corelight

Anleitung zum Threat Hunting

Einführung

Diese Anleitung zum Threat Hunting wurde erstellt, um Ihnen mithilfe von Corelight-Netzwerkdaten simple und relevante Möglichkeiten zu zeigen, um Angriffe aufzudecken, bevor diese stattfinden. Dieses Dokument soll Ihnen helfen, eine Theorie für das Threat Hunting zu entwickeln und Priorisierungen festzulegen. Es beruht auf dem MITRE-ATT&CK-Framework.

MITRE ATT&CK ist eine global zugängliche Wissensdatenbank über Taktiken und Techniken von Angreifern, die auf Beobachtungen in der Praxis basiert. Sie wird als Grundlage für bestimmte Bedrohungsmodelle und -methoden im privaten Sektor wie auf staatlicher Ebene und in der Cybersicherheitsbranche genutzt. Mit der Schaffung von ATT&CK kommt MITRE seinem Ziel näher, Problemlösungen für eine sicherere Welt zu bereitzustellen, indem Communitys zusammenkommen, um gemeinsam effektivere Cybersicherheitslösungen zu entwickeln. ATT&CK ist eine offene und für jede Person und Organisation zugängliche, kostenfreie Plattform.[1]

Was ist Threat Hunting?

Threat Hunting durchsucht Ihr Netzwerk aktiv nach Angreifern, *auch wenn Sie gar nicht wissen, dass sich welche eingeschleust haben*. Das unterscheidet sich vom Abgleich mit Gefahrenindikatoren, der nur auf bereits bekannte Anzeichen von Angreifern achtet, z. B. IP-Adressen oder Datei-Hash. Die Durchführung von Threat Hunting umfasst normalerweise die Recherche nach einer Theorie oder einer Vermutung, ehe die Daten auf der Suche nach etwas *Interessantem* analysiert werden. *Interessante* Elemente können mehrere Formen annehmen, z. B. löste im „Kuckucksei“ von Clifford Stoll ein Buchhaltungsfehler die Bedrohungssuche aus.

> ***„Und so geschah es, daß Dave an meinem zweiten Arbeitstag in mein Büro marschierte und etwas von einem Schluckauf im Unix-Abrechnungssystem murmelte. Irgend jemand mußte ein paar Sekunden Rechenzeit verbraucht haben, ohne dafür zu bezahlen. Die Computerbücher gingen nicht ganz auf: Die letzte Monatsrechnung über 2387 Dollar wies ein Defizit von 75 Cents aus.“***

Diese Differenz um 75 Cent war der Indikator dafür, dass zahlreiche Unternehmens- und Regierungssysteme kompromittiert waren. Das Attribut „interessant“ wird in dieser Anleitung durchgängig verwendet und wird lediglich durch Ihre Fantasie begrenzt.

Warum sollte man Threat Hunting durchführen?

Die meisten host- oder netzwerkbasierten Erkennungssysteme beruhen auf eindeutigen Zuordnungen, auch als Signaturen bezeichnet, um Warnungen zu erzeugen und somit den betroffenen Sicherheitsteams zu signalisieren, dass etwas Unerwünschtes seinen Weg ins Netzwerk gefunden hat. Angreifer feilen jedoch

kontinuierlich neue Techniken aus, um die Erkennungssysteme zu umgehen, und die Signaturen werden erst entwickelt, nachdem das Artefakt in einem anderen Netzwerk entdeckt wurde. Wenn Sie also nicht aktiv nach Artefakten in Ihrer Netzwerkumgebung suchen, wie können Sie dann potenzielle Angreifer finden, die Ihre bestehenden Sicherheitsmechanismen umgehen?
Threat Hunting hat mehrere Vorteile. Erstens finden Sie Artefakte eines aktiven Eindringlings, die von Ihren bestehenden Sicherheitsmechanismen nicht gefunden wurden. Während ein solcher Fund für einige Sicherheitsexperten bereits einer Tragödie gleichkommt, ist es für andere ein großer Erfolg, insbesondere wenn der Angreifer sein Ziel (noch) nicht erreicht hat. Bei jeder Bedrohungssuche werden Schwachstellen aufgedeckt,

z. B. Netzwerk- oder Softwarefehlkonfigurationen, die eine Gefahr darstellen können, zumal sie die Netzwerkperformance beeinträchtigen oder eine Sicherheitslücke offenbaren könnten. Threat Hunting erkennt außerdem kleinere Infektionen wie Adware oder andere inaktive Malware, die Ihr Unternehmen zwar nicht direkt anvisieren, aber dennoch eine Bedrohung darstellen. Drittens können offiziell nicht unterstützte Dienste wie Schatten-IT oder auch der Missbrauch von Ressourcen die Netzwerkperformance beeinträchtigen oder den Weg für neue Angriffsvektoren ebnen und dadurch Risiken bergen. Mit jeder Bedrohungssuche lernen Sie etwas Neues über das Netzwerk.

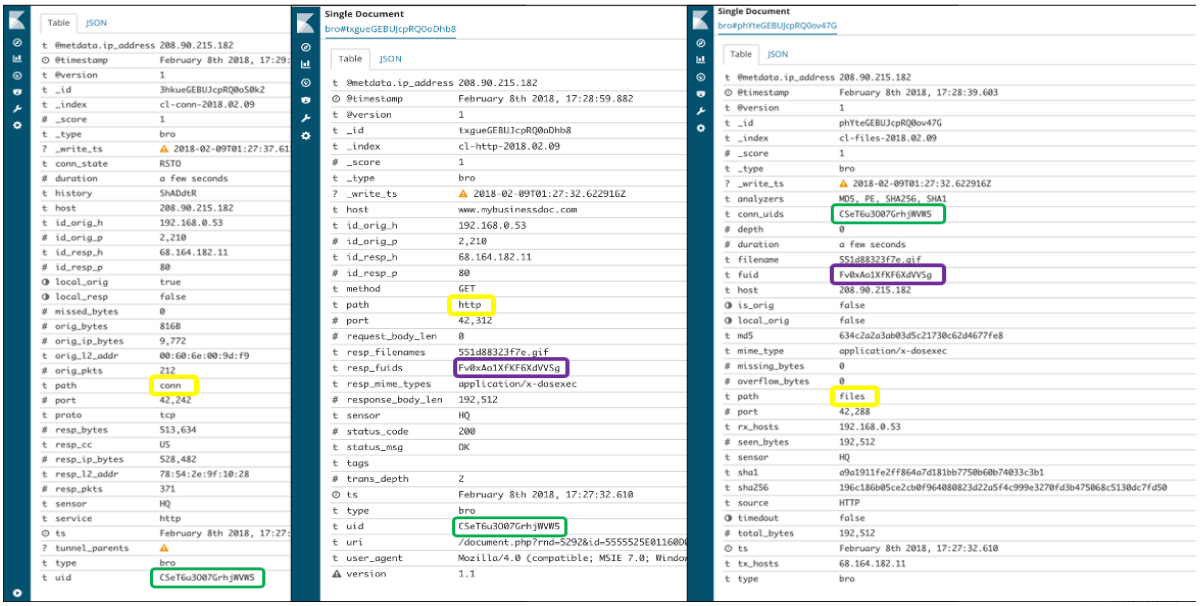
Warum sollte man Netzwerkdaten zum Threat Hunting nutzen?
Pakete lügen nicht.

Es ist so einfach, wie es klingt. Ist ein netzwerkinterner Eindringling in Ihrem Netzwerk aktiv, entstehen Netzwerkartefakte. Artefakte weisen darauf hin, was passiert. Besser gesagt schlüsseln sie anhand eines präzisen Moment-für-Moment-Verlaufs das Geschehene auf. Nutzt ein Command-and-Control-Kanal z. B. DNS als einen Transportmechanismus, gibt es DNS-Abfragen und -Antworten. IP-Adressen, die sich an den Enden einer TCP-Verbindung befinden, müssen zudem korrekt sein; sie können nicht gefälscht werden, wenn Daten ausgetauscht werden. Alle Angriffe durchqueren das Netzwerk, es sei denn, sie sind auf einen Host isoliert, wodurch Pakete entstehen.

Nomenklatur der Corelight-Protokolle
Corelight stellt datenzentrierte Lösungen bereit, die den Netzwerkverkehr analysieren und Automatisierungstools anhand der Transformation von Netzwerkverkehr zu verbundenen Protokollen und Extraktionsdaten verbessern. Das zentrale Protokoll ist das Verbindungsprotokoll, das allgemeine Informationen über alle Netzwerksitzungen aufzeichnet.

Das Verbindungsprotokoll speichert Informationen über jeden Netzwerkendpunkt und den Dienst (Anwendung) und weist eine UID (Unique Identifier) zu. Die UID verbindet das Verbindungsprotokoll mit zugehörigen Protokollen, in denen spezifische Sitzungsinformationen verfügbar sind. Das Verbindungsprotokoll kann z. B. http als Dienst auflisten und mithilfe der UID können Sie zum HTTP-Protokoll wechseln, um spezifische Protokollinformationen über die Sitzung zu erhalten. Die UID unterscheidet die Corelight-Lösungen von anderen Sicherheitstools. Dieses Feld verknüpft disparate Informationen zu

übersichtlichen Protokollen. Die UID ist fundamental für die Durchführung von Link-Analysen und ein wichtiges Feld, das das Pivoting oder Zusammenfügen mehrerer Protokolle ermöglicht.



Die Informationen über jeden Netzwerkendpunkt werden durch das ID-Feld zusammengefasst, das normalerweise in vier Unterfeldern dargestellt wird:

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

Diese Nomenklatur mag seltsam erscheinen, da Netzwerkmitarbeiter in Sitzungen üblicherweise Client und Server nutzen. Die Verwendung von „orig“ (Originator) und „resp“ (Responder) ermöglicht es dem Sicherheitspersonal jedoch, die Verbindung genau zu beschreiben. Stellen Sie sich den sendenden Host (orig_h) als Quelle bzw. Client und den antwortenden Host (resp_h) als Ziel bzw. Server vor. Die Felder „id.orig_p“ und „id.resp_p“ werden jeweils mit den entsprechenden Port-Nummern ausgefüllt.

Einige der verbleibenden Felder im Verbindungsprotokoll und in anderen Protokollen sind selbsterklärend. Wenn Sie dennoch Schwierigkeiten haben, werfen Sie einen Blick auf die Zeek-Dokumentation unter https://docs.zeek.org/en/current/ für nähere Informationen oder besuchen sie den Community-Slack-Kanal unter http://corelightcommunity.slack.com/.

Benutzer und Geräte identifizieren

Beim Identifizieren von Geräten in einem Netzwerk werden die IP- oder MAC-Adresse häufig genutzt, um die „Identität“ zu schaffen. Die IP-Adresse eines Geräts wird öfters für die Remote-Identität von einem Gerät genutzt, weil sie Router-Grenzen überdauert. Innerhalb eines Netzwerksegments wird die MAC-Adresse zur Identifizierung bevorzugt, weil sie ein bestimmtes Gerät auf zuverlässige Weise identifizieren kann. Jede

Identifizierungsmöglichkeit hat Vor- und Nachteile. Die Fähigkeit von Corelight, beide Möglichkeiten zu erfassen, hilft den Mitarbeitern des Security Operations Center bei den Untersuchungen von Vorfällen.

IP-Adressen sind für interne Untersuchungen beständig[2], aber innerhalb eines Netzwerks aufgrund der Implementierung von DHCP (Dynamic Host Configuration Protocol) oft flüchtig. Flüchtige IP-Adressen können für Sicherheitsteams zu einem Problem werden, wenn Warnungen des Angriffserkennungssystems (Intrusion Detection System, IDS) die Sitzungen anhand IP-Adressen identifizieren. Diese IP-Adressen stehen nur zu dem Zeitpunkt mit der Warnung in Verbindung, *zu dem die Warnung erzeugt wurde*.

Sie können Open-Source-Tools zur Durchführung einer Untersuchung (z. B. nslookup) nutzen, um DNS-Informationen für Remote-IPs zu erhalten. Dabei handelt es sich jedoch um eine zeitpunktbezogene Information *zum Zeitpunkt der Untersuchung, nicht zum Zeitpunkt des Vorfalls*. Eine bessere Technik ist die Nutzung von Protokollen, die zum Zeitpunkt der ausgegebenen Warnung erstellt wurden, um die IP-Adresse und den FQDN (Fully Qualified Domain Name) für das Remote-Gerät zu erfassen. Um das interne Gerät zu lokalisieren und identifizieren, können Sie DHCP-Protokolle auslesen. Es gibt verschiedene Möglichkeiten, einen Host zu identifizieren, und Corelight stellt die Daten in multiplen Protokollen bereit, die jeweils einen anderen Aspekt der Geschichte erzählen. Üben Sie sich in Kreativität und folgen Sie jedem Hinweis.

Hostnamen können hier gefunden werden:

- **dhcp.log:** Die Felder „host_name“ und „domain“ stehen für den Hostnamen und die Domain, die von einem Host bei Anfrage einer IP-Adresse via DHCP gemeldet wurde. Das Feld „assigned_addr“ ist die IP-Adresse, die dem Host zugeordnet wurde.
- **dns.log:** Wenn im Feld „answers“ eine IP-Adresse steht, dann enthält das Feld „query“ den Hostnamen, den der DNS-Server (zu diesem Zeitpunkt) für die IP-Adresse aufgezeichnet hat.
- **ntlm.log:** „server_dns_computer_name“ und „server_nb_computer_name“ beziehen sich auf die DNS- und Netbios-Namen des Geräts mit der IP-Adresse im Feld „id.resp_h“. Das Feld „hostname“ besteht aus dem Hostnamen des Geräts mit der IP-Adresse im Feld „id.orig_h“.
- **kerberos.log:** In einer Windows-Umgebung bei domainverbundenen Geräten ist bei Kerberos-Anfragen, bei denen das Feld „client“ einen Namen mit der Endung „$“ enthält, das Feld „client“ der Hostname und das Feld „id.orig_h“ die IP-Adresse dieses Hosts. Das Feld „client“ ist oft wie HOSTNAME$/EXAMPLEDOMAIN.COM aufgebaut, wobei HOSTNAME der Hostname und EXAMPLEDOMAIN.COM der Name der Windows-Domain und des Kerberos-Realms ist.
- **http.log:** Das Feld „host“ enthält den Hostnamen, Domainnamen oder die IP-Adresse des Clients, der Daten vom HTTP-Server angefordert hat. Manchmal ist dieses Feld ein Hinweis auf die Identität des Servers, das Gerät mit der IP-Adresse im Feld „id.resp_h“.
- **ssl.log:** Das Feld „server_name“ wird aus dem Feld „Server Name Indication“ (SNI) in der TLS/SSL-Aushandlung extrahiert und wird ähnlich wie das Feld „host“ des HTTP-Protokolls verwendet. Außerdem wird das Feld „subject“ aus dem Betreff des Server-Zertifikats extrahiert und der Teil des kanonischen Namens CN des Betreffs kann Anhaltspunkte zur Identifizierung eines Servers liefern.

Beim Identifizieren von Benutzern gibt es mehrere Protokolle, die wertvolle Informationen liefern.

- **rdp.log:** Abhängig von der Version des RDP-Protokolls ist der Wert des Feldes „cookie“ der vom Client angegebene Benutzername und die Client-IP steht im Feld „id.orig_h“.[3]
- **ftp.log:** Das Feld „user“ enthält den vom Client angegebenen Benutzernamen und die IP-Adresse des Clients steht im Feld „id.orig_h“.
- **irc.log:** Das Feld „user“ enthält den vom Client angegebenen Benutzernamen und die IP-Adresse des Clients steht im Feld „id.orig_h“.
- **socks.log:** Das Feld „user“ enthält den vom Client angegebenen Benutzernamen und die IP-Adresse des Clients steht im Feld „id.orig_h“.
- **http.log:** Das Feld „username“ enthält den vom Client angegebenen Benutzernamen und die IP-Adresse des Clients steht im Feld „id.orig_h“ bzw. kann im Feld „proxied“ angegeben werden, wenn die Verbindung über einen Proxy hergestellt wurde. Im Falle einer Verbindung über einen Proxy enthält das Feld „id.orig_h“ die IP-Adresse des Proxys.
- **ntlm.log:** Das Feld „username“ enthält den vom Client angegebenen Benutzernamen und die IP-Adresse des Clients steht im Feld „id.orig_h“.
- **kerberos.log:** In einer Windows-Umgebung enthalten Kerberos-Anfragen den Benutzernamen im Feld „client“ (außer bei Anfragen, bei denen das Feld „client“ einen Namen enthält, der auf „$“ endet, was bedeutet, dass die angegebene Identität ein Gerät und das Feld „id.orig_h“ die IP-Adresse des Quellgeräts ist). Das Feld „client ist oft wie USERNAME/EXAMPLEDOMAIN.COM aufgebaut, wobei USERNAME der Benutzername und EXAMPLEDOMAIN.COM der Name der Windows-Domain und des Kerberos-Realms ist.

Eine Warnung zu möglichen Schlussfolgerungen über die Identität eines Geräts oder seinem Benutzer: Kennen Sie Ihre Grenzen (und die der Daten). Nur weil ein Benutzername im Netzwerkverkehr aufgezeichnet wurde, heißt das nicht, dass die entsprechende Person tatsächlich verantwortlich ist – es handelt sich lediglich um einen Hinweis. Prüfen Sie, ob sich der Benutzer erfolgreich authentifiziert hat. Staatlich finanzierte Cyberspione und Saboteure tendieren immer öfters zum Setzen falscher Flaggen.[4] Der Benutzername wurde möglicherweise *angegeben*, aber wenn die Authentifizierung fehlgeschlagen ist, spricht das nicht dafür, dass der Benutzer involviert war. Beachten Sie, dass Geräte und Software Zugriffsberechtigungen zwischenspeichern. Das Benutzerkonto bleibt somit aktiv, aber die tatsächliche Person könnte dennoch unschuldig sein. Sie müssen weitere Informationen sammeln, bevor Sie Ihren Täter zuverlässig identifizieren können.

Zum Beispiel:

- Ein Benutzer geht in die Mittagspause und hinterlässt sein Gerät unbeaufsichtigt und ohne Bildschirmsperre.
- Ein Gerät wird mit einem Remote-Access-Trojaner (RAT) kompromittiert, womit ein Benutzer am anderen Ende der Welt heimlich die Identität unseres Opfers annimmt, *während der eigentliche Benutzer das Gerät gleichzeitig auch für reguläre Geschäfte verwendet*.
- Ein böswilliger Benutzer innerhalb des Unternehmens hat einen Mitarbeiter dabei belauscht, wie er sein Passwort in einem Gespräch laut ausgesprochen hat, und versucht nun, sich mit diesen Anmeldedaten bei anderen Systemen anzumelden.

Vergewissern Sie sich außerdem, welche Informationen von Clients oder Servern kontrolliert oder angegeben werden und wer die Kontrolle darüber hat. Befindet sich ein Angreifer in Ihrem Netzwerk, ist es für die Erstellung eines Reaktionsplans fundamental zu wissen, welche Informationen vertrauenswürdig sind. Ein Eindringling könnte z. B. DHCP deaktivieren und eine IP-Adresse statisch zuweisen und sie nutzen, um sich durch das Netzwerk zu bewegen. Da der DHCP-Server Einträge mit falschen Informationen bereitstellen würde, könnte der Eindringling somit eine Identifizierung umgehen. Zusätzlich könnte der Hacker eine falsche MAC-Adresse bereitstellen, wenn ein Client eine DHCP-Adresse anfordert. Daher ist es wichtig, passive Protokolle zum Zeitpunkt des Vorfalls aufzuzeichnen.

Bestimmte TTPs abwehren

Erstzugriff

Der Erstzugriff ist der Zeitpunkt, zu dem Eindringlinge ihren ersten Fuß in die Tür setzen.

Drive-by-Exploits

Unter einem Drive-by-Exploit versteht man das unerwünschte und automatische Herunterladen von Malware durch das bloße Aufrufen einer infizierten Webseite. Wenn Sie in Corelight-Daten nach Anzeichen eines Drive-by-Exploits suchen, sollte Ihr Hauptaugenmerk auf Downloads von externen Webseiten liegen.

Beginnen Sie die Suche mit dem HTTP-Protokoll und suchen Sie nach Anzeichen für heruntergeladene ausführbare Dateien:

1. Starten Sie bei HTTP-Protokollen, bei denen das Feld „resp_fuids“ nicht leer ist, denn das bedeutet, dass eine Datei vom Responder zurückgegeben wurde.
2. Wenn das Datenvolumen zu groß ist, filtern Sie lokale (netzwerkinterne) Responder heraus. Sie können filtern, indem Sie die Ergebnisse mit dem Verbindungsprotokoll über die UID verbinden und dann alle Datensätze herausfiltern, in denen „local_resp“ im Verbindungsprotokoll „true“ ist.
3. Überprüfen Sie „resp_mime_types“ aus dem HTTP-Protokoll und filtern Sie uninteressante Ergebnisse heraus (z. B. Bilder, Text, OCSP-Antworten oder Zertifikate). Meistens sind die interessantesten Ergebnisse ausführbare Dateien sowie DLL-Dateien und Archive/Container.
4. Gruppieren Sie die Ergebnisse nach den Feldern „host“ und „resp_mime_types“, um die Analyse zu vereinfachen.

Halten Sie bei der Prüfung Ausschau nach interessanten oder auffälligen Ergebnissen, wie z. B. Downloads von ausführbaren Dateien, seltsamen Dateierweiterungen und Unstimmigkeiten beim MIME-Typ.

Da immer mehr Angreifer dazu übergehen, TLS zur Verschlüsselung des Austauschs zwischen kompromittierten Clients und von ihnen kontrollierten Webseiten zu verwenden, wird die Sichtbarkeit über das HTTP-Protokoll geringer. Um diese Sichtbarkeit wiederzuerlangen, sollten Sie den Einsatz einer SSL-Entschlüsselungslösung für Unternehmen in Betracht ziehen und den entschlüsselten HTTP-Verkehr an Ihren Corelight-Sensor weiterleiten.

Externe Remote-Dienste

Externe Remote-Dienste werden von Hackern genutzt, um eine Verbindung mit internen Netzwerkressourcen herzustellen. Die Suche nach Fehlkonfigurationen oder -nutzungen bei Remote-Diensten umfasst normalerweise zwei Schritte: Erkennung und Analyse. Zunächst müssen Sie die genutzten Remote-Dienste identifizieren. Informationen zum Bestand der Ressourcen und Dienste sollten zuerst gesammelt werden. Doch meistens ist das nicht genug. Oft verlieren Unternehmen den Überblick, wenn IT-Teams Änderungen an der Infrastruktur vornehmen und Schwierigkeiten haben, die Ressourcen-Dokumentation aktuell zu halten. Benutzer mit erweiterten Berechtigungen erschweren dieses Problem, indem sie Ressourcen und Dienste einbeziehen, ohne das IT-Team darüber zu informieren. Dieser Prozess wird auch als „Schatten-IT“ bezeichnet.

Bekannte Remote-Dienste wie RDP, VNC (Remote Framebuffer) und SSH (Secure Shell) enthalten eine Server- und eine Clientkomponente. Hosten Sie in Ihrer Netzwerkumgebung einen Remote-Dienst, können Angreifer sich extern Zugriff verschaffen, um die Geräte innerhalb des Netzwerks zu infizieren. Um diese Dienste zu identifizieren, halten Sie Ausschau nach Verbindungsprotokolleinträgen, in denen das Feld „service“ entweder „rfb“, „rdp“ oder „ssh“ enthält und „local_orig“ „false“ und „local_resp“ „true“ ergeben oder in denen die Absender-IP (id.orig_h) extern und die Responder-IP (id.resp_h) im Unternehmensnetzwerk ist. Achten Sie auf alle RFP/VNC-, RDP- oder SSH-Server, die Verbindungen aus dem Internet annehmen.

Einige Remote-Dienste funktionieren in umgekehrter Weise, d. h. ein Agent wird auf dem lokalen Gerät installiert und greift von innerhalb des Netzwerks auf eine Reihe von externen Servern zu, z. B. GoToMyPC und TeamViewer. Diese Konfiguration dient zur Unterstützung von Benutzern (hauptsächlich Heimanwendern), die die Netzwerkadressübersetzung (Network Address Translation, NAT) oder die Firewall nicht kontrollieren oder nicht über die nötige Erfahrung verfügen, um die Port-Weiterleitung oder die Firewall-Regeln zu verwalten.

Um festzustellen, ob diese Remote-Dienste in Ihrer Umgebung verwendet werden, suchen Sie nach Anzeichen für ausgehende Verbindungen zu den Diensten. Z. B. verwendet TeamViewer den TCP-Port 5938, um mit TeamViewer-Servern zu kommunizieren. Überprüfen Sie also einfach die Verbindungsprotokolle auf Verbindungen, bei denen die „id.resp_p“ „5938“ und „local_orig“ „true“ und „local_resp“ „false“ ist. Da TeamViewer ebenfalls SSL verwendet und der Domainname der Verbindungen „*.teamviewer.com“ sein sollte, können Sie zusätzlich nach Einträgen im SSL-Protokoll suchen, in denen der „server_name“ „teamviewer.com“ enthält oder besser noch damit endet. (Hinweis: Da diese Sitzung umgekehrt funktioniert, ist „id.orig_h“ das Gerät in Ihrem Netzwerk, auf dem der TeamViewer-Client installiert ist.) In unserem zweiten Beispiel versucht GoToMyPC, „poll.gotomypc.com“ zu kontaktieren. Untersuchen Sie das Feld „host“ des HTTP-Protokolls nach „poll.gotomypc.com“ oder Einträgen im SSL-Protokoll, in denen „server_name“ „poll.gotomypc.com“ lautet. Für jedes Client-Softwarepaket variiert die Liste der Ports und Domainnamen.

Nachdem wir uns mit der Erkennung von Remote-Diensten befasst haben, sollten Sie die Corelight-Daten mit einer Liste aller Remote-Dienste vergleichen, die die IT-Abteilung anbietet, z. B:

- RDP-Gateways (Remote Desktop Protocol)

- VDI-Gateways (Virtual Desktop Infrastructure)
- VPN-Gateways (Virtual Private Network)
- SSH-Server (Secure Shell)

Stellen Sie für jeden Internetdienst eine Liste der Verbindungen zu diesem Dienst aus dem Verbindungsprotokoll zusammen und fügen Sie die folgenden Felder hinzu:

- id.orig_h: Absender-IP-Adresse (Client)
- id.resp_h: Responder-IP-Adresse (Server)
- id.resp_p: Responder-Port
- service: das von Zeek erkannte Anwendungsprotokoll
- history: der Verbindungsverlauf, z. B., welche Arten von TCP-Flags gesehen wurden
- orig_cc: Der Ländercode des Absenders

Stellen Sie beim Filtern von Protokollen sicher, dass das Feld „history“ mit „Sh“ beginnt. Bei TCP-Verbindungen bedeutet dies, dass der Absender ein SYN-Paket versendet und der Responder mit einem SYN/ACK-Paket geantwortet hat (Handshake). Diese Prüfung eliminiert Verbindungen, bei denen der Server nicht zuhört oder eine Firewall die Verbindung blockiert.

Durchstöbern Sie nach Erfassung aller Daten die Protokolle nach interessanten Informationen, z. B. einer unerwarteten Verbindung aus einem spezifischen Land. Verwenden Sie die UID aus dem Verbindungsprotokoll zur Nachverfolgung mit den anwendungsspezifischen Zeek-Protokollen (rdp, rfb, ssh). Das RDP-Protokoll liefert z. B. mehr Details über die Verbindung, wie das Feld „cookie“, das den Benutzernamen des authentifizierenden Benutzers enthalten kann. Der letzte Schritt besteht darin, mit dem Benutzer zu überprüfen, ob er das System zu diesem Zeitpunkt aktiv verwendet hat.

Corelight-Kunden haben Zugriff auf die Encrypted Traffic Collection (ETC), die Rückschlüsse auf verschlüsselten Datenverkehr ermöglicht. Das SSH-Protokoll enthält interessante Informationen über die SSH-Verbindung, wie z. B.:

- KS für Verbindungen, die scheinbar Client-Keystrokes enthalten
- FU und FD für Verbindungen, die scheinbar jeweils einen Dateiupload oder -download enthalten
- ABP für Verbindungen, die scheinbar keine Authentifizierung enthalten, aber dennoch erfolgreich sind („Authentication bypass“)
- SV oder SC für Clients, die scheinbar eine Versions- bzw. Fähigkeitsprüfung durchführen

Für nähere Informationen zur Corelight ETC wenden Sie sich bitte an unser Vertriebsteam unter 510 281 0760.

Spearphishing-Anhang

Um in ein Unternehmen einzudringen, kann ein Angreifer im Rahmen einer Spearphishing-Kampagne einen gut gestalteten bösartigen Anhang an eine Einzelperson oder eine kleine Gruppe senden. Im Anhang könnte sich ein Dokument befinden, das den Benutzer zu einer bestimmten Aktion auffordert, z. B. zum Klicken auf

einen Link und/oder zur Anmeldung bei einem Portal. Es könnte auch eine Datei sein, die Schwachstellen der Software ausnutzt, mit der sie geöffnet wird, z. B. Adobe Acrobat oder Microsoft Word.

Das Corelight-SMTP-Protokoll enthält Einträge im Feld „fuids“, wenn an eine über SMTP zugestellte Nachricht Dateien angehängt sind. Dieses Feld kann verwendet werden, um zum Dateiprotokoll zu navigieren, das detaillierte Informationen über die Datei enthält, einschließlich Dateiname, Hashes und die Quelle. Zum Beispiel:

path: smtp
from: Your Friend <Jeremy.Rigeur@gmail.com>
fuids: [Fh5GBc1wdVp3x9MKxc]
mailfrom: attacker@fake-mail.com
rcptto: [victim@corp-mail.com]
subject: Definitely not a spear-phish
to: [victim@corp-mail.com]
uid: CzKseq1Y3zo2qsTYH5
user_agent: Apple Mail (2.3608.80.23.2.2)

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

Um potenzielle Spearphishing-Versuche aufzudecken, können Sie in den Dateiprotokollen danach suchen:

1. Der Wert im Feld „source“ ist SMTP.
2. Filtern Sie alle uninteressanten „mime_type“- und/oder „filename“-Werte heraus, wie bereits erklärt.
3. Verwenden Sie den Hash (MD5, SHA1 oder SHA256) mit einem Datei-Reputationsdienst (z. B. Virustotal), um nach bekannten schädlichen Dateien zu suchen.

Zusätzlich können Sie das SMTP-Protokoll durchsuchen:

1. Um die Datenmenge zu reduzieren, suchen Sie nach Einträgen, bei denen das Feld „fuids“ nicht leer ist.
2. Filtern Sie bekannte gute Kombinationen von „mailfrom“- und „from“-Werten heraus.
3. Filtern Sie uninteressante „subject“-Werte heraus.
4. Erwägen Sie, den „fuid“-Wert aus den verbleibenden Datensätzen zu verwenden, um zum Dateiprotokoll zu navigieren und weitere Informationen über die Datei zu erhalten.

Corelight kann eine Hochgeschwindigkeitsdateiextraktion durchführen und auf Basis des MIME-Typs filtern, sodass alle interessanten Dateien, wie z. B. ausführbare Dateien, Office-Dokumente und PDF-Dateien, bei Bedarf für eine genauere Untersuchung zur Verfügung stehen.

Heute wird ein Großteil des E-Mail-Verkehrs mit STARTTLS über das SMTP verschlüsselt, wodurch die Sichtbarkeit erschwert wird. Um eine bessere Sichtbarkeit zu erreichen, ohne den Datenschutz und die Sicherheit für Ihre Benutzer zu opfern, ist es eine bewährte Methode, eingehendes SMTP an einem System anzunehmen, das STARTTLS unterstützt, und dann die Mail über einen Proxy an das interne Mailsystem weiterzuleiten, damit Corelight die entsprechenden Protokolle erstellen kann.

Spearphishing-Link
Anstatt Dateien an ein Unternehmen zu senden, wo sie von einem E-Mail-Filter geprüft werden können, senden einige Angreifer E-Mails, die nur Links enthalten. Diese Links führen zu Webseiten, die vom Angreifer kontrolliert werden, um den Benutzer mit folgenden Mitteln zu täuschen:

- Eingabe von Anmeldedaten, die die Angreifer abgreifen
- Ausnutzen einer Sicherheitslücke im Browser des Benutzers
- Herunterladen einer Datei zum Ausnutzen einer Sicherheitslücke einer anderen Anwendung auf dem Gerät des Benutzers

Corelight-Sensoren haben ein Paket[5], das Links aus SMTP-Nachrichten in einem separaten smtp_links-Protokoll aufzeichnen kann. Das Protokoll dieses Pakets enthält ein Feld „fuid“, das das smtp_links-Protokoll mit dem SMTP-Protokoll verknüpft. Sie können schnell zum SMTP-Protokoll mit den Details zur Nachricht navigieren, über die der bösartigen Link übermittelt wurde.
Zum Beispiel:

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: Your Friend <Jeremy.Rigeur@gmail.com>
fuids: [FhahXA1eJ32gHvNP27]
mailfrom: attacker@fake-mail.com
rcptto: [victim@corp-mail.com]
subject: Click this link, please
to: [victim@corp-mail.com]
uid: C62txO1FHoJFJpsgP1

user_agent: Apple Mail (2.3608.80.23.2.2)

Um nach Spearphishing-Links zu suchen, beginnen Sie mit dem smtp_links-Protokoll und überprüfen das Feld „link“, wobei Sie gutartige Domains herausfiltern, bis Sie interessante Ergebnisse finden. Eine andere Möglichkeit besteht darin, das smtp_links-Protokoll über das „fuids“- oder „uid“-Feld mit dem SMTP-Protokoll zu verbinden und gutartige Kombinationen der Felder „mailfrom“ und „from“ herauszufiltern, um nach Nachrichten von eindeutigen Absendern zu suchen.

Heute wird ein Großteil des E-Mail-Verkehrs mit STARTTLS über SMTP verschlüsselt. Um eine bessere Sichtbarkeit zu erreichen, ohne den Datenschutz und die Sicherheit für Ihre Benutzer zu opfern, ist es eine bewährte Methode, eingehendes SMTP an einem System anzunehmen, das STARTTLS unterstützt, und dann die Mail über einen Proxy an das interne Mailsystem weiterzuleiten, damit Corelight die entsprechenden Protokolle erstellen kann.

Durchführung

Der Angreifer versucht, bösartigen Code auszuführen.

Kommandozeilen-Skripte (Powershell)

Kommandozeilen-Skripte wurden lange verwendet, um *nix-basierte Systeme zu verwalten. Die Fähigkeit, Skripte zu erstellen und auszuführen, wird häufig von Angreifern ausgenutzt. Jahrelang gab es kein Äquivalent unter Windows. In den frühen 2000er Jahren begann Microsoft mit der Entwicklung eines neuen Ansatzes für die Verwaltung von Kommandozeilen. Kurz danach entstand PowerShell (PS) 1.0. PS ist ein auf dem .NET-Framework basierendes, integriertes Tool, das zur Automatisierung von Systemadministrationsaufgaben eingesetzt wird. Es bietet eine Schnittstelle für Benutzer, um auf Dienste des Windows-Betriebssystems zuzugreifen.

Obwohl bestimmte PS-Befehle standardmäßig eingeschränkt sind, stehen viele Befehle zur Verfügung, um Systeminformationen ohne eine ausführbare Datei zu erhalten. Sie können LNK-Erweiterungen verwenden, um Schutzmechanismen zu umgehen und ein PS-Skript auszuführen. LNK-Dateien sind in der Regel als Verknüpfungen zu sehen, die sich meistens auf dem Desktop und im Startmenü der Benutzer befinden. Bösartige LNK-Dateien sind oft in scheinbar legitime Dokumente oder Bilder eingebettet. Nach dem Öffnen führt die LNK-Datei eine legitime Windows-Anwendung „CMD.exe“ oder „MSHTA.exe“ aus, um die Sicherheitseinstellungen zu umgehen.

Die Dateiextraktionsfähigkeiten von Corelight und die Möglichkeit zur Integration in mehrere Informationsplattformen bieten Einblick in nach Dateityp verschleierte Malware. Mithilfe der in Corelight integrierten Filterung können Sie die Dateiextraktionsparameter so einstellen, dass sie auf bestimmte Mime-Typen abzielen, die häufig für die Verbreitung von Malware verwendet werden, z. B:

- komprimierte Dateien
- Microsoft-Office-Dateien (Word, Powerpoint etc.)
- PDF-Dateien
- TXT-Dateien (Powershell, VBS)

Persistenz

Unter Persistenz versteht man, dass ein Angreifer über einen längeren Zeitraum versucht, seine Stellung zu halten.

BITS-Aufträge

Der Background Intelligent Transfer Service (BITS) von Microsoft wurde 2001 als ein Mechanismus zum Verwalten von Dateiübertragungen eingeführt, um Unterbrechungen für den Anwender zu minimieren. BITS wird häufig für den Download von Windows-Updates und anderen Softwareupdates von großen Anbietern verwendet.

Angreifer haben zwei Möglichkeiten, BITS zu missbrauchen:

- Bei der am häufigsten genutzten Methode wird ein BITS-Übertragungsauftrag direkt auf einem Host erstellt. Das ermöglicht einen Download von sekundären Nutzdaten über einen integrierten Windows-Dienst, der normalerweise Firewalls und andere Sicherheitskontrollen umgeht.
- Eine weitere Möglichkeit ist die Exfiltration von Daten durch einen BITS-Upload-Auftrag. Uploads müssen sich mit einem IIS-Server verbinden, damit BITS richtig funktioniert, aber diese Anforderung ist für Malware-Autoren leicht zu unterlaufen.

BITS-Datenübertragungen können über HTTP, SSL und SMB erfolgen. Wenn BITS HTTP-Verkehr verwendet, gibt es eine unverwechselbare User-Agent-Zeichenfolge von „Microsoft BITS/7.5“ (oder 7.8 in späteren Versionen). Leider gibt es keine Unterscheidungsmerkmale von BITS-SSL- und -SMB-Netzwerkverkehr. Daher ist das Vorhandensein von BITS-Netzwerkverkehr nicht unbedingt verdächtig, da er überall dort vorhanden ist, wo Windows-Rechner mit dem Internet verbunden sind. Analysten können mithilfe der Corelight-Daten dennoch beurteilen, ob der BITS-Datenverkehr legitim ist, indem sie die für die BITS-Datenübertragungen verwendeten Remote-Systeme analysieren. Wenn sie sich außerhalb von Content Delivery Networks (CDN) oder den Netzwerken großer Softwareanbieter befinden, sollten alle BITS-Uploads untersucht werden, bis sie sich als gutartig erweisen, da dieser Anwendungsfall bei legitimen Softwareanbietern besonders selten ist.

Das Codebeispiel unten ist ein HTTP-Protokoll, das zeigt, wie die BITS-Daten aussehen, wenn sie über HTTP übertragen werden.

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: */*

Externe Remote-Dienste

- Siehe *Erstzugriff: Externe Remote-Dienste*

Portknocking

Portknocking ist eine Technik, um ein Remote-System dazu zu bringen, den Zugriff auf einen ansonsten geschlossenen Port zu ermöglichen. Sie besteht typischerweise aus einer vordefinierten Abfolge von Verbindungen zu anderen (oft geschlossenen) Ports, manchmal mit speziellen Flags auf Protokollebene, Layer-7-Banner-Strings usw.

Zeek fasst jede TCP-, UDP- und ICMP-Verbindung im Verbindungsprotokoll zusammen. Dieses detaillierte Protokoll bietet nützliche Statistiken zu Verbindungen. Die Felder „history“, „conn_state“ und „network tuple“ (src/dest ip/port) liefern die zum Sichten von Portknocking erforderlichen Informationen. Wichtig: Das Sichten von Portknocking ohne einen zusätzlichen Hinweis kann zu einer schwierigen Aufgabe werden, da es einfach ist, Sequenzen von Verbindungen bewusst unter dem Rauschen eines typischen Netzwerks zu verstecken.

Server-Software-Komponente: Web-Shell
Eine Web-Shell ist eine webbasierte Implementierung einer Command-Shell. Eine Web-Shell ist im Allgemeinen eine bösartige Webseite oder einen bösartigen Codeschnipsel, das in einen bestehenden Webserver oder eine Webanwendung eingeschleust wird, um unberechtigten Zugriff zu ermöglichen. Dieser Zugriff kann über eine CLI-Shell, ein Dateiverwaltungsprogramm oder ein Datenbankzugriffstool erfolgen. Dies ist eine gängige Taktik, da sich bösartiger Datenverkehr mit gutartigem Datenverkehr zum bzw. vom Webserver vermischt und es schwierig sein kann, ihn über IDS-Signaturen zu identifizieren, da die Spezifika der Web-Shell leicht geändert werden können.

Wenn eine Web-Shell ausgeführt wird, läuft sie mit den Benutzerrechten der Webserver-Software, die eingeschränkt sein sollten. Angreifer verwenden Web-Shells, um Angriffe zur Privilegienerweiterung durchzuführen, indem sie lokale Schwachstellen im System ausnutzen, um Root-Rechte anzunehmen.

Die Erkennung von Web-Shells im Netzwerk mithilfe signaturbasierter Erkennungen ist relativ einfach – Web-Shells haben bestimmte Dateipfade, Kommunikationsmethoden oder andere Verhaltensweisen, die eine Warnung auslösen können. Wie die meisten „atomaren“ Gefahrenindikatoren (Indicator of Compromise, IOC) sind sie leicht zu umgehen, da sie bestimmte Verhaltensweisen identifizieren, die leicht geändert werden können. Wenn möglich, sollten Sie die signaturbasierte Erkennung mit einem Threat-Hunting-Programm ergänzen, um allgemeinere Verhaltensweisen anomaler Aktivitäten zu finden.

Web-Shells versuchen, bösartige Aktivitäten im normalen HTTP-Verkehr zu verstecken. Daher ist das HTTP-Protokoll eine hervorragende Datenquelle für die Untersuchung von Web-Shell-Aktivitäten. Mögliche Hypothesen über potenzielle Bedrohungen, deren Abwehr durch Corelight-HTTP-Daten unterstützt wird, sind:

- Ungewöhnliche HTTP-POST-Aktivität, z. B. unerwartete HTTP-POSTs im Feld „method“ des HTTP-Protokolls, wo GETs erwartet werden (wenn die betroffene Webseite hauptsächlich Inhalte liefert).

Der „normale“ Webverkehr gelangt zu einer Auswahl gängiger Seiten, wobei die Navigation über einen internen Hyperlink erfolgt. Eine Web-Shell geht direkt auf die versteckte Seite und erscheint als HTTP-Anfrage ohne verweisende Seite. Zusätzlich zeigt der Webdatenverkehr eine Vielzahl von anfordernden IP-Adressen, User-Agent-Strings, JA3s usw. Eine Web-Shell kann eine homogenere Gruppe von Benutzern haben.

- Aufspüren von verdächtigen Logins, die von internen Subnetzen auf DMZ-Servern ausgehen und umgekehrt.

Diese Art der Threat-Hunting-Analyse und Erkennung von Anomalien ist ein effektiver Weg, um bösartige (oder verdächtige) Aktivitäten zu identifizieren, aber moderne Netzwerke sind laute, chaotische Orte. Wie bei den meisten Bedrohungssuchen müssen Sie wissen, wie „normale“ Daten aussehen, damit Sie sie erfolgreich herausfiltern können.
(https://github.com/nsacyber/Mitigating-Web-Shells)

Umgehung der Cybersicherheit

Angreifer nutzen bestimmte Techniken, um eine Erkennung ihrer bösartigen Aktivitäten zu umgehen.

BITS-Aufträge

- Siehe *Persistenz: BITS-Aufträge*

Portknocking

- Siehe *Persistenz: Portknocking*

Root-Zertifikate installieren

Öffentliche Zertifikate werden zum Aufbau sicherer TLS/SSL-Kommunikation genutzt. Root-Zertifikate werden genutzt, um die Zertifizierungsstelle (Certificate Authority, CA) zu identifizieren. Root-Zertifikate sind selbstsigniert und bilden einen Vertrauensanker für die Public-Key-Verschlüsselung. Wenn z. B. ein Root-Zertifikat installiert ist, vertraut das System oder die Anwendung den untergeordneten Zertifikaten dieses Root-Zertifikats. Während kein Gerät auf Netzwerkebene (z. B. Router oder Switches) die auf einem Client-System installierte Zertifikatskette anzeigen kann, besteht der Sinn der Installation eines bösartigen Root-Zertifikats darin, die Vertrauensüberprüfung zu umgehen.

Mit Corelight-Daten können Sie alle Aspekte der TLS/SSL-Sitzung anhand der SSL- und X.509-Protokolle beobachten. Diese beiden Protokolle ermöglichen es Analysten, mit den folgenden Aktionen verdächtig erscheinende Zertifikate zu identifizieren:

1. Durchsuchen Sie das SSL-Protokoll nach allen Einträgen, bei denen das Feld „validation_status“ nicht den Wert „ok“ hat.
2. Überprüfen Sie Datensätze, bei denen das Feld „validation_status“ entweder ein selbstsigniertes Zertifikat hat oder eines in der Zertifikatskette enthält.
3. Überprüfen Sie die Felder „subject“ und „server_name“, um die Organisation oder Webseite zu ermitteln, die den Server steuert.
4. Filtern Sie Ergebnisse, bei denen legitime selbstsignierte Zertifikate im Einsatz sind, wie z. B. bei der Kommunikation zwischen IoT-Geräten und der unterstützenden Cloud-Infrastruktur.
5. Untersuchen Sie die IP-Adresse „id.resp_h“, um festzustellen, zu welchem autonomen System (Autonomous System, AS) die Sitzung gehört und ob es sich um eine sinnvolle AS-Organisation handelt (z. B. eine, die mit den Informationen auf dem Server übereinstimmt, oder ein häufig verwendeter Cloud-Hosting-Anbieter).
6. Verwenden Sie für die verbleibenden Verbindungen die Werte in „cert_chain_fuids“, um zu den Zertifikaten im X.509-Protokoll zu navigieren und die Zertifikatdetails zu überprüfen.

Präzisieren Sie Ihre Untersuchungen, indem Sie die lokale Root-Zertifizierungsstelle auf dem Endpunkt prüfen.

Zugriffsberechtigung

Mit einem Angriff auf Zugriffsberechtigungen versucht der Hacker, Kontonamen und Passwörter auszuschleusen.

Brute-Force

Ein Angreifer versucht, unbefugten Zugriff zu erlangen, indem er das Passwort eines Benutzers systematisch mit einem sich wiederholenden oder iterativen Mechanismus errät. Manchmal geht ein Brute-Force-Angriff von einer Liste mit bekannten Informationen aus, was die Erfolgswahrscheinlichkeit erhöht.

Wenn ein Angreifer z. B. versucht, das Passwort eines Active-Directory-Kontos zu erraten, kommt es wahrscheinlich zu vielen Verbindungen zu einem Domain Controller am LDAP-Port (389 oder 636). Ein Angreifer, der versucht, API-URLs in einem E-Commerce-System ausfindig zu machen, generiert im Vergleich zu anderen Clients in einem ähnlichen Zeitraum viel mehr Verbindungen zum Webserver und erzeugt mehr 400- und 500-stufige HTTP-Statuscodes (Fehlermeldungen) als andere Clients.

Um nach einem Brute-Force-Angriff zu suchen, gehen Sie wie folgt vor:

1. Aggregieren Sie im Verbindungsprotokoll nach „id.orig_h“, „id.resp_h“, „id.resp_p“, „proto“ und (optional) „service“.
2. Fügen Sie einen Zähler für die Anzahl der Operationen hinzu und sortieren Sie nach den höchsten Werten.
3. Wählen Sie einen sinnvollen Zeitraum, der sich an der Größe des Netzwerks/Datensatzes orientiert, und gehen Sie der Größe nach aufsteigend vor.
4. Filtern Sie Datensätze, die offensichtlich zulässig sind, wie z. B. wiederholte Kontakte aus Überwachungssystemen der Netzwerk- oder Anwendungsleistung, Schwachstellenmanagementsystemen oder Geschäftsanwendungen.
5. Führen Sie bei unbekannten oder verdächtigen Datensätzen eine genauere Untersuchung des Verhaltens durch. Suchen Sie z. B. nach anderen von der Remote-IP-Adresse ausgehenden Verbindungen.
6. Achten Sie bei Protokollen, die Verbindungen über mehrere Transaktionen oder Versuche aufrechterhalten können, auf lange bestehende Verbindungen. Solche Verbindungen können auch auf repetitives Verhalten hinweisen.

Corelight-Sensoren umfassen ein Skript, das Verbindungen protokolliert, die länger als festgelegte, spezifische Schwellenwerte bestehen, von zehn Minuten bis zu drei Tagen. Wenn Sie kein Corelight-Kunde sind, aber Open-Source-Zeek verwenden, ist dieses Skript über die Corelight-GitHub-Seite verfügbar.

Wenn Sie das „Long-Connections“-Paket installiert haben und lange bestehende Verbindungen finden möchten, gehen Sie wie folgt vor:

1. Untersuchen Sie das Meldungsprotokoll.
2. Überprüfen Sie die Einträge, bei denen der Hinweis „LongConnection::found,“ lautet.
3. Prüfen Sie jeden Satz von „id.orig_h“, „id.resp_h“ und „id.resp_p“, um zu verstehen, ob diese Geräte lange Verbindungen haben sollten.

Wenn Sie das „Long-Connections“-Paket nicht installiert haben und lange bestehende Verbindungen finden möchten, gehen Sie wie folgt vor:

1. Untersuchen Sie das Verbindungsprotokoll.

2. Sammeln Sie eine Liste aller Verbindungen mit den folgenden Feldern: „id.orig_h“, „id.resp_h“, „id.resp_p“, „proto“, „service“ und „duration“. Hier werden nur Verbindungen erfasst, die entweder ordnungsgemäß oder durch Zeitüberschreitung beendet wurden. Aktuell offene Verbindungen werden in den Ergebnissen nicht berücksichtigt.
3. Sortieren Sie die Ergebnisse nach Dauer, sodass die längsten Verbindungen ganz oben stehen.
4. Prüfen Sie jedes Ergebnis auf legitimes oder erwartetes Verhalten.
5. Filtern Sie erwartete Verhaltensweisen heraus und untersuchen Sie alles, was verdächtig erscheint, gründlich.

Corelight bietet mit der Encrypted Traffic Collection (ETC) ein Produkt, das automatisch nach Brute-Force-Attacken gegen SSH-Server innerhalb einer Verbindung sucht, bei denen versucht wird, das Passwort zu erraten.

Erzwungene Authentifizierung
Einige Protokolle authentifizieren sich automatisch, wenn ein Benutzer auf eine Ressource zugreift, ohne vorher zu prüfen, ob diese Ressource vertrauenswürdig ist. Ein Angreifer kann z. B. in einem Microsoft-Office-Dokument einen Verweis auf eine Datei einbetten, die auf einem vom Angreifer kontrollierten UNC-Pfad (\\servername\sharename\path\to\file) gehostet wird. Wenn der Benutzer die Datei öffnet, versucht das Gerät, auf die Ressource zuzugreifen. Der vom Angreifer kontrollierte Server fordert dann den Rechner zur Authentifizierung auf. In den meisten Fällen stellt der betroffene Rechner automatisch zwischengespeicherte Anmeldeinformationen bereit, normalerweise in Form eines NTLM-Hashs. Der Angreifer kann dann versuchen, die Anmeldeinformationen für einen nicht autorisierten Zugriff zu verwenden, in der Regel durch Umkehrung des Hashs, um das Passwort zu erhalten, oder durch Wiederverwendung des Hashs in einem Pass-the-Hash-Angriff.

Dafür muss der Angreifer die Server-Infrastruktur kontrollieren. Daher ist der wahrscheinlichste Angriffsvektor Spearphishing. Der Angreifer *phisht* einen Benutzer im Netzwerk und der betroffene Rechner verbindet sich dann über das Internet mit dem vom Angreifer kontrollierten Server. Um nach diesem Verhalten zu suchen, halten Sie im Internet Ausschau nach Authentifizierung:
1. Suchen Sie im NTLM-Protokoll nach Anzeichen für eine NTLM-Authentifizierung, bei der die Ziel-IP im externen Netzwerk liegt.
2. Suchen Sie nach Einträgen im Verbindungsprotokoll, in denen das Feld „service“ „smb“ (und/oder „ntlm“) enthält und „local_resp“ „false“ ist.

Bei LLMNR- oder NBT-NS-Vergiftungen lauscht ein Angreifer auf lokale LLMNR- oder NBT-NS-Broadcasts, die nach einer bestimmten Ressource mit Namen fragen. Der Angreifer antwortet dann dem anfragenden Client, indem er die tatsächliche Ressource fälscht. Wenn es sich um eine Ressource handelt, die normalerweise eine Authentifizierung erfordert, kann der Angreifer den Client zur Authentifizierung auffordern. Wenn sich der Client authentifiziert (in der Regel mit einem Passwort-Hash), verwendet der Angreifer die Anmeldedaten, um sich als Client auszugeben und auf Ressourcen zuzugreifen.

Mit Corelight-Daten können Sie gezielt nach solchen Angriffen suchen, aber der Sensor muss sich innerhalb der Broadcast-Domain befinden, da der Broadcast-Verkehr normalerweise keine Router durchläuft. In der Regel müssen Sie ganze VLANs erweitern oder spiegeln oder LLMNR- oder NBT-NS-Datenverkehr von Client-Subnetzen und VLANs an Stellen im Netzwerk weiterleiten, die Corelight überwacht.

Suchen Sie nach DNS-Protokollen, bei denen „id.resp_p“ „5355“ (LLMNR) oder „id.resp_p“ „137“ (NBT-NS) ist, und filtern Sie nach Datensätzen, bei denen das Feld „answers“ nicht leer ist. Zählen Sie dann die Anzahl der eindeutigen „query“-Felder pro „id.resp_h“. Diese Suche ergibt IPs, die auf mehr als einen Namen reagieren.

Netzwerk-Sniffing

Sie können einen Eindringling, der im Datenverkehr Ihres Netzwerks *schnüffelt*, nicht anhand von Netzwerkprotokollen erkennen, da diese Aktion unsichtbar ist; Sie können jedoch *einen Eindringling erkennen, indem Sie in Ihrem eigenen Netzwerk schnüffeln*, da der Angreifer das wiederum nicht sehen kann.

Corelight-Sensoren ermöglichen Ihnen, ein Out-of-Band-Sensornetz einzusetzen, das verknüpfte Protokolle erzeugt. Diese Protokolle beschleunigen die zuverlässige Beobachtung und Erkennung und helfen dabei, den Fallstrick der Präventionsabhängigkeit zu vermeiden, und liefern gleichzeitig den Kontext für eine tiefere und genauere historische Analyse. Wie Rob Joyce, Chef der NSA-Abteilung *Tailored Access Operations*, es in seinem USENIX-Vortrag 2016 formulierte: „Wir beuten den Nationalstaat aus ... Wie verteidigen Sie sich, um mir das Leben schwer zu machen?“

Erkennung

Der Angreifer versucht, etwas über Ihre Umgebung zu erfahren.

Scannen von Netzwerkdiensten

Ein Eindringling kann aktiv danach scannen, welche Geräte in einem Netzwerk Schwachstellen aufweisen und welche Dienste auf diesen Geräten verfügbar sind. Aktive Scanmethoden sind u. a.:

- Horizontale Scans: Senden von Verbindungsanforderungen an einen bestimmten Port über viele IPs, um zu sehen, welche IPs antworten. Wenn Sie z. B. viele Geräte auf Port TCP/22 scannen, werden normalerweise Geräte angezeigt, auf denen ein SSH-Server läuft. Das Scannen über viele Geräte auf Port TCP/445 kann die Windows-Infrastruktur effektiv aufzählen.
- Vertikale Scans: Senden von Verbindungsanforderungen an eine einzelne IP-Adresse über viele Ports, um zu sehen, welche Ports antworten. Mit dieser Methode können Angreifer auf die von dieser IP-Adresse verfügbaren Dienste schließen.

Jede dieser Methoden kann mit einem kostenlosen oder kommerziell erhältlichen Schwachstellenscanner durchgeführt werden. Diese Produkte verfügen oft über weitere Möglichkeiten, um die Verfügbarkeit von Diensten und Versionsinformationen zu prüfen und festzustellen, ob Dienste für bekannte Ausnutzungstechniken anfällig sind.

Wenn ein Eindringling eine oder mehrere der oben genannten Methoden verwendet, um einen Dienst zu finden, ist das Nebenprodukt eine *fehlgeschlagene* oder *verweigerte* Verbindung. In Corelight-Daten werden diese im Verbindungsprotokoll als Verbindungen mit einem „conn_state“ von „S0“ (initiiert und ignoriert) oder „REJ“ (initiiert und abgewiesen) aufgezeichnet und haben typischerweise ein „history“-Feld, in dem kein „D“ (Post-Synchronisierungsdaten vom Initiator) vorhanden ist. Um Scans von Netzwerkdiensten innerhalb des Netzwerks zu suchen, gehen Sie wie folgt vor:

1. Suchen Sie nach Einträgen im Verbindungsprotokoll, bei denen „conn_state“ „S0“ bzw. „REJ“ ist.
2. Filtern Sie nach Datensätzen, bei denen „local_orig“ und „local_resp“ „true“ sind.
3. Gruppieren und zählen Sie die Ergebnisse nach „id.orig_h“ und der Anzahl der eindeutigen „id.resp_p“, um die Horizontalität/Vertikalität des Scans zu beurteilen.
4. Untersuchen Sie die Liste, beginnend mit den Datensätzen, die den höchsten Wert von „id.resp_h“ oder „id.resp_p“ aufweisen.
5. Identifizieren Sie den Absender (id.orig_h) und prüfen Sie die Liste der Responder (id.resp_h) und Ports (id.resp_p).
6. Bestimmen Sie anhand der Identität der Quelle, der beteiligten Ports und der Ziele, ob das Verhalten akzeptabel ist.

Nicht alle aufgelisteten Elemente sind bösartig. DHCP-Server werden z. B. häufig so konfiguriert, dass sie eine IP-Adresse *anpingen*, um zu prüfen, ob die Adresse in Gebrauch ist, bevor sie sie aus dem Pool zuweisen. Druckerserver mit einer großen Anzahl von Druckwarteschlangen versuchen, SNMP- und/oder Netzwerkdruckdienste an Drucker zu senden, auch wenn diese Drucker offline sind. Aus diesem Grund können Druckerserver eine große Anzahl von S0-Verbindungen verursachen. Natürlich kann auch legitim scannende Software, wie z. B. ein vom Unternehmen genehmigter Schwachstellenscanner oder ein

Bestandsverwaltungssystem, in der Liste erscheinen. Abschließend führen Netzwerktechniker Ad-hoc-Netzwerk-Scans zur Fehlersuche durch. Wenn Sie auf Netzwerk-Scans stoßen, ändern Sie die ursprüngliche Abfrage, um die gutartigen Datensätze auszulassen, und setzen Sie die Suche dann fort.

Erkennung von Netzwerkfreigabe
Das am häufigsten von Angreifern missbrauchte Netzwerkfreigabeprotokoll ist SMB, der Windows-Standard für die Dateifreigabe. SMB wird von allen modernen Betriebssystemen unterstützt Hochwertige Dokumente, in denen personenbezogene Daten, Geschäftsgeheimnisse, Netzwerkdiagramme und andere sensible Daten gespeichert sind, befinden sich typischerweise auf SMB-Freigaben in Unternehmen aller Größen.

Das Scannen nach und Erkennen von Freigaben auf einem SMB-Server erfolgt in der Regel mit einem DCE/RPC-Befehl auf TCP-Port 445. Konkret folgt auf eine Verbindung zur „srvsvc“-Pipe, die in den dce_rpc-Protokollen als gleichnamiger Endpunkt auftaucht, ein Aufruf der Funktionen „NetShareEnumAll“ oder „NetShareEnum“ (im Zeek-Protokoll „operations“ genannt). Diese Funktionsaufrufe werden für legitime Zwecke der Dateifreigabe verwendet und sind für sich genommen kein ausreichender Hinweis auf böswillige Absichten. In Kombination mit anderen Lateral-Movement-Indikatoren veranschaulichen sie jedoch, wie sich ein Angreifer lateral innerhalb eines Netzwerks bewegt. Primäre Ziele für weitere Untersuchungen sind solche, die eine große Anzahl von DCE_RPC-Funktionsaufrufen über eine große Anzahl von Hosts in einem kurzen Zeitraum erzeugen.

Netzwerk-Sniffing (X-reference)
- Siehe Zugriffsberechtigung: Netzwerk-Sniffing

Erkennung von Remote-Systemen
Die gleichen Prinzipien für das Erkennen von Netzwerkdienst-Scans gelten für das Erkennen von Remote-Systemen. Lesen Sie diesen Abschnitt für weitere Informationen.

Lateral-Movement

Angreifer nutzen Lateral-Movement-Techniken, um sich Zugang zu Remote-Systemen in einem Netzwerk zu verschaffen und sie zu kontrollieren.

Remote Desktop Protocol (RDP)
Das Microsoft Remote Desktop Protocol (RDP) wird zur Fernkontrolle eines Windows-Endpunktes verwendet. Dieses Protokoll kann von einem Angreifer missbraucht werden, um unbefugten Zugriff auf Ihr Netzwerk zu erhalten (siehe Erstzugriff: Externe Remote-Dienste). Befindet sich der Eindringling bereits im Netzwerk, kann er sich mithilfe RDP lateral zwischen den Geräten bewegen.

RDP ist eines von vielen Protokollarten, die Corelight analysiert. In manchen Umgebungen reicht das Vorhandensein von RDP bzw. dessen Vorhandensein auf bestimmten Systemen aus, um eine Untersuchung auszulösen. In Netzwerken, in denen RDP erlaubt ist, enthält das Zeek-RDP-Protokoll zahlreiche Informationen, mit denen festgestellt werden kann, ob eine Verbindung legitim ist, z. B. die Aufzeichnung von Daten wie Tastaturlayout, Verschlüsselungsstufen oder Client-Namen für eine Verbindung.

Bei der Suche mit dem RDP-Protokoll:

1. Achten Sie auf die Felder „id.orig_h“, „id.resp_h“, „id.resp_p“ und „cookie“. Das Feld „cookie“ kann einen beliebigen Wert enthalten, der vom RDP-Client an den Server gesendet wird, aber es enthält häufig den vom RDP-Client gesendeten Benutzernamen.
2. Aggregieren Sie die Datensätze basierend auf diesen vier Feldern und zeigen Sie eine Zählung für jeden eindeutigen Satz an.
3. Iterieren Sie durch den Satz und identifizieren Sie den Ursprung und das Ziel jeder Verbindung (z. B. können Sie die Einträge aus den DNS- und DHCP-Protokollen verwenden).
4. Einige RDP-Verbindungen nutzen ein nicht standardmäßiges Tastaturlayout. Um danach zu suchen, untersuchen Sie das Feld „keyboard_layout“. Zählen Sie die Anzahl der Instanzen jedes Wertes und wenden Sie Daten-Stacking an, um nach abweichenden oder selten auftretenden Werten zu suchen.
5. Identifizieren Sie den Ursprung und das Ziel und stellen Sie fest, ob das nicht standardmäßige Tastaturlayout zu erwarten ist, z. B. wenn bekannt ist, dass der Ursprungsbenutzer nicht Englisch als Primärsprache hat und letztere die angeforderte Sprache in der RDP-Verbindung ist.

Stellen Sie sich nach dem Erhalt dieser Information folgende Fragen:

- Stimmt der „cookie“-Wert mit dem erwarteten Benutzer auf dem Quell- oder Zielrechner überein?
- Gibt es einen legitimen Grund für den Absender, RDP zu verwenden?
- Gibt es Benutzer, die RDP verwenden, bei denen Sie das für ihre Arbeitsfunktion nicht erwarten würden?

Remote-Dienste

Die Ausnutzung einer Software-Schwachstelle liegt vor, wenn ein Angreifer einen Programmierfehler ausnutzt, um Code auszuführen, den er selbst kontrolliert. Die Schwachstelle kann in einem Programm, Dienst oder innerhalb der Betriebssystemsoftware oder des Kernels selbst ausgenutzt werden. Ein häufige Methode für die Ausnutzung von Schwachstellen bei Remote-Diensten nach der Kompromittierung ist die Lateral-Movement-Technik.

Angesichts der Komplexität heutiger Unternehmensnetzwerke sind oft eine Vielzahl von Drittanbieter- und externen Diensten im Einsatz. Diese Dienste ermöglichen es Angreifern, Erstzugriff zu erhalten oder sich lateral zu bewegen. Alle Verbindungen werden im Verbindungsprotokoll aufgezeichnet. Je nach Art des angegriffenen Remote-Dienstes können jedoch weitere Details in den spezifischen Protokollen verfügbar sein. Sie können z. B. die Datei „http.log“ auf verdächtige und unerwartete HTTP-Anfragen (z. B. OPTIONS-Anfragen) überwachen.

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,

Zusätzlich extrahiert Corelight Informationen über im Netzwerk beobachtete Software in das Software-Protokoll. Diese Datei liefert Sicherheitsteams wertvolle Daten zur Überwachung unerwarteter oder nicht autorisierter Server, anfälliger oder veralteter Dienste und ungepatchter Client-Software.

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

Admin-Freigaben unter Windows
Windows-Systeme verfügen über versteckte Netzwerkfreigaben, auf die nur Administratoren zugreifen können und die Remote-Dateikopien und die Nutzung anderer administrativer Funktionen ermöglichen. Beispiele für Netzwerkfreigaben sind C$, ADMIN$ und IPC$.

Angreifer verwenden SMB häufig, um sich mit administrativen Freigaben auf Microsoft-Windows-Workstations und -Servern zu verbinden. Sie möchten mehr über das Ziel erfahren, sensible Dateien extrahieren, bösartige Nutzdaten hochladen oder sich authentifizieren, damit weitere Tools genutzt und Angriffe durchgeführt werden können. Corelight ermöglicht es Sicherheitsteams, Muster von administrativen Authentifizierungsversuchen zu erfassen und protokollieren sowie den SMB-Verkehr zu überwachen, um übertragene Dateien zu extrahieren. Das folgende Beispiel zeigt, wie die Aktion „FILE_OPEN“ unter Verwendung der versteckten Admin-Freigabe ausgeführt wird, und enthält MAC-Informationen. Corelight protokolliert die durchgeführte Aktion einschließlich Öffnen/Umbenennen/Löschen/Schreiben.

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

Datenerfassung

Der Angreifer versucht, Daten zu sammeln, um sein Ziel zu erreichen.

Erfasste Daten archivieren

Um Daten zu verschleiern, können Angreifer Daten in komprimierten Archivdateien zusammenfassen, z. B. in ZIP-, RAR-, TAR- oder CAB-Dateien. Um dieser Verschleierungstechnik auf den Grund zu gehen, verwenden Sie das Dateiprotokoll.

Gehen Sie wie folgt vor, um nach komprimierten Dateien zu suchen:

1. Durchsuchen Sie alle Dateiprotokolle und rufen Sie die Felder „tx_hosts“, „rx_hosts“, „mime_type“, „total_bytes“ und „source“ ab.
2. Entfernen Sie Datensätze mit uninteressanten „mime_types“ aus den Ergebnissen, wie z. B.:
   a. application/x-x509-*
   b. application/ocsp*
   c. image/*
   d. audio/*
   e. video/*
   f. text/*
   g. application/xml
   h. application/chrome-ext

Automatisierte Erfassung

Angreifer können automatisierte Tools auf einem kompromittierten Host einsetzen, um Intranet-Dienste auf sensible Daten und Firmengeheimnisse zu durchsuchen. Diese Tools können Skripte enthalten, die in bestimmten Zeitintervallen nach Informationen wie Dateityp, Speicherort oder Name suchen (und diese kopieren). Eindringlinge können Tools für den Remote-Zugriff zur automatisierten Datenerfassung nutzen.

Ein benutzerdefiniertes Tool kann z. B. einen Intranet-Webserver oder einen internen E-Mail-Server abfragen und regelmäßig nach neuen Inhalten suchen. Corelight überwacht mehrere Protokolle, darunter HTTP-, E-Mail-, MySQL-, FTP- und SMB-Datenverkehr, um einen Einblick in diese Abfragen zu geben.

Indem Sicherheitsteams auf sich wiederholende Abfragen oder regelmäßig geplante Verbindungen achten, können sie automatisierte Tools zur Datenerfassung identifizieren. Wenn ein Eindringling z. B. Web Scraping betreibt, wird es eine große Anzahl an Verbindungen aus einer endlichen Anzahl an IP-Adressen geben.

Zusätzlich können Sie die SMB-Protokolle („smb_files“ oder „smb_mapping“) verwenden, um anomale Verkehrsmuster zu identifizieren.

Daten eines freigegebenen Netzlaufwerks
Freigegebene Netzlaufwerke sind eine Fundgrube für sensible Unternehmensdokumente. Die meisten Unternehmensnetzwerke hosten freigegebene Netzlaufwerke über SMB, aber einige nutzen auch FTP, HTTP oder sogar RDP. Zeek kann den Zugriff auf freigegebene Netzlaufwerke überwachen, wenn Protokolle wie SMB, FTP oder HTTP verwendet werden. Remote-Steuerungsprotokolle wie RDP werden ebenfalls in spezifischen Protokollen analysiert. Überall, wo Corelight diesen Datenverkehr sieht, wird er überwacht und im spezifischen Protokoll aufgezeichnet.

Das folgende Beispiel veranschaulicht das FTP-Protokoll. Corelight protokolliert den Befehl und die Argumente.

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

Command-and-Control

Der Angreifer versucht, mit kompromittierten Systemen zu kommunizieren, um sie zu kontrollieren.

Häufig verwendete Ports/Nicht-Standard-Ports
Angreifer können einen häufig verwendeten Port verwenden, um eine genauere Prüfung zu vermeiden.

Die Suche nach C2-Kanälen über häufig genutzte Ports ist schwierig, aber nicht unmöglich. Um C2-Kanäle zu finden, suchen Sie nach bekannten Ports, die mit einem ungewöhnlichen Dienst verwendet werden.

Gehen Sie bei der Suche nach C2-Kanälen über häufig genutzte Ports wie folgt vor:

1. Achten Sie zunächst auf das Feld „service“ und suchen Sie im Verbindungsprotokoll nach Einträgen, bei denen das Feld „service“ nicht dem entspricht, was Sie für den Standard-Port erwarten würden (das Feld „service“ könnte entweder ein „-“ oder ein anderer Dienst sein).
   a. Beginnen Sie mit den häufigsten Protokollen.
      - TCP:80 (HTTP) TCP:443 (HTTPS)

- TCP:25 (SMTP)
- TCP/UDP:53 (DNS)

2. Die Encrypted Traffic Collection von Corelight enthält ein Paket mit dem Namen „Encryption Detection“. Encryption Detection erzeugt einen Hinweis, wenn Klartextverkehr auf normalerweise verschlüsselten Ports beobachtet wird. Die Beobachtung von Hinweisen für Viz::UnencryptedService hebt dieses Verhalten hervor und hilft Ihnen, potenziell bösartige Verbindungen zu identifizieren, die gängige Ports verwenden.

Das Encrypted-Traffic-Collection-Paket von Corelight weist Sie außerdem darauf hin, wenn eine Sitzung Sofortverschlüsselung nutzt. Das Paket sucht nach Pre-shared Keys oder verschlüsselten Verbindungen, die ohne eine traditionelle Schlüsselverhandlung beginnen. Die Beobachtung von Hinweisen für Viz::CustomCrypto hebt dieses Verhalten hervor und hilft Ihnen, potenziell bösartige Verbindungen zu identifizieren, die gängige Ports verwenden.

Zusätzlich können Sie die Corelight-DPD- und WEIRD-Protokolle verwenden, um unerwartetes Protokollverhalten zu identifizieren. Diese Protokolle zeigen Debugging- und Analysefehler an und identifizieren die nicht spezifizierte Nutzung gängiger Ports und Protokolle – was auf bösartige Aktivitäten oder die verdeckte Nutzung bekannter Ports und Protokolle hindeuten könnte.

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

Verschlüsselter Kanal
Siehe Abschnitt Häufig verwendete Ports für eine Beschreibung des Encryption-Detection-Pakets von Corelight, dem DPD- und dem WEIRD-Protokoll. Diese helfen Ihnen, potenzielle eigene kryptografische Protokolle zu identifizieren.

Fallback-Kanäle, Multi-Stage-Kanäle
Es ist bekannt, dass Angreifer die Kommunikation zwischen verschiedenen Protokollen aufteilen, indem sie eines für eingehende C2 und ein anderes für ausgehende Daten verwenden. Dies ermöglicht die Umgehung von Firewall-Beschränkungen bei der Kommunikation.

Malware, die die Kommunikation zwischen zwei Hosts für Anweisungen und zur Exfiltration aufteilt, stellt eine neue Herausforderung für Sicherheitsteams dar. Die Verbindung zwischen verdächtigem Kontrollverkehr und großen Datenübertragungen zu erkennen, ist eine Herausforderung, aber Zeek bietet Pakete und Frameworks, die Daten synthetisieren. Z. B. gibt es ein Paket zur Ermittlung des Produzent-Konsument-

Verhältnisses (Producer/Consumer Ratio, PCR) für Verbindungen, das unausgewogene und möglicherweise verdächtige Datenübertragungen identifiziert. Darüber hinaus ermöglicht das Intelligence Framework die Koordination mit anderen Sicherheitsteams, indem es mögliche Gefahrenindikatoren (IP-Adressen, E-Mail-Adressen und Domainnamen) in den Corelight-Daten identifiziert.

Es ist schwierig, Angreifer zu identifizieren, die verschiedene Kommunikationsmethoden und -kanäle nutzen, aber die Inhalte von Corelight sowie die Frameworks und Pakete von Zeek können dabei helfen. Sie ermöglichen es den Sicherheitsteams, die versteckten Kanäle unauffällig zu identifizieren und bieten mehrere Möglichkeiten zur Erkennung.

Neben der Beobachtung der zuvor erwähnten C2-Kommunikationsmechanismen gibt es noch einige andere Anzeichen, die in den Corelight-Daten vorhanden sind:

- Verwenden Sie das Verbindungsprotokoll, um Kommunikationsmuster zu identifizieren, die auf zusätzliche Kanäle hinweisen (z. B. mithilfe von „orig_h“ und „resp_h“, um Verbindungen auf ein Zeitfenster einzugrenzen und Verbindungen zwischen den Hosts zu beobachten, die ungewöhnliche Ports oder interessante/verdächte Elemente enthalten oder solche, die fehlgeschlagen sind oder verweigert wurden).
- Verwenden Sie die Encrypted Traffic Collection von Corelight oder selbst entwickelte Inhalte in Kombination mit der Erkennung von Verbindungsprotokollen, um potenzielle Beziehungen zwischen sich überschneidenden, benachbarten oder interessanten Verbindungen zu finden.
- Suchen Sie nach Sequenzen von Verbindungen zu nicht verwandten Hosts mit unterschiedlichen Protokollen oder Vorfällen in den DPD- und WEIRD-Protokollen, wie in Häufig verwendete Ports beschrieben.

Ingress Tool Transfer

Eindringlinge verschieben in der Regel Dateien auf kompromittierte Systeme – sowohl Tools, die zur Ausführung weiterführender Lateral-Movement-Techniken genutzt werden, als auch sensible Dateien, die zur Exfiltration bestimmt sind. Diese Dateien werden normalerweise über eine HTTP(S)-, SSH- oder SMB-Verbindung übertragen.

Bei Dateien, die über Klartext-HTTP verschoben werden, können Details wie der Name des Remote-Hosts sowie der Name und der MIME-Typ der übertragenen Datei nützliche Hinweise sein. Benutzer sollten auch das Dateiprotokoll nach den Hashes der verschobenen Dateien durchsuchen, da viele beliebte Angreifer-Tools bekannte Krypto-Hashes haben, die eine Identifizierung leicht machen. Im Falle von HTTPS können Sicherheitsteams die IP-Adresse des Remote-Systems sowie die im SSL-Protokoll vermerkten Zertifikatdetails (d. h. Organisationsname, FQDN des Remote-Hosts aus dem CN usw.) verwenden, um nach anomalen Verbindungen zu suchen.

Eindringlinge kopieren Dateien von einem Endpunkt zu einem anderen, während sie sich lateral zwischen kompromittierten Ressourcen bewegen. Traditionell erfolgt das Kopieren von Dateien in oder aus Unix/Linux-Systemen über das SSH-Protokoll mit dem Befehl „scp“. Bei Windows-Systemen erfolgt der Remote-Up- bzw. -Download von Dateien in der Regel über SMB. SSH kann aber auch über PUTTY verwendet werden.

Corelight-Sensoren mit dem aktivierten ETC-SSH-Inferenzpaket erweitern das SSH-Protokoll. Die Erweiterung enthält das Feld „inferences“, das abgeleitete Merkmale über den SSH-Verkehr hinzufügt. Z. B., wenn die Sitzung zum Verschieben von Dateien verwendet wird oder wenn sie interaktiv ist:

- LFU: Upload großer Dateien
- LFD: Download großer Dateien
- KS: Keystrokes

Nutzen Sie das Feld „inferences“ im ETC-SSH-Paket, um nach interessanten SSH-Sitzungen zu suchen:

1. Identifizieren Sie Sitzungen, in denen das Feld „inferences“ „LFU“, „SFU“, „LFD“ oder „SFD“ enthält.
2. Stellen Sie fest, ob die Datei-Aktivität über SSH legitim und zu erwarten ist.

Corelight-Sensoren sind mit dem MITRE-BZAR-Paket (Bro/Zeek ATT&CK-Based Analytics and Reporting) ausgestattet. MITRE BZAR identifiziert MITRE-ATT&CK-Techniken für Remote-Dateikopien, also Dateien, die auf C$- oder ADMIN$-Freigaben kopiert werden. Dieses Paket erzeugt Einträge im Meldungsprotokoll, wie unten abgebildet:

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: Saved a copy of the file written to SMB admin file share,
sub: 23.10.2020/6f24ac6ce591baf02acd64684f596d2db0ec97c0,
src: 192.168.38.104,
dst: 192.168.38.102,
p: 445,
actions: [Notice::ACTION_LOG],suppress_for:3600.0

Auch wenn Sie das MITRE-BZAR-Paket auf Ihrem Corelight-Sensor nicht aktivieren, protokolliert Corelight SMB-Freigabezugriffe im smb_mapping-Protokoll und Dateizugriffe und -änderungen im smb_files-Protokoll. Die folgenden Protokolle veranschaulichen die Daten, die in der Corelight-Familie der SMB-Protokolle enthalten sind:

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

Gehen Sie wie folgt vor, um nach lateralen Bewegungen zu suchen:

1. Beginnen Sie mit der Suche in den smb_files-Protokollen und achten Sie auf die Felder „id.orig_h“, „id.resp_h“, „path“ und „name“.
2. Filtern Sie Datensätze heraus, bei denen „id.resp_h“ ein bekannter Dateiserver ist, wodurch die Ergebnisse auf potenziell interessante Verbindungen eingegrenzt werden.
3. Stellen Sie mithilfe der Felder „path“ und „name“ fest, von welcher Freigabe aus auf die Datei zugegriffen wurde oder in sie geschrieben wurde, und bestimmen Sie, ob das Verhalten verdächtig ist.
4. Um zusätzlichen Kontext über die verbleibenden interessanten Datensätze zu erhalten, können Sie zum Dateiprotokoll navigieren und mithilfe der UID spezifische Informationen über die Datei(en) sammeln. Z. B. werden die MD5/SHA1/SHA256-Hashes automatisch berechnet und können zum Identifizieren bekannter Malware in externen Systemen wie VirusTotal verwendet werden.
    a. Es stehen auch andere Felder und eventuell Protokolle zur Verfügung (z. B. PE-Protokoll), die zum Ausschluss uninteressanter Datensätze verwendet werden können.

Protokoll ohne Anwendungsschicht

Angreifer nutzen mehrere Techniken, um sich im legitimen Datenverkehr zu verstecken: Sie senden ihre Kommunikation über ein benutzerdefiniertes Protokoll an einem allgemein erlaubten Port wie 80, 443 oder 53 und betten ihre Nachrichten in die Struktur legitimer, aber typischerweise weniger überwachter Protokolle wie ICMP ein.

Siehe Abschnitt Häufig verwendete Ports/Nicht-Standard-Ports für Informationen zur Nutzung eigener Protokolle an Standard-Ports und für eine Beschreibung des Encryption-Detection-Pakets von Corelight, dem DPD- und dem WEIRD-Protokoll. Diese helfen Ihnen, benutzerdefinierte C2-Kommunikationen zu identifizieren, die eine nicht standardmäßige Verschlüsselung verwenden oder gegen herkömmliche Protokollspezifikationen verstoßen.

Malware verwendet manchmal standardisierte Protokolle auf niedrigerer Ebene wie ICMP, UDP und SOCKS, um eine Erkennung zu vermeiden, da diese Protokolle selten überwacht werden. Malware-Autoren könnten z. B. C2-Anweisungen in ein ICMP-Echo-Request-Paket („ping“) einbetten.

Corelight überwacht jegliche Verbindungen, unabhängig von Protokollen, und zeichnet die Verbindungsdaten im Verbindungsprotokoll auf. C2-Kanäle, die benutzerdefinierte UDP-Protokolle oder TCP-basierte SOCKS-Protokolle (aber keine Standardprotokolle der Anwendungsschicht) verwenden, haben Verbindungsprotokolleinträge ohne identifizierbares „service“-Feld. Diese Felder und Protokolle bieten einen Einblick in die Verkehrsströme im Netzwerk – sogar ICMP, UDP und SOCKS. Bei ICMP-Sitzungen enthalten die Corelight-Daten mehr als nur die Quelle und das Ziel, z. B. die Anzahl der Pakete, die übertragenen Bytes und die Größe der ICMP-Daten sowohl für den Sender als auch für den Empfänger.

Mit diesen Daten haben Sie die nötigen Informationen, um ungewöhnlich umfangreiche oder häufige ICMP-Kommunikationen zu entdecken, die auf C2 hinweisen können. Das folgende Protokoll ist ein Beispiel für das SOCKS-Protokoll.

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

Um einen Eindringling zu suchen, der ein Standardprotokoll ohne Anwendungsschicht zum Tunneln von Informationen verwendet, gehen Sie wie folgt vor:

1. Suchen Sie im Verbindungsprotokoll nach Einträgen, bei denen das Feld „service“ leer, „local_orig“ „true“ und „local_resp“ „false“ ist.

2. Aggregieren Sie diese Ergebnisse nach „id.orig_h“, „id.resp_h“, „id.resp_p“ und fassen Sie sie nach Anzahl zusammen.
3. Filtern Sie nach „normalen“ Einträgen.
4. Untersuchen Sie die verbleibenden Elemente und achten Sie dabei zunächst auf jene mit der größten Anzahl.

Nicht-Standard-Ports

Jede Verbindung, die in einer von Corelight überwachten Umgebung hergestellt wird, wird im Verbindungsprotokoll aufgezeichnet. Nachdem Sie eine Liste mit regelmäßig verwendeten Ports (z. B. 22/SSH, 25/SMTP, 80/HTTP und 443/SSL) erstellt haben, können Sie die Corelight-Daten abfragen, um Verbindungen zu Ports zu finden, die nicht in dieser Liste enthalten sind.

Wenn Sie auf Verbindungen stoßen, die auf anderen Nicht-Standard-Ports erscheinen, untersuchen Sie den Layer-7-Dienst, den Corelight beobachtet und im Feld „service“ des Verbindungsprotokolls aufzeichnet. Fälle ohne erkannten Dienst sind am verdächtigsten, besonders wenn große Datenmengen übertragen werden oder die Verbindungsdauer lang ist.

Wenn Sie auf bekannte Dienste an irregulären Ports stoßen, untersuchen Sie die Details im entsprechenden Protokoll auf zusätzliche Hinweise. Notieren Sie z. B. im HTTP-Protokoll den Namen des Remote-Hosts, die User-Agent-Zeichenfolge des Clients und den Uniform Resource Identifier (URI). In Kombination können sie alle Hinweise auf die Software enthalten, die die Anfrage auf dem ungewöhnlichen Port erzeugt.

Path: conn,
uid: CrIlbI1BJ8Al8ryyX6,
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
Obwohl die Verwendung von Proxys selbst nicht die Anwesenheit eines Eindringlings beweist, können Eindringlinge Proxys zum „Waschen“ von Verbindungen verwenden, um die Kommunikation vor Sicherheitsteams zu verschleiern. Es gibt viele Methoden, dies zu beobachten, einschließlich der traditionellen Analyse der zugrunde liegenden Verbindung (Signatur, Anomalie, Verhalten) und der statistischen Analyse der Verbindungseigenschaften. Die genaue Identifizierung von Proxy-Verbindungen ist entscheidend für den Beginn einer Suche oder Untersuchung.

Wenn Sie im HTTP-Protokoll von Zeek einen Wert im Feld „proxied“ sehen, bedeutet dies, dass eine HTTP-Verbindung über einen Proxy hergestellt wurde. Das HTTP-Protokoll erfasst Proxy-Details aus den HTTP-Headern. Suchen Sie nach allen Datensätzen im HTTP-Protokoll, bei denen das Feld „proxied“ nicht leer ist.

- host: Domainname der Webseite
- id.orig_h: IP-Adresse des Proxys oder Reverse-Proxys
- id.resp_h: IP-Adresse des Webservers
- proxied: identifiziert den Proxy und die originale IP-Adresse des Clients

Z. B. initiierte ein Client mit der IP 219.90.98.8 diese HTTP-Anfrage. Die Anfrage wurde über 172.16.1.30 an den Webserver unter 172.16.2.95 weitergeleitet.

host: www.totallyfakedomain.com
id.orig_h: 172.16.1.30 //the proxy
id.orig_p: 53,828
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

Identifizieren Sie anhand dieses Beispiels den Proxy und bestimmen Sie, ob es sich um einen internen oder externen Proxy handelt. Wenn er extern ist, werten Sie die Sitzung aus und erhalten Sie mithilfe der Corelight-Daten den nötigen Kontext, um zu entscheiden, ob er blockiert werden soll oder nicht. Im Falle eines internen Proxys, stellen Sie fest, ob es sich um einen legitimen Teil der IT-Infrastruktur oder um einen ungenehmigten Rogue-Proxy handelt, der zur Umgehung von Richtlinien eingerichtet wurde (Schatten-IT).

Zudem ist SOCKS ein häufig verwendetes Proxy-Protokoll, das von Corelight-Sensoren analysiert wird. Wenn SOCKS erkannt wird, wird ein SOCKS-Protokoll erstellt, das Details zu Benutzern und Protokollen aufzeichnet. Diese Informationen können verwendet werden, um sicherzustellen, dass die Verbindungen nicht bösartig sind und den Richtlinien entsprechen. Achten Sie im SOCKS-Protokoll auf folgende Felder:

- id.orig_h: IP-Adresse des Clients
- id.resp_h: IP-Adresse des Proxys
- request: Domain oder IP, auf die der Client zugreifen möchte

user: Benutzer des Proxys (bei authentifizierter Verbindung)

Webdienste

Angreifer können einen legitimen externen Webdienst nutzen, um Daten an ein kompromittiertes System bzw. von einem kompromittierten System weiterzuleiten.

Angreifer nutzen bekannte Webdienste für C2-Kanäle, um sich im Rauschen zu verstecken. Diese Taktik erschwert zwar die Identifizierung, aber die Corelight-Daten, insbesondere die HTTP-, SSL-, Verbindungs- und X.509-Protokolle, helfen Ihnen, verdächtige Verbindungen zu erkennen. Beginnen Sie mit der Suche nach Gefahrenindikatoren, einschließlich URI, Hostname oder spezifischen Zertifikatdetails (wie SNI oder CN). Im Folgenden finden Sie einige Beispiele für „certificate“-Felder, die eine Untersuchung erfordern könnten:

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

Exfiltration

Automatisierte Exfiltration

Wenn ein Angreifer eine automatisierte Methode zur Exfiltration verwendet, werden Datenartefakte in den Corelight-Daten erfasst.

Um eine Exfiltration in Ihrem Netzwerk aufzudecken, können Sie das Zeek-Paket verwenden, das zur Ermittlung des Produzent-Konsument-Verhältnisses (PCR) entwickelt wurde. Die PCR-Werte zeigen an, ob die Ströme verbrauchend (Download) oder produktiv (Upload) sind. Die PCR-Werte reichen von -1 (verbrauchend) bis +1 (produktiv). Um nach Exfiltration zu suchen, gehen Sie wie folgt vor:

1. Installieren und aktivieren Sie das PCR-Paket.
2. Erzeugen Sie eine Tabelle mit „id.orig_h“, „id.resp_h“, „id.resp_p“ und „pcr“ aus dem Verbindungsprotokoll.
3. Um die Ergebnisse einzugrenzen, wenden Sie die Filter „local_orig“ = „false“ oder „local_resp“ = „true“ an.
4. Grenzen Sie die Ergebnisse weiter ein, indem Sie den Filter pcr ≤ 0 anwenden.
5. Überlegen Sie für jeden Host, der Ströme erzeugt, bei denen pcr ≥ 0 ist, ob dieser Host voraussichtlich Daten innerhalb oder außerhalb des Netzwerks übertragen wird.

Eine andere Möglichkeit ist die Verwendung eines SIEM zur Berechnung der PCR anhand der im Corelight-Verbindungsprotokoll verfügbaren Informationen. Die folgende Abfrage erstellt eine nach Host organisierte Tabelle, die die abgehenden und antwortenden Bytes sowie einen PCR-Wert enthält.

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

Beschränkungen der Datenübertragung

Ein Angreifer kann versuchen, Daten oder Dateien zu übertragen, indem er sie in kleinere Teile zerlegt, um hartcodierte Datenübertragungsgrenzen oder -schwellenwerte zu umgehen. Wir stellen zwei Methoden vor, um diese Technik zu erkennen.

Die erste Methode analysiert die Daten, die das Netzwerk verlassen, auf der Grundlage von Quell- und Zielpaaren und erfordert eine Aggregations-/Visualisierungsplattform von Daten (es sei denn, Sie nutzen gerne awk und grep, um Daten zu untersuchen):

1. Erstellen Sie eine Tabelle aus dem Verbindungsprotokoll mit den Angaben „id.orig_h“, „id.resp_h“, „id.resp_p“ und „sum(orig_bytes)“.
2. Sortieren Sie die Ergebnisse nach dem größten „sum(orig_bytes)“-Wert.
3. Überprüfen Sie jeden Host und stellen Sie fest, ob es einen legitimen Grund für Uploads zu diesem Ziel gibt.

Die zweite Methode analysiert die Häufigkeit und den Umfang der ausgehenden Übertragungen von jeder Quelle:

1. Erstellen Sie eine Tabelle aus dem Verbindungsprotokoll mit den Angaben „id.orig_h“, „id.resp_h“, „id.resp_p“ und „count(orig_bytes)“.
2. Sortieren Sie die Ergebnisse nach dem größten „count(orig_bytes)“-Wert.

3. Untersuchen Sie die Ergebnisse und ermitteln Sie den Grund für alle Verbindungen mit der gleichen Datenmenge, die von der Quelle zum Ziel fließen.

[1] https://attack.mitre.org/
[2] Wenn die IP als Informationsindikator verwendet wird, gilt sie als anfällig, da die Angreifer leicht zu einem neuen Host oder Provider wechseln können.
[3] Nicht alle Versionen von RDP geben den Benutzernamen im Feld „cookie“ an. Einige machen keine Angaben oder weisen Unstimmigkeiten auf. In diesen Fällen müssen Sie ihn aus dem NTLM- oder Kerberos-Protokoll ableiten.
[4] https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/
[5] Besuchen Sie https://packages.zeek.org/ für nähere Informationen zu Zeek-Paketen.

Sicherheitsteams haben schon immer die Höhe gesucht, um weiter sehen und Angriffe vorausschauend abwehren zu können. Corelight bietet einen umfassenden Überblick über Ihr Netzwerk, sodass Sie Angreifer überlisten und überdauern können. Wir erfassen, interpretieren und verknüpfen die Daten, die für Sicherheitsteams relevant sind.

info@corelight.com | 888 547 9497