip, RAR, TAR o CAB. Para buscar esta técnica de ocultación, utilice el registro de archivos.

Para buscar archivos comprimidos:

1. Busque en todos los registros de archivos, recuperando los campos *tx_hosts*, *rx_hosts*, *mime_type*, *total_bytes* y *source*.
2. Elimine de los resultados los registros con *mime_types* poco interesantes, por ejemplo:
   a. application/x-x509-*
   b. application/ocsp*
   c. image/*
   d. audio/*
   e. video/*
   f. text/*
   g. application/xml
   h. application/chrome-ext

Recopilación automatizada

Los atacantes pueden desplegar herramientas automatizadas en un host atacado para supervisar los servicios de intranet en busca de datos confidenciales y secretos corporativos. Estas herramientas pueden incluir scripts para buscar (y copiar) información como el tipo de archivo, la ubicación o el nombre en intervalos de tiempo específicos. Los intrusos pueden utilizar herramientas de acceso remoto para llevar a cabo la recopilación automática.

Por ejemplo, una herramienta personalizada puede consultar un servidor web de la intranet o un servidor de correo electrónico interno, sondeando regularmente los nuevos contenidos. Corelight supervisa varios protocolos, como el tráfico HTTP, de correo electrónico, MySQL, FTP y SMB, para proporcionar información sobre estas consultas.

Al buscar el uso de la recopilación automatizada, los defensores pueden identificar las herramientas automatizadas observando las consultas repetitivas o las conexiones programadas regularmente. Por ejemplo, si un intruso está haciendo web scraping, habrá un gran número de conexiones desde un número finito de direcciones IP. Además, puede utilizar los registros SMB (smb_files o smb_mapping) para identificar patrones de tráfico anómalos.

Datos de la unidad compartida de red

Las unidades compartidas en red son un tesoro oculto de documentos corporativos confidenciales. La mayoría de las redes empresariales alojan unidades de red compartidas mediante SMB, pero algunas pueden recurrir a FTP, HTTP o incluso RDP. Zeek puede supervisar el acceso a las unidades de red compartidas cuando se utilizan protocolos como SMB, FTP o HTTP. Los protocolos de control remoto, como RDP, también se analizan en los registros específicos del protocolo. En cualquier lugar en el que Corelight vea este tráfico, lo analiza y registra en el registro específico del protocolo.

El siguiente ejemplo muestra el registro ftp. Corelight registra el comando y los argumentos.

path: ftp,
uid: C0EeI73um1Aw3rrOib,
id.orig_h: 10.0.0.11,
id.orig_p: 45831,
id.resp_h: 119.74.138.214,
id.resp_p: 21,
user: 1,
password: <hidden>,
command: RETR,
arg: ftp://119.74.138.214/doc.exe,
reply_msg: Transfer OK

Mando y control

El adversario intenta comunicarse con los sistemas atacados para controlarlos.

Puertos utilizados habitualmente/Puertos no estándar

Los adversarios pueden utilizar un puerto utilizado habitualmente para evitar una inspección más detallada.

La búsqueda de canales C2 en los puertos más utilizados es difícil, pero no imposible. Para buscar canales C2, busque puertos conocidos que se estén utilizando con un servicio poco común.

Cuando busque C2 utilizando puertos utilizados habitualmente:

1. Inicialmente, céntrese en el campo *service* y busque en el registro *conn* las entradas en las que el campo *service* no sea el que esperaría para el puerto estándar (el campo *service* podría ser un "-" u otro servicio).
   a. Empiece por los protocolos más habituales.
      - TCP:80 (HTTP) TCP:443 (HTTPS)
      - TCP:25 (SMTP)
      - TCP/UDP:53 (DNS)

2. La Recopilación de tráfico cifrado de Corelight contiene un paquete titulado Detección de cifrado. La Detección de cifrado genera un aviso cuando se observa tráfico de texto plano en puertos habitualmente cifrados. La observación de avisos para Viz::UnencryptedService pone de manifiesto este comportamiento y le ayuda a identificar las conexiones potencialmente maliciosas que utilizan puertos habituales.

El paquete de Recopilación de tráfico cifrado de Corelight también tiene una función que le notifica cuando una sesión utiliza el cifrado instantáneo. El paquete busca claves precompartidas o conexiones cifradas que se inician sin una negociación de claves tradicional. La observación de avisos para Viz::CustomCrypto pone de manifiesto este comportamiento y le ayuda a identificar las conexiones potencialmente maliciosas que utilizan puertos habituales.

Además, puede utilizar los registros de Corelight *dpd* y *weird* para identificar comportamientos inesperados del protocolo. Estos registros muestran errores de depuración y análisis e identifican el uso fuera de especificación de puertos y protocolos habituales, lo que podría indicar una actividad maliciosa o el uso encubierto de puertos y protocolos conocidos.

path: dpd,
uid: C5LNtk1n9NkT8m300j,
id.orig_h: 192.168.0.54,
id.orig_p: 52841,
id.resp_h: 54.89.42.30,
id.resp_p: 80,
proto: tcp,
analyzer: HTTP,
failure_reason: not a http request line

Canal cifrado

Consulte el apartado Puertos utilizados habitualmente para obtener una descripción del paquete de detección de cifrado de Corelight, el registro *dpd* y el registro *weird*. Esto le ayuda a identificar posibles protocolos criptográficos propios.

Canales de retorno, canales multietapa

Se sabe que los adversarios dividen las comunicaciones entre diferentes protocolos, utilizando uno para la entrada C2 y otro para la salida de datos. Esto permite que la comunicación se salte las restricciones del cortafuegos.

El malware que divide la comunicación entre dos hosts para las instrucciones y para la exfiltración introduce un nuevo reto para los defensores. Reconocer la relación entre el tráfico de control sospechoso y las grandes transferencias de datos es un reto, pero Zeek proporciona paquetes y marcos que sintetizan los datos. Por ejemplo, existe un paquete para determinar la relación productor-consumidor de las conexiones que identifica las transferencias de datos desequilibradas y posiblemente sospechosas.

Además, el Marco de inteligencia permite la coordinación con otros defensores al identificar posibles indicadores de ataque (direcciones IP, direcciones de correo electrónico y nombres de dominio) en los datos de Corelight.

Es difícil identificar a los atacantes que utilizan diferentes métodos y canales de comunicación, pero el contenido de Corelight, junto con los marcos y paquetes de Zeek pueden ayudar. Permiten a los defensores identificar los canales ocultos de forma discreta, proporcionando múltiples oportunidades de detección.

Además de vigilar los mecanismos de comunicación C2 mencionados anteriormente, estas son otras señales disponibles en los datos de Corelight:

- Utilice conn.log para identificar patrones de comunicación que indiquen canales adicionales (por ejemplo, utilizando *orig_h* y *resp_h* para limitar las conexiones a una ventana de tiempo y observar las conexiones entre los hosts que incluyen puertos extraños, conexiones fallidas o rechazadas, o elementos interesantes/sospechosos).
- Utilizar Corelight (ETC), o contenidos de elaboración propia, junto con la detección de registros de conexión para encontrar posibles relaciones entre conexiones superpuestas, adyacentes o interesantes.
- Busque secuencias de conexiones a hosts no relacionados usando diferentes protocolos o eventos en los registros *dpd* y *weird* como se describe en Puertos utilizados habitualmente.

Transferencia de herramientas de entrada

Los intrusos suelen trasladar archivos a los sistemas atacados, tanto herramientas que pueden ayudar a seguir realizando movimientos laterales, como archivos sensibles diseñados para la exfiltración. Estos archivos se mueven normalmente a través de una conexión HTTP(S), SSH o SMB.

Para los archivos que se mueven a través de HTTP en texto plano, detalles como el nombre del host remoto y el nombre y tipo MIME del archivo que se transfiere pueden ser indicadores útiles; los usuarios también deberían consultar el registro de archivos para los hashes de los archivos que se mueven, ya que muchas herramientas de ataque populares tienen hashes criptográficos conocidos que facilitan su identificación. En el caso de HTTPS, los defensores pueden utilizar la dirección IP del sistema remoto, así como los detalles del certificado anotados en el registro ssl (es decir, el nombre de la organización, el FQDN del host remoto del CN, etc.) para buscar conexiones anómalas.

Los intrusos copian archivos de un terminal a otro mientras se mueven lateralmente entre los activos comprometidos. Tradicionalmente, las copias de archivos hacia o desde sistemas Unix/Linux se realizan a través del protocolo SSH utilizando el comando scp. En los sistemas Windows, las cargas o descargas remotas de archivos suelen realizarse a través de SMB, pero también pueden utilizar SSH a través de PUTTY.

Los sensores Corelight con el paquete de inferencias ETC SSH activado amplían el registro ssh. La extensión incluye un campo de inferencias que añade características inferidas sobre el tráfico SSH. Por ejemplo, si la sesión se utiliza para mover archivos, o si es interactiva:

- LFU: Carga de archivos grandes
- LFD: Descarga de archivos grandes
- KS: Pulsaciones de teclas

Para empezar a buscar sesiones SSH interesantes, utilice el campo *inferences* del paquete ETC SSH:

1. Identifique las sesiones en las que el campo *inferences* contiene LFU, SFU, LFD o SFD
2. Determine si la actividad de los archivos a través de SSH es legítima y esperada

Los sensores Corelight están precargados con el paquete MITRE BZAR (Análisis e información basados en Bro/Zeek ATT&CK). MITRE BZAR identifica las técnicas de MITRE ATT&CK para la copia de archivos remotos, concretamente los archivos que se copian en los recursos compartidos C$ o ADMIN$. Este paquete genera entradas en el registro de avisos, como se muestra a continuación:

Path: notice,
uid: CiAtaM363GcEbU63zk,
id.orig_h: 192.168.38.104,
id.orig_p: 65431,
id.resp_h: 192.168.38.102,
id.resp_p: 445,
fuid: FSeaVF4qnjl8cT3HF8,
file_mime_type: text/plain,
file_desc: Windows\\Temp\\hbaVJpzdnG,
proto: tcp,
note: ATTACK::Lateral_Movement_Extracted_File,
msg: Guarda una copia del archivo escrito en el recurso compartido SMB admin,
sub: 2020-10-23/6f24ac6ce591baf02acd64684f596d2db0ec97c0,
src: 192.168.38.104,
dst: 192.168.38.102,
p: 445,
actions: [Notice::ACTION_LOG],suppress_for:3600.0

Aunque no active el paquete MITRE BZAR en su sensor Corelight, Corelight sigue registrando el acceso a recursos compartidos SMB en el registro *smb_mapping* y el acceso y la modificación de archivos en el registro *smb_files*. Los siguientes registros ilustran los datos contenidos en la familia Corelight de registros SMB:

path: smb_mapping,
uid: CiAtaM363GcEbU63zk,

id.orig_h: 192.168.38.104,
id.orig_p: 65431,
id.resp_h: 192.168.38.102,
id.resp_p: 445,
path: \\\\192.168.38.102\\C$,
share_type: DISK

path: smb_files,
uid: CiAtaM363GcEbU63zk,
id.orig_h: 192.168.38.104,
id.orig_p: 65431,
id.resp_h: 192.168.38.102,
id.resp_p: 445,
action: SMB::FILE_OPEN,
path: \\\\192.168.38.102\\C$,
name: Windows\\Temp\\hbaVJpzdnG,
size: 1894,
times.modified: 2019-12-31T10:28:02.800834Z,
times.accessed: 2019-12-31T10:28:02.753959Z,
times.created: 2019-12-31T10:28:02.566496Z,
times.changed: 2019-12-31T10:28:02.800834Z

Para buscar movimiento lateral:

1. Comience buscando en los registros *smb_files*, y cénrese en los campos *id.orig_h*, *id.resp_h*, *path* y *name*
2. Filtre los registros en los que *id.resp_h* es un servidor de archivos conocido, lo que reduce los resultados a las conexiones potencialmente interesantes.
3. Revise los campos *path* y *name* para identificar desde qué recurso compartido se accedió al archivo o se escribió en él, y determine si el comportamiento es sospechoso.
4. Para obtener un contexto adicional sobre el resto de los registros interesantes, puede pivotar al registro de archivos, utilizando el UID para recopilar información específica sobre los archivos. Por ejemplo, los hashess MD5/SHA1/SHA256 se calculan automáticamente y pueden utilizarse para identificar el malware conocido en sistemas externos, como VirusTotal.
    a. También hay otros campos y posiblemente registros disponibles (por ejemplo, el registro *pe*) que pueden utilizarse para descartar los registros que no sean interesantes.

Protocolo de capa de no aplicación

Los atacantes suelen utilizar un par de técnicas para ocultarse dentro del tráfico legítimo: enviar sus comunicaciones a través de un protocolo propio en un puerto comúnmente permitido como el 80, 443 o 53, e incrustar sus mensajes dentro de la estructura de protocolos legítimos, pero habitualmente menos monitoreados como ICMP.

Para el uso de protocolos propios en puertos estándar, consulte el apartado Puertos utilizados habitualmente/Puertos no estándar para obtener una descripción del paquete de Detección de cifrado de Corelight, el registro *dpd* y el registro *weird*. Le ayudan a identificar las comunicaciones C2 personalizadas que utilizan un cifrado no estándar o que incumplen las especificaciones de los protocolos tradicionales.

El malware a veces emplea protocolos estandarizados de nivel inferior como ICMP, UDP y SOCKS para evitar su detección, ya que estos protocolos rara vez se supervisan. Por ejemplo, los autores de malware pueden incrustar instrucciones C2 en un paquete ICMP Echo Request ("ping").

Corelight supervisa todas las conexiones, independientemente del protocolo, y almacena los datos de conexión en el registro *conn*. Los canales C2 que emplean protocolos UDP propios o protocolos SOCKS basados en TCP (pero no protocolos de capa de aplicación estándar) tienen entradas de registro de conexión sin campo de servicio identificable. Estos campos y registros proporcionan visibilidad de los flujos de tráfico en la red, incluso ICMP, UDP y SOCKS. En el caso de las sesiones ICMP, los datos de Corelight contienen algo más que el origen y el destino, por ejemplo; el recuento de paquetes, los bytes transferidos y el tamaño de los datos ICMP tanto para el emisor como para el receptor.

Con estos datos, se tiene la información necesaria para detectar comunicaciones ICMP anormalmente grandes o frecuentes que pueden ser indicativas de C2. El siguiente registro es una muestra del registro *socks*.

Path: socks,
uid: C5u9ig4ACZvweN5my6,
id.orig_h: 192.168.0.2,
id.orig_p: 55951,
id.resp_h: 192.168.0.1,
id.resp_p: 1080,
version: 5,
user: bob,
status: succeeded,
request.host: 192.168.0.2,
request_p: 22,
bound.host: 192.168.0.1,
bound_p: 55951

Para buscar a un intruso utilizando un protocolo estándar de capa de no aplicación para canalizar la información:

1. Busque en el registro *conn* las entradas en las que el campo de servicio esté vacío, *local_orig* sea *true* y *local_resp* sea *false*
2. Agregue esos resultados por *id.orig_h*, *id.resp_h*, *id.resp_p* y resuma por conteo
3. Filtre las entradas "normales"

4. Analice los elementos restantes, centrándose primero en los elementos con mayor recuento

Puertos no estándar

Cada conexión realizada en un entorno supervisado por Corelight se registra en el registro *conn*. Después de crear una lista de puertos utilizados regularmente (por ejemplo, 22/SSH, 25/SMTP, 80/HTTP y 443/SSL), puede consultar los datos de Corelight para encontrar conexiones a puertos que no estén en esa lista.

Si encuentra conexiones que aparecen en otros puertos no estándar, examine el servicio de Capa 7 que Corelight observa y registra en el campo *conn log service*. Los casos sin servicio reconocido son los más sospechosos, sobre todo si se transfieren grandes volúmenes de datos o la duración de la conexión es larga.

Cuando encuentre servicios conocidos en puertos irregulares, examine los detalles en el registro del protocolo correspondiente para obtener pistas adicionales. Por ejemplo, en el registro *HTTP*, anote el nombre del host remoto, la cadena Usuario-Agente del cliente y el URI. Juntos, podrían contener pistas sobre el software que está generando la solicitud en el puerto no habitual.

Path: conn,
uid: CrIIbI1BJ8Al8ryyX6,
id.orig_h: 192.168.0.53,
id.orig_p: 4388,
id.resp_h: 46.108.156.146,
id.resp_p: 22205,
proto: tcp,
service: http,
duration: 0.0013911724090576172,
orig_bytes: 412,
resp_bytes: 377,
conn_state: RSTO,
local_orig: true,
local_resp: false,
missed_bytes: 0,
history: ShADadfR,
orig_pkts: 7,
orig_ip_bytes: 700,
resp_pkts: 5,
resp_ip_bytes: 585,
resp_cc: DE,
orig_l2_addr: 00:60:6e:00:9d:f9,
resp_l2_addr: 78:54:2e:9f:10:28,
id.orig_h_name.src: HTTP_HOST,
id.orig_h_name.vals: [192.168.0.53:2869],
id.resp_h_name.src: HTTP_HOST,
id.resp_h_name.vals:
[zzwfbedgue.yjuggczkkq.gq:39349,gxgfwamxzl.yjuggczkkq.gq:17805,uugzv.yjuggczkkq.gq:22205,uaayo.nipekpidbkfyjyp.ml:26749],
mss: 1400,
sack_ok: true,

pcr: 0.044359949302915088,
enrichment_orig.device_type: Workstation,
enrichment_orig.role: Sales,
enrichment_orig.user: Chris Jones,
enrichment_orig.city_location: Austin, TX,
enrichment_orig.building: Teleworker,
community_id: 1:ZHZczAcdJVGk0WMPotThj9efcU4=

Proxy

Aunque el uso de proxies no demuestra por sí mismo la presencia de un intruso, los intrusos pueden utilizarlos para "blanquear" las conexiones y ocultar la comunicación a los defensores. Hay muchos métodos para detectarlo, incluido el análisis tradicional de la conexión subyacente (firma, anomalía, comportamiento) y el análisis estadístico de las propiedades de la conexión. Identificar específicamente las conexiones proxies es fundamental para comenzar la búsqueda o la investigación.

Si ve un valor en el campo *proxied* del registro *http* de Zeek, eso significa que una conexión HTTP se hizo con proxy. El registro *http* captura los detalles del proxy a partir de las cabeceras http. Busque cualquier registro en el registro *http* que tenga un campo *proxied* que no esté vacío.

- *host*: el nombre del dominio del sitio web
- *id.orig_h*: la dirección IP del proxy o proxy inverso
- *id.resp_h*: la dirección IP del servidor web
- *proxy*: identifica el proxy y la dirección IP original del cliente

Por ejemplo, un cliente en la IP 219.90.98.8 inició esta petición HTTP. La solicitud se hizo con proxy a través de 172.16.1.30 al servidor web en 172.16.2.95.

host: www.totallyfakedomain.com
id.orig_h: 172.16.1.30 //the proxy
id.orig_p: 53828
id.resp_h: 172.16.2.95 //the web server
id.resp_p: 80
method: POST
post_body: dXNlcm5hbWU9cm9vdCZwYXNzd29yZD1tb25rZXk=
proxied: X-FORWARDED-FOR -> 219.90.98.8 //the real client
status_code: 200
status_msg: OK
uri: /xmlrpc.php
user_agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
log: http

Utilizando este ejemplo, identifique el proxy y determine si es interno o externo. Si es externo, evalúe la sesión y obtenga el contexto, utilizando los datos de Corelight para decidir si lo bloquea o no. Si el proxy

es interno, hay que determinar si se trata de una pieza legítima de la infraestructura de TI, o si es un proxy fraudulento creado para eludir la política: TI en la sombra.

Además, SOCKS es un protocolo proxy de uso común que los sensores Corelight analizan de forma nativa. Cuando se encuentra SOCKS, se genera un registro *socks* que registra los detalles de los usuarios y los protocolos. Esta información puede utilizarse para garantizar que las conexiones no son maliciosas y cumplen la política. En el registro *socks*, céntrese en estos campos:

- *id.orig_h*: la dirección IP del cliente
- *id.resp_h*: la dirección IP del proxy
- *request*: el dominio o la IP a la que el cliente intenta acceder

user: si se trata de una conexión autenticada, el usuario que utiliza el proxy

Servicio web

El servicio web es cuando los atacantes utilizan un servicio web externo legítimo para retransmitir datos hacia o desde un sistema atacado.

Los atacantes a veces utilizan servicios web conocidos para los canales C2 para esconderse entre el ruido. Aunque esta táctica dificulta la identificación, los datos de Corelight (especialmente los registros http, ssl, conn y x509) le ayudan a identificar las conexiones sospechosas. Buscar IOC que incluyan URI, el nombre de host o detalles específicos del certificado (como SNI o CN) es un buen punto de partida. A continuación, se ofrecen algunos ejemplos de campos de certificados que podrían justificar una investigación:

path: x509,
id: FfUGTX1VqS1qR3OJm7,
certificate.version: 3,
certificate.serial: 00,
certificate.subject:emailAddress=obama@us.com,O=Obama inc.,L=Gaza City,ST=Gaza Strip,C=12,
CN=http://usrep3.reimage.com,
certificate.issuer: emailAddress=obama@us.com,O=Obama inc.,L=Gaza City,ST=Gaza
strip,C=12,CN=http://usrep3.reimage.com,
certificate.not_valid_before: 2010-04-01T13:17:48.000000Z,
certificate.not_valid_after: 2011-04-01T13:17:48.000000Z,
certificate.key_alg: rsaEncryption,
certificate.sig_alg: sha1WithRSAEncryption,
certificate.key_type: rsa,
certificate.key_length: 1024,
certificate.exponent: 65537

Exfiltración

Exfiltración automatizada

Si un atacante utiliza un medio automatizado de exfiltración, los artefactos de datos se capturan en los datos de Corelight.

Para buscar exfiltración en su red, puede utilizar el paquete Zeek desarrollado para calcular la relación productor/consumidor (PCR, por sus siglas en inglés). Los valores de PCR indican si los flujos son consuntivos (descarga) o productivos (subida). Los valores de PCR van de -1 (consuntivo) a +1 (productivo). Para buscar exfiltraciones utilizando este paquete:

1. Instale y active el paquete PCR.
2. Genere una tabla de *id.orig_h*, *id.resp_h*, *id.resp_p*, y *pcr* a partir del registro *conn*.
3. Utilice *local_orig* es *false* o *local_resp* es *true* para filtrar los resultados.
4. Reduzca los resultados filtrando cuando pcr <= 0.
5. Para cada host que genere flujos en los que pcr >= 0, considere si se espera que ese host transmita datos, dentro o fuera de la red.

Otra opción es utilizar un SIEM para calcular el PCR utilizando la información disponible en el registro *conn* de Corelight. La siguiente consulta crea una tabla organizada por host que contiene los bytes de origen y respuesta y un valor PCR.

```
index=corelight sourcetype=corelight_conn | stats sum(orig_bytes) as Total_orig_bytes, sum(resp_bytes) as Total_resp_bytes by id.orig_h id.resp_h | eval PCR=(Total_orig_bytes-Total_resp_bytes)/(Total_orig_bytes+Total_resp_bytes) | fields id.orig_h id.resp_h Total_orig_bytes Total_resp_bytes PCR
```

Límites de tamaño para la transferencia de datos

Un atacante puede intentar transferir datos o archivos "troceándolos" en partes más pequeñas, para evitar los límites o umbrales de transferencia de datos codificados. Presentaremos dos métodos para detectar esta técnica.

El primer método analiza los datos que salen de la red basándose en los pares de origen y destino y requiere una plataforma de agregación/visualización de datos (a menos que le guste hacer AWKing y GREPing a través de los datos):

1. Genere una tabla desde el registro *conn* que incluya el *id.orig_h*, *id.resp_h*, *id.resp_p*, y *sum (orig_bytes)*.
2. Ordene los resultados por el mayor *sum (orig_bytes)*.
3. Examine cada host y determine si hay una razón legítima para subir a ese destino.

El segundo método analiza la frecuencia, y el tamaño, de las transferencias salientes de cada fuente:

1. Genere una tabla desde el registro *conn* que incluya el *id.orig_h*, *id.resp_h*, *id.resp_p*, y *count (orig_bytes)*.
2. Ordene los resultados por el mayor *count (orig_bytes)*.
3. Examine los resultados y determine la razón de todas las conexiones con la misma cantidad de datos que fluyen del origen al destino.

[1] https://attack.mitre.org/
[2] Cuando se utiliza como indicador de información, la IP se considera frágil, debido a la facilidad con la que los adversarios pueden trasladarse a un nuevo host o proveedor.
[3] No todas las versiones de RDP declaran el nombre de usuario en el campo *cookie*. Algunas no declaran nada, o solo muestran incoherencias. En esos casos, tendría que deducirlo del NTLM o el registro de Kerberos.
[4] https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/
[5] Visite https://packages.zeek.org/ para obtener más información sobre los paquetes Zeek

Los defensores siempre han buscado un terreno elevado desde el que poder ver más lejos y revetir los ataques. Corelight ofrece una visión dominante de su red para que pueda actuar con mayor astucia y vencer a sus adversarios. Capturamos, interpretamos y conectamos los datos que lo son todo para los defensores.

info@corelight.com | 888-547-9497