Malware : le Top 10 des menaces en France (mars 2018)

1 > Coinhive

Ce cheval de Troie est conçu pour effectuer l'extraction en ligne de la crypto-monnaie Monero lorsqu'un internaute visite une page Web sans l'approbation de l'utilisateur.
Le script java implanté utilise les ressources informatiques des utilisateurs finaux pour extraire de la monnaie cryptée.

2 > Roughted

Campagne de publicité malveillante à grande échelle, elle est utilisée pour diffuser divers sites Web et charges embarquées malveillants tels que des escroqueries, des logiciels publicitaires, des kits d'exploitation de vulnérabilité et les logiciels de rançon.
Il peut être utilisé pour attaquer n'importe quel type de plateforme et de système d'exploitation, et utilise le contournement des bloqueurs de publicités pour attaquer de la manière la plus efficace.

3 > Rig ek

Ce kit d'exploitation a été créé en avril 2014. Il a, depuis, reçu plusieurs mises à jour importantes et continue d'être actif aujourd'hui.
L'infection commence avec une redirection vers une page d'accueil contenant du code JavaScript qui vérifie les plug-ins vulnérables et libère le kit d'exploitation.

4 > Necurs

Ce botnet est l'un des plus actifs au monde, et on estime qu'en 2016, il comptait environ 6 millions de bots. Il propage de nombreuses variantes de logiciels malveillants, principalement des chevaux de Troie bancaires et des ransomwares.

5 > Cryptoloot

Ce malware utilise la puissance du processeur ou du GPU de la victime et les ressources existantes pour le crypto-mining – en ajoutant des transactions à la chaîne de blocage et en libérant de nouvelles devises.
Similaire à Coinhive, ce programme est implanté sur des pages Web et utilise le pouvoir de traitement des internautes pour exploiter tous types de crypto-monnaies.

6 > Jsecoin

Ce mineur JavaScript peut être intégré à n'importe quel site Web. JSEcoin permet de lancer un mineur directement dans le moteur de recherche en échange d'une navigation Web sans publicité.

7 > Conficker

Ver informatique qui cible le système d'exploitation Windows. Il exploite les vulnérabilités de l'OS pour voler des données telles que des mots de passe.
Ainsi, il prend le contrôle des ordinateurs touchés, les transformant en « zombie ». Les ordinateurs contrôlés forment alors un réseau, utile aux hackers.

8 > Fireball

Logiciel publicitaire largement distribué par la société chinoise de marketing numérique Rafotech. C'est un détourneur de navigateur qui change le moteur de recherche par défaut et installe des pixels de suivi, mais qui peut aussi servir à télécharger des logiciels malveillants.

9 > Dyreza

Un Cheval de Troie qui attaque les utilisateurs des sites bancaires en interceptant le trafic web non chiffré.

10 > XWRig

Apparu pour la première fois en 2017, XMRig est un logiciel d'exploitation de CPU open-source utilisé pour extraire des crypto-monnaies Monero.