Plongée dans le monde des cybercriminels

Tout d'abord un aperçu. Un regard sur la scène. Les menaces et fraudes sur Internet augmentent, non seulement en termes de chiffres mais aussi par leur sophistication, et les profits de la cybercriminalité sont encore en train de transformer la nature de ce « jeu » dangereux. En 2013, le **phishing numérique** seul – soit l'équivalent d'un pickpocket qui vole votre portefeuille – a représenté **5,9 milliards de dollars de pertes** pour les grandes entreprises. Autre chiffre : trois fuites de données sur quatre sont liées à des questions financières ou de fraude. La vérité est que les cybercriminels sont plus organisés et qu'ils continuent à développer des solutions de 'fraude-as-a-service', où les attaques sont disponibles sous forme de services prêts à l'emploi. Ce qui met à disposition d'une large base d'utilisateurs certaines des fraudes et menaces les plus innovantes et avancées.

« Pickpockets » numériques

Appelons les « pickpockets » numériques. Le soi-disant « hameçonnage » numérique, ou phishing. Le premier marché pour ce type de cybercriminalité est l'Amérique du Nord, à savoir États-Unis et Canada. Suivi par le Royaume-Uni. Ce marché, en plus de son organisation, est **un marché saisonnier**. En novembre, les attaques augmentent ; l'activité diminue à partir de décembre, au moment de Noël. Il y a une explication très simple à ce phénomène étrange : une fois les données volées… les criminels doivent aller faire du shopping ! Selon Daniel Cohen, un des responsables de cette question chez RSA (la division sécurité d'EMC), les attaques augmentent de nouveau en avril, saison du paiement des taxes aux États-Unis et, bien évidemment, en août, pour les vacances.

La complexité de ce marché ne fait que s'accroître. Ainsi, les pirates, les cybercriminels qui volent des données, ne savent la plupart du temps pas quoi faire desdites données, et les vendent à des experts qui savent comment les utiliser et les transformer en argent réel. « *Il faut savoir comment faire des emplettes dans le monde numérique sans laisser de traces* », explique Daniel Cohen. En effet, ce marché est si organisé qu'il existe des 'places de marché' undeground où on peut trouver des données de cartes de crédit. Avec des garanties. Si la carte de crédit a expiré ou a été annulée par l'utilisateur, la place de marché va rembourser l'acheteur ou remplacer la carte inutilisable.

Ces sites ont même des **centres d'appels pour aider les escrocs** utilisant de cartes frauduleuses à appeler la banque du possesseur légal de la carte, afin de changer d'adresse par exemple. Imaginez que vous achetiez une carte dans ce monde souterrain et que vous vouliez modifier l'adresse qui y est associée. Évidemment, la banque se montrerait suspicieuse si la carte était émise au Texas par exemple, et que votre accent semblait plutôt correspondre à la Caroline du Nord. Ou à l'Angleterre. Un des services offerts par les magasins du crime online est précisément de mettre à disposition des hommes et femmes avec des accents différents afin d'appeler – et de tromper – les banques. Et ceci n'est qu'un exemple des services fournis…

MUSD contre monnaie réelle

Ce monde souterrain a aussi ses propres monnaies. Que l'on parle de « PerfectMoney », « Less Pay », « Bitcoin » ou du « MUSD », l'une des monnaies les plus récentes créées dans ce monde souterrain. **Les célèbres Bitcoins n'offrent pas le niveau d'anonymat** que ce type d'opération nécessite. Le MUSD, créé en novembre 2013, est très employé par la pègre russe et ukrainienne. On peut lire par exemple des publicités affirmant : « le bureau à Kiev échange des MUSD contre de la monnaie réelle ». « *C'est un marché si mature qu'il a déjà sa propre monnaie. Et ses propres règles. C'est un marché orienté vers le client, et axé sur le service, comme n'importe quel autre marché* ».

Mais comment sont volées nos données ? De bien des façons, à savoir par le biais de Chevaux de Troie. Un petit programme, un virus associé, habituellement utilisé pour obtenir des informations ou réaliser des instructions sur un ordinateur spécifique. Un dispositif qu'on retrouve dans les fichiers musicaux, les messages électroniques, caché dans les téléchargements ou sur les sites Web malveillants, et qui tire souvent parti des vulnérabilités des navigateurs afin d'être installé sur l'ordinateur ciblé sans être remarqué.

Et depuis leur naissance aux débuts d'Internet, on peut positionner les Chevaux de Troie sur une ligne chronologique. Il y a ceux qui sont pleinement opérationnels, tels que Zeus, SpyZeus, IceIX, Citadelle ou GoZ et ceux appartenant au groupe 'Mutant Ninja Chevaux de Troie', comme Daniel Cohen les appelle. Parce qu'ils sont encore dans une période d'adolescence et sont souvent encore incapables de voler de l'information.

Imparable ingénierie sociale

De toute évidence, la mobilité, et surtout **le système Android**, a ouvert de nouvelles perspectives aux criminels. Et pas besoin de malware. Une ingénierie sociale sophistiqué suffit, exposant les utilisateurs et créant d'énormes failles dans les systèmes. « *L'ingénierie sociale utilisée passe souvent par des apps comportant des zones de texte renfermant de nombreuses informations comme : l'application doit avoir la permission d'accéder à Internet, envoyer des messages, etc. Personne ne lit le message complet et l'utilisateur appuie simplement sur OK parce qu'il veut installer l'application sur l'ordinateur. Ce n'est pas vraiment un malware, le procédé reposant sur le consentement de l'utilisateur* ».

Il y a aussi l'approche « classique » : une alerte s'affiche affirmant que nous avons regardé de la pornographie juvénile et que, par conséquent, nous devons payer une amende. « *Ce sont des messages hautement sophistiqués. Par exemple le programme malveillant ouvre une fenêtre avec une vidéo, la caméra étant utilisée pour prendre une photo de l'utilisateur en train de regarder son téléphone mobile. Beaucoup de gens prennent peur et payent l'amende.* »

Mais au nom de qui agit la division d'EMC ? Elle opère dans ce monde souterrain pour le compte de ses clients, notamment de la finance, **s'infiltrant dans cet univers** et essayant de comprendre où les crimes sont commis. RSA travaille aussi à la détection des menaces afin d'aider à la protection des grandes entreprises.

Un monde du crime très codifié

L'activité de RSA est hébergée dans des locaux ressemblant à la salle de lancement d'un engin spatial. Sur le dessus, le management, généralement trois personnes, et à l'étage inférieur des techniciens qui surveillent les attaques. Sur de grands écrans d'affichage électronique où nous pouvons voir la carte du monde, de **petites épingles rouges** apparaissent de manière dynamique, illustrant les endroits où les attaques sont les plus fortes. En-dessous apparaissent les numéros de cartes de crédit volées : trois chiffres, le prénom et le nom des titulaires de cartes de crédit.

Dans cette pièce, le but est de trouver où les programmes malveillants sont hébergés. Souvent les sites qui accueillent ce type de programmes ne savent pas qu'ils sont infectés. Il est nécessaire d'appeler le propriétaire du site, d'expliquer ce qui se passe et de s'assurer de la fermeture du site. « *Parfois, c'est difficile parce que les gens ne savent pas comment faire. La plupart du temps, les sites Web en question sont de petite taille, dans de nombreuses langues différentes, nous avons besoin de traducteurs en soutien pour aider les propriétaires dans cette tâche.* »

Ensuite, nous passons à une autre pièce où tout se passe. Dans cette très petite salle, les experts RSA infiltrent le cybercrime et surveillent qui vend les données volées. Il existe de nombreux forums, sur l'Internet « standard » et dans le « web profond » – le côté obscur de l'Internet, un monde non-accessible pour les utilisateurs normaux d'Internet – où les données sont négociées. Et c'est assez impressionnant, nous pouvons vous l'assurer. Presque comme si nous étions à **une vente aux enchères** de tout autre type de produits. Ces experts, pour s'infiltrer dans ce monde, **« achètent » des cartes volées pour masquer leurs opérations**. « *Évidemment, nous y dépensons très peu d'argent parce que nous ne voulons pas promouvoir ce marché. Mais nos clients mettent à disposition ces fonds pour passer des transactions et garantir notre couverture* ».

Sur les écrans, les couleurs riches font leur apparition, jaune fluo, rose et rouge vif : ce sont les petites annonces. « *J'ai des cartes de crédit à vendre. 25 dollars l'une, avec le numéro de sécurité sociale.* » Les experts expliquent qu'ici, dans ce monde parallèle, la confiance est la chose la plus importante et que les forums ont des niveaux élevés de sécurité. Les utilisateurs doivent payer **8 000, 10 000 parfois 20 000 dollars pour entrer**. « *Et ils ont besoin de références. Par exemple, je ne peux entrer si quatre autres utilisateurs me donnent en référence. Et si mon comportement n'est pas correct et que je suis expulsé du groupe, tous les utilisateurs qui m'ont donné leur référence seront également expulsés* ».

Par Susana Marvão

A lire aussi :
Sécurité : le cybercrime est la deuxième cause de fraude financière en France
Europol prédit une vague de cybercrimes par objets connectés