Vocabulaire

Hacker

- Amateur d’informatique et de nouvelles technologies qui crée, analyse et modifie des programmes informatiques pour améliorer ou apporter de nouvelles fonctionnalités à l'utilisateur
- Spécialiste en informatique qui utilise ses connaissances de la sécurité informatique pour en rechercher et en exploiter les faiblesses

Black hat, grey hat, white hat

Il existe souvent plusieurs facettes à la pratique des individus intervenant aux marges du numérique et sur les réseaux.

S’ils sont tous des hackers qui réalisent des tentatives d'intrusion et autres afin de tester la sécurité des systèmes d'information, les white hats avertissent lors de la découverte de vulnérabilités, les grey hats vont généralement donner un délai aux entreprises pour régler le problème avant de rendre la vulnérabilité publique, ils s'opposent aux black hats qui sont des hackers mal intentionnés

Cracker

Type de pirate informatique

- Piratage de systèmes informatiques
- Cassage des protections dites de sécurité (cryptographie, protection des logiciels payants)

Phreaker

Activité des personnes étudiant, testant, ou exploitant de manière frauduleuse les systèmes téléphoniques

Warez

Activités illégales de diffusion de contenus numériques protégés par les droits d'auteurs

Social engineering

Ingénierie sociale, pratiques de manipulation psychologique à des fins d'escroquerie

- Hameçonnage ou phishing
- Fraude au président (la victime est dans une situation de subordination hiérarchique)
- Pretexte ou bohoing (l'attaquant cherche à se faire passer pour un membre de l'entreprise ou un autorité comme la police, la banque, un enquêteur...)

Geek

Personne accro à la technologie spécialement de l'information, des nouveaux médias, comme les réseaux sociaux

Exploit

Élément de programme permettant à un individu malveillant d'exploiter une faille de sécurité dans un système informatique, le but est de s'emparer des ressources d'un ordinateur ou d'un réseau ou d'effectuer une attaque

Malware

- **Ver** : logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet, contrairement au virus, le ver se propage sans avoir besoin de se lier à d'autres programmes exécutables
- **Virus** : code malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés «hôtes»
- **Cheval de Troie** : logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante
- **Backdoor** : ouvre un ou plusieurs ports sur la machine, ce qui lui permet d'accéder à internet librement et de télécharger, à l'insu de l'utilisateur, un parasite
- **RAT** (remote administration tool) logiciel de prise de contrôle à distance d'un ordinateur
- **Zero-day** : vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu

Symptômes possibles d'une infection

- Activité anormale de la carte réseau ou du disque dur
- Réactions curieuses de la souris
- Ouvertures impromptues de programmes, du lecteur CD/DVD
- Plantages répétés
- Redémarrage répété du système
- Écran ou fenêtres avec des messages inhabituels
- Un comportement inhabituel dans le fonctionnement de l'ordinateur, tels que: changements d'économiseur d'écran de bureau, modification du rôle des boutons de la souris, modification du volume du lecteur audio
- Ouverture/Fermeture intempestive de fenêtres
- Les programmes commencent ou terminent leur exécution de manière inattendue
- Le navigateur accède tout seul à certains sites Internet
- Présence d'autres programmes qui n'ont pas été volontairement installés
- Vol de renseignements personnels : informations bancaires, mots de passe, codes de sécurité...
- Suppression, modification ou transfert de fichiers
- Exécution ou arrêt de processus
- Arrêt ou redémarrage impromptus de l'ordinateur
- Surveillance des frappes
- Captures d'écran impromptues
- Espace libre du disque dur occupé par des fichiers inutiles