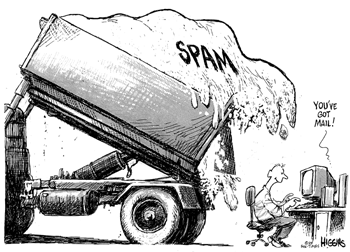
Présentation et définition des différents cybercriminels :





1. Enjeux
2. Attaque de type conventionnel

Ce type d’attaque utilise comme support, les technologies associées aux réseaux d’information et de communication. Généralement, le but est de profiter de la crédulité des utilisateurs pour leur soustraire des informations confidentielles et s'en servir ensuite de manière illégale.

Il existe toute sorte d’infractions dites conventionnelles, et leur nombre augmente continuellement. Les plus classiques étant :

* extorsions de fond;
* fraude liée à la carte de crédit;
* menaces répréhensibles diverses, de type «vengeance»;
* fraude commerciale;
* abus de confiance et escroqueries diverses;
* détournements de mineurs;
* usurpation d'identités.

Il s’agit en effet de l’ensemble des crimes et délits « traditionnels » qui se transpose sur les réseaux numériques d’information et de communication.

Ces attaques sont essentiellement motivées par la cupidité (la recherche d’un gain quel qu’il soit : financier ou encore matériel) ou des comportements immoraux, malsains et maladifs (telle que la pédophilie, les réseaux de prostitution, le racisme, révisionnisme...etc).

1. Attaque de type technologique

Ce type d’attaque a fortement évolué depuis son apparition ; elle exploite essentiellement les nombreuses vulnérabilités de l'outil informatique.

Les attaques les plus répandues sont :

* l'installation de programmes espions,
* l'installation de programmes pirates,
* les intrusions,
* les détériorations diverses,
* les destructions de sites,
* le vol d’informations,
* les dénis de service sur des sites,
* le rebond à partir de sites informatiques victimes…etc.

Une attaque de type technologique peut être fondée par l'une, ou la combinaison de plusieurs des motivations suivantes :

* stratégiques (vol d'informations sensibles classifiées),
* idéologiques (transformation de pensées prédominantes ou de courant d’idées en actes illicites),
* terroristes (visant à déstabiliser un ordre établi),
* cupide (recherche d’un gain financier ou matériel),
* ludique (pour s'amuser ou par loisir),
* vengeur (réaction à une frustration quelconque).

Elles visent soit la confidentialité, l’intégrité ou encore la disponibilité d’un système informatique (voire une combinaison des trois).

1. **Les différentes catégories de hackers**

En général, les hackers sont des individus qui possèdent un niveau très avancé en informatique, et ce sont également des personnes avides de connaissances, qui désirent tout comprendre sur le mécanisme de fonctionnement d’un système informatique, afin d’en localiser les failles de sécurité et les exploiter à son avantage. L’on peut distinguer plusieurs catégories de hackers.

Les différents types de hackers :

* Les « White Hat hackers » : Ce premier groupe est constitué de hackers de bonne volonté, qui ne ménagent pas leurs efforts pour chercher des innovations dans le cadre de la sécurisation d’un système informatique. Les White Hat contribuent habituellement à l’identification et à la réparation de failles de sécurité à l’intérieur d’un système, et ne peuvent être assimilés à des cybercriminels.
* Les « Grey Hat hackers » : A la différence des White Hats, le hacker « grey hat » accède illégalement à un système, informe l’existence de failles aux personnes responsables et proposent généralement des solutions, mais n’endommage pas le système.
* Les « Black Hat hackers » : Les « Black Hats » hackers sont des pirates informatiques qui détruisent tout sur leur passage. N’ayant pas le moindre scrupule, ils ne se contentent pas d’accéder illégalement dans un système, mais y introduisent également des virus et des malwares susceptibles de compromettre la sécurité du système et l’intégralité du système en question.
* Les « Lamers » et « Script Kiddies » : Ce sont des utilisateurs peu expérimentés mais susceptibles d’altérer et de détruire tout un système par simple maladresse.
* Les «  Crackers  » : Les crackers sont plutôt doués pour cracker des programmes, leur principal objectif consiste à violer les systèmes de protection contre la copie des logiciels payants.
* Les Phreakers : Ce sont également des pirates, mais spécialisés en « phreaking » ou piratage de lignes téléphoniques.
* Les Carders : Les Carders sont des hackers spécialisés en matière de « piratage de cartes à puce ».
* Les Hacktivistes : Les hacktivistes sont des hackers dont la seule motivation repose sur des idéologies sociales, politiques, religieuses ou autres.





1. **Exemple de cybercrimes et de leurs démantèlement (partiel ou non)**

* **Le groupe Anonymous n’est plus anonyme :**le groupe de pirates connu sous le nom d’Anonymous a conduit des attaques contre des cibles commerciales et politiques pendant plusieurs années et les organismes d’application de la loi avaient du mal à pénétrer dans l’organisation afin de la démanteler. L’un des premiers grands succès fut [les arrestations de membres d’Anonymous menées par les autorités dans plusieurs pays](https://threatpost.com/en_us/blogs/interpol-operation-leads-arrest-25-suspected-anons-022912). Les individus arrêtés ont été accusés de mener des attaques contre des sites situés au Chili, en Colombie ainsi que dans d’autres pays.
* **Les fédéraux arrêtent Sabu :** En mars 2012, les autorités ont peut-être connu leur plus grand succès contre Anonymous, quand les agents fédéraux ont [arrêté Sabu](https://threatpost.com/en_us/blogs/report-feds-arrest-top-lulzsec-members-030612), le célèbre leader du groupe rejeton d’Anonymous, LulzSec. L’[arrestation de Sabu](https://threatpost.com/en_us/blogs/chats-car-crushes-and-cut-n-paste-sowed-seeds-lulzsecs-demise-030712) a provoqué des ondes de choc parmi la communauté souterraine et a commencé à révéler peu à peu le groupe. Sabu, dont le vrai nom est Hector Xavier Monsegur, a coopéré avec le FBI et son jugement a été repoussé plusieurs fois, notamment en février dernier.
* **Le responsable présumé du plus grand botnet de Zeus a volé 100 millions de dollars :**Le [malware ZeuS](https://threatpost.com/en_us/blogs/zeus-source-code-leaked-051011) a probablement causé plus de dégâts et de pertes financières ces dernières années que n’importe quel autre, et les autorités ont suivi son utilisation dans le but d’essayer de remonter à son créateur ou aux individus qui gèrent les différents botnets ZeuS. En janvier, les autorités Malaisiennes ont arrêté un homme appelé Hamza Bendelladj, qu’elles suspectent d’être [l’opérateur d’un des plus larges Botnets de ZeuS](https://threatpost.com/en_us/blogs/alleged-zeus-botmaster-arrested-stealing-100-million-us-banks-011013), responsable du vol de plus de 100 millions de dollars auprès de différentes banques américaines.
* **Le botnet Butterfly démantelé :** Les botnets comme ceux utilisés par les utilisateurs de ZeuS, sont des outils clés de l’arsenal des cybercriminels. Ils sont utilisés pour des spams, des attaques DDoS et dans les opérations de fraude bancaire et, il est difficile d’en pincer les opérateurs. Un des succès récents les plus notables fut celui de l’opération menée par les autorités en Nouvelle-Zélande, aux Etats-Unis et dans d’autres pays, qui ont arrêté dix individus impliqués dans le fonctionnement du [botnet Butterfly](https://threatpost.com/en_us/blogs/facebook-security-fbi-take-down-butterfly-botnet-arrest-10-121212). Ce botnet utilisait le malware Yahos pour infecter les utilisateurs de Facebook : les malfaiteurs sont accusés d’avoir volé près d’un milliard d’euros au fil des années.
* **Le groupe du cheval de Troie Carberp**épinglé **:**Les chevaux de Troie bancaires tels que [Carberp](https://threatpost.com/en_us/blogs/carberp-trojan-evolves-and-advances-012111) se trouvent par douzaines, mais cela ne signifie pas que les organismes d’application de la loi ne poursuivent pas les pirates qui se cachent derrière ces virus. Le succès a mis du temps à venir, mais en 2012 les autorités russes ont arrêté plusieurs acteurs présumés impliqués dans [l’opération Carberp](https://threatpost.com/en_us/blogs/russian-agencies-take-down-carberp-gang-032012). Les bénéfices qu’en aurait tirés le gang Carberp sont relativement minces – deux millions de dollars – mais chaque arrestation dans ce domaine est une étape importante dans le démantèlement de la cybercriminalité.
* **SpyEye, l’espion qui m’aimait :** Avec ZeuS, SpyEye est l’un des chevaux de Troie existant les plus populaires de nos jours, et les deux malwares sont en fait très étroitement liés. En juillet 2012, les autorités ont arrêté Pavel Cyganok, un lituanien de 28 ans et Ilja Zakrevskim, un estonien de 26 ans. Ils sont accusés d’avoir utilisé le [cheval de Troie SpyEye afin de voler les identifiants de compte bancaire](https://threatpost.com/en_us/blogs/three-baltic-men-jailed-after-using-spyeye-malware-070212) en ligne de leurs victimes. Ils ont ensuite été accusés par l’unité spécialisée en cybercriminalité de la police métropolitaine centrale d’avoir violé la loi sur l’utilisation abusive de l’informatique au Royaume-Uni. Pendant ce temps, un troisième homme, Aldis Krummins, un lettonien de 45 ans a été jugé coupable de blanchiment d’argent dans le cadre de la même enquête.
* **MegaUpload démantelé dans un méga coup de filet :**La cybercriminalité prend plusieurs formes, et il ne s’agit pas toujours d’une violation évidente comme l’utilisation d’un malware ou l’usurpation d’identité. En janvier 2012, les autorités américaines et néo-zélandaises ont collaboré dans le [démantèlement du service de partage des données, MegaUpload](https://threatpost.com/en_us/blogs/us-shuts-down-megaupload-file-sharing-site-anonymous-retaliates-ddos-attacks-012012), et elles ont procédé à une fouille considérable du domicile de Kim Dotcom, le fondateur du service. Les représentants du gouvernement néo-zélandais se sont plus tard excusés auprès de Dotcom, pour avoir été trop loin et avoir mis en place une surveillance électronique illégale de ses communications. Plus d’un an après, la grande majorité de l’affaire n’est toujours pas résolue.