Le business model du Phishing

Janvier 2008

La genèse de l'attaque

Tout commence quand par naïveté, par manque de méfiance ou de connaissances suffisantes sur ce qui se pratique sur la toile, la future victime révèle ses coordonnées bancaires électroniques à un cyber-criminel qui utilise, pour les obtenir, la ruse et la technique dans le cadre d'un business model éprouvé.

Comment le cyber-criminel peut t'il réussir à faire que la victime lui révèle ses coordonnées bancaires ? Ce ne sont pas les moyens qui manquent, le social-engineering montre ici quelques-unes de ses multiples facettes !

Le Phishing

Le Phishing débute par deux impostures. D'abord la future victime reçoit un e-mail de sa banque qui l'avertit que la situation est critique et qu'il faut agir sans attendre parce que son compte a peut-être fait l'objet d'une agression et peut-être même il a été vidé. Autre variante, le système informatique de la banque a subit un regrettable incident et quelques comptes ont été effacés, aussi, il faut que la future victime se connecte immédiatement sur son compte électronique pour constater les dégâts éventuels la concernant. Bonjour le stress et les poussées d'adrénaline !

Pour ne pas perdre un temps précieux, le e-mail propose justement un hyperlien pour que le client, future victime, se connecte directement sur la page d'entrée de son compte bancaire, juste par un clic de souris. La future victime se retrouve donc sur cette page beaucoup plus rapidement que si elle avait du saisir l'URL de sa page de connexion à partir de la barre d'adresse de son navigateur. Elle fournit alors, dans l'urgence et le stress, les renseignements demandés : login, mot de passe, numéro de compte, numéro de carte de crédit, et pendant qu'on y est, code secret de la carte et tous autres renseignements indispensables. Mais le serveur de la banque s'est déconnecté juste après la saisie des paramètres demandés et avant que l'internaute ait pu arriver sur son compte. Celui-ci refait une tentative directement à partir de son navigateur et constate que, heureusement, tout va bien, son compte ne présente aucun problème. Si ce n'est que la future victime vient de passer au statut de victime potentielle et probable.

Le e-mail, vous l'aviez compris, n'a pas été envoyé par la banque et l'hyperlien dans cet e-mail ne conduisait pas sur le site de la banque mais vers un site appartenant au cyber-criminel, simulant celui de la banque de celui que nous appellerons désormais « la victime ». Le site simulant la banque n'ayant pas lieu d'exister plus longtemps à la même place, personne ne retrouvera de site Web à l'adresse laissée dans les fichiers logs de la victime qui a fournit ainsi au cyber-criminel tous les renseignements lui permettant de rentrer sur son compte bancaire et l'utiliser pour des transferts vers d'autres comptes.

Il existe des kits de Phishing qui aident à réaliser des sites Web parfaitement simulés.

Deux variantes du Phishing

Devant l'ampleur des attaques par Phishing tant par leur nombre que par leur sophistication, les banques ont averti leurs clients que jamais elles ne leur demanderont de cliquer sur un hyperlien pour entrer sur la page de connexion de leur espace bancaire électronique ; aussi l'appât par e-mail ne marche plus aussi bien qu'avant. Alors intervient une attaque plus technique et plus imparable : le Pharming.

Le Pharming

Si les êtres humains comprennent des adresses du genre « www.mabanque.com », dans le monde IP actuel, les machines comprennent plutôt des adresses sur quatre octets, du genre « 192.23.12.4 ». Il existe donc des tables de correspondance qui contentent êtres humains et machines en leur permettant de s'exprimer, les uns et les autres, dans leur langage, en traduisant les adresses « nom de domaine » en adresses IP et inversement. Ces tables de correspondance se trouvent sur votre PC, sur votre routeur, dans les routeurs ou les serveurs de noms de votre entreprise ou dans ceux de votre fournisseur d'accès internet.

En s'attaquant à ces tables de correspondance, souvent via une vulnérabilité du système, le cyber-criminel peut faire correspondre l'adresse « nom de domaine » de votre banque à l'équivalent « 4 octets » de son choix et qui est celui du site simulant votre banque. En entrant la vraie adresse de votre banque sur la barre d'adresse de votre navigateur, vous arrivez à l'insu de votre plein grès sur le site du cyber-criminel qui simule parfaitement celui de votre banque.

Cette attaque dite en « DNS Poisonning » est difficilement identifiable surtout quand on ignore ce qu'est une table de correspondance et que de plus on n'y a pas accès.

Le Vishing

Vous vous méfiez ou êtes allergiques au Web et à l'informatique en général, et pour discuter avec votre banque, vous préférez utiliser votre téléphone portable ? Alors a été conçue une variante du Phishing et du Pharming qui consiste à vous

envoyer un SMS vous alertant de téléphoner d'urgence à un numéro de téléphone vert, suite à un gros problème que vous avez avec votre banque. Le numéro vert est celui d'un centre d'appel qui simule celui de votre banque et qui vous pose les questions initiales que le faux Web vous aurait posées au sujet de vos coordonnées bancaires pour permettre de vous identifier et de cerner, par téléphone, où est le problème. On parle alors d'attaque en Vishing, la voix a remplacé la data mais le résultat est le même : vous avez révélé, au cyber-criminel, vos coordonnées bancaires électroniques.

Dans ce qui suit, quelle que soit la ruse utilisée pour obtenir les coordonnées bancaires de la victime, qu'elle n'aurait jamais du divulguer mais c'est trop tard, le « business model » s'applique.

Les acteurs en présence

Le cyber-criminel qui peut désormais accéder aux comptes bancaires de ses victimes ne va pas, bien évidemment, vider les comptes dont il a maintenant la maîtrise, de tout leur contenu pour remplir le sien. Ce n'est pas ainsi que fonctionne le business model car nous parlons ici des cyber-criminels, qui sont de vraies crapules sans scrupule, pas des naïfs comme le sont les victimes. C'est là qu'apparait un intermédiaire indispensable dans le business model : la mule.

Ainsi commence l'arnaque qui se joue entre trois familles d'acteurs, **les victimes** qui ont un rôle uniquement passif, **le cyber-criminel** qui va bénéficier, en toute impunité, d'un flot continu d'argent difficilement traçable et .. **les mules**, cheville ouvrière, qui par leurs actions intermédiaires permettent au business model de fonctionner si bien.

Les mules sont recrutées par le cyber-criminel ou ses complices parmi une population d'individus qui possèdent un compte en banque, une connexion internet et un peu de temps devant eux pour effectuer un travail bien rémunéré, simple, régulier, sans risque, et qui ne demande de plus aucune compétence particulière. Le recrutement des mules se fait par relations de parrainage, par forums, par sites Web d'offre d'emploi, ou même par des forums de recrutement tout à fait honnêtes par ailleurs. Le boulot proposé fait même l'objet d'un contrat en bonne et due forme, provenant souvent aujourd'hui d'un pays d'Europe de l'Est. La mule a un superviseur qui contrôle son travail. Tous les attributs qu'on peut s'attendre à trouver dans un contrat de travail honnête, à temps partiel et à domicile peuvent être réunis dans le contrat qui lie la mule au cyber-criminel dont la mule n'a pas flairé, ou n'a pas voulu flairer l'état peu recommandable**.**

Le déroulement de l'arnaque

Il est demandé à une mule de lire souvent sa messagerie car elle sera avertie par cet outil que des sommes d'argent vont être créditées régulièrement sur son compte bancaire, dont elle a communiqué les coordonnées électroniques à son « employeur » au moment de la signature du contrat. Chaque fois que son compte est crédité, ici d'une somme de 52,20 euros, là de 43,72 euros, une autre fois de 28,50 euros, jamais de très grosses sommes mais les transferts sont fréquents, la mule doit se rendre à sa banque et tirer l'équivalent de la somme en liquide. Elle peut garder pour elle, c'est écrit sur son contrat, 8% de la somme, au titre de sa commission.

Elle envoie le reste par **mandat international**, les frais de poste sont remboursés, vers une certaine adresse à garder secrète, sous forme de mandats qui ne laissent pas de traces, de mandats internationaux parce que si la mule réside en général dans la même région que sa victime, le cyber-criminel lui réside ailleurs, le plus souvent loin des mules et de ses victimes, dans un pays où la législation est peu contraignante concernant les transferts de fonds.

La pompe à billets étant amorcée, de partout arrivent vers le cyber-criminel, ou ses intermédiaires, des mandats et les petits ruisseaux finissent par former de grandes rivières, voire même des océans.

Oui mais si une mule garde tout l'argent qui arrive sur son compte ?

Alors le cyber criminel déclare que cette mule n'honore pas « honnêtement » son contrat sur un forum très lu par la société des cyber-criminels. Dès lors la mule n'a plus aucune chance de continuer à bénéficier de ces opérations lucratives et régulières (8% de l'argent versé sur son compte qui lui revient). Alors pourquoi la mule se compromettrait pour garder quelques dizaines d'euros alors que bon an, mal an, l'argent devrait tomber régulièrement avec les 8% des sommes en transit qu'elle conserve ? De plus, souvenez-vous, le cyber-criminel possède les coordonnées bancaires de ses mules qui peuvent bien se retrouver victimes d'un vidage électronique total de leur compte bancaire !

Mais la victime ne s'aperçoit-elle pas que des sommes sont tirées de son compte pour alimenter des comptes qu'elle ne connaît pas ? Oui parfois, alors elle s'en étonne auprès de son banquier mais les transactions sont régulières, la victime est bien la seule personne à pouvoir accéder à son compte ? puisqu'elle est la seule à connaître son

mot de passe et ses coordonnées bancaires ! Elle n'aurait pas été naïve au point de les communiquer à des tiers ?

Celui qui peut s'apercevoir à la longue que quelque chose ne tourne pas rond, c'est le banquier de la mule. Celle-ci peut être en peine d'expliquer l'origine des petites sommes qui arrivent régulièrement sur son compte, et qui précédent systématiquement des demandes de liquidités.

Quand le banquier réagit, la mule est frappée d'interdit bancaire, mais pour le cyber-criminel, qui ne fait ni dans la dentelle, ni dans les sentiments, quelle importance ? une mule de perdue, dix de retrouvées … Oui le métier de mule est éphémère, c'est là son moindre défaut.

Finalement de très nombreuses petites sommes d'argent transitent régulièrement par l'Internet, depuis les comptes des victimes dont le cyber-criminel, ou ses intermédiaires, possèdent l'accès vers les comptes bancaires des mules et de nombreux mandats internationaux sont émis par une cohorte de mules de tous pays vers l'adresse postale du cyber-criminel ou celles de ses intermédiaires.

Pas vu, pas pris mais s'il est vu et si des plaintes sont déposées, quelles sont alors les lois qui s'appliquent et celles de la législation de quels pays ?

Gérard Peliks,

Président de l'atelier sécurité

Forum ATENA

Exemple de recrutement d'une mule (je suppose ;-))

De : xxxxxxxxxx

Envoyé : mercredi 19 décembre 2007 19:59

*À : ***********

*Objet : For: ***********

Good day!

A respectable "E-Trust"; company is seeking for employees in the USA.
If you are interested in finding a secure job, please, respond to us and we will be happy to give you more details.
At this moment we are enlarging our staff and you have a chance to become a member of our team and get additional earnings spending 2 - 3 hours per week.
You don't need any special experience for this position.

What we offer:
Flexible program: two hours/week at your choice, daytime and evening time, mainly checking your e-mail Work at home: checking e-mail and going to the bank Part time - no need to leave your current job - if you already work.
2-3 hours free during the week (mainly in the evening / non-business hours) for communication.

Important:
Adult age (must be over 18 years old)
U.S. work authorization
You don't need to selling or buying anything.
You don't need to make personal investments to start your work.

Requirements:
general internet knowledge including working with Microsoft Office (Word/Excel) familiarized with financial terms (debit/credit, invoices etc.) familiarized with banking procedures (wire transfers, withdraws etc.) no diploma required students accepted

If You are interested in our job offer, please, reply to this letter.

Contact us: usaserviceofficer@gmail.com