Alerte à la fraude – Phishing : les dernières tactiques et leur impact sur votre entreprise

Sommaire

Alerte à la fraude – Phishing : les dernières tactiques et leur impact sur votre entreprise

Introduction

Partout de le monde, le *phishing* (ou *hameçonnage*) constitue l'une des grandes menaces qui planent sur les entreprises et leurs clients – et la situation ne fait qu'empirer. Ainsi, le premier semestre 2012 a vu une augmentation de 19 % du nombre d'attaques mondiales par rapport aux six derniers mois de l'année 2011. Quant aux entreprises victimes du phishing, elles ont dû essuyer une perte cumulée de 2,1 milliards de dollars US entre janvier 2011 et juin 2012.[1]

Deux facteurs expliquent cette forte recrudescence : (1) les attaques sont relativement faciles à exécuter, et (2) leur taux de réussite est généralement élevé. Pour partir au hameçonnage sur Internet, pas besoin d'être un fin limier du hacking. Un peu de malice, une bonne dose de motivation, un appât du gain surdimensionné, et le tour est joué grâce aux kits de phishing clé en main disponibles sur le marché florissant du cybercrime. À tel point que les acteurs de ce milieu sont en train de se muer en fournisseurs MaaS (Malware-as-a-Service), avec toute une offre de prestations connexes en complément du kit proprement dit.[2]

Chaque jour, se sont pas moins de 156 millions d'e-mails frauduleux qui sont envoyés, dont environ 16 millions parviennent à percer les filtres. Environ la moitié de ces e-mails – soit 8 millions – sont ouverts, et 800 000 internautes mordent à l'hameçon. Oui, vous avez bien lu : il ne s'agit pas de 800 000 par an, mais bien de *800 000 par jour.*[3] Pour lutter contre ce fléau, les entreprises doivent s'informer en permanence sur les derniers subterfuges employés par les cybercriminels. Seule cette parfaite connaissance des menaces en présence leur permettra de prendre les mesures proactives qui les protègeront contre la fraude.

C'est pourquoi ce document dresse un état des lieux des tendances actuelles dans le milieu du phishing, avec un focus tout particulier sur la nouvelle déferlante de menaces en provenance de Chine. Nous vous livrerons ensuite les clés d'une protection efficace de votre entreprise et de vos clients.

Phishing sans frontières

Véritable fléau tentaculaire dont l'emprise est planétaire, le phishing incite les personnes peu méfiantes à fournir des informations confidentielles – noms d'utilisateur, mots de passe ou coordonnées bancaires – par le biais de communications électroniques en apparence légitimes.

Sur 200 domaines de premier niveau (TLD) étudiés, le groupe de travail APWG (Anti-Phishing Working Group) a recensé au moins 93 462 attaques par phishing à l'échelle mondiale, rien qu'au cours du premier semestre 2012. L'APWG note ainsi une hausse spectaculaire par rapport aux 83 083 attaques détectées au cours des six mois précédents. Pour le groupe de travail, une grande partie de cette augmentation est à mettre sur le compte des attaques perpétrées à l'encontre des serveurs virtuels mutualisés. Autre chiffre marquant : 64 204 noms de domaine uniques ont été touchés au cours du premier trimestre 2012, avec pas moins de 486 organisations dans le viseur des phishers (voir Figure 1).[4]

CHIFFRES CLÉS

	1H2012	2H2011	1H2011	2H2010	1H2010
Noms de domaines frauduleux	64 204	50 298	79 753	42 624	28 646
Attaques	93 462	83 083	115 472	67 677	48 244

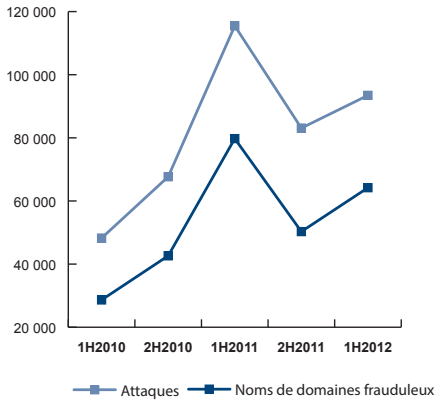

Figure 1 : le phishing a le vent en poupe.

1. « Phishing and the Social World », RSA, octobre 2012
2. « VeriSign iDefense 2012 Cyber Threats and Trends White Paper », VeriSign, janvier 2012.
3. « Phishing How Many Take the Bait? », Get Cyber Safe, février 2013.
4. « Global Phishing Survey 1H2012: Trends and Domain Name Use », Anti-Phishing Working Group, octobre 2012.

Phishing en Chine : l'irrésistible ascension de l'APT1

La majorité du phishing semble émaner de la Chine. Ainsi, au premier semestre 2011, on estimait à 70 % la part des noms de domaines frauduleux enregistrés par des phishers chinois au niveau mondial.[5]

En février 2013, Mandiant publiait un rapport alarmant consacré à un groupe de phishers particulièrement virulents, dont tous les éléments semblent indiquer qu'ils opèrent depuis l'Empire du Milieu. Baptisé « APT1 », ce collectif s'est illustré à de nombreuses reprises par ses activités d'espionnage depuis 2006. On peut donc en déduire avec une quasi-certitude qu'il agit au nom du pouvoir chinois, sous l'égide de l'Armée populaire de libération (APL). Selon Mandiant, APT1 aurait réussi à exfiltrer des dizaines de téraoctets de données à 141 organisations, et son rayon d'action peut s'étendre à des dizaines d'organisations en simultané. Ainsi, ces virtuoses du phishing seraient parvenus sévir en toute quiétude pendant une moyenne de 356 jours sur les réseaux de leurs victimes, avec un record de quatre années consécutives pour l'entreprise la plus touchée.[6]

Mandiant nous livre des éclairages passionnants sur les tactiques, les comportements et la localisation géographique de cette organisation criminelle. Sur ce dernier point, le constat ne laisse planer aucun doute : 97 % des connexions de l'APT1 vers sa plate-forme de lancement des attaques utilisaient des adresses IP enregistrées à Shanghai, et tous leurs systèmes étaient paramétrés en chinois simplifié. Sur 767 instances séparées, l'APT1 a eu recours au HUC Packet Transmit Tool (HTRAN) entre les systèmes de leurs victimes et leurs adresses IP, dont toutes étaient enregistrées en Chine.[7]

Aujourd'hui, la portée et la sophistication des attaques de l'APT1 ont atteint un niveau sans précédent. De toute évidence, ces phishers opèrent par centaines dans le cadre d'une organisation de grande envergure, sur une plate-forme équipée de plus d'un millier de serveurs, avec à leur service des linguistes, des développeurs de code malware et des experts informatiques chevronnés.[8]

Face à une menace d'une telle amplitude, la protection de votre entreprise et de vos clients passe par des mesures proactives et un dispositif renforcé. Pour vous aider à lutter efficacement contre l'APT1, Mandiant a publié pas moins de 3 000 indicateurs – dont les noms de domaines, adresses IP et les hashs MD5 – disponibles en téléchargement sur Redline, l'outil d'enquête gratuit de la société. Nous vous invitons à profiter au plus vite de ces précieuses ressources.

Serveurs virtuels mutualisés : la cible privilégiée

L'an dernier, nous avons assisté à une intensification alarmante des attaques perpétrées contre des serveurs virtuels mutualisés. Une fois que le phisher parvient à s'infiltrer sur l'un de ces serveurs, le ver est dans la pomme : il ne lui reste alors plus qu'à infecter les contenus de tous les domaines du serveur virtuel. Résultat : tous les sites hébergés sur le serveur compromis affichent des pages frauduleuses. Des milliers de sites peuvent ainsi être infectés en même temps.

Si l'on a observé un fléchissement de ces attaques en 2011, c'était pour mieux préparer leur retour en force en 2012. Rien qu'en juin, l'APWG a recensé un record de 7 000 attaques ciblant 44 serveurs virtuels différents.[9]

Gare aux spammeurs pendant les fêtes et autres événements d'actualité

Dans la course aux cadeaux de Noël 2012, des spammeurs ont usurpé l'identité d'un certain nombre de boutiques légitimes en proposant de « bonnes affaires de Noël », bons d'achats et autres voyages à gagner. Aux États-Unis, des phishers ont profité de l'approche de la date limite de déclaration d'impôts pour se faire passer pour l'IRS, le fisc américain.[10] Et comme toujours, les événements à retentissement planétaire s'accompagnent d'un déluge d'arnaques sur Internet – comme ce fut notamment le cas lors des Jeux olympiques de Londres.

Si les experts en sécurité avaient bien prédit un pic d'e-mails frauduleux en prélude à la quinzaine olympique londonienne,[11] les cyberarnaqueurs se sont plus que montrés à la hauteur. C'est ainsi que Zscaler attira rapidement l'attention sur la multiplication des sites de billetterie frauduleux,[12] tandis que de son côté, Omniquad démasquait un jeu-concours bidon sous couvert de promotion JO British Airways.[13] Qu'on ne s'y trompe pas, les grands événements sportifs qui se profilent (Coupe des confédérations 2013 et Coupe du monde de football 2014 au Brésil, Jeux olympiques de Sotchi 2014 en Russie, etc.) entraîneront la même vague d'arnaques autour de la ferveur populaire.

5. « Global Phishing Survey: Trends and Domain Name Use in 1H2011 », APWG, novembre 2011.
6. « APT1: Exposing One of China's Cyber Espionage Units », Mandiant, février 2013.
7. Ibid.
8. Ibid.
9. « Global Phishing Survey 1H2012: Trends and Domain Name Use », Anti-Phishing Working Group, octobre 2012.
10. « Christmas and End of Year Tax Phishing Scams », Northeastern University Information Services, décembre 2012.
11. « Symantec Intelligence Report », Symantec, janvier 2012.
12. « London Olympics: Stay Away from Scams, Data Theft, and Phishing », Zscaler, juillet 2012.
13. « Omniquad Warns Not to Fall for the London '2012 Olympic' Email Scam Fraudulently Evoking Both the Games and Their Sponsors », Omniquad, août 2012.

La crise économique, nouveau terreau du phishing

La crise économique offre aux cybercriminels un terrain fertile pour duper leurs victimes. Grand classique, les e-mails émanant soi-disant de l'établissement financier venant de racheter la banque de la personne ciblée.[14] Dans ce genre de situation, les consommateurs sont souvent dans le flou quant à l'opération de fusion-acquisition en cours – une aubaine pour les phishers.

Face à ces arnaques, la meilleure ligne de défense réside dans une communication simple, claire et cohérente avec vos clients, à chaque étape de l'opération. Mieux ils sont informés, moins ils sont susceptibles de tomber dans les pièges.

Menaces mixtes phishing/malware

Pour mettre toutes les chances de leur côté, les cybercriminels n'hésitent pas à combiner phishing et malware dans un mélange détonant.[15] Prenons l'exemple d'une personne qui reçoit par e-mail une e-card d'apparence anodine. En cliquant sur le lien de téléchargement de la carte, la personne est redirigée vers un site Web usurpé, qui charge un cheval de Troie dans l'ordinateur de la victime. Elle peut aussi tomber sur une boîte de dialogue l'invitant à télécharger une mise à jour logicielle pour pouvoir afficher la carte de vœux. Lorsque la victime s'exécute, elle télécharge en réalité un enregistreur de frappe (keylogger).

Les enregistreurs de frappe contiennent des composants de suivi dont le rôle consiste à surveiller des actions particulières, ainsi que des entreprises ciblées – établissements financiers, boutiques en ligne ou cybermarchands –, pour obtenir des informations confidentielles de type numéros de compte, identifiants d'utilisateur et mots de passe.

Phishing par texto et téléphone mobile

Outre le courrier électronique, les phishers ont aujourd'hui recours aux textos (SMS) pour se faire passer pour des établissements financiers légitimes. Si le support diffère, l'objectif reste le même : accéder à des informations bancaires confidentielles. Au premier semestre 2012, ce phénomène baptisé « SMiShing » a connu une explosion de 400 %[16]. Autre fait alarmant, en novembre dernier, des chercheurs de la North Carolina State University ont décelé de graves vulnérabilités SMiShing sur de nombreuses plates-formes Android.[17] (NB : une fois alerté, Google a corrigé ces bugs en l'espace de quelques semaines.)

Dans le SMiShing, l'arnaque la plus courante consiste à contacter une personne sur son mobile pour l'informer d'une soi-disant fraude sur son compte bancaire et de la désactivation de sa carte de crédit/retrait. La victime potentielle est alors invitée à appeler un numéro ou à se rendre sur un site Web contrefait pour réactiver la carte. Une fois la personne sur le site ou sur le serveur téléphonique, les phishers n'ont plus qu'à lui soutirer ses numéros de carte, coordonnées bancaires et codes confidentiels.

Impact potentiel du phishing sur votre activité

Même si l'industrie financière reste la cible privilégiée des phishers, d'autres secteurs sont également en ligne de mire : sites d'enchères, services de paiement, sites marchands, réseaux sociaux, sans oublier les fabricants et opérateurs de téléphonie mobiles. En résumé, aucune branche d'activité ni aucune marque n'est épargnée.

Non seulement les attaques par phishing portent atteinte à l'image de l'entreprise usurpée, mais elles dissuadent aussi les clients d'utiliser le site Web légitime, de crainte d'être victime d'une arnaque. Or, pour les entreprises en question, les conséquences vont bien au-delà d'un manque à gagner direct :

- Chute du chiffre d'affaires en ligne et/ou de la fréquentation en raison de la défiance des clients
- Risques d'amendes pour non-conformité en cas d'atteinte aux données des clients

On remarque également que les arnaques par phishing dirigées vers une marque donnée produisent un effet domino sur l'ensemble du secteur. Les craintes suscitées par le phishing entraînent en effet la défiance des consommateurs vis-à-vis des entités dont ils ne sont pas sûrs à 100 %.

Quelle protection pour votre entreprise ?

Bien qu'il n'existe pas de recette miracle, certaines technologies peuvent vous aider à protéger votre entreprise et vos clients. Les principales techniques de phishing actuelles tentent d'attirer les clients vers des sites Web frauduleux pour leur soutirer des informations confidentielles. Pour lutter contre ce phénomène et d'autres formes de cybercriminalité, des technologies de sécurisation comme le SSL (Secure Sockets Layer) et le SSL Extended Validation (EV) cryptent les informations confidentielles et permettent à vos clients d'authentifier facilement votre site.

14. « FTC Consumer Alert: Bank Failures, Mergers and Takeovers: A Phish-erman's Special », www.ftc.gov
15. « New Wave of Phishing Attacks Serves Malware to PCs and Macs », ZDNet, mars 2012.
16. « How to Avoid Becoming a Victim of SMiShing (SMS Phishing) », Network World, mars 2013.
17. « Smishing Vulnerability in Multiple Android Platforms (Including Gingerbread, Ice Cream Sandwich, and Jelly Bean) », NC State University, novembre 2012.

Les experts en sécurité préconisent d'appliquer les niveaux de cryptage et d'authentification maximum pour se protéger contre la fraude et renforcer la confiance des clients dans la marque. Norme internationale de sécurité en ligne, la technologie SSL sert à crypter et protéger les informations transmises sur la Toile en HTTP – le protocole de référence. SSL protège les données en transit contre tout risque d'interception et de modification susceptible de survenir en l'absence de cryptage. La plupart des systèmes d'exploitation, navigateurs Web, applications Web et serveurs physiques sont compatibles SSL.

Pour lutter contre le phishing et gagner la confiance de vos clients, vous devez trouver un moyen fiable de leur prouver votre authenticité et votre légitimité. Les certificats SSL Extended Validation (EV) répondent à ces enjeux. Leur mission : garantir le meilleur niveau d'authentification disponible sur un certificat SSL, tout en apportant aux internautes la preuve tangible de la légitimité d'un site.

SSL EV offre un moyen simple et fiable de gagner la confiance des internautes : concrètement, les navigateurs Web sécurisés affichent une barre d'adresse verte indiquant le nom de l'entité détentrice du certificat SSL et celui de l'autorité de certification émettrice.

La barre verte apporte la preuve visuelle que la transaction est cryptée et que le propriétaire du site a été authentifié selon la norme la plus stricte qui soit. Les cybercriminels sont impuissants face aux certificats SSL EV, et ce pour deux raisons : primo, l'affichage du nom de l'entreprise dans la barre d'adresse sort totalement du champ de leur contrôle ; et secundo, la rigueur du processus d'authentification EV leur interdit tout accès à ce type de certificat. En d'autres termes, les certificats Extended Validation restent hors de portée des cybercriminels.

Figure 2. Barre d'adresse verte activée par un certificat SSL EV dans Internet Explorer

Sensibilisation des consommateurs et des collaborateurs

Parallèlement à la mise en œuvre de la technologie SSL EV, les entreprises doivent poursuivre leurs efforts de sensibilisation de leurs clients et salariés aux pratiques de sécurité et aux réflexes anti-fraude à adopter sur Internet. En ce sens, vous devez leur apprendre à reconnaître rapidement les signes d'une tentative de phishing :

- Orthographe médiocre (moins courante de nos jours car les phishers ont fait des progrès en la matière)
- Salutation générale au lieu d'un message personnalisé
- Menaces sur l'intégrité de vos comptes
- Demandes d'informations personnelles
- Noms de domaine/liens falsifiés

Montrez-leur aussi les quelques précautions d'usage pour reconnaître un site Web valide et sécurisé avant de transmettre des informations personnelles ou confidentielles :

- Présence de la barre d'adresse verte
- URL commençant par HTTPS
- Clic sur l'icône du cadenas pour vérifier que les informations du certificat correspondent bien au site Web voulu

La clé de la confiance réside dans ces actions de sensibilisation. Dès lors que vos clients peuvent s'assurer concrètement de la sécurité de votre site, vous augmentez votre chiffre d'affaires et votre compétitivité, tout en réduisant vos coûts d'exploitation par le transfert d'une plus grande partie de vos opérations en ligne.

Mais n'oubliez jamais : le phishing est une hydre aux multiples têtes, appelée à poursuivre sa mue vers de nouvelles formes, tout en continuant de jouer sur la corde sensible des sentiments humains : compassion, confiance, curiosité, etc. Face à cette menace permanente, la protection de votre entreprise et de votre marque exige une attention de tous les instants. En adoptant les technologies SSL dernier cri, en vous informant sur les derniers types d'arnaques et en optant pour l'autorité de certification la plus rigoureuse sur les questions de sécurité, vous garderez un coup d'avance sur les phishers – et un coup d'avance sur la concurrence.

Glossaire

Autorité de certification (AC) : organisme de confiance indépendant chargé de délivrer des certificats numériques de type SSL (Secure Sockets Layer), après vérification de la véracité des informations figurant dans le certificat.

Cryptage : procédé de brouillage d'un message pour que seul le destinataire visé puisse accéder aux informations transmises. La technologie SSL (Secure Sockets Layer) établit un canal de communication privé, dans lequel les informations sont cryptées pendant leur transmission en ligne pour prévenir toute interception par voie électronique.

Certificat SSL Extended Validation (EV) : le processus EV met en œuvre une vérification plus poussée des demandeurs de certificats SSL (Secure Socket Layer), selon des pratiques édictées par le CA/Browser Forum, un organisme tiers indépendant. Dans Microsoft® Internet Explorer et d'autres navigateurs courants à sécurité renforcée, les sites Web sécurisés par les certificats SSL EV affichent une barre d'adresse URL de couleur verte.

HTTPS : les pages Web dont l'adresse commence par « https », au lieu de « http », permettent de transmettre des informations par un protocole http sécurisé. HTTPS figure parmi les points de sécurité à vérifier avant de communiquer des informations confidentielles sur Internet (numéros de carte de crédit, informations personnelles, données de partenaires commerciaux, etc.)

Technologie SSL (Secure Sockets Layer) : la technologie SSL et son successeur TLS (Transport Layer Security) recourent à la cryptographie pour assurer la sécurité des transactions en ligne. SSL s'appuie sur deux clés pour crypter et décrypter les données : une clé publique, connue de tous, et une clé privée, ou secrète, que seul le destinataire du message connaît.

Certificat SSL : un certificat SSL (Secure Sockets Layer) contient une signature numérique qui relie une clé publique à une identité. Les certificats SSL permettent de crypter les informations confidentielles durant leur transfert en ligne, et dans le cas de certificats validés par une autorité émettrice, servent aussi à vérifier l'identité du détenteur du certificat.

Pour approfondir le sujet :

- **Par téléphone**
  - **États-Unis : +1 888 484 2983**
  - **Royaume-Uni : +44 203 450 5486**
  - **Afrique du Sud : +27 21 819 2802**
  - **Allemagne : +49 69 3807 89081**
  - **France : +33 1 57 32 42 68**
- **Par e-mail : sales@thawte.com**
- **Sur notre site Web : https://www.thawte.fr/ssl**

Protégez votre activité et inspirez confiance à vos clients grâce à la sécurité renforcée des certificats numériques signés Thawte, leader mondial de la sécurité en ligne. Stabilité, fiabilité, infrastructure éprouvée, support client irréprochable… en 17 ans, Thawte a su s'imposer comme le partenaire international de choix pour les entreprises du monde entier.