Bilel Rahmouni

Analyse de Malware

Afin de comprendre le comportement d'un malware, nous vous fournissons la capture Wireshark capture-mal.pcap. Cette capture provient d'une vraie analyse après une attaque d'une entreprise.
Attention : Etant donné que ce malware infecte uniquement les plateformes Windows, il est fortement conseillé de réaliser cette partie sous Linux ou MacOS.

Mise en place :

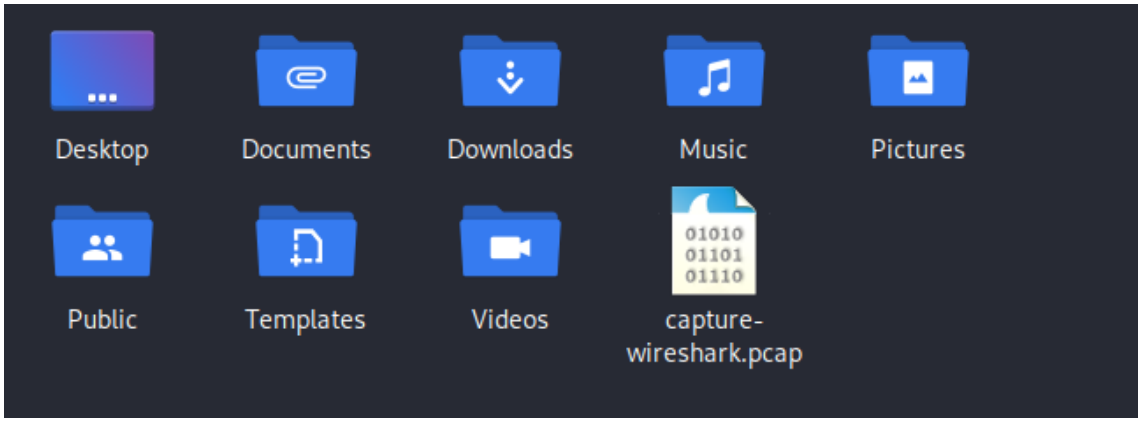
1. Assurez-vous d'avoir une machine virtuelle Kali Linux configurée avec soin. Dans les paramètres de la VM, veillez à définir le premier réseau en mode NAT et le deuxième en mode réseau interne (host-only).
2. Transférez le fichier capture-mal.pcap depuis un système Windows vers la machine virtuelle Kali Linux.
    a. Activer SSH sur la VM Kali Linux :

b. On regarde quelle est l'adresse ip de la machine Kali Linux et on ouvre le terminal windows ensuite à l'aide de la commande scp on copie le fichier dans la machine virtuelle.

```
┌──(rahmonex㉿rahmonex)-[~]
└─$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             UP
eth1             UP             192.168.56.103/24 fe80::a00:27ff:fe00:e449/64
```

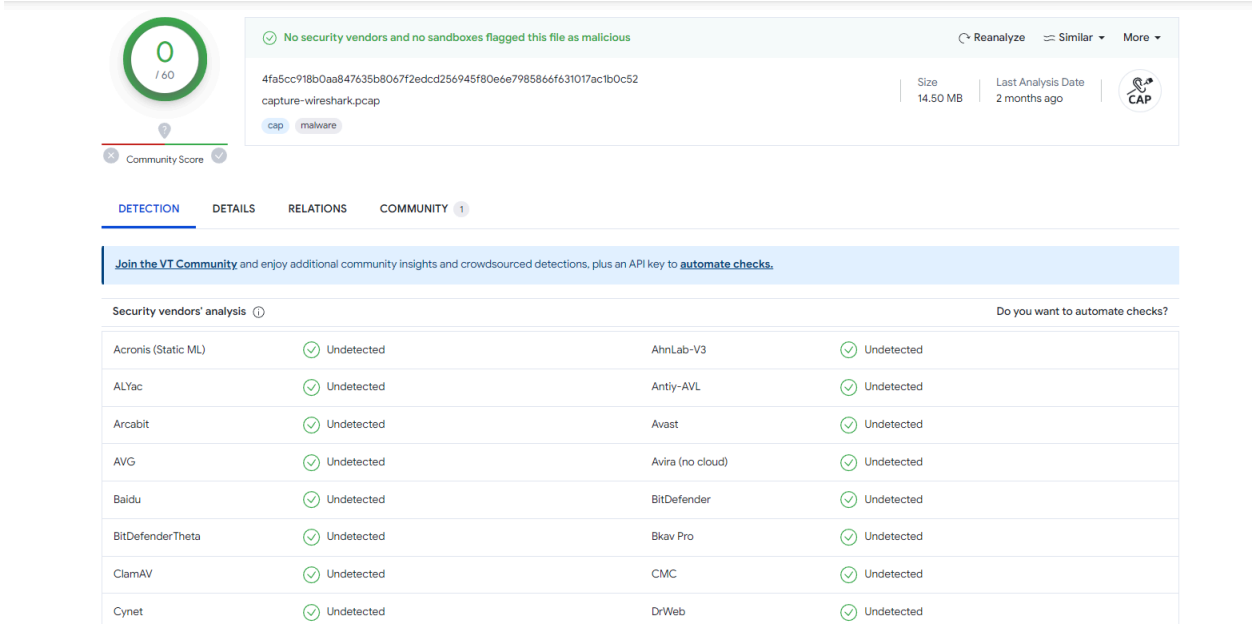
```
Command Prompt
Microsoft Windows [Version 10.0.22631.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rahmo>cd "C:\Users\rahmo\Downloads"

C:\Users\rahmo\Downloads>scp capture-wireshark.pcap rahmonex@192.168.56.103:.
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be established.
ED25519 key fingerprint is SHA256:cngNNZf4S2jEg01WyTKakpc+r/Juh/pOGKOqmxuSzXA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '192.168.56.103' (ED25519) to the list of known hosts.
rahmonex@192.168.56.103's password:
capture-wireshark.pcap                                    100%   15MB  31.5MB/s   00:00

C:\Users\rahmo\Downloads>
```

Ensuite, on s'assure que le fichier se trouve dans le répertoire principal de la machine virtuelle pour confirmer la réussite du transfert.



Une fois que la mise en place est effectuée, on peut commencer l'analyse du malware.

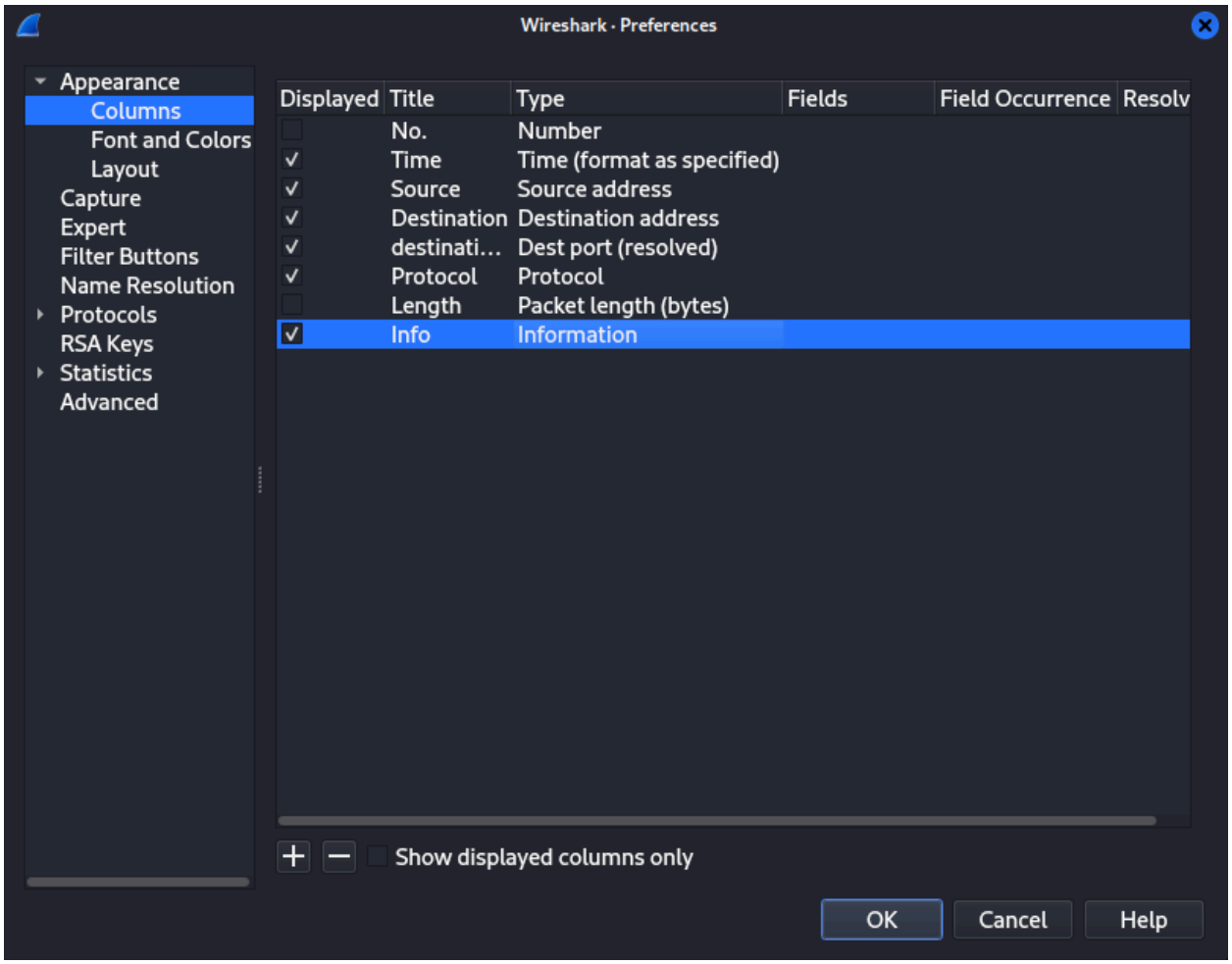
1. **Faites analyser le fichier de capture par le site VirusTotal. Quel est le résultat ?**



La capture Wireshark capture-wireshark.pcap semble ne pas être identifiée comme malveillante par les services de sécurité de VirusTotal, avec un score de 0/60. Cela signifie que, jusqu'à la date de l'analyse, aucun fournisseur de sécurité ni aucune sandbox n'a signalé de menace dans ce fichier.

2. **Afin de faciliter l'analyse de la capture, faire un filtre sur Wireshark afin de ne garder que les colonnes Time, Destination Address, Destination Port, Host et Info.**

Nous lançons Wireshark, ouvrons le fichier .pcap, puis pour configurer les colonnes, nous naviguons vers Edit > Preferences > Columns, où nous spécifions les colonnes requises.



On obtient cela :

Time	Source	Destination	destination port	Protocol	Host	Info
842.180837	170.238.117.187	10.9.25.101	49191	HTTP		HTTP/1.1
843.616384	10.9.25.101	170.238.117.187	8082	HTTP	170.238.117.187	POST /on
844.639136	170.238.117.187	10.9.25.101	49192	HTTP		HTTP/1.1
847.097696	10.9.25.101	170.238.117.187	8082	HTTP	170.238.117.187	POST /on
848.771327	170.238.117.187	10.9.25.101	49193	HTTP		HTTP/1.1
897.895194	10.9.25.101	170.238.117.187	8082	HTTP	170.238.117.187:8082	POST /on
898.924189	170.238.117.187	10.9.25.101	49196	HTTP		HTTP/1.1
899.325999	10.9.25.101	185.98.87.185	80	HTTP	185.98.87.185	GET /tab
901.514974	185.98.87.185	10.9.25.101	49197	HTTP		HTTP/1.1
906.338956	10.9.25.101	185.98.87.185	80	HTTP	185.98.87.185	GET /sam
908.430454	185.98.87.185	10.9.25.101	49197	HTTP		HTTP/1.1
953.509063	10.9.25.101	170.238.117.187	8082	HTTP	170.238.117.187:8082	POST /on
954.351610	170.238.117.187	10.9.25.101	49464	HTTP		HTTP/1.1

3. **Quelle est l'adresse IP de l'hôte infecté ?**

L'observation dans Wireshark des requêtes HTTP révèle que l'adresse IP 10.9.25.101 est la plus fréquemment impliquée. De plus, les différentes interactions semblent toutes émaner de cette adresse IP. Ces constatations laissent supposer que l'adresse IP de l'hôte cible est probablement 10.9.25.101.

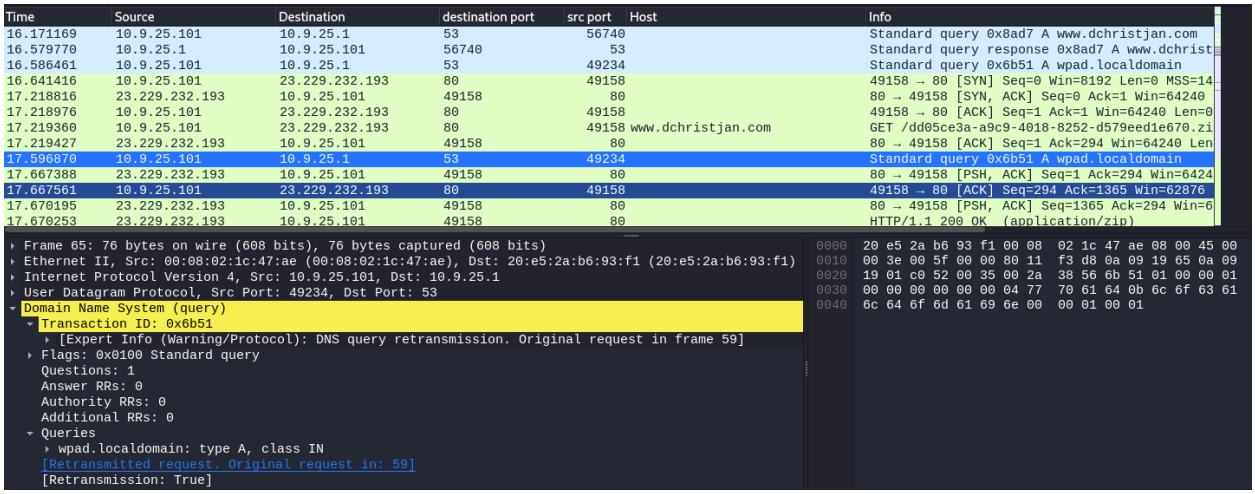
4. **Sur quels ports est échangé le trafic HTTPS et HTTP ?**

En analysant la capture Wireshark, on peut déterminer les ports sur lesquels le trafic HTTPS et HTTP est échangé. Pour le trafic HTTPS, le port par défaut est 443, tandis que pour le trafic HTTP, le port par défaut est 80. Ces informations peuvent être confirmées en examinant les colonnes "Destination Port" ou "Source Port" dans la capture pour identifier les numéros de port associés aux requêtes HTTP et HTTPS.

5. **Quel est le nom de domaine DNS contacté par malware ? Que trouve-t-on dans le fichier téléchargé à partir de ce site ?**

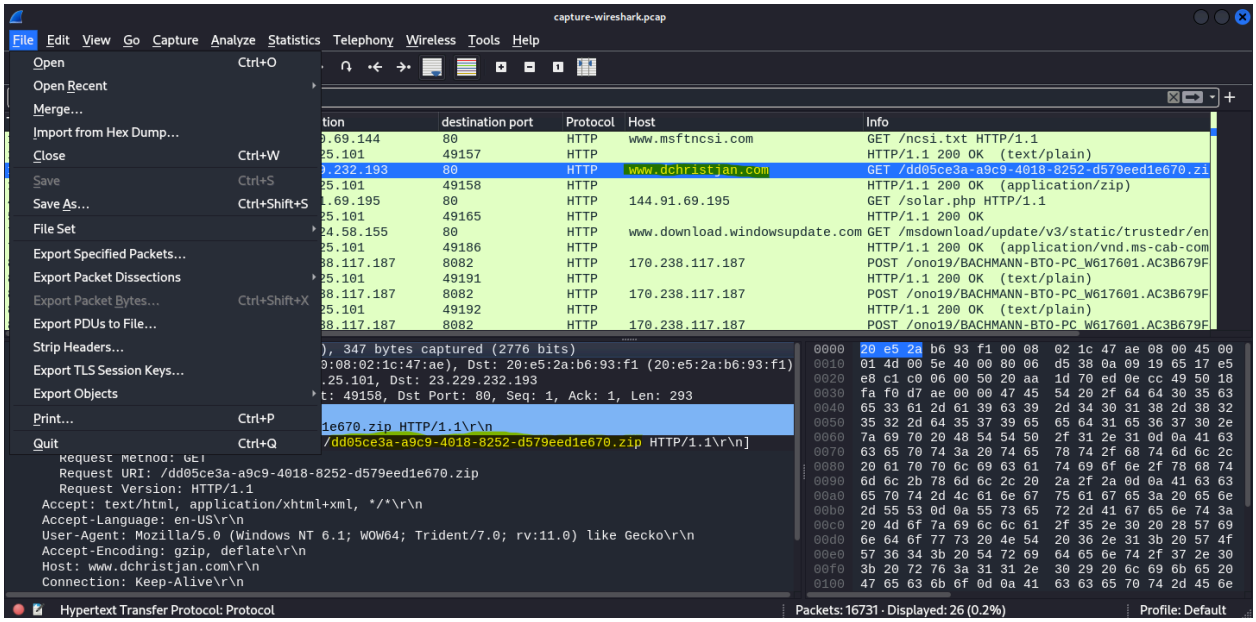
Je vérifie la capture du pare-feu, et en règle générale, les pare-feu laissent passer le trafic DNS ainsi que le trafic HTTP ou HTTPS. Ma première démarche consiste à voir si l'attaquant a opté pour le protocole HTTP, étant donné que c'est le protocole le plus fréquemment autorisé à travers le pare-feu.

Nous examinons la colonne "Host" et constatons la présence d'adresses URL ainsi que d'adresses IP brutes. De plus, nous repérons une requête HTTP incluant un téléchargement de fichier au format zip. On remarque après que le DNS qui suit la requête contenant le téléchargement du fichier Zip est wpad.localdomain de type A comme suit.

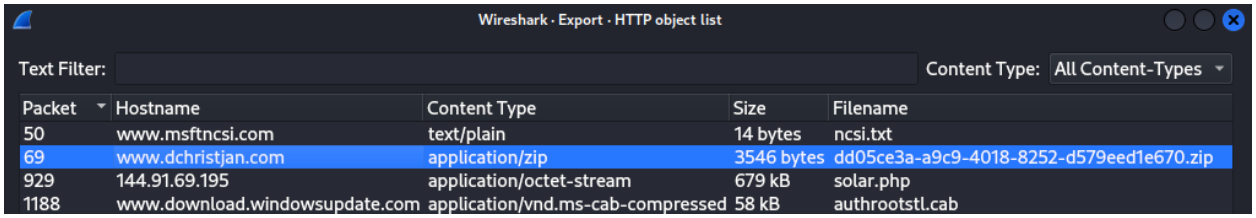


6. **Trouver l'exécutable envoyé à la victime. Comment confirmer que c'est bien un fichier en .exe ?**

Afin de récupérer ce fichier zip, nous naviguons vers "File", puis "Export Objects", et enfin "HTTP".



Et on choisit le fichier a save :



Après l'avoir téléchargé, nous vérifions qu'il s'agit bien d'un fichier zip, car parfois l'extension peut ne pas refléter le vrai format du fichier. Pour cela, nous utilisons la commande file.

```
┌──(rahmonex㉿rahmonex)-[~/Malware]
└─$ file dd05ce3a-a9c9-4018-8252-d579eed1e670.zip
dd05ce3a-a9c9-4018-8252-d579eed1e670.zip: Zip archive data, at least v2.0 to extract
, compression method=deflate
```

On remarque que c'est donc bien un fichier .zip

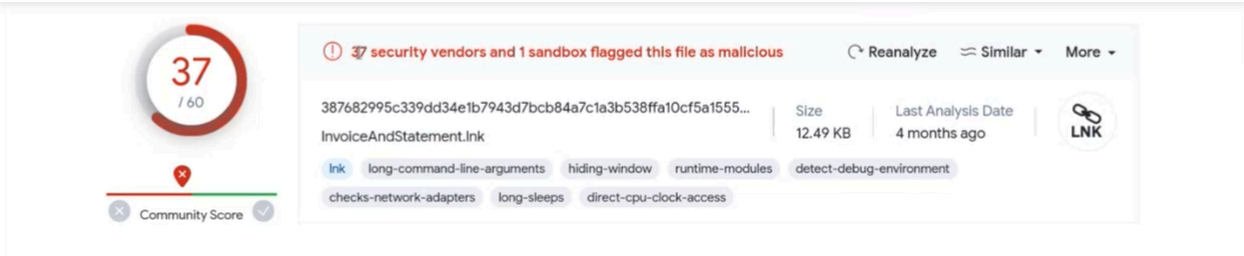
Maintenant que nous sommes certains qu'il s'agit d'un fichier zip, nous procédons à son extraction et on obtient le fichier "InvoiceAndStatement.lnk" qui peut nous faire penser à du phishing.

On va donc vérifier encore avec la commande file que signifie l'extension .lnk .

```
┌──(rahmonex㉿rahmonex)-[~/Malware]
└─$ file InvoiceAndStatement.lnk
InvoiceAndStatement.lnk: MS Windows shortcut, Item id list present, Points to a fil
e or directory, Has Description string, Has Relative path, Has command line argumen
ts, Icon number=1, Unicoded, HasEnvironment "%comspec%", MachineID win-jbf0q9el659
KnownFolderID 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7, Archive, ctime=Sat Nov 22 00:44
:59 2014, atime=Sat Nov 22 00:44:59 2014, mtime=Sat Nov 22 00:45:00 2014, length=35
7376, window=showminnoactive, IDListSize 0×0135, Root folder "20D04FE0-3AEA-1069-A2
D8-08002B30309D", Volume "C:\", LocalBasePath "C:\Windows\System32\cmd.exe"
```

Nous constatons que le fichier est un raccourci Windows qui ouvre directement l'exécutable C:\Windows\System32\cmd.exe, et il s'agit donc bien d'un fichier executable.

Ensuite, nous téléchargeons le fichier .lnk sur le site VirusTotal, qui nous fournit une analyse approfondie du fichier pour déterminer s'il est malveillant.



On remarque que c'est considéré comme un dropper, un type de logiciel malveillant qui sert à introduire et exécuter d'autres programmes malveillants sur un système. Il constitue souvent la première étape d'une attaque, déposant des charges utiles malveillantes sur la cible.

Continuons l'analyse des requêtes HTTP : On observe un téléchargement du fichier solar.php à partir d'une adresse IP brute, plutôt qu'une URL. Cette situation suscite des inquiétudes quant à la sécurité, car les téléchargements de fichiers depuis des adresses IP brutes peuvent être associés à des sources potentiellement malveillantes.

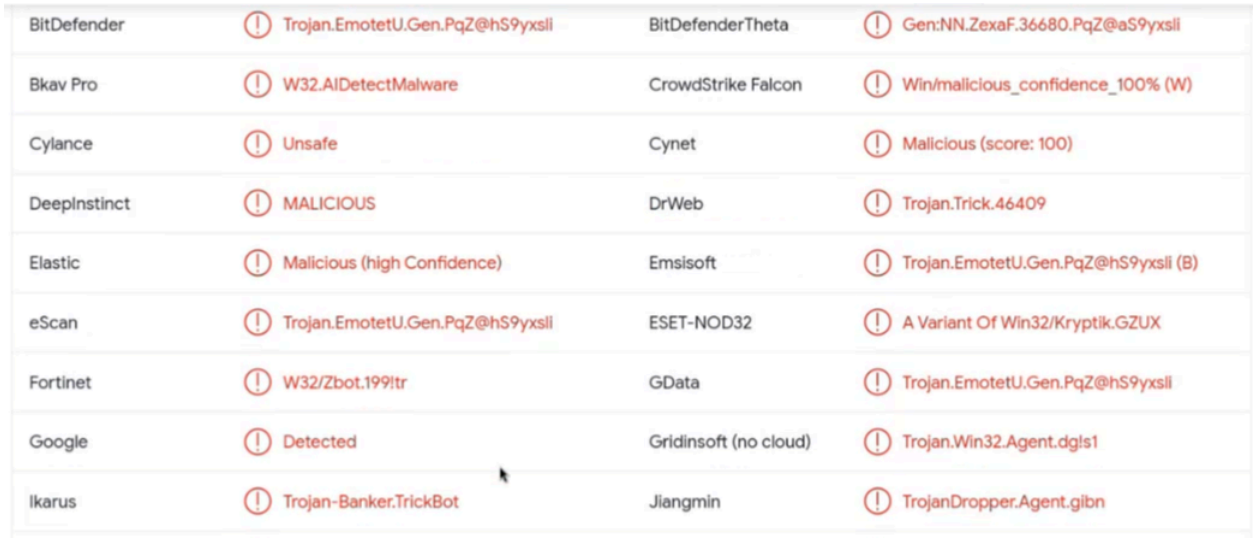
Time	Source	Destination	destination port	Protocol	Host	Info
14.529098	10.9.25.101	198.70.69.144	80	HTTP	www.msftncsi.com	GET /ncsi.txt HTTP/1.1
14.899128	198.70.69.144	10.9.25.101	49157	HTTP		HTTP/1.1 200 OK (text/plain)
17.219360	10.9.25.101	23.229.232.193	80	HTTP	www.dchristjan.com	GET /dd05ce3a-a9c9-4018-8252-d579eed1e670.zi
17.670253	23.229.232.193	10.9.25.101	49158	HTTP		HTTP/1.1 200 OK (application/zip)
47.209966	10.9.25.101	144.91.69.195	80	HTTP	144.91.69.195	GET /solar.php HTTP/1.1
51.981528	144.91.69.195	10.9.25.101	49165	HTTP		HTTP/1.1 200 OK
750.227369	10.9.25.101	104.124.58.155	80	HTTP	www.download.windowsupdate.com	GET /msdownload/update/v3/static/trustedr/en

De la même manière, nous procédons à l'exécution du fichier, puis nous vérifions sa nature effective avec la commande file pour confirmer qu'il s'agit bien d'un fichier au format .php, comme indiqué.

```
┌──(rahmonex㉿rahmonex)-[~/Malware]
└─$ file solar.php
solar.php: PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections
```

Contrairement à l'indication initiale, le fichier ne correspond pas à un script PHP, mais plutôt à un exécutable Windows. Cette divergence souligne une potentialité de manipulation ou d'obfuscation dans le but de masquer la véritable nature du fichier.

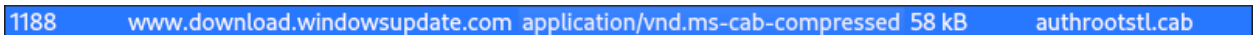
Par la suite, nous soumettons le fichier à VirusTotal pour analyse.



BitDefender	Trojan.EmotetU.Gen.PqZ@hS9yxsli	BitDefenderTheta	Gen:NN.ZexaF.36680.PqZ@aS9yxsli
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Trick.46409
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.EmotetU.Gen.PqZ@hS9yxsli (B)
eScan	Trojan.EmotetU.Gen.PqZ@hS9yxsli	ESET-NOD32	A Variant Of Win32/Kryptik.GZUX
Fortinet	W32/Zbot.199!tr	GData	Trojan.EmotetU.Gen.PqZ@hS9yxsli
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.dg!s1
Ikarus	Trojan-Banker.TrickBot	Jiangmin	TrojanDropper.Agent.gibn

Et les résultats indiquent sa malveillance, avec la détection d'Emotet et TrickBot. Emotet est un malware multifonction utilisé pour la distribution d'autres menaces, tandis que TrickBot est un cheval de Troie bancaire visant à voler des informations sensibles.

On remarque de même que l'on a un fichier de type vnd.ms-cab-compressed nommé authrootstl.cab qui a été téléchargé.



Le type de fichier vnd.ms-cab-compressed fait référence à un fichier compressé au format Cabinet (CAB). Les fichiers CAB sont des archives de compression de Microsoft utilisées pour regrouper plusieurs fichiers en un seul, tout en appliquant une compression pour économiser de l'espace de stockage.

Le type MIME vnd.ms-cab-compressed est associé aux fichiers CAB dans le contexte des types de médias Internet. Lorsque vous rencontrez ce type MIME, cela signifie généralement que le fichier est une archive CAB compressée. Ces archives sont couramment utilisées pour l'installation de logiciels sous Windows et pour la distribution de mises à jour de logiciels.

L'extension de fichier habituellement associée à ce type de fichier est .cab. Les fichiers CAB peuvent être extraits à l'aide d'utilitaires appropriés pour révéler les fichiers individuels contenus dans l'archive.

7. **Identifier les différentes tentatives de connexions après l'infection. Expliquer.**

En examinant la capture Wireshark après l'infection, j'ai observé une séquence de requêtes POST successives. Ces requêtes POST suggèrent l'envoi de données au serveur web.

841.164404	10.9.25.101	170.238.117.187	8082	49191 170.238.117.187	POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F
842.180837	170.238.117.187	10.9.25.101	49191	8082	HTTP/1.1 200 OK (text/plain)
843.616384	10.9.25.101	170.238.117.187	8082	49192 170.238.117.187	POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F
844.639136	170.238.117.187	10.9.25.101	49192	8082	HTTP/1.1 200 OK (text/plain)
847.097696	10.9.25.101	170.238.117.187	8082	49193 170.238.117.187	POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F
848.771327	170.238.117.187	10.9.25.101	49193	8082	HTTP/1.1 200 OK (text/plain)
897.895194	10.9.25.101	170.238.117.187	8082	49196 170.238.117.187:8082	POST /ono19/BACHMANN-BTO-PC_W617601.AC3B679F

Entre ces requêtes, j'ai identifié des résultats TXT qui semblaient contenir des informations liées aux tentatives de connexions. En procédant ainsi, j'ai pu identifier différentes tentatives de connexions après l'infection, en analysant les données transmises entre le client infecté et le serveur web.

8. **Le malware identifie l'adresse IP de la victime en contactant un site public. Lequel ? Pourquoi cette vérification ?**

Exercice 2 :

1. **A quelle date le malware Trickbot est-il apparu ? De quel type il est ? Quel est son domaine d'action ?**

Trickbot est apparu pour la première fois en 2016 en tant que cheval de Troie bancaire, mais il a évolué pour devenir un malware multifonction. Initialement conçu pour voler des informations bancaires, il s'est étendu pour inclure des fonctionnalités telles que la distribution de ransomwares et la création de botnets. Son domaine d'action couvre une variété d'activités malveillantes, allant de l'espionnage financier à la propagation de menaces plus larges.

2. **Quels sont les dégâts possibles qui peuvent être causés par ce malware ?**

Les dégâts potentiels causés par Trickbot sont vastes. Il peut permettre l'accès non autorisé à des informations sensibles, le vol d'identifiants bancaires, le déploiement de ransomwares et la participation à des attaques par déni de service distribué (DDoS). En compromettant la sécurité d'un système, Trickbot ouvre la porte à diverses activités malveillantes aux conséquences graves.

3. **Quelle est la méthode de diffusion la plus courante de ce Malware ?**

Trickbot se propage souvent via des campagnes de phishing, où les utilisateurs reçoivent des e-mails trompeurs avec des pièces jointes malveillantes. Ces pièces jointes peuvent contenir des documents infectés par des macros malveillantes ou des liens vers des sites web compromis. Lorsque les utilisateurs ouvrent ces pièces jointes ou cliquent sur les liens, Trickbot s'infiltre dans le système.

4. **Quelles sont les techniques utilisées pour inciter l'utilisateur à ouvrir le document infecté ?**

Les cybercriminels utilisent diverses tactiques pour inciter les utilisateurs à ouvrir des documents infectés par Trickbot. Cela peut inclure des techniques de leurres, des informations fausses ou urgentes, des prétendues factures, ou des communications prétendument officielles. L'objectif est d'induire les utilisateurs en erreur pour qu'ils ouvrent les pièces jointes malveillantes.

5. **Est-ce que ce malware peut faire des dégâts si l'utilisateur infecté n'est pas admin ?**

Trickbot peut causer des dégâts même si l'utilisateur infecté n'est pas administrateur. Bien que les privilèges administratifs facilitent la propagation et l'impact, Trickbot peut encore compromettre la confidentialité des données, voler des informations sensibles, et participer à des activités malveillantes même avec des droits d'utilisateur standard. La menace persiste, bien que l'étendue des dégâts puisse varier en fonction des privilèges d'accès de l'utilisateur infecté.