PHISHING

Les lignes de défense s'organisent

Yvon Avenel
Journaliste
Éditeur de
Smartcardtrends

Les attaques sur internet se multiplient combinant spams, virus et faux sites web. Les institutions financières sont particulièrement visées. Face à ce phénomène, la mobilisation est générale, qu'il s'agisse de faire de la prévention auprès des utilisateurs, de se doter de moyens légaux ou d'adopter de nouvelles technologies.

L'année 2004 a battu des records en matière d'activités criminelles sur internet. La prolifération d'une centaine de milliers de nouveaux virus s'est accompagnée d'une montée en puissance sans précédent d'attaques massives et répétées combinant "spam", virus, faux sites web. Visant plus particulièrement les banques et les institutions financières, ces attaques dont le nom de guerre peut, à tort, évoquer de paisibles "parties de pêche" – *phishing* en anglais – menacent de devenir un véritable fléau. Autant d'ailleurs par les pertes financières qu'elles pourraient entraîner que par la méfiance qu'elles inspirent déjà vis-à-vis des transactions en ligne, du paiement en particulier, des services de banque à domicile, voire de l'usage de l'internet en général.

LA PLUS PRÉOCCUPANTE DES NOUVELLES ARNAQUES APPARUES SUR LE NET

« *La plus dangereuse, et la plus préoccupante des nouvelles arnaques apparues sur le Net* » indiquait à la fin 2003, le FBI. Ce diagnostic s'est confirmé depuis. Apparu en 2002 – une première attaque contre une banque australienne –, le *phishing* a connu une véritable explosion en 2004. MessageLabs, une société américaine spécialisée dans les services d'emails sécurisés aux entreprises, notait en décembre, dans son rapport annuel, que l'année 2004 avait été celle qui avait vu le "gros poisson" – entendez le *big phish* – débarquer. Les chiffres parlent d'eux-mêmes : c'est très précisément en juillet que les premières attaques massives ont été lancées. En un seul mois, elles ont été multipliées par dix. MessageLabs intercepte 264 000 emails issus de *phishers* en juin. Un chiffre modeste... rétrospectivement. En juillet la société en capte en effet 2,5 millions ! Puis 3 millions en août, 4,8 millions en octobre, 4,5 millions en novembre. Au total 18 millions sur l'année. Une toute petite partie de l'iceberg des emails envoyés dans le monde, mais un fort indicateur. De son côté, le Anti-Phishing Working Group (APWG) [1] enregistre entre les mois d'août à novembre une multiplication par quatre (de 2 000 à plus de 8 000) du nombre de types de messages envoyés, soit une progression mensuelle moyenne de l'ordre de 34 %. Il note également un doublement (de 717 à 1 518, soit une progression moyenne mensuelle de 28 %) du nombre des sites "leurres" que les emails invitent à visiter. Ces emails sollicitent (*illustration 1*) leurs destinataires à aller sur ces sites "vérifier", – simple routine ou événement souvent dramatisé pour des raisons de fraudes (!) ou d'irrégularités –, leurs comptes. Ils les invitent à livrer, au passage, mots de passe, identifiants, voire numéros de sécurité sociale ou de carte bancaire. Ces faux sites web sont des copies quasi parfaites des vrais sites, copies obtenues par simple copier-coller du code-source des pages présentées. Un type d'arnaque que l'on peut comparer à celles qui se développèrent un mo-

GLOSSAIRE

- **Phishing :** le mot est bien sûr construit sur un jeu de mot (*fishing*), mais le remplacement du f par ph est aussi une référence au terme de *phreaking* qui désignait dans les années soixante, une opération de piratage du téléphone aux États-Unis.
- **Zombie computer :** un ordinateur qui est utilisé pour servir de base à des attaques (spam, virus), à l'insu de son utilisateur, grâce à un logiciel caché qui permet de le contrôler à distance.
- **Spyware :** logiciel espion dont la forme la plus connue est le *keylogger* (capture de la frappe au clavier des identifiants pour se « *logger* ») utilisé dans le *phishing*. Ce logiciel peut être caché dans la pièce jointe d'un email et s'installer dès que celle-ci est ouverte.
- **Money mule :** personne abusée par une fausse offre de recrutement (ou de mission rénumérée) pour assurer les transferts de fonds issus du *phishing*, depuis son propre compte vers les comptes à l'étranger des auteurs du *phishing*.
- **Challenge-response :** version cryptographique de la technique des "secrets partagés" qui permet d'assurer une authentification mutuelle entre une personne, par exemple, et un site web. La personne pose ainsi une question (*challenge*) via un *token* ou une carte à puce au site web qui répond (*response*) pour prouver qu'il partage bien le secret indiqué dans le *challenge*.

ment dans le monde bien physique avec la mise en place de faux distributeurs de billets, dont la spécialité était d'avaler les cartes bancaires après avoir récupéré les PIN codes...

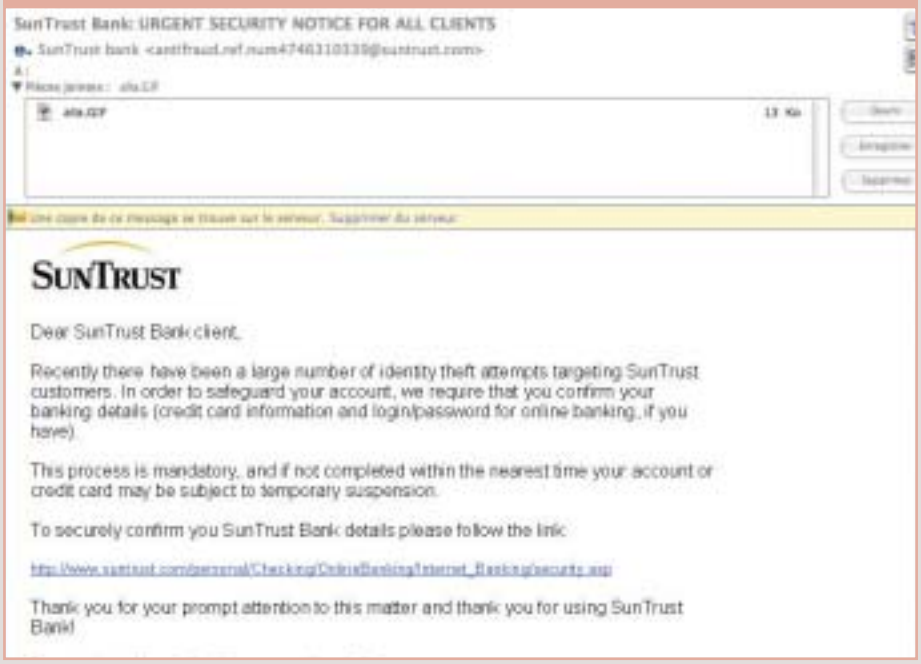
DES ATTAQUES CONCENTRÉES SUR CINQ OU SIX GRANDES SOCIÉTÉS

En novembre, l'APWG estimait qu'environ 5 % des destinataires de ces emails tombaient dans le piège. Ce chiffre est peut-être même inférieur (2 % est de plus en plus souvent invoqué), car si les moyens mis en œuvre sont massivement visibles – chaque internaute peut le vérifier en voyant passer les "projectiles" comme autant de mails qui ne lui sont pas directement destinés –, les sociétés visées restent réduites. 46 sociétés seulement étaient l'objet de ces attaques en août 2004, elles étaient 51 en novembre. 80 % des attaques ne portent, depuis le début du phénomène, que sur cinq ou six grands noms de la finance comme Citybank, US Bank, NatWest, ou du eCommerce comme eBay ou PayPal. En réalité, bien peu de "projectiles" atteignent leurs cibles. Belle illustration de la force de la menace par rapport à la faiblesse de la réalisation. Autre illustration de la médiatisation qui accompagne naturellement ces vagues d'attaques : la réalité des pertes financières qu'elles engendrent. Elles étaient estimées, en octobre dernier pour l'année 2004 dans le monde, à quelque 500 millions de dollars, par le cabinet d'études américain Ponemon Institute, soit à peu près la moitié de la fraude enregistrée dans le seul Royaume-Uni en 2003 sur les cartes bancaires (pas encore toutes équipées de puce). Mais, même ce chiffre relativement modeste paraît encore surestimé au cabinet d'études TowerGroup qui a publié ensuite – début décembre – son étude sur le *phishing*. Il table sur une perte de seulement 137 millions de dollars soit, cette fois, une part assez négligeable des pertes attribuées globalement à l'usage des cartes bancaires dans le monde, encore principalement à piste magnétique.

LA MESSAGERIE ET LE NAVIGATEUR WEB SONT DES ARMES

Ce tableau contrasté doit-il inviter à plus de "réalisme" et d'optimisme? Bon nombre d'experts et d'observateurs soulignent au contraire la force et la réalité de la menace.

1. DEUX EXEMPLES DE FAUX EMAILS


SunTrust Bank: URGENT SECURITY NOTICE FOR ALL CLIENTS

SUNTRUST

Dear SunTrust Bank client,

Recently there have been a large number of identity theft attempts targeting SunTrust customers. In order to safeguard your account, we require that you confirm your banking details (credit card information and login/password for online banking, if you have).

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

To securely confirm you SunTrust Bank details please follow the link:

Thank you for your prompt attention to this matter and thank you for using SunTrust Bank!

Ils craignent un raffinement des techniques utilisées par les organisations criminelles pour accroître l'efficacité de leurs attaques, et une recrudescence du *phishing* sous des formes inédites. "*Nous n'en sommes sans doute qu'au début*" affirme Laurent Charvériat, fondateur et directeur général de Cyber Networks, une société spécialisée dans la sécurité internet, "*la messagerie internet et le navigateur web sont en réalité deux armes qui peuvent se révéler redoutables. Ceux qui s'en servent généralement ne le savent pas. Une partie du problème est bien là*". Les techniques utilisées par les *phishers* frappent en effet par leur simplicité. Elles exploitent des possibilités offertes par la nature même des protocoles de messagerie (SMTP), et de navigation web (http), et en particulier la capacité à changer l'identité de l'expéditeur d'un message, à masquer une URL par une autre, ou encore à utiliser les vraies URL de certains serveurs ou simples PC comme relais de messagerie (technique du "rebond" et utilisation de PC "zombies"). Elles ont exploité également pour cela au tout début des failles découvertes, et corrigées depuis, dans le navigateur de Microsoft (Explorer), le plus répandu sur la planète. "*La sécurité est une affaire de compromis : plus un navigateur sait faire de choses, plus il est exposé à des attaques. Certaines options offertes dans ce type de logiciels peuvent ainsi ouvrir en grand des portes aux hackers. La sécurité est également une sorte de course-poursuite. Rien n'est jamais acquis. Une protection n'a qu'un temps. Il faut rester vigilant*" assure de son côté Julien Cohen, le responsable technique français de Websense, une société américaine, membre du APWG, qui propose aux entreprises des outils d'*anti-phishing* basés sur une analyse du comportement des sites web-leurres. "*Nous avons notamment* ●●●

●●● *remarqué depuis quelque temps une évolution importante du phishing. Celle-ci se traduit par l'utilisation intensive de logiciels espions (spywares), capables de capturer directement les frappes au clavier de l'utilisateur lorsque ce dernier donne son mot de passe et son identifiant lorsqu'il accède à son compte en ligne"* indique-t-il. Ce type de logiciel (The Banker AJ Trojan, par exemple) avait été également signalé en août 2004 par l'APACS, l'association de paiement anglaise, et le NHTCU (Hi-Tech Crime Unit). Il avait aussi déjà été identifié au Brésil quelques mois auparavant. Pour sa part, David Jevans, le chairman du AWPG, a tiré la sonnette d'alarme dès novembre dernier, en signalant l'apparition de nouvelles techniques accompagnant la montée en puissance du *phishing* et parmi celles-ci l'utilisation de *keyloggers* (capture de frappe au clavier), mais aussi de robots capables d'intensifier la rédaction, la réalisation, la diffusion des mails, mais aussi la création des faux sites web. "*Ces techniques pourraient accroître considérablement le taux de pénétration des attaques*" a-t-il indiqué.

UNE PROGRESSION DE 200 % PRÉVUE EN 2005

Combinées à l'augmentation prévue du nombre de ces attaques pour 2005, ces techniques pourraient en effet se révéler redoutables. TowerGroup prévoit pour l'an prochain une nouvelle explosion du *phishing* avec une progression de presque 200 % du nombre des attaques, plus particulièrement dirigées contre les institutions financières de taille plus modeste, et vers les sites de commerce en ligne, précise l'institut d'études. S'ajoute à cela une recrudescence des opérations de recrutement (*mule money*) via emails pour des "postes à responsabilité", qui s'avèrent bien être la dernière pièce du puzzle dans l'organisation du *phishing*. Après le vol des identifiants, il faut aussi trouver des comptes pour faire transiter les fonds dérobés en ligne.

On comprend donc que loin de minimiser les pertes financières actuelles du *phishing* pour dénoncer une surestimation ou surmédiatisation de sa menace, l'heure est plutôt à la mobilisation, à la prévention et l'éducation. Les banques et institutions financières, qui restent la principale cible (78 % des sociétés visées par les attaques en juillet 2004, 75 % en novembre), ont vite compris le danger en termes financiers directs mais aussi indirects. L'avenir des services de banque à distance basé sur la confiance des utilisateurs est bel et bien en jeu. Les fournisseurs d'accès internet sont logés à une enseigne similaire : ils entendent défendre également, et pas seulement en termes d'image, la qualité de leurs prestations, de messagerie en particulier, que pourraient leur disputer à l'avenir des "postiers" spécialisés dans la fourniture d'emails filtrées et "sécurisés", comme c'est déjà le cas aux États-Unis. Les gouvernements – police et justice en tête – sont loin d'être absents. Ils ont parfaitement identifié les liens mafieux du *phishing* avec d'autres activités criminelles. Quant aux fournisseurs de solutions, logicielles ou matérielles, *anti-phishing*, tous ont aujourd'hui de bonnes raisons d'être prêts pour apporter des réponses au défi de ce qui a déjà été identifié avec un peu d'emphase comme "l'une des guerres du XXI[e] siècle".

LA MOBILISATION EST GÉNÉRALE

Plusieurs lignes de défense se dessinent. La première touche à l'aspect légal mais aussi pédagogique de la lutte contre le *phishing*. On l'a vu avec la création à la fin 2003 de l'APWG qui regroupe désormais plus d'un millier de membres parmi lesquels on comptait, fin novembre, 677 sociétés. On le voit aussi avec la constitution de cellules de veilles, de sites internet, de groupements spécialisés (comme Digital PhisNet créé début décembre) ou de services web créés par des banques ou des fournisseurs d'accès internet. Il s'agit de collecter des informations mais aussi de prévenir en prodiguant des conseils. Même en France où le *phishing* est loin d'avoir connu le même essor qu'en Grande-Bretagne (une perte estimée à 4,5 millions de livres au cours des douze derniers mois), le niveau de vigilance est monté d'un cran à la fin de l'année. Le site "interactif" du Crédit Lyonnais affiche désormais, de façon très explicite, un lien vers des pages entièrement consacrées à expliquer en quoi consiste le *phishing*. La cellule "abuse. com" de Wanadoo dont le propos est également pédagogique, a, elle, vu défiler depuis septembre plus de 700 000 visiteurs. Les lois anti-spam à l'instar du "Anti-Spam Act" australien ou américain, commencent, par ailleurs, à faire l'objet de travaux et de réflexions pour converger au niveau international, afin de ne pas favoriser la création de sanctuaires. Les sites qui servent de leurres pour les campagnes de *phishing* sont toujours majoritairement localisés aux États-Unis, avec une durée de vie qui varie entre quelques heures et un mois. Des arrestations ont déjà eu lieu. Mais il n'est pas impossible que les organisations de *phishers* aient engagé une migration vers des pays comme la Chine, la Corée ou la Russie, de façon à se soustraire à des législations de plus en plus sévères. Dans son rapport de novembre 2004, l'AWPG montre un déclin de la part des sites américains (de 29 à 27 %), et une montée de la Chine (de 16 à 21 %). À noter, la timide apparition dans les statistiques, de la France qui aurait ainsi hébergé en novembre dernier quelque 24 sites de *phishing* (1,54 %).

> *"Plusieurs lignes de défense se dessinent avec la constitution de cellules de veille, de sites internet, de groupements spécialisés ou de services web créés par des banques ou des fournisseurs d'accès internet."*

QUELLE TECHNOLOGIE ADOPTER ? JUSQU'OÙ FAUT-IL INVESTIR ?

L'autre grande ligne de défense se fait plus ou moins discrète. Elle paraît plus discontinue aussi et moins coordonnée que la précédente. Elle reste la source de nombreux débats : quelle technologie adopter ? Jusqu'où faut-il investir ? Elle concerne les moyens d'*anti-phishing* mis en œuvre par les banques elles-mêmes, voire par les fournisseurs d'accès internet, ou encore par des particuliers plus sensibilisés que d'autres aux risques que représente le *phishing*, surtout dans ses formes les plus récentes, celles qui combinent étroitement virus "espions", spam et faux sites web. Faut-il miser sur les logiciels "anti-spam" et "anti-spywares" que l'on trouve désormais dans le com-

merce à l'usage des particuliers ou des entreprises ? Leur précision laisse parfois à désirer. Les ajouter à la panoplie déjà bien fournie de logiciels anti-virus, filtrage IP et autres *firewalls* peut, du coup, transformer la gestion de la sécurité en un véritable cauchemar. Traiter à la source ? "*Il n'y a pas de solutions définitives qui permettent d'identifier en amont des passerelles les emails dangereux. Les analyses de contenus ne sont pas compatibles avec le respect des données personnelles et de la vie privée de nos abonnés. L'analyse comparative des adresses IP et des noms de domaines n'est pas pertinente*" souligne-t-on chez Wanadoo, qui offre néanmoins des services anti-spam mais dont la mise en œuvre est confiée à l'utilisateur. Un travail qui peut être fastidieux et dont le résultat est encore une fois imprécis, voire contre-productif en bloquant des mails inoffensifs, voire vivement attendus. La société américaine Postini se targue pourtant de pouvoir traiter, grâce à une technologie spécifique de filtrage qu'elle a développée, plusieurs millions de connexions SMTP par jour sans avoir à ouvrir les messages, ni les stocker. Autre approche : le traitement du mail après sa réception, et du coup, celui du site web. "*Nous agissons en filtrant les URL, de façon à rendre impossible l'activation des liens vers les faux sites web*" précise de son côté Julien Cohen, qui met en avant la connaissance acquise par Websense ainsi que les bases de données d'adresses valides et de *black lists* mises en œuvre pour parvenir à la précision requise. Mais la solution ne s'applique qu'aux entreprises.

D'autres approches consistent à traiter les attaques au moment où elles se produisent, par des systèmes d'alertes et de contre-mesures. Bon nombre de banques en sont d'ores et déjà équipées, ce qui fait dire à certaines d'entre elles que les risques financiers sont globalement maîtrisés.

INSTAURER LA CONFIANCE

Dans un rapport publié en décembre, la Federal Deposit Insurance Corporation (FDIC) [2], l'organisme d'assurance des banques américaines, estime pourtant que l'usurpation d'identité (dont le *phishing* n'est que l'une des formes les plus récentes) aux États-Unis a coûté quelque 50 milliards de dollars en 2003, et fait 10 millions de victimes. Et de pointer le point faible du système : le manque d'authentification forte pour accéder aux services en ligne, et la carence de moyens pour authentifier emails et sites web.

"*La question fondamentale est en effet celle de la confiance*" résume de son côté Eddy Cormon, le responsable du Business Development chez Vasco Data Security, l'un des leaders mondiaux, fournisseur de solutions d'authentification forte (*tokens* et cartes à puce), "*le phishing tire parti de l'utilisation de mots de passe et d'identifiants statiques qui peuvent être rejoués facilement, c'est là qu'il faut agir*". Vasco propose ainsi d'utiliser une calculette (*token*), ou une calculette lecteur de carte à puce (qui peut être une carte EMV de paiement), pour assurer une authentification mutuelle du site web ou du service de banque à distance et de l'utilisateur (*illustration 2*). Le *token*, à partir de secrets partagés avec le serveur, calcule des mots de passe dynamiques (*one-time-password*) ou des signatures numériques très difficiles à falsifier. Même un logiciel espion serait dans ce cas inefficace. "*Parce qu'il a lui-même l'initiative de la procédure d'authentification – en lançant le challenge – et que celle-ci est simple, l'utilisateur a confiance dans le service auquel il accède. Il a tendance, du coup, à l'utiliser de plus en plus*" souligne Eddy Cormon. Fournisseur de solutions similaires à celles proposées par Vasco, ActivCard a récemment livré des cartes à puce à clés publiques (e-Badge PKI) qui permettent aux employés du Crédit Agricole de s'authentifier sur leurs postes de travail pour accéder à des services internes en ligne. La société a également livré des *tokens* (CA Certificat) qui permettent aux entreprises clientes de la banque d'accéder à leur compte en ligne grâce à des moyens d'authentification mutuelle et forte. "*Nous voyons depuis quelque temps, le nombre de demandes de la part des banques croître fortement pour ce type de produits et le lancement de pilotes*" souligne Marc Hudavert, vice-président et directeur général de la société. La Barclays en Grande-Bretagne serait ainsi en train d'étudier une solution de ce type, basée sur l'utilisation d'une carte EMV.

Ces solutions qui ne traitent que l'aspect serveur, ne résolvent pas le problème de l'authentification des emails eux-mêmes, dont la prolifération risque de devenir un véritable fléau en créant une grave défiance vis-à-vis de la messagerie, voire de l'internet tout court. 70 % des emails diffusés dans le monde seraient aujourd'hui du spam. Or ce problème qui avait commencé à recevoir un début de réponse grâce à des travaux menés au sein de l'IETF (l'instance de standardisation de l'internet) visant à établir un standard d'authentification pour les emails, est à nouveau entier. Le groupe de travail a brutalement clôturé ses travaux pour d'obscures raisons de "royalties" et de brevets. Microsoft qui entendait promouvoir sa technologie Sender ID au sein de ce groupe n'a pas eu gain de cause. Une carence intempestive qui fait paradoxalement à la fois le lit du *phishing*, et celui des moyens *anti-phishing* rapides et faciles à mettre en œuvre. ■

Yvon Avenel

2. OUTIL D'AUTHENTIFICATION MUTUELLE

■ **Vasco** propose d'utiliser une calculette (*token*), ou une calculette lecteur de carte à puce pour assurer une authentification mutuelle du site web ou du service de banque à distance et de l'utilisateur.

[1] Anti-Phishing Group : http://www. antiphing. org
[2] Rapport de la FDIC (Putting an End to Account-Hijacking Identity Theft. http://www.fdic.gov/