

Travaux pratiques - Examiner une attaque sur un hôte Windows

Objectifs

Au cours de ces travaux pratiques, vous allez:

Partie 1: Enquêter sur l'attaque avec Sguil

Partie 2: Utiliser Kibana pour enquêter sur les alertes

Ces travaux pratiques sont basés sur un exercice du site web malware-traffic-analysis.net qui est une excellente ressource pour apprendre à analyser les attaques de réseaux et d'hôtes. Merci à brad@malware-traffic-analysis.net pour l'autorisation d'utiliser le matériel de son site.

Contexte/scénario

En mars 2019, les outils de surveillance de la sécurité réseau ont alerté qu'un ordinateur Windows sur le réseau était infecté par des logiciels malveillants. Dans cette tâche, vous devez enquêter sur les alertes et répondre aux questions suivantes:

- Quelle était l'heure précise de l'attaque du 2019-03-19 ?
- Quel ordinateur hôte Windows a été infecté ? Qui était l'utilisateur ?
- Avec quoi l'ordinateur a-t-il été infecté ?

Ressources requises

- La machine virtuelle Security Onion,
- Accès Internet

Instructions

Partie 1: Enquêter sur l'attaque avec Sguil

Dans la partie 1, vous utiliserez Sguil pour vérifier les alertes IDS et recueillir plus d'informations sur la série d'événements liés à une attaque du 3-19-2019.

Remarque: Les identifiants d'alerte utilisés dans ces travaux pratiques ne sont que des exemples. Les identifiants des alertes sur votre VM peuvent être différents.

Étape 1: Ouvrez Sguil et localisez les alertes sur 3-19-2019.

- a. Ouvrez une session sur la machine virtuelle Security Onion avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**.
- b. Lancer Sguil placé sur le bureau. Connectez-vous avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**. Cliquez sur **Select All** et sur **Start Sguil** pour afficher toutes les alertes générées par les capteurs réseau.
- c. Localisez le groupe d'alertes à partir du 19 mars 2019.

Selon Sguil, quels sont les horodatages pour la première et la dernière des alertes qui ont eu lieu le 3-19-2019? Qu'est-ce qui est intéressant à propos des horodatages de toutes les alertes sur 3-19-2019?

Étape 2: Passez en revue les alertes en détail.

- a. Dans Sguil, cliquez sur la première des alertes du 3-19-2019 (ID d'alerte 5.439). Assurez-vous de cocher les cases **Show Packet Data** et **Show Rule** pour examiner les informations d'en-tête de paquet et la règle de signature IDS liées à l'alerte. Directement sur l' **ID d'alerte** et pivotez vers Wireshark. Sur la base des informations tirées de cette alerte initiale, répondez aux questions suivantes:

Quels étaient l'adresse IP et le numéro de port source et l'adresse IP et le numéro de port destination ?

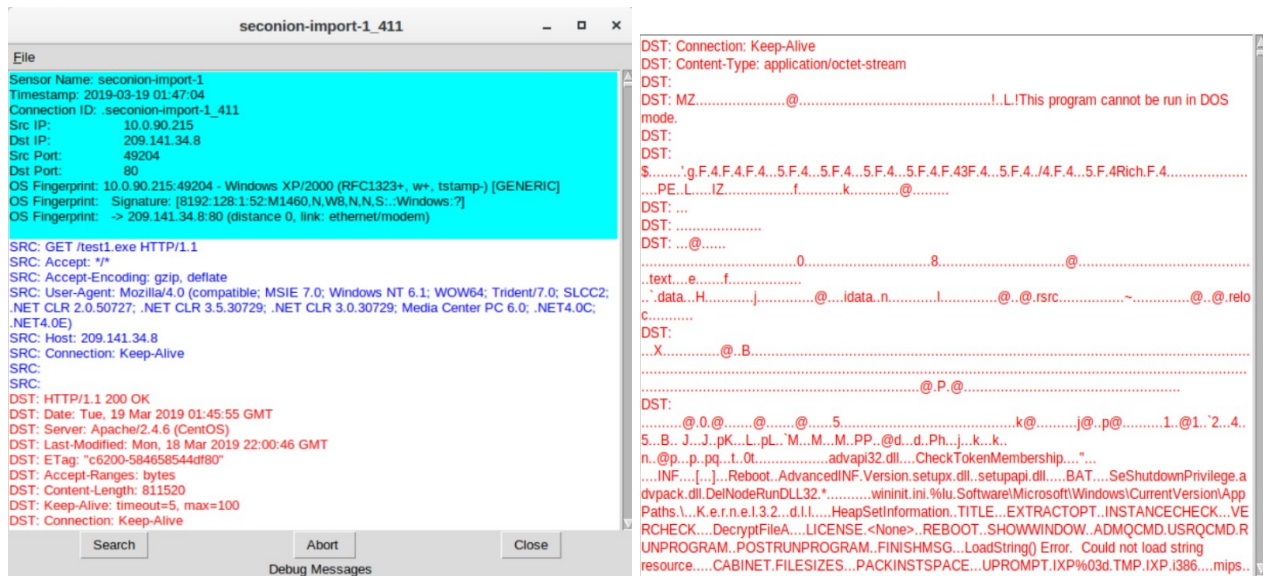
Quel type de protocole et de demande ou de réponse a été impliqué?

Qu'est-ce que l'alerte et le message IDS?

Pensez-vous que cette alerte résulte d'une erreur de configuration de l'IDS ou d'une communication suspecte légitime?

Quel est le nom d'hôte, le nom de domaine et l'adresse IP de l'hôte source dans la mise à jour DNS?

- b. Dans Sguil, sélectionnez la deuxième des alertes du 3-19-2019. Cliquez avec le bouton droit de la souris sur l'ID d'alerte 5.440 et sélectionnez **Transcript**.



D'après la transcription, répondez aux questions suivantes :

Quelles sont les adresses MAC et IP source et de destination et les numéros de port?

En regardant la requête (bleu), quelle était la requête?

En regardant la réponse (rouge), de nombreux fichiers révéleront leur signature de fichier dans les premiers caractères du fichier lorsqu'ils sont affichés sous forme de texte. Les signatures de fichier permettent d'identifier le type de fichier représenté. Utilisez un navigateur Web pour rechercher une liste de signatures de fichiers courantes.

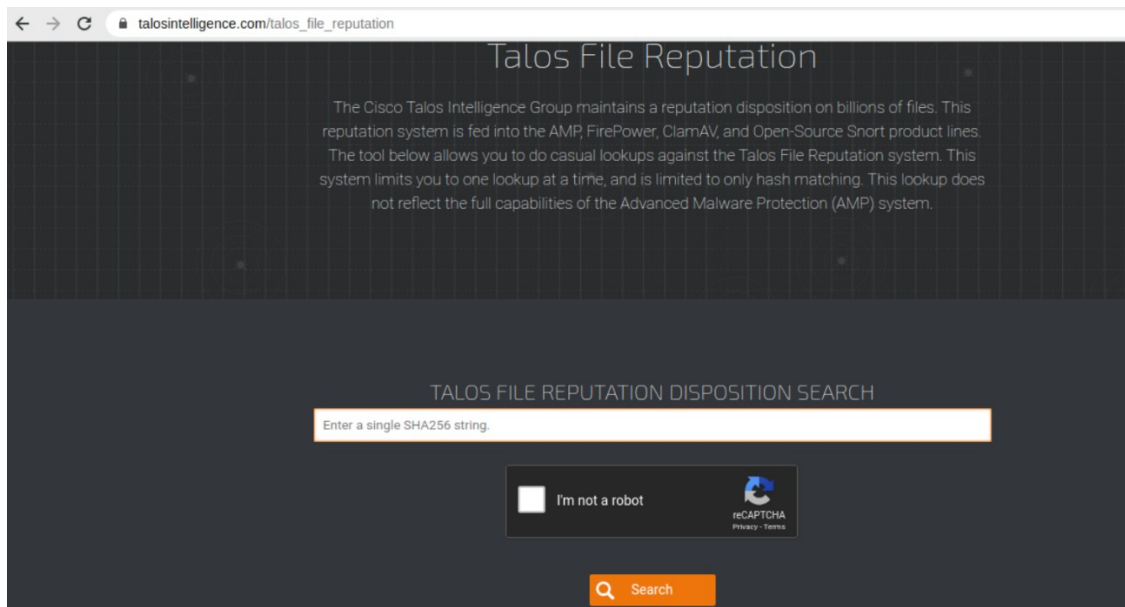
Quels sont les premiers caractères du fichier. Recherchez cette signature de fichier pour savoir quel type de fichier a été téléchargé dans les données ?

- c. Fermez la transcription. Utilisez Wireshark pour exporter le fichier exécutable à des fins d'analyse de programmes malveillants (**File > Export Objects > HTTP...**). Enregistrez le fichier dans le dossier d'accueil de l'analyste.
- d. Ouvrez un terminal dans Security Onion VM et créez un hachage SHA256 à partir du fichier exporté. Utilisez la commande suivante :

```
analyste @SecOnion : ~$ sha256sum test1.exe
```

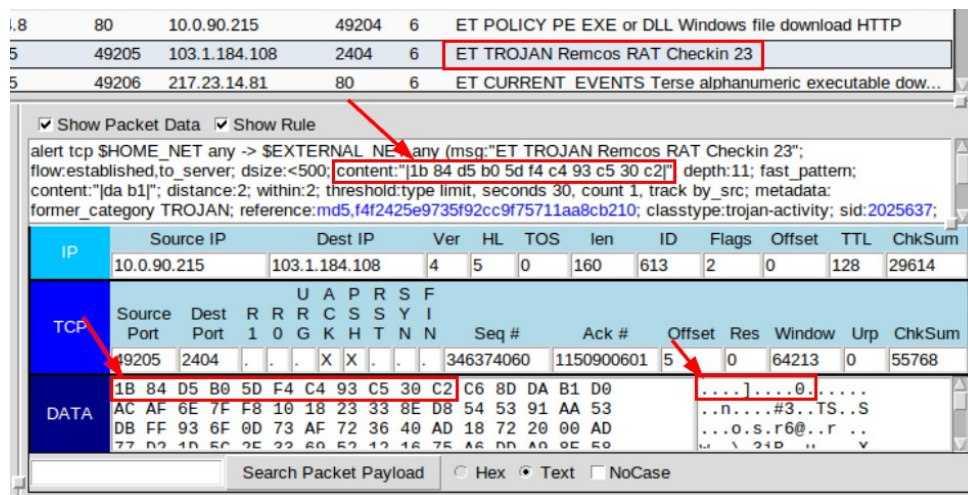
```
2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85 test1.exe
```

- e. Copiez le hachage de fichier et soumettez-le au centre de réputation de fichiers Cisco Talos à l' [adresse https://talosintelligence.com/talos_file_reputation](https://talosintelligence.com/talos_file_reputation).



Est-ce que Talos a reconnu le hachage de fichier et l'a identifié comme un logiciel malveillant ? Dans l'affirmative, quel genre de logiciels malveillants ?

- f. Dans Sguil, sélectionnez l'alerte avec l' **ID d'alerte 5.480** et le **message d'événement** Remcos RAT Checkin 23. Notez que la signature IDS a détecté le RAT Remcos en fonction des codes hexadécimaux binaires au début de la communication.



- g. Cliquez avec le bouton droit de la souris sur l'ID d'alerte et sélectionnez **Transcript**. Faites défiler la transcription et répondez aux questions suivantes :

Quel est le port de destination de la communication ? Est-ce un port bien connu ?

La communication est-elle lisible ou chiffrée ?

Faites des recherches en ligne sur Remcos RAT Checkin 23. Qu'est-ce que Remcos signifie ?

Selon vous, quel type de communication a été transmis ?

Quel type de cryptage et d'obfuscation a été utilisé pour contourner la détection ?

- h. À l'aide de Sguil et des alertes restantes du 3-19-2019, localisez le deuxième fichier exécutable téléchargé et vérifiez s'il s'agit d'un logiciel malveillant connu.

Quels Alert ID alertent un deuxième fichier exécutable en cours de téléchargement ?

À partir de quelle adresse IP du serveur et du numéro de port le fichier a-t-il été téléchargé ?

Quel est le nom du fichier téléchargé ?

Créez un hachage SHA256 du fichier et soumettez le hachage en ligne à Cisco Talos File Reputation Center pour voir s'il correspond à des logiciels malveillants connus. Le fichier exécutable est-il connu des logiciels malveillants et, si oui, quel type ? Qu'est-ce que le nom de la détection d'AMP ?

- i. Examinez les trois alertes restantes du 3-19-2019 en examinant les informations d'en-tête dans Show Packet Data, la signature IDS dans Afficher la règle et les transcriptions d'ID d'alerte.

Comment les trois alertes sont-elles liées ?

- j. Même si vous avez examiné toutes les alertes de Sguil liées à une attaque contre un hôte Windows le 3-19-2019, il peut y avoir d'autres informations connexes disponibles dans Kibana. Fermez Sguil et lancez Kibana placé sur le bureau.

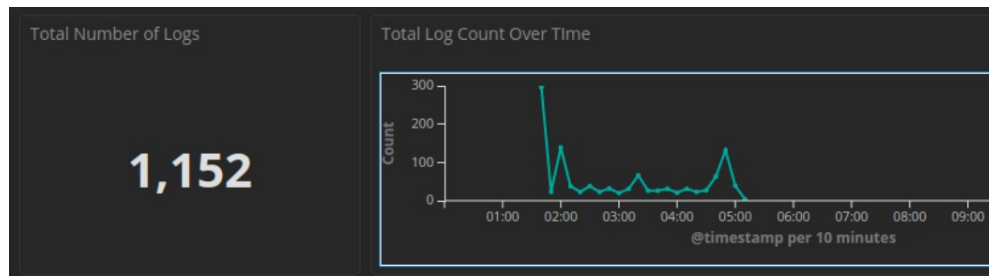
Partie 2: Utiliser Kibana pour enquêter sur les alertes

Dans la partie 2, utilisez Kibana pour enquêter plus avant sur l'attaque du 3-19-2019.

Étape 1: Ouvrez Kibana et affinez le calendrier.

- Ouvrez une session sur la machine virtuelle Security Onion avec le nom d'utilisateur **analyst** et le mot de passe **cyberops**.
- Ouvrez Kibana (identifiant **analyste** et mot de passe **cyberops**), cliquez sur **Last 24 Hours** et sur l'onglet Plage de temps **Absolute** pour changer la plage de temps au 1er mars 2019 au 31 mars 2019.

- c. La chronologie du **nombre total de journaux au fil du temps** affichera un événement le 19 mars. Cliquez sur cet événement pour affiner le focus à la plage de temps spécifique de l'attaque.



Étape 2: Passez en revue les alertes dans le délai réduit.

- a. Dans le tableau de bord Kibana, faites défiler jusqu'à la visualisation **All Sensors - Log Type**. Passez en revue les deux pages et notez la variété des types de journaux liés à cette attaque.

All Sensors - Log Type		All Sensors - Log Type	
Log Type(s)	Count	Log Type(s)	Count
snort	541	bro_weird	8
bro_conn	271	bro_notice	7
bro_dns	85	bro_smb_files	7
bro_dce_rpc	51	bro_http	4
bro_kerberos	50	bro_pe	2
bro_files	35		
bro_smb_mapping	29		
bro_ssl	29		
bro_x509	25		
bro_dhcp	8		
Export: Raw Formatted		Export: Raw Formatted	
1 2 »		« 1 2	

- b. Faites défiler vers le bas et notez que le NIDS Alert Summary dans Kibana contient plusieurs des mêmes alertes IDS que celles répertoriées dans Sguil. Cliquez sur la loupe pour filtrer la deuxième alerte ET TROJAN ABUSE.CH SSL Blacklist Certificat SSL malveillant détecté (Dridex) à partir de l'adresse IP source 31.22.4.176.

NIDS - Alert Summary

Alert	Source IP Address	Destination IP Address	Count
ET TROJAN Remcos RAT Checkin 23	10.0.90.215	103.1.184.108	404
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	31.22.4.176	10.0.90.215	16
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	203.45.1.75	10.0.90.215	13
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	115.112.43.81	10.0.90.215	3
ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2	209.141.34.8	10.0.90.215	12
ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2	217.23.14.81	10.0.90.215	12
ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserver (used by Unknown EK)	217.23.14.81	10.0.90.215	12
ET INFO EXE - Served Attached HTTP	217.23.14.81	10.0.90.215	12

- c. Faites défiler jusqu'à Tous les journaux et cliquez sur la flèche pour développer le premier journal de la liste avec l'adresse IP source 31.22.4.176.

All Logs

Limited to 10 results

Time	source_ip	source_port	destination_ip	destination_port
▶ March 19th 2019, 04:55:13.000	115.112.43.81	443	10.0.90.215	49298
▶ March 19th 2019, 04:54:57.000	115.112.43.81	443	10.0.90.215	49295
▶ March 19th 2019, 04:54:34.000	115.112.43.81	443	10.0.90.215	49289
▶ March 19th 2019, 04:50:21.000	31.22.4.176	3389	10.0.90.215	49281
▶ March 19th 2019, 04:50:21.000	31.22.4.176	3389	10.0.90.215	49281
▶ March 19th 2019, 04:50:15.000	31.22.4.176	3389	10.0.90.215	49280
▶ March 19th 2019, 04:50:15.000	31.22.4.176	3389	10.0.90.215	49280

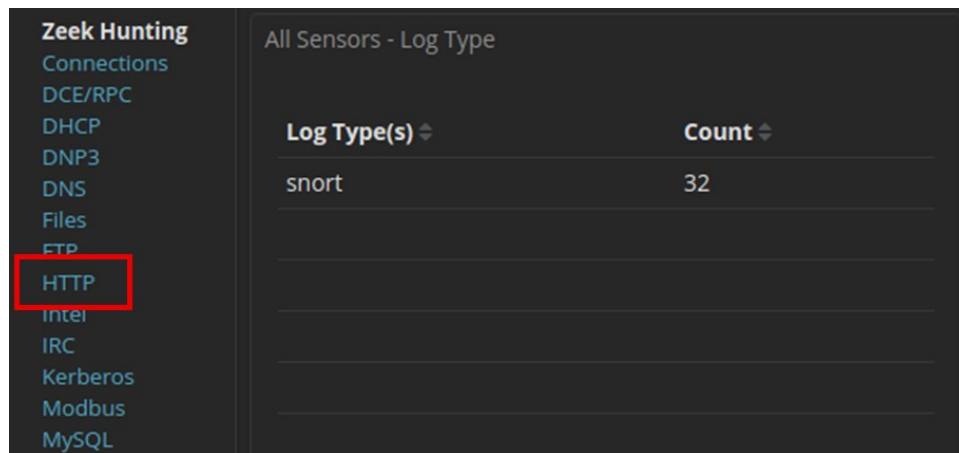
Quel est le pays géographique et la ville où se trouve cette alerte?

Royaume-Uni, Newcastle upon Tyne

Quel est le pays géographique et la ville pour l'alerte de 115.112.43.81?

Inde, Bombay

- d. Faites défiler vers le haut de la page et cliquez sur le lien Accueil sous Navigation.
- e. Auparavant, nous avons noté les types de journaux tels que bro_http répertoriés dans le tableau de bord Accueil. Vous pouvez filtrer les différents types de journal, mais les tableaux de bord intégrés auront probablement plus d'informations. Faites défiler vers le haut de la page et cliquez sur **HTTP** dans le lien du tableau de bord sous Zeek Hunting in Navigation.



Zeek Hunting	
All Sensors - Log Type	
Log Type(s) ↕	Count ↕
snort	32

Left sidebar menu items: Connections, DCE/RPC, DHCP, DNP3, DNS, Files, FTP, **HTTP**, Intel, IRC, Kerberos, Modbus, MySQL.

- f. Faites défiler le tableau de bord HTTP en prenant note des informations présentées et répondez aux questions suivantes:

Qu'est-ce que le nombre de journaux dans le tableau de bord HTTP? De quels pays?

Quelles sont les URI pour les fichiers qui ont été téléchargés?

- g. Faites correspondre les **URI HTTP** au **HTTP - Sites** sur le tableau de bord.

À quoi sont associés les fichiers CSPCA.crl et ncsi.txt? Utilisez un navigateur Web et un moteur de recherche pour obtenir des informations supplémentaires. réponses ici

- h. Faites défiler vers le haut de la page Web et sous Navigation - Zeek Hunting cliquez sur **DNS**. Faites défiler jusqu'à la visualisation des requêtes DNS. Notez les pages 1 et 3 des requêtes DNS.

Query	Count
WPAD	27
LITTLETIGERS	8
dns.msftncsl.com	6
wpad	6
littletigers-dc.littletigers.info	5
_ldap._tcp.default-first-site-name_sites.littletigers-dc.littletigers.info	4
_ldap._tcp.littletigers-dc.littletigers.info	4
wpad.littletigers.info	3
9.90.0.10.in-addr.arpa	2
bobby-tiger-pc	2

Query	Count
isatap.localdomain	1
toptoptop1.online	1
www.msftncsl.com	1

Est-ce que l'un des domaines semble potentiellement dangereux ? Essayez de soumettre l'URL toptoptop1.online à virustotal.com. Quel est le résultat ?

- i. Pour plus d'informations et de curiosité, essayez d'examiner les tableaux de bord Zeek Hunting suivants:

DCE/RPC - pour plus d'informations sur les procédures à distance réseau Windows et les ressources impliquées

Kerberos - pour plus d'informations sur les noms d'hôte et les noms de domaine utilisés

PE — pour plus d'informations sur les exécutables portables

SSL et x.509 — pour plus d'informations sur les noms des certificats de sécurité et les pays utilisés

SMB - pour plus d'informations sur les partages SMB sur le réseau littletigers

Bizarre - pour les anomalies de protocole et de service et les communications mal formées