Malware : le Top 10 des menaces en France (Mai 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. Le script java implanté utilise les ressources informatiques des utilisateurs finaux pour extraire de la monnaie cryptée.

2 – 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.

3 – 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.

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 – 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.

6 – Conficker : Conficker est un 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.

7 – Fireball : Fireball est un 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.

8 – Dorkbot : Dorkbot est un verre basé sur un IRC conçu pour permettre l'exécution de code à distance, ainsi que le téléchargement de logiciels malveillants vers le système déjà infecté. Ce dernier permet de voler des informations sensibles et de lancer des attaques par déni de service. Il installe un rootkit en mode utilisateur pour empêcher l'affichage ou l'altération des fichiers et modifie le registre pour s'assurer qu'il s'exécute chaque fois que le système démarre. Il enverra des messages à tous les contacts de l'utilisateur infecté, ou détournera un thread existant, pour diffuser un lien renvoyant vers la copie du verre.

9 – Murofet : Cheval de Troie qui cible la plate-forme Windows, ce logiciel malveillant est conçu

pour implanter des fichiers malveillants supplémentaires dans un système déjà infecté. Il peut se propager via des spams et les fonctionnalités provenant d'autres logiciels malveillants.

10 – Virut : Virut est l'un des principaux distributeurs de botnets et de logiciels malveillants sur Internet. Il est utilisé lors d'attaques DDoS, de distribution de spam, de vol de données et de fraude. Ce malware se propage par le biais d'exécutables provenant de périphériques infectés, tels que des clés USB, ou via des sites Web compromis. Par ces biais, Virut modifie les fichiers hôtes locaux et ouvre une porte dérobée permettant de rejoindre un canal IRC contrôlé à distance par un hacker.