info·SIRCO
ENQUÊTE ET PROTECTION

Largest coordinated international law enforcement action FBI

VOL DE RENSEIGNEMENTS PERSONNELS : LE CRIME DU FRAUDEUR,

ET DE LA COMPAGNIE QUI LES AVAIENT MAL PROTÉGÉS...

UNE PREMIÈRE DANS L'HISTOIRE AMÉRICAINE

Cela ne s'était jamais produit auparavant. Pour la première fois dans l'histoire américaine, la FTC a pour la première fois accusé une entreprise de ne pas avoir assuré assez de sécurité dans leurs système concernant les informations personnelles et bancaires de leurs clients.

En effet, Whyndam Worldwide, une grande chaine hôtelière américaine, a vu son système informatique piraté en 2008 et 2009. Ces attaques totalisent plus de 619 000 comptes bancaires compromis, les pirates informatiques s'étant introduits directement dans le système informatique de quelques hôtels de la chaine pour s'emparer des informations confidentielles ainsi que des numéros de cartes des différents clients.

Ce qui diffère des antécédents en matière de crime informatique, c'est la responsabilité des différents intervenants du dossier. L'entreprise fraudé a maintenant une responsabilité dans le vol des numéros de cartes de crédit et des informations personnelles de leurs clients.

Bien sur, cela créer un précédent. C'est-à-dire que si l'entité chargée de l'enquête sur le vol considère qu'avec des mesures plus sécuritaires et accessibles le détenteur des informations aurait pu assurer une meilleure qualité au niveau de la protection et de la sécurité, il est tenu coupable d'un manquement, et pourrait même être accusé de grave manquement menant à la fraude. Cela change évidement les risques en jeu dans le domaine du crime informatique, autant pour le fraudeur, que pour les victimes...

La menace des pirates informatiques ne cesse de s'accroitre, et la génération de la technologie ne tardera bien longtemps à alimenter la communauté criminelle invisible du net.

OPÉRATION «CARD SHOP»

Le FBI à récemment mis en état d'arrestation 24 pirates informatiques de renommée âgés entre 18 et 25 ans et provenants de 9 pays différents. Cette opération fut qualifiée, par le *American Law Enforcement* de «*largest coordinated international law enforcement action*» de l'histoire.

Ceux-ci, lors de l'arrestation, pouvaient déjà compter plus de 400 000 victimes à leur conteur. Leurs actes étaient majoritairement de nature monétaire, c'est-à-dire qu'ils cherchaient les numéros de cartes de crédit et les dossiers d'informations personnelles des victimes puis revendaient le tout. Le FBI estime le total des pertes des victimes à 200 millions de dollars.

Les pirates informatiques, et comment les piéger

CRIMES ET VIOLATION DE L'IDENTITÉ PRIVÉ

Jarand Moen Romtveit, un des pirates arrêté, à commis plusieurs méfaits. Il a lui même développer un programme qui, à ses dires, pouvaient décrypter des bases de données, ce qui lui était utile pour pirater les sites, par exemple, des banques.

Romtveit utilisait plusieurs techniques pour commettre ses crimes. Mis à part les milliers de numéros de cartes de crédit et d'informations personnelles vendues et volées, ce pirate agissait également à d'autres niveaux. Il avait, entre autres, offert des virus et des programmes à ses collègues fraudeurs qui permettaient au cyber-voyeurs de prendre le contrôle des caméras intégrées aux ordinateurs visés et de, littéralement, regarder la personne à qui l'ordinateur appartient sans que celle-ci en ait le moindre doute. Pourtant, aussi dérangeant soit cette information, ce n'est que la pointe de l'iceberg. En effet, la technologie de contrôle de matériel informatique à distance n'en est qu'à ses débuts.

24 arrestations
âgés entre 18 et 25 ans
9 pays différents

Pourquoi les cyber-criminels se sentent-ils invincibles?

Prise de conscience

Le fait d'agir dans un lieu clos, souvent loin de l'endroit où le crime à un impact, et devant un écran d'ordinateur que l'on peut fermer à tout instant, procure au criminel une fausse sensation d'invincibilité. Cela a pour impact de faire paraitre le crime moins grave, et la personne perd souvent sa notion morale de la chose. Elle à tendance à minimiser l'impact de ses actions, étant donné que les résultats réels sur les victimes lui sont inconnus.

Sensibilisation

Lorsque l'on fait affaire à la cybercriminalité, il est très difficile d'établir des mesures de prévention à toute épreuve, la meilleure solution reste souvent de réagir le plus rapidement lorsqu'on prend conscience qu'un crime est commis. En ce sens, à l'instar du meurtre ou de tout autre crime sur la personne, comme le vol direct, le cybercrime peut être fait à partir d'un endroit sur la planète et toucher des victimes à l'autre bout du monde. Par conséquent, même si une quelconque prévention est faite, il est difficile de savoir auprès de qui elle serait réellement efficace. D'autant plus que les cybercriminels sont souvent au dessus de tout soupçons.

COMMENT L'AGENT D'INFILTRATION PIÉGEA ROMTVEIT

L'agent spécial d'infiltration du FBI, John Leo Jr., qui enquêtait sur Jarand Moen Romtveit, fut témoin des nombreuses actions posées par ce dernier.

L'enquêteur pris connaissance de l'existence du pirate le 12 septembre 2010, alors que ce dernier s'inscrit sur le faux site de vente et d'échange de numéros de cartes de crédits volés que le FBI avait conçu dans le but de piéger les fraudeurs.

Leo se présenta à Romtveit comme l'administrateur du site. Le 9 février 2012, le pirate partagea son écran avec Leo pour lui présenter un programme qu'il disait avoir développé pour décrypter les bases de données. À ce moment, Leo pu voir de multiples fenêtres ouvertes sur l'écran de Romtveit, dont une où son nom complet apparaissait. À la suite de la démonstration dudit programme ainsi que d'un bref échange par messages, Romtveit fourni à Leo un lien vers sa page Facebook. De fil en aiguille, sur une période de plusieurs années, de fréquents échanges entre le fraudeur et l'agent d'infiltration menèrent à l'arrestation du criminel.

Ironiquement, cet homme qui était accusé d'avoir exploité les faiblesses d'utilisateurs sur le net et des informations confidentielles et personnelles de ses victimes pour faire un profit dans le cybercrime, a lui même fourni à un agent du FBI toutes les informations nécessaires à son arrestation.

« Le fait d'agir dans un lieu clos, souvent loin de l'endroit où le crime à un impact, et devant un écran d'ordinateur que l'on peut fermer à tout instant, procure au criminel une fausse sensation d'invincibilité.

De nouvelles percées en informatique, toutes plus surprenantes les unes que les autres, donne un accès quasi-illimité à nos vies aux différents criminels qui rodent sur la toile.