



CASES articles

Ce que les usagers d'internet doivent savoir sur les pirates

Révélation sur le mythe du pirate internet

Pour plus de sécurité, adoptez les réflexes CASES !

Comprendre les mécanismes de la cybercriminalité permet d'adopter les réflexes de protection nécessaires

L'Internet est devenu indispensable, tant pour notre vie quotidienne que pour le monde du travail. Cette technologie, avec tous ses avantages, a toutefois contribué à l'émergence de nouvelles formes de criminalité. Dévoiler certains aspects du mythe du « pirate Internet » permet aux utilisateurs de mieux appréhender les risques liés à la cybercriminalité et de colmater les failles de sécurité potentielles.

Aujourd'hui, en Europe, plus de la moitié des services publics sont accessibles en ligne. Un citoyen de l'UE sur deux utilise régulièrement l'Internet. Un quart de la croissance économique mondiale peut être attribué aux technologies de l'information et de la communication. Ces chiffres démontrent bien à quel point Internet, et les technologies qui l'accompagnent, sont devenus indispensables.

L'interconnexion de plus de 600 millions d'ordinateurs, ce qui correspond à environ 1 milliard d'utilisateurs, a toutefois contribué à l'émergence d'une nouvelle forme de criminalité – la cybercriminalité. L'augmentation constante du nombre d'applications possibles sur Internet s'accompagne malheureusement d'une augmentation non moins importante de l'activité criminelle sur ce réseau. La société de sécurité informatique McAfee estime que les attaques dirigées contre les applications permettant de téléphoner via l'Internet devraient augmenter d'environ 50 % au cours de l'année 2008. Pour 2008, la société part également du principe que le nombre de menaces dans le monde virtuel aura dépassé celui des menaces dans le monde réel. Selon



des indications de l'Institut de sécurité SANS, la popularité croissante des réseaux sociaux sur Internet, tels que Facebook et Hi5, facilitera les opérations d'espionnage et contribuera donc à leur augmentation.

Ces données et estimations suscitent certaines questions : Qu'est-ce que la cybercriminalité ? Qui sont les personnes dans l'ombre ? Quels sont les mobiles de cette activité criminelle ? Répondre à ces questions permet à un usager d'Internet de mieux appréhender les risques découlant de l'activité des pirates. La compréhension des réflexes de protection à employer s'en trouve améliorée. Cela permet en outre de mettre un visage sur ce « pirate Internet ». Ceci contribue de plus à la prise de conscience nécessaire collective, que ces crimes ne sont ni des délits mineurs, ni des exploits, ni des attractions médiatiques. Il s'agit bien de délits à part entière, qui vont à l'encontre des ré-

gles et des normes de notre société et qui, en tant que tels, doivent être punis.

Titre intermédiaire : Qu'est-ce que la cybercriminalité ?

Le terme de cybercriminalité regroupe tous les délits pour lesquels un ordinateur ou tout autre système d'information et de communication est utilisé en tant qu'outil ou constitue l'objet d'actes criminels.

Lorsque les technologies concernées sont utilisées en tant qu'outils procurant un avantage de manière illicite, l'on parle également d'attaques traditionnelles. L'objectif du criminel est souvent d'exploiter la crédulité de ses victimes, par exemple par le biais de courriers électroniques ou d'une fausse page Internet. Parmi les délits associés à ce genre d'attaque figurent par exemple l'enrichissement illicite,

la fraude à la carte de crédit, l'abus de confiance, le détournement de mineurs ou encore l'escroquerie. Il s'agit là de délits et de crimes conventionnels qui ont été transposés aux réseaux numériques d'information et de communication. Les motivations de ces attaques peuvent être la cupidité, la pédophilie, la prostitution, le racisme ou le révisionnisme.

Les délits au cours desquels des ordinateurs ou des réseaux d'information et de communication font l'objet d'actes criminels sont multiples. Peuvent ainsi, entre autres, être cités : l'installation clandestine de logiciels d'espionnage, l'accès illicite à des pages web ou la défiguration de celles-ci, le vol de données, la propagation de malwares ou encore l'usurpation d'identité. Les motivations de ces attaques sont souvent liées à la cupidité, à des raisons idéologiques, à des actes de vengeance ou terroristes ou simplement à un défi, voire à une combinaison de ceux-ci. Ces attaques visent principalement la disponibilité des systèmes d'information et de communication ainsi que leur confidentialité et leur exactitude.

Titre intermédiaire : **Les modes opératoires des cybercriminels**

Collecte d'informations

Avant d'effectuer une attaque, le cybercriminel recueille toutes les informations disponibles sur sa victime, que ce soit une entreprise ou un particulier. Les utilisateurs et les entreprises divulguent souvent un nombre important d'informations lors de leur utilisation d'Internet. Ils ne sont alors pas conscients de la valeur de ces informations et ignorent qu'elles peuvent être exploitées à des fins criminelles par des tiers. Les sociétés et les usagers d'Internet, persuadés que leurs informations ne sont que difficilement repérables dans la masse des données et applications circulant sur la toile sont dans l'erreur. Des moteurs de recherche permettent à des tiers, au bout de quelques secondes ou minutes de recherche, de découvrir de précieuses informations sur un utilisateur déterminé ou sur une société précise.

Scannage des réseaux

Les pirates sondent les systèmes qu'ils souhaitent attaquer afin de détecter les points faibles les plus courants.

État des lieux

Après la collecte d'informations et la détection des points faibles, le pirate tente d'identifier les comptes d'utilisateur ou les ressources utilisées en commun ou mal protégées. S'il parvient à déterminer un nom d'utilisateur ou une ressource, plus rien ne s'oppose à l'accès illicite au système. Le délai entre la détermination d'un nom d'utilisateur et la découverte du mot de passe correspondant est généralement très court. Même chose pour la détection d'une ressource et l'identification de ses points faibles.

Outils d'espionnage

Une fois la collecte d'informations sur une victime terminée, par exemple le collaborateur administratif X ou la secrétaire Y d'une entreprise, les pirates tentent de placer un logiciel d'espionnage, leur but étant de glaner un maximum d'informations sur la société. Pour ce faire, ils envoient par exemple des e-mails dissimulant des chevaux de Troie à une personne spécifique. Les informations qu'ils ont pu obtenir au préalable sur cette personne leur permettent de rédiger ce courrier électronique de façon à susciter l'intérêt du destinataire et ainsi à s'assurer qu'il sera bien ouvert. Si la victime active le malware en ouvrant l'e-mail ou en cliquant sur les pièces jointes, les pirates obtiennent fréquemment le contrôle de son ordinateur. Les pirates sont alors en mesure d'espionner l'entreprise. La collecte ciblée de données personnelles est souvent très aisée. Elle est de plus facilitée par les nombreuses utilisations des réseaux sociaux sur Internet, tels que Facebook. Nombreuses sont les personnes qui divulguent des informations d'ordre privé sur ces réseaux, sans être conscientes des risques potentiels.

L'ingénierie sociale ou « social engineering »

Dans ce cas, les pirates n'ont pas recours à leurs aptitudes techniques, mais utilisent des moyens beaucoup plus subtils : par exemple la pression psychologique ou encore l'exploitation du besoin d'autoreprésentation d'autrui. La victime est alors souvent directement confrontée au cybercriminel. Les pirates obtiennent ainsi, lors d'échanges directs avec la victime, des mots de passe ou d'autres informations importantes. Pour parvenir à ses fins, le pirate peut par exemple se faire passer pour un membre du service informatique de la société. Il contacte alors un collaborateur de cette même société et prétend que certains droits d'accès de cette personne doivent être actualisés et que l'accès à l'application ne serait plus possible sans cette actualisation. Afin de procéder à cette actualisation, le pirate prétend ensuite avoir besoin du mot de passe de la personne.

Titre intermédiaire : **Types de cybercriminels**

Les individus évoluant dans le monde de la cybercriminalité peuvent être classés dans trois catégories distinctes : les *hackers*, les *crackers* et les *script kiddies*.

Les *hackers* sont les cyberdélinquants les plus connus. Ils sont toutefois fréquemment méconnus, car le terme de « hacker » est souvent assimilé à tort aux *crackers* et *script kiddies*. Les *hackers* se distinguent fondamentalement des *crackers* et *script kiddies* de par leurs motivations et leur sens moral. Contrairement aux deux autres groupes, les *hackers* ne poursuivent pas des objectifs dictés par la cupidité, des raisons idéologiques, une rage destructrice, des pulsions malades, ou par simple jeu. Les *hackers* se contentent d'utiliser des moyens illégaux pour franchir les dispositifs de sécurité des systèmes visés afin de dévoiler leurs points faibles. Ils se perçoivent comme au service bienveillant des entreprises, organisations ou personnes visées car leurs attaques permettent d'améliorer la sécurité des systèmes concernés. La communauté des *hackers* regroupe des programmeurs expérimentés, des

spécialistes réseaux ainsi que des passionnés des technologies de l'information et de la communication. Cette communauté partage l'idéologie que la propriété intellectuelle devrait appartenir à tout le monde et son histoire remonte au développement des tout premiers ordinateurs. La communauté de hackers opérant dans la clandestinité est toutefois peu importante. Ses actions sont principalement axées sur l'intrusion dans des systèmes hautement sécurisés. Il est donc peu probable que les particuliers, les administrations ou les petites et moyennes entreprises deviennent la cible de leurs attaques et subissent des préjudices.

Les *crackers* représentent un groupe de criminels à part entière. Cette communauté est souvent organisée en réseaux et groupes similaires aux structures de la mafia. Les crackers possèdent d'excellentes connaissances techniques et travaillent pour leur propre compte ou au profit de tiers. Le but de leurs attaques est de se procurer des avantages personnels : l'objectif est de s'enrichir en faisant subir un préjudice à la victime. Contrairement aux hackers, ces individus n'ont aucun sens éthique et leur communauté comprend de nombreux membres. La majorité des cas de cybercriminalité rapportés par les médias sont à imputer aux crackers. Ces derniers représentent une menace réelle et très importante pour les particuliers, les organisations et les entreprises.

Les *script kiddies* représentent la couche inférieure de la cybercriminalité. Ils ne disposent pas de connaissances techniques très importantes. Il s'agit le plus souvent d'adolescents, voire même d'enfants, qui utilisent des listes de codes – les « scripts » – mises à disposition sur Internet par des crackers.

Les script kiddies ne connaissent pas le mode de fonctionnement de ces malwares prêts à l'emploi. Ils ne sont pas non plus pleinement conscients des effets de leurs actions illégales. Leurs actes sont irresponsables et peuvent toucher n'importe qui. Ce groupe, de par la multitude de ses membres, occasionne un grand nombre de préjudices. Ce sont principalement les particuliers et les petites entreprises disposant de moyens de protections insuffisants qui en font les frais.

Les méthodes sont toutefois généralement connues et de simples mesures de protection sont souvent suffisantes pour les déjouer. Ainsi, les e-mails d'origine inconnue ne devraient ainsi pas être ouverts et leurs fichiers joints ne devraient pas être exécutés. Les systèmes d'exploitation, logiciels antivirus et autres programmes devraient être mis à jour régulièrement. Le pare-feu doit être correctement configuré. L'analyse des systèmes par un programme anti-spyware devrait être effectuée régulièrement.

Conseil de sécurité :

Afin d'éviter de devenir victime d'actes de cybercriminalité ou de les favoriser, il convient d'appliquer certains réflexes de sécurité. Lors de l'utilisation des technologies de l'information et de la communication, l'on devrait toujours garder en mémoire le risque que constitue la cybercriminalité, que l'on soit un particulier, une entreprise ou une organisation. Une bonne dose de vigilance et de méfiance est vraiment recommandée. Les considérations relatives à la sécurité devraient être intégrées aux nouveaux systèmes et applications dès leur conception. Certains systèmes et applications devraient être soumis à une évaluation du risque. Ainsi, d'éventuelles vulnérabilités et leurs dommages potentiels peuvent être détectés et quantifiés. Ceci rend en outre possible la mise en œuvre de mesures ciblées visant à éviter les vulnérabilités ou à y remédier. Les informations privées devraient toujours être traitées avec la plus grande prudence. Celles-ci peuvent en effet se révéler très utiles pour des tiers et de nombreux utilisateurs n'en sont cependant pas conscients. La sensibilité des informations transmises sur des sites tels que Facebook devrait être vérifiée très attentivement avant leur publication. Les utilisateurs qui le souhaitent peuvent vérifier leurs réglages de sécurité sur Facebook grâce au lien : <http://www.cases.public.lu/fr/pratique/solutions> ; ceci leur permettra d'éviter la divulgation non souhaitée de données sensibles.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu