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 :

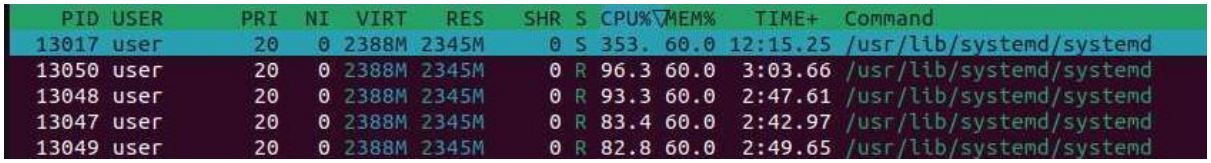
https://app.any.run/tasks/6dcf570e-df95-4cf2-ab23-71bcfbab069e

Exécution :

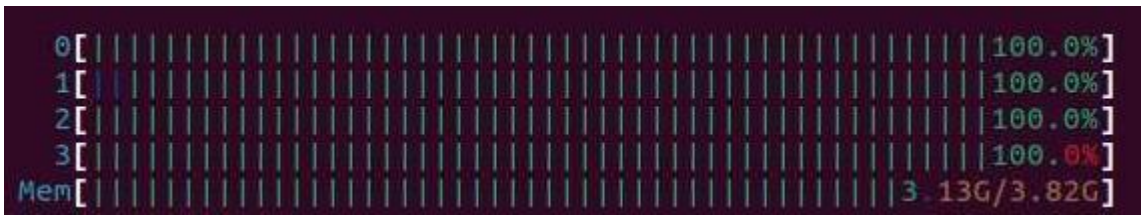
Le fichier que nous avons téléchargé et qu'il faut exécuter afin de déclencher le virus à un nom semblant être au hasard et son extension est '.o'. Les fichiers ayant cette extension sont des fichiers a compilé et à exécuté.

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.

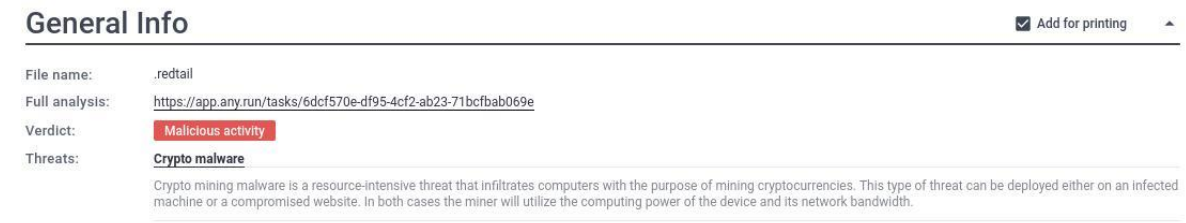


Cela peut également se remarquer par le fait que les 4 cœurs du CPU sont à 100% et la mémoire (RAM) qui est à un usage important.



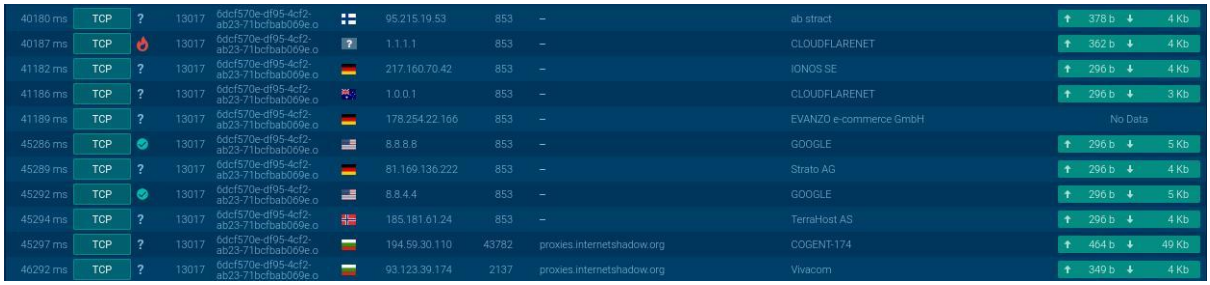
Détection du type de virus :

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.

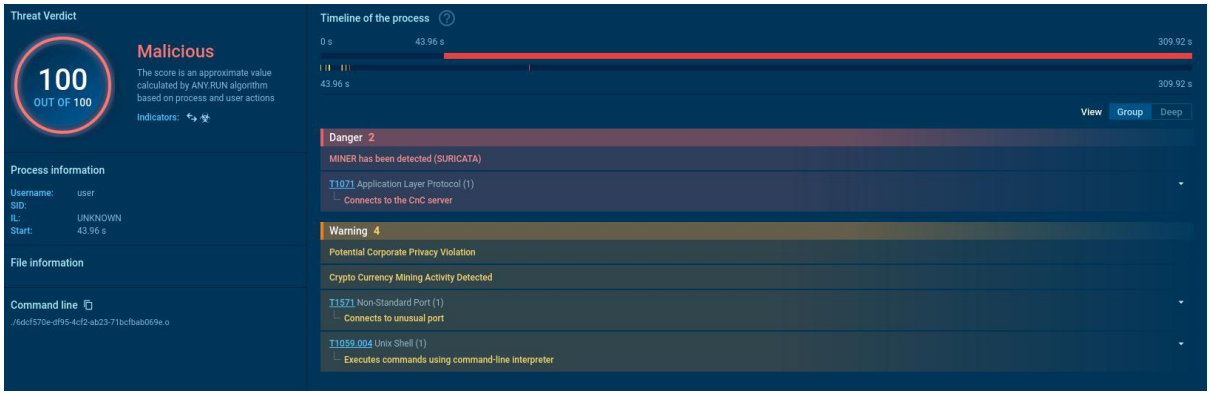


Analyse du réseau liée à ce virus :

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.



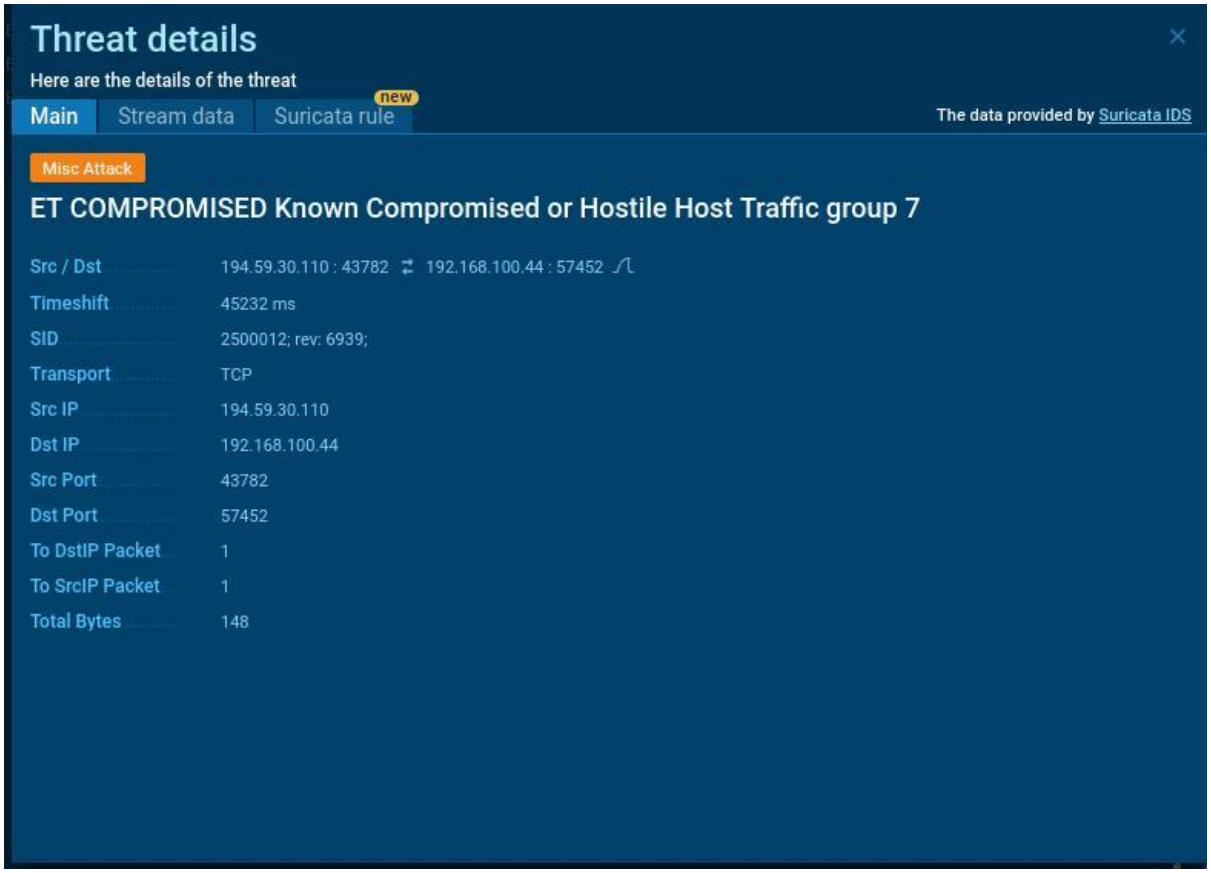
Cependant, elles sont tout de même toutes reliées au même PID et lorsque nous cliquons sur l'une d'elles, les informations suivantes apparaissent :



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.

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.



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

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 :

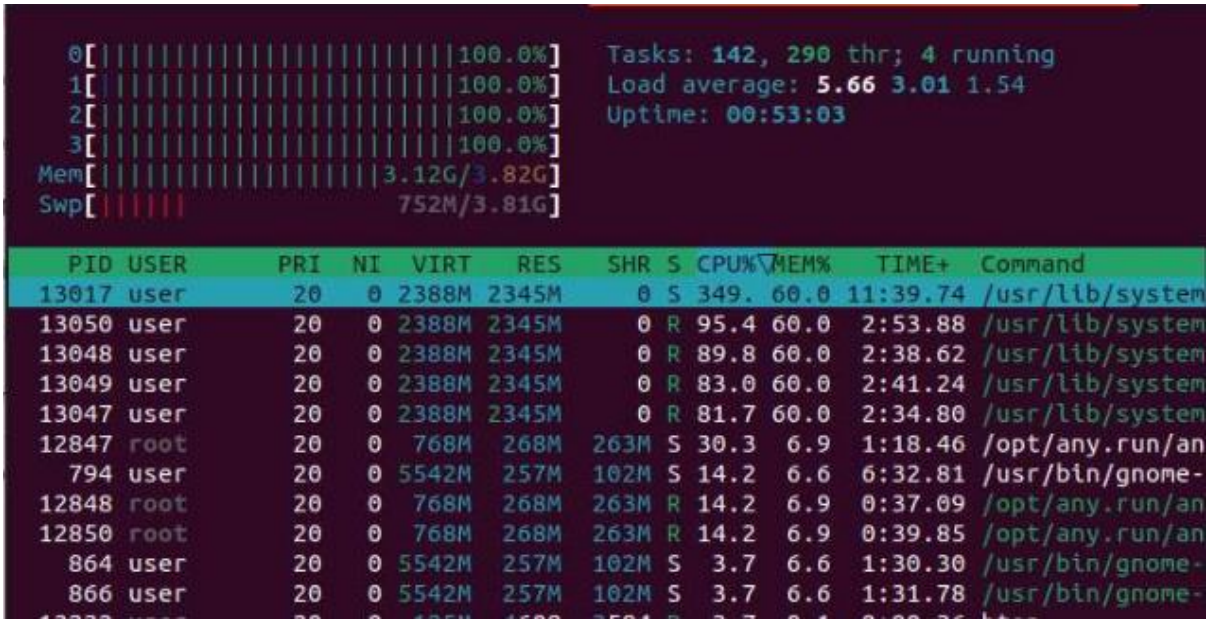
Le fichier que nous avons téléchargé et qu'il faut exécuter afin de déclencher le virus à un nom semblant être au hasard et son extension est '.o'. Les fichiers ayant cette extension sont des fichiers a compilé et à exécuté.

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$
```

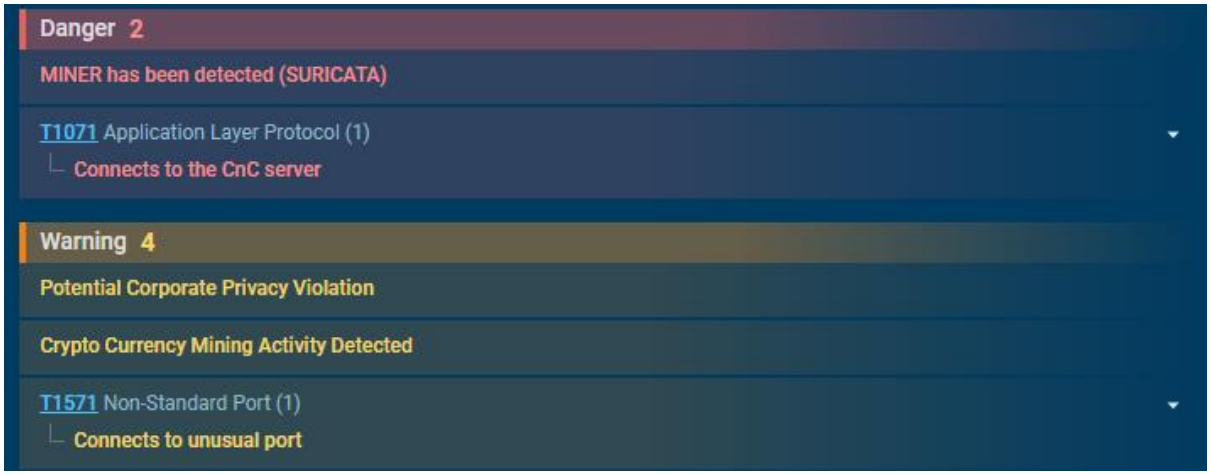
Valeurs anormales :

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 degâts 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 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 surement 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 inconnu et qu'ils puissent nous voler des informations en continue à des fins malveillantes.

Pentest & Rapport effectué par Morgan Salhi