FireEye™

Livre blanc

Attaques par harponnage — Les raisons de leur succès et les moyens de les contrer

Combattre l'attaque de prédilection des cybercriminels

Sommaire

Résumé	3
Introduction : l'essor des attaques par messages de harponnage	3
La raison de la progression des attaques par harponnage : leur efficacité	5
Exemples et caractéristiques de messages de harponnage	5
Etude du cas RSA : harponnage et menace persistante avancée	6
La solution : une protection contre les menaces de nouvelle génération	7
Conclusion	8

Résumé

Les attaques autrefois larges et dispersées ont rapidement cédé la place à des attaques ciblées avancées, lourdes de conséquences pour les entreprises. Les plus célèbres d'entre elles, telles que les attaques visant RSA et HBGary Federal ou l'opération Aurora, ont fait appel à des techniques de harponnage — en anglais, *spear phishing*. L'essor de ce type d'attaques est directement lié à son efficacité, puisque les systèmes de défense traditionnels sont incapables de les contrer. Ce livre blanc analyse de manière détaillée l'utilisation du harponnage dans les attaques ciblées avancées. Il offre une vue d'ensemble du harponnage, décrit ses caractéristiques et présente une étude de cas relative à une attaque tristement célèbre. Enfin, il étudie les mesures de protection essentielles que les entreprises doivent mettre en place pour combattre efficacement ces nouvelles menaces émergentes, en constante évolution.

Introduction : l'essor des attaques par messages de harponnage

De manière générale, les messages électroniques d'hameçonnage (*phishing*) constituent des attaques exploratoires lancées par des cybercriminels dans le but d'inciter des utilisateurs à leur révéler des données confidentielles, par exemple des informations d'identification personnelle ou encore des données d'authentification pour l'accès au réseau. Ces attaques ouvrent la voie à d'autres intrusions sur le réseau. L'hameçonnage recourt le plus souvent à l'ingénierie sociale et à des leurres pour amener la victime à ouvrir des documents joints, à cliquer sur des liens incorporés ou à divulguer des informations confidentielles.

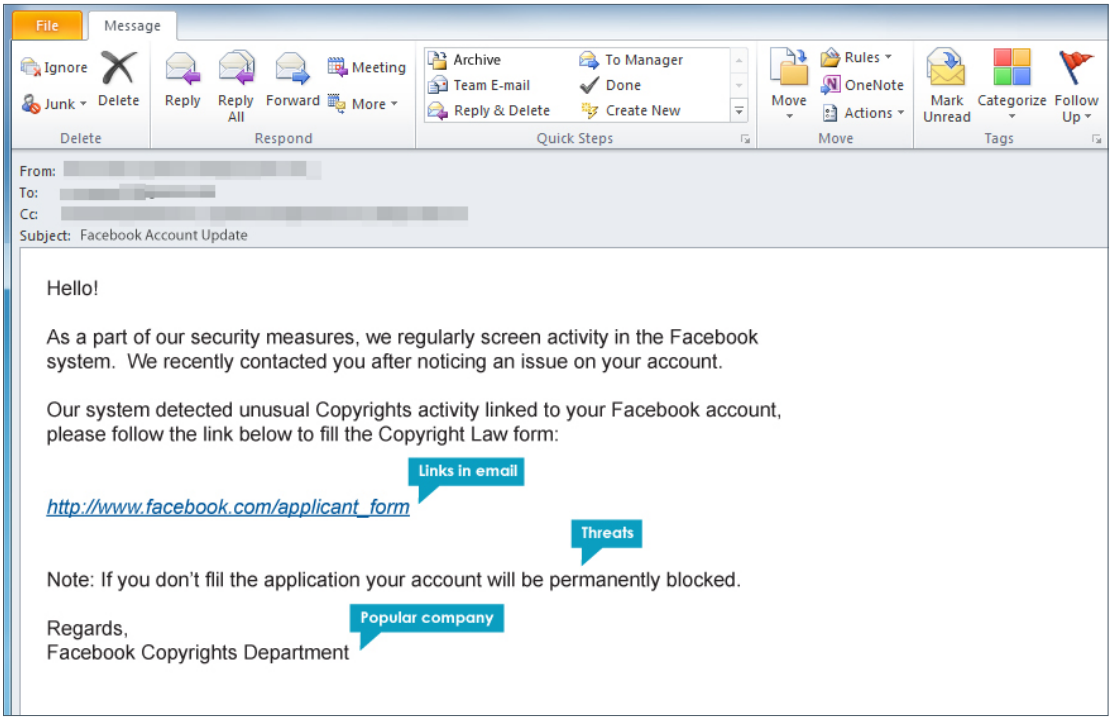

Figure 1 — Techniques courantes utilisées dans les messages de hameçonnage (*phishing*)

Le harponnage (*spear phishing*) est une version plus ciblée du hameçonnage. Il combine des techniques variées, notamment la segmentation des victimes, l'usurpation d'identité de l'expéditeur et la personnalisation des messages, pour contourner les mécanismes de filtrage de la messagerie et inciter des utilisateurs précis à cliquer sur un lien ou à ouvrir une pièce jointe. Là où une attaque par hameçonnage couvrira l'ensemble d'une base de données d'adresses électroniques, le harponnage va viser des utilisateurs spécifiques au sein d'entreprises soigneusement choisies. Grâce aux informations recueillies sur les réseaux sociaux, par exemple, la personnalisation et l'usurpation d'identité employées dans les messages de harponnage sont parfois extrêmement fines et convaincantes. Lorsqu'il clique sur un lien ou ouvre un fichier joint, l'utilisateur ouvre une brèche dans le réseau. Il ne reste plus aux pirates qu'à s'y engouffrer pour lancer une attaque ciblée avancée.

Il faut envisager les attaques par harponnage dans le contexte plus large des attaques ciblées avancées, également appelées menaces persistantes avancées. A l'heure actuelle, des cybercriminels (et certains États) très compétents lancent des attaques associées à des menaces persistantes avancées, exploitant pour ce faire des logiciels malveillants sophistiqués et des attaques soutenues, multivectorielles et multiphases pour atteindre leur objectif. Il s'agit, dans la plupart des cas, d'obtenir un accès durable aux réseaux, aux données et aux ressources sensibles d'une entreprise.

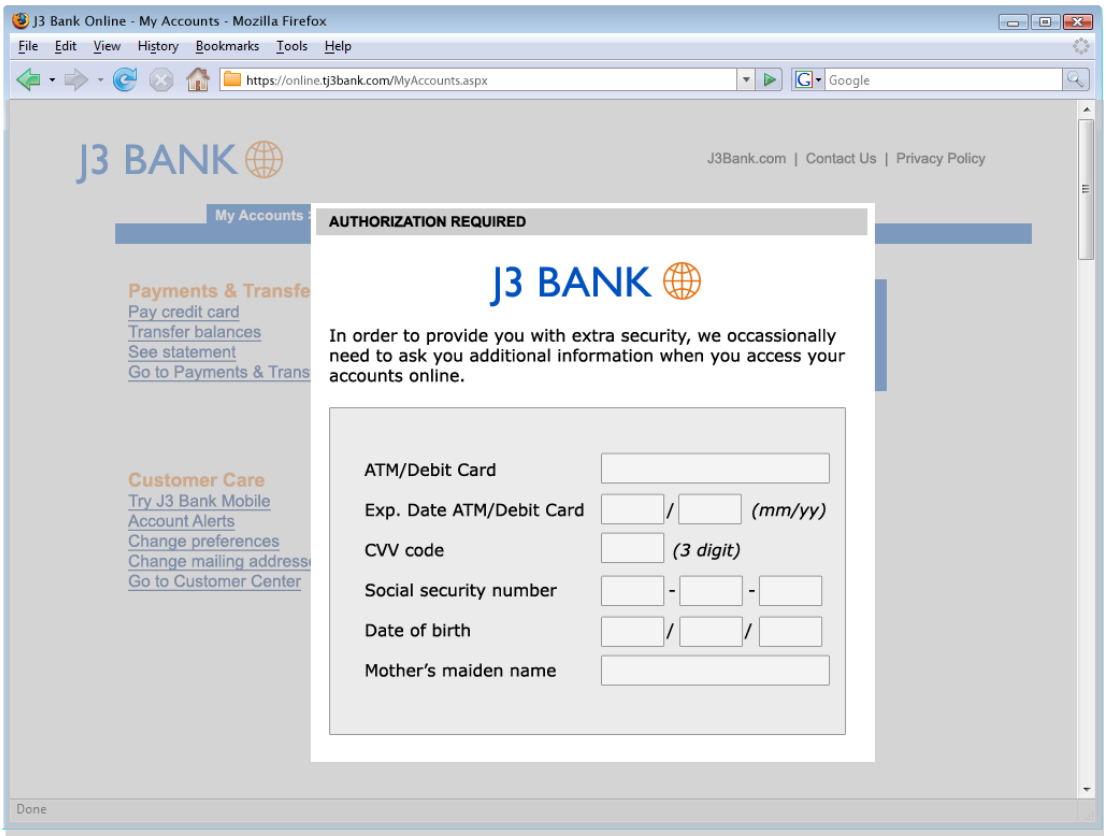

Figure 2 — Site Web falsifié pour inciter les utilisateurs à révéler leurs données d'authentification et informations d'identification personnelle

La raison de la progression des attaques par harponnage : leur efficacité

Les attaques ciblées avancées employant le harponnage ne constituent pas des cas isolés. Au contraire, elles reflètent une évolution radicale dans l'approche des cybercriminels. Ceux-ci délaissent peu à peu les attaques massives par hameçonnage pour mener des actions de harponnage plus ciblées, à plus petite échelle, ces dernières ayant démontré leur extrême efficacité.

Voici ce qu'une étude récente[1] met en évidence :

- Entre 2010 et 2011, les revenus annuels liés aux attaques massives par message électronique ont chuté de 1,1 milliard à 500 millions de dollars. Dans le même intervalle, le volume de spam est passé de 300 milliards à 40 milliards de messages par jour.
- Au cours de la même période, le nombre d'attaques par harponnage a triplé.
- Le taux d'ouverture des messages de harponnage a atteint 70 %, contre seulement 3 % pour les e-mails de spam distribués en masse. De plus, 50 % des destinataires qui ont ouvert les messages de harponnage ont ensuite cliqué sur les liens intégrés : un taux 10 fois supérieur à celui associé aux mailings de masse.
- Comparés aux e-mails à diffusion massive, les messages de harponnage coûtent 20 fois plus cher par individu ciblé. Toutefois, le retour moyen pour chaque victime de harponnage est 40 fois supérieur à celui de l'hameçonnage.
- Une campagne de harponnage comprenant 1 000 messages est susceptible de générer 10 fois plus de revenus qu'un mailing d'hameçonnage visant un million d'individus.

Exemples et caractéristiques de messages de harponnage

Voici quelques caractéristiques essentielles des attaques ciblées avancées par harponnage :

- **Menace combinée/multivectorielle.** Le harponnage utilise une combinaison de mécanismes d'usurpation d'identité, d'exploits d'applications « zero-day », d'URL dynamiques et de téléchargements à l'insu de l'utilisateur pour contourner les défenses traditionnelles.
- **Exploitation de vulnérabilités « zero-day ».** Les attaques avancées par harponnage exploitent les vulnérabilités « zero-day » des navigateurs, des plug-ins et des applications pour poste de travail dans le but de compromettre les systèmes.
- **Attaque multiphase.** L'exploitation initiale des systèmes constitue la première étape d'une menace persistante avancée comprenant d'autres phases, telles que des communications sortantes effectuées par des logiciels malveillants, des téléchargements de fichiers binaires et l'exfiltration de données.
- **Absence des caractéristiques du spam.** Les messages de harponnage sont des menaces ciblées, souvent individualisées, qui ne ressemblent aucunement au spam traditionnel diffusé en masse. Il est donc probable que les filtres basés sur la réputation ne détectent pas la vraie nature de ces messages, ce qui réduit l'éventualité qu'ils soient interceptés par les filtres antispam.

1 http://www.scmagazine.com/crooks-opt-for-spear-phishing-despite-higher-upfront-cost/article/206586/

Etude du cas RSA : harponnage et menace persistante avancée

Les attaques qui ont visé RSA, la division sécurité d'EMC Corp., en 2011 montrent clairement la façon dont le harponnage peut ouvrir la voie à une attaque dévastatrice, à l'impact considérable tant pour l'entreprise que pour ses clients.

L'assaut a été lancé à l'aide d'attaques par harponnage au cours desquelles des utilisateurs ciblés ont reçu un e-mail avec, en pièce jointe, un fichier Excel exploitant une brèche « zero-day » d'Adobe Flash. De toute évidence, l'attaque était non seulement confinée à RSA, mais elle visait exclusivement quatre utilisateurs, les destinataires du message malveillant. Il a suffi que l'un d'entre eux ouvre le message électronique et le fichier joint pour qu'un cheval de Troie soit téléchargé sur son ordinateur.

Cette attaque par harponnage faisait partie d'une attaque ciblée avancée bien plus complexe. Une fois le logiciel malveillant installé sur l'ordinateur de la victime, les cybercriminels ont pu parcourir le réseau de l'entreprise, recueillir les données d'identification des administrateurs et, en fin de compte, accéder à un serveur hébergeant des informations propriétaires relatives à la plate-forme d'authentification à deux niveaux SecurID.

Les pirates n'en sont pas restés là. Il ne s'agissait en fait que d'une première étape, leur objectif ultime étant de s'infiltrer dans les réseaux des clients de RSA, en particulier ceux appartenant au secteur industriel lié à la défense nationale américaine. Ils ont ensuite utilisé les données dérobées pour cibler de nombreux clients SecurID importants, tels que les sous-traitants du Pentagone Lockheed Martin, L-3 et Northrop Grumman.

Le principal enseignement à tirer est qu'une attaque en apparence rudimentaire peut se révéler la première étape d'une série de forfaits sophistiqués et coordonnés, aux effets potentiellement dévastateurs. Il faut également retenir qu'une attaque ciblée avancée contre des ressources pourtant non stratégiques ou des employés dépourvus de rôles ou de permissions sensibles peut malgré tout donner accès à des informations vitales et avoir de graves conséquences.

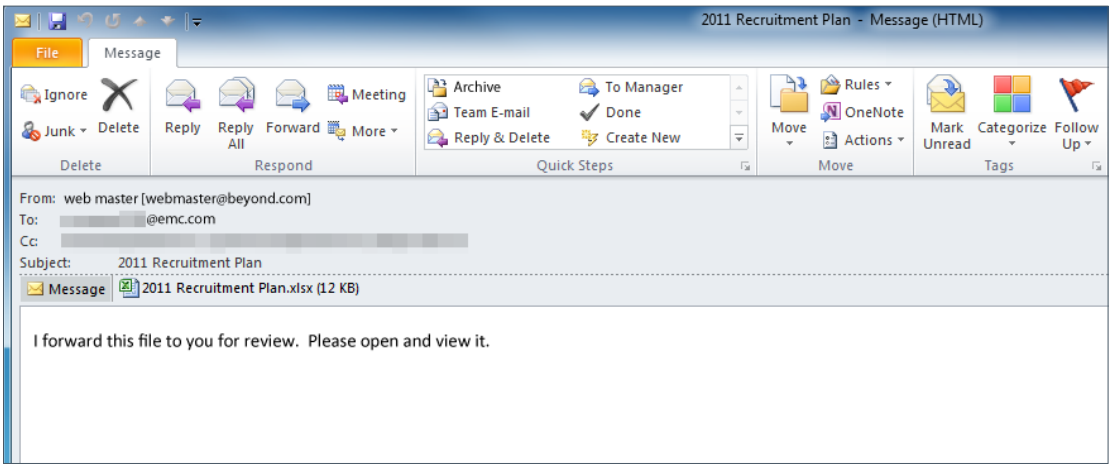

Figure 3 — Message de harponnage ayant servi à lancer une menace persistante avancée contre RSA

La solution : une protection contre les menaces de nouvelle génération

À l'heure actuelle, les entreprises ont besoin d'un système de sécurisation de nouvelle génération, capable de détecter et de bloquer les techniques d'attaque ciblée avancée telles que le harponnage. La solution FireEye ne manque pas d'atouts à cet égard.

Solution cohérente et intégrée pour la protection contre tous les vecteurs de menaces

FireEye offre aux entreprises une protection intégrée contre les vecteurs de menaces utilisés par les attaques ciblées avancées, à savoir la messagerie électronique et le Web. Ainsi, pour être en mesure de contrer une tentative de harponnage, la solution doit pouvoir identifier en temps réel une attaque via le Web, remonter jusqu'au message à l'origine de l'attaque et réaliser les analyses requises pour déterminer si d'autres utilisateurs ont été visés au sein de l'entreprise. Seul ce type de réponse en temps réel permet de lutter efficacement contre les attaques ciblées avancées.

Les solutions FireEye permettent aux entreprises d'analyser en temps réel les URL et les pièces jointes des messages électroniques ainsi que les objets Web afin de déterminer s'ils sont malveillants. Cette fonctionnalité est essentielle pour bloquer les tentatives de harponnage et autres attaques par messagerie dans la mesure où les techniques de type « zero-day » contournent facilement les mécanismes d'analyse basés sur la réputation ou sur des signatures. Par ailleurs, pour assurer la protection de leurs réseaux, les entreprises ont besoin de systèmes capables d'étendre l'inspection à différents protocoles, et ce dans toute la pile de protocoles, y compris la couche réseau, les systèmes d'exploitation, les applications, les navigateurs et les plug-ins tels que Flash.

Protection dynamique sans signatures pour neutraliser les exploits « zero-day »

Plutôt que de se contenter de comparer des segments de code à des signatures ou de se fier à l'évaluation de la réputation, les solutions FireEye analysent de façon dynamique et en temps réel les URL et les pièces jointes des messages électroniques à la recherche d'exploits. Le fait que l'analyse ne repose pas sur des signatures est essentiel pour contrer les techniques d'attaques avancées dans la mesure où toutes ont pour point de départ un exploit « zero-day ». La détection de ces exploits permet de neutraliser les logiciels malveillants avancés, qu'ils soient imbriqués dans des pièces jointes ou hébergés sur des domaines dynamiques à l'évolution rapide.

Protection contre l'installation de code malveillant et blocage des rappels

En plus de détecter les exploits, FireEye peut identifier si des pièces jointes ou d'autres objets suspects sont malveillants. Même les communications liées aux rappels sont inspectées. Pour ce faire, FireEye surveille en temps réel les communications hôte sortantes pour plusieurs protocoles et vérifie si elles indiquent la présence d'un système infecté sur le réseau. Les rappels peuvent alors être bloqués en fonction des caractéristiques propres aux protocoles de communication utilisés, plutôt que sur la base de l'adresse IP de destination ou du nom de domaine.

Dès lors qu'un code malveillant et ses communications sont marqués, les ports de communication, les adresses IP et les protocoles doivent être bloqués de façon à empêcher les transmissions de données sensibles. Cela permet de prévenir tout téléchargement ultérieur de charges actives binaires malveillantes et, ainsi, la propagation de l'infection dans toute l'entreprise.

Investigations numériques et renseignements sur les menaces pertinents et exploitables

Il est essentiel de pouvoir tirer pleinement parti des informations recueillies au cours de l'analyse détaillée d'un logiciel malveillant avancé. FireEye permet à ses clients d'exploiter ces informations à diverses fins :

- Les systèmes FireEye prennent l'empreinte numérique du code malveillant pour générer automatiquement des données de protection et identifier les systèmes compromis, empêchant ainsi l'infection de se propager.
- Les experts en investigations numériques peuvent étudier les fichiers un à un au moyen de tests hors ligne automatisés afin de vérifier la nature malveillante du code et de disséquer celui-ci.
- Les informations sont partagées par le biais de systèmes de renseignements unifiés pour tenir les experts et les entreprises informés.

Conclusion

Malgré les quelque 20 milliards de dollars investis chaque année dans la sécurité informatique, les attaques multivectorielles multiphases parviennent à infiltrer les réseaux avec une efficacité redoutable. Parmi ces attaques ciblées avancées, le harponnage connaît un essor considérable en raison de son taux de réussite exceptionnel. Tant que les entreprises se contenteront de leur niveau de protection actuel, inopérant face aux techniques de harponnage, les cybercriminels continueront d'exploiter ce type d'attaque. Seule une solution de protection contre les menaces de nouvelle génération, capable d'intervenir à chaque phase d'une attaque et de contrer de nombreux vecteurs de menaces, peut mettre les entreprises à l'abri de ces attaques ciblées avancées.

Les solutions FireEye offrent une telle protection de nouvelle génération. En effet, elles intègrent la protection de la messagerie et de l'environnement Web, bloquent les fichiers binaires malveillants à l'entrée et les rappels malveillants et exécutent un code spécifique de manière dynamique pour détecter les exploits « zero-day » sans utiliser de signatures. Grâce à FireEye, les entreprises disposent de vues contextuelles en temps réel sur les menaces véhiculées par le Web et la messagerie électronique. Une attaque Web « zero-day » peut ainsi être détectée en temps réel et bloquée. Il est ensuite possible de remonter au message de harponnage d'origine afin de déterminer si d'autres utilisateurs ont été pris pour cibles au sein de l'entreprise. Cette analyse de sécurité sensible au contexte constitue le seul moyen d'obtenir des informations précises et exploitables sur les attaques ciblées avancées et sur la manière de les contrer.

À propos de FireEye, Inc.

FireEye propose les meilleures solutions du marché pour neutraliser les attaques ciblées avancées qui combinent des logiciels malveillants sophistiqués, des exploits « zero-day » et les tactiques des menaces persistantes avancées. Les solutions FireEye complètent les pare-feux traditionnels et de nouvelle génération, les systèmes IPS, les antivirus et les passerelles, des outils qui à eux seuls sont incapables de repousser les menaces évoluées, laissant ainsi des brèches de sécurité dans les réseaux. FireEye propose en outre la seule solution en mesure de détecter et de bloquer les attaques exploitant le Web et la messagerie électronique comme vecteurs ainsi que les logiciels malveillants latents résidant sur les partages de fichiers. Cette solution couvre toutes les phases du cycle de vie des attaques au moyen d'un moteur sans signatures qui utilise l'analyse dynamique pour détecter les menaces « zero-day ». Établi à Milpitas, en Californie, FireEye est soutenu par des partenaires financiers de premier plan, dont Sequoia Capital, Norwest Venture Partners et Juniper Networks.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | france@FireEye.com | www.FireEye.com