



Cyber Threat Intelligence

22.03.2019

—

Description du travail à fournir :

- Résumé de l'attaque
- Détails de l'analyse
- Annexe contenant les IOC identifiés
- Echéance : 29.03.2019

Anthony Houdaille

Alexandre Bec

Maël Fabien

Contexte

Le groupe d'attaquants Baier fait encore parler de lui. Plusieurs fuites de données massives ont été attribuées à ce groupe que les chercheurs estiment implanté en Russie. La première attaque attribuée à ce groupe date de 2015, lorsque plusieurs institutions gouvernementales situées aux USA avaient été attaquées par une campagne de spearphishing visant à installer un ver nommé à l'époque Lombrix.

Les secteurs ciblés pour cette nouvelle campagne baptisée Banacry sont ceux des télécommunications, de l'aéronautique et de la défense notamment de pays situés en zone Europe.

Les techniques utilisées n'ont pas été formellement identifiées mais des connexions à des serveurs de contrôle (C&C) ont été repérées par les experts de McTersky.

Les url et les adresses IP de ces C&C apparaissent ci dessous ainsi que les condensés (hash) des fichiers infectés.

Données à disposition

Nous disposons des logs des employés de l'entreprise. Les champs dont nous disposons sont les suivants :

- **Bluecoat** : proxy web
- **Cisco:esa** : Passerelle Mail
- **Fgt_traffic** : Firewall réseau
- **Linuxsecure** : Infos d'authentification Linux
- **Portcontrol** : Branchement de support amovible réseau
- **Streammysql** : Ecoute réseau et interprétation protocolaire de SQL
- **Winhostmon** : Infos de la création de process Windows

Les données sont mises à disposition sur Splunk.

Exploration de l'attaque

Identification des machines infectées

La première étape consiste à identifier l'adresse source commune aux adresses IP compromises :

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

Avec cette requête on identifie les hôtes **10.11.36.115** et **10.11.36.93**, qui ont communiqué avec toutes les machines identifiées comme compromises.

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

Avec la requête suivante, on affiche tout le trafic d'interaction avec les machines compromises :

```
46.252.242.1 OR 46.252.242.2 OR 46.252.242.7 OR 46.252.242.8 OR
46.252.242.9 OR 46.252.242.10 OR 81.94.32.10 OR 81.94.32.11 OR
81.94.32.17 OR 81.94.32.18 OR 81.94.32.19 OR 212.24.32.56 OR
212.24.32.57 OR 212.24.32.62 OR 212.24.32.63 OR 212.24.32.64 OR
212.24.32.65
```

Dans l'origine du trafic (champs **src**) on voit que ce sont uniquement les deux adresses identifiées.

Valeurs	Nombre	%	
10.11.36.115	104	50,485 %	
10.11.36.93	102	49,514 %	

Premières attaques

La **première attaque** a eue lieu le 21/03/19 à 13:10:41,000 sur la machine 10.11.36.93. La première URL du destinataire ayant infecté la machine est **81.94.32.19:443**.

La **deuxième** machine contaminée était la 10.11.36.115, le 21/03/19 à 13:14:38,0000. Voici le log de l'attaque :

```

> 21/03/19 1553170478 duration=547 dest=212.24.32.63 action=TCP_TUNNELED status=200 bytes_in=388 http_method=CONNECT url=tcp://212
13:14:38,000 .24.32.63:443/ - src=10.11.36.115 category=none bytes_out=346 http_user_agent="54591/5.0 (compatible; MSIE 9.0; Windows
NT 6.1; Trident/5.0)" - - - -
bytes_in = 388 | bytes_out = 346 | source = eventgen | sourcetype = bluecoat | src = 10.11.36.115 |
url = tcp://212.24.32.63:443/

> 21/03/19 1553170478 duration=543 dest=81.94.32.10 action=TCP_TUNNELED status=200 bytes_in=369 http_method=CONNECT url=tcp://81.9
13:14:38,000 4.32.10:443/ - src=10.11.36.93 category=none bytes_out=431 http_user_agent="79665/5.0 (compatible; MSIE 9.0; Windows NT
6.1; Trident/5.0)" - - - -
bytes_in = 369 | bytes_out = 431 | source = eventgen | sourcetype = bluecoat | src = 10.11.36.93 | url = tcp://81.94.32.10:443/

> 21/03/19 1553170241 duration=588 dest=81.94.32.19 action=TCP_TUNNELED status=200 bytes_in=382 http_method=CONNECT url=tcp://81.9
13:10:41,000 4.32.19:443/ - src=10.11.36.93 category=none bytes_out=381 http_user_agent="41198/5.0 (compatible; MSIE 9.0; Windows NT
6.1; Trident/5.0)" - - - -
bytes_in = 382 | bytes_out = 381 | source = eventgen | sourcetype = bluecoat | src = 10.11.36.93 | url = tcp://81.94.32.19:443/

```

Origine de l'attaque

Afin de remonter à l'**origine de l'attaque**, on peut chercher le premier log sur lequel la machine 10.11.36.93 a été infectée par une source malveillante.

Nous devons chercher un **fichier commun** qui aurait été reçu peu avant l'infection, ou **une action commune** effectuée par les deux machines. Avec la recherche suivante, nous pouvons accéder aux logs pour lesquels les machines 10.11.36.93 et 10.11.36.115 étaient destinataires :

```
dest = "10.11.36.93" OR dest = "10.11.36.115"
```

Le **paquet suspect** a été reçu à le 21/03/19 à 13:10:11,0000, soit 30 secondes avant l'infection.

>	21/03/19 13:10:11,000	03/21/19 13:10:11 Type=Process process_name=PDFRd32.exe dest=10.11.36.115 ProcessId=14399 Host="ejodor-0TNY60F9.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf" host = workstation-xx.buttercupgames.com source = eventgen sourcetype = winhostmon
>	21/03/19 13:10:11,000	03/21/19 13:10:11 Type=Process process_name=PDFRd32.exe dest=10.11.36.93 ProcessId=11451 Host="pdence-94DA3SF7.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf" host = workstation-xx.buttercupgames.com source = eventgen sourcetype = winhostmon

D'après les logs ci-dessus, un même **email** aurait été envoyé 30 secondes avant l'infection de la machine 10.11.36.93, et 3 minutes avant celui 10.11.36.115. Il s'agit d'une pièce jointe reçue sur le mail de l'entreprise, via Outlook.

-	75	75 %	
c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf	6	6 %	
c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe	6	6 %	

Qui était visé ?

On peut alors s'intéresser à ce fichier en particulier. On identifie un email envoyé à une liste de diffusion liste@marinemobilite.com et reçu par :

- Pierre Dence sur l'email : pierre.dence@defense.fr
- Eloise Jodor sur l'email : eloise.jodor@defense.fr
- Capucine Palaci sur l'email : capucine.palaci@defense.fr
- Emmanuel Coraigh sur l'email : emmanuel.coraigh@defense.fr

4 collaborateurs ont reçu le courrier électronique.

>	21/03/19 13:09:31,000	Mon Mar 21 13:09:31 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=emmanuel.coraigh@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa
>	21/03/19 13:09:31,000	Mon Mar 21 13:09:31 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=capucine.palaci@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa
>	21/03/19 13:09:31,000	Mon Mar 21 13:09:31 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=eloise.jodor@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa
>	21/03/19 13:09:31,000	Mon Mar 21 13:09:31 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=pierre.dence@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf host = sfo-resources-12.it.buttercupgames.com source = eventgen sourcetype = cisco:esa

On remarque que les deux utilisateurs ont reçus plusieurs fois le même mail :

Une première fois à 13h09, une seconde fois 13h15 puis 14h23, 18h55, 19h45 et enfin 22h35, sur la date du 21/03/2019. Cette diffusion de mail a été réalisée par un host distant ayant pour adresse IP : 212.53.36.199. Cette adresse ne figure pas dans la liste des IPs des C&C.

>	21/03/19 13:15:48,000	Mon Mar 21 13:15:48 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=pierre.dence@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf orig_dest = 204.118.100.129 orig_src = 212.53.36.199 recipient = pierre.dence@defense.fr source = eventgen sourcetype = cisco:esa
>	21/03/19 13:09:31,000	Mon Mar 21 13:09:31 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=pierre.dence@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf orig_dest = 204.118.100.129 orig_src = 212.53.36.199 recipient = pierre.dence@defense.fr source = eventgen sourcetype = cisco:esa
>	21/03/19 13:15:48,000	Mon Mar 21 13:15:48 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=eloise.jodor@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf orig_dest = 204.118.100.129 orig_src = 212.53.36.199 recipient = eloise.jodor@defense.fr source = eventgen sourcetype = cisco:esa
>	21/03/19 13:09:31,000	Mon Mar 21 13:09:31 2019 orig_dest=204.118.100.129 orig_recipient=liste@marinemobilite.com orig_src=212.53.36.199 protocol=SMTP recipient=eloise.jodor@defense.fr subject="Opportunité reconversion" file_name=reconversion_2018.pdf orig_dest = 204.118.100.129 orig_src = 212.53.36.199 recipient = eloise.jodor@defense.fr source = eventgen sourcetype = cisco:esa

Qui a ouvert le fichier infecté ?

Ce fichier, s'il est infecté, doit entraîner l'exécution d'un script malveillant. C'est bel et bien le cas, étant donné que les scripts "stuxbar.exe" se sont exécutés directement à l'ouverture du fichier.

i	Heure	Événement
>	21/03/19 13:16:38,000	03/21/19 13:16:38 Type=Process process_name=stuxbar.exe dest=10.11.36.93 ProcessId=9801 Host="pdence-94DA3SF7.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe" source = eventgen sourcetype = winhostmon src = 10.11.36.93
>	21/03/19 13:16:28,000	03/21/19 13:16:28 Type=Process process_name=PDFRd32.exe dest=10.11.36.93 ProcessId=11451 Host="pdence-94DA3SF7.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf" source = eventgen sourcetype = winhostmon src = 10.11.36.93
>	21/03/19 13:10:21,000	03/21/19 13:10:21 Type=Process process_name=stuxbar.exe dest=10.11.36.93 ProcessId=9801 Host="pdence-94DA3SF7.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe" source = eventgen sourcetype = winhostmon src = 10.11.36.93
>	21/03/19 13:10:11,000	03/21/19 13:10:11 Type=Process process_name=PDFRd32.exe dest=10.11.36.93 ProcessId=11451 Host="pdence-94DA3SF7.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf" source = eventgen sourcetype = winhostmon src = 10.11.36.93

Parmi les 4 collaborateurs qui ont reçu le mail, deux l'ont ouvert, Pierre et Eloise :

>	21/03/19 13:10:11,000	03/21/19 13:10:11 Type=Process process_name=PDFRd32.exe dest=10.11.36.115 ProcessId=14399 Host="ejodor-0TNY60F9.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf" Host = ejodor-0TNY60F9.defense.fr dest = 10.11.36.115 source = eventgen sourcetype = winhostmon src = 10.11.36.115
>	21/03/19 13:10:11,000	03/21/19 13:10:11 Type=Process process_name=PDFRd32.exe dest=10.11.36.93 ProcessId=11451 Host="pdence-94DA3SF7.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf" Host = pdence-94DA3SF7.defense.fr dest = 10.11.36.93 source = eventgen sourcetype = winhostmon src = 10.11.36.93

Ils l'ont d'ailleurs ouvert deux fois :

>	21/03/19 13:16:28,000	03/21/19 13:16:28 Type=Process process_name=PDFRd32.exe dest=10.11.36.115 ProcessId=14399 Host="ejodor-0TNY60F9.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf"
		Host = ejodor-0TNY60F9.defense.fr dest = 10.11.36.115 source = eventgen sourcetype = winhostmon src = 10.11.36.115
>	21/03/19 13:16:28,000	03/21/19 13:16:28 Type=Process process_name=PDFRd32.exe dest=10.11.36.93 ProcessId=11451 Host="pdence-94DA3SF7.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion_2018.pdf"
		Host = pdence-94DA3SF7.defense.fr dest = 10.11.36.93 source = eventgen sourcetype = winhostmon src = 10.11.36.93

Lorsque l'on remonte sur l'heure d'ouverture des fichiers, Pierre et Eloise auraient ouvert la pièce jointe à la même heure. Les scripts ont été exécutés en même temps, ce qui tient plus du hasard.

Actions directes

Les 4 utilisateurs ayant reçu le fichier doivent être prévenus, et nous devons empêcher une nouvelle infection. Il faut donc suspendre l'accès d'Eloise et Pierre à leurs postes, et prévenir Capucine et Emmanuel afin de supprimer les fichiers infectés de leur boîte mail.

Une fois cette situation contrôlée, il faut également modifier le firewall pour bloquer les accès des IP identifiées comme malveillantes.

Dans un second temps, il faut agir sur le comportement des employés de l'entreprise, et comprendre comment Eloise et Pierre ont pu ouvrir cette pièce jointe.

Où sont parties les données ?

Maintenant que nous avons identifié les postes compromis, et l'heure de l'infection, on peut filtrer le trafic sortant ainsi :

- Identifier le trafic sortant des machines infectées : **src = 10.11.36.115**
- Analyser le trafic sortant à partir du **21 Mars, à partir de 13h10**

On trouve alors dans le trafic sortant, des tunnels TCP établis après l'infection des postes :

>	21/03/19 13:20:56,000	1553170856 duration=633 dest=78.138.128.106 action=TCP_TUNNELED status=200 bytes_in=421 http_method=CONNECT url=tcp://78.138.128.106:443/ - src=10.11.36.115 category=none bytes_out=455 http_user_agent="41129/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - dest = 78.138.128.106 host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.115
>	21/03/19 13:16:58,000	1553170618 duration=643 dest=46.252.242.4 action=TCP_TUNNELED status=200 bytes_in=387 http_method=CONNECT url=tcp://46.252.242.4:443/ - src=10.11.36.115 category=none bytes_out=373 http_user_agent="12215/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - dest = 46.252.242.4 host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.115
>	21/03/19 13:14:38,000	1553170478 duration=547 dest=212.24.32.63 action=TCP_TUNNELED status=200 bytes_in=388 http_method=CONNECT url=tcp://212.24.32.63:443/ - src=10.11.36.115 category=none bytes_out=346 http_user_agent="54591/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - dest = 212.24.32.63 host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.115
>	21/03/19 13:10:41,000	1553170241 duration=619 dest=78.138.128.15 action=TCP_TUNNELED status=200 bytes_in=359 http_method=CONNECT url=tcp://78.138.128.15:443/ - src=10.11.36.115 category=none bytes_out=396 http_user_agent="73089/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - dest = 78.138.128.15 host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.115

Les multiples adresses concernées se situent en Russie, on retrouve donc les différentes adresses cibles de la fuite de données.

IP Address	Country	Region	City
78.138.128.15	Russian Federation 🇷🇺	Tatarstan, Respublika	Kazan

78.138.128.106	Russian Federation 🇷🇺	Tatarstan, Respublika	Kazan
----------------	-----------------------	-----------------------	-------

IP Address	Country	Region	City
212.24.32.63	Russian Federation 🇷🇺	Moskva	Moscow

IP Address	Country	Region	City
46.252.242.4	Russian Federation 🇷🇺	Sankt-Peterburg	Saint Petersburg
46.252.242.8	Russian Federation 🇷🇺	Sankt-Peterburg	Saint Petersburg

L'intégralité des IP malveillantes sont situées en Russie :

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

Country	nombre
Russia	220

La liste d'IP malveillantes transmises est-elle complète ?

Afin de limiter les risques futurs et vérifier la liste des IP malveillantes transmises dans le rapport, nous devons vérifier que cette liste est complète. Il s'avère que de nombreuses IP localisées en Russie reçoivent également des paquets depuis les postes infectés. Par exemple, nous identifions également les adresses suivantes :

81.94.32.11, 81.94.32.18, 46.252.242.8, 212.24.32.63, 78.138.128.106, 78.138.128.15, 78.138.128.10...

Quel volume de données a été envoyé ?

Maintenant que l'on a isolé les adresses vers lesquelles les données sont envoyées, on peut estimer le volume de données sorties du réseau.

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

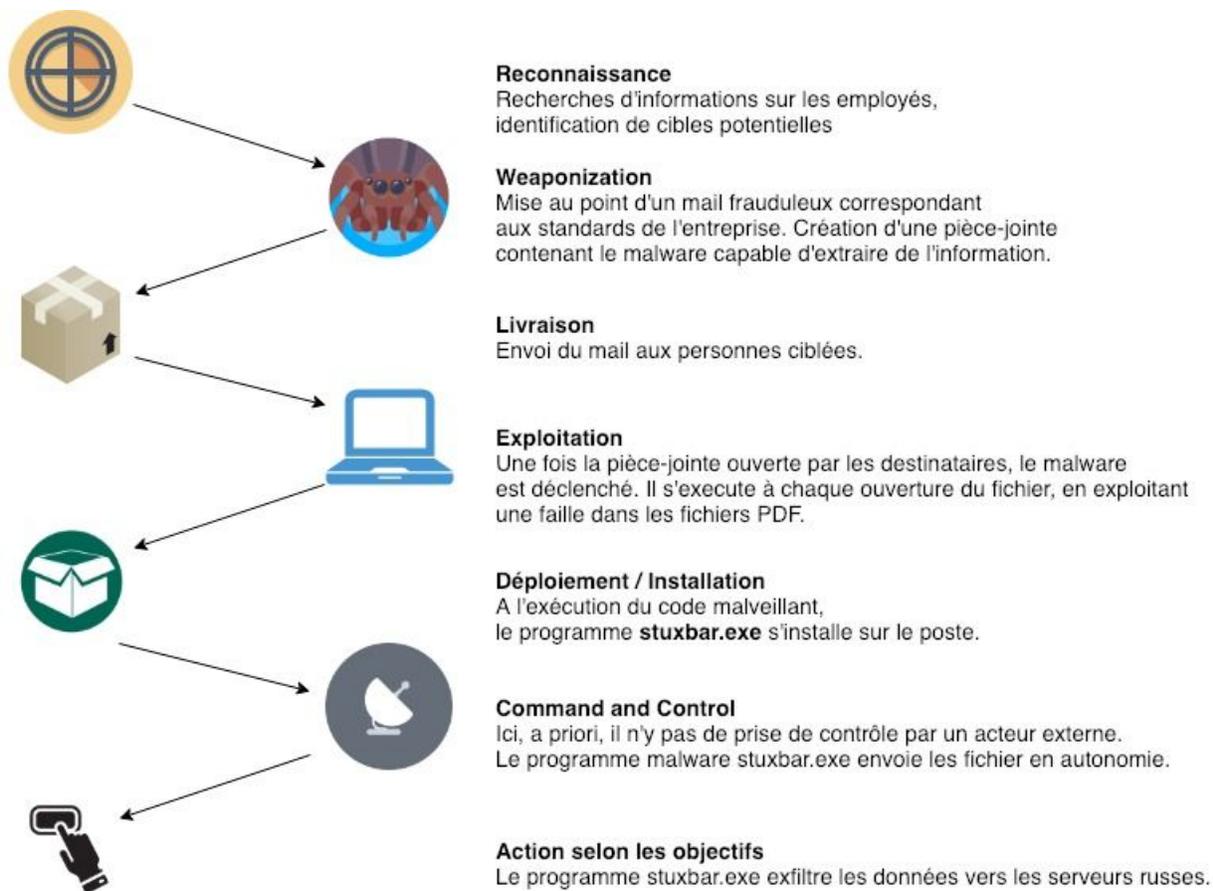
src	sum(bytes_out)
10.11.36.115	43315
10.11.36.93	44720

En tout, rien qu'avec la liste d'adresses dans le fichier *banet.csv* initialement transmise, ce sont plus de 87'000 bytes transmis, soit 0.087 Mo.

Modèle en Diamant



Cyber Kill Chain



Perspectives de Cyber Threat Intelligence

Afin de contrer d'éventuelles nouvelles attaques, plusieurs axes d'amélioration peuvent être envisagés :

- **Prévention** : Formation et sensibilisation du personnel aux menaces les plus courantes. Inclusion d'un bandeau/message d'avertissement pour l'ouverture des pièces jointes.
- **Protection** : Déploiement d'une solution antivirus sur les postes des employés. Etablissement de règles firewall sur les flux identifiés comme suspects.
- **Anticipation** : Veille sur les menaces existantes, identification des flux dangereux, mise à disposition d'une base de données actualisée de menaces.

- **Détection** : Surveillance des flux et mise en place d'alertes. Exercices d'intrusion interne pour identifier les faiblesses. Emploi de services de tests d'intrusion sur le réseau interne.
- **Investigation** : Comprendre les motivations des attaquants, les fichiers ciblés. Analyse forensic des postes compromis comme vu dans ce TP.
- **Remédiation** : Bloquer les adresses IP des attaquants, application rapide de correctifs contre le même type d'attaque.

Conclusion

Nous avons identifié et caractérisé la menace. Nous avons identifié la source et estimé la volumétrie de données concernées. Nous proposons également des séries de mesures à prendre afin de limiter la propagation de l'attaque dans l'immédiat, et éviter que des événements similaires ne se produisent à nouveau.