CyberDélinquance

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

Internet, « toile d'araignée mondiale », a ouvert des perspectives nouvelles aux citoyens et aux entreprises, cependant cet objet d'innovation technologique a également conduit à l'émergence d'une nouvelle forme de délinquance, communément qualifiée de « cyber-délinquance ». En effet, du fait de leur inter-connexion croissante, les systèmes et réseaux d'information sont désormais exposés à un nombre exponentiel et à un éventail plus large d'agents menaçants, toujours avides d'exploiter, à profit, les failles disponibles...

Table des matières

1 C'est quoi ?

La cyber-délinquance se définit, communément, comme toute action illicite, visant l'intégrité d'un site informatique déterminé, ou bien menée à l'aide d'un outil informatique. Cette définition se décline selon l'utilisation faite du médium informatique. 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)

REMARQUE :

Pour décrire ce même phénomène est également utilisé le terme « cyber-criminalité », voire « crime numérique » ou encore « crime binaire ». Afin de ne pas paraître restrictif nous choisirons le terme de « cyber-délinquance » plus global et aussi celui de « pirate informatique » pour tout acteur social attaquant une machine de manière illégale.

2 Qui est concerné ?

Tous les citoyens, PME et administrations, connectés, via leur ordinateur sur Internet, peuvent être victimes d'un, voire de plusieurs cas de piratages informatiques. Les caractéristiques peuvent être variées et correspondre soit à un délit, soit à un crime conventionnel, en utilisant l'ordinateur comme relais, ou bien en prenant véritablement l'ordinateur pour cible. Le simple fait de connecter sa machine à Internet suffit pour ouvrir une porte d'accès potentielle à toutes ces menaces. Actuellement, les statistiques établissent un court délai d'environ quinze minutes de connexion, avant de subir au moins une tentative de connexion illicite (de type scan) ou tout du moins non sollicitée.

suite au verso

CyberDélinquance

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

3 Comment cela fonctionne-t-il ?

3.1 Attaque de type «conventionnel»

Ce type d'attaques utilise les réseaux d'information et de communication en tant que support, il s'agit de profiter de ce type d'innovation technologique pour 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 de manière illégale. Il existe toute sorte d'infractions classées dans cette catégorie, et ce type de menaces demeure en augmentation constante, nous pouvons notamment citer :

- Les extorsions de fond
- La fraude à la carte de crédit
- Les menaces répréhensibles diverses, de type «vengeance»
- La fraude commerciale
- Les abus de confiance et escroqueries diverses
- Les détournements de mineurs...etc

STATISTIQUES :

Une étude récente (McAfee Edition – début 2005) montre que les « crimes » en ligne couvrent toute la planète et sont en constante augmentation. En Allemagne, les crimes et délits informatiques enregistrés sont passés de 15 000 en 1993 à 60 000 en 2003. Les 7 053 cas recensés en Russie en 2003 sont passés à près de 5 000 rien que sur le premier semestre 2004. Enfin, selon l'Anti-Phishing Working Group (APWG), 1 518 nouvelles attaques par phishing ont été enregistrées en novembre 2004, contre 176 seulement en janvier. Le nombre de cas devrait doubler chaque mois au cours de l'année 2005.

EXEMPLE :

C'est le cas des escroqueries dite « à la nigérienne ». Il s'agit d'un mail proposant de manière urgente le dépôt d'une somme importante sur votre compte bancaire moyennant une rétribution non négligeable « pour service rendu » ! Le but est, bien entendu, de récupérer vos données bancaires pour un usage illégal. C'est le cas aussi des diverses tentatives maquillées d'obtention de données bancaires, via la technique dénommée « phishing » (voir le dossier CASES consacré à ces techniques).

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 cupide (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).

3.2 Attaque de type «technologiques»

Ce type d'attaques apparaît non négligeable en regard de leur évolution. Elles concernent essentiellement celles qui visent l'intégrité du médium informatique. A ce titre, elles sont nombreuses et corrélatives au nombre des vulnérabilités à exploiter.

Elles se déclinent, principalement, ainsi :

- Usurpation d'adresses I.P.
- Dépôt de programmes espions
- Dépôt de programmes pirates
- Intrusions
- Détériorations diverses
- Destruction de sites
- Vol d'informations
- Saturations de sites
- Rebond à partir de sites informatiques victimes...etc

Les motivations diffèrent quant à l'attaque numérique du médium, elles peuvent-être :

- Stratégiques (visant des informations sensibles classifiées)
- Idéologiques (transformations de pensées prédominantes ou de courant d'idées en actes illicites)
- Terroristes (toute action visant à destabiliser l'ordre établi)
- Cupide (le but est la recherche d'un gain quel qu'il soit, financier ou encore matériel)
- Ludique (agissements par amusement ou loisir)
- Vengeur (réaction à une frustration quelconque)

Souvent plusieurs de ces motivations peuvent être combinées lors d'une attaque de ce type. Elles visent soit la confidentialité, l'intégrité ou encore la disponibilité d'un système informatique (voire une combinaison des trois).

suite au verso

CyberDélinquance

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

Le pirate informatique use généralement de procédures diverses pour attaquer une ressource visée. Les pratiques les plus souvent rencontrées sont les suivantes :

La prise d'empreintes

Généralement avant d'attaquer une cible particulière, le pirate procède à un relevé de toute information pouvant mener à une cartographie (photographie détaillée) de l'organisation ou de l'individu qu'il vise.

Le balayage systématique de réseau

Correspond à la recherche d'informations au sens large (image consistant à « clencher » chaque porte pour déterminer celles qui peuvent s'ouvrir). Les pirates testent des systèmes cibles pour vérifier s'ils sont actifs, et déterminer quels ports de communications peuvent être en veille.

Le recensement

Après la prise d'empreinte et le balayage de réseau, le pirate va ensuite chercher à identifier des comptes d'utilisateurs valides ou des ressources partagées mal protégées. Ces opérations sont appelées les opérations de « recensement ». Il s'agit véritablement de la phase précédente à celle active de pénétration et d'intrusions. Généralement, lorsqu'un nom d'utilisateur ou de ressource partagée est recensé, le délai est court avant que l'intrus ne parvienne à deviner le mot de passe correspondant ou à identifier une faille associée au protocole de partage de ressource.

Le fichier "piégé"

Le pirate peut tenter une attaque en envoyant un e-mail piégé, contenant un « cheval de Troie » (voir fiche CASES « Cheval de Troie ») masqué dans un programme de type lambda, qui pourra lui permettre, si le destinataire l'active, de prendre par la suite, à distance, la main sur le micro-ordinateur victime.

Le "social-engineering"

Dans ce cas précis la victime n'est pas confrontée à une manipulation technique mais directement à un pirate qui se fait passer pour une personne identifiée afin d'avoir accès à des informations tel qu'un mot de passe par exemple. Ce scénario est pratique courante ; les pirates agissent souvent par pression psychologique ou invoquent l'urgence pour obtenir rapidement les renseignements sur la victime.

STATISTIQUE :

L'étude 2004 « e-crime watch » du Computer Emergency and Response Team - Coordination Center (CERT-CC - Etats-Unis) a relevé, auprès des organismes ayant répondu à cette enquête, un préjudice total de 666 millions $.

4 Pourquoi se protéger ?

La cyber-délinquance constitue une menace considérable sur Internet, les pertes peuvent être véritablement conséquentes, pouvant entraîner des pertes financières directes, de réputation ou encore de temps, que l'on soit un particulier, une entreprise ou encore une administration. Elle affiche des visages multiples et ne connaît pas de frontières. Ce caractère générique et instable nécessite une nécessaire prise de conscience ainsi que la mise en place des contre-mesures adéquates.

5 Comment se protéger ?

Nécessaire prise de conscience du phénomène et choix de contre-mesures adéquates :

- Penser au phénomène de la cyber-délinquance dès que l'on se connecte, mais surtout dès qu'un élément particulier non prévu survient
- Mettre en place des réflexes de sécurité de base : ne pas ouvrir des e-mails en provenance d'inconnus et ne pas exécuter de pièces-jointes associées, mettre à jour son OS, son anti-virus et son firewall, ne pas surfer sur des sites « trop » underground, se méfier des inconnus...etc
- Effectuer une veille quant aux menaces courantes
- Faire un usage raisonné et adapté d'Internet
- Ne pas faire « trop facilement confiance au premier venu »

Autant de règles simples qui pourront vous permettre de ne pas devenir trop facilement un catalyseur de la « menaçante » cyber-délinquance.