



Projet Cyber Threat Intelligence

- Benyang SUN
- Di WU
- Li XU

25.03.2020

Sommaire

Sommaire	2
Contexte	3
Données à disposition	3
Le résumé de l'attaque et sa chronologie	5
Identification des IPs infectés	5
Identification d'attaque	7
Une annexe contenant les IOC confirmés et les nouveaux IOC identifiés	13
IOC confirmés	13
IOC identifiés	14
Conclusion	17

Contexte

De nos jours, la cybersécurité est de plus en plus importante. Dans ce projet, nous sommes donnés un scénario imaginaire d'une attaque organisée comme illustré le suivant.

Profitant de la situation chaotique liée au Covid-19, le groupe d'attaquants Baïnet 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.

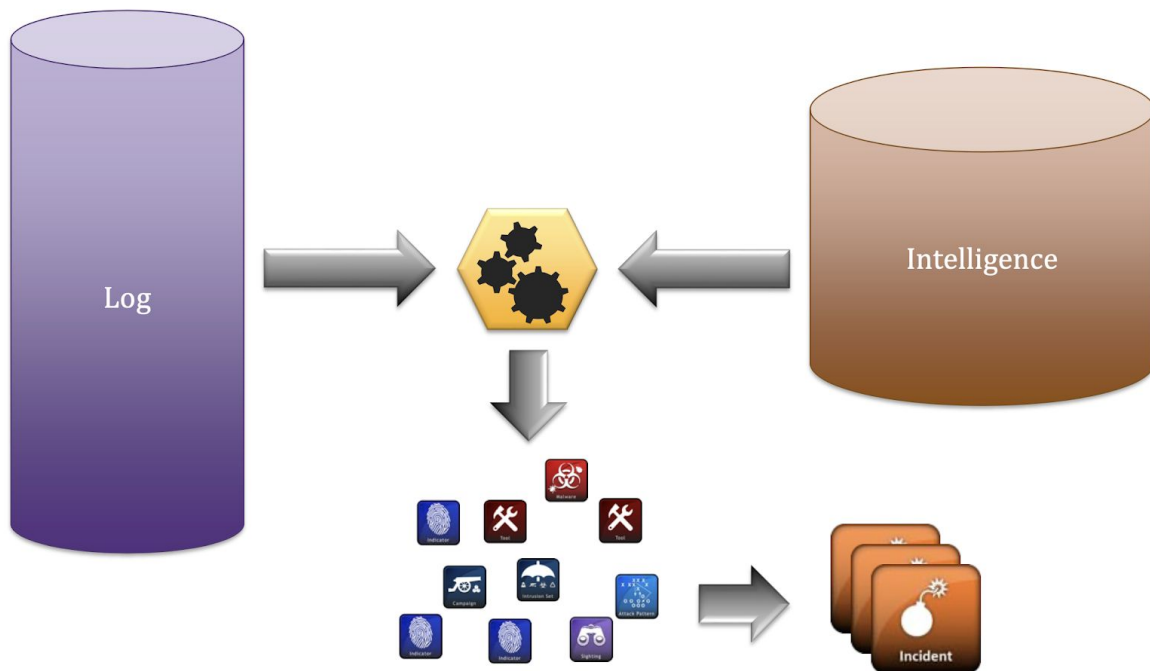
Avec les informations fournies par le platform de gestion de données Splunk, nous avons pu identifier et analyser les attaques. Et nous avons réussi à comprendre quand cela se produit et comment cela se produit.

Données à disposition

Toutes les informations détaillées récupérées depuis comme par exemple proxy web et courrier électronique sont enregistrées dans le log. Et nous pouvons lire et analyser les informations du log du réseau sur le platform Splunk.

Le platform Splunk prennent en entrée les événements collectés du SI, les journaux système des équipements : pare-feu, routeurs, serveurs, bases de données... Ils permettent de prendre en compte différents formats (syslog, Traps SNMP, fichiers plats, OPSEC, formats propriétaires, etc.) ou nativement le format IDMEF (Intrusion Détection Message Exchange Format), spécialement conçu et validé par l'IETF sous

forme de RFC pour partager l'information qui intéresse un système de détection et protection aux intrusions.



Cyber Threat Intelligence - Nicolas Pierson

- **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

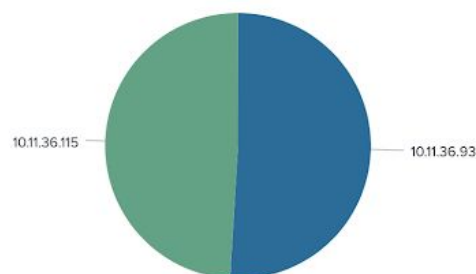
Le résumé de l'attaque et sa chronologie

Identification des IPs infectés

Une partie des attaquants suspects (par Indicateurs de compromissions (IOC)) ont été déjà identifiés. Tout d'abord, nous allons chercher les postes internes qui sont attaqués. Par une recherche de la liste des IOC fournies, nous pouvons voir que les deux postes internes attaqués sont **10.11.36.115** et **10.11.36.93**. Et la distribution des sources est montrée ci-dessous.

Requête :

```
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
```



Les Host des 2 sources sont montré ci-dessous.

splunk>enterprise App: Search & Reporting ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

dest = "10.11.36.93" OR dest = "10.11.36.115"

✓ 270 events (before 3/19/20 4:31:51.000 PM) No Event Sampling ▾

Events (270) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ ✎ Format 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- a action 1
- a date_wday 3
- a dest 2
- a Host 2
- a host 1
- a source 1
- a sourcetype 2

INTERESTING FIELDS

- # date_hour 24

Host

2 Values, 96.296% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
pdence-94DA3SF7.defense.fr	133	51.154%
ejodor-0TNY60F9.defense.fr	127	48.846%

Les deux Host devraient avoir fait les mêmes manipulations pour être attaqués. Maintenant on va chercher les manipulations suspectes en commun pour les deux Host.

Identification d'attaque

Les premières connexions au IOC par les 2 sources étaient à **1:14 PM le 3/18/2020**.

>	3/18/20 1:18:07.000 PM	1584533887 duration=573 dest=212.24.32.62 action=TCP_TUNNELED status=200 bytes_in=402 http_method=CONNECT url=tcp://212.24.32.62:443/ - src=10.11.36.115 category=none bytes_out=386 http_user_agent="87353/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.115
>	3/18/20 1:18:07.000 PM	1584533887 duration=611 dest=212.24.32.63 action=TCP_TUNNELED status=200 bytes_in=437 http_method=CONNECT url=tcp://212.24.32.63:443/ - src=10.11.36.93 category=none bytes_out=407 http_user_agent="36092/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.93
>	3/18/20 1:14:10.000 PM	1584533650 duration=558 dest=46.252.242.9 action=TCP_TUNNELED status=200 bytes_in=377 http_method=CONNECT url=tcp://46.252.242.9:443/ - src=10.11.36.115 category=none bytes_out=371 http_user_agent="34029/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.115
>	3/18/20 1:14:10.000 PM	1584533650 duration=656 dest=212.24.32.57 action=TCP_TUNNELED status=200 bytes_in=436 http_method=CONNECT url=tcp://212.24.32.57:443/ - src=10.11.36.93 category=none bytes_out=376 http_user_agent="78197/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" - - - - host = proxy-xx.buttercupgames.com source = eventgen sourcetype = bluecoat src = 10.11.36.93

Donc la manipulation suspecte devrait s'être effectuée avant cette heure. En cherchant le log précédemment, nous avons aperçu que le fichier **"stuxbar.exe"** est exécuté 10 seconds exactement après l'ouverture du fichier **"reconversion.pdf"** pour les postes **"10.11.36.93"** et **"10.11.36.115"**.

>	3/18/20 11:39:29.000 AM	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
>	3/18/20 11:39:29.000 AM	03/18/20 10:39:29 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" host = workstation-xx.buttercupgames.com source = eventgen sourcetype = winhostmon
>	3/18/20 11:39:19.000 AM	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
>	3/18/20 11:39:19.000 AM	03/18/20 10:39:19 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.pdf" host = workstation-xx.buttercupgames.com source = eventgen sourcetype = winhostmon

Comme l'attaque s'effectue via Outlook, nous sommes intéressés par tous les processus relatifs à Outlook pour les postes contaminés, afin de détecter les processus anormaux.

Nous pouvons voir qu'il y a en total 2 processus : "**PDFRd32.exe**" et "**stuxbar.exe**". Chaque fois "**stuxbar.exe**" s'est effectué 10 secondes après le "**PDFRd32.exe**". Nous en déduisons que le PDF a attaché potentiellement le fichier malveillant "**stuxbar.exe**".

Pour vérifier cette idée, nous allons chercher tous les Host qui ont ouvert le fichier "**reconversion.pdf**". L'ouverture de PDF est effectuée par un "**sourcetype**" qui est "**winhostmon**".

Requête :

```
sourcetype="winhostmon" reconversion.pdf
```

i	_time	host	source	sourcetype	process	Host
>	3/19/20 1:02:58.000 AM	workstation- xx.buttercupgames.com	eventgen	winhostmon	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion.pdf	ejodor- 0TNY60F9.defense.fr
>	3/19/20 1:02:58.000 AM	workstation- xx.buttercupgames.com	eventgen	winhostmon	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion.pdf	pdence- 94DA3SF7.defense.fr
>	3/18/20 10:09:16.000 PM	workstation- xx.buttercupgames.com	eventgen	winhostmon	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion.pdf	ejodor- 0TNY60F9.defense.fr
>	3/18/20 10:09:16.000 PM	workstation- xx.buttercupgames.com	eventgen	winhostmon	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion.pdf	pdence- 94DA3SF7.defense.fr
>	3/18/20 6:07:23.000 PM	workstation- xx.buttercupgames.com	eventgen	winhostmon	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion.pdf	ejodor- 0TNY60F9.defense.fr
>	3/18/20 6:07:23.000 PM	workstation- xx.buttercupgames.com	eventgen	winhostmon	c:\users\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\reconversion.pdf	pdence- 94DA3SF7.defense.fr

Nous pouvons également rechercher des machines sur lesquelles "**stuxbar.exe**" a été exécuté.

Requête :

```
process_name=stuxbar.exe | fields "_time" "src"
"process_name"| sort -"_time"
```

_time ▾	src ▾	process_name ▾
2020-03-19 01:03:08	10.11.36.115	stuxbar.exe
2020-03-19 01:03:08	10.11.36.93	stuxbar.exe
2020-03-18 22:09:26	10.11.36.115	stuxbar.exe
2020-03-18 22:09:26	10.11.36.93	stuxbar.exe
2020-03-18 18:07:33	10.11.36.115	stuxbar.exe
2020-03-18 18:07:33	10.11.36.93	stuxbar.exe
2020-03-18 17:04:36	10.11.36.115	stuxbar.exe
2020-03-18 17:04:36	10.11.36.93	stuxbar.exe
2020-03-18 14:08:28	10.11.36.115	stuxbar.exe
2020-03-18 14:08:28	10.11.36.93	stuxbar.exe
2020-03-18 13:01:58	10.11.36.115	stuxbar.exe
2020-03-18 13:01:58	10.11.36.93	stuxbar.exe
2020-03-18 12:34:04	10.11.36.115	stuxbar.exe
2020-03-18 12:34:04	10.11.36.93	stuxbar.exe
2020-03-18 11:43:00	10.11.36.115	stuxbar.exe
2020-03-18 11:43:00	10.11.36.93	stuxbar.exe
2020-03-18 11:39:29	10.11.36.115	stuxbar.exe
2020-03-18 11:39:29	10.11.36.93	stuxbar.exe
2020-03-18 11:34:48	10.11.36.115	stuxbar.exe
2020-03-18 11:11:24	10.11.36.115	stuxbar.exe

Donc on peut en déduire que l'attaque est dû à l'ouverture de PDF nommé **"reconversion.pdf"**.

Maintenant on veut savoir les personnes qui étaient visés au premier temps, et pourquoi les deux postes sont enfin contaminées et pas les autres. Nous allons rechercher les adresses email du destinataire avec les emails contenant **"reconversion.pdf"**.

Requête :

sourcetype="cisco:esa" AND file_name="reconversion.pdf"

New Search

sourcetype="cisco:esa" AND file_name="reconversion.pdf"

✓ 8 events (3/18/20 6:00:00.000 PM to 3/19/20 6:42:42.000 PM) No Event Sampling ▼

Events (8) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a orig_recipient 1
- a recipient 4
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # date_hour 2

orig_recipient

1 Value, 100% of events

Selected

Reports

- Top values
- Top values by time
- Rare values
- Events with this field

Values

	Count	%
liste@marinemobilite.com	8	100%

Table ▼ Format 20 Per Page ▼

i	_time	host	source	sourcetype	orig_recipient	recipient
>	3/19/20 1:02:18.000 AM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	emmanuel.coraidh@defense.fr
>	3/19/20 1:02:18.000 AM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	capucine.palaci@defense.fr
>	3/19/20 1:02:18.000 AM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	eloise.jodor@defense.fr
>	3/19/20 1:02:18.000 AM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	pierre.dence@defense.fr
>	3/18/20 10:08:36.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	emmanuel.coraidh@defense.fr
>	3/18/20 10:08:36.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	capucine.palaci@defense.fr
>	3/18/20 10:08:36.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	eloise.jodor@defense.fr
>	3/18/20 10:08:36.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	pierre.dence@defense.fr
>	3/18/20 6:06:43.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	emmanuel.coraidh@defense.fr
>	3/18/20 6:06:43.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	capucine.palaci@defense.fr
>	3/18/20 6:06:43.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	eloise.jodor@defense.fr
>	3/18/20 6:06:43.000 PM	sfo-resources-12.it.buttercupgames.com	eventgen	cisco:esa	liste@marinemobilite.com	pierre.dence@defense.fr

On peut trouver que les mails sont envoyés à une liste liste@marinemobilite.com, et reçu par 4 personnes :

- Emmanuel Coraigh (emmanuel.coraigh@defense.fr)
- Capucine Palaci (capucine.palaci@defense.fr)
- Eloise Jodor (eloise.jodor@defense.fr) (ip : 10.11.36.115)
- Pierre Dence (pierre.dence@defense.fr) (ip : 10.11.36.93)

Les 4 personnes ont reçu autant de fois le mail comme montré ci-dessous.

Requête :

```
file_name=reconversion.pdf | fields recipient | top recipient
```



Cependant, il y a que les postes de **Eloise Jodor** et **Pierre Dence** qui sont attaqués. Parce que tous les 4 personnes ont reçu le mail comme elles sont tous dans la liste liste@marinemobilite.com, mais les autres autres personnes n'ont pas ouvert le PDF.

Une annexe contenant les IOC confirmés et les nouveaux IOC identifiés

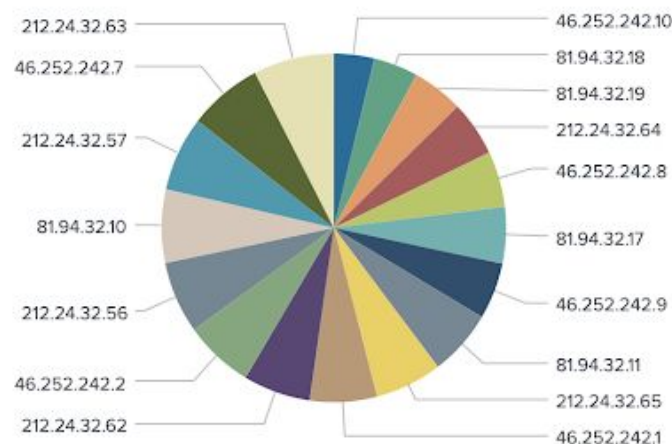
IOC confirmés

La menace est définie par une fuite des données. Donc nous sommes amenés à chercher les adresses IP à qui ont envoyé des données par les 2 sources. La liste est triée par l'ordre décroissance.

Nous avons trouvé que tous les adresses IP sont présentées dans la liste de menace de l'entreprise banacry (banet.csv), donc les IOC sont confirmés.


Requête :

```
Sourcetype =*[inputlookup banet.csv|rename ipaddress as  
dest|fields dest] src="10.11.36.93" OR src="10.11.36.115" |  
stats sum(bytes_out) by dest | sort sum(bytes_out)
```



IOC identifiés


La région des attaquants identifiée précédemment se situe à Russe :

IP Address	Country	Region	City
46.252.242.1	Russian Federation 	Sankt-Peterburg	Saint Petersburg
ISP	Organization	Latitude	Longitude
Lombardy	Not Available	59.8944	30.2642

Dans la liste de menace de l'entreprise banacry, nous pouvons voir que les adresses IP classés en haut et non identifiées sont commencées par 78.138.128 :

*	<i>a</i> ipaddress	<i>a</i> threat
1	46.252.242.1	banacry
2	46.252.242.2	banacry
3	46.252.242.3	banacry
4	46.252.242.4	banacry
5	46.252.242.5	banacry
6	46.252.242.6	banacry
7	46.252.242.7	banacry
8	46.252.242.8	banacry
9	46.252.242.9	banacry
10	46.252.242.10	banacry
11	78.138.128.10	banacry
12	78.138.128.11	banacry
13	78.138.128.12	banacry
14	78.138.128.13	banacry
15	78.138.128.14	banacry
16	78.138.128.15	banacry
17	78.138.128.16	banacry
18	78.138.128.17	banacry
19	78.138.128.18	banacry
20	78.138.128.19	banacry

En effet, les adresses IP commencées par 78.138.128 dans la liste de menace se trouve également à Russe, dans la même région des attaquants qui ont envoyé le PDF par Outlook.

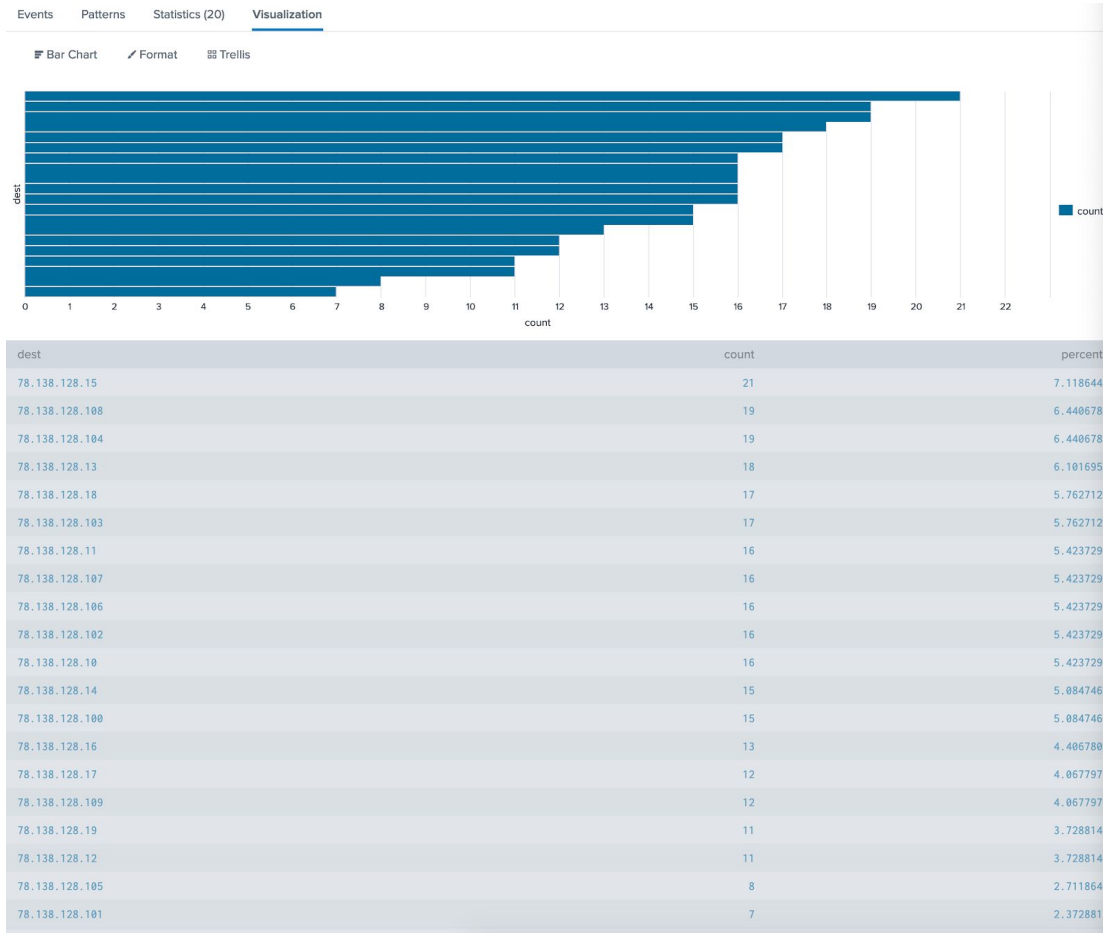
IP Address	Country	Region	City
78.138.128.10	Russian Federation 	Tatarstan, Respublika	Kazan
ISP	Organization	Latitude	Longitude
OJSC Oao Tattelecom	Not Available	55.7887	49.1221

IP Address	Country	Region	City
78.138.128.100	Russian Federation 	Tatarstan, Respublika	Kazan
ISP	Organization	Latitude	Longitude
OJSC Oao Tattelecom	Not Available	55.7887	49.1221

Donc nous sommes intéressés à voir la quantité des communications avec tous les adresses IP commencées par 78.138.128.

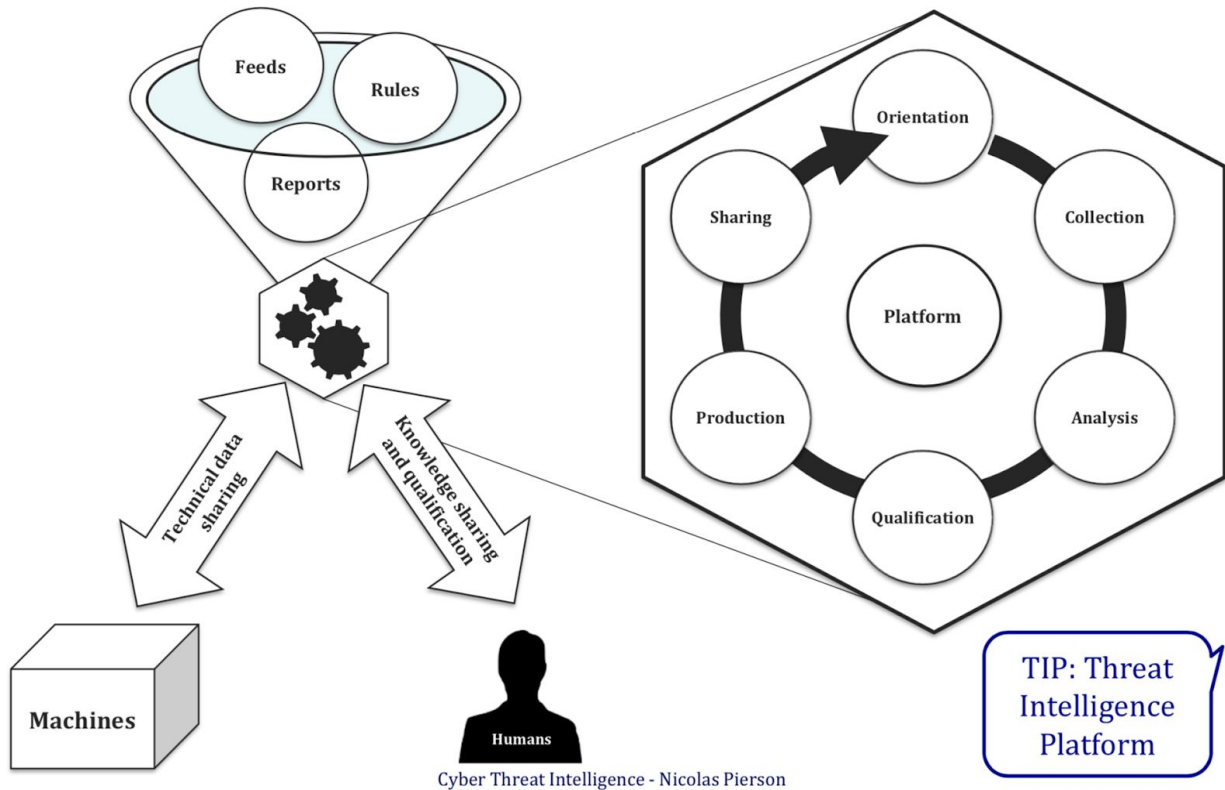
Requête :

78.138.128| top limit=50 dest



Effectivement, beaucoup d'adresses IP menaçantes de cette région communiquent avec banacry, ce qui n'est pas normal. Donc nous pouvons déduire que les adresses IP commencées par 78.138.128 appartiennent aussi dans IOC.

Conclusion



Nous pouvons identifier les menaces et les attaquants via le log d'entreprise. Tout le log est tracé et stocké dans la base de données. Dans notre cas, c'est dans le platform Splunk.

La bonne pratique est de suivre le log régulièrement, identifier les anomalies, et réaliser un plan de réaction. Dans notre exemple, après avoir identifié la mode d'attaque, les adresses IP potentiellement menaçant ont été également identifiés. Finalement, pour maintenir une meilleur système de cybersécurité, en combinant notre cas d'études, et notre cours, les 4 démarches sont sollicitées:

- **Prévention :**

Sensibiliser aux employés l'importance de cybersécurité, passer d'une bonne pratique du travail, comme par exemple: ne pas utiliser le PC du travail

pour faire les activités privées, ne pas ouvrir les documents avec un titre non concerné du travail ou avec un expéditeur inconnu.

- **Anticipation :**

Analyser des risques et des motivations des attaquants, mettre en place du pare-feu pour bloquer les IP suspect et les expéditeurs de mail inconnus.

- **Détection :**

Établir un centre des opérations de sécurité pour détecter les menaces et des fuites de données en temps réel.

- **Réaction :**

Faire l'entraînement opérationnel et construire les plans d'urgence en cas d'incidents sous la crise.

