Anticiper les menaces informatiques : le phishing

Une menace de sécurité des données personnelles sur Internet

Le *phishing* est une technique informatique d'"hameçonnage" associant un message électronique (email/SMS) non sollicité à un site Web illégal dans le but d'obtenir des données confidentielles. Le site Web reproduit généralement un site commercial officiel, le plus souvent celui d'une banque. Le message incite l'utilisateur à déposer ses coordonnées confidentielles en se faisant passer pour une personne digne de confiance ayant un besoin légitime de l'information demandée. Cette forme d'attaque informatique est en partie basée sur l'ingénierie sociale, car c'est l'humain qui révèle lui-même ses informations personnelles.

Les risques : la fraude, l'usurpation de votre identité et l'infection de votre ordinateur

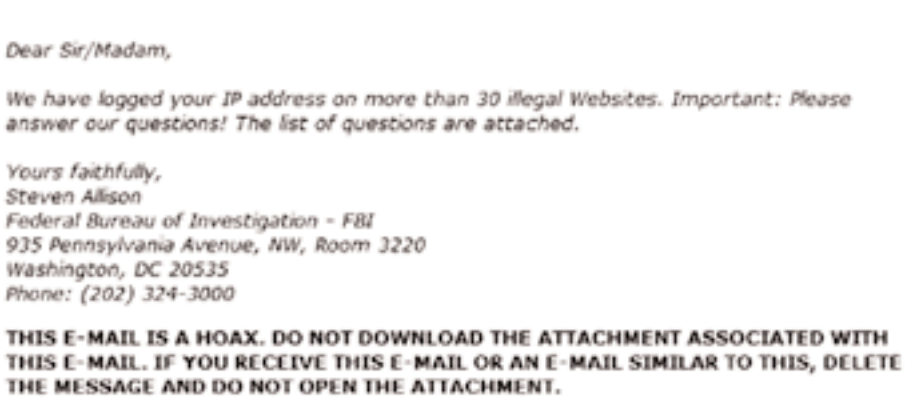
En pratique

Tout commence lorsqu'un e-mail ou un SMS vous incite à vous connecter à un espace personnel réservé (boîte mails, site de banque à distance, etc.), pour mettre à jour vos données, vous annoncer une « alerte sécurité », ou un faux débit bancaire. Nombreux sont les prétextes inventés pour exposer vos codes d'accès et données confidentielles.

Pour faire illusion, cet email provient d'une adresse usurpée, imitant une adresse officielle.
Le message, la plupart du temps au format HTML, contient un lien censé vous diriger sur une page sécurisée, qui est en fait reliée à un site factice (copie du site officiel…) destiné à capturer votre code d'accès.

Comme le rappelle Stéphane Koch, conseiller en lutte contre la criminalité économique et spécialiste du média Internet : *« Le format HTML se distingue par la mise en exergue des éléments de l'email tels que texte en gras, présence de logos ou colorisation. La particularité du format HTML est son aspect multicouche : ce qui est visible n'est pas forcément représentatif des éléments présents dans le code lui-même. Cela permet au fraudeur d'afficher l'adresse Internet authentique de l'entité visée, mais de faire pointer le lien sur le site de fraude. »*
La supercherie peut aller jusqu'à la proposition d'un numéro de téléphone renvoyant sur une messagerie vocale. *« On peut rappeler le cas de fraude téléphonique* [où] *le numéro était surtaxé 4 euros à la seconde. »*

Dans le cas de l'email-hameçon ou SMS, l'utilisateur accède à une page Web qui l'invite à saisir ses coordonnées confidentielles, numéro de compte ou de carte bancaire, numéro de sécurité sociale, voire les codes d'accès de sa messagerie personnelle... Dans le cas de la messagerie téléphonique, le message enregistré demandera de fournir les mêmes informations personnelles.
Finalement, le pirate disposera d'un fichier d'informations confidentielles qu'il pourra exploiter pour escroquer de nombreux sites commerciaux ou détourner des fonds.



Dear Sir/Madam,

We have logged your IP address on more than 30 illegal Websites. Important: Please answer our questions! The list of questions are attached.

Yours faithfully,
Steven Allison
Federal Bureau of Investigation - FBI
935 Pennsylvania Avenue, NW, Room 3220
Washington, DC 20535
Phone: (202) 324-3000

THIS E-MAIL IS A HOAX. DO NOT DOWNLOAD THE ATTACHMENT ASSOCIATED WITH THIS E-MAIL. IF YOU RECEIVE THIS E-MAIL OR AN E-MAIL SIMILAR TO THIS, DELETE THE MESSAGE AND DO NOT OPEN THE ATTACHMENT.

Figure 1 : Le FBI n'a pas été épargné par ces usurpations.
Source : The Internet Crime Complaint Center : www.ic3.gov

Lors de la consultation de sites sécurisés l'adresse du site doit commencer par HTTPS

Une menace avérée

Les cibles sont de plus en plus nombreuses et répertoriées sur différents sites web dédiés à ces arnaques : Microsoft, Yahoo, AOL, Amazon, eBay, CIC, LCL, Crédit Agricole, Banque AGF, TCF, BNP Paribas, VISA, Wells Fargo Bank, CitiBank, Barclays, SwiftPay.com, Regulations.gov, PayPal, etc.

Le FBI n'a pas été épargné par ces usurpations. (Voir figure 1).
Quelques critères de méfiance face à un email non sollicité : le champ émetteur est vide, il contient la même adresse que celle du destinataire, ou une adresse inconnue ; le champ émetteur contient une adresse connue mais le contenu du message est non conforme aux habitudes de l'émetteur.

***Statistiques du* phishing**
Par FraudWatch International

Sites actifs : 634
Total détections : 56 261
Mise à jour : 08/06

Source des statistiques :
FraudWatchInternational.com

Mesures de protection

1) Ne jamais communiquer des données sensibles en cliquant sur un lien de provenance inconnue.

2) Partir de la page d'accueil du site pour accéder aux autres pages.

3) S'assurer de l'activation du cryptage des données lors de la consultation de sites sécurisés (préfixe HTTPS et non HTTP).

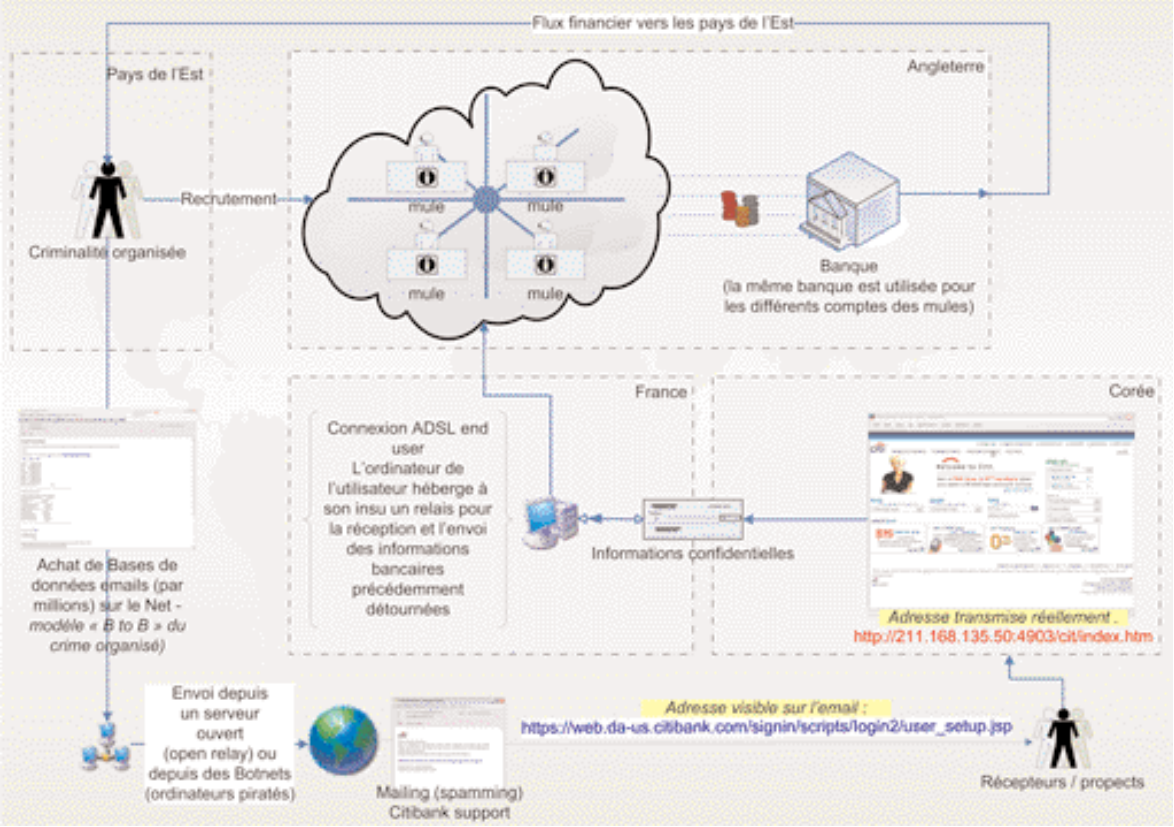
4) En cas de doute, s'abstenir de donner des informations, et prendre contact directement avec l'entreprise concernée pour lui signaler le message suspect.

Recours juridiques

En cas d'infraction constatée, ou tentative, trois règles sont impératives : sauvegarder les traces, agir vite, ne pas contacter l'auteur. Tout d'abord « sauvegarder les traces », les *logs*,

Anticiper les menaces informatiques : le phishing

Une menace de sécurité des données personnelles sur Internet (suite)



Analyse du mode opérationnel d'un *phishing*. Source : S.Koch, www.intelligentzia.net

ne pas réutiliser le matériel en cause, et le déconnecter. Ensuite « agir vite », car les différents intervenants peuvent disparaître en moins de 24 heures. De plus, les informations sont conservées 24 heures pour les proxys Internet ; les *logs* d'IP sont conservés 3 mois chez la plupart des FAI, et au maximum 1 an selon la CNIL.

Enfin, « ne pas contacter l'auteur » de l'acte malveillant et le laisser dans l'ignorance de la plainte, afin de ne pas le pousser à effacer les traces de ses actes.

L'organe national compétent pour ce type d'infractions est l'OCLCTIC - Office Central de Lutte contre la Criminalité liée aux Technologies de l'information et de la Communication. Cette structure dépend de la Direction Centrale de la Police Judiciaire (DCPJ). Elle coordonne au niveau national la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions liées aux nouvelles technologies. Par ailleurs, l'OCLCTIC est le correspondant d'Interpol et de ses homologues étrangers.

En cas d'infraction, vous pouvez contacter directement le SRPJ de votre lieu de résidence.

Pour Paris et sa région, l'interlocuteur est la BEFTI (Brigade d'enquête sur les fraudes liées aux technologies de l'information),
163, avenue d'Italie,
75013 Paris,
Tél. 01 40 79 67 50

Pour la province :
l'OCLCTIC,
101, rue des 3 Fontanots,
92000 NANTERRE,
Tél. 01 49 27 49 27
Fax. 01 40 97 88 59
oclctic@interieur.gouv.fr.

Vincent GRÈZES,
Diplômé de la Faculté de Droit et Sciences Politiques de l'université Lyon 3

Quelques références

- **Anti Phishing Working Group**
http://www.antiphishing.org/
- **Tout sur les derniers *phishing***
http://www.millersmiles.co.uk/
- **The Internet Crime Complaint Center**
http://www.ic3.gov
- **Repérer la criminalité informatique**
http://www.intelligentzia.net