# Combattre le phishing

Auteur
Sébastien GOUTAL
*Chief Science Officer*

# Index

# Introduction

Le phishing est une menace persistante dans le domaine de l'email: la très grande rentabilité de cette activité, sa facilité à la mettre en œuvre, associées à la grande difficulté à la combattre autant d'un point de vue technique que juridique, rendent le phishing très attractif pour les criminels. Il est donc raisonnable de s'attendre à un maintien - voire à un accroissement - de cette menace dans les prochaines années.

Nous allons présenter les principales techniques utilisées pour combattre les emails indésirables - spam et phishing essentiellement - chacune ayant leurs avantages et leurs inconvénients.

# Typologies du phishing et du spam

Tout d'abord, il est indispensable de présenter les caractéristiques du phishing. Un phishing est un email contenant un lien vers un site frauduleux, dont le but est d'amener l'utilisateur à communiquer des informations sensibles : numéro de carte bleue, identifiants de connexion, données personnelles... Les informations capturées étant à haute valeur ajoutée, le phishing est une activité rapidement rentable : par conséquent, les campagnes de phishing sont de faible volumétrie – en général quelques milliers d'emails - et sont de courte durée - quelques heures, au plus. Cette forte rentabilité à court terme, associée à la relative facilité technique de mise en œuvre[1], font que cette activité attire beaucoup de criminels, essentiellement amateurs.

La typologie du spam est différente : il s'appuie sur les botnets, qui sont des infrastructures très complexes à mettre en œuvre, et est souvent associé à d'autres activités criminelles complexes, telles que la diffusion de malware ou le blanchiment d'argent à grande échelle. Les botnets étant de taille considérable[2], les campagnes de spam ont une volumétrie très importante, en général plusieurs millions d'exemplaires, et peuvent durer plusieurs jours.

(1) L'envoi de quelques milliers d'emails ne nécessite pas un niveau de compétences élevé. En outre, des logiciels clé en main peuvent être utilisés à cet effet.
(2) Par exemple, on estime que le botnet BredoLab est constitué d'environ 30.000.000 de machines zombies.

# Techniques de filtrage des emails indésirables

Nous allons présenter les techniques de filtrage des emails indésirables. Ces techniques ne sont en aucun cas exclusives : elles sont complémentaires, et permettent chacune de traiter une partie de la problématique du filtrage des emails indésirables.

## Filtrage par blacklist IP

Le filtrage par blacklist IP est la technique la plus simple pour se protéger contre les emails indésirables : il consiste à refuser tous les emails envoyés par des expéditeurs - identifiés par leur adresse IP - qui ne sont pas considérés comme fiables. Une machine zombie, appartenant à un botnet, et qui envoie essentiellement du spam, est un exemple d'expéditeur qui doit être blacklisté.

La mise en blacklist d'une adresse IP prend toutefois du temps : il faut la détecter, éventuellement modérer la décision, et ensuite diffuser cette information. Cette technique fonctionne très bien avec le spam, car ce dernier a une grande visibilité, du fait de la volumétrie et de la durée des campagnes. Toutefois, concernant le phishing, la faible volumétrie associée à la courte durée font que beaucoup de campagnes de phishing ne sont même pas détectées par ce biais.

## Filtrage par signature

Le filtrage par signature est très largement utilisé dans la lutte contre les emails indésirables. Son principe est simple: un utilisateur qui estime avoir reçu un email indésirable le signale, ce qui a pour effet de remonter une signature de cet email. Les signatures sont ensuite regroupées, modérées – car un utilisateur peut se tromper et se plaindre d'un email parfaitement légitime – et ensuite diffusées pour protéger la messagerie contre des emails indésirables similaires.

Si cette technologie s'avère efficace pour lutter contre le spam, elle n'est par contre, pas très adaptée pour lutter contre le phishing, pour les mêmes raisons que celles évoquées précédemment. Le temps de détecter, de produire et de diffuser une signature permettant de bloquer une campagne d'emails indésirables est assez long : il est donc probable que la campagne de phishing soit terminée avant que le filtre antispam n'ait été mis à jour.

## Filtrage heuristique

Le filtrage heuristique se base sur des règles utilisant des caractéristiques de l'email pour prendre une décision. Par exemple, les spams envoyés par des botnets partagent un certain nombre de caractéristiques qui les différencient des emails légitimes : ils sont en général peu structurés, envoyés depuis des machines zombies et contiennent des mots clés suspects (viagra, cialis...)... L'intérêt du filtrage heuristique est qu'il est prédictif, et qu'il permet de bloquer des vagues de spam qui n'ont pas encore été bloquées par les mécanismes précédents.

Ce filtrage s'avère relativement efficace avec le phishing car il est prédictif : une petite variation d'une campagne de phishing à l'autre aura peu de conséquences, car le phishing conserve un certain nombre de caractéristiques propres. Il est toutefois nécessaire de suivre les tendances du phishing et de faire évoluer les règles de manière à garder un niveau d'efficacité élevé.

## DMARC

DMARC - qui signifie *Domain-based Message Authentication, Reporting & Conformance* - est une spécification technique dont le but est de standardiser l'authentification des emails en se basant sur les technologies déjà existantes DKIM et SPF. DMARC a été adopté par des acteurs majeurs du marché de l'email, ainsi que par de grandes sociétés comme PayPal et Facebook.

DMARC traite de manière efficace le cas du *exact-domain phishing*, c'est à dire du phishing dont l'adresse de l'expéditeur contient le nom de domaine exact de la marque contrefaite[3]. Ce type de phishing représentait en 2012 44 % du phishing aux Etats-Unis, 53 % du phishing au Royaume-Uni et 18 % du phishing en France[4]. Par contre, il ne traite pas le phishing dont l'adresse de l'expéditeur ne contient pas le nom de domaine exact de la marque contrefaite.

## Filtrage par blacklist d'URLs

Le filtrage par blacklist d'URLs consiste à filtrer les emails en fonction des URLs contenues dans ce dernier. Cette technique est particulièrement adaptée au phishing, car un phishing contient toujours une URL qui va amener l'utilisateur sur le site frauduleux. A ce titre, la plupart des navigateurs web propose une protection contre le phishing, en disposant d'une base de données d'URL de phishings : si l'utilisateur visite une page suspecte, alors un message d'avertissement sera affiché pour dissuader l'utilisateur de continuer.

La mise en blacklist d'une URL a a priori, les mêmes contraintes que le filtrage par signature ou le filtrage par blacklist IP, car il faut détecter l'URL, éventuellement modérer la décision, et ensuite diffuser cette information. Toutefois, la forte coopération entre les différentes acteurs - sociétés victimes de phishing, navigateurs web, vendeurs antispam - et le fait que la menace puisse être détectée autant au niveau SMTP que HTTP font que la réactivité est plus forte, et que le filtrage s'avère plus efficace.

(3) Par exemple, un *exact-domain phishing* visant PayPal aura *paypal.com* comme nom de domaine dans l'entête *From* de l'email.

(4) Se référer à notre étude *The expected impact of DMARC on phishing publiée* en Avril 2012.

# Conclusion

Il n'existe à notre connaissance, aucune solution technologique unique permettant de traiter le phishing de manière définitive, et seul un ensemble de mesures peut combattre le phishing de manière efficace. Il est donc conseillé d'associer les techniques présentées précédemment pour traiter cette menace de manière efficace.

En outre, les sociétés victimes de phishing - telles que les banques et les services financiers en ligne - devraient implémenter l'authentification forte pour des opérations critiques telles que des virements bancaires. L'authentification forte est une procédure qui requiert la présentation d'au moins deux facteurs d'authentification parmi les trois facteurs d'authentification existants (ce que l'utilisateur connait, ce que l'utilisateur détient et ce que l'utilisateur est). Une approche classique est d'envoyer un code de confirmation par SMS vers un téléphone mobile (ce que l'utilisateur détient), et ainsi de renforcer une procédure d'authentification. La généralisation des procédures d'authentification forte devrait ainsi limiter les dommages causés par le phishing.

Enfin, il est indispensable d'éduquer les utilisateurs. En particulier, l'utilisation du protocole HTTPS devrait être systématique dès que des informations sensibles sont échangées, alors que la quasi-totalité du phishing utilise le protocole HTTP[(5)]. Les utilisateurs devraient donc en avoir pleinement conscience.

(5) On estime que moins de 0.1% du phishing utilise le protocole HTTPS.

## A propos de Vade Secure

Vade Secure est le leader reconnu de la lutte, à base d'une technologie de filtre heuristique, contre les phishing, spear-phishing, malware et ransomware. Indépendant du langage, le filtre analyse individuellement les emails dans leur globalité (méthode d'envoi, liens, pièces jointes, contenu…) pour détecter toutes les menaces, même les attaques très ciblées en zero-day. Vade Secure complète son offre avec des solutions innovantes de gestion du graymail. La classification automatique des emails ainsi que la désinscription en 1 clic permettent aux utilisateurs de gérer leur boite de réception très simplement.

Protégeant plus de 500 millions de boîtes aux lettres dans plus de 76 pays, nos solutions sont utilisées par les plus grands FAI, OEM et entreprises. Vade Secure est implanté dans 5 pays (USA, Canada, France, Hong Kong et Japon) pour assurer un support 24/7.