REPUBLIQUE TUNISIENNE

Ministère des Technologies de la Communication et de l'Économie Numérique

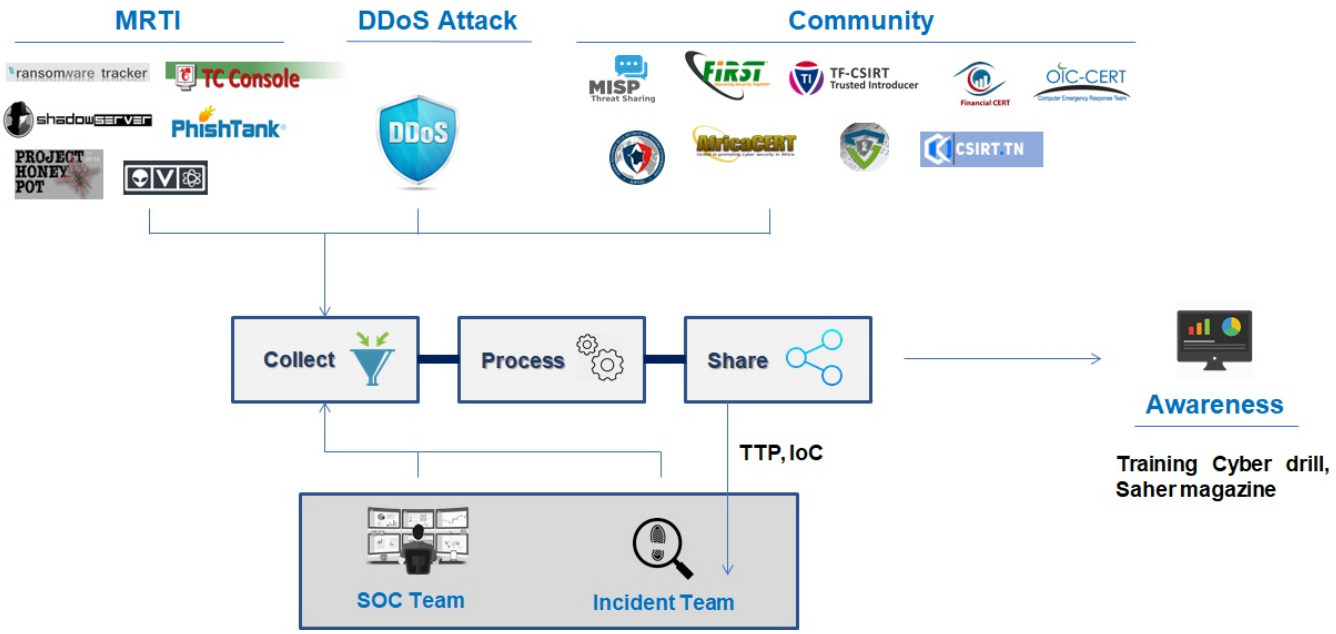
الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Statistiques SAHER
Rapport mensuel

Janvier 2020

TLP:WHITE

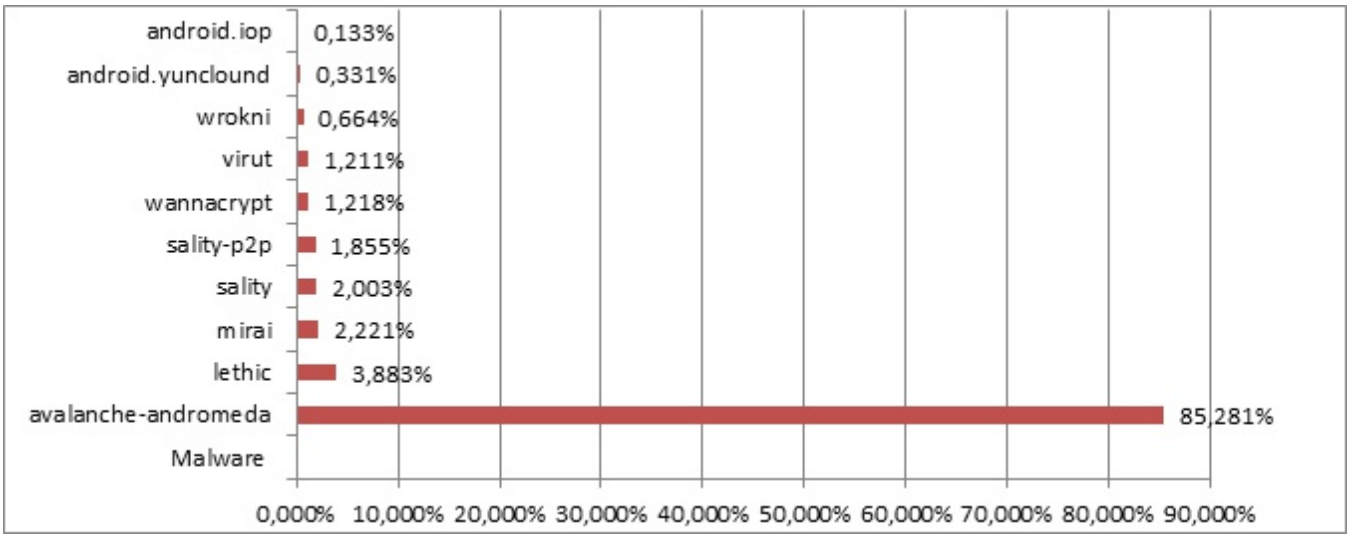
Architecture de SAHER



Statistiques SAHER feeds

1. Top 10 des malwares pendant le mois de janvier 2020

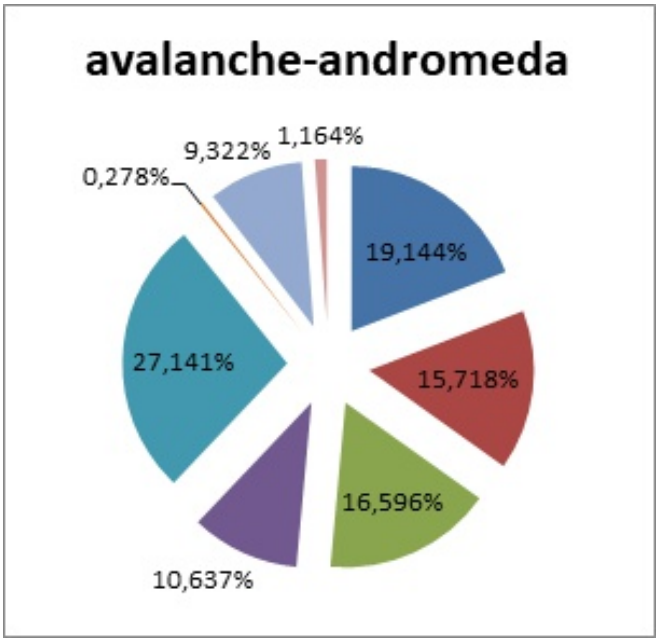
Pour évaluer le niveau de criticité des attaques effectuées par botnet dans le cyberespace tunisien, nous avons calculé le pourcentage de différentes infections durant cette période. Voici une statistique qui élabore ce qui précède.

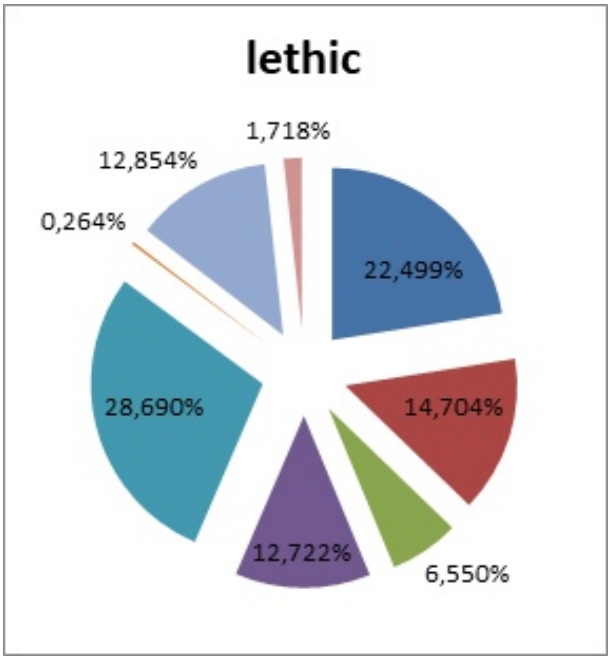


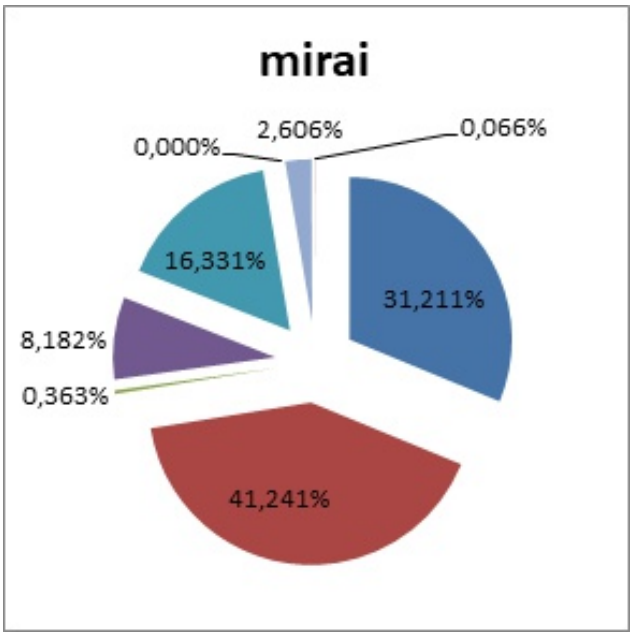
Le diagramme ci-dessus montre qu'avalanche-andromeda se positionne en premier rang de la liste des malwares.

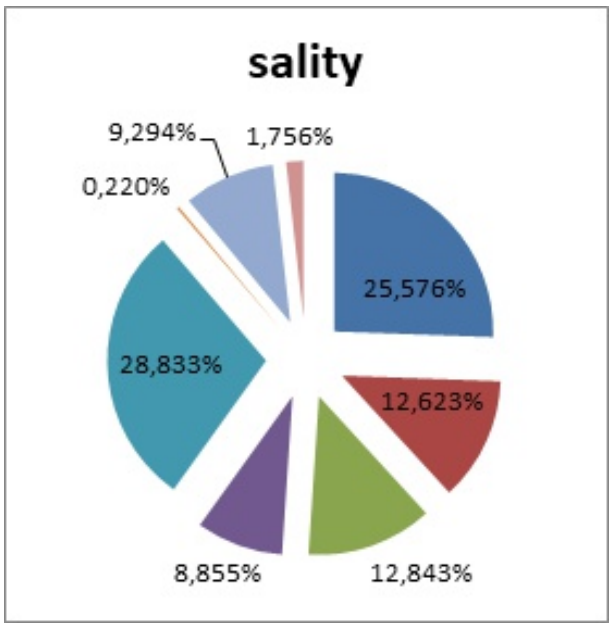
2. Distribution des malwares par fournisseur d'accès internet

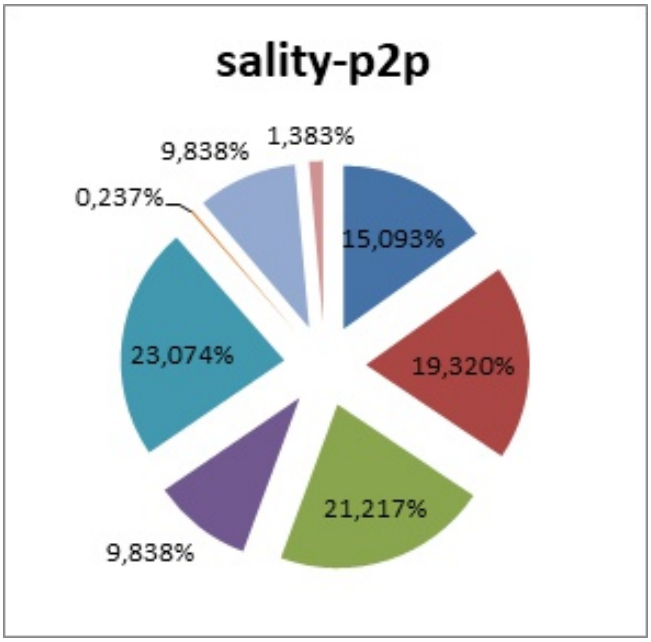
Pendant janvier 2020, on a examiné tous les hôtes infectés par ces botnets sur le cyberespace tunisien et en particulier par fournisseurs d'accès internet. Ainsi, on a dégagé les statistiques suivantes :

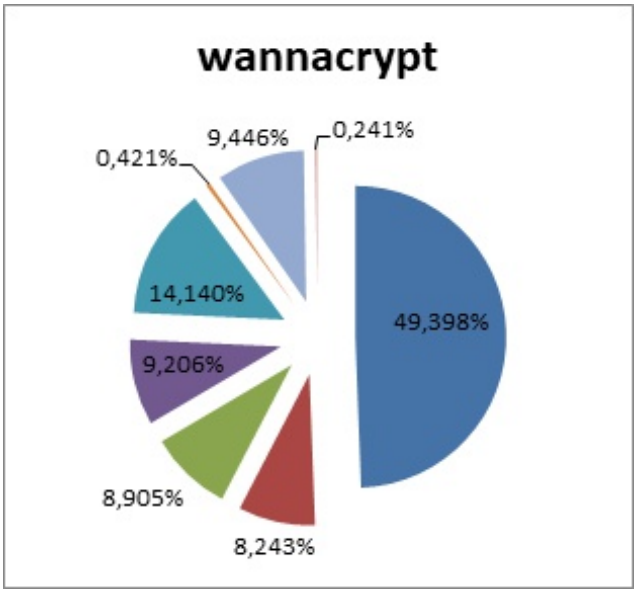

avalanche-andromeda
1,164%
9,322%
0,278%
19,144%
27,141%
15,718%
16,596%
10,637%

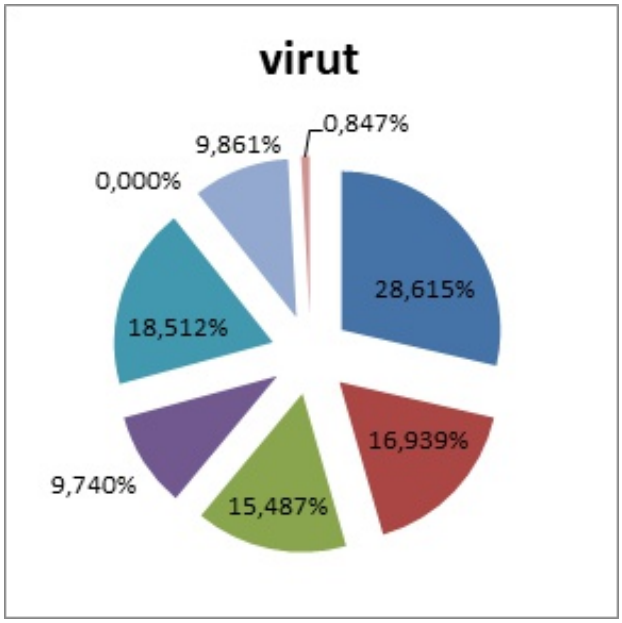

lethic
1,718%
12,854%
0,264%
22,499%
28,690%
14,704%
12,722%
6,550%

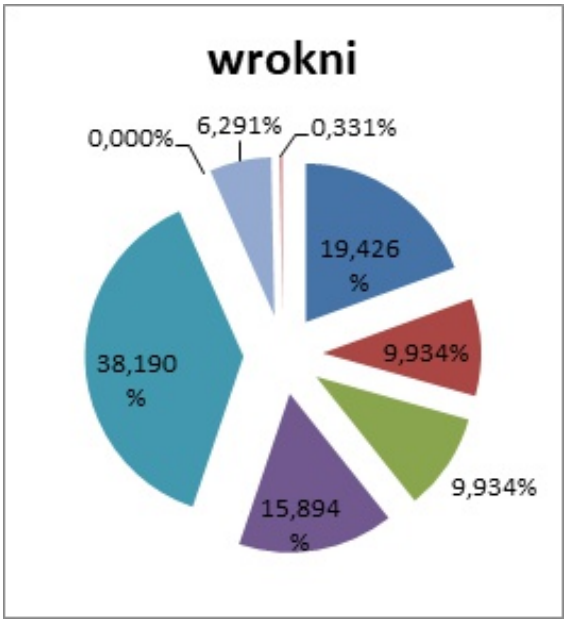

mirai
2,606%
0,066%
0,000%
16,331%
31,211%
8,182%
0,363%
41,241%

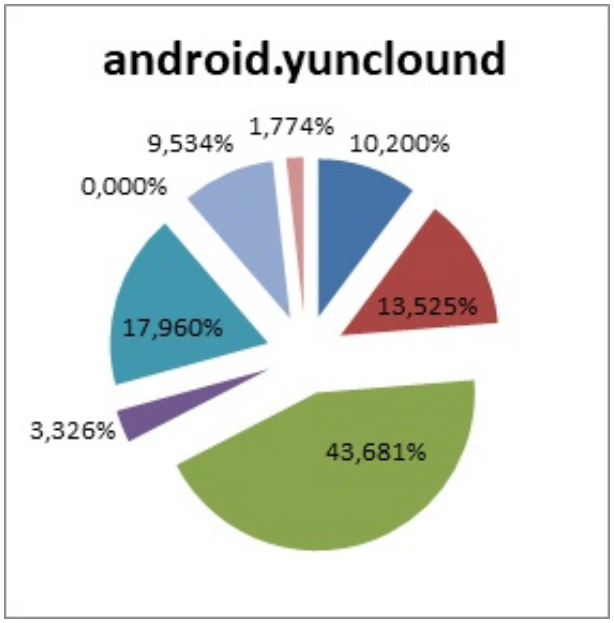

sality
9,294%
1,756%
0,220%
25,576%
28,833%
12,623%
8,855%
12,843%

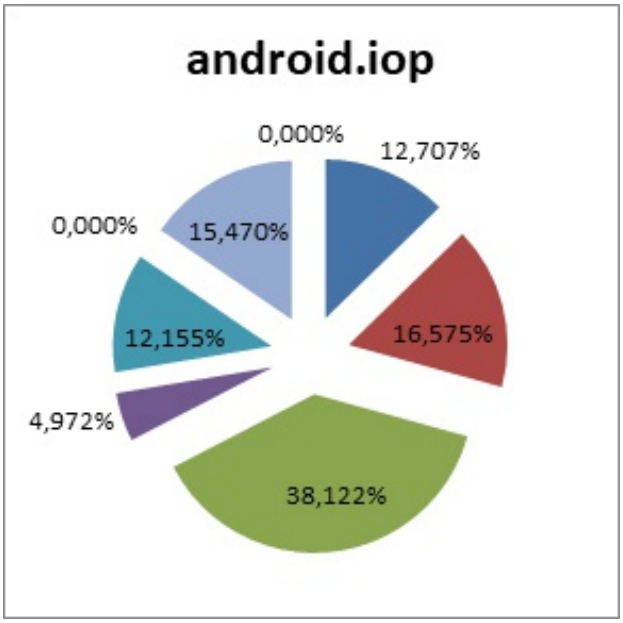

sality-p2p
1,383%
9,838%
0,237%
15,093%
23,074%
19,320%
21,217%
9,838%


wannacrypt
0,421%
9,446%
0,241%
14,140%
49,398%
9,206%
8,905%
8,243%


virut
9,861%
0,847%
0,000%
28,615%
18,512%
16,939%
9,740%
15,487%

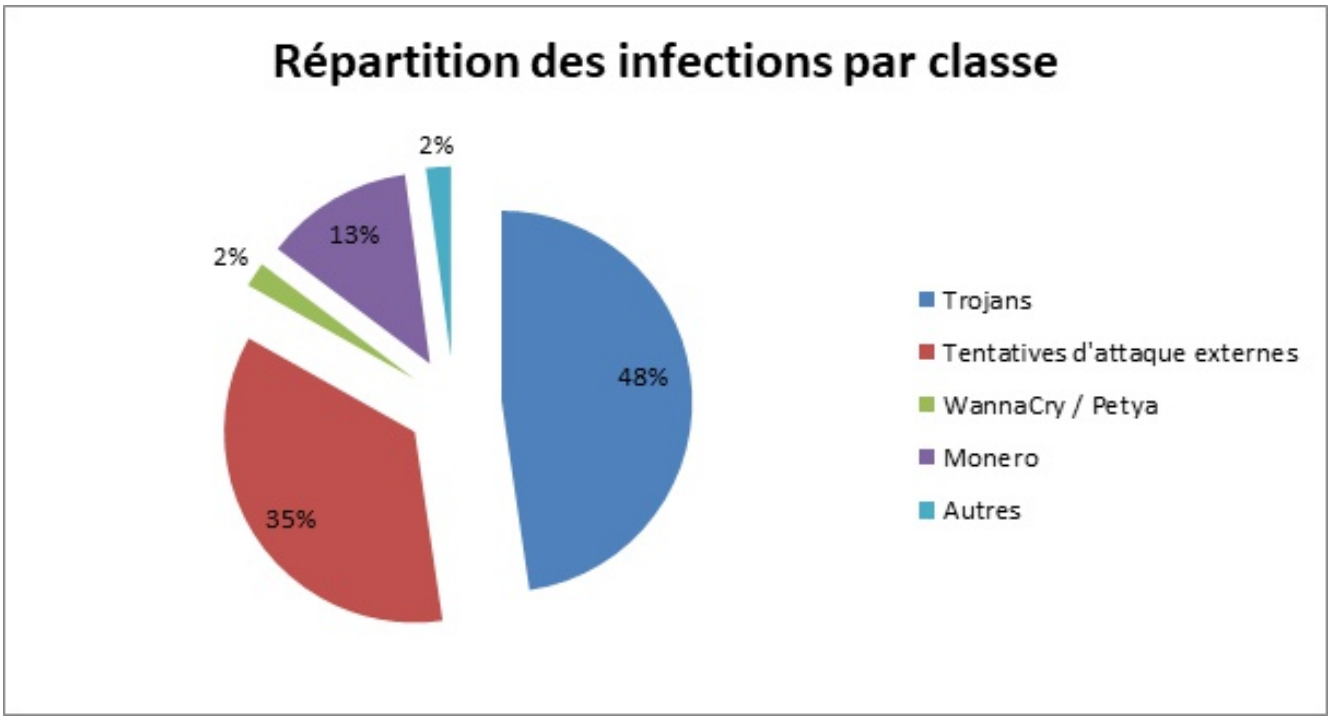

wrokni
0,000%
6,291%
0,331%
19,426 %
9,934%
38,190 %
9,934%
15,894 %


android.yunclound
9,534%
1,774%
10,200%
0,000%
13,525%
17,960%
3,326%
43,681%


android.iop
0,000%
12,707%
0,000%
15,470%
16,575%
12,155%
4,972%
38,122%

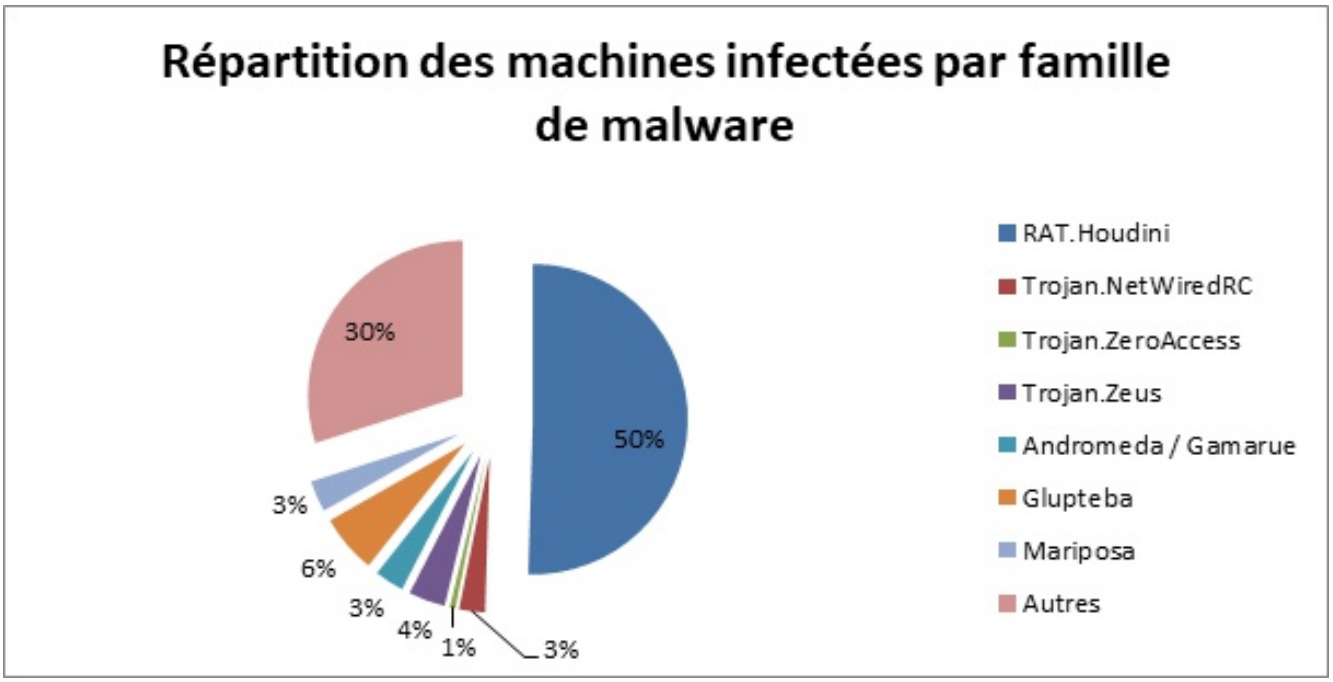
Statistiques sondes SAHER

Durant le mois de Janvier, les sondes SAHER ont détecté plus de 400 000 évènements provenant des 2 sondes actives, à savoir CIMS et CNTE.
Une analyse approfondie de ces alertes a réduit ce nombre à seulement 1093. Ce nombre correspond aux alertes qui ont passé les étapes de filtrage de faux positif, élimination des doublons, et finalement par un tri par criticité.



1. Infections par Trojans

On a regroupé les alertes par famille afin de mieux cerner le taux de pénétration de chaque type de malware. Les taux présentés ci-dessous sont calculés à la base du nombre des machines infectées.



On constate que la famille Houdini/njRAT est dominante. Il s'agit d'un RAT (Remote Access Trojan) qui est très répandu au nord d'Afrique et au Moyen-Orient.

Ce malware met la machine victime sous le contrôle total du C&C, et peut comporter les capacités suivantes :

- Keylogger
- Extracteur des mots de passe navigateur / messagerie
- Téléchargement, exécution et suppression de fichiers
- Etc...

Concernant le groupe « Autres », il se compose de plusieurs trojans différents qui ont été détectés par une communication vers un domaine suspect (comme les TLD .pw, .ru).

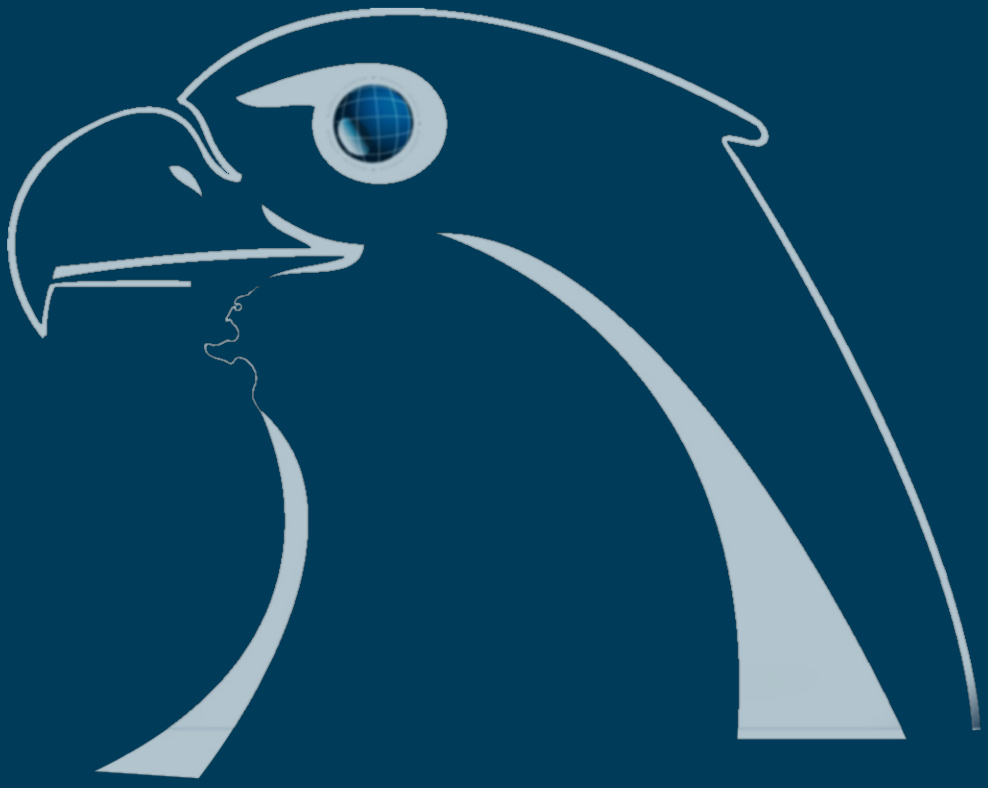
2. Infections par Ransomware

Aucun incident ransomware n'a été détecté ce mois. Cependant, les sondes ont décelé 23 machines ayant une vulnérabilité critique : EternalBlue. Cette vulnérabilité est utilisée par les 2 ransomwares Petya et WannaCry.

Une mise à jour Windows de ces machines est fortement recommandée.

3. Cryptomining

On a détecté une importante activité de cryptomining sur 138 machines. Cette activité concerne principalement Monero (XMRig). Cette activité est probablement liée à la présence de trojans sur ces machines.



49 avenue Jean Jaurès, 1000 Tunis

(+216) 71 846 020

ansi@ansi.tn
incident@ansi.tn
saher@ansi.tn
cert-tcc@ansi.tn
audit@ansi.tn
sahermag@ansi.tn