KASPERSKY lab

LES DANGERS DU PHISHING : COMMENT ÉVITER QUE LES EMPLOYÉS NE MORDENT À L'HAMEÇON DE LA CYBERCRIMINALITÉ

PHISHING

/ˈfɪʃɪŋ/

nom

1. Pratique consistant à utiliser des e-mails frauduleux et des imitations de sites Web légitimes afin de dérober les données bancaires d'utilisateurs. [1]

Le phishing est la méthode préférée des cybercriminels pour infecter les ordinateurs des utilisateurs. Les employés des entreprises sont particulièrement vulnérables ; ils sont régulièrement pris pour cible car ils représentent un point d'entrée pour accéder à des données sensibles.

En général, la définition d'« l'ingénierie sociale » correspond aux astuces utilisées pour inciter les utilisateurs à dévoiler des informations. Pour y parvenir, les hackers doivent être en mesure d'attaquer simultanément des centaines, voire des milliers d'utilisateurs, ce qui a donné lieu à une nouvelle méthode que nous appelons « phishing » (en français, « hameçonnage »).

Dans cet eBook, nous présenterons quelques attaques classiques de phishing, l'évolution du hameçonnage au fil des années ainsi que nos conseils pour protéger votre entreprise.

1 Traduction de l'anglais du site Dictionary.com

PHISHING POUR LES DÉBUTANTS

Le phishing correspond à l'attaque suprême d'ingénierie sociale. Auparavant, la plupart des attaques d'ingénierie sociale étaient effectuées en « one-to-one », efficaces mais non évolutives. Depuis, le phishing permet une attaque à plus grande échelle : un hacker peut toucher en une seule fois des centaines ou des milliers d'utilisateurs.

Dans une attaque de phishing, les cybercriminels créent de fausses adresses e-mail et des imitations de sites Web (semblables à des ressources populaires sur Internet, comme des réseaux sociaux, des jeux ou des services de banque en ligne). Pour essayer d'attirer les utilisateurs sur leurs sites Web frauduleux, les hackers utilisent diverses méthodes d'ingénierie sociale. En général, une page de phishing contient des champs de texte pour que les utilisateurs saisissent leurs données personnelles.

Suivant le type de données qui les intéressent, les cybercriminels lancent une certaine attaque de phishing. Par exemple, si un hacker a pour objectif malveillant d'accéder à des comptes sur les réseaux sociaux, alors il essayera d'obtenir les adresses e-mail et les mots de passe de ses victimes au moyen d'un faux site Web, qu'il aura conçu en lui donnant une apparence semblable à celle d'un réseau social. Parmi les méthodes d'ingénierie sociale souvent utilisées figurent l'envoi de messages comportant des liens vers des sites de phishing et l'envoi d'e-mails contenant des pièces jointes avec des 'exploits'. L'objectif des hackers consiste à obtenir des identifiants de compte ou des données personnelles, des informations de contact, ainsi que des liens vers d'autres comptes, tout ceci en vue de faire des profits en usurpant des identités et en dérobant de l'argent.

ÉVOLUTION DU PHISHING

Selon le «rapport du groupe de travail anti-phishing pour le quatrième trimestre de 2013», le nombre de sites de phishing détectés a augmenté considérablement en 2013, qui est devenue l'une des années les plus actives pour ce type d'attaque malveillante :

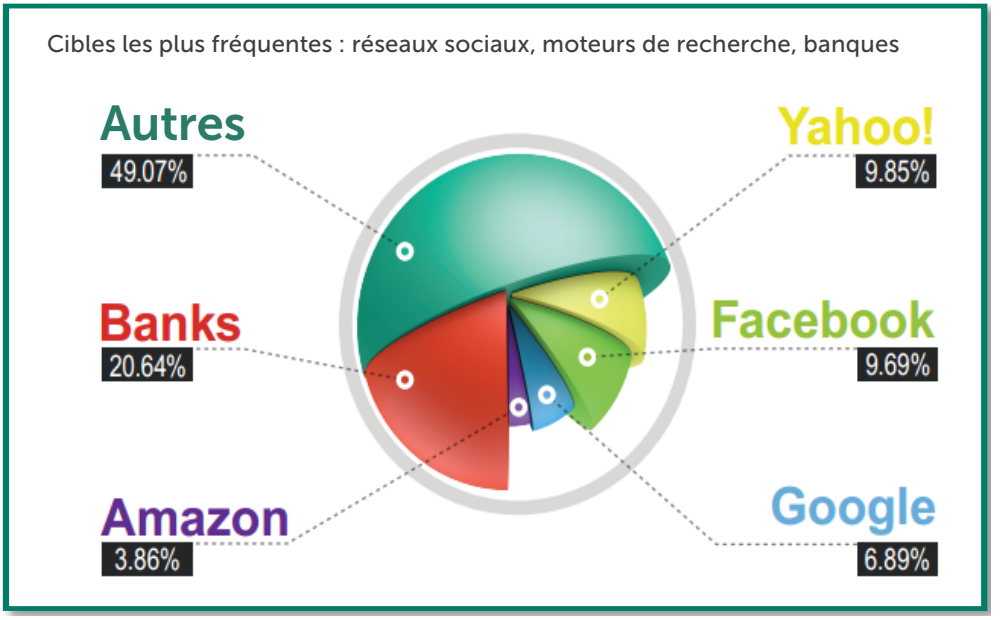
- En 2012-2013, 37,3 millions d'utilisateurs dans le monde entier ont été victimes d'attaques de phishing, ce qui représente une augmentation de 87 % par rapport à 2011-2012.[2]
- Plus de 20 % de l'ensemble des attaques visent des banques, ainsi que d'autres organismes financiers qui peuvent avoir une incidence sur les activités professionnelles des entreprises.[3]
- Chaque jour, 102 100 utilisateurs d'Internet du monde entier ont été victime d'attaques de phishing[4]
- Au cours du quatrième trimestre de 2013, les Etats-Unis sont restés le pays à héberger le plus de sites de phishing.[5]

De toute évidence, les cybercriminels ont plus souvent recours au phishing pour tenter de voler de l'argent ou de dérober des informations bancaires directement auprès des utilisateurs.

2,3,4,5 Rapport d'analyse de Kaspersky Lab sur l'évolution des attaques de phishing sur la période 2011-2013.


En 2012-2013,
37,3 millions d'utilisateurs
ont été pris pour cible
pour des attaques de
phishing.

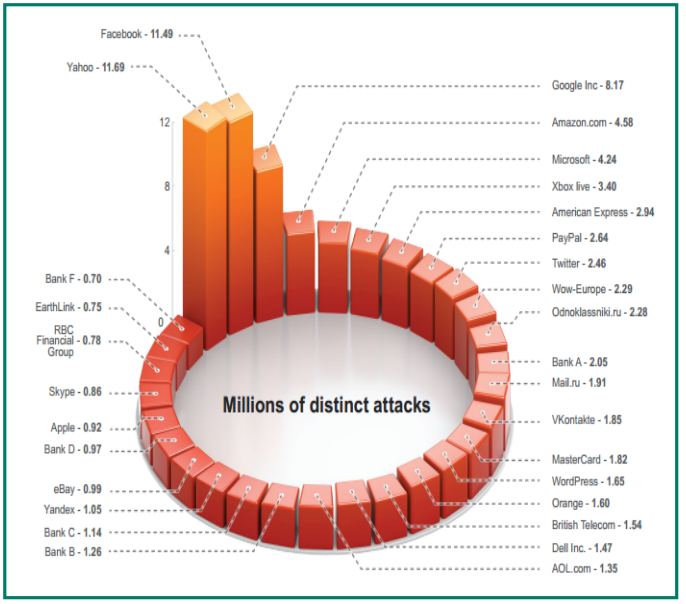
LES CIBLES DU PHISHING



6

En plus de prendre pour cible des sites d'entreprises, les cybercriminels visent des sites commerciaux utilisés par des professionnels pendant leurs heures de travail.

6 Rapport d'analyse de Kaspersky Lab sur l'évolution des attaques de phishing sur la période 2011-2013



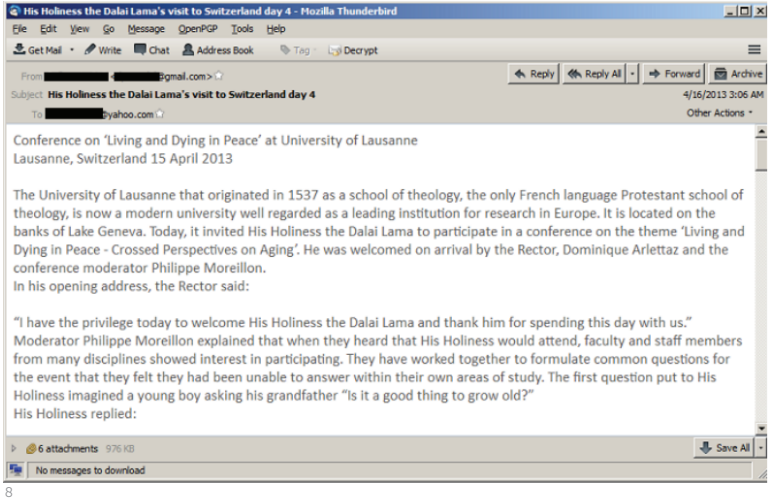
	USA
1	Yahoo!
2	Facebook
3	Google Inc
4	Amazon.com: Online Shopping
5	Wow-Europe
6	Microsoft Corporation
7	AOL.com
8	American Express
9	Bank A
10	Twitter

7

Les cybercriminels utilisent généralement les boutiques en ligne et les sites de banques pour obtenir des données d'utilisateurs, qu'ils utilisent ensuite dans le but de s'infiltrer dans le réseau d'une entreprise, mettant en péril cette dernière.

7 Kaspersky Analysis Report, The Evolution of Phishing Attacks 2011-2013

LE DALAI LAMA : EXEMPLE DE PHISHING



8

Parfois, les stratagèmes de phishing sont utilisés pour lancer des attaques ciblées. En juin 2014, les chercheurs de Kaspersky Lab ont par exemple analysé une campagne de cyberespionnage baptisée « NetTraveler ». Les attaquants avaient envoyé un e-mail de spear phishing (en français, harponnage) informant un certain nombre de groupes d'activistes de la venue du Dalaï-lama en Suisse. L'e-mail contenait plusieurs images, destinées à leurrer les récepteurs, représentant de nombreux Tibétains et le Dalaï-lama en train de s'exprimer.

L'e-mail comportait en pièce jointe plusieurs documents Word malveillants qui exploitaient des vulnérabilités connues. Bien que Microsoft® ait publié des patchs, ces vulnérabilités sont toujours fréquemment utilisées dans les attaques ciblées pour trouver des victimes dont les systèmes n'ont pas été corrigés. De nouveau, il s'agit d'une combinaison dangereuse entre l'ingénierie sociale et l'exploitation courante des vulnérabilités. Dans ce cas, l'attaque s'est déroulée en 2013 et utilisait une vulnérabilité qui avait été corrigée en 2010.

8 Kaspersky Lab, Equipe internationale de chercheurs et d'analystes, « The NetTraveler », 4 juin 2013

DES ATTAQUES DE PLUS EN PLUS ÉLABORÉES

Qu'arrive-t-il si les techniques présentées précédemment ne fonctionnent pas ? Les attaquants essayeront alors une approche plus centrée et personnalisée : les attaques de 'spear phishing' et les attaques ciblées.

L'envoi d'e-mails de « spear phishing », utilisés dans des attaques ciblées, est l'une des méthodes les plus fréquemment utilisées pour toucher des cibles de valeur dans les entreprises.

D'après la Global IT Security Risks Survey de 2014:

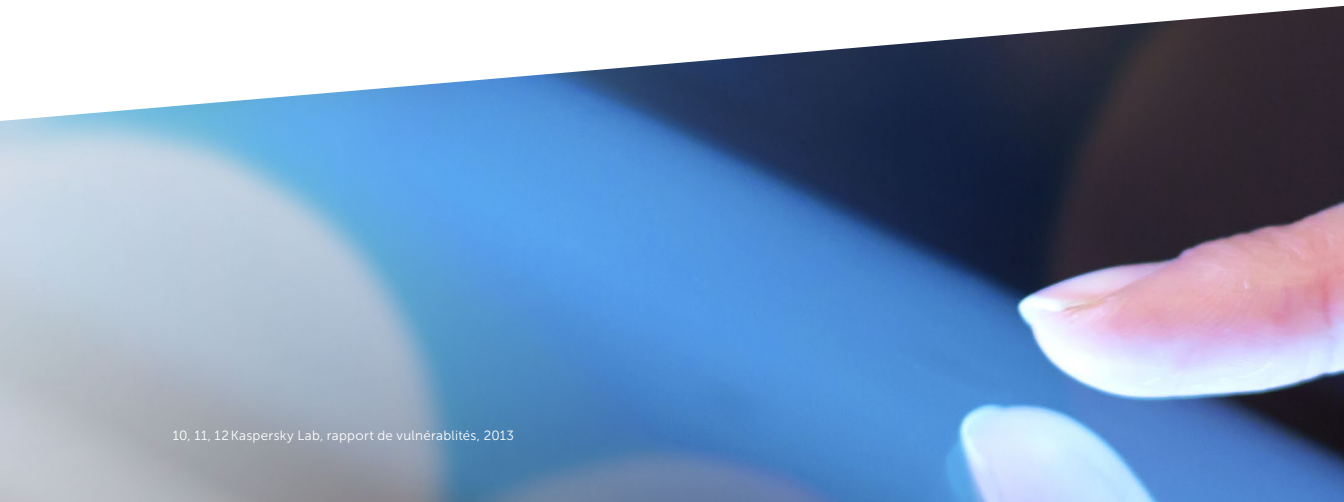
- 94 % des entreprises sondées ont déploré au moins un incident de sécurité externe.
- Les répercussions estimées d'une violation des données d'une entreprise ont augmenté de 14 %, atteignant les 798 000 dollars américains.
- 87 % des entreprises qui ont perdu des données ont dû faire appel aux services de professionnels externes et 47 % ont subi d'importantes pertes supplémentaires.
- En général, les dommages provoqués par une violation de données (notamment les coûts pour contracter les services de professionnels, les temps d'arrêt et les pertes d'opportunités commerciales) étaient de l'ordre de 35 000 dollars américains pour les petites et moyennes entreprises et de 690 000 dollars américains pour les plus grandes entreprises.[9]

9 B2B International et Kaspersky Lab, B2B International et Kaspersky Lab

UN PROBLÈME MAJEUR

1 En 2013, les vulnérabilités que contenait Oracle Java® ont été exploitées dans plus de 90 % de l'ensemble des cyberattaques.[10]

2 Les spécialistes en sécurité informatiques ont rapporté plus de 160 vulnérabilités auprès d'Oracle.[11]



10, 11, 12 Kaspersky Lab, rapport de vulnérablités, 2013

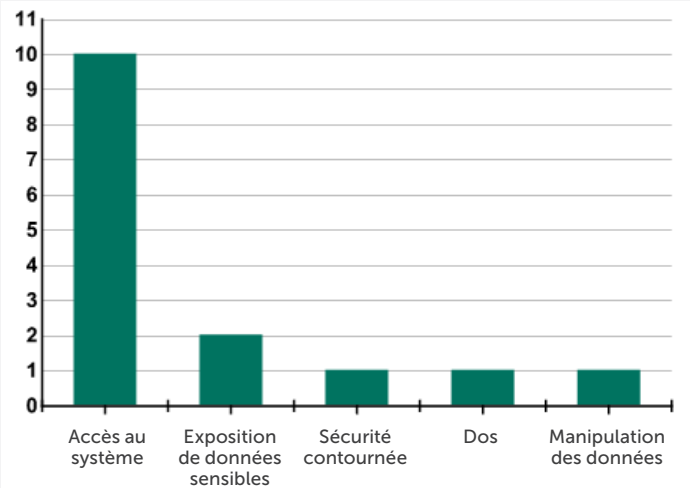
3

En 2013, Kaspersky Lab a détecté plus de 14,1 millions d'attaques qui utilisaient Java.[12]

4

Les composants de Windows®, le système AndroidTM et le logiciel Adobe Acrobat Reader® comportent le plus grand nombre de vulnérabilités encore exploitées.

EXPLOITATION DES VULNÉRABILITÉS



13

- Les vulnérabilités permettent aux hackers d'exécuter des codes malveillants et de prendre le contrôle total d'un système.
- Accès.

CONSEILS POUR LES RESPONSABLES INFORMATIQUES AFIN D'ÉVITER LE PHISHING

- N'affichez pas la liste de tous les employés sur le site Web de votre entreprise.
- Consultez régulièrement Internet pour identifier les adresses e-mails et/ou les données exposées.
- Expliquez aux utilisateurs les dangers liés au fait de partager trop d'informations sur les réseaux sociaux.
- Réalisez des simulations d'attaques de « spear phishing » afin de sensibiliser les employés.
- Mettez à jour votre système et vos programmes.
- Installez une solution de sécurité fiable et utilisez toutes ses fonctionnalités, notamment la recherche de vulnérabilités, la gestion de correctifs et la détection rapide des virus.
- Conseillez aux utilisateurs de se montrer prudents par rapport aux sites Web auxquels ils accèdent et aux fichiers qu'ils ouvrent lorsqu'ils utilisent les ordinateurs et les appareils de l'entreprise.
- Sensibilisez les employés au fait qu'ils travaillent pour une entreprise dont les données et les informations ont beaucoup de valeur sur le marché noir de la cybercriminalité.
- Prenez conscience que chaque employé sera pris pour cible au moins une fois dans sa carrière. Même si les attaquants préfèrent s'en prendre aux directeurs, aux membres des ressources humaines et au personnel des services juridiques, ils essayeront avec tout le monde.
- Sachez que les attaques seront de plus en plus sophistiquées en termes d'ingénierie sociale.
- Faites attention car les e-mails pourraient provenir d'autres employés ou même de membres de la direction.
- Informez les utilisateurs qu'ils doivent toujours être vigilants et doivent faire attention aux e-mails qu'ils reçoivent.

UNE PROTECTION À PLUSIEURS NIVEAUX EST NÉCESSAIRE CONTRE LES MENACES SOPHISTIQUÉES

Les cybercriminels et les malwares qu'ils développent sont en constante évolution, et il est impossible de protéger un organisme sans se tenir au courant des dangers. B2B International a réalisé un sondage auprès d'entreprises et Kaspersky Lab a analysé les données tirées dans son rapport le plus récent sur les menaces en matière de sécurité informatique et les violations de données. Publié en 2014, ce rapport a révélé l'existence d'un fossé entre la perception et la réalité[14]:

- En 2013 et 2014, Kaspersky Lab a détecté environ 315 000 échantillons de malware par jour, mais seuls 4% des entreprises sondées se disent conscients de ce chiffre.
- Fin 2013, les chercheurs de Kaspersky Lab avaient détectés 200 000 échantillons uniques de codes malveillants. A la fin du premier semestre de 2014, ce nombre a grimpé jusqu'à 375 000.

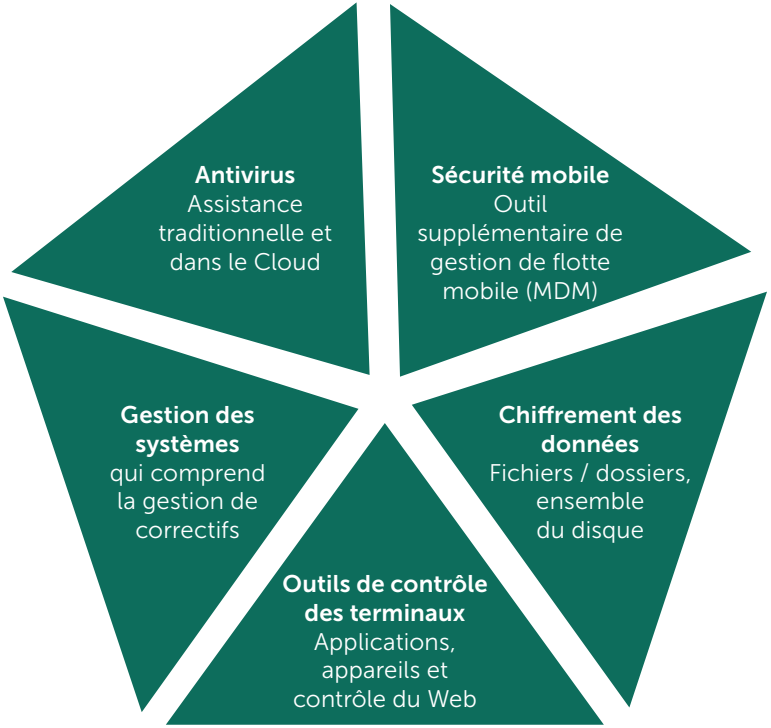
14 B2B International et Kaspersky Lab, "IT Security Threats and Data Breaches," octobre 2014

De simples étapes, comme la gestion des correctifs, peuvent réduire considérablement votre exposition. Les programmes les plus souvent visés par des attaques ciblées sont Microsoft Office®, Adobe Reader®, Adobe Flash®, Internet Explorer® et Oracle Java. Par conséquent, la mise à jour des logiciels, des systèmes d'exploitation et des applications tierses devrait constituer une priorité.

Pour des structures informatiques plus grandes et plus complexes, la mise en œuvre de patchs peut prendre plus de temps, ce qui augmente les risques que des vulnérabilités publiées soient exploitées. Considérez la possibilité d'utiliser des technologies de protection avancée, comme la protection automatique des « exploits » (AEP, Automatic Exploit Prevention), lesquelles utilisent les mécanismes de protection de l'exécution des données (DEP, Data Execution Prevention) et de distribution aléatoire de l'espace d'adressage (ASLR, Address Space Layout Randomization) comme méthodes d'analyse heuristique et de contrôle sur les codes exécutables. Ainsi, vous bloquerez l'exécution d'un code malveillant avant qu'une vulnérabilité ne soit corrigée ou quand une vulnérabilité zero-day est utilisée.

KASPERSKY SECURITY FOR BUSINESS

PHYSIQUE » VIRTUEL » MOBILE »



Recherche de vulnérabilités

Outils à distance

Gestion des systèmes

Gestion de correctifs

Gestion des licences

Contrôle d'admission du réseau (NAC)

GESTION DES SYSTÈMES & DES PATCHS

GESTION DES SYSTÈMES

- Création d'images
- Stockage et mise à jour
- Déploiement

RECHERCHE DE VULNÉRABILITÉS

- Inventaires HW et SW
- Plusieurs bases de données de vulnérabilités

GESTION DES LICENCES

- Vérification de l'utilisation
- Gestion des renouvellements
- Conformité des licences

GESTION DES CORRECTIFS AVANCÉE

- Priorisation automatique
- Options de redémarrage

OUTILS À DISTANCE

- Installation d'applications
- Mise à jour d'applications
- Résolution des problèmes

CONTRÔLE D'ACCÈS AU RÉSEAU (NAC)

- Gestion de la politique d'accès aux données pour les visiteurs
- Portail visiteurs

PROTÉGEZ VOTRE ENTREPRISE DÈS MAINTENANT.

Rejoignez-nous sur les réseaux sociaux

Regardez-nous sur YouTube

'Likez' notre page sur Facebook

Consultez notre blog

Suivez-nous sur Twitter

Rejoignez-nous sur LinkedIn

RECEVEZ VOTRE VERSION GRATUITE MAINTENANT >

Pour en savoir plus
kaspersky.fr/entreprise-securite-it/

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est le principal fournisseur mondial à capitaux privés de solutions de protection des postes de travail. La société se classe parmi les quatre premiers éditeurs mondiaux de solutions de sécurité dans ce domaine1. En 17 ans d'histoire, Kaspersky Lab n'a cessé d'innover dans la sécurité informatique et offre des solutions logicielles efficaces aux consommateurs, PME et grandes entreprises. La société est aujourd'hui présente dans près de 200 pays, protégeant plus de 400 millions d'utilisateurs dans le monde.

Plus d'informations sur www.kaspersky.fr

KASPERSKY lab

LE POUVOIR
DE PROTÉGER