

Rapport d'analyse d'un virus

Morgan Salhi



Autorisation :

Cette analyse a été réalisé avec l'accord de Monsieur Thomas PROVOST à l'IUT de Sophia Antipolis en R&T qui nous a autorisé à faire des observations sur l'impact d'un virus sur un ordinateur virtuel dans le but d'un travail dirigé.

Objectif :

Le but de ce pentest est de trouver le plus d'informations possible sur un virus téléchargé dans un ordinateur virtuel.

Début de l'analyse :

Etape 1 - Observation du virus en tant que root:

Nous commençons par aller sur le site suivant afin de pouvoir analyser les dégâts :

<https://app.any.run/tasks/6dcf570e-df95-4cf2-ab23-71bcfbab069e>

Exécution :

Le fichier que nous avons téléchargé et qu'il faut exécuter afin de déclencher le virus à un nom semblant être au hasard et son extension est '.o'. Les fichiers ayant cette extension sont des fichiers a compilé et à exécuté.



Valeurs anormales :

Lorsque la commande pour lancer 'htop' est effectuée, nous nous rendons vite compte que de nombreuses données sont anormales.

Premièrement, nous pouvons observer un usage très important du CPU qui se trouve dans les environs des 360% ainsi que les 4 en dessous de celui qui ne se trouve pas sous la barre des 80% d'utilisation.

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
13017	user	20	0	2388M	2345M	0	S	353.	60.0	12:15.25	/usr/lib/systemd/systemd
13050	user	20	0	2388M	2345M	0	R	96.3	60.0	3:03.66	/usr/lib/systemd/systemd
13048	user	20	0	2388M	2345M	0	R	93.3	60.0	2:47.61	/usr/lib/systemd/systemd
13047	user	20	0	2388M	2345M	0	R	83.4	60.0	2:42.97	/usr/lib/systemd/systemd
13049	user	20	0	2388M	2345M	0	R	82.8	60.0	2:49.65	/usr/lib/systemd/systemd

Cela peut également se remarquer par le fait que les 4 cœurs du CPU sont à 100% et la mémoire (RAM) qui est à un usage important.



Détection du type de virus :

Lorsque nous analysons le [Text Report](#), nous pouvons voir en haut de page que c'est bien et bien un danger et qu'il s'agit d'un crypto malware.

General Info

☒ Add for printing

File name: .redtail

Full analysis: <https://app.any.run/tasks/6dcf570e-df95-4cf2-ab23-71bcfbab069e>

Verdict: **Malicious activity**

Threats: **Crypto malware**

Crypto mining malware is a resource-intensive threat that infiltrates computers with the purpose of mining cryptocurrencies. This type of threat can be deployed either on an infected machine or a compromised website. In both cases the miner will utilize the computing power of the device and its network bandwidth.

Analyse du réseau liée à ce virus :

Lorsque nous allons dans l'onglet 'Connections', et que nous nous dirigeons vers les connexions avec un PID de 13017, nous pouvons y observer de nombreuses adresses IP lié à différents pays.

40180 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	95.215.19.53	853	-	ab stract	↑ 378 b ↓ 4 Kb
40187 ms	TCP	🔥	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	1.1.1.1	853	-	CLOUDFLARENET	↑ 362 b ↓ 4 Kb
41182 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	217.160.70.42	853	-	IONOS SE	↑ 296 b ↓ 4 Kb
41186 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	1.0.0.1	853	-	CLOUDFLARENET	↑ 296 b ↓ 3 Kb
41189 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	178.254.22.166	853	-	EVANZO e-commerce GmbH	No Data
45286 ms	TCP	🟢	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	8.8.8.8	853	-	GOOGLE	↑ 296 b ↓ 5 Kb
45289 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	81.169.136.222	853	-	Strato AG	↑ 296 b ↓ 4 Kb
45292 ms	TCP	🟢	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	8.8.4.4	853	-	GOOGLE	↑ 296 b ↓ 5 Kb
45294 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	185.181.61.24	853	-	TerraHost AS	↑ 296 b ↓ 4 Kb
45297 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	194.59.30.110	43782	proxies.internetshadow.org	COGENT-174	↑ 464 b ↓ 49 Kb
46292 ms	TCP	?	13017	6dcf570e-df95-4cf2-ab23-71bcfbab069e.o	93.123.39.174	2137	proxies.internetshadow.org	Vivacom	↑ 349 b ↓ 4 Kb

Cependant, elles sont tout de même toutes reliées au même PID et lorsque nous cliquons sur l'une d'elles, les informations suivantes apparaissent :

Threat Verdict

100

OUT OF 100

Malicious

The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions

Indicators:

Process information

Username: user

SID: UNKNOWN

Start: 43.96 s

File information

Command line

./6dcf570e-df95-4cf2-ab23-71bcfbab069e.o

Timeline of the process

0 s 43.96 s 309.92 s

43.96 s

MINER has been detected (SURICATA)

T1071 Application Layer Protocol (1)

Connects to the CnC server

Warning 4

Potential Corporate Privacy Violation

Crypto Currency Mining Activity Detected

T1571 Non-Standard Port (1)

Connects to unusual port

T1059.004 Unix Shell (1)

Executes commands using command-line interpreter

On peut voir ici à quel point ce malware est dangereux et qu'il s'est rapidement incrusté dans le système.

Ensuite, si nous allons dans l'onglet 'Threats', nous y voyons les différentes menaces qui ont été détectés ainsi que leur niveau de menace ainsi que l'activité qui a été perçue.

45232 ms	Misc Attack	13017	6dcf570e-df95-4cf2-ab2...	ET COMPROMISED Known Compromised or Hostile Host Traffic group 7
45235 ms	Misc Attack	13017	6dcf570e-df95-4cf2-ab2...	ET DROP Spamhaus DROP Listed Traffic Inbound group 38
45238 ms	Misc Attack	13017	6dcf570e-df95-4cf2-ab2...	ET 3DORESec Poor Reputation IP group 6
45244 ms	Crypto Currency Mining Activity Detected	13017	6dcf570e-df95-4cf2-ab2...	MINER [ANY.RUN] CoinMiner Agent CnC Initial Connection
47769 ms	Potential Corporate Privacy Violation	13017	6dcf570e-df95-4cf2-ab2...	ET POLICY Cryptocurrency Miner Checkin
47770 ms	Misc Attack	13017	6dcf570e-df95-4cf2-ab2...	ET DROP Spamhaus DROP Listed Traffic Inbound group 14
47771 ms	Misc Attack	13017	6dcf570e-df95-4cf2-ab2...	ET 3DORESec Poor Reputation IP group 12
102.55 s	Potential Corporate Privacy Violation	13017	6dcf570e-df95-4cf2-ab2...	ET POLICY Cryptocurrency Miner Checkin
209.56 s	Not Suspicious Traffic	13147	http	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management

En cliquant sur la première, nous pouvons voir une adresse IP, celle-ci correspond à l'adresse de la Bulgarie que nous avons trouvés dans la liste plus haut. On peut également observer plus profondément via WireShark.

Threat details

Here are the details of the threat

Main
Stream data
Suricata rule
new

The data provided by [Suricata IDS](#)

Misc Attack

ET COMPROMISED Known Compromised or Hostile Host Traffic group 7

Src / Dst	194.59.30.110 : 43782 → 192.168.100.44 : 57452
Timeshift	45232 ms
SID	2500012; rev: 6939;
Transport	TCP
Src IP	194.59.30.110
Dst IP	192.168.100.44
Src Port	43782
Dst Port	57452
To DstIP Packet	1
To SrcIP Packet	1
Total Bytes	148

Pour WireShark, nous allons en observer une intéressante, la 5ème. A la fin de celle-ci, nous pouvons observer deux trames suspectes :

12289	293	656977	93.123.39.174	192.168.100.44	TCP	428	[TCP Spurious Retransmission] 2137 → 58248 [PSH, ACK] Seq=4887 Ack=359 Win=64384 Len=354 TSval=49287400 TSecr=2788327130
12290	293	656923	192.168.100.44	93.123.39.174	TCP	78	[TCP Dup ACK 12289] 58248 → 2137 [ACK] Seq=359 Ack=4361 Win=64128 Len=0 TSval=2788330838 TSecr=49287400 RLE=4887 SRE=4361

Etape 2 - Observation du virus en tant qu'utilisateur :

Nous commençons par aller sur le site suivant afin de pouvoir analyser les dégâts :

<https://app.any.run/tasks/6dcf570e-df95-4cf2-ab23-71bcfbab069e>

Exécution :

Le fichier que nous avons téléchargé et qu'il faut exécuter afin de déclencher le virus à un nom semblant être au hasard et son extension est '.o'. Les fichiers ayant cette extension sont des fichiers a compilé et à exécuté.



Nous devons donc exécuter le fichier dans le terminal :

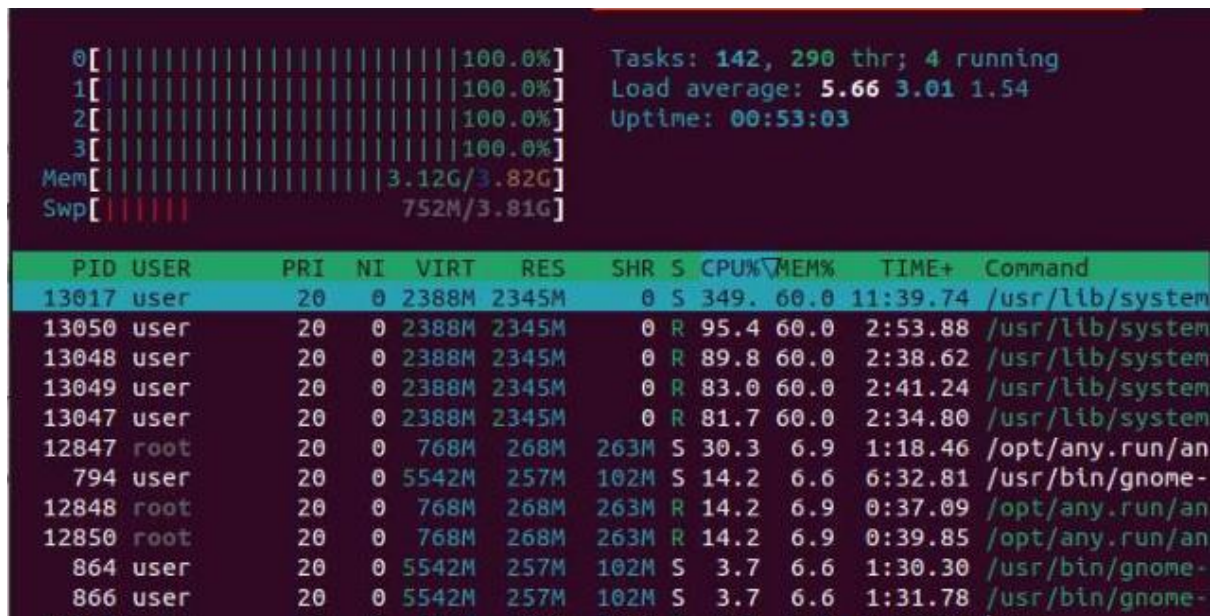
```

user@ubuntu22:~$ cd Desktop/
user@ubuntu22:~/Desktop$ ls -a
.  ..  6dcf570e-df95-4cf2-ab23-71bcfbab069e.o
user@ubuntu22:~/Desktop$ file 6dcf570e-df95-4cf2-ab23-71bcfbab069e.o
6dcf570e-df95-4cf2-ab23-71bcfbab069e.o: ELF 64-bit LSB pie executable, x86-64, v
ersion 1 (SYSV), statically linked, no section header
user@ubuntu22:~/Desktop$ ./6dcf570e-df95-4cf2-ab23-71bcfbab069e.o
user@ubuntu22:~/Desktop$ htop
Command 'htop' not found, but can be installed with:
sudo snap install htop # version 3.3.0, or
sudo apt install htop # version 3.0.5-7build2
See 'snap info htop' for additional versions.
user@ubuntu22:~/Desktop$

```

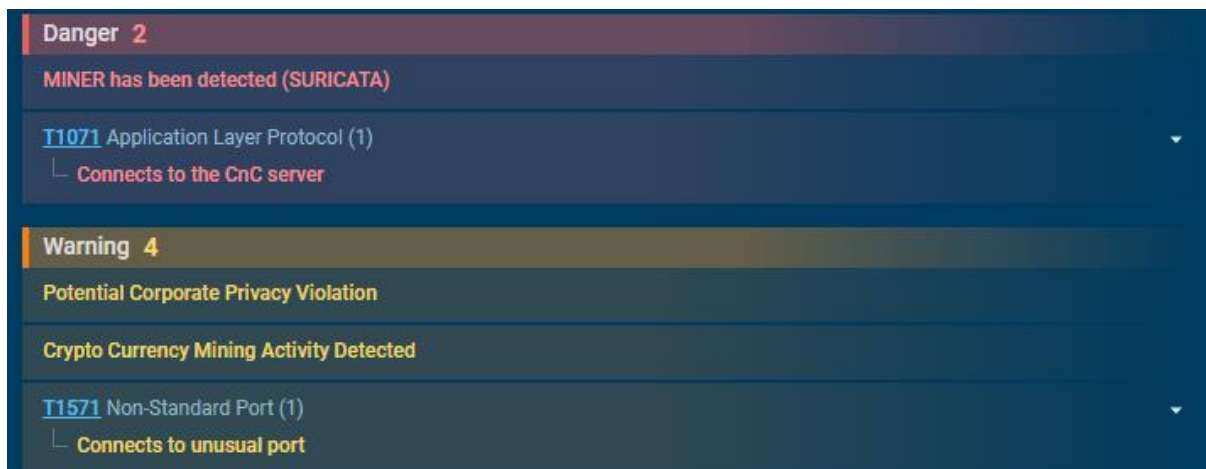
Valeurs anormales :

Comme pour le fichier que nous avons exécuté lorsque nous étions en root, nous remarquons instantanément des valeurs disproportionnées et incohérente qui sont beaucoup trop élevée, on en conclut donc pour l'instant qu'au niveau du matériel, les dégâts sont les mêmes que l'on soit en root ou en user.



Détection du type de virus :

Comme nous pouvons le voir ci-dessous, encore une fois on confirme bel et bien qu'il s'agit d'un virus servant à miner du Bitcoin sur notre ordinateur pour leurs fins personnelles



Conseils afin d'éviter d'avoir des virus sur nos ordinateurs :

Afin d'éviter d'avoir tout type de virus sur nos ordinateurs, je recommande premièrement de mettre à jour les composants ainsi que l'OS et les logiciels de l'ordinateur. Ensuite, je recommande l'acquisition d'un anti-virus, tous les fichiers que vous téléchargerez seront scannés ainsi que votre pc dans son intégralité, cela évite et prévient des dangers.

Pour finir, faites attention aux sites sur lesquels vous allez, vérifiez bien que le site en question soit en https et non en http, ne téléchargez pas de fichier qui peuvent paraître suspects ou encore sur des sites non officiels ou version non officielle.

Tous ces conseils devraient énormément baisser le risque de virus sur votre pc et vous pourrez surfer en paix.

Conclusion :

On en conclut donc que lorsqu'un virus est initialisé sur notre ordinateur, un retour en arrière est difficile en vue de ce qu'ils peuvent faire en fonction du type de virus. Dans notre cas, l'impact de ce virus est visuel et nous pouvons potentiellement tenter un processus afin de supprimer intégralement le virus de notre pc mais nos données à l'intérieur de celui-ci sont sûrement déjà aux mains des attaquants. Dans d'autres cas où le virus est discret il pourrait être encore plus dangereux dû au fait que sa présence nous soit inconnue et qu'ils puissent nous voler des informations en continu à des fins malveillantes.

Pentest & Rapport effectué par Morgan Salhi