INF726 - Cybersécurité

Telecom Paris

MS Big Data et Analyse de données massives

Mars 2020

Prise en main de l'outil Splunk

TP organisé par:

Nicolas Pierson

Table des matières

I. Contexte

Profitant de la situation chaotique liée au Covid-19, le groupe d'attaquants Ваиет a lancé une attaque de grande ampleur. Depuis le 18 mars 2020, plusieurs fuites massives de données ont été attribuées à ce groupe que les chercheurs estiment lié aux services secrets russes et implanté en Russie. La première attaque attribuée à Ваиет date de 2018, lorsque plusieurs institutions gouvernementales situées aux USA avaient été attaquées par une campagne de spear phishing visant à installer un ver nommé à l'époque Lombrix. Les secteurs cibles pour cette nouvelle campagne baptisée Banacry sont des acteurs des télécommunications, de l'aéronautique et de la défense notamment de pays situés en zone Europe et membres de l'OTAN. Les techniques utilisées n'ont pas été formellement identifiées mais des connexions à des serveurs C&C ont été repérées par les experts de McTersky (éditeur d'antivirus) Les url et les adresses IP de ces C&C apparaissent ci-dessous ainsi que les condensats (hash) des fichiers infectés.

II. Démarche de recherche (Investigation)

- **<u>Analyse des informations reçues par MacTersky:</u>**

La société McTersky nous a communiqué un ensemble de journaux Splunk, catégorisés comme suit:

La société McTersky nous a communiqué un ensembles de journaux d'événements SI, afin d'investiguer et analyser l'origine de l'attaque. L'ensemble des données qui nous ont été communiquées, sont scindées en plusieurs types de log:

- **Bluecoat :** Proxy web
- **cisco:esa** : Passerelle Mail
- **fgt_traffic** : Firewall réseau
- **linuxsecure** : Infos d'authentification Linux
- **portcontrol** : Branchement support amovible
- **streammysql** : Ecoute réseau et interprétation protocolaire de SQL
- **winhostmon**: Infos de création de process Windows

Toutes ces données sont disponibles sur Splunk pour analyse, où nous avons mené toute notre analyse.

On commence par effectuer les recherches de base avec quelques indicateurs de compromission (IOC) dont on dispose : URL de connections, IP et hash (signatures de fichiers malveillants) :

Indicateurs de compromissions (IOC) :

C2
jsaxsd.jelas.lunaclouds[.]com
info.akademy.rhclouds[.]com
46.252.242.1
46.252.242.2
46.252.242.7
46.252.242.8
46.252.242.9
46.252.242.10
81.94.32.10
81.94.32.11
81.94.32.17
81.94.32.18
81.94.32.19
212.24.32.56
212.24.32.57
212.24.32.62
212.24.32.63
212.24.32.64
212.24.32.65

Hashes
53555938742c97ff01f9a7f8b6f15587
bb911912db1295abf8d7613852624b50
b6469dcaffd168b7d0afc414b89685b5
f15443b088f7dfaa289af9e192c9cfc8
bfe3e1817c0c87d23980d87a8c0abbad

Une première recherche sur les URL et les hash s'avère infructueuse :

recherche des URL:

jsaxsd.jelas.lunaclouds OR info.akademy.rhclouds

No matching events found.

recherche des hash:

53555938742c97ff01f9a7f8b6f15587 OR bb911912db1295abf8d7613852624b50 OR b6469dcaffd168b7d0afc414b89685b5 OR f15443b088f7dfaa289af9e192c9cfc8 OR bfe3e1817c0c87d23980d87a8c0abbad

No matching events found.

Ni les URL ni les hash n'apparaissent dans nos logs. On ne peut donc pas initialement exploiter ces informations.

On essaie alors une recherche sur les IP dont on dispose :

recherche des adresses IP

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

Time	Event
2020-03-19T17:35:45+0100	1584635745 duration=634 dest=81.94.32.19 action=TCP_TUNNELED status=200 bytes_in=427 http_method=CONNECT url=tcp://81.94.32.19:443/ - src=10.11.36.115 category=none bytes_out=447 http_user_agent=" 18924/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - -
2020-03-19T17:31:48+0100	1584635508 duration=632 dest=46.252.242.8 action=TCP_TUNNELED status=200 bytes_in=436 http_method=CONNECT url=tcp://46.252.242.8:443/ - src=10.11.36.93 category=none bytes_out=430 http_user_agent=" 50984/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - -
2020-03-19T17:27:51+0100	1584635271 duration=636 dest=212.24.32.57 action=TCP_TUNNELED status=200 bytes_in=452 http_method=CONNECT url=tcp://212.24.32.57:443/ - src=10.11.36.115 category=none bytes_out=443 http_user_agent=" 81455/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - -
2020-03-19T17:27:51+0100	1584635271 duration=566 dest=46.252.242.8 action=TCP_TUNNELED status=200 bytes_in=371 http_method=CONNECT url=tcp://46.252.242.8:443/ - src=10.11.36.93 category=none bytes_out=400 http_user_agent=" 25196/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - -
2020-03-19T17:23:54+0100	1584635034 duration=622 dest=212.24.32.63 action=TCP_TUNNELED status=200 bytes_in=377 http_method=CONNECT url=tcp://212.24.32.63:443/ - src=10.11.36.93 category=none bytes_out=378 http_user_agent=" 69162/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - -

On obtient de très nombreux éléments de réponse. On dispose donc dans nos logs, de traces de IP des C&C qui ont mené l'attaque. Il faut maintenant affiner l'information. En premier lieu, on considère la date :

date: année

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| top limit=20 date_year

date_year	count	percent
2020	249	100.000000

date: mois

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| top limit=20 date_month

date_month	count	percent
march	82	100.000000

date: jour

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| top limit=20 date_mday

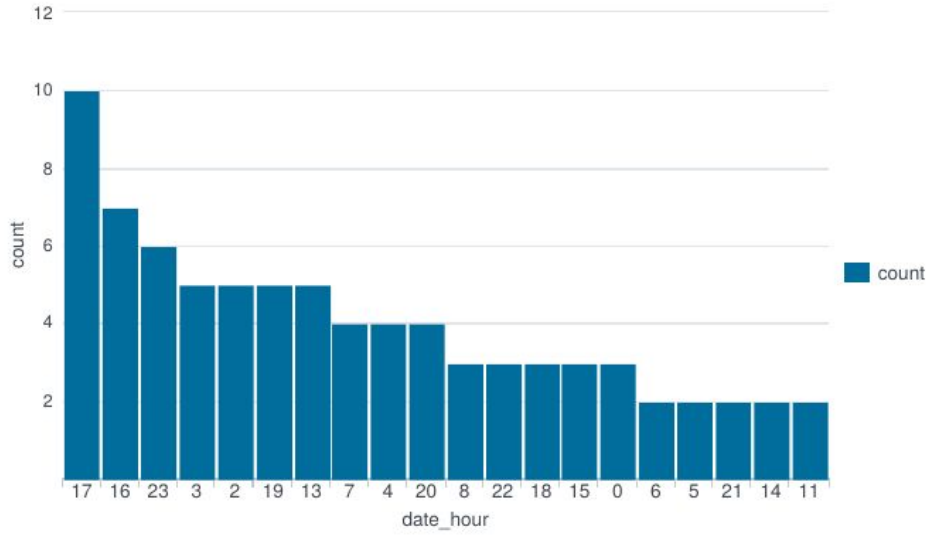
date_mday	count	percent
19	51	62.195122
18	31	37.804878

On remarque que les attaques se sont donc concentrées sur deux jours : les mercredi 18 et jeudi 19 mars 2020.

Regardons l'heure des attaques :

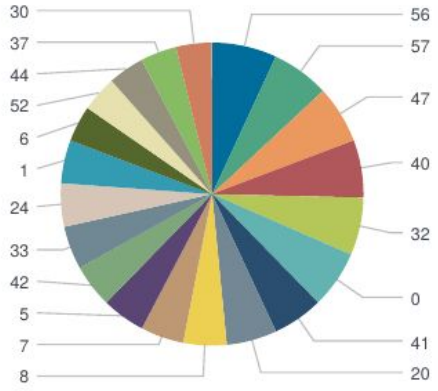
date: heures

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| top limit=20 date_hour



dates: minutes

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| top limit=20 date_minute



On se rend compte que les attaques sont régulièrement réparties, tant en terme d'horaires que de minutes, donc pas d'insights à tirer concernant les plages horaires des fuites d'informations.

On peut trouver des informations complémentaires utiles sur ces attaques.

En faisant par exemple une recherche sur le host et le sourcetype des IP :

host du site à l'origine de l'attaque

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| top limit=20 host

host	count	percent
proxy-xx.buttercupgames.com	259	100.000000

type de source à l'origine de l'attaque

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 source=eventgen| top limit=20 sourcetype

sourcetype	count	percent
bluecoat	259	100.000000

On constate que les attaques proviennent toutes du même host de type **bluecoat** (un proxy web) : le site proxy-xx-buttercupgames.com. Le site a un nom suspicieux, et clairement ne devrait pas communiquer en temps normal avec le ministère des armées.

On s'intéresse enfin à l'élément le plus important : les sources, c'est-à-dire les machines du ministère des armées, qui ont établi une connexion avec les adresses IP incriminées, les sources à partir desquelles les informations ont fuité :

source de connexion

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| top limit=20 src

src	count	percent
10.11.36.93	136	52.918288
10.11.36.115	121	47.081712

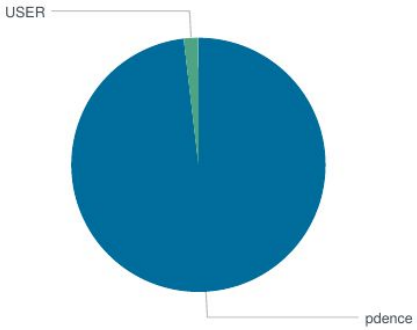
Les connexions proviennent de deux adresses IP: 10.11.36.93 et 10.11.36.115.

- **<u>Analyses relatives aux deux IP privées trouvées:</u>**

On s'intéresse à ces deux adresses, l'une après l'autre.
On commence par faire une recherche sur la 10.11.36.93 :

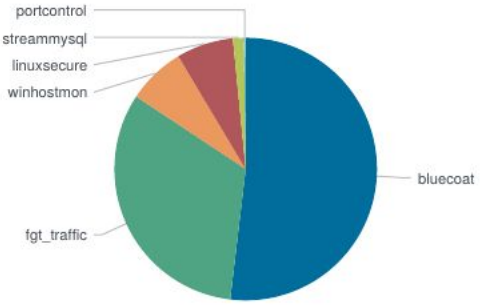
utilisateur de l'IP source de connexion

10.11.36.93| top limit=20 user



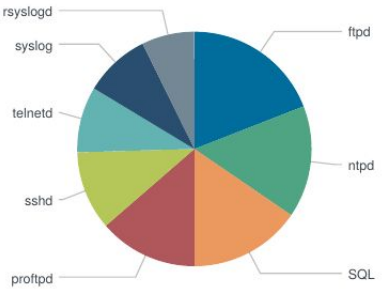
type de source de connexion

10.11.36.93| top limit=20 sourcetype



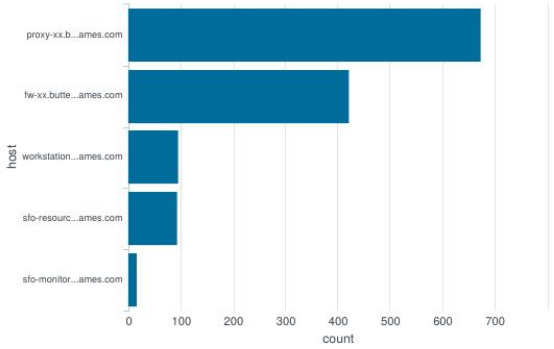
applications incriminées dans la connexion

10.11.36.93| top limit=20 app



proxy de connexion

10.11.36.93| top limit=20 host



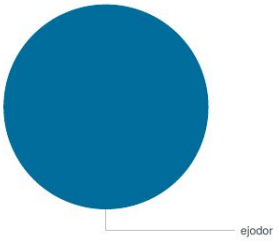
Les connexions venant de cette IP privée, sont quasiment toutes, le fait du même user : pdence (Pierre Dence). Elles émanent de logs bluecoat (proxy web), confirmant une fuite d'informations par source web. Bien qu'elles émanent de plusieurs proxy différents, on retrouve dans tous les proxy le fragment d'URL buttercupgames.com, ce qui confirme une attaque centralisée depuis une même source.

Enfin, on peut noter dans les applications incriminées, l'utilisation conséquente de SQL, et ce à des heures de non ouverture, ce qui peut laisser craindre le transfert massif de données lors de l'attaque. Une analyse plus technique des éléments malveillants devra être menée, afin de bien cerner l'étendue réelle de cette attaque.

On procède de façon similaire avec la seconde IP 10.11.36.115, en se concentrant uniquement sur cet utilisateur :

utilisateur de l'IP source de connexion

10.11.36.115| top limit=20 user



On a là encore un seul utilisateur : ejodor (Eloise JODOR).

- **<u>Analyse préalable des processus windows (.exe) déclenchés par pdence et ejodor:</u>**

On peut donc poursuivre la recherche en se focalisant sur deux utilisateurs cibles de l'attaque : pdence et ejodor.

On se focalise sur ejodor en faisant une recherche basique.

On obtient des résultats généraux intéressants. Par exemple, de nombreux logs de l'utilisateur ejodor relèvent de la saisie de mots de passe, ici à un horaire où clairement aucun utilisateur ne peut être présent sur son lieu de travail :

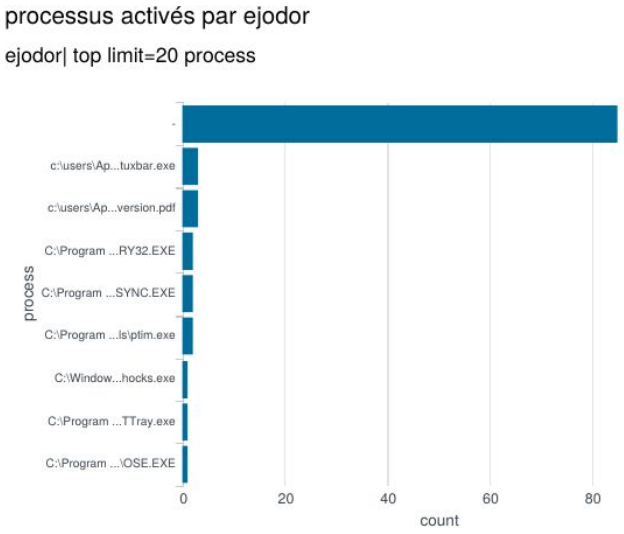
2020-03-19T00:04:03+0100	Mar 18 23:04:03 dest=sfo-resources-04.it.defense.fr telnetd[25576]: action=success Accepted password for user= ejodor from src=10.11.36.115 port 13825 app=telnetd

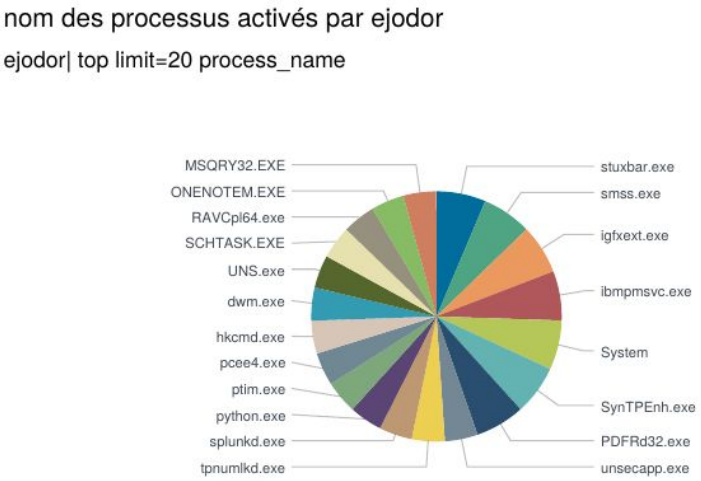
Egalement, certains logs de l'utilisateur ejodor relèvent de la requête SQL massive :

2020-03-18T22:33:00+0100	{timestamp:"2020-03-18T21:33:00" ,app=SQL,user=ejodor,bytes=581,src=10.11.36.115,src_port=44754,dest=10 .100.0.2,dest_port=3306,duration=465,transport=tcp,query=" SELECT * FROM customers WHERE customer_uid= 0f9222a0-44b4-4045-8e54-8f1a79403405"}

Tout cela laisse craindre une attaque ayant pour but la saisie de mots de passe et la collecte massive d'informations.

Plus spécifiquement, on s'intéresse aux processus activés par ejodor :

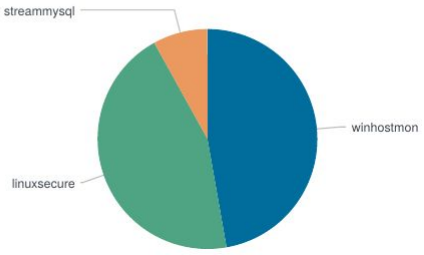




On constate qu'outre les processus réguliers, deux processus sont plus fréquents que les autres : stuxbar.exe et reconversion.pdf (de nom stuxbar.exe et PDFR32.exe).

type de processus activés par pdence

pdence| top limit=20 sourcetype

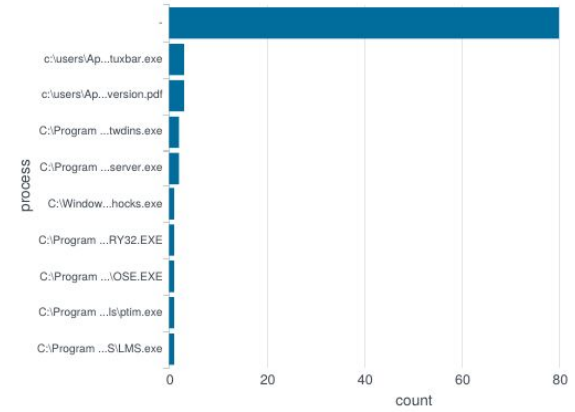


Ces processus sont de type linuxsecure (infos d'authentification), winhostmon (création de process Windows) et streamysql (protocle sql), ce qui laisse encore penser qu'on a affaire à des process qui tentent de collecter des informations ou de créer des processus d'écoute, sur plusieurs canaux différents.

Si on regarde ensuite les processus déclenchés par Pierre Dence :

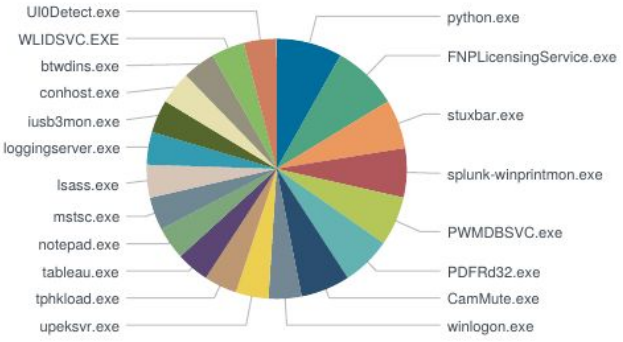
processus activés par pdence

pdence| top limit=20 process



nom des processus activés par pdence

pdence| top limit=20 process_name



Là encore, deux processus reviennent le plus fréquemment : stuxbar.exe et reconversion.pdf. Il faut donc s'intéresser à ces deux processus.

- **<u>Analyse chronologique de la réception d'email entre le 17 et le 18/03:</u>**
  - **<u>Analyse des emails reçus le 17/03:</u>**

Rappelons à ce stade aussi, que le début des fuites pour les deux adresses sources, a commencé respectivement:

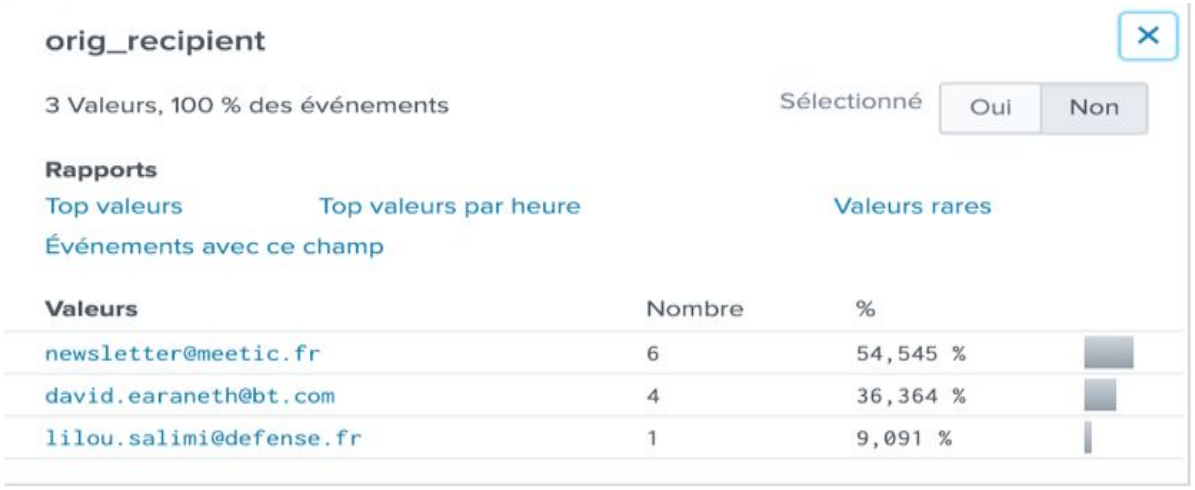
le 18/03/2020 à 11:15:41,000 pour l'adresse privée : 10.11.36.93 (Pierre Dence)
et à 11:43:20,000 pour la seconde ip privée : 10.11.36.115 (Eloise Jodor).

Nous proposons alors de continuer les investigations, et ce avant ces deux dates, afin de confirmer notre intuition suivant laquelle, il s'agit de processus suspects derrière cette fuite d'information.

Etant donné que le groupe Banet est reconnu pour avoir effectué des attaques de Spear Phishing de par son passé, on serait tenté d'aller voir les mails qui ont été reçus par ces deux utilisateurs (Pierre Dence et Eloise Jodor), et ce avant le 18/03 (date exclue), date à laquelle les informations ont commencé à fuiter.

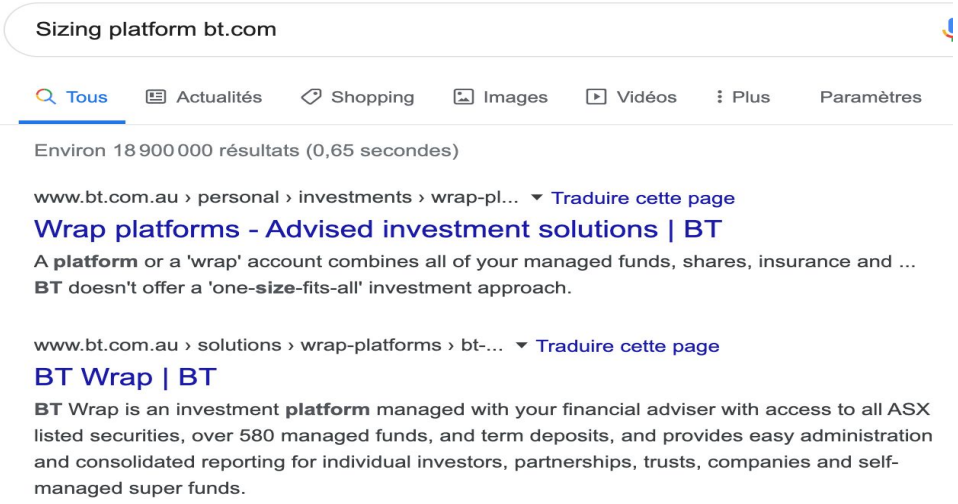
On remarque que pour les deux users, il existe deux plages de dates à analyser. La première plage concerne le 17/03 :
Les mails reçus le 17, par chacun des deux utilisateurs :

Les mails reçus par l'utilisateur Pierre Dence :



mentionnant respectivement, des expéditeurs :
=> meetic, bt et un mail d'un collègue lilou.salimi@defense.fr

au passage, suite à une brève vérification de l'adresse @bt.com, il s'avère qu'il s'agit d'un échange avec un commercial probablement de la boîte Advised Investment Solutions BT =>



donc, rien d'alarmant reçu le 17/03/2020.

Les mails reçus le même jour par Eloise :

Rien d'alarmant non plus, dans la mesure où les expéditeurs ne sont que :
Uber, Société Générale, Betclic, et un mail d'un collègue.

Ceci dit, nous notons d'ores et déjà l'utilisation risquée, faite de leurs adresses emails professionnelles. Ces utilisateurs ne sont pas assez sensibilisés à la gravité d'utiliser leur adresse professionnelle, compte tenu de leur poste au sein de la défense Française.

- **<u>Analyse des emails reçus le 18/03 (avant le début des fuites):</u>**

Passons au 18/03, et ce peu avant le début des fuites, c'est à dire avant 11:15:41,000 (Pierre Dence) et 11:43:20,000 (Eloise Jodor) :

Les mails reçu par Pierre Dence ce jour là, respectivement à 11:14:43,000 et 11:10:34,000 :

Les mails reçus par Eloise Jodor ce jour là :

avec les heures qui correspondent à l'envoi du mail de la marine mobilité, 11:10:34,000 // 11:33:58,000 // 11:38:39,000.

- **Conclusion intermédiaire:**

Il en ressort une adresse email non anodine, envoyée à ces utilisateurs, et qui après vérification, ne correspond pas à une adresse mail de la Marine Française => "***liste@marinemobilite.com***"

On trouve aussi que ce mail contient une PJ suspecte, reconversion.pdf.

A ce stade, nous devons encore faire le lien entre les fuites d'informations et cette pj éventuellement malveillante.

- **Analyse des processus .exe déclenchés par cette PJ:**

Logiquement, si les deux utilisateurs ont cliqué sur cette PJ, certains processus doivent avoir été déclenchés et à l'origine de la fuite d'information.

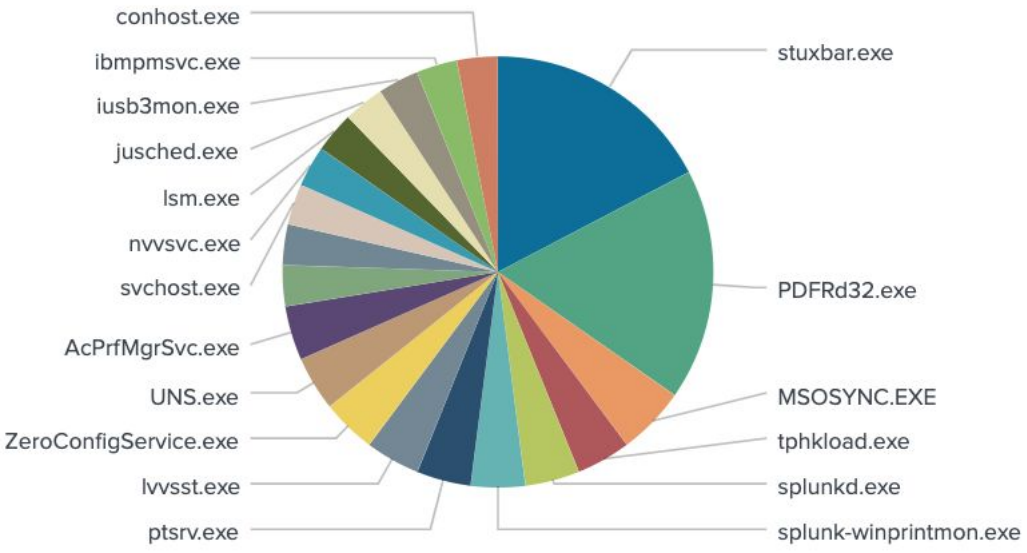
Pour cela nous allons analyser les processus windows, ou les .exe, qui ont été déclenchés sur les ordinateurs potentiellement infectés, ejodor et pdence.

i	Heure	Événement
>	18/03/2020 11:43:00,000	03/18/20 10:43:00 Type=Process process_name=stuxbar.exe dest=10.11.36.115 ProcessId=13201 Host="ejodor-0TNY60F9.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:42:50,000	03/18/20 10:42:50 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.pdf" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:39:29,000	03/18/20 10:39:29 Type=Process process_name=stuxbar.exe dest=10.11.36.115 ProcessId=13201 Host="ejodor-0TNY60F9.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:39:19,000	03/18/20 10:39:19 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.pdf" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:34:48,000	03/18/20 10:34:48 Type=Process process_name=stuxbar.exe dest=10.11.36.115 ProcessId=13201 Host="ejodor-0TNY60F9.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:34:38,000	03/18/20 10:34:38 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.pdf" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:11:24,000	03/18/20 10:11:24 Type=Process process_name=stuxbar.exe dest=10.11.36.115 ProcessId=13201 Host="ejodor-0TNY60F9.defense.fr" process="c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:11:14,000	03/18/20 10:11:14 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.pdf" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon

En effet, il s'avère que Eloise JODOR a cliqué sur la PJ reconversion.pdf, qui contenait le malware, et ce à plusieurs reprises. Ceci déclenche directement un autre malware qui doit certainement être à l'origine de la fuite d'informations => « Stuxbar.exe » qu'on a remarqué avant l'analyse des emails, tout cela avant 11:43:20,000.

```
sourcetype=winhostmon ejodor| top limit=20 process_name
```

✓ 235 événements (18/03/2020 11:10:00,000 à 31/05/2020 11:15:40,000)



Le camembert met en avant, ce jour là, la prépondérance des deux processus malveillants, pour Eloise, comparés aux autres processus qui sont beaucoup moins nombreux.

- **<u>Remarque Importante:</u>**

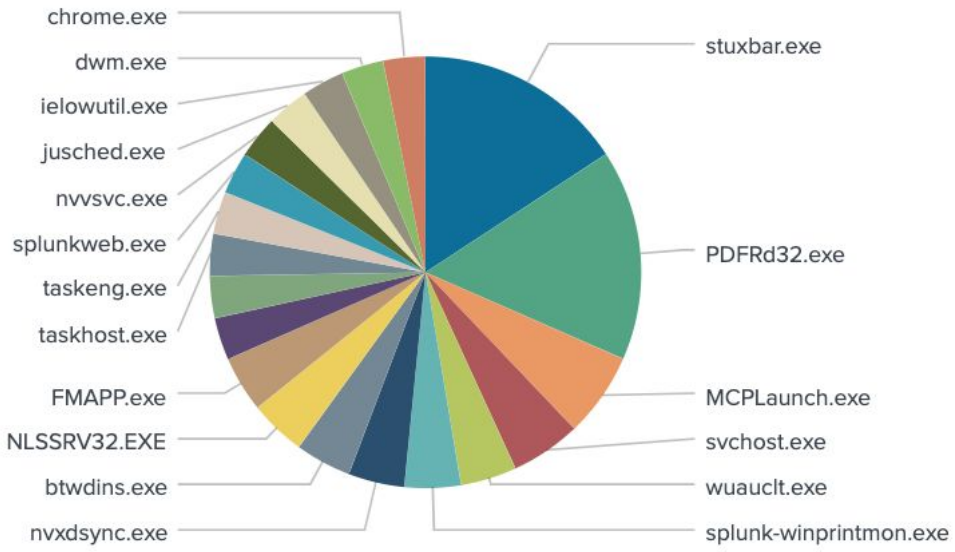
Pour Pierre Dence, nous remarquons une incohérence, dans la mesure que sont premier clic sur le fichier reconversion.pdf a été effectué à 11:39:19,000, alors que la fuite d'informations a commencé à 11:15:40 depuis son ordinateur. Ceci est une information à éclaircir encore. Ceci doit certainement être dû à un log journal qui manque, dans la mesure où il est clair maintenant que l'origine de l'attaque provient du fichier infecté "reconversion.pdf":

i	Heure	Événement
>	18/03/2020 11:13:33,000	03/18/20 10:13:33 Type=Process process_name=PsiService_2.exe dest=10.11.36.93 ProcessId=5112 Host="pdence-94DA3SF7.defense.fr" process="-" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:13:23,000	03/18/20 10:13:23 Type=Process process_name=ONENOTEM.EXE dest=10.11.36.93 ProcessId=6708 Host="pdence-94DA3SF7.defense.fr" process="-" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:11:24,000	03/18/20 10:11:24 Type=Process process_name=stuxbar.exe dest=10.11.36.115 ProcessId=13201 Host="ejodor-0TNY60F9.defense.fr" process="c:\users \AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\stuxbar.exe" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon
>	18/03/2020 11:11:14,000	03/18/20 10:11:14 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.pdf" host = workstation-xx.buttercupgames.com | source = eventgen | sourcetype = winhostmon

On voit donc bien le processus reconversion.pdf qui déclenche aussi, 10 secondes après le processus malveillant Stuxbar.exe.

```
sourcetype=winhostmon pdence | top limit=20 process_name
```

✓ 235 événements (18/03/2020 11:10:00,000 à 31/05/2020 11:15:40,000)



De même, les deux processus malveillants sont bien visibles et majoritaires ce jour là toujours, contrairement au reste des processus, et ce pour Pierre aussi.

A ce stade nous confirmons donc l'origine de l'attaque, avec ces deux processus malveillants, PDFRd32.exe (reconversion.pdf) et stuxbar.exe.

- **<u>Élargissement du contexte d'investigation:</u>**

Regardons de plus près les deux processus. Une recherche sur stuxbar.exe n'apprend pas grand-chose de nouveau. En revanche, la recherche sur reconversion.pdf fournit de nouveaux éléments :

expéditeur du fichier reconversion.pdf

reconversion| top limit=20 orig_recipient

orig_recipient	count	percent
liste@marinemobilite.com	12	100.000000

Le fichier incriminé a donc été expédié par l'adresse liste@marinemobilite.com. C'est probablement une fausse adresse utilisée pour tromper les employés du ministère: Chose que l'on vérifie facilement auprès des utilisateurs internes.

Une recherche sur liste@marinemobilite.com donne :

destinataires des mails de liste@marinemobilité.com

marinemobilite.com| top limit=20 recipient

recipient	count	percent
pierre.dence@defense.fr	3	25.000000
emmanuel.coraidh@defense.fr	3	25.000000
eloise.jodor@defense.fr	3	25.000000
capucine.palaci@defense.fr	3	25.000000

On constate que l'adresse liste@marinemobilite.com a envoyé le mail contenant le fichier reconversion.pdf à quatre personnes au total, et pas uniquement à Pierre et Eloise:

- Pierre Dence (qui est donc l'utilisateur pdence),
- Emmanuel Coraidh,
- Eloise Jodor (qui est donc l'utilisateur ejodor),
- Capucine Palaci.

L'attaque était donc très ciblée, ce qui est cohérent avec l'information d'une campagne de Spearfishing (mailing ciblé).

Maintenant, la question qui se pose, est comment ces quatre utilisateurs ont été identifiés comme cibles potentielles.

Si on fait une recherche sur Pierre Dence, on remarque que celui-ci a des comportements à risque, puisqu'il utilise son adresse professionnelle pour recevoir des messages personnels. Par exemple, Pierre utilise son adresse professionnelle pour son compte Meetic :

2020-03-19T21:21:26+0100	Mon Mar 19 20:21:26 2020 orig_dest=204.118.100.129 orig_recipient=newsletter@meetic.fr orig_src=14.6.136.59 protocol=SMTP recipient=pierre.dence@defense.fr subject="Capucine souhaite vous parler" file_name="-"

De même, Eloise Jodor utilise son mail professionnel pour son compte Betclic, un site de pari en ligne :

2020-03-19T23:40:45+0100	Mon Mar 19 22:40:45 2020 orig_dest=204.118.100.129 orig_recipient=newsletter@betclic.com orig_src=205.2.107.170 protocol=SMTP recipient=eloise.jodor@defense.fr subject="Votre pari est gagnant" file_name="-"

On peut formuler les hypothèses suivantes :

1/ profils ciblés en raison de leurs comportements qui les ont fait identifier par l'attaquant comme des profils moins prudents et plus susceptibles d'ouvrir des pièces jointes.

2/ profils identifiés comme étant en reconversion (page Linkedin publique avec cette information?), d'où l'adresse marinemobilité et la pièce jointe reconversion.pdf.

3/ envoi du mail à Capucine Palaci car soupçon de liaison avec Pierre Dence (intitulé message Meetic : Capucine veut vous parler) et donc pas de méfiance entre les deux individus.

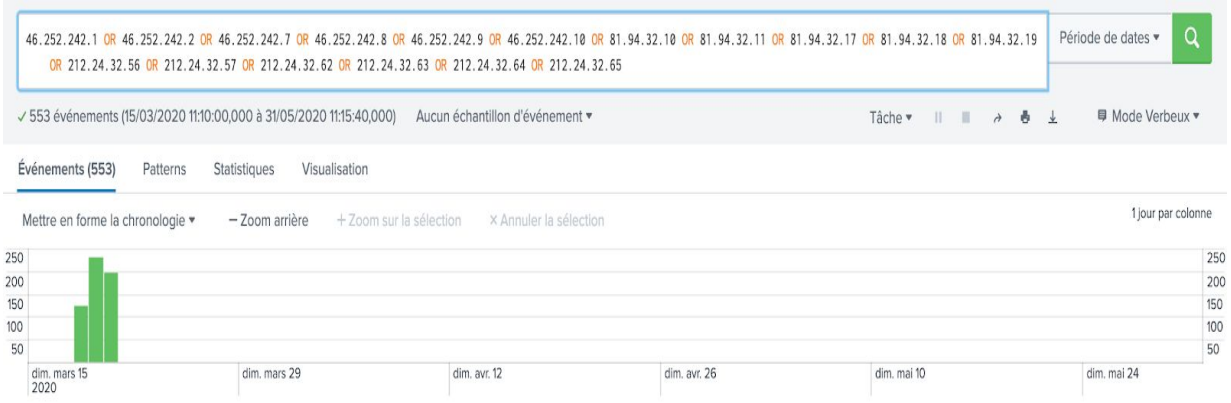
On peut enfin s'intéresser aux aspects suivants : possibles adresses IP d'attaquants non détectées. Par exemple, la liste des logs indique comme IP :

212.24.32.56
212.24.32.57
212.24.32.62
212.24.32.63
212.24.32.64
212.24.32.65

On remarque un pattern clair dans les adresses. On pourrait supposer par exemple que les IP 212.24.32.58, 212.24.32.59, 212.24.32.60 et 212.24.32.61 ont pu aussi lancer une attaque. Une recherche sur ces IP montre qu'en effet elles apparaissent toutes dans nos logs. Il pourrait être utile de les pister.

- **<u>Elargissement des plages de recherches IP aux patterns décrit:</u>**

De plus, en faisant une recherche rapide, sur les adresses ip malveillantes communiquées : nous remarquons qu'elles sont aux nombres de **553** communications envoyées



[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]

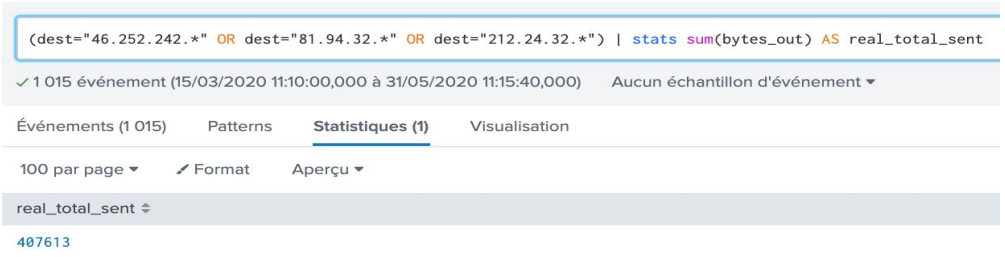
En élargissant la recherche à ces autres adresses potentielles, nous confirmons notre intuition, dans la mesure où ces fuites, s'étendent à beaucoup d'autres adresses que celles communiquées par McTersky :

dont le nombre s'élève à **1009** paquets, ce qui sous-entend que les adresses malveillantes sont beaucoup plus nombreuses que celles communiquées initialement.

=> [dest="46.252.242.*" **OR** dest="81.94.32.*" **OR** dest="212.24.32.*"]

Ceci implique que l'ampleur de l'attaque est beaucoup plus grande que ce qui a été anticipé, en termes de volume d'informations envoyées. En effet, nous passons de **223369** bytes :

à **407613** bytes, envoyés en deux jours :



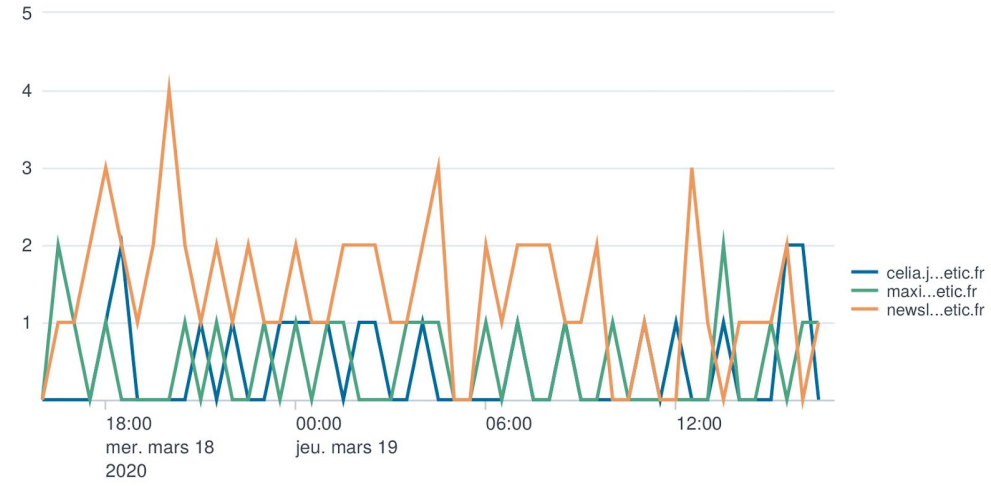
Ce qui augmente l'ampleur de l'attaque.

- **<u>Use Case Meetic.fr:</u>**

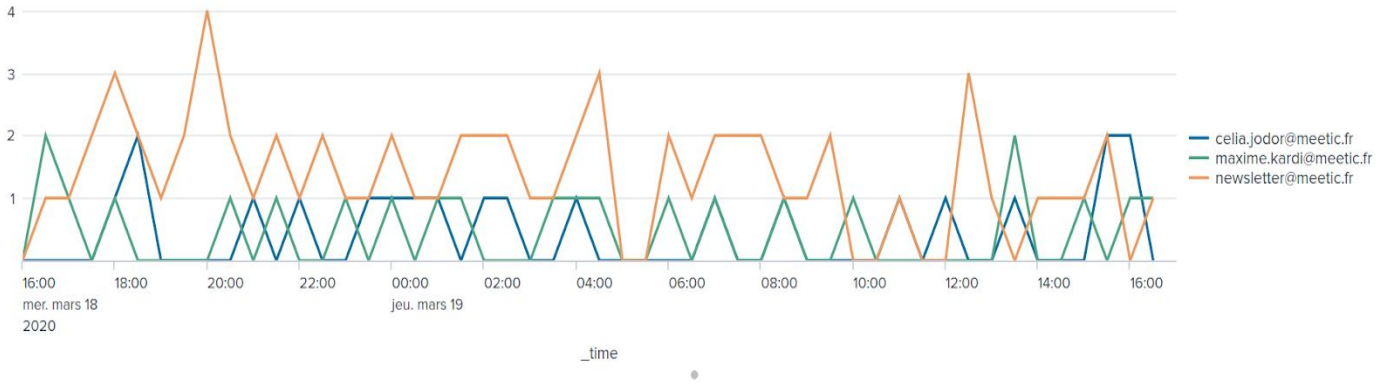
Une brève analyse de l'utilisation des emails professionnels, relative au site de rencontres Meetic, montre qu'il y a bien d'autres employés (non pas uniquement les 4 utilisateurs ciblés par les attaquants) qui utilisent leur adresse professionnelle à des fins personnelles.

```
meetic| timechart count by orig_recipient limit=10
```

Adresses sources provenant de Meetic et horaires le 18 et 19 Mars



Les 4 utilisateurs mentionnés, envoient reçoivent des emails et des newsletters provenant directement de meetic:



On peut éventuellement penser que l'attaquant a su en tirer profit, en faisant du social engineering, ce qui lui a permis de récupérer assez d'informations sur ces 4 utilisateurs, à partir des sites sociaux: meetic par exemple.
On remarque l'utilisation faite des utilisateurs de la Défense Française, de leurs adresses emails, par exemple ici des emails reçus de la plateforme meetic, sur des adresses professionnelles defense.fr:

subject

5 Valeurs, 100 % des événements

Sélectionné Oui Non

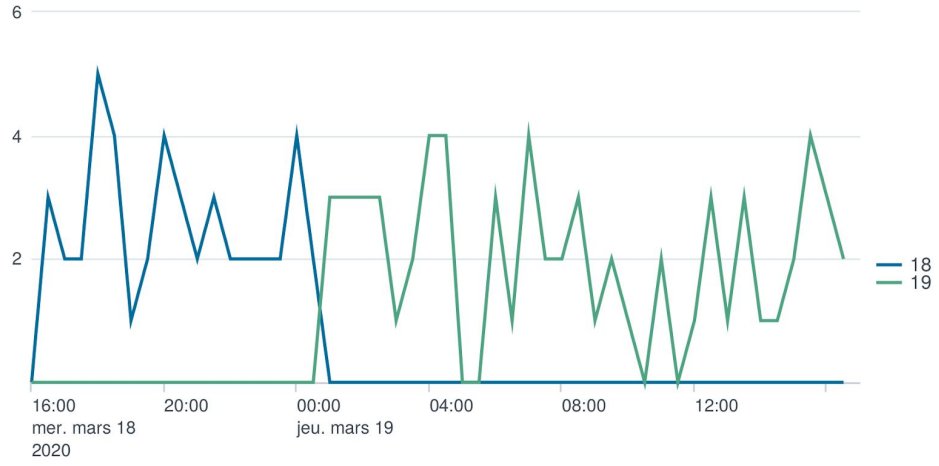
Rapports

Top valeurs Top valeurs par heure Valeurs rares

Événements avec ce champ

Valeurs	Nombre	%
Rose a flashe sur vous	29	24,786 %
Alex souhaite vous parler	25	21,368 %
Nicolas vous a repondu	25	21,368 %
Christophe vous a repondu	20	17,094 %
Capucine souhaite vous parler	18	15,385 %

Horaires d'envoi de mail Meetic



Ceci soulève clairement un point qui est que d'autres utilisateurs peuvent d'ores et déjà faire partie d'un plan d'attaque, étant donné leur utilisation non professionnelle de leur compte @defense.fr. On peut supposer qu'une deuxième vague pourrait avoir ultérieurement pour ne pas éveiller les soupçons avec les nouvelles cibles.

III. Résumé de l'attaque (Cyberkill chain)

A. Reconnaissance:

La reconnaissance consiste à identifier des personnes cibles qui seront une voie d'entrée pour l'attaquant. Au vu du caractère très spécifique de l'attaque, c'est à dire des victimes qui sont en situation de recherche de reconversion professionnelle et à l'affût de nouvelles opportunités, on peut penser que l'attaquant a pu avoir recours à de l'ingénierie sociale.
On peut faire l'hypothèse que ces personnes ont dû afficher leur volonté de changer de profession sur les réseaux sociaux tels que linkedin et en affichant leur adresse mail comme contact primaire.
Suite à cela, l'attaquant n'avait qu'à leur adresser un mail contenant une offre correspondant à leurs aspirations.

B. Préparation

L'étape d'après consiste à créer un malware « stuxbar.exe » qui s'exécute à l'ouverture du mail et téléchargement du fichier reconversion.pdf qui semble intéressant pour la personne en recherche de possibilités de reconversion.

C. Livraison

L'étape de livraison consiste à envoyer aux cibles identifiées les mails avec en pièce jointe le fichier pdf et le malware.

D. Exploitation

Une fois que la victime ouvre le mail et la pièce jointe, le code du malware est exécuté et l'intrusion peut être possible avec le code déployé. L'attaquant s'est introduit sur le réseau et peut donc copier les données, continuer à se propager à travers le réseau...

E. Installation

Après l'installation de « stuxbar.exe », l'attaquant peut installer un tunnel VPN reliant le poste affecté donc le serveur interne à un réseau externe.
Le malware peut continuer à installer des logiciels malveillants pour endommager ou non l'ordinateur...

F. Contrôle

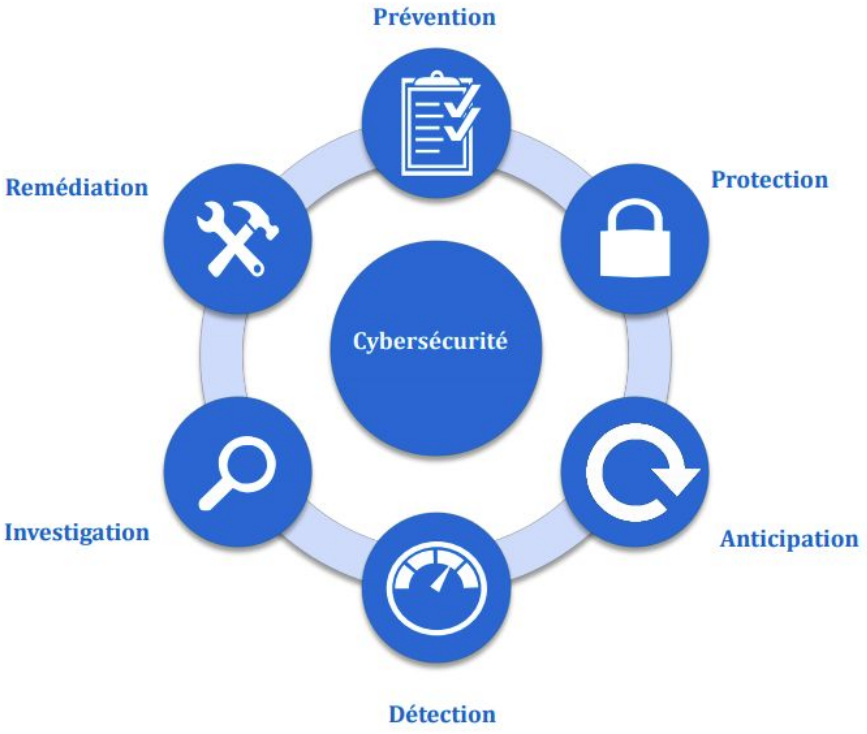
L'attaquant a désormais le contrôle de la machine. Il peut décider de ralentir la machine de la victime, la bombarder avec des publicités intempestives, voler des données personnelles ou professionnelles... Encore mieux que tout cela, il peut se faire passer pour la victime en interne et user de son titre ou de son poste pour obtenir d'autres informations. Il peut aussi contrôler le réseau de la victime, et profiter de ses droits d'accès (encore plus s'il s'agit d'un

administrateur) pour envoyer des paquets sur le réseau interne vers les serveurs de l'attaquant.

G. Action

L'attaquant peut continuer à chercher des IP pour obtenir d'autres sources d'informations, et se déployer davantage sur le réseau.
En plus de cela, on remarque que l'attaquant a réussi à récupérer d'autres mots de passe. Au vu des requêtes effectuées depuis l'adresse d'Eloïse Jodor, (SELECT * FROM …), on peut faire l'hypothèse que l'attaquant a effectué des requêtes SQL malveillantes à partir de l'exécution de Stuxbar.exe et peut-être utilisé ces mots de passe pour accéder à d'autres bases de données.
Suite à cela, il peut demander des rançons pour ne pas rendre publiques les informations dérobées, ou restituer le poste à la victime par exemple.

IV. Mesures à prendre en compte issues de l'analyse de la Threat Intelligence réalisée



A. Anticipation:

Les utilisateurs doivent respecter une charte d'utilisation stricte, et ce des outils professionnels qui leur sont mis à disposition. En effet, ces quatres utilisateurs ont mis le SI de la défense Française dans une situation à risque. Aussi, il faudra équiper le serveur

SMTP par un anti-virus plus puissant, capable de détecter les fichier infectés, capable de détecter les hoax.
Sensibiliser le personnel avec des formations et des campagnes cybersécurité.

B. Détection

Monitoring régulier des événements SI et des journaux machines, avec des logiciels spécialisés (Splunk), afin de détecter des processus inhabituels, pour plus de réactivité. Par exemple, analyser les logs pour détecter de possibles process tournant la nuit hors des horaires d'ouverture.
Equiper les équipements informatiques (serveurs et ordinateurs personnels) de logiciels antivirus performants avec antispam capable de détecter des mails infectés ou suspicieux évidents.

C. Investigation

Grâce aux activités d'investigation réalisées sur Splunk, il est important d'avoir des outils capables de tracer tous les événements ayant affecté le SI, dans la mesure qu'il est possible d'analyser et d'investiguer les journaux dès qu'il y a une menace.
Disposer de personnel qualifié en cybersécurité, maîtrisant les outils d'analyse et d'enquête, pour pouvoir bien qualifier les attaques une fois constatées.
Recruter des experts IT capables de recueillir et analyser les processus malveillants utilisés dans l'attaque, afin d'en maîtriser le fonctionnement et les symptômes non apparents.

D. Remédiation

Afin de remédier à ce genre d'attaques, il faut absolument alerter les utilisateurs ayant déjà reçu le mail et la pj infectée, et les prévenir afin qu'ils ne cliquent plus sur le pdf, ou qu'ils ne cliquent pas (si aucun clic de leur part). Dans un second temps, et parallèlement à la première action, il faut bloquer l'hémorragie et arrêter immédiatement la fuite d'informations. Dans un troisième temps.

Certains Hashes de fichiers malveillants n'ont pu être utilisés, ceux-ci peuvent être comparés aux traces laissés par les processus malveillants, ou comparés à tout autre fichier ayant le même Hashe, cette analyse pouvant aboutir à la découverte d'une seconde origine d'infection. On a bien vu que la fuite d'information de l'ordinateur de Pierre Dence, est venu avant que celui-ci ne clique sur la pj reconversion.pdf, donc ces Hashes peuvent permettre de trouver l'origine de l'infection de l'ordinateur de Pierre Dence.

Enfin, on effectuera des prélèvements sur les postes infectés afin de récupérer les deux fichiers malveillants. Après analyse, on pourra comprendre comment ils se sont comportés, et éventuellement déterminer leur origine ainsi que les manières de les déjouer.

Dans un second temps, il est nécessaire d'aller voir les 4 personnes ayant été ciblées par l'attaque. Le cas échéant, s'il s'avère que l'attaque résulte d'une violation grave des règlements intérieurs et des règles de sécurité, on pourra prendre à leur égard une sanction disciplinaire.

E. Prévention et protection

Pour éviter que d'autres incidents ne se répètent, il sera nécessaire de rappeler les consignes de bon usage des adresses mails. Il est important de se mettre à la place de l'utilisateur, pour anticiper les fautes humaines qui ne manqueront pas de se produire.
On pourra enfin faire le point sur le règlement et discuter une possible mise à jour si celui-ci s'avère insuffisant en termes de protection.
D'un point de vue plus technique, il est nécessaire de renforcer la sécurité du serveur SMTP, avec un antivirus pouvant détecter ce genre de menaces. Il faut aussi limiter les accès internet pour certains sites aux utilisateurs internes et ne whitelister certains sites qu'après considération des risques et des besoins.

V. Diamond