Le voyage d'un sample

chez VirusTotal

Le trajet d'un fichier, son parcours entre les partenaires,
une investigation sur les machines utilisées,
et des idées de contre-attaques.

Par Neosama
@Rafios06

Sommaire

Introduction au service VirusTotal

Développé par Hispasec Sistemas et filiale de Google depuis 2012, VirusTotal est un service gratuit d'analyse de fichiers et URL.

Interrogeant un large panel d'antivirus partenaires, il est un outil redoutable contre les fichiers malveillants.

Introduction au service VirusTotal

Selon leur dire, par défaut, tout fichier soumis détecté par au moins un scanner est envoyé librement à tous les scanners qui ne le détectent pas.

De plus, tous les fichiers soumis entre dans une base de donnée privé auquel les utilisateurs (ayant un accès privilégié) peuvent accéder afin d'améliorer leurs produits et services de sécurité.

Introduction au service VirusTotal

Pour avoir accès a ce privilège, il faut leur faire une demande par écrit pour leur montrer patte blanche.

Car donner un tel accès peut permettre d'étudier les défenses, et donc d'améliorer ses « attaques » .

Ce sont généralement des entreprises, organisations de sécurité, chercheurs et développeurs d'anti-malwares qui y ont droit.

Sample

Le sample utilisé est un programme codé en C++, une fois exécuté il récolte et envoi quelques informations sur un serveur.

Afin d'obtenir une vague idée du système sur lequel il est lancé.

Au fil de mes tests plusieurs versions ont été développées.

Toutes les versions ainsi que les logs récoltés sont disponible sur Github.

Sample VRT00 (V1)

VRT00 est la première version, elle contient plusieurs strings provenant de malwares connus afin de paraître suspects.

Elle permet de récupérer :

- **Le nom de la machine**
- **Le nom d'utilisateur**
- **La position du curseur**
- **Le path d'exécution**
- **Le hash MD5 du fichier exécuté**
- **L'adresse IP (Prise depuis le serveur)**

Sample VRT00 (V1)

Une fois soumis le fichier est partagé et exécuté une multitude de fois assez rapidement.

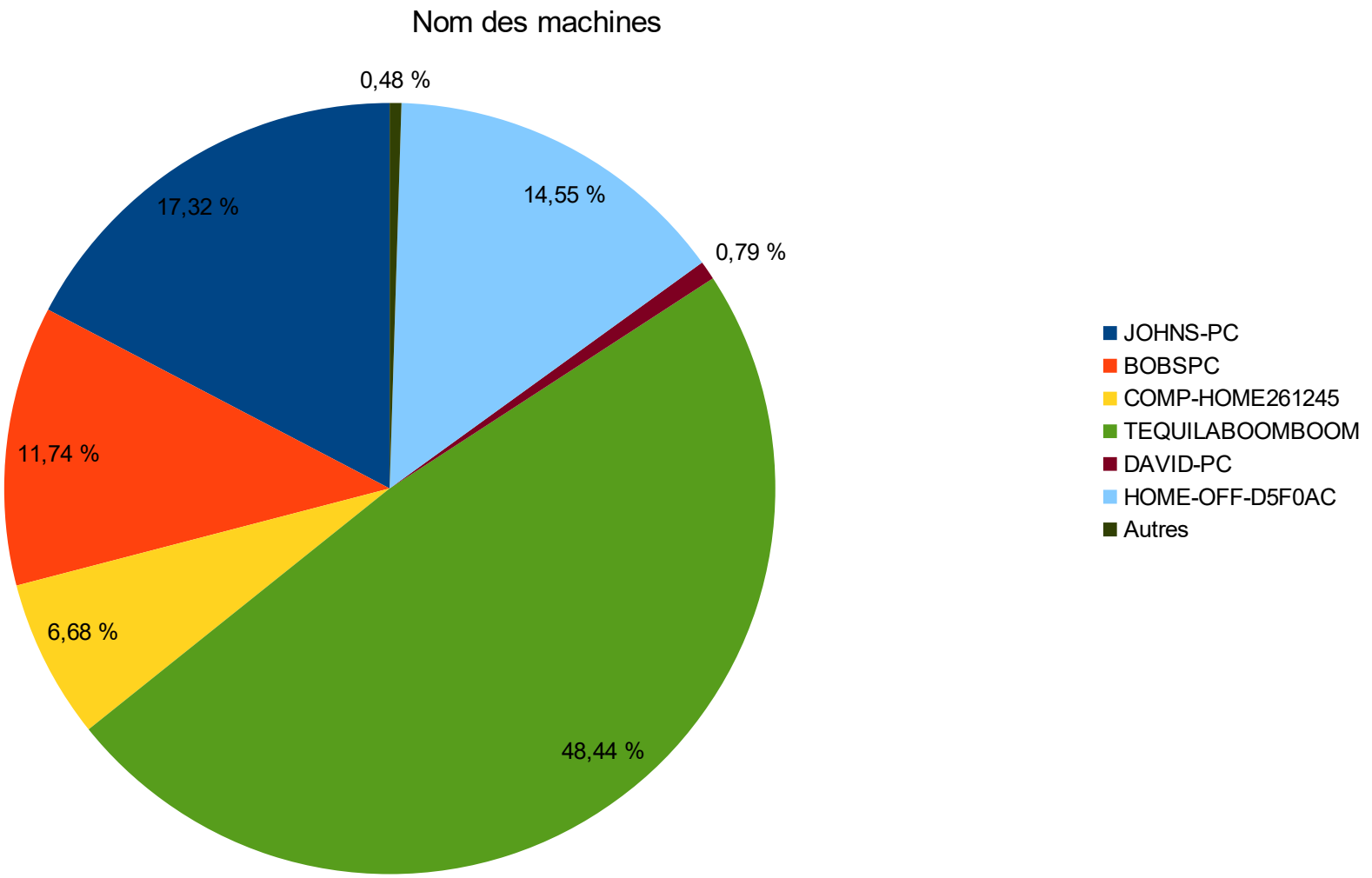
Les logs nous apprennent que certains font transiter leurs trafics via TOR, d'autres utilisent leurs propres IP-Ranges (Par exemple AVAST)

Les noms des machines et d'utilisateurs sont très souvent les mêmes mais quelques fois aléatoires.

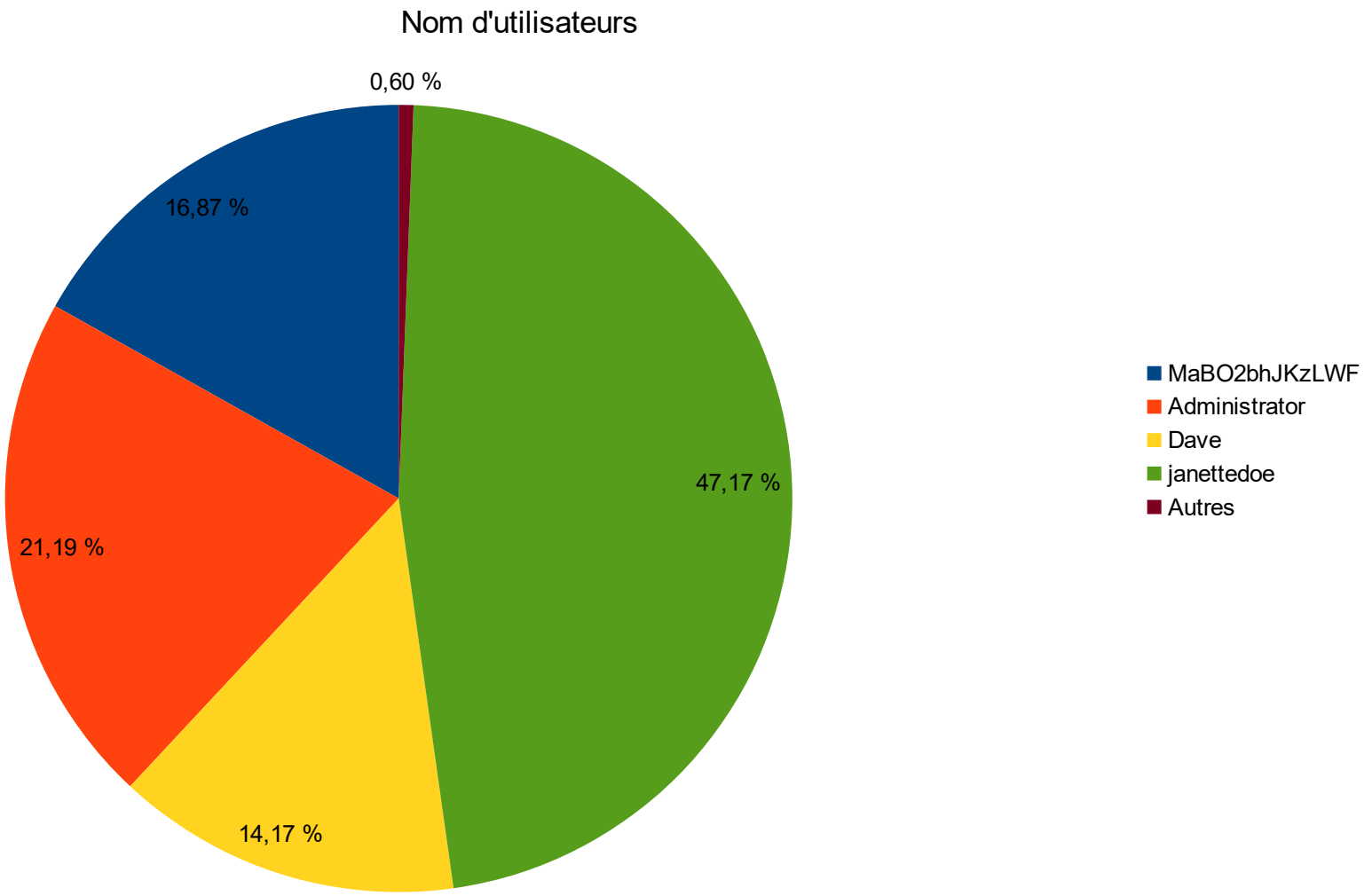
La positions du curseurs est aussi aléatoire sauf chez certains.

Le path d'exécution est généré selon la date, le hash ou aléatoirement.

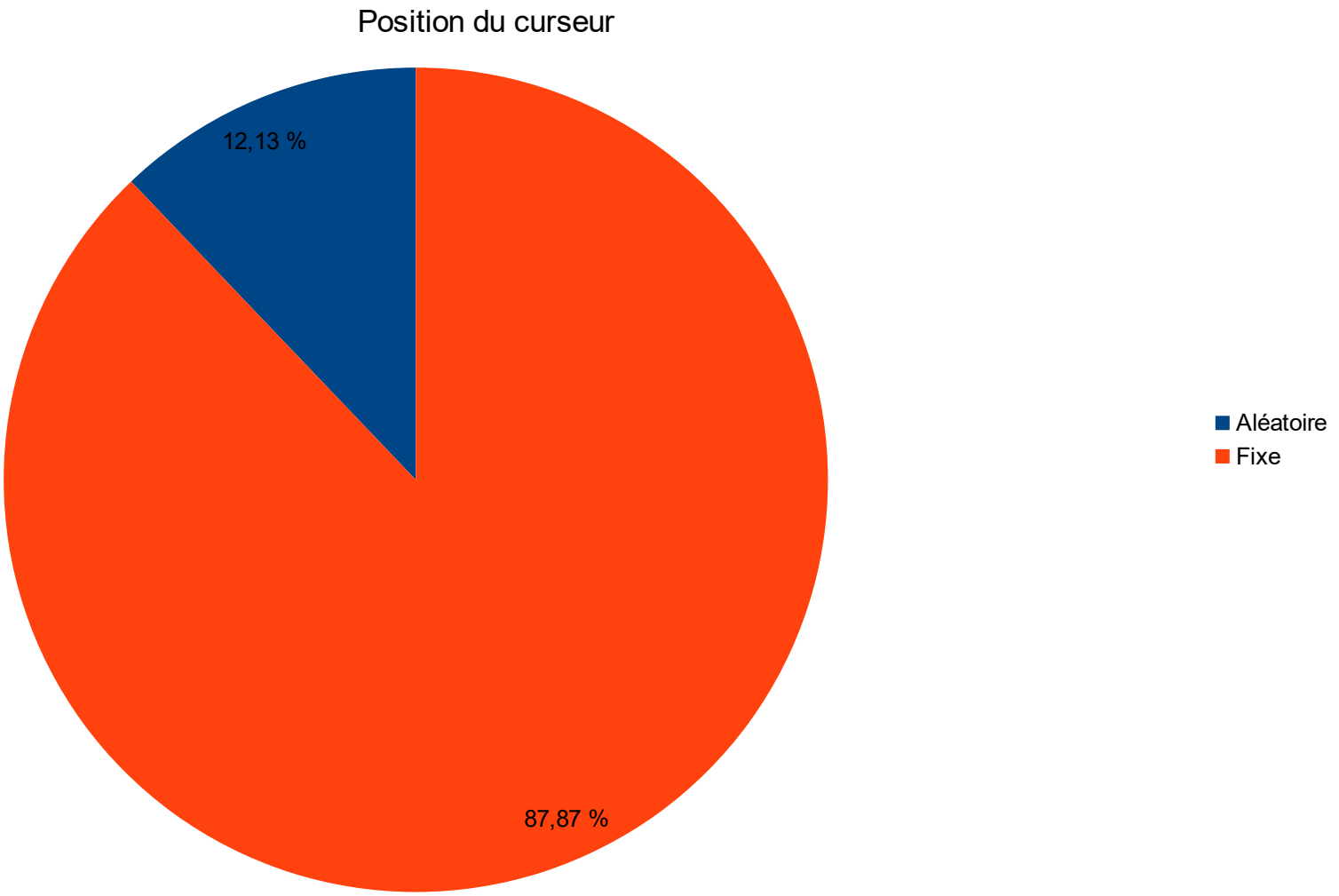
Exploitation des logs de VRT00 (V1)



Exploitation des logs de VRT00 (V1)



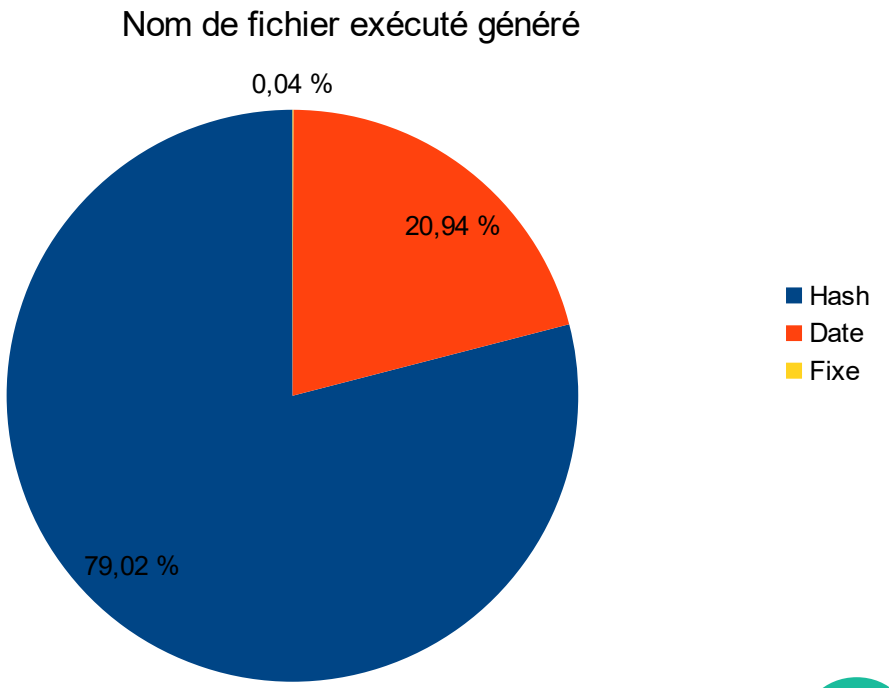
Exploitation des logs de VRT00 (V1)



Exploitation des logs de VRT00 (V1)

Les paths d'exécutions sont soit générés via le Hash du fichier, soit via la date ou encore fixe.

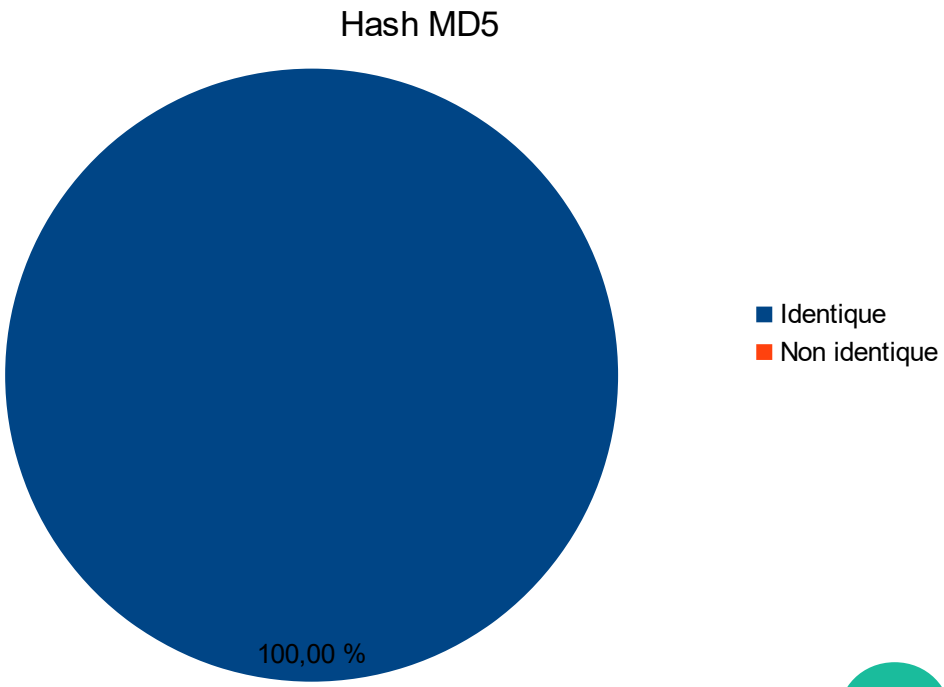
Le diagramme se limite au nom du fichier et non au path complet.



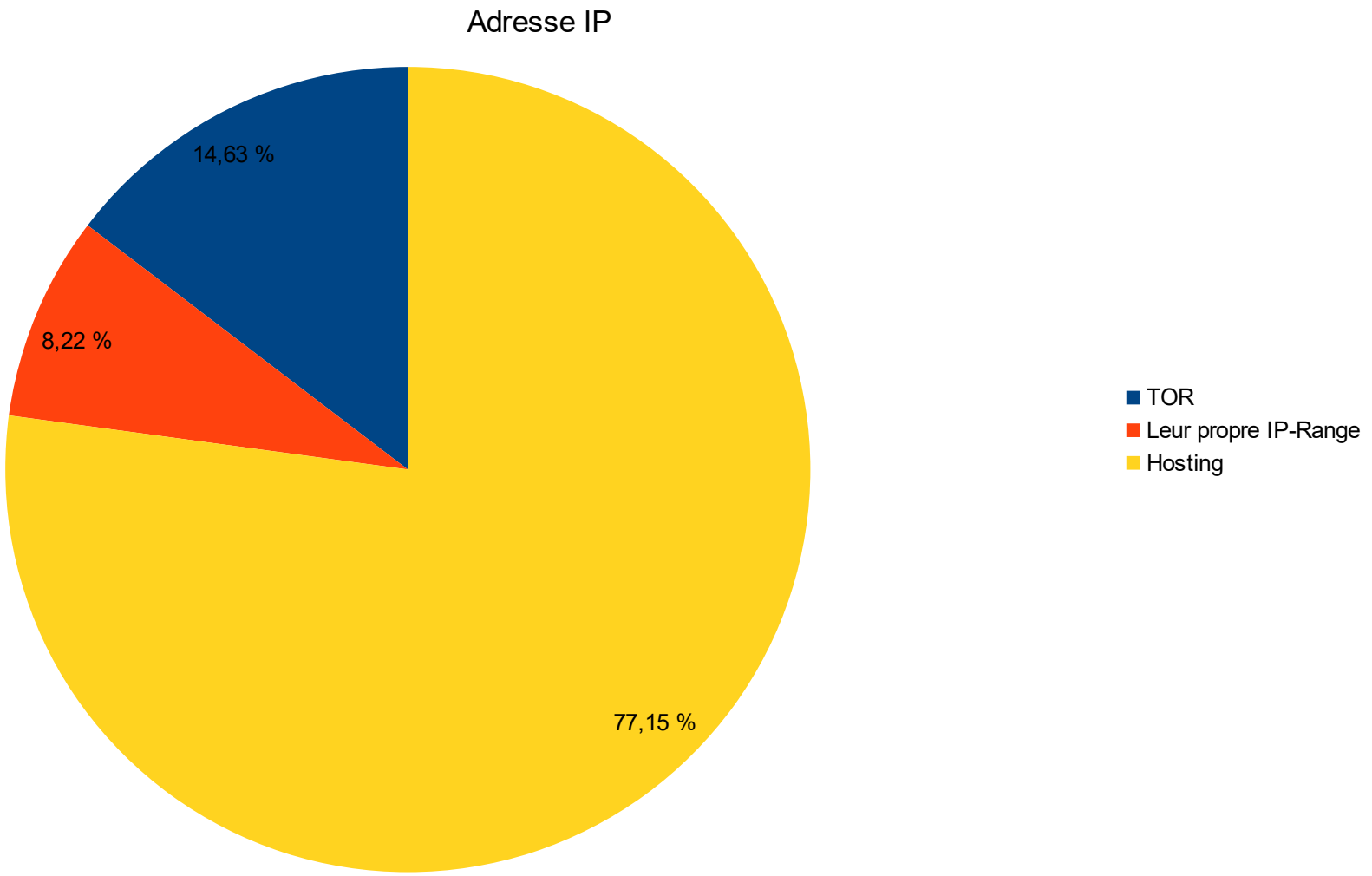
Exploitation des logs de VRT00 (V1)

Le sample envoyé calcule son propre hash MD5, afin de savoir si le fichier a été modifié.

Aucun ne l'a modifié.



Exploitation des logs de VRT00 (V1)



Contre-Attaque

Plusieurs contre-attaques sont envisageable,

j’ai doté un sample (VRT02) d’un contrôle de nom de fichier.

Si il n’est pas identique le programme s’exécute pas totalement.

Très peu ont réussi a passer outre.

Contre-Attaque

Avec toutes les données récoltée sur leurs adresses IP, l'établissement d'une liste d'IP est possible ...

Composé d'après ce que j'ai récolté avec les samples et agrandi via leurs IP-ranges.

Un module de vérification basé sur l'adresse IP et la blacklist peut être intégré dans un malware afin de rester à l'abri des scanners.

Les listes sont également disponibles dans les ressources.

Contre-Attaque

Ce sont des idées (bonnes ou non) pas très poussées et surtout très simples. Juste à des fins de test.

Tout ce petit monde de défenseurs/attaquants évolue MUTUELLEMENT et en permanence.

« C'est plus marrant d'être un pirate que de s'engager dans la marine. »

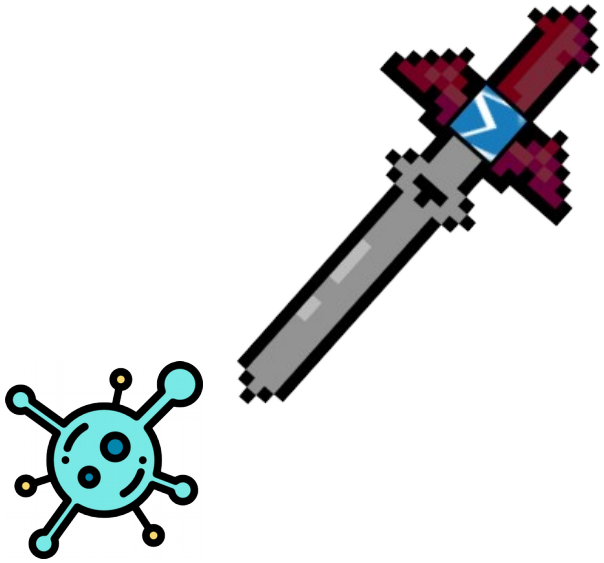
Conclusion

J’ai d’abord voulu en savoir plus sur le fonctionnement interne de VirusTotal, puis au fil du temps et des résultats je me suis demandé si de simples contre-mesures pouvaient les rendre inefficaces.

La réponse n’est pas si simple, Oui un simple contrôle du nom de fichier permet de passer entre les mailles avec pas mal d’antivirus sur VirusTotal.

Non, car beaucoup ne tombe pas dans le subterfuge et comme vu précédemment VirusTotal distribue de façon libre le sample si il est détecté par au moins un scanner et cela de façon périodique.

Conclusion



Une fois le fichier chez VirusTotal quelque soit les mesures en place,

il sera tôt ou tard détecté par tous au fils de leurs mise à jours.

(si celui-ci a quelque chose a se reprocher bien sûr)

Difficile de ne pas faire le parallèle avec une épée Damoclès.

Conclusion

Je n’ai traité que les premiers résultats (Log_010917) et survolé le reste.

Dans les logs, il y a un machine qui m’a intrigué avec comme nom de machine « SPVMTECH-PC », « SPVM TECH » pour nom d’utilisateur et «24.138.88.182» pour IP.

Après vérification ce sigle correspond au Service de Police de la Ville de Montréal mais cela peut être une simple coïncidence.

Étonnant de finir là en partant de VirusTotal.

Ressources

Toutes les sources des samples, listes d'IP ainsi que les logs sont disponible sur Github.

https://www.github.com/Neosama/Le-voyage-d-un-sample-chez-VirusTotal