INF726 - Cybersécurité

Cyberdéfense et Big Data – Nicolas Pierson
Utilisation de Splunk – Production d'un rapport

Telecom ParisTech – MS Big Data 2019
Stéphane REYNAL
Guillaume SOUFFLET
Mohamed DHAOUI

Table des matières

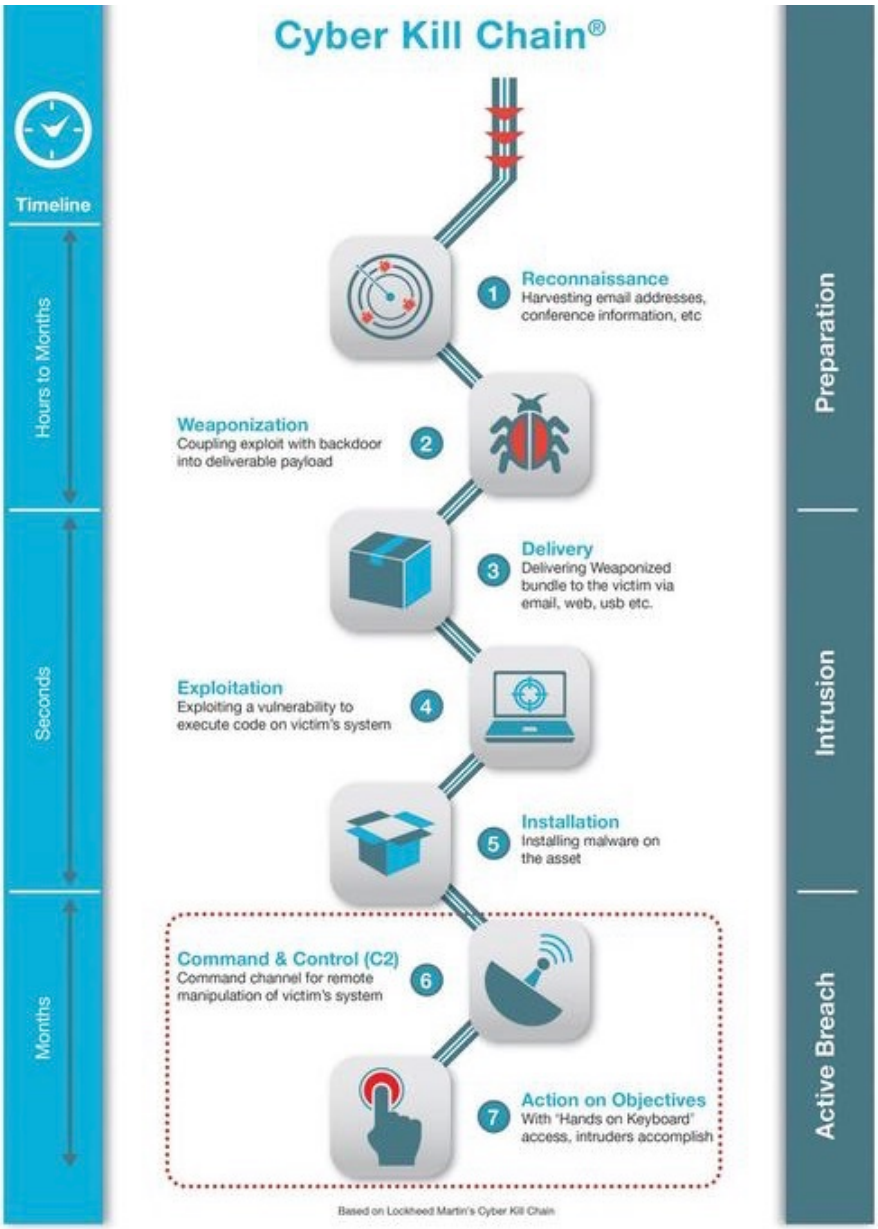
Contexte

Suite à la réception du rapport McTersky du 22/03/19 version 1.2, nous avons mené une investigation numérique à l'aide de Splunk pour décrire l'attaque en cours et les indices de compromission.

I- Résumé de l’attaque

Afin de décrire l’attaque, nous reprenons le modèle de la « Cyber Kill Chain », établi par Lockheeed Martin, dérivé du concept de la chaîne criminelle d’un modèle militaire qui avait pour but d’identifier une cible, préparer l’attaque, puis engager l’objectif et le détruire.

Le modèle de la « Cyber Kill Chain » peut se résumer comme suit :



Appliquons la trame de ce modèle pour décrire l’attaque subie :

→ 1. Reconnaissance

L’attaquant a vraisemblablement eu recours à de l’ingénierie sociale pour cibler ses victimes. Cette hypothèse est avancée compte tenu du caractère très spécifique sur le thème de la reconversion professionnelle.

→ 2. Préparation

Le logiciel malveillant « stuxbar.exe » d'accès à distance est encapsulé dans un support livrable. Ici, le fichier malicieux prend la forme d’un document Adobe PDF, intitulé à dessein « reconversion_2018.pdf», afin d’éveiller la curiosité de la cible et de l’inciter à l’ouvrir, action marquant l’initialisation de l’attaque.

→ 3. Livraison

L’attaque menée ici est une attaque ciblée, véhiculée par mail avec pièce jointe, dont le contenu affiché correspond a un centre d’intérêt identifié de la cible.

→ 4. Exploitation

Une fois le support livré et la pièce jointe ouverte, le code de l’attaque peut être déployé, exploitant les systèmes d'applications vulnérables.

→ 5. Installation

L’ouverture de la pièce jointe permet le démarrage d’un fichier exécutable (.exe), mettant en place une backdoor sur le système cible. Un tunnel VPN est mis en place entre les postes affectés et un serveur externe.

→ 6. Contrôle

Un serveur externe communique avec les ordinateurs attaqués (données entrantes), et facilite l’accès et le contrôle du réseau de la cible. Ici, on constate que le fichier exécutable permet l’envoi, depuis la machine de la victime, de paquets aux serveurs de l’attaquant.

→ 7. Action

On constate que l’attaque permet l’envoi, depuis la machine de la victime, de paquets aux serveurs de l’attaquant. L’objectif de l’attaquant serait donc de récupérer des données de l’entreprise cible.

II- Détail de l’analyse

→ Anticipation

En premier lieu, l’entreprise doit en amont se doter de moyens lui permettant d’assurer sa sécurité dans le cyber espace.

Les standards de la sécurité comme l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et le CIS (Center for Internet Security), entre autres, plébiscitent le recours à un SOC (Security Operating Center) dans le cadre d'une politique de sécurité renforcée. Un SOC a vocation à être le point central de la sécurité d'une entité. Il doit permettre l'amélioration et le contrôle de la sécurité à tous les niveaux temporels d'un incident.

Afin d’anticiper les menaces, une entreprise doit avoir une vision exhaustive globale, opérationnelle et permanente de ses sécurités, ainsi qu'une information rapide sur les incidents qu'elle peut rencontrer. Elle doit également assurer la collecte et l'organisation de toutes les informations liées aux menaces du cyber espace, afin de dresser un portrait des attaquants ou de mettre en exergue des tendances (secteurs d'activités touchés, méthode utilisée, etc) (= cyber threat intelligence (CTI)).

Dans notre cas, l’entreprise ciblée par l’attaque a choisi d’utiliser Splunk comme solution de sécurité de l'information et de gestion des événements (SIEM).

→ Détection

La détection de l’attaque passe tout d’abord par la recherche sur Splunk, des adresses IP identifiées comme suspectes, et l’identification des actions inhabituelles, des incohérences, des incidents potentiels, voir des systèmes compromis impliquant ces adresses, ou des machines ayant interagi avec ces adresses.

→ Investigation

Ensuite, nous concentrons nos investigations sur les IP ayant effectivement interagi avec les IP malveillantes. Ainsi, nous identifions 2 adresses IP de collaborateurs.

Nous remarquons que ces utilisateurs ont ouvert depuis le service de messagerie Outlook, un fichier pdf intitulé « reconversion_2018.pdf », puis, 10 secondes après, ont lancé un fichier exécutable nommé « stuxbar.exe ». Il s’agit des IP 10.11.36.93, et 10.11.36.115, correspondant aux noms d’utilisateurs pdense et ejodor.

Nous détaillons dans la troisième partie de ce rapport, les requêtes qui nous ont permis d’arriver à cette conclusion, et les indicateurs de compromission relevés.

→ **Remédiation**

Afin de remédier à ces attaques, il convient tout d'abord de prévenir les collaborateurs ayant ouvert les pièces jointes qu'elles sont victimes d'une attaque. Il convient également de prévenir les personnes n'ayant pas ouvert les pièces jointes de ne pas les ouvrir.

Ensuite, le responsable de la sécurité peut choisir de bloquer immédiatement les IP malveillantes, par exemple en les inscrivant dans le firewall de l'entreprise.

Il peut aussi choisir, dans un premier temps, de les laisser agir afin d'étudier leurs actions pour mieux appréhender l'attaque, et identifier de manière plus fine l'ensemble des vulnérabilités potentielles de l'entreprise.

→ **Prévention & Protection**

La première action de prévention et de protection que peut mener l'entreprise, consiste à déployer en interne des politiques généralisées de sensibilisation et de formation du personnel à la cybersécurité et aux techniques courantes auxquelles les collaborateurs sont susceptibles d'être exposés lors d'attaques.

Il est nécessaire de porter une attention particulière aux personnels ou services ayant accès à des données sensibles, de cartographier les privilèges et droits d'accès, et de s'assurer du bon cloisonnement de ceux-ci entre services.

L'entreprise doit ensuite s'assurer de la mise à niveau continue de la sécurité de ses systèmes d'information, identifier ses potentielles vulnérabilités, et mener une politique de CTI permanente en assurant la collecte et l'organisation de toutes les informations liées aux menaces du cyber espace afin de dresser un portrait des attaquants ou de mettre en exergue des tendances.

L'entreprise peut également, en s'appuyant sur une équipe interne ou sur un prestataire externe spécialisé, scruter le web en continue, à la recherche de fuites de données.

III- Annexe : les indicateurs de compromission (IOC)

→ Le périmètre

L'entreprise possède des applications exposées aux utilisations externes (certaine pouvant en plus utiliser des infrastructures de cloud privé et public), permettant divers types d'accès à distance aux ressources internes. La portion du réseau exposée représente un vecteur d'attaque, ainsi qu'un point d'identification d'éventuelles compromissions.

Les indicateurs de compromission (IOC) comprennent par exemple :

=> les ports non concordant / trafic d'applications ;
=> l'augmentation du nombre de lectures / trafics de données ;
=> les irrégularités géographiques (sources de communication anormales).

Plus finement, on peut surveiller les IOC sur les points particuliers que sont les points de terminaison, les connexions, le mouvement latéral, et l'accès aux données.

→ Les points de terminaison

Les points de terminaison représentent la partie du réseau constamment accessible en dehors du périmètre : ils permettent de surfer sur le Web et de servir de réceptacles aux emails entrants. Ils comprennent les processus rouges (processus qui n'ont jamais été exécutés sur un point de terminaison auparavant), ou la persistance anormale de tâches.

→ Les connexions

Concernant les connexions, les indicateurs incluent les anomalies suivantes :

- Le point de terminaison utilisé (par exemple un commercial ne se connectera pas d'une machine du service comptable).
- La date et l'heure d'utilisation (un utilisateur travaillant de 9:00 à 17:00 se connectant le samedi à 3 heures du matin).
- La fréquence (un utilisateur, qui se connecte généralement une fois le matin et se déconnecte le soir, commence soudainement à se connecter et se déconnecter sur de courtes périodes,).
- La concurrence (un utilisateur se connectant soudain depuis plusieurs points de terminaison à la fois).

→ **Le mouvement latéral**

Le mouvement latéral est une étape nécessaire pour la plupart des attaques étant donné que leur point d'ancrage initial est un poste de travail de bas niveau sans aucun droit d'accès particulier. Dans ce cas de figure, les indicateurs comprennent :

- Une contradiction au niveau des utilisateurs/applications (les utilisateurs de bas niveau n'utilisent que très rarement d'outils liés à l'informatique, au scriptage, etc., et les utilisateurs n'utilisant jamais de session RDP, etc., sont également suspects).
- Un trafic réseau anormal (tout type d'existence ou d'excès de trafic qui n'est pas normal (par exemple, SMB, RPC, RDP, etc.) indiquent une compromission potentielle).

→ **L'accès aux données**

La recherche des anomalies suivantes peut indiquer une compromission:

- La date et l'heure d'accès ;
- Le lieu d'accès ;
- La quantité de données.

→ **Les IOC relevés à l'aide de Splunk au cours de l'attaque subie**

Les **indicateurs de compromission** fournis dans le rapport donnent des adresses IP suspectes.

A partir de ces IP, nous menons nos recherches sur Splunk, et tentons de répondre aux questions listées ci-dessous, dans le but de retracer l'attaque, et de relever au fil de l'eau les indicateurs de compromission pertinents :

- 1. Avec qui ont interagi les adresses IP suspectes ?
- 2. Quand ont commencé les interactions entre les adresses IP internes et celles suspectes ?
- 3. Quels sont les activités / processus sur les postes internes à ce moment là ?
- 4. Comment ces processus ont pu pénétrer en interne ?
- 5. Quel est l' e-mail malveillant ?
- 6. Quels est le type d'attaque en cours ?
- 7. Quelles sont les adresses IP externes concernées par ce type d'action (TCP_TUNNELED) ?
- 8. De quels pays vient l'attaque ?

- 1. <u>Avec qui ont interagi les adresses IP suspectes ?</u>

Nous avons identifié **les adresses IP internes ayant interagi avec les IP suspectes** via une simple recherche des ces adresses dans le bandeau de recherche de Splunk :

- **10.11.36.115**
- **10.11.36.93**

Liste des adresses IP internes en contact avec les adresses malveillantes

src	values(dest)
10.11.36.115	212.24.32.56 212.24.32.57 212.24.32.62 212.24.32.63 212.24.32.64 212.24.32.65 46.252.242.1 46.252.242.10 46.252.242.2 46.252.242.7 46.252.242.8 46.252.242.9 81.94.32.10 81.94.32.11 81.94.32.17 81.94.32.18 81.94.32.19
10.11.36.93	212.24.32.56 212.24.32.57 212.24.32.62 212.24.32.63 212.24.32.64 212.24.32.65 46.252.242.1 46.252.242.10 46.252.242.2 46.252.242.7 46.252.242.8 46.252.242.9 81.94.32.10 81.94.32.11 81.94.32.17 81.94.32.18 81.94.32.19

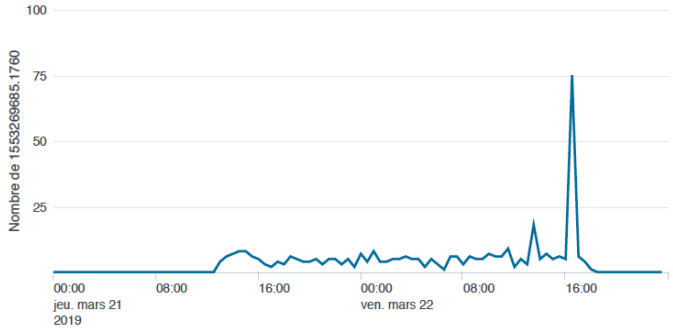
NB- On peut aussi retrouver ces IP en entrant utilisant l'expression régulière suivante :

```
index=*[|inputlookup banet.csv | rename ipaddress as dest | fields dest] | stats values(dest) by src
```

- 2. <u>Quand ont commencé les interactions entre les adresses IP internes et celles suspectes ?</u>

On voit qu'elles ont commencé le jeudi 21 mars vers 13h00.

Evolution temporelle des interactions entre les adresses IP suspectes et celles internes affectées



- 3. Quels sont les activités / processus sur les postes internes à ce moment là ?

Liste des processus exécutés par les adresses IP internes affectées

_time	src	Host	process	process_name	Nombre de 1553273080.1924
2019-03-21 13:10:14	10.11.36.115	ejodor-0TNY60F9.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf	PDFRd32.exe	1
2019-03-21 13:10:14	10.11.36.93	pdence-94DA3SF7.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf	PDFRd32.exe	1
2019-03-21 13:10:24	10.11.36.115	ejodor-0TNY60F9.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe	stuxbar.exe	1
2019-03-21 13:10:24	10.11.36.93	pdence-94DA3SF7.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe	stuxbar.exe	1
2019-03-21 13:22:43	10.11.36.115	ejodor-0TNY60F9.defense.fr	-	PsiService_2.exe	1
2019-03-21 13:55:13	10.11.36.93	pdence-94DA3SF7.defense.fr	C:\Users\ekylasam\AppData\Roaming\Spotify\Data\SpotifyWebHelper.exe	SpotifyWebHelper.exe	1
2019-03-21 14:00:23	10.11.36.93	pdence-94DA3SF7.defense.fr	-	wordpad.exe	1
2019-03-21 14:04:04	10.11.36.115	ejodor-0TNY60F9.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf	PDFRd32.exe	1
2019-03-21 14:04:04	10.11.36.93	pdence-94DA3SF7.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf	PDFRd32.exe	1
2019-03-21 14:04:14	10.11.36.115	ejodor-0TNY60F9.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe	stuxbar.exe	1
2019-03-21 14:04:14	10.11.36.93	pdence-94DA3SF7.defense.fr	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe	stuxbar.exe	1
2019-03-21 14:31:27	10.11.36.93	pdence-94DA3SF7.defense.fr	-	nvvsvc.exe	1
2019-03-21 14:43:08	10.11.36.93	pdence-94DA3SF7.defense.fr	-	WINWORD.EXE	1
2019-03-21 14:48:38	10.11.36.115	ejodor-0TNY60F9.defense.fr	-	splunkweb.exe	1
2019-03-21 15:00:29	10.11.36.93	pdence-94DA3SF7.defense.fr	-	p4v.exe	1

On constate que les deux adresses IP internes ont exécuté les deux processus suivants :

- **PDFRd32.exe à 13:10:14**
- **stuxbar.exe 10 secondes plus tard**

puis aussi une heure plus tard à 14:04:04

Dans cette période, aucun autre processus commun aux adresses IP internes affectées n'est identifié. Nous concluons que l'exécution de ces processus sont la charge qui a permis le début de l'attaque.

- 4. <u>Comment ces processus ont pu pénétrer en interne ?</u>

Ces processus sont stockés dans les archives mail Outlook attachés à un fichier pdf nommé « reconversion_2018.pdf »

Ce fichier est donc une pièce-jointe d'un e-mail ouverte par les victimes et qui a permis l'activation des processus malveillants.

NB- L'expression régulière suivante nous permet également d'extraire, pour chacune des deux IP des postes des collaborateurs identifiés précédemment, le nom des fichiers qui ont été ouverts à partir d'Outlook, l'identité de l'hôte ayant effectué l'action et son adresse IP, ainsi que la date et l'heure de l'évènement :

```
sourcetype="winhostmon" dest="10.11.36.93" (ou .115)
| rex field=process ".+(?<outlook>Content\.Outlook)\\\(?<fichier>\S+)"
| search outlook=*
| rename dest as Poste
| rename fichier as fichier
| table _time Poste Host process_name process Fichier
```

- 5. <u>Quel est l' e-mail malveillant ?</u>

_time	subject	orig_recipient	orig_src	orig_dest	recipient	Nombre de 1553250007.1345
2019-03-22 14:04:55	Opportunite reconversion	liste@marinemobilite.com	212.53.36.199	204.118.100.129	capucine.palaci@defense.fr	1
2019-03-22 14:04:55	Opportunite reconversion	liste@marinemobilite.com	212.53.36.199	204.118.100.129	eloise.jodor@defense.fr	1
2019-03-22 14:04:55	Opportunite reconversion	liste@marinemobilite.com	212.53.36.199	204.118.100.129	emmanuel.coraidh@defense.fr	1
2019-03-22 14:04:55	Opportunite reconversion	liste@marinemobilite.com	212.53.36.199	204.118.100.129	pierre.dence@defense.fr	1

Ce mail a pour titre:

- **Opportunité reconversion**

est envoyé par:

- **liste@marinemobilite.com**

4 personnes en interne ont reçu ce mail avec la pièce-jointe suspecte.

Liste des hôtes ayant ouvert le pdf suspect

Host	src	Nombre de 1553248542.1155
ejodor-0TNY60F9.defense.fr	10.11.36.115	1
pdence-94DA3SF7.defense.fr	10.11.36.93	1

Deux collaborateurs l'ont ouverte :

- Eloise Jodor
- Pierre Dence

Les deux autres ne l'ont pas ouverte :

- Capucine Palaci
- Emmanuel Coraidh

- 6. <u>Quels est le type d'attaque en cours ?</u>

Description des interactions entre les adresses IP internes et les adresses suspectes

_time	action	dest	src	bytes_in	bytes_out	Nombre de 1553269685.1760
2019-03-21 13:10:44	TCP_TUNNELED	81.94.32.19	10.11.36.93	440	430	1
2019-03-21 13:18:39	TCP_TUNNELED	46.252.242.9	10.11.36.93	395	445	1
2019-03-21 13:22:36	TCP_TUNNELED	81.94.32.11	10.11.36.93	389	408	1
2019-03-21 13:26:33	TCP_TUNNELED	81.94.32.19	10.11.36.93	358	402	1
2019-03-21 13:38:25	TCP_TUNNELED	212.24.32.65	10.11.36.115	347	391	1
2019-03-21 13:46:20	TCP_TUNNELED	212.24.32.56	10.11.36.93	459	422	1
2019-03-21 13:46:20	TCP_TUNNELED	46.252.242.2	10.11.36.115	346	354	1
2019-03-21 13:50:17	TCP_TUNNELED	81.94.32.11	10.11.36.93	435	366	1
2019-03-21 13:58:11	TCP_TUNNELED	46.252.242.1	10.11.36.115	380	349	1
2019-03-21 13:58:11	TCP_TUNNELED	46.252.242.9	10.11.36.93	349	420	1
2019-03-21 14:02:09	TCP_TUNNELED	81.94.32.19	10.11.36.93	389	370	1
2019-03-21 14:08:31	TCP_TUNNELED	46.252.242.10	10.11.36.93	376	428	1
2019-03-21 14:16:25	TCP_TUNNELED	212.24.32.56	10.11.36.115	401	396	1
2019-03-21 14:16:25	TCP_TUNNELED	81.94.32.10	10.11.36.93	374	401	1
2019-03-21 14:20:23	TCP_TUNNELED	81.94.32.18	10.11.36.115	357	351	1
2019-03-21 14:28:17	TCP_TUNNELED	212.24.32.63	10.11.36.93	423	429	1
2019-03-21 14:28:17	TCP_TUNNELED	81.94.32.17	10.11.36.115	349	438	1
2019-03-21 14:32:14	TCP_TUNNELED	46.252.242.8	10.11.36.115	390	370	1
2019-03-21 14:40:09	TCP_TUNNELED	212.24.32.65	10.11.36.115	365	369	1
2019-03-21 14:48:03	TCP_TUNNELED	46.252.242.8	10.11.36.115	385	365	1
2019-03-21 14:48:03	TCP_TUNNELED	81.94.32.10	10.11.36.93	425	441	1
2019-03-21 14:52:01	TCP_TUNNELED	212.24.32.65	10.11.36.93	345	443	1
2019-03-21 14:55:58	TCP_TUNNELED	46.252.242.1	10.11.36.93	454	353	1
2019-03-21 14:55:58	TCP_TUNNELED	81.94.32.19	10.11.36.115	447	364	1
2019-03-21 14:59:55	TCP_TUNNELED	81.94.32.18	10.11.36.93	394	398	1

Via une connexion VPN, des données entrent et sortent des adresses IP internes vers celles suspectes.

- 7. Quelles sont les adresses IP externes concernées par ce type d'action (TCP_TUNNELED) ?

Y a-t-il d'autres adresses IP suspectes?

dest	Nombre de 1553272641.1876
46.252.242.1	12
46.252.242.2	14
46.252.242.3	19
46.252.242.4	21
46.252.242.5	17
46.252.242.6	22
46.252.242.7	9
46.252.242.8	13
46.252.242.9	14
46.252.242.10	13
81.94.32.10	11
81.94.32.11	13
81.94.32.12	14
81.94.32.13	14
81.94.32.14	13
81.94.32.15	15
81.94.32.16	20
81.94.32.17	17
81.94.32.18	16
81.94.32.19	18
212.24.32.56	14
212.24.32.57	18
212.24.32.58	17
212.24.32.59	16
212.24.32.60	12
212.24.32.61	17
212.24.32.62	11
212.24.32.63	13
212.24.32.64	8
212.24.32.65	17

Les adresses IP suspectes sont donc:

- **46.252.242.xx, xx = 1...10**
- **81.94.32.yy, yy = 10...19**
- **212.24.32.zz, zz = 56...65**

Nous constatons qu'il y a des machines supplémentaires de celles identifiées dans le rapport McTersky du 22/03/19 version 1.2:

- **46.252.242.ii, ii = 3,4,5,6**
- **81.94.32.jj, jj = 12, 13, 14, 15, 16**
- **212.24.32.kk, kk = 58, 59, 60, 61**

Action: mettre à jour le rapport avec cette liste d'adresse IP

- 8. <u>De quels pays vient l'attaque ?</u>

D'où vient l'attaque? Recherche sur la base de l'adresse IP

Country	count
Russia	231

Outre le fait qu'il n'y a a priori aucune raison qu'il y ait autant de trafic entre l'entreprise et la Russie, on identifie clairement l'origine de l'attaque comme étant reliée à des adresses IP basées dans ce pays.

NB- L'expression régulière suivante nous permet d'identifier le pays d'origine des IP malveillantes en interactions avec les deux IP des postes des collaborateurs identifiés :

index=*[|inputlookup banet.csv | rename ipaddress as dest | fields dest] |iplocation dest | stats count by Country