

# 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 :**

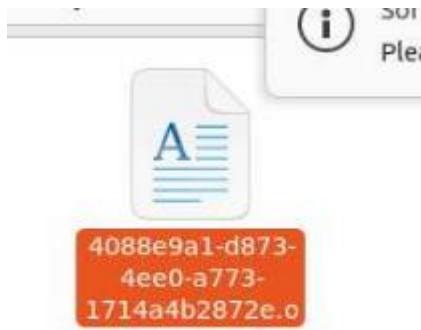
#### **Etape 1 - Observation du virus en tant que root:**

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.



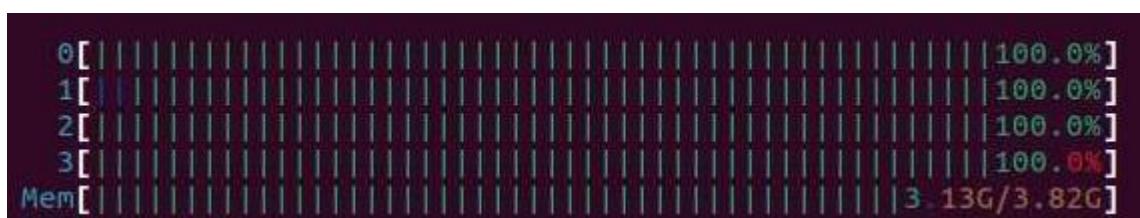
## Valeurs anormales :

Lorsque la commande pour lancer ‘htop’ est effectué, 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 coeurs 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: | <a href="https://app.any.run/tasks/6dcf570e-df95-4cf2-ab23-71bcfbab069e">https://app.any.run/tasks/6dcf570e-df95-4cf2-ab23-71bcfbab069e</a> |
| 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 lié 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 liées 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 | ? | 10.0.1         | 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 :

The screenshot shows the ANY.RUN analysis interface for a file named .redtail. The Threat Verdict is 'Malicious' (100 OUT OF 100). The Timeline of the process shows a single event at 43.96 s. The main pane displays several findings under 'Danger' and 'Warning' levels:

- Danger 2:** MINER has been detected (SURICATA)
- T1071 Application Layer Protocol (1):** Connects to the CnC server
- Warning 4:** Potential Corporate Privacy Violation
- 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 perçu.

|          |   |       |                           |  |
|----------|---|-------|---------------------------|--|
| 45232 ms | <b>Misc Attack</b>                              | 13017 | 6dcf570e-df95-4cf2-ab2... | ET COMPROMISED Known Compromised or Hostile Host Traffic group 7                 |
| 45235 ms | <b>Misc Attack</b>                              | 13017 | 6dcf570e-df95-4cf2-ab2... | ET DROP Spanhaus DROP Listed Traffic Inbound group 38                            |
| 45238 ms | <b>Misc Attack</b>                              | 13017 | 6dcf570e-df95-4cf2-ab2... | ET 3CORESec Poor Reputation IP group 6   |
| 45244 ms | <b>Crypto Currency Mining Activity Detected</b> | 13017 | 6dcf570e-df95-4cf2-ab2... | MINER [ANY.RUN] CoinMiner Agent CrC Initial Connection                           |
| 47769 ms | <b>Potential Corporate Privacy Violation</b>    | 13017 | 6dcf570e-df95-4cf2-ab2... | ET POLICY Cryptocurrency Miner Checkin   |
| 47770 ms | <b>Misc Attack</b>                              | 13017 | 6dcf570e-df95-4cf2-ab2... | ET DROP Spanhaus DROP Listed Traffic Inbound group 14                            |
| 47771 ms | <b>Misc Attack</b>                              | 13017 | 6dcf570e-df95-4cf2-ab2... | ET 3CORESec Poor Reputation IP group 12  |
| 102.55 s | <b>Potential Corporate Privacy Violation</b>    | 13017 | 6dcf570e-df95-4cf2-ab2... | ET POLICY Cryptocurrency Miner Checkin   |
| 209.56 s | <b>Not Suspicious Traffic</b>                   | 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 avions trouvés dans la liste plus haut. On peut également observer plus profondément via Wireshark.

The screenshot shows a 'Threat details' page from a security tool. At the top, it says 'Here are the details of the threat'. Below that are three tabs: 'Main' (which is selected), 'Stream data', and 'Suricata rule'. To the right, it says 'The data provided by Suricata IDS'. Under the 'Main' tab, there is a single threat entry highlighted with an orange box:

**Misc Attack**

**ET COMPROMISED Known Compromised or Hostile Host Traffic group 7**

Below this, there is a table of threat details:

|                 |  |
|-----------------|--|
| 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 293.656917 93.123.39.174 192.168.100.44 TCP 429 [TCP Spurious Retransmission] 2137 - 50240 [PSH, ACK] Seq=4007 Ack=350 Win=64384 Len=354 TStamp=407287400 TSecr=2798327330    |
| 12290 293.659283 93.123.39.174 192.168.100.44 TCP 78 [TCP Dup ACK 12288#1] 50240 - 2137 [ACK] Seq=350 Ack=4361 Win=64128 Len=0 TStamp=2798358850 TSecr=4097287400 SLE=4007 SRE=4981 |

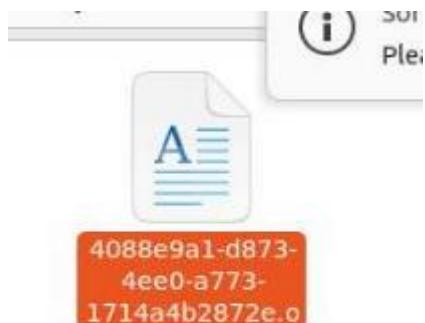
## Etape 2 - Observation du virus en tant qu'utilisateur :

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$ █

```

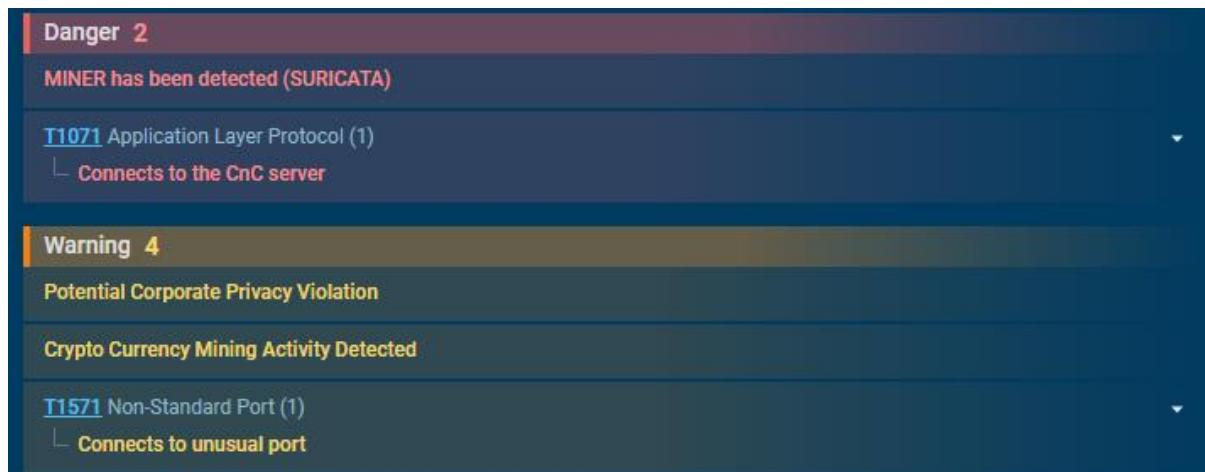
## Valeurs anormales :

Comme pour le fichier que nous avions 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.

| CPU Usage Summary |      |             |    |                                |       |                              |   |          |          |
|-------------------|------|-------------|----|--------------------------------|-------|------------------------------|---|----------|----------|
|                   |      |             |    |                                |       |                              |   |          |          |
| 0[██████]         |      | 100.0%      |    | Tasks: 142, 290 thr; 4 running |       | Load average: 5.66 3.01 1.54 |   |          |          |
| 1[██████]         |      | 100.0%      |    | Uptime: 00:53:03               |       |                              |   |          |          |
| 2[██████]         |      | 100.0%      |    |                                |       |                              |   |          |          |
| 3[██████]         |      | 100.0%      |    |                                |       |                              |   |          |          |
| Mem[██████]       |      | 3.12G/3.82G |    |                                |       |                              |   |          |          |
| Swp[██████]       |      | 752M/3.81G  |    |                                |       |                              |   |          |          |
| Process List      |      |             |    |                                |       |                              |   |          |          |
| PID               | USER | PRI         | NI | VIRT                           | RES   | SHR                          | S | CPU% ▷   | MEM%     |
| 13017             | user | 20          | 0  | 2388M                          | 2345M | 0                            | S | 349.60.0 | 11:39.74 |
| 13050             | user | 20          | 0  | 2388M                          | 2345M | 0                            | R | 95.460.0 | 2:53.88  |
| 13048             | user | 20          | 0  | 2388M                          | 2345M | 0                            | R | 89.860.0 | 2:38.62  |
| 13049             | user | 20          | 0  | 2388M                          | 2345M | 0                            | R | 83.060.0 | 2:41.24  |
| 13047             | user | 20          | 0  | 2388M                          | 2345M | 0                            | R | 81.760.0 | 2:34.80  |
| 12847             | root | 20          | 0  | 768M                           | 268M  | 263M                         | S | 30.36.9  | 1:18.46  |
| 794               | user | 20          | 0  | 5542M                          | 257M  | 102M                         | S | 14.26.6  | 6:32.81  |
| 12848             | root | 20          | 0  | 768M                           | 268M  | 263M                         | R | 14.26.9  | 0:37.09  |
| 12850             | root | 20          | 0  | 768M                           | 268M  | 263M                         | R | 14.26.9  | 0:39.85  |
| 864               | user | 20          | 0  | 5542M                          | 257M  | 102M                         | S | 3.76.6   | 1:30.30  |
| 866               | user | 20          | 0  | 5542M                          | 257M  | 102M                         | S | 3.76.6   | 1:31.78  |
| 12852             | root | 20          | 0  | 175M                           | 158M  | 258M                         | S | 3.76.1   | 0:00.26  |

## 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 scanné ainsi que votre pc dans son intégralité, cela évite et préviens des dangers.

Pour finir, faites attention aux sites sur lesquels vous allez, vérifier 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 officiel.

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