

Guide de «Threat Hunting»

Introduction

- Qu'est-ce que le «Threat Hunting» ?
- Pourquoi faire du «Threat Hunting» ?
- Pourquoi utiliser les données du réseau ?
- Nomenclature des logs Corelight
- Identification des utilisateurs et des appareils

Accès initial

- Menace furtive
- Services distants externes
- Pièce jointe de harponnage
- Lien de harponnage

Exécution

- Interface en ligne de commande, PowerShell

Persistance

- Tâches du BITS
- Services distants externes
- Port Knocking (tocage à la porte)
- Composant logiciel de serveur : shell web (code encoquillé)

Contournement des défenses

- Tâches du BITS
- Port Knocking (tocage à la porte)
- Installation d'un certificat racine

Accès aux identifiants

- Attaque en force
- Authentification forcée
- Reniflage réseau

Découverte

- Analyse de service réseau
- Découverte de partage réseau
- Reniflage réseau (référence X)
- Découverte de système à distance

Mouvement latéral

- Protocole RDP
- Services distants
- Partages administratifs Windows

Collecte

- Archivage de données collectées
- Collecte automatisée
- Données de lecteur réseau partagé

Commande et contrôle

- Ports couramment utilisés/Ports non standard
- Chaîne cryptée
- Canaux de secours, canaux à étages multiples
- Transfert d'outil d'entrée
- Protocole de couche non applicative
- Ports non standard
- Proxy
- Service web

Exfiltration

- Exfiltration automatisée
- Limitation de la taille pour transférer des données

Introduction

Ce Guide de chasse aux menaces (ou « Threat Hunting ») a été créé pour vous apprendre à détecter des attaques avant qu'elles ne se produisent en utilisant les données des sondes Corelight. Ce document (fondé sur la matrice MITRE ATT&CK®) est conçu pour vous aider à développer une théorie de «Threat Hunting» et établir vos priorités.

MITRE ATT&CK est une base de connaissances des tactiques et techniques adverses recueillies à partir d'observations réelles et accessible dans le monde entier. Elle est utilisée comme base pour des modèles et des méthodologies de menaces spécifiques dans le secteur privé, les institutions gouvernementales et le secteur de la cybersécurité. Grâce à ATT&CK, MITRE remplit sa mission de résoudre les problèmes pour parvenir à un monde plus sûr en rapprochant les communautés pour développer une cybersécurité plus efficace. ATT&CK est ouvert et disponible gratuitement pour toute personne ou entreprise qui souhaite l'utiliser¹.

Qu'est-ce que le «Threat Hunting» ?

À un niveau élevé, le «Threat Hunting» consiste à chercher activement des adversaires dans son réseau *sans savoir s'ils y ont pénétré*. C'est une pratique différente de celle basée sur la correspondance d'indicateurs, qui ne surveille que les signes bien connus d'attaquants, par exemple, les adresses IP ou le hachage de fichier. En général, le «Threat Hunting» implique de rechercher une théorie ou de suivre une intuition puis d'analyser des données en cherchant quelque chose d'*intéressant*. Les éléments *intéressants* peuvent se présenter sous de nombreuses formes. Par exemple, dans *Le Nid du coucou* de Clifford Stoll, c'est une erreur comptable qui a déclenché la chasse.

« Dave est entré dans mon bureau, en marmonnant quelque chose à propos d'un hic dans le système de comptabilité Unix. Quelqu'un a dû utiliser l'ordinateur pendant quelques secondes sans payer. Les registres de l'ordinateur n'étaient pas tout à fait cohérents ; les factures de 2387 \$ du mois dernier présentaient un déficit de 75 centimes. »

C'est cet écart de 75 centimes qui a permis de découvrir que les systèmes de plusieurs entreprises et gouvernements étaient compromis. Le terme « intéressant » est utilisé tout au long du guide et c'est vous qui en fixez les limites.

Pourquoi faire du «Threat Hunting» ?

La plupart des systèmes de détection basés sur l'hôte ou le réseau s'appuient sur la correspondance, également appelée détection par signatures, pour générer des alertes afin de signaler au défenseur la présence de quelque chose d'indésirable dans le réseau. Mais les attaquants évoluent en permanence pour échapper à la détection, et les signatures ne sont développées qu'après que l'artefact ait été découvert dans un autre réseau. Alors, si vous ne cherchez pas activement les artefacts qui menacent votre environnement, comment allez-vous découvrir que des attaquants contournent vos défenses ?

Guide de «Threat Hunting»

Le «Threat Hunting» présente plusieurs avantages. Le premier est que vous pouvez trouver des traces laissées par un intrus actif qui n'ont pas été détectées par vos défenses actuelles. Certains penseront que c'est catastrophique, mais cela peut être une grande victoire, surtout si l'intrus n'a pas atteint son objectif. Il y a toujours *quelque chose* à trouver dans des exercices de «Threat Hunting».

Vous pouvez identifier des problèmes de configuration dans votre réseau ou les logiciels qui peuvent constituer une menace, que ce soit parce qu'ils diminuent le rendement du réseau ou parce qu'ils comportent des vulnérabilités. Ensuite, la chasse peut permettre de détecter des infections ordinaires comme des adwares ou d'autres malwares dormants qui ne visent pas directement votre entreprise, mais qui restent une menace. Enfin, l'abus des ressources et des pratiques de «shadow IT» ou informatique parallèle, des services qui ne sont pas officiellement pris en charge peuvent comporter des risques en raison de la diminution de la performance de réseau ou de l'existence de vecteurs d'attaque. Chaque chasse vous apprend quelque chose sur le réseau qui vous sera utile pour la suite.

Pourquoi utiliser les données de réseau ?

Les paquets ne mentent pas

C'est aussi simple que ça. Si un intrus résidant dans le réseau est actif sur votre réseau, il y laissera des traces. Les traces donnent des indices de ce qu'il se passe ou, mieux encore, permettent de savoir exactement ce qu'il s'est passé, pas à pas. Par exemple, si un canal de commande et contrôle (C2) utilise un DNS comme mécanisme de transport, il y aura des requêtes et des réponses DNS. En outre, les adresses IP qui se trouvent aux extrémités de la connexion TCP doivent être correctes, elles ne peuvent pas être usurpées s'il y a un échange d'informations. Toutes les attaques traversent le réseau, à moins qu'elles ne soient isolées sur un seul hôte, il existera donc des paquets.

Nomenclature de logs Corelight

Corelight fournit des solutions centrées sur les données, qui analysent le trafic du réseau et améliorent les outils d'automatisation en transformant le trafic du réseau en logs liés et en procédant à l'extraction de fichiers. Le log central est le log conn (connexion), qui rassemble des informations générales sur toutes les sessions du réseau.

Le log conn enregistre des informations sur chaque point de terminaison du réseau et le service (application), et attribue également un uid (identifiant unique). L'identifiant unique (uid) relie le log conn aux logs de protocole associés, où des informations de session spécifiques sont disponibles. Par exemple, le log conn peut répertorier le protocole http en tant que service et en utilisant l'identifiant unique, vous pouvez basculer vers le log http pour obtenir des informations de protocole spécifiques sur la session. L'identifiant unique sépare les solutions Corelight des autres outils de sécurité. Ce champ met en lien des informations qui seraient sinon disparates dans des logs facilement assimilables. L'uid est fondamental pour effectuer une analyse des liens et un champ d'une importance critique qui permet de faire pivoter ou de relier plusieurs logs ensemble.

Guide de «Threat Hunting»

Field	Value
@metdata.ip_address	208.90.215.182
@timestamp	February 8th 2018, 17:29:32.610
@version	1
_id	3hkueGEBUJcpRQ0v58k2
_index	cl-conn-2018.02.09
_score	1
_type	bro
_write_ts	2018-02-09T01:27:37.610Z
conn_state	RSTO
duration	a few seconds
history	5x40tR
host	208.90.215.182
id.orig_h	192.168.0.53
id.orig_p	2,210
id.resp_h	68.164.182.11
id.resp_p	80
local_orig	true
local_resp	false
missed_bytes	0
orig_bytes	8168
orig_ip_bytes	9,772
orig_ip_addr	00:60:6e:00:19d:f9
orig_pkts	212
path	conn
port	42,242
proto	tcp
resp_bytes	513,634
resp_cc	US
resp_ip_bytes	528,482
resp_ip_addr	78:54:2e:9f:10:28
resp_pkts	371
sensor	HQ
service	http
ts	February 8th 2018, 17:27:32.610
tunnel_parents	
t_type	bro
t_uid	CSeT6u3087GrhJWWS

Field	Value
@metdata.ip_address	208.90.215.182
@timestamp	February 8th 2018, 17:28:59.882
@version	1
_id	txqueGEBUJcpRQ0vDhb8
_index	cl-http-2018.02.09
_score	1
_type	bro
_write_ts	2018-02-09T01:27:32.622916Z
host	www.mybusinessdoc.com
id.orig_h	192.168.0.53
id.orig_p	2,210
id.resp_h	68.164.182.11
id.resp_p	80
method	GET
path	http
port	42,312
request_body_len	0
resp_filenames	551d88323f7e.gif
resp_fuids	Fv8xAo1XFK6XdV5g
resp_mime_types	application/x-dosexec
response_body_len	192,512
sensor	HQ
status_code	200
status_msg	OK
tags	
trans_depth	2
ts	February 8th 2018, 17:27:32.610
t_type	bro
t_uid	CSeT6u3087GrhJWWS
t_uri	/document.php?rnd=52926id=555525E611600
user_agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows
version	1.1

Field	Value
@metdata.ip_address	208.90.215.182
@timestamp	February 8th 2018, 17:28:39.603
@version	1
_id	phYteGEBUJcpRQ0v47G
_index	cl-files-2018.02.09
_score	1
_type	bro
_write_ts	2018-02-09T01:27:32.622916Z
analyzers	MDS, PE, SHA256, SHA1
conn_uids	CSeT6u3087GrhJWWS
depth	0
duration	a few seconds
filename	551d88323f7e.gif
fuid	Fv8xAo1XFK6XdV5g
host	208.90.215.182
ix_orig	false
local_orig	false
md5	634c2a2a3ab03d5c21738c62d4677fe8
mime_type	application/x-dosexec
missing_bytes	0
overflow_bytes	0
path	files
port	42,288
rx_hosts	192.168.0.53
seen_bytes	192,512
sensor	HQ
sha1	a0a1911fe2ff864e7d181bb7750b60b74033c3b1
sha256	196c186b05ce2cb0f964080823d22a5f4c999e3270fd3b475068c5130dc7fd50
source	HTTP
timeout	false
total_bytes	192,512
ts	February 8th 2018, 17:27:32.610
tx_hosts	68.164.182.11
t_type	bro

Les informations relatives à chaque point de terminaison du réseau sont résumées par le champ id, qui est généralement représenté par quatre champs distincts :

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

Cette nomenclature peut sembler étrange à l'utilisateur, car le personnel en charge des réseaux se réfère généralement aux sessions en utilisant le client et le serveur ; cependant, l'utilisation de orig (*originator* ou expéditeur) et resp (*responder* ou destinataire) permet au personnel de sécurité de décrire avec précision la connexion. Considérez que l'hôte d'origine (orig_h) est la source, ou le client, et l'hôte répondant (resp_h) est la destination ou le serveur. Les champs id.orig_p et id.resp_p seront renseignés avec les numéros de port correspondants.

La plupart des autres champs du log conn et des autres logs de protocole sont autodéscriptifs, mais si vous avez des doutes, vous pouvez consulter la documentation Zeek sur <https://docs.zeek.org/en/current/> (en anglais) pour obtenir des informations plus détaillées ou faire un tour sur le canal Slack de la communauté Corelight sur <http://corelightcommunity.slack.com/> (en anglais).

Identification des utilisateurs et des appareils

Au moment d'identifier un appareil sur un réseau, les adresses IP ou MAC sont souvent utilisées pour créer « l'identité ». L'adresse IP de l'appareil est plus généralement utilisée pour l'identité distante, périphérique, car elle survit au-delà des limites du routeur. Alors qu'à l'intérieur d'un segment de réseau, l'adresse MAC est privilégiée pour l'identification, car elle peut constituer un identifiant fiable d'une machine spécifique. Chaque identifiant a ses avantages et ses inconvénients, et la capacité de

Guide de «Threat Hunting»

Corelight à capturer les deux identifiants permet d'aider le personnel chargé de la sécurité opérationnelle lorsqu'il analyse des événements.

Les adresses IP sont fiables² pour les analyses internes, mais elles sont souvent transitoires au sein d'un réseau, car la plupart des réseaux utilisent le protocole DHCP (*Dynamic Host Configuration Protocol*). Les adresses IP transitoires sont problématiques pour les défenseurs lorsque l'alerte IDS identifie la session au moyen d'adresses IP. Ces adresses IP sont uniquement associées à l'alerte *au moment où l'alerte a été générée*.

Vous pouvez utiliser des outils open source lorsque vous menez une analyse (par exemple, nslookup), pour fournir des informations DNS pour les adresses IP distantes. Cependant, il s'agit d'une information ponctuelle disponible *au moment de l'analyse, et non au moment où l'événement s'est produit*. Une meilleure technique consiste à utiliser les logs créés au moment de l'alerte pour capturer l'adresse IP et le FQDN (*fully qualified domain name* ou nom de domaine totalement qualifié) de l'appareil distant. Pour localiser un appareil interne, vous pouvez extraire les logs DHCP pour l'identifier. Il existe plusieurs façons d'identifier un hôte et Corelight fournit ces données dans plusieurs logs qui racontent chacun un aspect différent de l'histoire. Faites preuve de créativité et suivez chaque piste.

Voici où trouver les noms d'hôtes :

- **dhcp.log** : les champs `host_name` et `domain` correspondent au nom d'hôte et au domaine indiqués par un hôte lors d'une requête d'adresse IP via DHCP, et le champ `assign_addr` est l'adresse IP qui a été attribuée à cet hôte.
- **dns.log** : s'il existe une adresse IP dans le champ de réponses, le champ de requête contiendra le nom d'hôte que le serveur DNS a enregistré (à ce moment-là) pour l'adresse IP.
- **ntlm.log** : les champs `server_dns_computer_name` et `server_nb_computer_name` font référence aux noms DNS et NetBIOS de la machine avec l'adresse IP dans le champ `id.resp_h`. Le champ `hostname` correspond au nom d'hôte de la machine avec l'adresse IP dans le champ `id.orig_h`.
- **kerberos.log** : dans un environnement Windows, pour les appareils joints au domaine, les requêtes Kerberos dans lesquelles le champ `client` contient un nom se terminant par \$, le champ `client` est le nom d'hôte et le champ `id.orig_h` est l'adresse IP de cet hôte. Le champ `client` est souvent structuré sous la forme `HOSTNAME$/EXAMPLEDOMAIN.COM`, où `HOSTNAME` est le nom d'hôte et `EXAMPLEDOMAIN.COM` est le nom de domaine Windows et le nom de domaine Kerberos.
- **http.log** : le champ `host` contient le nom d'hôte, le nom de domaine ou l'adresse IP du client qui a effectué une requête de données au serveur HTTP. Parfois, ce champ est une indication de l'identité du serveur, l'appareil dont l'adresse IP figure dans le champ `id.resp_h`.
- **ssl.log** : le champ `server_name` est extrait du champ Server Name Indication (SNI) dans la négociation TLS/SSL et il est utilisé de la même manière que le champ `host` du log `http`. De plus, le champ `objet` est extrait de l'objet du certificat du serveur, et la partie du nom canonique (CN) de l'objet peut fournir des indices pour identifier un serveur.

Guide de «Threat Hunting»

Lors de l'identification des utilisateurs, plusieurs logs fournissent des informations précieuses :

- **rdp.log** : en fonction de la version du protocole RDP, la valeur du champ cookie est le nom d'utilisateur déclaré par le client, et l'IP du client figure dans le champ id.orig_h.³
- **irc.log** : le champ user contient le nom d'utilisateur déclaré par le client et l'adresse IP du client apparaîtra dans le champ id.orig_h.
- **irc.log** : le champ user contient le nom d'utilisateur déclaré par le client et l'adresse IP du client apparaîtra dans le champ id.orig_h.
- **socks log** : le champ user contient le nom d'utilisateur déclaré par le client et l'adresse IP du client apparaîtra dans le champ id.orig_h.
- **http.log** : le champ user contient le nom d'utilisateur déclaré par le client et l'adresse IP du client apparaîtra dans le champ id.orig_h, ou il peut être indiqué dans le champ proxy si la connexion est de type proxy. En cas de connexion proxy, le champ id.orig_h contiendra l'adresse IP du proxy.
- **ntlm.log** : le champ user contient le nom d'utilisateur déclaré par le client et l'adresse IP du client apparaîtra dans le champ id.orig_h.
- **kerberos.log** : dans un environnement Windows, les requêtes Kerberos contiennent le nom d'utilisateur dans le champ client (sauf pour les requêtes où le champ client contient un nom se terminant par \$, ce qui signifie que l'identité déclarante est un appareil, et le champ id.orig_h correspond à l'adresse IP de l'appareil source. Le champ client est souvent structuré sous la forme USERNAME/EXAMPLEDOMAIN.COM, où USERNAME est le nom d'utilisateur et EXAMPLEDOMAIN.COM est le nom de domaine Windows et le nom de domaine Kerberos.

Quelques précautions à prendre avant de tirer des conclusions sur l'identité d'une machine ou de l'utilisateur d'un appareil : connaissez vos limites (et les limites des données). Ce n'est pas parce qu'un nom d'utilisateur a été enregistré dans le trafic du réseau que la personne réelle avec ce nom est responsable, c'est juste un indice. Vous devez vérifier si l'utilisateur s'est correctement identifié, car les cyber espions et ceux derrière lequel se trouve un état, sont de plus en plus expérimentés et utilisent un autre stratagème : planter de faux drapeaux.⁴ Le nom d'utilisateur peut avoir été *déclaré*, mais si l'authentification a échoué, cela n'indique pas clairement que l'utilisateur était impliqué. N'oubliez pas que les appareils et les logiciels peuvent mettre en cache les identifiants, de sorte que le compte de l'utilisateur peut être actif, mais la personne réelle toujours innocente. Vous devez continuer à collecter des informations avant de pouvoir confirmer un comportement malveillant.

Par exemple :

- Un utilisateur va déjeuner et ne verrouille pas son appareil
- Un appareil est compromis par un cheval de Troie d'accès distant (RAT, *Remote Access Trojan*) et un utilisateur à l'autre bout du monde assume subrepticement l'identité de notre victime, *tandis que l'utilisateur d'origine utilise simultanément l'appareil pour réaliser des activités régulières*
- Un utilisateur malveillant au sein de l'organisation a entendu un collègue dire son mot de passe à haute voix au cours d'une conversation, et il essaie maintenant d'utiliser ces identifiants pour se connecter à d'autres systèmes

Guide de «Threat Hunting»

Assurez-vous également de bien comprendre quels éléments d'information sont contrôlés et déclarés par les clients ou les serveurs, et déterminez qui contrôle chacun d'eux. Si un adversaire se trouve à l'intérieur de votre réseau, il est primordial de déterminer quelles informations sont dignes de confiance lors de la préparation du plan de réponse. Par exemple, un intrus pourrait désactiver le protocole DHCP et assigner une adresse IP de manière statique et l'utiliser pour naviguer sur le réseau, ce qui rendra l'identification difficile, car les enregistrements du serveur DHCP fourniraient des informations contradictoires. De plus, lorsqu'un client effectue une requête d'adresse DHCP, un intrus peut fournir une fausse adresse MAC. D'où l'importance de capturer des logs passifs ponctuels lorsque l'événement s'est produit.

Comment traquer certaines tactiques, techniques et procédures

Accès initial

L'accès initial correspond au moment où les intrus établissent leur point d'ancrage initial.

Menace furtive

Une menace furtive se produit généralement lorsqu'un fichier est téléchargé subrepticement à partir d'un site web compromis. Lorsque vous recherchez des signes de menace furtive dans les données Corelight, vous devez vous centrer sur les téléchargements à partir de sites web externes.

Commencez la traque dans le log http et recherchez des signes d'exécutables téléchargés :

1. Commencez par les logs http dans lesquels resp_fuids n'est pas vide. Cela signifie qu'un fichier a été renvoyé par le destinataire.
2. Si le volume de données est trop important, filtrez les destinataires locaux (dans le réseau). Vous pouvez filtrer en associant les résultats au log conn sur l'identifiant unique (iud), puis en filtrant tous les enregistrements dans lesquels la valeur de local_resp est « true » dans le log conn.
3. Examinez les resp_mime_types du log http et filtrez les résultats inintéressants (par exemple, images, texte, réponses OCSP et certificats). Les résultats les plus intéressants sont souvent les exécutables, les dll et les archives/conteneurs.
4. Regroupez les résultats en fonction des champs host et resp_mime_types pour faciliter l'analyse.

Examinez les résultats et recherchez tout ce qui semble intéressant ou étrange, par exemple les téléchargements de fichiers exécutables, ou une extension de fichier et une incompatibilité de type MIME.

De plus en plus d'attaquants utilisent le protocole TLS pour crypter les échanges entre les clients qu'ils menacent et les sites web qu'ils contrôlent, ce qui réduit la visibilité via le log http. Pour récupérer cette visibilité, envisagez d'utiliser une solution de déchiffrement SSL d'entreprise et de transmettre le trafic HTTP déchiffré à votre sonde Corelight.

Services distants externes

Les services distants externes sont utilisés par les adversaires pour se connecter aux ressources du réseau interne, et la recherche d'une mauvaise utilisation des services distants s'effectue généralement en deux étapes : la découverte et l'analyse. Tout d'abord, vous devez découvrir quels sont les services distants utilisés. Vous devez commencer par collecter les informations sur l'inventaire des services et des éléments, mais cela est généralement insuffisant. Il se produit souvent une « dérive » naturelle lorsque les équipes informatiques apportent des modifications à l'infrastructure et luttent pour maintenir à jour la documentation sur tous les éléments. Les utilisateurs habilités rendent la tâche encore plus difficile lorsqu'ils installent des éléments et des services sans faire appel au service informatique ou sans l'informer, un processus connu sous le nom de « shadow IT » ou informatique parallèle.

Les services distants traditionnels, par exemple, RDP, VNC (protocole Remote Frame Buffer) et SSH (protocole Secure Shell) contiennent un composant serveur et un composant client. Si un service distant est hébergé dans votre environnement, les attaquants peuvent l'exploiter en externe pour compromettre les machines à l'intérieur du réseau. Pour identifier ces services, recherchez les entrées du log conn dans lesquelles le champ service contient rfb, rdp ou ssh, et où la valeur de local_orig est « false » et celle de local_resp est « true », ou dans lesquelles l'adresse IP de l'expéditeur (id.orig_h) est externe et l'adresse IP du destinataire (id.resp_h) appartient au réseau de l'organisation. Notez tous les serveurs RFP/VNC, RDP ou SSH qui acceptent les connexions depuis Internet.

Certains services distants fonctionnent à l'inverse, lorsqu'un agent est installé sur l'appareil local et atteint l'*extérieur* depuis l'intérieur du réseau vers un ensemble de serveurs externes, par exemple, GoToMyPC et TeamViewer. Cette configuration est conçue pour aider les utilisateurs (principalement les utilisateurs domestiques) qui ne contrôlent pas les règles de NAT ou le pare-feu ou qui ne sont pas assez expérimentés pour gérer la redirection de port ou les règles de pare-feu.

Pour savoir si ces services distants sont utilisés dans votre environnement, recherchez des signes de connexions sortantes vers ces services. Par exemple, TeamViewer utilise le port TCP 5938 pour communiquer avec les serveurs TeamViewer, il suffit donc de consulter les logs conn pour vérifier les connexions où id.resp_p indique 5938 et local_orig est « true » et local_resp est « false ». TeamViewer utilise également SSL, et le nom de domaine des connexions est normalement *.teamviewer.com, vous pouvez donc rechercher les entrées dans le log SSL, dans lesquelles server_name contient, ou mieux encore, se termine par « teamviewer.com ». (Remarque : comme cette session fonctionne à l'inverse, id.orig_h est l'appareil de votre réseau sur lequel le client TeamViewer est installé.) Dans notre deuxième exemple, GoToMyPC tente de contacter poll.gotomypc.com. Examinez le champ host du log http et recherchez poll.gotomypc.com ou les entrées du log SSL dans lesquelles server_name est poll.gotomypc.com. La liste des ports et des noms de domaine varie en fonction de chaque progiciel client.

Après cette première étape de découverte des services distants, vous devez ensuite comparer les données Corelight avec une liste de tous les services distants proposés par le service informatique, tels que :

Guide de «Threat Hunting»

- Passerelles RDP (protocole d'accès à distance)
- Passerelles VDI (infrastructure de postes de travail virtuels)
- Passerelles VPN (réseau privé virtuel)
- Serveurs SSH

Pour chaque service exposé à Internet, établissez une liste des connexions à ce service à partir du log conn et incluez les champs suivants :

- id.orig_h : adresse IP d'origine (client)
- id.resp_h : adresse IP du destinataire (serveur)
- id.resp_p : port de réponse
- service : le protocole d'application détecté par Zeek
- history : l'historique de la connexion, par exemple les types de drapeaux TCP qui ont été vus
- orig_cc : le code pays de l'expéditeur

Lorsque vous filtrez les logs, assurez-vous que le champ history commence par « Sh ». Pour les connexions TCP, cela signifie que l'expéditeur a envoyé un SYN et que le destinataire a répondu par un SYN/ACK (mécanisme de poignée de main). Cette vérification élimine les connexions où le serveur n'est pas à l'écoute ou les cas où un pare-feu bloque la connexion.

Après avoir rassemblé toutes les données, commencez à passer au crible les logs pour rechercher tout ce qui est intéressant, par exemple une connexion depuis un pays inattendu. Utilisez l'identifiant unique du log conn pour effectuer un suivi avec les logs Zeek spécifiques à l'application (rdp, rfb, ssh). Par exemple, le log rdp contient plus de détails sur la connexion, tels que le champ cookie qui peut contenir le nom d'utilisateur de l'utilisateur qui s'authentifie. La dernière étape consiste à vérifier auprès de l'utilisateur s'il utilisait activement le système à ce moment-là.

Les clients de Corelight ont accès à la collection Encrypted Traffic Collection (ETC - trafic chiffré), qui génère des inférences ou des connaissances sur le trafic chiffré. Le log ssh contient des informations intéressantes déduites de la connexion SSH, telles que :

- KS pour les connexions qui semblent contenir des saisies au clavier (*keystroke*)
- FU et FD pour les connexions qui semblent contenir respectivement un chargement (*upload*) ou un téléchargement (*download*) de fichier
- ABP pour les connexions qui semblent ne contenir aucune authentification, mais qui malgré tout réussissent (*authentication bypass*)
- SV ou SC pour les clients qui semblent être une analyse de version (*version scanning*) ou de capacité (*capability scanning*)

Si vous voulez en savoir plus sur la collection ETC de Corelight, contactez notre équipe commerciale au (510) 281-0760

Guide de «Threat Hunting»

Pièce jointe de harponnage

Une des méthodes d'entrée dans une organisation consiste à envoyer une pièce jointe malveillante bien réalisée à un individu ou à un petit groupe dans le cadre d'une campagne de harponnage. La pièce jointe peut être un document qui demande à l'utilisateur d'effectuer une action, par exemple cliquer sur un lien et/ou se connecter à un portail ; ou il peut s'agir d'un fichier conçu pour exploiter une vulnérabilité dans le logiciel utilisé pour l'ouvrir, par exemple Adobe Acrobat ou Microsoft Word.

Le log smtp de Corelight contient des enregistrements dans le champ fuids en cas d'existence de fichiers joints à un message transmis via SMTP. Ce champ peut être utilisé pour basculer vers le log files (fichiers) qui contient des informations détaillées sur le fichier, notamment le nom du fichier, les hachages et la source. Par exemple :

```
path: smtp
from: Votre ami <Jeremy.Rigueur@gmail.com>
fuids: [ Fh5GBc1wdVp3x9MKxc ]
mailfrom: attaquant@fake-mail.com
rcptto: [ victime@corp-mail.com ]
subject: Ceci n'est pas du harponnage
to: [ victime@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
```

Pour traquer d'éventuelles tentatives de harponnage, vous pouvez rechercher dans le log files (fichiers) :

1. La valeur dans le champ source est SMTP.
2. Filtrez toutes les valeurs mime_type et/ou filename sans intérêt, comme mentionné précédemment.
3. Utilisez le hachage (MD5, SHA1 ou SHA256) avec un service de réputation de fichiers (tel que Virustotal) pour rechercher les fichiers malveillants connus.

Vous pouvez également commencer à partir du journal smtp :

1. Pour réduire les données, recherchez les entrées où le champ fuids n'est pas vide.
2. Filtrez les combinaisons correctes connues pour les valeurs mailfrom et from.
3. Filtrez les valeurs subject sans intérêt.

Guide de «Threat Hunting»

4. Pensez à utiliser la valeur fuid des enregistrements restants pour basculer vers le log files pour obtenir plus d'informations sur le fichier.

Corelight peut réaliser une extraction de fichiers à grande vitesse et filtrer en fonction du type MIME, de sorte que tous les fichiers sans intérêt, tels que les exécutables, les documents Office et les PDF, sont disponibles pour réaliser un examen plus approfondi si vous le souhaitez.

Une grande partie des mails qui circulent sur Internet sont aujourd'hui cryptés via STARTTLS avec le protocole SMTP, ce qui nuit à la visibilité. Pour obtenir une meilleure visibilité sans sacrifier la confidentialité et la sécurité de vos utilisateurs, il est recommandé d'accepter le SMTP entrant sur un système prenant en charge STARTTLS, puis de transférer le mail vers le système de messagerie interne, afin que Corelight puisse générer les logs correspondants.

Lien de harponnage

Au lieu d'envoyer des fichiers dans une organisation où ils peuvent être examinés par un filtre de messagerie d'entreprise, certains adversaires envoient des e-mails qui ne contiennent que des liens. Ces liens mènent à des sites web contrôlés par l'attaquant et tentent de duper l'utilisateur en :

- Introduisant des identifiants collectés par les attaquants
- Exploitant une vulnérabilité dans le navigateur de l'utilisateur
- Téléchargeant un fichier pour exploiter une autre application sur l'appareil de l'utilisateur

Corelight Sensors est doté d'un package⁵ qui peut enregistrer les liens des messages SMTP dans un log séparé, le log smtp_links. Ce journal contient un champ fuid qui associe le log smtp_links au log smtp. Vous pouvez rapidement basculer vers le log smtp contenant les détails du message envoyé par le lien malveillant.

Par exemple :

```
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: Votre ami <Jeremy.Rigueur@gmail.com>
fuids: [ FhahXA1ej32gHvNP27 ]
mailfrom: attaquant@fake-mail.com
rcptto: [ victime@corp-mail.com ]
subject: Veuillez cliquer sur ce lien
```

Guide de «Threat Hunting»

to: [victime@corp-mail.com]
uid: C62txO1FHojFJpsgP1
user_agent: Apple Mail (2.3608.80.23.2.2)

Pour rechercher les liens de harponnage, commencez par le journal smtp_links et examinez le champ link, en filtrant les domaines bénins jusqu'à trouver des résultats intéressants. Une autre option consiste à associer le log smtp_links au log smtp via le champ fuids ou le champ uid, et à filtrer les combinaisons bénignes des champs mailfrom et from, pour rechercher les messages provenant d'expéditeurs uniques.

Sachant qu'une grande partie des mails qui circulent sur Internet sont aujourd'hui cryptés via STARTTLS avec le protocole SMTP. Pour obtenir une meilleure visibilité sans sacrifier la confidentialité et la sécurité de vos utilisateurs, il est recommandé d'accepter le SMTP entrant sur un système prenant en charge STARTTLS, puis de transférer le mail vers le système de messagerie interne, afin que la solution Corelight puisse générer les logs correspondants.

Exécution

L'adversaire essaie d'exécuter un code malveillant.

Interface en ligne de commande, PowerShell

Les scripts d'interface en ligne de commande ont longtemps été utilisés pour gérer les systèmes basés sur *nix, et la capacité de créer et d'exécuter des scripts est souvent exploitée par les attaquants. Pendant des années, aucun équivalent n'était disponible sur Windows, mais au début des années 2000, Microsoft a commencé à développer une nouvelle approche de gestion de la ligne de commande. Peu de temps après, PowerShell (PS) 1.0 a été créé. PowerShell ou PS, dans ses différentes itérations, est un outil intégré basé sur le .NET Framework, qui est utilisé pour automatiser les tâches d'administration du système. Il fournit une interface permettant aux utilisateurs d'accéder aux services du système d'exploitation Windows.

Bien que certaines commandes PS soient restreintes par défaut, de nombreuses commandes sont disponibles pour obtenir des informations sur le système sans fichier exécutable. Vous pouvez utiliser les extensions LNK pour contourner les sauvegardes et exécuter un script PS. Les fichiers LNK sont généralement considérés comme des raccourcis, et ils se trouvent en principe sur le bureau de l'utilisateur et dans le menu Démarrer.

Les fichiers LNK malveillants sont souvent intégrés dans des documents ou des images apparemment légitimes. Une fois ouvert, le LNK exécute une application Windows légitime, CMD.exe ou MSHTA.exe, pour contourner les paramètres de sécurité.

Grâce à ses capacités d'extraction de fichiers et son intégration à diverses plateformes Intel, Corelight fournit un aperçu des logiciels malveillants masqués par type de fichier. Le système de filtrage intégré de Corelight vous permet d'ajuster les paramètres d'extraction de fichiers pour cibler des types MIME spécifiques couramment utilisés pour diffuser des logiciels malveillants, notamment :

Guide de «Threat Hunting»

- Fichiers compressés
- Microsoft Office (Word, PowerPoint, etc.)
- Fichiers PDF
- Fichiers TXT (PowerShell, vbs)

Persistance

On parle de persistance lorsque l'adversaire tente de maintenir son emprise.

Tâches du BITS

Microsoft Background Intelligent Transfer Service (BITS) est un système créé en 2001 pour gérer les transferts de fichiers en minimisant les perturbations pour l'utilisateur final. BITS est couramment utilisé pour télécharger les mises à jour Windows et autres mises à jour logicielles des principaux fournisseurs.

Les attaquants ont deux méthodes pour utiliser les BITS à des fins malveillantes :

- La plus courante consiste à créer une tâche de transfert BITS directement sur un hôte, permettant le téléchargement de charges utiles secondaires via un service Windows intégré qui contourne généralement les pare-feu et autres systèmes de sécurité.
- Une autre méthode consiste à exfiltrer les données via une tâche de chargement (*upload*) BITS. Pour réaliser les chargements, les adversaires doivent se connecter à un serveur IIS pour que BITS fonctionne correctement, mais ce n'est qu'un détail pour les auteurs de logiciels malveillants qui veulent miner un système.

Les transferts de données utilisant le service BITS peuvent être réalisés via HTTP, SSL et SMB. Lorsque BITS utilise le trafic HTTP, il existe une chaîne « User-Agent » distincte pour « Microsoft BITS/7.5 » (ou 7.8 pour les versions ultérieures). Malheureusement, il n'existe pas de caractéristiques permettant de distinguer si le trafic réseau BITS est réalisé via SSL ou SMB. Par conséquent, la présence du trafic réseau BITS n'est pas nécessairement suspecte, car elle est présente partout où les machines Windows sont connectées à Internet. Les analystes peuvent toujours utiliser les données Corelight pour évaluer si le trafic BITS est légitime, en analysant les systèmes distants utilisés pour les transferts de données BITS. S'ils se trouvent en dehors des CDN ou des réseaux des principaux fournisseurs de logiciels, tous les téléchargements BITS doivent être examinés jusqu'à ce qu'ils soient bénins, car ce cas d'utilisation est particulièrement rare chez les fournisseurs de logiciels légitimes.

Guide de «Threat Hunting»

L'exemple de code suivant est un log http qui montre à quoi ressemblent les données BITS si elles sont transmises via 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/20
18/05/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: */*
```

Services distants externes

- Voir [Accès initial : services distants externes](#)

Port Knocking (tocage à la porte)

Le *port knocking*, également connu sous le nom de tocage à la porte, est une technique utilisée pour atteindre un système distant permettant l'accès à un port fermé. Il s'agit généralement d'une séquence prédéfinie de connexions à d'autres ports (souvent fermés), parfois avec des drapeaux spéciaux au niveau du protocole, des chaînes de bannière de couche 7, etc.

Zeek résume chaque connexion TCP, UDP et ICMP dans le log conn. Ce log détaillé fournit des statistiques utiles sur les connexions. Les champs history, conn_state et network tuple (src/dest ip/port) fournissent les informations nécessaires pour visualiser le *port knocking*. Il est important de souligner qu'observer une pratique de *port knocking* sans indice supplémentaire peut être fastidieux, car il est facile de cacher des séquences intentionnelles de connexions au milieu du bruit d'un réseau conventionnel.

Composant logiciel de serveur : shell web

La technique du shell web ou encore appelée code encoquillé consiste l'implantation d'une interface système (shell) pour exécuter une commande. Il s'agit généralement d'une page web ou d'un extrait de code malveillant introduit dans un serveur web ou une application existant(e) pour fournir un accès non autorisé. Cet accès peut être une interface en ligne de commandes (CLI), un outil de gestion de fichiers ou d'accès à la base de données. Il s'agit d'une tactique courante, car le trafic malveillant se mélange au trafic bénin vers/ depuis le serveur web, et il peut être difficile de l'identifier via les signatures IDS, car les spécificités du shell web sont facilement modifiables.

Lorsqu'un shell web est exécuté, il le fait avec les autorisations d'utilisateur de logiciel du serveur web, qui doivent être limitées. Les attaquants utilisent les shells web pour tenter des attaques par élévation des privilèges en exploitant les vulnérabilités locales du système pour obtenir des privilèges de type root.

Détecter des shells web sur le réseau à l'aide de détections basées sur les signatures est relativement simple : les shells web ont des chemins de fichiers, des méthodes de communication ou d'autres comportements spécifiques, qui peuvent déclencher une alerte. Comme la plupart des indicateurs de compromissions (IoC) « atomiques », ils sont faciles à contourner, car ils identifient des comportements spécifiques qui peuvent facilement être modifiés. Dans la mesure du possible, vous devez compléter la détection des signatures par un programme de «Threat Hunting» pour trouver des comportements plus généraux caractéristiques d'une activité anormale.

Les shells web tentent de masquer les activités malveillantes dans le trafic HTTP ordinaire. Par conséquent, le log http est une excellente source de données pour examiner l'activité des shells web. Voici des exemples d'hypothèses de chasse prises en charge par les données HTTP de Corelight :

- Activité HTTP POST inhabituelle. Cela peut être aussi simple que des requêtes HTTP POST inattendues dans le champ method du log http, où les requêtes GET sont attendues (si le site concerné sert principalement du contenu).

Le trafic web « normal » se dirige vers une liste restreinte de pages ordinaires, avec une navigation via un lien hypertexte interne. Un shell web va directement à la page cachée et apparaît comme une requête HTTP sans page de référence. De plus, le trafic web affiche une variété d'adresses IP de requêtes, de chaînes user-agent, de JA3, etc. Un shell web peut présenter un groupe d'utilisateurs plus homogène.

- Débusquer les connexions suspectes provenant des sous-réseaux internes vers les serveurs DMZ et vice versa.

Ce type d'analyse de chasse et de détection d'anomalies est un moyen efficace d'identifier les activités malveillantes (ou suspectes), mais les réseaux modernes sont des lieux bruyants et chaotiques. Comme pour la plupart des chasses, vous devez savoir à quoi ressemblent les données « normales », afin de pouvoir les filtrer correctement.

(<https://github.com/nsacyber/Mitigating-Web-Shells>)

Contournement des défenses

Le contournement des défenses est une consiste utilisée par les adversaires pour éviter d'être détectés pendant qu'ils réalisent leurs activités malveillantes.

Tâches du BITS

- Voir [Persistence : tâches du BITS](#)

Port Knocking (tocage à la porte)

- Voir [Persistence : Port Knocking \(tocage à la porte\)](#)

Installation d'un certificat racine

Les certificats publics sont utilisés pour établir des communications TLS/SSL sécurisées. Les certificats racine sont utilisés pour identifier l'autorité de certification racine. Les certificats racine sont auto-signés et constituent une ancre de confiance pour la cryptographie à clé publique. Par exemple, si un certificat racine est installé, le système ou l'application fera confiance aux certificats de la chaîne de confiance de la racine. Bien qu'aucun périphérique au niveau du réseau (par exemple, les routeurs et les commutateurs) ne puisse afficher la chaîne de certificats installée sur un système client, le but de l'installation d'un certificat racine malveillant est de contourner la validation de confiance.

Grâce aux données de Corelight, vous pouvez observer tous les aspects de la session TLS/SSL en utilisant les logs ssl et x509. Ces deux logs permettent aux analystes d'identifier les certificats qui semblent suspects en :

1. Recherchant dans le log SSL toutes les entrées dans lesquelles le champ validation_status ne contient pas la valeur « ok ».
2. Examinant les enregistrements dans lesquels le champ validation_status contient un certificat auto-signé ou contient un certificat auto-signé dans la chaîne de certificats.
3. Examinant les champs subject et server_name pour déterminer l'organisation ou le site web susceptible de contrôler le serveur.
4. Filtrant les résultats pour obtenir ceux où des certificats auto-signés légitimes sont utilisés, comme dans les communications entre les appareils IoT (Internet des Objets) et l'infrastructure cloud de prise en charge.
5. En analysant l'adresse IP id.resp_h pour voir à quel système autonome la session appartient et s'il s'agit d'une organisation à système autonome raisonnable (telle que l'organisation qui coïncide avec les informations sur le serveur, ou un fournisseur d'hébergement cloud couramment utilisé).
6. Pour les connexions restantes, utilisez les valeurs de cert_chain_fuids pour basculer vers les certificats dans le log x509 et examinez les détails du certificat.

Centrez vos recherches sur la vérification de l'autorité de certification racine locale au point de terminaison.

Accès aux identifiants

Guide de «Threat Hunting»

L'accès aux identifiants se produit lorsque l'adversaire essaie de voler les noms de compte et les mots de passe.

Force brute

Avec cette technique d'attaque, un adversaire tente d'obtenir un accès non autorisé en devinant systématiquement le mot de passe d'un utilisateur à l'aide d'un mécanisme répétitif ou itératif. Parfois, une attaque par force brute provient d'une liste d'informations connues, ce qui augmente les chances de réussite.

Par exemple, si un attaquant tente de deviner le mot de passe d'un compte Active Directory, cela entraînera probablement de nombreuses connexions à un contrôleur de domaine sur le port LDAP (389 ou 636). Un attaquant qui tente de découvrir des URL d'API dans un système de commerce électronique génère beaucoup plus de connexions au serveur web que d'autres clients au cours d'une période similaire et crée plus de codes d'état HTTP dans la plage 400 et 500 (erreurs) par rapport aux autres clients.

Pour rechercher une attaque par force brute :

1. Dans le log conn, regroupez par id.orig_h, id.resp_h, id.resp_p, proto et (optionnellement) service.
2. Ajoutez un décompte pour le nombre d'opérations et triez par les décomptes les plus élevés.
3. Choisissez une période de temps qui a du sens, en fonction de la taille du réseau/ensemble de données, en commençant petit et en augmentant progressivement.
4. Filtrez les enregistrements qui sont manifestement autorisés, tels que les contacts répétés des systèmes de surveillance des performances du réseau ou des applications, des systèmes de gestion des vulnérabilités ou des applications commerciales.
5. Pour les enregistrements inconnus ou suspects, effectuez une recherche plus approfondie sur ce comportement. Par exemple, recherchez d'autres connexions provenant de l'adresse IP distante.
6. Pour les protocoles qui peuvent maintenir des connexions sur plusieurs transactions ou tentatives, recherchez des connexions prolongées. Ces connexions prolongées peuvent également indiquer un comportement répétitif.

Corelight Sensors inclut un script qui enregistre les connexions qui se maintiennent plus longtemps qu'un ensemble de seuils, à partir de dix minutes et jusqu'à trois jours. Si vous n'êtes pas client de Corelight, mais que vous utilisez Zeek en open source, ce script est disponible sur la [page Corelight GitHub](#).

Pour rechercher de longues connexions avec le package Long Connections installé :

1. Examinez le log notice.
2. Examinez les entrées qui contiennent la note « LongConnection::found, »
3. Examinez chaque ensemble de id.orig_h, id.resp_h et id.resp_p pour comprendre si ces appareils doivent avoir de longues connexions.

Pour rechercher de longues connexions sans que le package Long Connections soit installé :

1. Examinez le log conn.

Guide de «Threat Hunting»

2. Rassemblez une liste de toutes les connexions avec les champs suivants dans chaque cas : champs id.orig_h, id.resp_h, id.resp_p, proto, service et duration. Cela inclut uniquement les connexions qui se sont terminées, soit correctement, soit avec un délai d'attente. Les connexions en cours ne sont pas représentées dans les résultats.
3. Triez les résultats par durée, en commençant par les connexions les plus longues.
4. Examinez chaque résultat pour déterminer s'il s'agit d'un comportement légitime ou attendu.
5. Filtrez les comportements attendus et analysez en profondeur tout ce qui semble suspect.

Corelight vous propose également sa solution Encrypted Traffic Collection (ETC), qui recherche automatiquement les tentatives d'attaque par force brute des serveurs SSH au sein d'une même connexion pour deviner un mot de passe.

Authentification forcée

Certains protocoles procèdent automatiquement à une authentification lorsqu'un utilisateur accède à une ressource sans vérifier au préalable si la ressource à laquelle il accède est fiable. Par exemple, un attaquant peut intégrer une référence dans un document Microsoft Office vers un fichier hébergé sur un chemin UNC contrôlé par l'attaquant (\\nom du serveur\nom partagé\chemin\vers\fichier). Lorsque l'utilisateur ouvre le fichier, la machine tente d'accéder à la ressource. Le serveur contrôlé par l'attaquant force ensuite la machine à s'authentifier, dans la plupart des cas, la machine victime fournit automatiquement des informations d'identification mises en cache, généralement sous la forme d'un hachage NTLM. L'attaquant peut alors tenter d'utiliser les informations d'identification pour un accès non autorisé, généralement en inversant le hachage pour obtenir le mot de passe, ou en réutilisant le hachage dans une attaque de type Pass the Hash (qui consiste à se connecter à une machine uniquement à partir du hash).

Cette méthode nécessite que l'attaquant contrôle l'infrastructure du serveur. Par conséquent, le vecteur d'attaque le plus probable est le lien de harponnage. L'attaquant hameçonne un utilisateur sur le réseau, et la machine victime contacte ensuite le serveur contrôlé par l'attaquant sur Internet. Pour traquer ce comportement, recherchez l'authentification sur Internet :

1. Recherchez dans le log ntlm tout signe d'authentification NTLM dans lequel l'adresse IP de destination se trouve sur le réseau externe.
2. Recherchez les entrées dans le log conn dans lesquelles le champ service contient smb (et/ou ntlm) et où la valeur de local_resp est « false ».

Dans le cas d'une attaque par empoisonnement du protocole LLMNR ou NBT-NS, un attaquant écoute les diffusions LLMNR ou NBT-NS locales demandant une ressource particulière par son nom. L'attaquant répond alors au client qui effectue une requête en usurpant la ressource réelle. Si la ressource est une ressource qui nécessite normalement une authentification, l'attaquant peut alors forcer le client à s'authentifier. Lorsque le client s'authentifie, généralement avec un hachage de mot de passe, l'attaquant utilise les informations d'identification pour usurper l'identité du client et accéder aux ressources.

Guide de «Threat Hunting»

Vous pouvez traquer efficacement ces attaques avec les données de Corelight, mais le capteur doit se trouver à l'intérieur du domaine de diffusion, car le trafic de diffusion ne traverse généralement pas les routeurs. En règle générale, vous devez répartir ou mettre en miroir des VLAN entiers, ou transférer le trafic LLMNR ou NBT-NS des sous-réseaux clients et des VLAN vers des emplacements du réseau surveillés par Corelight.

Recherchez les logs DNS dans lesquels `id.resp_p=5355` (LLMNR) ou `id.resp_p=137` (NBT-NS) et filtrez les enregistrements pour lesquels le champ réponses n'est pas vide. Comptez ensuite le nombre de champs de requête distincts par `id.resp_h`. Cette recherche donne des adresses IP qui répondent à plusieurs noms.

Reniflage réseau

Vous ne pouvez pas détecter un intrus qui renifle le trafic sur votre réseau à l'aide des logs network, car l'action est invisible. Cependant, *vous pouvez détecter un intrus en reniflant sur votre propre réseau*, car votre adversaire ne peut pas le voir.

La solution Corelight Sensors vous permet de déployer une grille de capteurs hors bande qui génère des logs associés. Ces logs permettent une observation et une détection rapides et fiables et aident à éviter l'écueil de la dépendance à la prévention, tout en fournissant un contexte pour une analyse historique plus approfondie et plus précise. Comme l'a indiqué Rob Joyce, chef de la division des opérations d'accès sur mesure de la NSA, dans son discours lors de la conférence de l'USENIX en 2016, « nous exploitons l'État-nation... que pouvez-vous faire pour vous défendre et me rendre la vie difficile ? ».

Découverte

L'adversaire essaie de se renseigner sur votre environnement.

Analyse de service réseau

Un intrus peut réaliser une analyse active pour déterminer quels appareils d'un réseau sont exploitables et les services disponibles sur ces appareils. Les méthodes d'analyse active sont les suivantes :

- L'analyse horizontale : consiste à envoyer des demandes de connexion à un port spécifique sur de nombreuses IP pour voir quelles IP répondent. Par exemple, une analyse de nombreux appareils sur le port TCP/22 révèle généralement que des appareils exécutent un serveur SSH. Une analyse de nombreux appareils sur le port TCP/445 peut énumérer efficacement l'infrastructure Windows.
- Analyse verticale : consiste à envoyer des demandes de connexion à une seule adresse IP sur plusieurs ports pour voir quels ports répondent. Cette méthode permet aux attaquants de déduire les services disponibles à partir de cette adresse IP.

Chacune de ces méthodes peut être exécutée à l'aide d'un scanner de vulnérabilités gratuit ou disponible dans le commerce. Ces produits ajoutent souvent une autre logique pour vérifier la disponibilité des services, les informations relatives aux versions et si les services sont vulnérables aux techniques d'exploitation connues.

Si un intrus utilise une ou plusieurs des méthodes précédemment énumérées pour tenter de découvrir un service, le sous-produit est une connexion qui *échouée* ou *rejetée*. Dans les données de Corelight, ces connexions sont enregistrées dans le log conn en tant que connexions où la valeur de conn_state est S0 (initiée et ignorée) ou REJ (initiée et rejetée), et généralement, la valeur du champ history n'est pas égale à « D » (post-synchronisation des données par l'initiateur). Pour rechercher l'existence d'une attaque par analyse de service réseau interne au réseau :

1. Recherchez les entrées dans le log conn où conn_state a pour valeur S0 REJ.
2. Filtrez les enregistrements dans lesquels local_orig=true et local_resp=true.
3. Regroupez et comptez les résultats par id.orig_h et le nombre d'id.resp_p uniques, pour évaluer l'horizontalité/verticalité de l'analyse.
4. Examinez la liste, en commençant par les enregistrements qui ont le nombre le plus élevé d'id.resp_h ou id.resp_p.
5. Identifiez l'expéditeur (id.orig_h) et examinez la liste des destinataires (id.resp_h) et des ports (id.resp_p).
6. Déterminez si le comportement est acceptable en fonction de l'identité de la source, des ports impliqués et des destinations.

Tous les éléments de la liste ne sont pas forcément malveillants. Les serveurs DHCP, par exemple, sont généralement configurés pour envoyer une requête ping à une adresse IP pour confirmer si l'adresse est utilisée avant de l'attribuer à partir du pool. Les serveurs d'impression avec un grand nombre d'impressions en file d'attente tentent des services d'impression SNMP et/ou réseau vers les imprimantes, même si ces imprimantes sont hors ligne. Par conséquent, les serveurs d'impression peuvent générer un grand nombre de connexions S0. Bien entendu, les logiciels qui réalisent des

Guide de «Threat Hunting»

analyses légitimes, par exemple une analyse de vulnérabilité approuvée par l'entreprise ou un système de gestion des stocks, peuvent apparaître dans la liste. De même, les ingénieurs réseau peuvent effectuer une analyse réseau ad hoc pour résoudre des problèmes. Si vous exécutez une analyse réseau, modifiez la requête d'origine pour omettre les enregistrements connus pour être bénins, puis relancez la recherche.

Découverte de partage réseau

Le protocole de partage réseau le plus couramment utilisé à mauvais escient par les attaquants est SMB, la norme pour le partage de fichiers Windows. SMB est pris en charge par tous les systèmes d'exploitation modernes. Dans les entreprises de toutes tailles, les documents de grande valeur qui stockent les informations personnelles, les secrets commerciaux, les diagrammes de réseau et d'autres données sensibles, résident généralement sur des partages SMB.

Pour rechercher et découvrir les partages sur un serveur SMB, on utilise généralement une commande DCE/RPC sur le port TCP 445. Plus précisément, une connexion au canal « srvsvc » – qui apparaît dans les logs dce_rpc en tant que point de terminaison du même nom – est suivie d'un appel vers les fonctions NetShareEnumAll ou NetShareEnum (appelées « opérations » dans le log Zeek). Ces appels de fonction sont utilisés à des fins légitimes de partage de fichiers et, considérés isolément, ils ne constituent pas des indicateurs d'intention malveillante. Toutefois, lorsqu'ils sont associés à d'autres indicateurs de mouvement latéral, ils illustrent comment un attaquant s'est déplacé latéralement au sein d'un réseau. Les cibles principales pour une recherche plus approfondie sont celles qui génèrent un grand nombre d'appels de fonctions DCE_RPC, sur un grand nombre d'hôtes et sur une courte période.

Reniflage réseau (référence X)

- Voir [Accès aux identifiants : reniflage réseau](#)

Découverte de système à distance

Les mêmes principes de détection que pour l'[analyse de service réseau](#) s'appliquent à la détection d'attaques par découverte de système à distance. Se reporter à cette section pour plus d'informations.

Mouvement latéral

Le mouvement latéral est la technique utilisée par les adversaires pour entrer et contrôler des systèmes distants sur un réseau.

Protocole RDP

Le protocole Microsoft Remote Desktop Protocol (RDP) est utilisé pour contrôler à distance un point de terminaison Windows. Ce protocole peut être utilisé à mauvais escient par un attaquant pour obtenir un accès non autorisé à votre réseau (voir [Accès initial : services distants externes](#)). Une fois qu'un intrus est à l'intérieur de votre réseau, il peut utiliser le protocole RDP pour se déplacer latéralement entre les appareils.

Guide de «Threat Hunting»

RDP est l'un des nombreux protocoles analysés par Corelight. Pour certains environnements, la présence du protocole RDP, ou sa présence sur des systèmes spécifiques est suffisante pour déclencher une analyse. Pour les réseaux où RDP est autorisé, le log Zeek RDP fournit des informations précieuses qui aident à déterminer si une connexion est légitime, par exemple, en enregistrant des données telles que la disposition du clavier, les niveaux de cryptage ou le nom du client pour une connexion spécifique.

Lors du «Threat Hunting» avec le log rdp :

1. Centrez les recherches sur les champs `id.orig_h`, `id.resp_h`, `id.resp_p` et `cookie`. Le champ `cookie` peut contenir n'importe quelle valeur arbitraire envoyée par le client RDP au serveur, mais il contient souvent le nom d'utilisateur envoyé par le client RDP.
2. Regroupez les enregistrements en fonction de ces quatre champs et affichez un décompte pour chaque ensemble unique.
3. Répétez l'opération pour l'ensemble et identifiez l'origine et la destination de chaque connexion (par exemple, vous pouvez utiliser les enregistrements des log DNS et DHCP).
4. Certaines connexions RDP utiliseront une disposition de clavier non standard. Pour les rechercher, examinez le champ `keyboard_layout`. Comptez le nombre d'instances de chaque valeur et appliquez un empilement de données pour rechercher les valeurs aberrantes ou rares.
5. Identifiez l'origine et la destination et déterminez si la disposition du clavier non standard n'est pas surprenante, par exemple, si vous savez que l'utilisateur d'origine utilise une langue autre que la langue habituelle de votre pays comme langue principale et que cette langue est la langue demandée dans la connexion RDP.

Après avoir obtenu ces informations, posez-vous plusieurs questions :

- La valeur du `cookie` correspond-elle à l'utilisateur attendu sur la machine source ou de destination ?
- Existe-t-il une raison légitime pour laquelle l'expéditeur utilise RDP ?
- Observez-vous que certains utilisateurs utilisent RDP alors que cela semble surprenant compte tenu de leur fonction ?

Services distants

L'exploitation d'une vulnérabilité logicielle se produit lorsqu'un adversaire profite d'une erreur de programmation pour exécuter du code qu'il contrôle. Cette exploitation peut se produire dans un programme, un service ou dans le logiciel du système d'exploitation ou encore le noyau lui-même. Un objectif habituel pour l'exploitation après avoir compromis des services distants est le mouvement latéral.

Compte tenu de la complexité actuelle des réseaux d'entreprise, divers services tiers et externes sont souvent utilisés. Ces services permettent aux attaquants d'obtenir un accès initial ou de se déplacer suivant un mouvement latéral. Toutes les connexions sont enregistrées dans `conn.log`, cependant, plus de détails peuvent être disponibles dans les logs spécifiques du protocole en fonction de la nature du service distant attaqué. Par exemple, vous pouvez surveiller le fichier `http.log` pour détecter les requêtes HTTP suspectes et inattendues (telles que les requêtes `OPTIONS`).

Guide de «Threat Hunting»

```
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,
```

Corelight extrait également des informations sur les logiciels observés sur le réseau dans le log software. Ce fichier fournit aux défenseurs des données précieuses pour surveiller les serveurs inattendus ou non autorisés, les services vulnérables ou obsolètes et les logiciels clients non corrigés.

```
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
```

Partages administratifs Windows

Les systèmes Windows ont des partages réseau cachés qui ne sont accessibles qu'aux administrateurs et offrent la possibilité de copier des fichiers à distance et d'autres fonctions d'administration. C\$, ADMIN\$ et IPC\$ sont des exemples de partages réseau.

Les attaquants utilisent souvent SMB pour se connecter aux partages administratifs sur les postes de travail et serveurs Microsoft Windows. Leur but peut être d'obtenir plus d'informations sur la cible, extraire des fichiers sensibles, télécharger des charges utiles malveillantes ou s'authentifier afin que d'autres outils et attaques puissent être utilisés. Corelight surveille le trafic SMB, y compris les tentatives d'authentification, ce qui permet aux défenseurs de consigner et de remarquer les modèles de tentatives d'authentification administrative, ainsi que de surveiller le trafic SMB pour extraire les fichiers transférés. L'exemple suivant montre l'action FILE_OPEN en cours d'exécution à l'aide du partage administratif masqué et inclut des informations MAC. Corelight enregistre l'action effectuée, notamment Ouvrir/Renommer/Supprimer/Écrire.

Guide de «Threat Hunting»

```
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
```

Collecte

L'adversaire essaie de recueillir des données pour atteindre son objectif.

Archivage de données collectées

Pour dissimuler des données, les attaquants peuvent les consolider dans des fichiers d'archive compressés, tels que des fichiers Zip, RAR, TAR ou CAB. Pour traquer cette technique de brouillage, utilisez le log files.

Pour rechercher des fichiers compressés :

1. Recherchez tous les logs files, en récupérant les champs tx_hosts, rx_hosts, mime_type, total_bytes et source.
2. Supprimez des résultats les enregistrements qui contiennent des types MIME sans intérêt, par exemple :
 - a. application/x-x509-*
 - b. application/ocsp*
 - c. image/*
 - d. audio/*
 - e. video/*
 - f. text/*
 - g. application/xml
 - h. application/chrome-ext

Collecte automatisée

Les attaquants peuvent déployer des outils automatisés sur un hôte compromis pour surveiller les services intranet afin de rechercher des données sensibles et des secrets d'entreprise. Ces outils peuvent inclure des scripts pour rechercher (et copier) des informations telles que le type de fichier, l'emplacement ou le nom, à des intervalles de temps spécifiques. Les intrus peuvent utiliser des outils d'accès à distance pour effectuer une collecte automatisée.

Guide de «Threat Hunting»

Par exemple, un outil personnalisé peut interroger un serveur web intranet ou un serveur de messagerie interne, en lançant régulièrement des requêtes pour obtenir de nouveaux contenus. Corelight surveille plusieurs protocoles, notamment le trafic HTTP, e-mail, MySQL, FTP et SMB, pour fournir un aperçu de ces requêtes.

Pour traquer les attaques basées sur la collecte automatisée, les défenseurs peuvent identifier les outils automatisés en surveillant les requêtes répétitives ou les connexions régulièrement programmées. Par exemple, si un intrus utilise la technique du moissonnage web, un grand nombre de connexions à partir d'un nombre fini d'adresses IP pourra être observé. De plus, vous pouvez utiliser les logs SMB (smb_files ou smb_mapping) pour identifier les modèles de trafic anormaux.

Données de lecteur réseau partagé

Les lecteurs réseau partagés sont une mine de documents d'entreprise sensibles. La plupart des réseaux d'entreprise hébergent des lecteurs réseau partagés utilisant le protocole SMB, mais certains peuvent s'appuyer sur FTP, HTTP ou même RDP. Zeek peut surveiller l'accès aux lecteurs réseau partagés lorsque des protocoles tels que SMB, FTP ou HTTP sont utilisés. Les protocoles de contrôle à distance, comme RDP, sont également analysés dans des logs spécifiques aux protocoles. Partout où Corelight observe ce trafic, il est surveillé et enregistré dans le log spécifique au protocole.

L'exemple suivant montre le log ftp. Corelight enregistre la commande et les arguments.

```
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
```

Commande et contrôle

L'adversaire essaie de communiquer avec des systèmes compromis pour les contrôler.

Ports couramment utilisés/Ports non standard

Les adversaires peuvent utiliser un port couramment utilisé pour éviter une vérification plus détaillée.

Guide de «Threat Hunting»

La traque de canaux C2 sur les ports couramment utilisés est difficile, mais pas impossible. Pour rechercher les canaux C2, recherchez les ports bien connus qui sont utilisés avec un service peu habituel.

Lors de la recherche de canaux C2 à l'aide des ports couramment utilisés :

1. Centrez-vous tout d'abord sur le champ service et recherchez dans le log conn les entrées pour lesquelles le champ service n'est pas ce que vous attendez pour le port standard (le champ service peut contenir soit « - » ou un autre service).
 - a. Commencez par les protocoles les plus courants.
 - o TCP:80 (HTTP) TCP:443 (HTTPS)
 - o TCP:25 (SMTP)
 - o TCP/UDP:53 (DNS)
2. Encrypted Traffic Collection (ETC) de Corelight contient un package dénommé Encryption Detection (détection de cryptage). Encryption Detection génère une notification lorsqu'un trafic en texte clair est observé sur des ports généralement chiffrés. Les notifications pour Viz::UnencryptedService met en évidence ce comportement et vous aide à identifier les connexions potentiellement malveillantes à l'aide de ports couramment utilisés.

Le package ETC de Corelight dispose également d'une fonctionnalité qui vous avertit lorsqu'une session utilise le cryptage instantané. Le package recherche les clés prépartagées ou les connexions chiffrées qui commencent sans négociation de clé traditionnelle. Les notifications pour Viz::CustomCrypto mettent en évidence ce comportement et vous aident à identifier les connexions potentiellement malveillantes à l'aide des ports couramment utilisés.

Vous pouvez également utiliser les logs dpd et weird de Corelight pour identifier tout comportement de protocole inattendu. Ces logs affichent les erreurs de débogage et d'analyse et identifient l'utilisation des ports et protocoles courants qui sont hors des spécifications, ce qui peut indiquer une activité malveillante ou une utilisation secrète de ports et de protocoles connus.

```
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
```

Chaîne cryptée

Voir la section [Ports couramment utilisés](#) pour obtenir une description du package Encryption Detection de Corelight, du log dpd log et du log weird. Cela vous aide à identifier les potentiels protocoles cryptographiques personnalisés.

Canaux de secours, canaux à étages multiples

Les adversaires sont connus pour diviser les communications entre différents protocoles, en utilisant un protocole pour le C2 entrant et un autre pour les données sortantes. Cela permet à la communication de contourner les restrictions du pare-feu.

Les logiciels malveillants qui divisent la communication entre deux hôtes pour les instructions et pour l'exfiltration sont une nouvelle difficulté pour les défenseurs. Reconnaître le lien entre le trafic de contrôle suspect et les transferts de données volumineux est une tâche difficile, mais Zeek fournit des packages et des frameworks qui synthétisent les données. Par exemple, un package permet de déterminer le rapport producteur-consommateur pour les connexions, qui identifie les transferts de données déséquilibrés et éventuellement suspects. De plus, Intelligence Framework permet la coordination avec d'autres défenseurs en identifiant d'éventuels indicateurs de compromission (adresses IP, adresses e-mail et noms de domaine) dans les données Corelight.

Il est difficile de corréler les attaquants en utilisant différentes méthodes et canaux de communication, mais le contenu de Corelight et les frameworks et packages Zeek peuvent aider. Ils permettent aux défenseurs d'identifier les canaux cachés discrètement, en offrant de multiples possibilités de détection.

Au-delà de la surveillance des mécanismes de communication C2 mentionnés précédemment, voici quelques autres indicateurs disponibles dans les données Corelight :

- Utilisez `conn.log` pour identifier les modèles de communication qui indiquent des canaux supplémentaires (par exemple, en utilisant `orig_h` et `resp_h` pour restreindre les connexions à une fenêtre de temps et observer les connexions entre les hôtes qui incluent des ports impairs, des connexions qui ont échoué ou refusées, ou des éléments intéressants/suspects).
- Utilisez Corelight (ETC) ou du contenu que vous avez vous-même développé, en association avec la découverte des logs de connexion pour trouver des relations potentielles entre des connexions qui se chevauchent, adjacentes ou intéressantes.
- Recherchez les séquences de connexions à des hôtes non associés à l'aide de différents protocoles ou événements dans les logs `dpd` et `weird`, comme décrit dans la section sur [Ports couramment utilisés](#).

Transfert d'outil d'entrée

Les intrus déplacent généralement des fichiers sur des systèmes compromis, que ce soit des outils pouvant aider à d'autres mouvements latéraux et/ou des fichiers sensibles conçus pour l'exfiltration. Ces fichiers se déplacent généralement via une connexion HTTP(S), SSH ou SMB.

Pour les fichiers qui se déplacent via HTTP en texte brut, certains détails tels que le nom d'hôte distant et le nom et le type MIME du fichier en cours de transfert peuvent être des indicateurs utiles ; vous devez également consulter le log `files` pour les hachages de fichiers déplacés, car de nombreux outils d'attaquant populaires ont des hachages cryptographiques connus qui facilitent leur identification. Dans le cas de HTTPS, les défenseurs peuvent utiliser l'adresse IP du système distant, ainsi que les détails du

Guide de «Threat Hunting»

certificat consignés dans le log SSL (c'est-à-dire le nom de l'organisation, le nom de domaine complet FQDN de l'hôte distant du CN, etc.) pour rechercher des anomalies au niveau des connexions.

Les intrus copient les fichiers d'un point de terminaison à un autre lorsqu'ils se déplacent latéralement parmi les éléments compromis. Généralement, les copies de fichiers vers ou depuis les systèmes Unix/Linux se produisent via le protocole SSH en utilisant la commande scp. Pour les systèmes Windows, les chargements ou les téléchargements de fichiers à distance se produisent généralement via SMB, mais peuvent également utiliser le protocole SSH via PUTTY.

Corelight Sensors avec le package d'inférences ETC SSH activé étendent le log ssh. L'extension comprend un champ d'inférences qui ajoute des caractéristiques inférées sur le trafic SSH. Par exemple, si la session est utilisée pour déplacer des fichiers, ou si elle est interactive :

- LFU: Large File Upload (chargement de fichiers volumineux)
- LFD: Large File Download (téléchargement de fichiers volumineux)
- KS: Keystrokes (saisies clavier)

Pour commencer à rechercher les sessions SSH intéressantes, utilisez le champ d'inférences du package ETC SSH :

1. Identifiez les sessions où le champ d'inférences contient LFU, SFU, LFD ou SFD
2. Déterminer si l'activité des fichiers via SSH est légitime et attendue

Les capteurs Corelight Sensors sont préchargés avec le package MITRE BZAR (analyses et rapports basés sur Bro/Zeek ATT&CK). MITRE BZAR identifie les techniques MITRE ATT&CK pour rechercher la copie de fichiers à distance, à savoir les fichiers copiés sur des partages C \$ ou ADMIN\$. Ce package génère des entrées dans le log notice, comme illustré ci-dessous :

```
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: FSeaVF4qnl8cT3HF8,  
file_mime_type: text/plain,  
file_desc: Windows\\Temp\\hbaVJpzdng,  
proto: tcp,  
note: ATTACK::Lateral_Movement_Extracted_File,
```

```
msg: Enregistrement d'une copie du fichier écrit sur le partage de fichiers administrateur SMB,  
sub: 2020-10-23/6f24ac6ce591baf02acd64684f596d2db0ec97c0,  
src: 192.168.38.104,  
dst: 192.168.38.102,
```

Guide de «Threat Hunting»

p: 445,

actions: [Notice::ACTION_LOG],suppress_for:3600.0

Même si vous n'activez pas le package MITRE BZAR sur votre Corelight Sensor, Corelight enregistrera toujours l'accès au partage SMB dans le log smb_mapping et l'accès et la modification de fichiers dans le log smb_files. Les logs suivants illustrent les données contenues dans la famille Corelight de log 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

Pour traquer les mouvements latéraux :

1. Commencez par rechercher les logs smb_files et centrez-vous sur les champs id.orig_h, id.resp_h, path et name
2. Filtrez les enregistrements dans lesquels id.resp_h est un serveur de fichiers connu, ce qui réduit les résultats à des connexions potentiellement intéressantes
3. Examinez les champs path et name pour identifier le partage à partir duquel on a accédé au fichier où écrit dans le fichier, et déterminez si le comportement est suspect.
4. Pour plus de contexte sur les autres enregistrements intéressants, vous pouvez basculer vers le log files en utilisant l'UID pour collecter des informations spécifiques sur le ou les fichiers. Par exemple, le ou les hachages MD5/SHA1/SHA256 sont calculés automatiquement et peuvent être utilisés pour identifier les logiciels malveillants connus dans des systèmes externes, tels que VirusTotal.

Guide de «Threat Hunting»

- a. Il existe également d'autres champs et logs éventuellement disponibles (par exemple, le log pe) qui peuvent être utilisés pour exclure les enregistrements sans intérêt.

Protocole de couche non applicative

Les attaquants utilisent souvent une série de techniques pour se cacher à l'intérieur du trafic légitime : en envoyant leurs communications via un protocole personnalisé sur un port généralement autorisé comme les ports 80, 443 ou 53, et en intégrant leur messagerie à l'intérieur de la structure légitime, mais avec des protocoles généralement moins surveillés comme ICMP.

Pour l'utilisation de protocoles personnalisés sur les ports standard, se reporter à la section [Ports couramment utilisés/Ports non standard](#) pour obtenir une description du package Encryption Detection de Corelight, du log dpd et du log weird. Ils vous aideront à identifier les communications C2 personnalisées qui utilisent un cryptage non standard ou violent les spécifications de protocole traditionnelles.

Les logiciels malveillants utilisent parfois des protocoles standardisés de niveau inférieur comme ICMP, UDP et SOCKS pour éviter la détection, car ces protocoles sont rarement surveillés. Par exemple, les auteurs de logiciels malveillants peuvent intégrer des instructions C2 dans un paquet ICMP Echo Request (« ping »).

Corelight surveille toutes les connexions, quel que soit le protocole et stocke les données de connexion dans le log conn. Les canaux C2 qui utilisent des protocoles UDP personnalisés ou des protocoles SOCKS basés sur TCP (mais pas de protocoles de couche applicative standard) ont des entrées de log de connexion sans champ service identifiable. Ces champs et logs offrent une visibilité sur les flux de trafic sur le réseau, même ICMP, UDP et SOCKS. Pour les sessions ICMP, les données Corelight contiennent plus que la source et la destination, par exemple, le nombre de paquets, les octets transférés et la taille des données ICMP pour l'expéditeur et le destinataire.

Grâce à ces données, vous disposez des informations nécessaires pour découvrir les communications ICMP anormalement volumineuses ou fréquentes qui peuvent être indicatives de canaux C2. Le journal suivant est un exemple de log 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,
```

Guide de «Threat Hunting»

```
request.host: 192.168.0.2,  
request_p: 22,  
bound.host: 192.168.0.1,  
Bound_p: 55951
```

Pour rechercher un intrus à l'aide d'un protocole standard de couche non applicative pour transmettre des informations par tunnel :

1. Recherchez dans le log conn les entrées où le champ service est vide, et où la valeur de local_orig est « true » et celle de local_resp est « false »
2. Regroupez ces résultats par id.orig_h, id.resp_h, id.resp_p et résumez par nombre
3. Filtrez les entrées « normales »
4. Examinez tous les éléments restants, en vous centrant d'abord sur les lignes de saisie avec le plus grand nombre

Guide de «Threat Hunting»

Ports non standard

Toutes les connexions établies dans un environnement surveillé par Corelight sont enregistrées dans le log conn. Après avoir créé une liste des ports régulièrement utilisés (par exemple, 22/SSH, 25/SMTP, 80/HTTP et 443/SSL), vous pouvez interroger les données Corelight pour trouver des connexions aux ports qui ne figurent pas sur cette liste.

Si vous détectez des connexions qui apparaissent sur d'autres ports non standard, examinez le service de couche 7 que Corelight observe et enregistre dans le champ service du log conn. Les cas sans service reconnu sont les plus suspects, en particulier si de gros volumes de données sont transférés ou si les connexions sont longues.

Lorsque vous détectez des services connus sur des ports irréguliers, examinez les détails dans le log protocol correspondant pour obtenir des indices supplémentaires. Par exemple, dans le log HTTP, notez le nom de l'hôte distant, la chaîne User-Agent du client et l'URI (identifiant uniforme de ressource). Ensemble, ils peuvent tous contenir des indices sur le logiciel qui génère la requête sur le port inhabituel.

```
Path: conn,  
uid: CrlIbl1BJ8Al8ryyX6,  
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.ni  
pekpidbkfyjyp.ml:26749],  
mss: 1400,
```

Guide de «Threat Hunting»

```
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

Bien que l'utilisation de proxys ne prouve pas en soi la présence d'un intrus, les intrus peuvent utiliser des proxys pour « blanchir » les connexions afin de masquer la communication des défenseurs. Il existe de nombreuses méthodes pour observer cette stratégie, notamment l'analyse traditionnelle de la connexion sous-jacente (signature, anomalie, comportementale) et l'analyse statistique des propriétés de la connexion. L'identification spécifique des connexions proxy est essentielle pour commencer la traque ou la recherche.

Si vous voyez une valeur dans le champ proxy du journal http de Zeek, cela signifie qu'une connexion HTTP a été établie en utilisant un proxy. Le log http capture les détails du proxy à partir des en-têtes http. Recherchez tous les enregistrements dans le log http avec un champ proxy non vide.

- host: le nom de domaine du site web
- id.orig_h: l'adresse IP du proxy ou du proxy inverse
- id.resp_h: l'adresse IP du serveur web
- proxied: identifie le proxy et l'adresse IP d'origine du client

Par exemple, un client avec l'adresse IP 219.90.98.8 a lancé cette requête HTTP. La requête a été transmise par proxy via 172.16.1.30 au serveur web à 172.16.2.95.

```
host: www.totallyfakedomain.com  
id.orig_h: 172.16.1.30 //le proxy  
id.orig_p: 53 828  
id.resp_h: 172.16.2.95 //le serveur web  
id.resp_p: 80  
method: POST  
post_body: dXNlcm5hbWU9cm9vdCZwYXNzd29yZD1tb25rZXk=  
proxied: X-FORWARDED-FOR -> 219.90.98.8 //le client réel  
status_code: 200  
status_msg: OK  
uri: /xmlrpc.php  
user_agent: Mozilla/4.0 (compatible ; MSIE 6.0 ; Windows NT 5.0)  
log: http
```

Guide de «Threat Hunting»

À l'aide de cet exemple, identifiez le proxy et déterminez s'il est interne ou externe. S'il est externe, évaluez la session et obtenez plus de contexte, en utilisant les données Corelight pour décider de la bloquer ou non. Si le proxy est interne, déterminez s'il s'agit d'un élément légitime de l'infrastructure informatique, ou s'il s'agit d'un proxy malveillant configuré pour contourner la politique (« shadow IT »).

Par ailleurs, SOCKS est un protocole proxy couramment utilisé que Corelight Sensors analyse nativement. Lorsque SOCKS est détecté, un log socks est généré et enregistre les détails sur les utilisateurs et les protocoles. Cette information peut être utilisée pour s'assurer que les connexions ne sont pas malveillantes et sont conformes à la politique. Dans le logs socks, soyez particulièrement attentifs aux champs suivants :

- `id.orig_h` : l'adresse IP du client
- `id.resp_h` : l'adresse IP du proxy
- `request` : le domaine ou l'adresse IP auquel le client tente d'accéder
- `user` : s'il s'agit d'une connexion authentifiée, l'utilisateur qui utilise le proxy

Service web

L'attaque par service web se produit lorsque des attaquants utilisent un service web externe légitime pour relayer des données vers et/ou à partir d'un système compromis.

Les attaquants utilisent parfois des services web bien connus pour les canaux C2, pour se dissimuler au milieu du bruit. Bien que cette tactique rende l'identification plus difficile, les données Corelight, en particulier les logs http, ssl, conn et x509, vous aident à identifier les connexions suspectes. La recherche d'indicateurs de compromissions (IoC), notamment l'URI, le nom d'hôte ou des détails sur un certificat spécifique (par exemple SNI ou CN) est un bon point de départ. Voici quelques exemples de champs de certificat pouvant justifier une recherche :

```
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

Exfiltration automatisée

Si un attaquant utilise un moyen d'exfiltration automatisé, les artefacts de données sont capturés dans les données Corelight.

Pour rechercher une exfiltration dans votre réseau, vous pouvez utiliser le [package Zeek](#) développé pour calculer le [ratio Producteur/Consommateur](#) (PCR). Les valeurs PCR indiquent si les flux sont de type consommateurs (téléchargement) ou producteurs (téléchargement). Les valeurs de PCR vont de -1 (consommateur) à +1 (producteur). Pour traquer l'exfiltration à l'aide de ce package :

1. Installez et activez le package PCR.
2. Générez une table des champs `id.orig_h`, `id.resp_h`, `id.resp_p` et `pcr` à partir du log `conn`.
3. Utilisez `local_orig=false` ou `local_resp=true` pour filtrer les résultats.
4. Réduisez les résultats en filtrant les champs où `pcr <= 0`.
5. Pour chaque hôte générant des flux où `pcr > 0`, déterminez si cet hôte est censé transmettre des données, à l'intérieur ou à l'extérieur du réseau.

Une autre option consiste à utiliser un SIEM (outils de gestion des événements et informations de sécurité) pour calculer le PCR à l'aide des informations disponibles dans le log `conn` de Corelight. La requête suivante crée une table organisée par hôte, contenant les octets d'origine et de réponse et une valeur 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
```

Limitation de la taille pour transférer des données

Un attaquant peut tenter de transférer des données ou des fichiers en les « fragmentant » en morceaux plus petits, afin d'éviter les limites ou les seuils de transfert de données codés en dur. Il existe dans ce cas deux méthodes pour traquer cette technique.

La première méthode consiste à analyser les données qui quittent le réseau en fonction des paires source et destination et effectuer une requête de plateforme d'agrégation/visualisation de données (sauf si vous aimez AWK et GREP pour les données) :

1. Générez une table à partir du log `conn` comprenant les champs `id.orig_h`, `id.resp_h`, `id.resp_p` et `sum(orig_bytes)`.
2. Triez les résultats par la plus grande somme (`orig_bytes`).
3. Examinez chaque hôte et déterminez s'il existe une raison légitime pour réaliser des téléchargements vers cette destination.

La deuxième méthode consiste à analyser la fréquence et la taille des transferts sortants de chaque source :

Guide de «Threat Hunting»

1. Générez une table à partir de log conn comprenant les champs id.orig_h, id.resp_h, id.resp_p et sum (orig_bytes).
2. Triez les résultats par le plus grand nombre (orig_bytes).
3. Examinez les résultats et déterminez la raison de toutes les connexions avec la même quantité de données circulant de la source à la destination.

¹ <https://attack.mitre.org/>

² Lorsqu'elle est utilisée comme indicateur Intel, l'IP est considérée comme fragile, du fait de la facilité avec laquelle les adversaires peuvent se déplacer vers un nouvel hôte ou fournisseur.

³ Toutes les versions de RDP ne déclarent pas le nom d'utilisateur dans le champ cookie. Certains ne déclarent rien, ou c'est du charabia. Dans ces cas, vous devrez le déduire du log NTLM ou Kerberos.

⁴ <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>

⁵ Consultez <https://packages.zeek.org/> pour plus d'informations sur les packages Zeek



Les défenseurs cherchent toujours à prendre de la hauteur pour voir plus loin et faire reculer les attaques. Corelight offre une vue imprenable sur votre réseau afin de vous permettre de déjouer les pièges et survivre à vos adversaires. Nous capturons, interprétons et connectons les données les significatives pour les défenseurs.

info@corelight.com | 888-547-9497