Cyberdélinquants

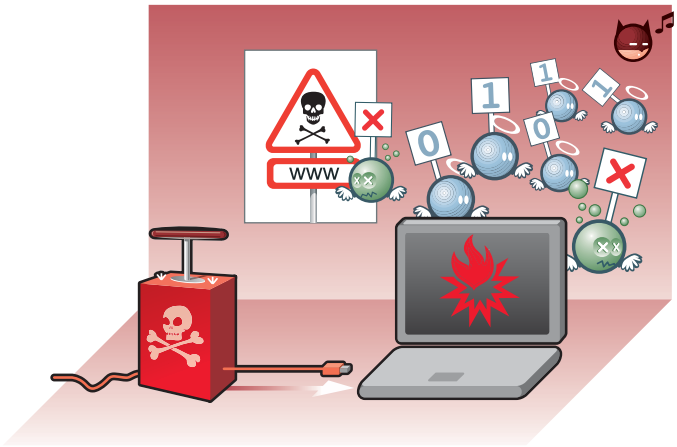
CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Les actes de piratage informatique, au cœur des réseaux d'information et de la communication, sont l'œuvre d'acteurs sociaux qu'il convient de connaître et de comprendre, notamment afin d'appréhender correctement les différents aspects de ce type de menaces. Il est commun de dénommer ces acteurs : « cyber-délinquants ».

Ces derniers se caractérisent par des capacités techniques et des motivations diverses, tout en provenant d'horizons sociaux multiples. Afin d'en faciliter la compréhension, il est d'usage commun de procéder à leur classification. Ainsi, sont principalement catégorisés, au cœur de la cyber-délinquance, trois groupes d'acteurs majeurs, à savoir les hackers, les crackers et les script-kiddies.

Table des matières



1 C'est quoi ?

Les cyber-délinquants se définissent, communément, soit comme acteurs, visant à attaquer illégalement un site informatique déterminé, soit comme acteurs menant un délit ou crime conventionnel à l'aide d'un outil informatique. La différence se décline selon l'utilisation faite, par le cyber-délinquant, du médium informatique.

1.1 Attaque de type conventionnel

En effet, soit ce dernier est **utilisé par le délinquant comme outil** d'un délit ou d'un crime conventionnel (escroquerie, menaces, etc.), soit l'ordinateur est la cible même visée par le délinquant (vol, utilisation frauduleuse ou encore destructions de données, etc.) (Voir fiche CASES « Cyber-délinquance »).

REMARQUE :

Pour décrire ces mêmes acteurs sociaux, est souvent également utilisé, et de manière très générale, voire abusive, le terme « cyber-criminels ».

Les actes des cyber-délinquants, utilisant le médium informatique, sont de compréhension aisée puisqu'il s'agit **de délits et de crimes conventionnels** transposés via les réseaux d'information et de communication, généralement afin d'en tirer profit de manière illicite. Souvent, le but est de profiter de la crédulité des personnes victimes pour obtenir des informations confidentielles et les utiliser ensuite à profit, de manière illégale.

Nous trouvons donc dans cette catégorie des cyber-délinquants de type :

- cyber-escrocs (phishers...),
- cyber-fraudeurs (revente illégale de
- CD gravés...),
- cyber-voleurs,
- cyber-abuseurs,
- cyber-déviants
- cyber-pédophiles, etc.

Il s'agit véritablement de l'ensemble des crimes et délits «traditionnels» se transposant via les réseaux numériques d'information et de communication.

Les motivations quant à ces attaques sont essentiellement de type cupides (le but est la recherche d'un gain quel qu'il soit : financier ou encore matériel) ou bien encore immorales, « malsaines » et maladives (pédophilie, réseaux de prostitution, racisme, révisionnisme etc...).

Cyberdélinquants

1.2 Attaque de type technologique

Quant à la seconde catégorie, les acteurs s'attaquant au médium informatique, ces derniers jouissent, depuis l'avènement d'Internet, d'un véritable succès médiatique ouvrant à une véritable catégorisation, qui, en terme de recherche, demeure critiquable, mais qui en terme de compréhension permet d'appréhender les formes possibles de menaces effectives.

Ces personnages principaux, catégorisés au cœur de la cyber-délinquance, se regroupent au sein de trois communautés bien distinctes se composant principalement des hackers, des crackers et des script-kiddies. Si ces différentes communautés ont bien pour point commun l'illégalité reconnue dans laquelle elles agissent, leurs motivations respectives, quant à elles, divergent fortement.

2 Les Hackers

Le terme de hacker est souvent utilisé à mauvais escient par la presse écrite pour couvrir l'ensemble des pirates informatiques. Cet amalgame contribue à propager une image fantasmée et alarmiste des menaces informatiques. Situation fortement paradoxale, quand on sait que les hackers constituent, certainement, la communauté la moins nuisible, au sein de l'univers encore très méconnu de la cyber-délinquance.

En réalité, si tout hacker peut être «étiqueté» en tant que cyber-délinquant, tous les cyber-délinquants ne sont pas des hackers.

Les hackers ou « chapeaux blancs » sont certainement les plus connus, mais aussi les plus incompris des cyber-délinquants. Ils se démarquent des crackers et des script-kiddies par leur sens de l'éthique. Contrairement à ces derniers, ils n'attaquent pas leurs cibles, mais se contentent d'enfreindre la sécurité de leurs systèmes pour en souligner les failles. Il s'agit pour le hacker, à travers des moyens, illicites, il est vrai, de relever un «challenge» technologique tout en agissant pour le bien des organisations attaquées, puisqu'il permet l'amélioration de la sécurité du système d'information concerné.
Hautement qualifiés et compétents, les hackers sont quasiment indétectables. Leurs actions sont motivées par une idéologie commune, à savoir, la conviction que la propriété intellectuelle doit appartenir à tous ceux qui en ont la compréhension et que toute tentative de légiférer en matière de cyber-espace doit être combattue.

La communauté hacker partage une culture commune rassemblant des programmeurs expérimentés, des spécialistes réseaux et des passionnés des technologies de l'information et de la communication, au sens large du terme.

L'histoire de cette communauté date de plusieurs décennies, remontant aux premiers développements du concept d'ordinateur, et aux premières expériences du réseau ARPAnet. Ce sont les propres membres de cette communauté qui se sont dénommés hackers (du verbe to hack, littéralement «taper sur le clavier» avec pour sens la volonté de mieux comprendre, mieux développer, et par extension mieux sécuriser). Ces derniers sont à l'origine du développement d'Internet (le World Wide Web), et ont, entre autre, également permis le développement des systèmes d'exploitation tels que Unix, et récemment Linux.

De cette explication, il convient d'associer ces acteurs sociaux au concept de bâtisseurs plutôt que de destructeurs, dernier terme d'importance qui différencie, respectivement et définitivement, les hackers des crackers.

REMARQUE :

Eric S. Raymond, célèbre auteur de «Jargon File» et de «New hacker's dictionnary», permet de définir très finement la terminologie relative au hacker, avec le respect de l'ensemble de la communauté concernée. Un célèbre article «How to become a hacker» permet de mieux comprendre ce contexte.
Pour aller plus loin : http://www.catb.org/~esr/

3 Les Crackers

Le cracker ou « chapeau noir », souvent confondu avec le hacker, pénètre les systèmes informatiques avec l'intention de nuire. Il peut arriver que le cracker attaque pour des raisons ludiques, mais en général, il essaye de tirer un gain de ses méfaits, comme le fait de nuire à un concurrent, un enrichissement personnel ou l'acquisition de données confidentielles.

Bien souvent, il s'agit de véritables criminels, fonctionnant dans des réseaux mafieux, pour leur propre compte ou le compte d'autrui. Souvent très compétents techniquement, ils peuvent égaler les compétences des hackers, cependant, ils en représentent véritablement le côté sombre, car ne font pas profiter une victime de leur savoir pour le mettre au profit de l'amélioration de la sécurité à mettre en place, bien au contraire, leur but est de maximiser cette connaissance à leur profit.

Cyberdélinquants

Aucune éthique n'est présente dans la réalisation des actes des crackers, au contraire des hackers. Souvent, les piratages relevés par la presse font état des actes de crackers, il s'agit généralement des piratages de serveurs web (transformation de pages), de saturation de sites, de transformations de données, de rebond pour pirater d'autres sites, etc. Mais, chaque action révèle toujours une volonté de nuire vers la victime potentielle.
En terme de cracking, d'autres acteurs sociaux sont catégorisés comme étant particulièrement dangereux : les « enfants du script » ou encore « script kiddies »

4 Les scripts-kiddies

Les scripts-kiddies, quant à eux, forment le bas-de-gamme du piratage informatique. Si les deux communautés précédentes se focalisent sur des cibles spécifiques, les script-kiddies eux, lancent leurs attaques de manière totalement aléatoire en utilisant des listes de commandes groupées dans un script, d'où leur nom.

Ce type d'attaque ne demande pas un très haut niveau de connaissance informatique ; c'est pourquoi le script-kiddy est souvent un adolescent voire parfois un enfant. Ce dernier utilise des logiciels « prêt à l'emploi », ne maîtrisant ni leur fonctionnement, ni les conséquences de l'action illégale entreprise. Son comportement est totalement irresponsable, pouvant atteindre n'importe quelle ressource informatique, y compris les ressources informatiques de la compagnie où travaillent ses parents, par exemple.

5 Conclusions

Dans l'ensemble, ces communautés, composant la cyber-délinquance, ne se mélangent pas. Les hackers portent très peu de considération pour les crackers (véritables pirates informatiques) et inversement. Quant aux script-kiddies, ils font partie d'un monde totalement à part, ne bénéficiant d'aucune considération.

A partir de cet état des lieux des personnages de la cyber-délinquance, la possibilité pour une commune ou une PME de se faire attaquer par un hacker apparaît pratiquement nulle. La véritable communauté hackers, très underground, ne comporterait que quelques centaines de membres au niveau mondial, et n'est attirée que par les sites hautement sécurisés qui représentent un véritable défi technologique.
Si les crackers sont plus nombreux, plusieurs milliers, ces derniers se concentrent généralement sur les grandes compagnies, n'ayant aucun intérêt à viser une cible de moindre importance. Cependant, cette menace générique n'est pas nulle.

En fait, la masse nuisible, qu'une petite organisation ou que le citoyen est susceptible de rencontrer très régulièrement, car ils se comptent par centaines de milliers et attaquent de manière complètement aléatoire, est constituée par les script-kiddies.
Cependant, leurs attaques étant courantes et connues, il est relativement facile de les prévenir. Cela, en appliquant les patchs de sécurité relatifs aux systèmes d'exploitation utilisés, en surveillant les accès aux réseaux et en mettant en place un plan de réponse sur incidents. En quelque sorte, le respect du minimum requis en terme de sécurité des systèmes d'information et de la communication.
Ainsi organisée, la sécurité offre une garantie non négligeable de maîtrise organisationnelle, face à ces attaques potentielles connues.

CASES,
pour plus de sécurité dans l'utilisation des systèmes d'information électroniques.
Une initiative européenne soutenue par l'Etat luxembourgeois

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie et du Commerce extérieur