Cybercriminalité

Comme la criminalité traditionnelle, la cybercriminalité peut prendre diverses formes et peut se produire à tout moment et n'importe où. Les cybercriminels utilisent un certain nombre de méthodes, en fonction de leurs compétences et de leurs objectifs. Cela n'a rien de surprenant : après tout, la cybercriminalité est un type de criminalité, perpétrée à l'aide d'un ordinateur ou dans le cyberespace.

La convention sur la cybercriminalité du Conseil de l'Europe utilise le terme "cybercriminalité" pour faire référence aux délits allant de toute activité criminelle portant atteinte aux données, au non-respect des droits d'auteur. Toutefois, d'autres auteurs comme Zeviar-Geese suggèrent que la définition de cette notion est beaucoup plus vaste et comprend des activités telles que la fraude en ligne, l'accès non autorisé, la pédopornographie, et le harcèlement dans le cyberespace. Le manuel des Nations Unies sur la prévention et la répression de la criminalité liée à l'informatique inclut la fraude, la contrefaçon et l'accès non autorisé [Nations Unies, 1995] dans sa définition de la cybercriminalité.

Ces définitions donnent une bonne indication de la variété d'attaques que la cybercriminalité peut englober. Il est important de comprendre l'étendue de ces attaques car divers types de cybercriminalité requièrent des approches différentes afin d'améliorer la sécurité de votre ordinateur.

Symantec s'inspire des nombreuses définitions de la cybercriminalité et donne la définition concise suivante : tout acte criminel perpétré à l'aide d'un ordinateur ou sur un réseau, ou à l'aide de matériel informatique. L'ordinateur ou le matériel peuvent être l'agent de l'acte criminel, son facilitateur, ou sa cible. L'acte criminel peut se produire sur l'ordinateur uniquement ou à d'autres emplacements également.L'étendue de la cybercriminalité est davantage compréhensible si on la divise en deux catégories générales, nommées dans le cadre de cette étude cybercriminalité de type I et de type II.

La cybercriminalité de type I présente les caractéristiques suivantes :

* Il s'agit généralement d'un événement ponctuel du point de vue de la victime. Par exemple, une victime télécharge sans le savoir un cheval de Troie qui installe un programme d'enregistrement des frappes clavier sur sa machine. Il est possible également que la victime reçoive un courrier électronique contenant un lien prétendu légitime alors qu'il s'agit en réalité d'un lien vers un site Web hostile.
* Il est généralement fourni par des logiciels criminels tels que les programmes d'enregistrement de frappes clavier, les virus, les rootkits ou les chevaux de Troie.

Les failles ou les vulnérabilités d'un logiciel ouvrent généralement la porte à l'attaquant. Par exemple, des criminels contrôlant un site Web pourraient profiter d'une vulnérabilité d'un navigateur Web pour placer un cheval de Troie sur l'ordinateur de la victime.

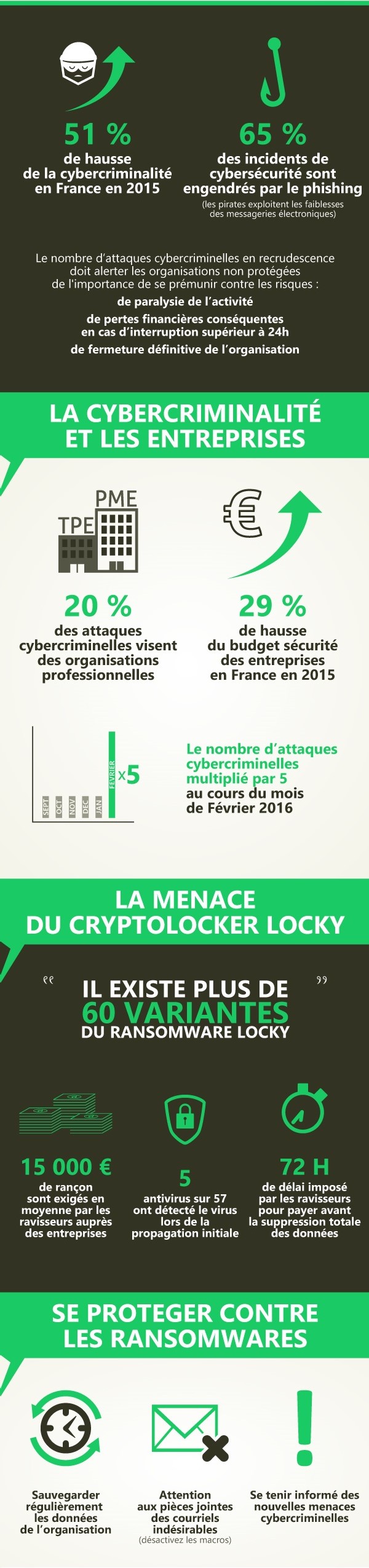
Quant à la cybercriminalité de type II, elle comprend :

le harcèlement sur Internet, la prédation contre les enfants, l'extorsion de fonds, le chantage, la manipulation des marchés boursiers, l'espionnage industriel de haut niveau, ainsi que la planification ou l'exécution d'activités terroristes.

La cybercriminalité de type II présente les caractéristiques suivantes :

Il s'agit généralement d'une série continue d'événements impliquant des interactions répétées avec la cible. Par exemple, la cible est contactée par une personne dans un forum de discussion. Petit à petit, cette personne tente d'établir une relation avec la cible. Le criminel finit par exploiter cette relation dans le but de perpétrer un acte criminel. Des membres d'une cellule terroriste ou d'une organisation criminelle pourraient également communiquer sur un forum de discussion de façon codée et, par exemple, planifier des activités ou débattre du blanchiment de leur argent.

Ce type de cybercriminalité est généralement rendu possible par des programmes qui ne font pas partie de la catégorie des logiciels criminels. Par exemple, les conversations pourraient avoir lieu par le biais de clients de messagerie instantanée.



* 5 entreprises sur 6 employant plus de 2 500 personnes ont été la cible de cyberattaques en 2014
* Entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120% dans le monde et le coût estimé de la cybercriminalité pour les entreprises s’élève en moyenne à 7,6 millions de dollars par an, soit une augmentation de 10%
* 61 % des victimes d’une attaque DDoS ont temporairement perdu l’accès à des informations critiques
* 38 % ont été dans l’incapacité de poursuivre leur activité principale
* 33 % font état de pertes d’opportunités et de contrats
* Dans 29 % des cas, le succès d’une attaque DDoS a eu un impact négatif sur la cote de crédit de l’entreprise
* Dans 26 % des cas, a entraîné une augmentation de ses primes d’assurance
* A la suite d’une attaque DDOS, 49 % ont payé pour faire modifier leur infrastructure informatique, 46 % ont eu recours à leurs avocats et 41 % ont fait appel à des gestionnaires de risque
* 72 % des victimes ont divulgué des informations relatives à une attaque DDoS contre leurs ressources. En particulier, 43 % des responsables interrogés ont informé leurs clients d’un incident, 36 % l’ont signalé aux autorités et 26 % en ont parlé aux médias. 38 % des entreprises ont subi une atteinte à leur réputation à la suite d’une attaque DDoS et près d’une sur trois a dû demander l’aide de conseillers en image
* 48 % des attaques cibleraient directement des applications web des e-commerçants.
* 40 % des attaques par injection SQL et 64 % des campagnes de trafic http malveillant concernent les sites de commerce en ligne.
* Selon l’enquête d’Imperva, les sites de commerce en ligne sont attaqués deux fois plus souvent que des sites plus classiques. Les attaques durent aussi plus longtemps : près de deux fois plus longtemps qu’en 2013.
* 68% des internautes envisagent un achat sur internet d’ici la fin de l’année.
* La valeur économique pillée par la cybercriminalité en 2013 représente 190 milliards d’euros.
* Pour illustrer un coût :

« Sony s’est fait voler 1,5 million de données de cartes bleues. Le dommage direct : 150 millions. Mais Sony réclame à son assureur 1,3 milliard de dollars pour compenser l’arrêt complet de leur serveur pollué de e-commerce, c’est-à-dire de leurs ventes, la modification de leur système d’information et la campagne de communication qui a suivi. »

* Après avoir analysé les données de plus de 100.000 incidents de sécurité sur 10 ans, Verizon a indiqué que 92 % des attaques peuvent être réparties en 9 types de menaces (les attaques de malwares, la perte ou le vol d’appareils, les attaques DDoS, les arnaques à la carte bancaire, les attaques d’applications web, le cyber-espionnage, les intrusions, le vol interne et les erreurs humaines), ce qui signifie que les entreprises font toujours face aux mêmes risques et aux mêmes attaques, depuis tout ce temps, et à plusieurs reprises.

Les fraudes en ligne par carte bancaire ont représenté 64,6% du total des fraudes en 2013, soit un rapport de un à vingt par rapport aux magasins physiques.

* Les e-commerçants ne sont que 43 % à utiliser ces méthodes de protection renforcés (par SMS ou par biométrie) 10 millions de français, 33% des Internautes majeurs victimes de cybercrime (Symantec/Norton 2013).
* Les condamnations d’entreprises ayant piraté des logiciels se sont élevées à 1,3 millions d’euros en 2013, en hausse de 30% par rapport à 2012, représentant 12% du montant des condamnations européennes.
* En juin 2014, 3,2 millions de premiers avertissements ont été expédiés depuis sa création et 333.723 deuxièmes avertissements (lettre recommandée) et 71 dossiers transmis à la justice.
* 75 % des messages partent de machines classiques (ordinateurs de bureau ou portables, smartphones, tablettes), le reste provient d’appareils connectés.
* Dans 33% des cas, l’introduction d’un malware est réalisée au travers d’une application mobile.
* 58% des entreprises pointent l’inefficacité des antivirus du marché pour lutter contre les malwares.
* 56% des PC sont infectés via des emails de type « phishing ».
* 40% des infections par Malware sont dues aux sites pornographiques.
* Plus de 30% de nos ordinateurs personnels stockent des fichiers illicites à notre insu. .
* 61% des sites malveillants sont en fait des sites institutionnels.
* 1 site Internet sur 500 est infecté par de malwares
* Google bloque 10000 sites Internet par jour
* 400 Millions de personnes sont concernées par des cyberattaques chaque année

Liens vers des organismes luttant contre les crimes :

* <https://fr.norton.com/cybercrime-definition>
* <http://www.kaspersky.fr/internet-security>
* <https://www.avast.com//fr-fr/index>
* <http://www.bullguard.com/fr>
* <http://www.mcafee.com/cf/index.html>
* <https://www.avira.com/fr/index>