Guida al Threat Hunting

Introduzione

Questa guida al Threat Hunting è stata creata per insegnarvi delle maniere semplici e pertinenti per scoprire gli attacchi prima che si perpetrino, utilizzando i dati di rete forniti da Corelight. Questo documento, organizzato attorno al framework MITRE ATT&CK®, è stato concepito per aiutarvi a sviluppare una metodologia di Threat Hunting e a stabilire delle priorità.

MITRE ATT&CK è una base di conoscenze accessibile a livello globale, riguardante le tattiche e le tecniche avversarie basata su osservazioni del mondo reale. È usata come base per modelli e metodologie specifiche di rilevamento di minacce nel settore privato, governativo e nel settore della sicurezza informatica. Con la creazione di ATT&CK, MITRE sta assolvendo alla propria missione di risolvere i problemi per un mondo più sicuro - riunendo le comunità al fine di sviluppare una cybersecurity più efficace. ATT&CK è aperto e disponibile gratuitamente per qualsiasi persona o organizzazione.[1]

Cos'è il threat hunting?

Ad alto livello, il Threat Hunting consiste nel cercare proattivamente gli avversari nella vostra rete *quando non sapete se sono all'interno della stessa*. È una cosa diversa rispetto all'*indicator matching*, che si limita a cercare segnali ben noti di attaccanti, ad esempio, indirizzo(i) IP o hash di file. Di solito condurre una caccia alle minacce comporta l'elaborazione di una teoria, o un'intuizione, per poi effettuare l'analisi dei dati alla ricerca di qualcosa di *interessante*. Item considerati *interessanti* possono apparire in svariate forme, ad esempio "nell'*Uovo del Cuculo*", di Clifford Stoll, un errore contabile ha dato il via alla caccia.

> ***"Dave entrò nel mio ufficio, borbottando su un intoppo nel sistema di contabilità Unix. Qualcuno deve aver usato qualche secondo di tempo di calcolo senza pagarlo. I libri contabili del computer non quadravano del tutto; le fatture del mese scorso di 2.387 dollari mostravano un deficit di 75 centesimi".***

Questa differenza di 75 cent fu l'indicatore che portò alla scoperta della compromissione dei sistemi di svariate società e organismi governativi. Il termine "interessante" viene ampiamente usato in tutta questa guida ed il limite dello stesso dipende esclusivamente dalla vostra immaginazione.

Perché effettuare un threat hunt?

La maggior parte dei sistemi di rilevamento basati su host o su rete fanno affidamento sul matching, noto anche come *signature matching* (matching di firme), per generare avvisi volti a segnalare ai difensori che c'è qualcosa di indesiderato nella rete. Tuttavia, gli aggressori continuano ad evolvere nelle loro tattiche per eludere il rilevamento, e le firme vengono sviluppate solo dopo che l'artefatto è stato scoperto in un'altra rete. Pertanto, se non siete a caccia di artefatti nel vostro ambiente, come farete a scoprire che gli attaccanti stanno eludendo le vostre attuali difese?

La caccia attiva offre svariati risultati positivi. Il primo è che potreste trovare degli artefatti di un intruso attivo che le vostre attuali difese non hanno rilevato. Mentre alcuni possono pensare che questa sia una tragedia, può invece essere considerata una grande vittoria, soprattutto se l'intruso non ha portato a buon fine il/i suo/i obiettivo/i. In ogni caccia, c'è sempre *qualcosa* da trovare.

Potreste scoprire degli errori di configurazione della rete o del software che rappresentano una minaccia, perché degradano le prestazioni della rete o introducono una vulnerabilità. Inoltre, la caccia potrebbe rilevare delle infezioni ordinarie come adware, o altri malware dormienti che non prendono direttamente di mira la vostra organizzazione, ma che sono comunque una minaccia. Infine, l'abuso di risorse e lo Shadow IT, servizi che non sono ufficialmente supportati, possono rappresentare un rischio, attraverso prestazioni di rete degradate o nuovi vettori di attacco avversari. Ogni caccia vi insegna qualcosa di nuovo sulla rete che vi aiuterà nella vostra prossima indagine.

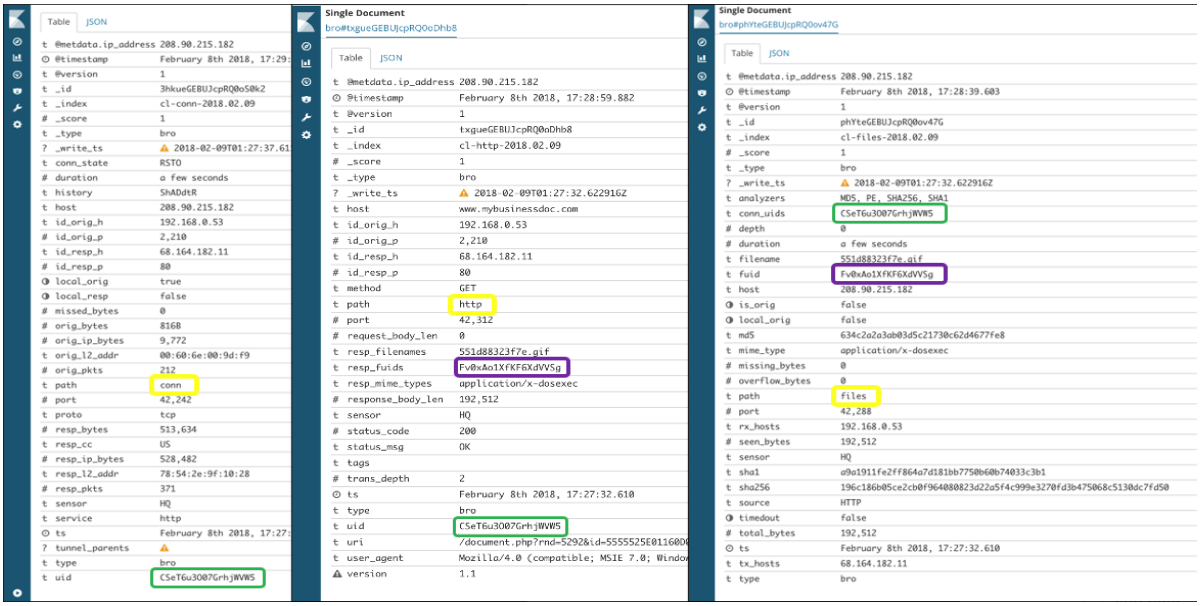
Perché cacciare con i dati di rete?
I pacchetti non mentono

È davvero semplice. Se un intruso residente nella rete è attivo nella vostra rete, ci saranno degli artefatti di rete. Negli artefatti, ci sono indizi di ciò che sta accadendo, o meglio ancora, un esatto racconto, momento per momento, di ciò che è accaduto. Ad esempio, se un canale di Command and Control usa il DNS come meccanismo di trasporto, ci saranno query e risposte DNS. Inoltre, gli indirizzi IP che si trovano alle estremità di una connessione TCP devono essere accurati, non possono essere "spoofati" se vengono scambiati dei dati. Tutti gli attacchi attraversano la rete, a meno che non siano isolati in un host, quindi esisteranno dei pacchetti.

Nomenclatura dei log di Corelight

Corelight fornisce soluzioni incentrate sui dati che analizzano il traffico di rete e migliorano gli strumenti di automazione trasformando il traffico di rete in log collegati ed estraendo file. Il log centrale è il conn log, che documenta informazioni generali di tutte le sessioni di rete.

Il conn log registra informazioni su ogni endpoint di rete e sul servizio (applicazione) assegnando inoltre un uid (identificatore unico). L'uid collega il conn log ai log di protocollo correlati, dove sono disponibili informazioni specifiche riguardanti la sessione. Ad esempio, il conn log può elencare http come servizio, e usando l'uid si può passare al http log per ottenere informazioni specifiche sul protocollo della sessione. L'uid separa le soluzioni Corelight da altri strumenti di sicurezza. Questo campo collega informazioni altrimenti disparate in log facilmente digeribili. L'uid è fondamentale per condurre l'analisi dei collegamenti ed è un campo estremamente importante che facilita il pivoting, o l'unione di più log insieme.



Le informazioni su ogni endpoint di rete sono riassunte dal campo id, che viene normalmente rappresentato da quattro campi separati:

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

Questa nomenclatura può sembrare strana da usare, perché il personale di rete tradizionalmente si riferisce alle sessioni usando client e server; tuttavia, usare orig (originator) e resp (responder) permette al personale di sicurezza di descrivere accuratamente la connessione. Pensate all'host di origine (orig_h) come fonte, o client, e all'host che risponde (resp_h) come destinazione, o server. I campi id.orig_p e id.resp_p saranno popolati con i numeri di porta corrispondenti.

Molti dei campi rimanenti all'interno del conn log e di altri log di protocollo sono auto-descrittivi, ma se avete delle difficoltà, guardate la documentazione di Zeek su https://docs.zeek.org/en/current/ per informazioni più dettagliate o visitate il canale di slack della comunità su http://corelightcommunity.slack.com/.

Identificazione di utenti e dispositivi

Quando si identificano i dispositivi in una rete, gli indirizzi IP o MAC sono regolarmente utilizzati per creare 'l'identità'. L'indirizzo IP del dispositivo è usato più spesso per l'identità remota di un dispositivo perché sopravvive ai confini dei router. Una volta all'interno di un segmento di rete, l'indirizzo MAC è preferito per l'identificazione perché può essere un identificatore affidabile di una macchina specifica. Ogni identificatore ha dei pro e dei contro, e la capacità di Corelight di catturare entrambi aiuta il personale del SOC a indagare sugli eventi.

Mentre gli indirizzi IP sono durevoli[2] per le indagini interne, spesso sono transitori all'interno di una rete, dato che la maggior parte delle reti implementa il protocollo DHCP (Dynamic Host Configuration Protocol). Gli IP transitori sono problematici per i difensori quando l'allarme IDS identifica la sessione in base agli indirizzi IP. Detti indirizzi IP sono collegati all'allarme solo *nel momento in cui l'allarme è stato generato.*

È possibile utilizzare strumenti open source quando si conduce un'indagine (ad esempio, nslookup), per fornire informazioni DNS per gli IP remoti. Ciononostante, si tratta di informazioni puntuali, *al momento dell'indagine, non quando l'evento si è verificato.* Una tecnica migliore è quella di utilizzare i log creati al momento dell'allarme per catturare l'IP e il FQDN (fully qualified domain name) del dispositivo remoto. Per localizzare il dispositivo interno, è possibile estrarre i DHCP log per identificarlo. Ci sono più modi per identificare un host e Corelight fornisce questi dati in più log, che raccontano ciascuno un aspetto diverso della storia. Pratica la creatività e segui ogni pista.

Dove si possono trovare gli hostname:

- **dhcp.log:** i campi host_name e domain rappresentano l'hostname e il dominio riportati da un host quando richiede un indirizzo IP tramite DHCP, e il campo assigned_addr è l'indirizzo IP che è stato assegnato a quel host.
- **dns.log:** se c'è un IP nel campo risposte, allora il campo query contiene l'hostname che il server DNS ha registrato (in quel momento) per l'indirizzo IP.
- **ntlm.log:** server_dns_computer_name e server_nb_computer_name si riferiscono ai nomi DNS e Netbios della macchina con l'indirizzo IP nel campo id.resp_h. Il campo hostname è l'hostname della macchina con l'indirizzo IP nel campo id.orig_h.
- **kerberos.log:** in un ambiente Windows, per dispositivi uniti da un dominio, nelle richieste di kerberos in cui il campo client contiene un nome che termina con $, il campo client è il nome dell'host e il campo id.orig_h è l'indirizzo IP di quell'host. Il campo client è spesso strutturato come HOSTNAME$/EXAMPLEDOMAIN.COM dove HOSTNAME è il nome dell'host e EXAMPLEDOMAIN.COM è il nome del dominio Windows e il nome del realm Kerberos.
- **http.log:** il campo host contiene l'hostname, il nome di dominio o l'indirizzo IP del client che ha richiesto dati dal server HTTP. A volte questo campo è un'indicazione dell'identità del server, il dispositivo con l'indirizzo IP nel campo id.resp_h.
- **ssl.log:** il campo server_name è estratto dal campo Server Name Indication (SNI) nella negoziazione TLS/SSL, ed è usato in modo simile al campo host del http log. Inoltre, il campo dell'oggetto viene estratto dall'oggetto del certificato del server, e la porzione CN del nome canonico dell'oggetto può fornire indizi per identificare un server.

Quando si identificano gli utenti, ci sono diversi log che forniscono informazioni preziose:

- **rdp.log:** a seconda della versione del protocollo RDP, il valore del campo cookie è il nome utente asserito dal client, e l'IP del client è nel campo id.orig_h.[3]
- **ftp.log:** il campo user contiene il nome utente asserito dal client, e l'indirizzo IP del client sarà nel campo id.orig_h.
- **irc.log:** il campo user contiene il nome utente asserito dal client, e l'indirizzo IP del client sarà nel campo id.orig_h.
- **socks log:** il campo user contiene il nome utente asserito dal client, e l'indirizzo IP del client sarà nel campo id.orig_h.
- **http.log:** il campo username contiene l'username asserito dal client, e l'indirizzo IP del client sarà nel campo id.orig_h, o può essere indicato nel campo proxy se la connessione era attraverso proxy. Se attraverso proxy, il campo id.orig_h conterrà l'indirizzo IP del proxy.
- **ntlm.log:** il campo user contiene il nome utente asserito dal client, e l'indirizzo IP del client sarà nel campo id.orig_h.
- **kerberos.log:** in un ambiente Windows, le richieste kerberos contengono il nome utente nel campo client (eccetto per le richieste in cui il campo client contiene un nome che termina con $, il che significa che l'identità dell'asserente è un dispositivo, e il campo id.orig_h è l'indirizzo IP del dispositivo sorgente. Il campo client è spesso strutturato come USERNAME/EXAMPLEDOMAIN.COM dove USERNAME è il nome utente e EXAMPLEDOMAIN.COM è il nome del dominio Windows e il nome del realm Kerberos.

Qualche parola di avvertimento sul trarre conclusioni sull'identità di una macchina o dell'utente di un dispositivo: conoscete i vostri limiti (e i limiti dei dati). Solo perché un nome utente è stato registrato nel traffico di rete non significa che la persona reale con quel nome sia responsabile - è solo un indizio. Dovreste controllare se l'utente si è autenticato correttamente, dato che le cyberspie e i sabotatori sponsorizzati dallo stato hanno ampiamente sperimentato l'inserimento di false flags.[4] Il nome utente potrebbe essere stato *asserito*, ma se l'autenticazione non è riuscita, non si tratta di un chiaro indicatore che l'utente fosse coinvolto. Non dimenticate che i dispositivi e il software possono memorizzare le credenziali, quindi l'account utente può essere attivo, ma la persona reale potrebbe comunque essere innocente. È necessario continuare a raccogliere informazioni prima di poter confermare un comportamento nefasto.

Ad esempio:

- Un utente va a pranzo e lascia il suo dispositivo sbloccato.
- Un dispositivo è compromesso con un Remote Access Trojan (RAT) e un utente dall'altra parte del mondo sta assumendo surrettiziamente l'identità della nostra vittima, *mentre l'utente originale sta anche lui utilizzando il dispositivo simultaneamente svolgendo la sua attività regolare*
- Un utente malintenzionato all'interno dell'organizzazione ha sentito un collega pronunciare la propria password ad alta voce durante una conversazione, e ora sta cercando di usare tali credenziali per accedere ad altri sistemi

Inoltre, assicuratevi di capire quali pezzi di informazione sono controllati e asseriti dai client o dai server, e considerate chi controlla entrambi. Se un avversario è all'interno della vostra rete, determinare quali informazioni sono affidabili è fondamentale quando si prepara il piano di risposta. Per esempio, un intruso potrebbe disabilitare il DHCP e assegnare staticamente un indirizzo IP ed usarlo per navigare in rete, rendendo difficile l'identificazione, poiché i record del server DHCP fornirebbero informazioni contrastanti. Inoltre, quando un client richiede un indirizzo DHCP, un intruso potrebbe fornire un falso indirizzo MAC. Da qui l'importanza di catturare point-in-time log passivi quando l'evento si è verificato.

Come cacciare TTP specifici

Initial Access (Accesso iniziale)

L'accesso iniziale è quando gli intrusi stabiliscono il loro punto d'appoggio iniziale.

Drive-By Compromise

Un attacco drive-by compromise di solito avviene quando un file viene scaricato surrettiziamente da un sito web che è compromesso. Quando si va a caccia di segni di drive-by compromise nei dati Corelight, il vostro obiettivo principale sono i download da siti esterni.

Iniziate la caccia con il http log e cercate segni di eseguibili scaricati:

1. Inizia con i http log dove resp_fuids non è vuoto. Questo significa che un file è stato restituito dal responder.
2. Se il volume di dati è troppo grande, filtrare i risponder locali (in rete). È possibile filtrare unendo i risultati al conn log sull'uid, quindi filtrando qualsiasi record in cui local_resp sia "true" nel conn log.
3. Esaminare i resp_mime_types dal http log e filtrare i risultati non interessanti (ad esempio, immagini, testo, risposte OCSP e certificati). Spesso i risultati più interessanti sono eseguibili, dll e archivi/contenitori
4. Raggruppare i risultati per i campi host e resp_mime_types per facilitarne l’analisi.

Scansionare i risultati e cercare qualsiasi cosa interessante o strana, come il download di file eseguibili, o la mancata corrispondenza dell'estensione dei file e del mime-type.

Poiché sempre più aggressori iniziano ad usare TLS per crittografare gli scambi tra i client compromessi e i siti web che controllano, ci sarà meno visibilità attraverso il http log. Per recuperare questa visibilità, si può considerare l'uso di una soluzione di decrittografia SSL aziendale e passare il traffico HTTP decrittato al vostro Corelight Sensor.

External Remote Services (Servizi Remoti Esterni)

I servizi remoti esterni sono usati dagli avversari per connettersi alle risorse di rete interne, e la caccia all'uso improprio dei servizi remoti di solito comporta due fasi: scoperta e analisi. Innanzitutto, si deve scoprire quali servizi remoti sono in uso. In primo luogo dovrebbero essere raccolte informazioni sull'inventario dei beni e dei servizi ma, di solito, non sono sufficienti. Spesso, c'è una “deriva” naturale quando i team

IT apportano modifiche all'infrastruttura e lottano per mantenere aggiornata la documentazione delle risorse. Spesso gli utenti autorizzati rendono il tutto più difficile impostando risorse e servizi senza coinvolgere o informare l'IT, un processo noto come “shadow IT”.

Servizi in remoto tradizionali, ad esempio: RDP, VNC (framebuffer remoto) e SSH (secure shell) contengono un componente server e un componente client. Se avete un servizio remoto ospitato nel vostro ambiente, gli aggressori possono sfruttarlo esternamente per compromettere le macchine all'interno della rete. Per identificare questi servizi, cercate le voci del conn log in cui il campo service contiene rfb, rdp, o ssh, e dove local_orig è “false” e local_resp è “true”, o dove l'IP originator (id.orig_h) è esterno e l'IP responder (id.resp_h) è sulla rete dell'organizzazione. Prendete nota di qualsiasi server RFP/VNC, RDP o SSH che accetta connessioni da Internet.

Alcuni servizi remoti funzionano al contrario, dove un agente è installato sul dispositivo locale, e raggiunge dall'interno della rete un insieme di server esterni, per esempio, GoToMyPC e TeamViewer. Questa configurazione è progettata per assistere gli utenti (principalmente gli utenti domestici) che non controllano il NAT o il firewall o non sono abbastanza sofisticati da essere in grado di gestire il port forwarding o le regole del firewall.

Per scoprire se questi servizi remoti sono in uso nel vostro ambiente, cercate segni di connessioni in uscita ai servizi. Per esempio, TeamViewer utilizza la porta TCP 5938 per comunicare con i server TeamViewer, quindi basta esaminare i conn log per le connessioni in cui l'id.resp_p è 5938 e local_orig è “true” e local_resp è “false”. TeamViewer utilizza anche SSL, e il nome di dominio delle connessioni dovrebbe essere *.teamviewer.com, quindi in aggiunta potete cercare voci nel ssl log in cui il server_name contenga, o meglio ancora, finisca con “teamviewer.com”. (Nota: poiché questa sessione funziona al contrario, l'id.orig_h è il dispositivo nella vostra rete su cui è installato il client TeamViewer). Il nostro secondo esempio, GoToMyPC, tenta di contattare poll.gotomypc.com. Esaminate il campo host del http log per poll.gotomypc.com, o le voci nel ssl log in cui il server_name è poll.gotomypc.com. Per ogni pacchetto software client, l’elenco delle porte e dei nomi di dominio varia.

Ora che abbiamo discusso della scoperta dei servizi remoti, dovreste confrontare i dati di Corelight con un elenco di tutti i servizi remoti che il dipartimento IT offre, come ad esempio:

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

Per ogni servizio esposto a Internet, aggregate un elenco di connessioni a quel servizio dal conn log e includete i seguenti campi:

- id.orig_h: Indirizzo IP di origine (client)
- id.resp_h: Indirizzo IP del responder (server)
- id.resp_p: Porta del responder
- servizio: il protocollo dell'applicazione rilevato da Zeek

- cronologia: la cronologia della connessione, ad es. quali tipi di flag TCP sono stati visti
- orig_cc: Il codice paese dell'originator

Quando si filtrano i log, assicurarsi che il campo della cronologia inizi con “Sh”. Per le connessioni TCP questo significa che l'originator ha inviato un SYN e il responder ha risposto con un SYNACK (handshake). Questo controllo elimina le connessioni in cui il server non è in ascolto, o c'è un firewall che blocca la connessione.

Dopo aver raccolto tutti i dati, iniziate a setacciare i log alla ricerca di qualcosa di interessante, come una connessione da un paese non contemplato. Usare l'UID dal conn log per eseguire il follow-up con i log Zeek specifici dell'applicazione (rdp, rfb, ssh). Ad esempio, il registro rdp contiene maggiori dettagli sulla connessione, come il campo cookie che può contenere il nome utente dell'utente che esegue l'autenticazione. L'ultimo passaggio consiste nel verificare con l'utente se in quel momento stava utilizzando attivamente il sistema.

I clienti Corelight hanno accesso alla Encrypted Traffic Collection (ETC) che genera inferenze, o approfondimenti, sul traffico crittografato. Il ssh log contiene informazioni interessanti dedotte dalla connessione SSH, come ad esempio:

- KS per connessioni che sembrano contenere keystroke del cliente
- FU e FD per le connessioni che sembrano contenere un upload o un download di file, rispettivamente
- ABP per le connessioni che sembrano non contenere alcuna autenticazione, ma che hanno comunque successo (“authentication bypass”)
- SV o SC per i client che sembrano essere rispettivamente una versione o una scansione delle capacità

Se volete saperne di più sul Corelight ETC, contattate il nostro team di vendita al (510) 281-0760

Allegato Spearphishing

Come metodo di ingresso in un'organizzazione, un avversario può inviare un allegato maligno ben fatto a un individuo o a un piccolo gruppo in una campagna di spearphishing. L'allegato potrebbe essere un documento che indica all'utente di compiere determinate azioni, come cliccare su un link e/o accedere ad un portale; o potrebbe essere un file creato per sfruttare una vulnerabilità nel software utilizzato per aprirlo, come Adobe Acrobat o Microsoft Word.

Il smtp log di Corelight contiene record nel campo fuids se c'erano dei file allegati ad un messaggio consegnato via SMTP. Questo campo può essere usato per pivotare al files log che contiene informazioni dettagliate sul file, inclusi nome del file, hash e fonte. Ad esempio:

path: smtp
da: Il vostro Amico <Jeremy.Rigeur@gmail.com>
fuid: [Fh5GBc1wdVp3x9MKxc]

mailfrom: attacker@fake-mail.com
rcptto: [victim@corp-mail.com]
oggetto: Sicuramente non uno spear-phish
a: [victim@corp-mail.com]
uid: CzKseq1Y3zo2qsTYH5
user_agent: Apple Mail (2.3608.80.23.2.2)

path: files
conn_uids: [CzKseq1Y3zo2qsTYH5]
nome del file: WIRE_FRAUD.pdf
fuid: Fh5GBc1wdVp3x9MKxc
md5: e71c36cddd2aa42670d89d63e653d1da
mime_type: application/pdf
sha1: bb24829550c0ca17db73d80a1d2f969e3b06ff5f
fonte: SMTP

Per dare la caccia a potenziali tentativi di spearphish, si può cercare nel files log:

1. Il valore nel campo source è SMTP.
2. Filtra tutti i valori mime_type e/o filename non interessanti, come menzionato in precedenza.
3. Usare l'hash (MD5, SHA1, o SHA256) con un servizio di file reputation (come Virustotal) per cercare file maligni conosciuti.

Inoltre, si può partire dal smtp log:

1. Per ridurre i dati cercare le voci in cui il campo fuids non sia vuoto.
2. Filtrare le combinazioni note di valori mailfrom e from.
3. Filtrare i valori di oggetto non interessanti.
4. Considerare l'utilizzo del valore fuid dai record rimanenti per pivotare sul files log al fine di ottenere maggiori informazioni sul file.

Corelight può eseguire l'estrazione di file ad alta velocità e può filtrare in base al tipo MIME, quindi tutti i file interessanti, come gli eseguibili, i documenti Office e i PDF sono disponibili per un esame più approfondito, se desiderato.

Gran parte della posta che attraversa internet oggi è criptata tramite STARTTLS sul protocollo SMTP, e questo ne ostacola la visibilità. Per ottenere una migliore visibilità senza sacrificare la privacy e la sicurezza per i vostri utenti, è una buona pratica accettare SMTP in entrata in un sistema che supporta STARTTLS, poi fare il proxy della posta al sistema di posta interno, in modo che Corelight possa generare i log corrispondenti.

Link Spearphishing

Invece di inviare file a un'organizzazione dove possono essere esaminati da un filtro di posta aziendale, alcuni avversari inviano e-mail che contengono solo link. Questi link portano a siti web che sono controllati dall'attaccante, e tentano di ingannare l'utente:

- Inserendo credenziali che gli aggressori raccolgono
- Sfruttando una vulnerabilità nel browser dell'utente
- Scaricando un file per sfruttare un'altra applicazione sul dispositivo dell'utente

Corelight Sensors dispone di un pacchetto[5] che può registrare i collegamenti dai messaggi SMTP in un log separato, il smtp_links log. Questo log contiene un campo fuid, che collega il smtp_links log al smtp log. È possibile passare rapidamente al smtp log con i dettagli sul messaggio che ha consegnato il link dannoso.
Ad esempio:

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
da: Il vostro Amico <Jeremy.Rigeur@gmail.com>
fuid: [FhahXA1eJ32gHvNP27]
mailfrom: attacker@fake-mail.com
rcptto: [victim@corp-mail.com]
oggetto: Si prega di cliccare su questi link
a: [victim@corp-mail.com]
uid: C62txO1FHoJFJpsgP1
user_agent: Apple Mail (2.3608.80.23.2.2)

Per andare a caccia di link di spearphishing, iniziare con il smtp_links log ed esaminare il campo dei link, filtrando i domini benigni fino a trovare risultati interessanti. Un'altra opzione è quella di unire smtp_links log al smtp log attraverso il campo fuid o uid, e filtrare le combinazioni benigne dei campi mailfrom (posta da) e from (da) per cercare messaggi da mittenti unici.

Anche se gran parte della posta che attraversa internet oggi è criptata tramite STARTTLS su SMTP. Per ottenere una migliore visibilità senza sacrificare la privacy e la sicurezza per i vostri utenti, è una buona pratica accettare SMTP in entrata in un sistema che supporta STARTTLS, poi fare il proxy della posta al sistema di posta interno, in modo che una soluzione Corelight possa generare i log corrispondenti.

Execution (Esecuzione)

L'avversario sta cercando di eseguire un codice maligno.

Command Line Interface, PowerShell

Lo scripting dell'interfaccia a riga di comando è stato a lungo utilizzato per gestire sistemi basati su *nix, e la capacità di costruire ed eseguire script è spesso sfruttata dagli attaccanti. Per anni non c'è stato un equivalente disponibile su Windows, e nei primi anni 2000 Microsoft ha iniziato a sviluppare un nuovo approccio alla gestione della riga di comando. Poco dopo, fu creato PowerShell (PS) 1.0. PS, nelle sue varie iterazioni, è uno strumento integrato basato sul framework .NET che viene utilizzato per automatizzare i compiti di amministrazione del sistema. Fornisce un'interfaccia per consentire agli utenti di accedere ai servizi del sistema operativo Windows.

Nonostante alcuni comandi PS siano limitati per impostazione predefinita, molti comandi sono disponibili per ottenere informazioni sul sistema senza un file eseguibile. Potete usare le estensioni LNK per bypassare le protezioni ed eseguire uno script PS. I file LNK sono di solito visti come scorciatoie, generalmente si trovano sul desktop e nel menu di avvio degli utenti.

I file LNK dannosi sono spesso incorporati in quelli che sembrano essere documenti o immagini legittime. Una volta aperto, l'LNK esegue un'applicazione Windows legittima CMD.exe o MSHTA.exe per aggirare le impostazioni di sicurezza.

Le capacità di estrazione dei file di Corelight e l'integrazione con varie piattaforme intel forniscono informazioni sul malware offuscato dal tipo di file. Utilizzando il filtraggio integrato di Corelight, è possibile regolare i parametri di estrazione dei file per mirare a specifici mime-type che sono comunemente utilizzati per la consegna di malware, tra cui:

- File compressi
- Microsoft Office (Word, PowerPoint, ecc.)
- File PDF
- File TXT (powershell, vbs)

Persistence (Persistenza)

Persistenza è l'avversario che cerca di mantenere il proprio punto d'appoggio.

BITS Jobs

Microsoft Background Intelligent Transfer Service (BITS) è stato creato nel 2001 come un meccanismo di gestione dei trasferimenti di file che riduce al minimo le interruzioni per l'utente finale. BITS è comunemente usato per scaricare gli aggiornamenti di Windows e altri aggiornamenti software dai principali fornitori.

Gli attaccanti dispongono di due metodi per abusare dei BITS:

- Il più comune consiste nel creare un processo di trasferimento BITS direttamente su un host, consentendo il download di payload secondari tramite un servizio Windows integrato che, in genere, ignora i firewall e altri controlli di sicurezza.
- Un'altra alternativa consiste nell'esfiltrare i dati tramite un processo di caricamento BITS. Gli upload devono connettersi ad un server IIS affinché BITS funzioni correttamente, ma questo requisito è facilmente sovvertibile dagli autori di malware.

I trasferimenti di dati utilizzando il servizio BITS possono avvenire su HTTP, SSL e SMB. Quando BITS utilizza il traffico HTTP, esiste una stringa User-Agent distintiva di “Microsoft BITS/7.5” (o 7.8 nelle versioni successive). Purtroppo, non ci sono caratteristiche distintive del traffico di rete BITS SSL e SMB. Pertanto, la presenza di traffico di rete BITS non è necessariamente sospetta, perché è presente ovunque i computer Windows siano connessi a Internet. Gli analisti possono ancora utilizzare i dati Corelight per valutare se il traffico BITS è legittimo, analizzando i sistemi remoti utilizzati per i trasferimenti di dati BITS. Se sono al di fuori dei CDN o delle reti dei principali fornitori di software, tutti i caricamenti di BITS dovrebbero essere indagati fino a quando non si dimostrino benigni, poiché questo caso d'uso è particolarmente raro tra i fornitori di software legittimi.

L'esempio di codice riportato di seguito è un http log che mostra l'aspetto dei dati BITS se è su HTTP.

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

External Remote Services (Servizi Remoti Esterni)

- Vedi *Initial Access: External Remote Services*

Port Knocking (Bussare alla porta)

Il port knocking è una tecnica per far sì che un sistema remoto permetta l'accesso a una porta altrimenti chiusa. Tipicamente consiste in una sequenza predefinita di connessioni ad altre porte (spesso chiuse), a volte con speciali flag a livello di protocollo, stringhe di banner Layer 7, ecc.

Zeek riassume ogni connessione TCP, UDP e ICMP nel conn log. Questo registro dettagliato fornisce utili statistiche sulle connessioni. I campi history, conn_state, e network tuple (src/dest ip/port) forniscono le informazioni necessarie per rilevare il port knocking. È importante notare che l'avvistamento di port knocking senza un ulteriore suggerimento può essere un compito scoraggiante, poiché è facile nascondere sequenze intenzionali di connessioni tra il rumore di una tipica rete.

Server Software Component (Componente software del server): Web Shell

Una web shell è un'implementazione basata sul web di una shell di comando. Una web shell è generalmente una pagina web dannosa o un frammento di codice introdotto in un web server o un'applicazione esistente per fornire un accesso non autorizzato. Questo accesso può essere una vera e propria CLI

shell, uno strumento di gestione dei file o di accesso al database. Questa è una tattica comune perché il traffico maligno si mescola con il traffico benigno da e verso il server web, e può essere difficile da identificare tramite le firme IDS perché le specifiche della web shell sono facilmente modificabili.

Quando una web shell viene eseguita, viene eseguita con i permessi dell'utente del software del server web, che dovrebbero essere limitati. Gli aggressori usano le web shell per tentare attacchi di escalation dei privilegi sfruttando le vulnerabilità locali del sistema per assumere privilegi di root.

Rilevare le web shell sulla rete utilizzando i rilevamenti basati sulle firme è relativamente semplice - le web shell hanno specifici file path, metodi di comunicazione o altri comportamenti che possono far scattare l'allarme. Come la maggior parte degli IOC 'atomici', sono facili da eludere perché identificano comportamenti specifici che possono essere facilmente modificati. Dove possibile, si dovrebbe integrare il rilevamento delle firme con un programma di caccia alle minacce per trovare comportamenti più generali di attività anomale.

Le web shell tentano di nascondere l'attività malevola nel normale traffico HTTP, quindi l'http.log è un'eccellente fonte di dati per indagare sull'attività delle web shell. Esempi di ipotesi di caccia supportate dai dati HTTP di Corelight sono:

- Attività insolita HTTP POST. Questo può essere semplice come POST HTTP imprevisti nel campo 'metodo' del http.log dove sono previsti GET (se il sito interessato serve principalmente contenuti).

Il traffico web 'normale' viaggia verso una shortlist di pagine comuni, con navigazione tramite un collegamento ipertestuale interno. Una web shell va direttamente alla pagina nascosta e appare come una richiesta HTTP senza pagina di riferimento. Inoltre, il traffico web mostra una varietà di IP richiedenti, stringhe user-agent, JA3 e così via. Una web shell può avere un gruppo di utenti più omogeneo.

- Individuare gli accessi sospetti provenienti da sottoreti interne ai server DMZ e viceversa.

Questo tipo di analisi di caccia e rilevamento di anomalie è un modo efficace per identificare attività malevole (o sospette), ma le reti moderne sono luoghi rumorosi e caotici. Come per la maggior parte delle cacce, bisogna sapere come sono i dati 'normali' in modo da poterli filtrare con successo.
(https://github.com/nsacyber/Mitigating-Web-Shells)

Defense Evasion (Evasione della difesa)

L'evasione della difesa consiste in tecniche che gli avversari utilizzano per evitare di essere scoperti durante le loro azioni.

BITS Jobs

- Vedi *Persistence: BITS Jobs*

Port Knocking (Bussare alla porta)

- Vedi *Persistence: Port Knocking*

Install root certificate (Installare Certificato radice)

I certificati radice sono utilizzati per stabilire comunicazioni sicure TLS/SSL. I certificati radice sono usati per identificare l'autorità di certificazione radice (CA). I certificati radice sono autofirmati e formano un'ancora di fiducia per la crittografia a chiave pubblica. Ad esempio, quando un root certificate è installato, il sistema o l'applicazione riterrà attendibili i certificati nella catena di attendibilità del root. Mentre nessun dispositivo a livello di rete (ad esempio, router e switch) può mostrare la catena di certificati installati su un sistema client, lo scopo di installare un certificato root malevolo è quello di bypassare la convalida di attendibilità.

Utilizzando i dati di Corelight, è possibile osservare tutti gli aspetti della sessione TLS/SSL utilizzando gli ssl log e x509. Questi due log permettono agli analisti di identificare i certificati che sembrano sospetti:

1. Cercando nel ssl log tutte le voci in cui il campo validation_status non ha un valore “ok”.
2. Rivedendo i record in cui il campo validation_status ha un certificato autofirmato o contiene un certificato autofirmato nella catena dei certificati.
3. Esaminando i campi subject e server_name per determinare la probabile organizzazione o sito web che controlla il server.
4. Filtrando i risultati in cui sono in uso certificati autofirmati legittimi, come nelle comunicazioni tra i dispositivi IOT e l'infrastruttura cloud di supporto.
5. Indagando l'indirizzo IP id.resp_h per vedere a quale sistema autonomo appartiene la sessione e se si tratta di un'organizzazione AS ragionevole (come l'organizzazione che corrisponde alle informazioni sul server, o un provider di cloud hosting abitualmente usato).
6. Per le connessioni rimanenti, usare i valori in cert_chain_fuids per eseguire il pivot ai certificati nel x509 log e rivedere i dettagli del certificato.

Incentrare le indagini ispezionando l'autorità di certificazione radice locale sull'endpoint.

Credential Access (Accesso alle Credenziali)

L'accesso alle credenziali è quando l'avversario cerca di rubare nomi di account e password.

Brute Force (attacco di forza bruta)

Un avversario cerca di ottenere un accesso non autorizzato cercando di indovinare sistematicamente la password di un utente utilizzando un meccanismo ripetitivo o iterativo. A volte un attacco di forza bruta ha origine da un elenco di informazioni note, aumentando le probabilità di successo.

Per esempio, un utente malintenzionato che tenti di indovinare la password di un account Active Directory probabilmente si traduce in molte connessioni ad un controller di dominio sulla porta LDAP (389 o 636). Un utente malintenzionato che tenti di scoprire gli URL API in un sistema di e-commerce genera molte

più connessioni al web server rispetto agli altri client in un periodo di tempo simile e crea più codici di stato HTTP nell'intervallo 400 e 500 (errori) rispetto agli altri client.

Per cercare un attacco di forza bruta:

1. Nel conn log, aggregare per id.orig_h, id.resp_h, id.resp_p, proto e (opzionalmente) service.
2. Aggiungere un conteggio per il numero di operazioni e ordinare per i conteggi più alti.
3. Scegliere un periodo di tempo che abbia senso, in base alle dimensioni della rete/del set di dati, iniziando in piccolo e aumentando gradualmente.
4. Filtrare i record che sono ovviamente ammissibili, come i contatti ripetuti dai sistemi di monitoraggio delle prestazioni di rete o delle applicazioni, i sistemi di gestione delle vulnerabilità o le applicazioni aziendali.
5. Per i record sconosciuti o sospetti, eseguire un'indagine più approfondita su tale comportamento. Per esempio, cercare altre connessioni originate dall'indirizzo IP remoto.
6. Per i protocolli in grado di mantenere le connessioni su più transazioni o tentativi, cercare connessioni di lunga durata. Queste connessioni di lunga durata possono anche indicare comportamenti ripetitivi.

I sensori Corelight includono uno script che registra le connessioni che sono mantenute per più di una serie di soglie, a partire da dieci minuti fino a tre giorni. Se non siete clienti di Corelight, ma usate Zeek open source, questo script è disponibile attraverso Corelight GitHub page.

Per cercare connessioni lunghe con il pacchetto Long Connections installato:

1. Esaminare il notice log.
2. Esaminate le voci per le quali la nota è "LongConnection::found,".
3. Esaminate ogni set di id.orig_h, id.resp_h, id.resp_p per capire se questi dispositivi devono avere connessioni lunghe.

Per cercare connessioni lunghe senza il pacchetto Long Connections installato:

1. Esaminare il conn log.
2. Riunire un elenco di tutte le connessioni con i seguenti campi per ciascuna: id.orig_h, id.resp_h, id.resp_p, proto, service e duration. Questo include solo le connessioni che sono state completate, correttamente o tramite timeout. Le connessioni attualmente aperte non sono rappresentate nei risultati.
3. Ordinare i risultati per durata, collocando le connessioni più lunghe in cima.
4. Esaminare ogni risultato per determinare se si tratta di un comportamento legittimo o atteso.
5. Filtrare i comportamenti attesi e indagare in profondità su tutto ciò che sembra sospetto.

Corelight offre anche la Encrypted Traffic Collection (ETC), che cerca automaticamente i tentativi di indovinare la password con la forza bruta contro i server SSH all'interno di una singola connessione.

Forced Authentication (autenticazione forzata)

Alcuni protocolli si autenticano automaticamente quando un utente accede ad una risorsa senza prima controllare se la risorsa a cui si accede è affidabile. Per esempio, un utente malintenzionato può

incorporare un riferimento in un documento di Microsoft Office a un file che è ospitato su un percorso UNC controllato dall'utente malintenzionato (\servername\sharename\path\tofile). Quando l'utente apre il file, la macchina tenta di accedere alla risorsa. Il server controllato dall'attaccante quindi sfida la macchina per l'autenticazione, e nella maggior parte dei casi, la macchina vittima fornisce automaticamente le credenziali memorizzate nella cache, di solito sotto forma di un hash NTLM. L'attaccante può quindi tentare di utilizzare le credenziali per un accesso non autorizzato, di solito attraverso l'inversione dell'hash per ottenere la password, o riutilizzando l'hash in un attacco pass-the-hash.

Questo metodo richiede che l'attaccante controlli l'infrastruttura del server. Di conseguenza, il vettore di attacco più probabile è lo spearphishing. L'attaccante esegue il phishing di un utente sulla rete, e la macchina vittima raggiunge il server controllato dall'attaccante attraverso internet. Per dare la caccia a questo comportamento, cercare l'autenticazione su internet:

1. Guardare nel ntlm log cercando eventuali segni di autenticazione NTLM in cui l'IP di destinazione sia sulla rete esterna.
2. Cercare voci nel conn log in cui il campo service contenga smb (e/o ntlm), e local_resp sia “false”.

Nel LLMNR or NBT-NS poisoning, un attaccante ascolta le trasmissioni locali LLMNR o NBT-NS richiedendo una particolare risorsa per nome. L'attaccante quindi risponde al client che lo interroga mimando la risorsa reale. Se la risorsa è una che di solito richiede l'autenticazione, l'attaccante può richiedere l'autenticazione al client. Quando il client si autentica, di solito con un password hash, l'attaccante utilizza le credenziali per impersonare il client e accedere alle risorse.

Si può effettivamente dare la caccia a questi attacchi con i dati Corelight, ma il sensore deve essere all'interno del dominio di trasmissione perché, normalmente, il traffico di trasmissione non attraversa i router. In genere è necessario estendere o effettuare il mirroring di intere VLAN, o inoltrare il traffico LLMNR o NBT-NS dalle sottoreti e VLAN dei client a punti della rete monitorati da Corelight.

Cercare i dns log dove id.resp_p=5355 (LLMNR) o id.resp_p=137 (NBT-NS), e filtrare i record dove il campo answers non è vuoto. Quindi contate il numero dei distinti campi di query per id.resp_h. Questa ricerca produce IP che rispondono a più di un nome.

Network Sniffing

Non potete rilevare un intruso che sta ‘sniffando’ il traffico sulla vostra rete usando i network log (log di rete) perché l'azione è invisibile; tuttavia, *potete rilevare un intruso ‘sniffando’ voi stessi la vostra rete* perché il vostro avversario non può vederlo.

Corelight Sensors consente di distribuire una griglia di sensori fuori banda che genera log collegati. Questi log accelerano l'osservazione e il rilevamento affidabili e aiutano a evitare la trappola della dipendenza dalla prevenzione, fornendo al contempo un contesto per un'analisi storica più profonda e accurata. Come Rob Joyce, capo della divisione Tailored Access Operations della NSA, ha affermato nel suo

discorso di USENIX del 2016: “Stiamo “ “sfruttando” (Exploit in inglese)” lo stato-nazione... cosa potete fare per difendervi, per rendermi la vita difficile?”

Discovery (Scoperta)

L'avversario sta cercando di conoscere il vostro ambiente.

Network Service Scanning

Per determinare quali dispositivi su una rete possono essere colpiti da “exploit” e i servizi disponibili su tali dispositivi, un intruso può utilizzare la scansione attiva. I metodi di scansione attiva includono:

- Scansione orizzontale: Invio di richieste di connessione ad una porta specifica attraverso più IP per vedere quali IP rispondono. Per esempio, la scansione di molti dispositivi sulla porta TCP/22 rivela tipicamente i dispositivi che utilizzano un server SSH. La scansione su molti dispositivi sulla porta TCP/445 può efficacemente enumerare l'infrastruttura Windows.
- Scansione verticale: Invio di richieste di connessione ad un indirizzo IP specifico attraverso più porte per vedere quali porte rispondono. Questo metodo permette agli aggressori di dedurre i servizi disponibili da quell'indirizzo IP.

Ognuno di questi metodi può essere eseguito utilizzando uno scanner di vulnerabilità gratuito o disponibile in commercio. Questi prodotti spesso aggiungono altra logica per controllare la disponibilità del servizio, informazioni sulla versione e se i servizi sono vulnerabili, a tecniche di sfruttamento note.

Se un intruso usa uno o più dei metodi di cui sopra per tentare di scoprire un servizio, il sottoprodotto è una connessione *failed* (fallita) o *rejected* (rifiutata). Nei dati Corelight, queste sono registrate nel conn log come connessioni con un conn_state di S0 (iniziato, e ignorato) o REJ (iniziato, e rifiutato), e tipicamente hanno un campo cronologia dove non c'è ‘D’ (dati post-syn dall'iniziatore). Per cercare la scansione dei servizi di rete interni alla rete:

1. Cercare le entrate nel conn log in cui conn_state sia S0 REJ.
2. Filtrare cercando record in cui local_orig=true e local_resp=true.
3. Raggruppare e contare i risultati per l'id.orig_h, e il numero di id.resp_p unici, per valutare l'orizzontalità/verticalità della scansione.
4. Ispezionare l'elenco, iniziando dai record che hanno il maggior numero di id.resp_h o id.resp_p.
5. Identificare l'originator (id.orig_h) ed esaminare l'elenco dei responder (id.resp_h) e delle porte (id.resp_p).
6. Determinare se il comportamento è accettabile in base all'identità della fonte, le porte coinvolte e le destinazioni.

Non tutte le voci della lista sono maligne. I server DHCP, per esempio, sono comunemente configurati per eseguire il ping di un indirizzo IP per confermare se l'indirizzo è in uso prima di assegnarlo dal pool. I server di stampa con un gran numero di code di stampa tentano i servizi di stampa SNMP e/o di rete sulle stampanti, anche se queste stampanti sono offline. Per questo motivo, i server di stampa possono causare un gran numero di connessioni S0. Naturalmente, nell’elenco potrebbe apparire il software che scansiona legittimamente, come uno scanner di vulnerabilità approvato dall'azienda o un sistema di gestione dell'inventario. Infine, gli ingegneri di rete eseguono una scansione della rete ad-hoc per la risoluzione dei problemi. Se vi imbattete in una scansione di rete, modificate la query originale per omettere i record noti come benigni e poi riprendete la caccia.

Network Share Discovery

Il protocollo di condivisione di rete più comunemente abusato dagli attaccanti è SMB, lo standard per la condivisione di file di Windows. SMB è supportato da ogni sistema operativo moderno. I documenti di alto valore che archiviano PII, segreti commerciali, diagrammi di rete e altri dati sensibili, in genere risiedono su condivisioni SMB in aziende di tutte le dimensioni.

La scansione e il rilevamento delle condivisioni su un server SMB viene in genere eseguita utilizzando un comando DCE/RPC sulla porta TCP 445. In particolare, una connessione alla pipe "srvsvc" - che appare nei dce_rpc log come un endpoint con lo stesso nome - è seguita da una chiamata alle funzioni NetShareEnumAll o NetShareEnum (chiamate “operazioni” nel log di Zeek). Queste "function calls " (chiamate di funzione) sono utilizzate per scopi legittimi di condivisione di file, e prese da sole non sono indicatori sufficienti di un intento malevolo. Tuttavia, in combinazione con altri indicatori di movimento laterale, illustrano come un attaccante si sia spostato lateralmente all'interno di una rete. Gli obiettivi principali per ulteriori indagini sono quelli che generano un gran numero di chiamate di funzioni DCE_RPC su un gran numero di host in un breve periodo.

Network Sniffing (X-reference)

- Vedi Credential Access: Network Sniffing

Remote System Discovery

Gli stessi principi per il rilevamento di Network Service Scanning si applicano al rilevamento di Remote System Discovery. Vedi questa sezione per maggiori informazioni.

Lateral Movement (Movimento laterale)

Il movimento laterale è quello che gli avversari usano per entrare e controllare i sistemi remoti di una rete.

Remote Desktop Protocol (Protocollo di Desktoo remoto)

Il protocollo RDP (Remote Desktop Protocol) di Microsoft è usato per controllare a distanza un endpoint Windows. Questo protocollo può essere abusato da un utente malintenzionato per ottenere un accesso non autorizzato alla vostra rete (vedere Initial Access: External Remote Services). Una volta che un intruso è dentro, può usare RDP per muoversi lateralmente tra i dispositivi.

RDP è uno dei molti protocolli analizzati da Corelight. Per alcuni ambienti, la presenza di RDP, o la sua presenza su sistemi specifici, è sufficiente per avviare un'indagine. Per le reti in cui RDP è consentito, il log di Zeek RDP è ricco di informazioni che aiutano a stabilire se una connessione è legittima, per esempio, registrando dati come il layout della tastiera, i livelli di crittografia, o il nome del client per una connessione.

Quando si caccia con il rdp log:

1. Concentrarsi sui campi id.orig_h, id.resp_h, id.resp_p e cookie. Il campo cookie può contenere qualsiasi valore arbitrario inviato dal client RDP al server, ma spesso contiene il nome utente inviato dal client RDP.
2. Aggregare i record in base a questi quattro campi e mostrare un conteggio per ogni set univoco.
3. Iterare attraverso l'insieme e identificare l'origine e la destinazione di ogni connessione (ad esempio, potete usare i record dai log DNS e DHCP).
4. Alcune connessioni RDP useranno un layout di tastiera non standard. Per cercarlo, esaminare il campo keyboard_layout. Contare il numero di istanze di ciascun valore e applicare il *data stacking* per cercare valori anomali o che si verificano raramente.
5. Identificare l'origine e la destinazione e determinare se il layout di tastiera non standard è previsto, per esempio, se l'utente di origine è noto per avere una lingua non inglese come lingua principale, e quella lingua è la lingua richiesta nella connessione RDP.

Dopo aver ottenuto queste informazioni, porre diverse domande:

- Il valore del cookie corrisponde all'utente previsto sul computer di origine o di destinazione?
- C'è una ragione legittima per cui l'originator sta usando RDP?
- Esistono degli utenti che utilizzano RDP e che non dovrebbero usarlo per le loro mansioni?

Remote Services (Servizi Remoti)

Lo sfruttamento di una vulnerabilità del software si verifica quando un avversario approfitta di un errore di programmazione per eseguire adversary-controlled code (codice controllato dall'avversario). Questo può avvenire in un programma, un servizio o all'interno del software del sistema operativo o del kernel stesso. Un obiettivo comune per lo sfruttamento post-compromissione dei servizi remoti è il movimento laterale.

Data la complessità delle reti aziendali odierne, viene spesso utilizzata una varietà di servizi di terze parti ed esterni. Questi servizi permettono agli aggressori di ottenere un accesso iniziale o di muoversi lateralmente. Tutte le connessioni sono registrate all'interno di conn.log, tuttavia, maggiori dettagli possono essere disponibili nei log specifici del protocollo a seconda della natura del servizio remoto oggetto dell'attacco. Per esempio, è possibile monitorare il file http.log per richieste HTTP sospette e inaspettate (come le richieste OPTIONS).

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

version: 1.1,

Inoltre, Corelight estrae informazioni sul software osservato sulla rete nel software.log. Questo file fornisce ai difensori dati preziosi per monitorare server imprevisti o non autorizzati, servizi vulnerabili o non aggiornati e software client senza patch.

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

Windows Admin Shares

I sistemi Windows hanno condivisioni di rete nascoste che sono accessibili solo agli amministratori e forniscono la possibilità di copiare file a distanza e altre funzioni amministrative. Esempi di condivisioni di rete includono C$, ADMIN$ e IPC$.

Gli attaccanti spesso usano SMB per connettersi alle condivisioni amministrative su workstation e server Microsoft Windows. Può essere che vogliano saperne di più sul target, estrarre file sensibili, caricare payloads maligni, o autenticarsi in modo da poter porre in atto ulteriori strumenti e attacchi. Corelight monitora il traffico SMB, compresi i tentativi di autenticazione, consentendo ai difensori di registrare e notare i modelli di tentativi di autenticazione amministrativa, nonché di monitorare il traffico SMB per estrarre i file trasferiti. L'esempio seguente dimostra che l'azione FILE_OPEN viene eseguita utilizzando la condivisione admin nascosta e include le informazioni MAC. Corelight registra l'azione eseguita, incluso Open/Rename/Delete/Write.

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

Collection (Raccolta)

L'avversario sta cercando di raccogliere dati per raggiungere il suo obiettivo.

Archive Collected Data (Dati di Archivi raccolti)

Per nascondere i dati, gli aggressori possono consolidare i dati in file di archivio compressi, come i file Zip, RAR, TAR o CAB. Per cercare questa tecnica di offuscamento, usate il files log.

Per cercare i file compressi:

1. Cercare tutti i files log, recuperando i campi tx_hosts, rx_hosts, mime_type, total_bytes e source.
2. Rimuovere i record con mime_types non interessanti dai risultati, per esempio:
   a. application/x-x509-*
   b. application/ocsp*
   c. image/*
   d. audio/*
   e. video/*
   f. text/*
   g. application/xml
   h. application/chrome-ext

Automated Collection (Raccolta automatica)

Gli aggressori possono implementare strumenti automatizzati su un host compromesso per monitorare i servizi intranet alla ricerca di dati sensibili e segreti aziendali. Questi strumenti possono includere script per cercare (e copiare) informazioni come il tipo di file, la posizione o il nome a intervalli di tempo specifici. Gli intrusi possono utilizzare strumenti di accesso remoto per condurre raccolte automatizzate.

Per esempio, uno strumento personalizzato può interrogare un web server intranet o un server di posta elettronica interno, eseguendo regolarmente il polling per nuovi contenuti. Corelight monitora più protocolli tra cui HTTP, e-mail, MySQL, FTP e traffico SMB per fornire una visione di queste query.

Nella caccia all'uso della raccolta automatizzata, i difensori possono identificare gli strumenti automatizzati osservando le query ripetitive o le connessioni regolarmente programmate. Ad esempio, se un intruso sta effettuando il web scraping, ci sarà un gran numero di connessioni da un numero finito di indirizzi IP. Inoltre, è possibile utilizzare i SMB log (smb_files o smb_mapping) per identificare modelli di traffico anomali.

Data From Network Shared Drive (dati da drive condiviso in rete)

Le unità condivise in rete sono un tesoro di documenti aziendali sensibili. La maggior parte delle reti aziendali ospita unità di rete condivise usando SMB, ma alcune possono affidarsi a FTP, HTTP o anche

RDP. Zeek può monitorare l'accesso alle unità di rete condivise quando vengono utilizzati protocolli come SMB, FTP o HTTP. I protocolli di controllo remoto, come RDP, sono anche analizzati nei log specifici del protocollo. Ovunque Corelight veda questo traffico, viene monitorato e registrato nel log specifico del protocollo.

L'esempio seguente mostra il ftp log. Corelight registra il comando e gli argomenti.

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 (Comando e Controllo)

L'avversario sta cercando di comunicare con i sistemi compromessi per controllarli.

Commonly Used Ports/Non-Standard Ports (Porte comunemente usate/ Porte non standard)

Gli avversari possono usare una porta comunemente usata per evitare un'ispezione più dettagliata.

La ricerca dei canali C2 sulle porte comunemente utilizzate è difficile, ma non impossibile. Per cercare i canali C2, cercare le porte ben note che vengono utilizzate con un servizio non comune.

Quando si va a caccia di C2 usando porte comunemente usate:

1. Inizialmente conviene concentrarsi sul campo del servizio, e cercare nel conn log le voci in cui il campo del servizio non è quello che ci aspetterebbe per la porta standard (il campo del servizio potrebbe essere un '-' o un altro servizio).
   a. Iniziare con i protocolli più tipici:
      - TCP:80 (HTTP) TCP:443 (HTTPS)
      - TCP:25 (SMTP)
      - TCP/UDP:53 (DNS)
2. La Encrypted Traffic Collection di Corelight contiene un pacchetto intitolato Encryption Detection. Encryption Detection genera un avviso quando viene rilevato traffico di testo in chiaro su porte solitamente crittografate. Osservare gli avvisi per Viz::UnencryptedService evidenzia questo

comportamento e aiuta ad identificare le connessioni potenzialmente dannose che utilizzano porte comuni.

Il pacchetto Corelight Encrypted Traffic Collection ha anche una funzione che notifica quando una sessione usa la crittografia istantanea. Il pacchetto cerca chiavi pre-condivise o connessioni criptate che iniziano senza una tradizionale negoziazione di chiavi. Osservare gli avvisi per Viz::CustomCrypto evidenzia questo comportamento e aiuta ad identificare le connessioni potenzialmente dannose che utilizzano porte comuni.

Inoltre, è possibile utilizzare i log di Corelight dpd e weird per identificare il comportamento inaspettato del protocollo. Questi registri mostrano errori di debug e parsing e identificano l'uso fuori specifica di porte e protocolli comuni - che potrebbero indicare attività malevole o l'uso nascosto di porte e protocolli conosciuti.

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

Encrypted Channel (Canali Encriptati)

Per l'uso di protocolli personalizzati su porte standard, vedere la sezione Commonly Used Ports/Non Standard Ports per una descrizione del pacchetto Encryption Detection di Corelight, il dpd log e il weird log. Questi aiutano a identificare potenziali protocolli crittografici personalizzati.

Fallback Channels, Multi-Stage Channels (Canali Fallback, Canali Multistage)

È noto che gli avversari suddividono le comunicazioni tra protocolli diversi, utilizzandone uno per C2 in entrata e un altro per i dati in uscita. Questo permette alla comunicazione di aggirare le restrizioni del firewall.

Il malware che divide la comunicazione tra due host per le istruzioni e per l'esfiltrazione introduce una nuova sfida per i difensori. Riconoscere il legame tra traffico di controllo sospetto e grandi trasferimenti di dati è impegnativo, ma Zeek fornisce pacchetti e framework che sintetizzano i dati. Ad esempio, esiste un pacchetto per determinare il rapporto produttore-consumatore per le connessioni che identifica i trasferimenti di dati sbilanciati e possibilmente sospetti. Inoltre, l'Intelligence Framework permette il coordinamento con altri difensori identificando possibili indicatori di compromissione (indirizzi IP, indirizzi e-mail e nomi di dominio) nei dati Corelight.

È difficile correlare gli aggressori utilizzando diversi metodi e canali di comunicazione, ma i contenuti Corelight, insieme ai framework e ai pacchetti Zeek, possono aiutare. Permettono ai difensori di identificare i canali nascosti in modo discreto, fornendo molteplici opportunità di rilevamento.

Oltre a osservare i meccanismi di comunicazione C2 menzionati in precedenza, ecco alcuni altri segnali disponibili nei dati Corelight:

- Usare conn.log per identificare i modelli di comunicazione che indicano canali aggiuntivi (per esempio, usando orig_h e resp_h per restringere le connessioni a una finestra temporale e osservare le connessioni tra gli host che includono porte inconsuete, connessioni fallite o rifiutate, o elementi interessanti/sospetti).
- Usare Corelight (ETC), o contenuto auto-sviluppato, in combinazione con il rilevamento del conn log per trovare potenziali relazioni tra connessioni sovrapposte, adiacenti o interessanti.
- Cercare sequenze di connessioni a host non correlati usando diversi protocolli o eventi nei log di dpd e weird come descritto in Commonly Used Ports.

Ingress Tool Transfer (Trasferimento di Strumenti di Ingresso)

Gli intrusi tipicamente spostano i file su sistemi compromessi, entrambi strumenti che possono aiutare con ulteriori movimenti laterali e/o file sensibili progettati per l'esfiltrazione. Questi file si muovono tipicamente su una connessione HTTP(S), SSH o SMB.

Per i file che si spostano su HTTP in chiaro, dettagli come il nome dell'host remoto e il nome e il mime-type del file che viene trasferito possono essere indicatori utili; gli utenti dovrebbero anche consultare il files log cercando gli hash dei file che vengono spostati, poiché molti strumenti di attacco popolari hanno hash crittografici noti che ne rendono facile l'identificazione. Nel caso di HTTPS, i difensori possono usare l'indirizzo IP del sistema remoto, così come i dettagli del certificato annotati nel ssl log (cioè, nome dell'organizzazione, FQDN dell'host remoto dal CN, ecc.) per cercare delle connessioni anomale.

Gli intrusi copiano i file da un endpoint all'altro mentre si spostano lateralmente tra le risorse compromesse. Tradizionalmente, le copie di file da o verso sistemi Unix/Linux avvengono tramite il protocollo SSH usando il comando scp. Per i sistemi Windows, l'upload o il download di file remoti avviene tipicamente su SMB, ma può anche usare SSH via PUTTY.

Corelight Sensors con il pacchetto ETC SSH inferences abilitato estende il ssh log. L'estensione include un campo inferenze che aggiunge caratteristiche dedotte sul traffico SSH. Per esempio, se la sessione viene utilizzata per spostare file o se è interattiva:

- LFU: Large File Upload (Caricamento di file di grandi dimensioni)
- LFD: Large File Download (Download di file di grandi dimensioni)
- KS: Keystrokes

Per iniziare a cercare sessioni SSH interessanti usare il campo inferenze nel pacchetto ETC SSH:

1. Identificare le sessioni in cui il campo inferenze contiene LFU, SFU, LFD o SFD
2. Determinare se l'attività dei file via SSH è legittima e prevista

I sensori Corelight sono precaricati con il pacchetto MITRE BZAR (Bro/Zeek ATT&CK-Based Analytics and Reporting). MITRE BZAR identifica le tecniche MITRE ATT&CK per la copia remota dei file, in particolare i file che vengono copiati nelle condivisioni C$ o ADMIN$. Questo pacchetto genera voci nel notice log, come illustrato di seguito:

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, (Salvata una copia del file scritto sulla condivisione di file SMB admin,)
sub: 2020-10-23/6f24ac6ce591baf02acd64684f596d2db0ec97c0,
src: 192.168.38.104,
dst: 192.168.38.102,
p: 445,
actions: [Notice::ACTION_LOG],suppress_for:3600.0

Anche se non abilitate il pacchetto MITRE BZAR sul vostro Corelight Sensor, Corelight continua a registrare l'accesso alla condivisione SMB nel smb_mapping log e l'accesso e la modifica dei file nel smb_files log. I seguenti log illustrano i dati contenuti nella famiglia Corelight dei SMB log:

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

Per cercare il movimento laterale:

1. Iniziare a cercare nei smb_files log e concentrarsi sui campi id.orig_h, id.resp_h, path e name
2. Filtra i record in cui id.resp_h è un file server noto, il che riduce i risultati alle connessioni potenzialmente interessanti
3. Esaminare il path e i campi name per identificare da quale condivisione è stato effettuato l'accesso o in cui è stato scritto il file e determinare se il comportamento è sospetto.
4. Per un contesto aggiuntivo sui restanti record interessanti, è possibile eseguire il pivot al files log, usando l'UID per raccogliere informazioni specifiche sui file. Per esempio, gli hash MD5/SHA1/SHA256 sono calcolati automaticamente e possono essere usati per identificare malware conosciuti in sistemi esterni, come VirusTotal.
    a. Ci sono anche altri campi ed eventualmente log disponibili (per esempio, pe log) che possono essere usati per escludere i record non interessanti.

Non-Application Layer Protocol (Protocollo di Layer non-application)

Gli attaccanti spesso fanno uso di un paio di tecniche per nascondersi all'interno del traffico legittimo: inviando le loro comunicazioni su un protocollo personalizzato su una porta comunemente consentita come 80, 443, o 53, e incorporando la loro messaggistica all'interno della struttura di protocolli legittimi, ma tipicamente meno monitorati, come ICMP.

Per l'uso di protocolli personalizzati su porte standard, vedere la sezione Commonly Used Ports/Non Standard Ports per una descrizione del pacchetto Encryption Detection di Corelight, il dpd log e il weird log. Questi aiutano a identificare le comunicazioni C2 personalizzate che usano una crittografia non standard o violano le specifiche del protocollo tradizionale.

Il malware a volte utilizza protocolli standardizzati di livello inferiore come ICMP, UDP e SOCKS per evitare il rilevamento, poiché questi protocolli sono raramente monitorati. Per esempio, gli autori di malware potrebbero incorporare istruzioni C2 in un pacchetto ICMP Echo Request ("ping").

Corelight monitora tutte le connessioni, indipendentemente dal protocollo, e memorizza i dati di connessione all'interno del conn log. I canali C2 che impiegano protocolli UDP personalizzati o protocolli SOCKS basati su TCP (ma non protocolli standard di livello applicativo) hanno voci di conn log senza un campo di servizio identificabile. Questi campi e log forniscono visibilità sui flussi di traffico attraverso la rete - anche ICMP, UDP e SOCKS. Per le sessioni ICMP, i dati Corelight contengono più della semplice fonte e destinazione; per esempio; il conteggio dei pacchetti, i byte trasferiti e la dimensione dei dati ICMP sia per il mittente che per il destinatario.

Con questi dati, avete le informazioni necessarie per scoprire comunicazioni ICMP anormalmente grandi o frequenti che possono essere indicative di C2. Il seguente log è un esempio del socks log.

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

Per dare la caccia a un intruso che usa un protocollo standard di livello non applicativo per trasmettere informazioni:

1. Cercare nel conn log le voci in cui il campo service è vuoto, local_orig è “true” e local_resp è “false”
2. Aggregare questi risultati per id.orig_h, id.resp_h, id.resp_p e riassumere per conteggio
3. Filtrare le voci ‘normali’
4. Esaminare tutte le voci rimanenti, concentrandosi prima sulle voci con il conteggio maggiore

Non-Standard Ports (Porte non standard)
Ogni connessione effettuata in un ambiente monitorato da Corelight è registrata nel conn log. Dopo aver costruito una lista di porte utilizzate regolarmente (per esempio, 22/SSH, 25/SMTP, 80/HTTP e 443/SSL), si può fare una query ai dati di Corelight per trovare connessioni a porte che non sono su quella lista.

Se si incontrano connessioni che appaiono su altre porte non standard, esaminare il servizio Layer 7 che Corelight osserva e registra nel campo conn log service. I casi senza un servizio riconosciuto sono i più sospetti, soprattutto se vengono trasferiti grandi volumi di dati o le lunghezze di connessione sono lunghe.

Quando si incontrano servizi noti su porte irregolari, esaminare i dettagli nel log di protocollo corrispondente per ulteriori indizi. Per esempio, nel HTTP log, prendete nota del nome del host remoto, della stringa User-Agent del client e dell'URI. Insieme, potrebbero tutti contenere indizi sul software che sta generando la richiesta sulla porta non comune.

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

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

Proxy

Sebbene l'uso dei proxy non dimostri di per sé la presenza di un intruso, gli intrusi possono utilizzare i proxy per “riciclare” le connessioni per oscurare la comunicazione dai difensori. Ci sono molti metodi per osservarlo, tra cui l'analisi tradizionale della connessione sottostante (firma, anomalia, comportamentale) e l'analisi statistica delle proprietà della connessione. L'identificazione specifica delle connessioni proxy è fondamentale per iniziare la ricerca o l'indagine.

Se vedete un valore nel campo proxy del http log di Zeek, significa che una connessione HTTP è stata effettuata attraverso proxy. Il http log cattura i dettagli del proxy dalle intestazioni http. Cercare qualsiasi record nel http log che abbia un campo “proxied” non vuoto.

- host: il nome del dominio del sito web
- id.orig_h: l’indirizzo IP del proxy o del reverse proxy
- id.resp_h: l’indirizzo IP di un web server
- proxied: identifica il proxy e l'indirizzo IP originale del client

Per esempio, un cliente all'IP 219.90.98.8 ha iniziato questa richiesta HTTP. La richiesta è stata inoltrata tramite 172.16.1.30 al web server a 172.16.2.95.

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

Con questo esempio, identificate il proxy e determinate se è interno o esterno. Se è esterno, valutare la sessione e ottenere il contesto, usando i dati di Corelight per decidere se bloccarlo o meno. Se il proxy è

interno, determinare se si tratta di una parte legittima dell'infrastruttura IT o se si tratta di un proxy non autorizzato configurato per eludere la policy - shadow IT.

Inoltre, SOCKS è un protocollo proxy comunemente utilizzato che Corelight Sensors analizza in modo nativo. Quando SOCKS viene incontrato, viene generato un socks log che registra i dettagli degli utenti e dei protocolli. Queste informazioni possono essere utilizzate per garantire che le connessioni non siano dannose e siano conformi alla politica. Nel socks log, concentrarsi su questi campi:

- id.orig_h: l'indirizzo IP del cliente
- id.resp_h: l'indirizzo IP del proxy
- request: il dominio o l'IP a cui il client sta tentando di accedere

user: se si tratta di una connessione autenticata, l'utente che utilizza il proxy

Servizi Web

Web service si verifica quando gli aggressori utilizzano un servizio Web esterno legittimo per inoltrare dati a e/o da un sistema compromesso.

Gli aggressori a volte usano servizi web ben noti per i canali C2 per nascondersi nel rumore. Mentre questa tattica rende l'identificazione più difficile, i dati di Corelight - specialmente i log http, ssl, conn e x509 - aiutano a identificare le connessioni sospette. Cercare gli IOC che includono URI, hostname, o dettagli specifici del certificato (come SNI o CN) è un buon punto di partenza. Quanto segue fornisce alcuni esempi di campi di certificato che potrebbero giustificare un'indagine:

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 (Esfiltrazione)

Automated Exfiltration (Esfiltrazione Automatizzata)

Se un attaccante sta usando un mezzo automatizzato di esfiltrazione, gli artefatti di dati sono catturati nei dati Corelight.

Per cercare l'esfiltrazione nella vostra rete, potete usare il Zeek package sviluppato per calcolare il rapporto Producer/Consumer Ratio (PCR). I valori PCR indicano se i flussi sono di consumo (download) o produttivi (upload). I valori della PCR vanno da -1 (consumo) a +1 (produttivo). Per cacciare l'esfiltrazione utilizzando questo pacchetto:

1. Installare e abilitare il pacchetto PCR.
2. Generare una tabella di id.orig_h, id.resp_h, id.resp_p e pcr dal conn log.
3. Usare local_orig è “false” o local_resp è “true” per filtrare i risultati.
4. Ridurre i risultati filtrando dove pcr <= 0.
5. Per ogni host che genera flussi in cui pcr >= 0, considerare se ci si aspetta che quell'host trasmetta dati, all'interno o all'esterno della rete.

Un'altra opzione consiste nell'utilizzare un SIEM per calcolare il PCR utilizzando le informazioni disponibili nel conn log di Corelight. La seguente query crea una tabella organizzata per host che contiene i byte di origine e di risposta e un valore 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
```

Data Transfer Size Limits (Limiti nella dimensione del trasferimento dati)

Un utente malintenzionato può tentare di trasferire dati o file “suddividendoli” in parti più piccole, per evitare limiti o soglie di trasferimento dati hard-coded (codificati). Presenteremo due metodi per cacciare questa tecnica.

Il primo metodo analizza i dati in uscita dalla rete in base alle coppie di origine e destinazione e richiede una piattaforma di aggregazione/visualizzazione dei dati (a meno che non vi piaccia “AWKing” e “GREPing” attraverso i dati):

1. Generare una tabella dal conn log che includa id.orig_h, id.resp_h, id.resp_p, e sum(orig_bytes).
2. Ordinare i risultati per la somma più grande (orig_bytes).
3. Esaminare ogni host e determinare se esiste un motivo legittimo per gli upload verso quella destinazione.

Il secondo metodo analizza la frequenza e le dimensioni dei trasferimenti in uscita da ogni fonte:

1. Generare una tabella dal conn log che includa id.orig_h, id.resp_h, id.resp_p, e count(orig_bytes).
2. Ordinare i risultati per il conteggio più grande (orig_bytes).

3. Esaminare i risultati e determinare la ragione di tutte le connessioni con la stessa quantità di dati che fluiscono dalla fonte alla destinazione.

[1] https://attack.mitre.org/
[2] Quando viene usato come indicatore di intel l'IP è considerato fragile, a causa della facilità con cui gli avversari possono spostarsi su un nuovo host o provider.
[3] Non tutte le versioni di RDP asseriscono il nome utente nel campo del cookie. Alcuni semplicemente non affermano nulla o scrivono cose incomprensibili. In questi casi, si dovrebbe dedurlo da NTLM o Kerberos log.
[4] https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/
[5] Si prega di visitare https://packages.zeek.org/ per maggiori informazioni su Zeek packages