ATTAQUES DE SPEAR PHISHING

LES RAISONS DE LEUR SUCCÈS ET LES MOYENS DE LES CONTRER

FireEye

LIVRE BLANC

LE PAYSAGE DES MENACES A CONNU RÉCEMMENT UN VIRAGE SPECTACULAIRE. LES ATTAQUES DE SPAM DE GRANDE AMPLEUR ONT FAIT PLACE À DES CAMPAGNES CIBLÉES DE SPEAR PHISHING PAR E-MAIL, AVEC POUR CONSÉQUENCE D'IMPORTANTS PRÉJUDICES EN TERMES FINANCIERS, OPÉRATIONNELS ET D'IMAGE DE MARQUE POUR LES ENTREPRISES DU MONDE ENTIER.

Bon nombre des cyberattaques qui ont récemment défrayé la chronique — et pris pour cible grandes banques, groupes média et même éditeurs de solutions de sécurité — ont commencé par un simple clic sur un message de spear phishing.

Si les attaques de spear phishing ont la cote, c'est avant tout parce qu'elles sont efficaces. Les dispositifs de sécurité traditionnels sont tout simplement incapables de les détecter et de les bloquer. Du point de vue du cybercriminel, le spear phishing est le vecteur idéal pour une longue série de manœuvres illicites. De plus en plus, les pirates ciblent les cadres dirigeants ou d'autres postes à responsabilités, les incitant par la ruse à activer un malware qui leur assurera un accès à l'environnement de leurs entreprises. Il peut s'agir d'un ransomware qui crypte les données de l'entreprise, puis exige le paiement d'une rançon pour déverrouiller les fichiers. Le malware introduit peut être un cheval de Troie servant à la reconnaissance de l'environnement cible, par exemple des services bancaires ou des points de vente dans les secteurs du commerce de détail et de l'hôtellerie. Les cadres dirigeants visés par ce type de menace sont généralement des décideurs à des postes clés : directeurs financiers, vice-présidents, directeurs. Les messages de spear phishing contiennent suffisamment de détails exacts pour berner même des experts en sécurité chevronnés.

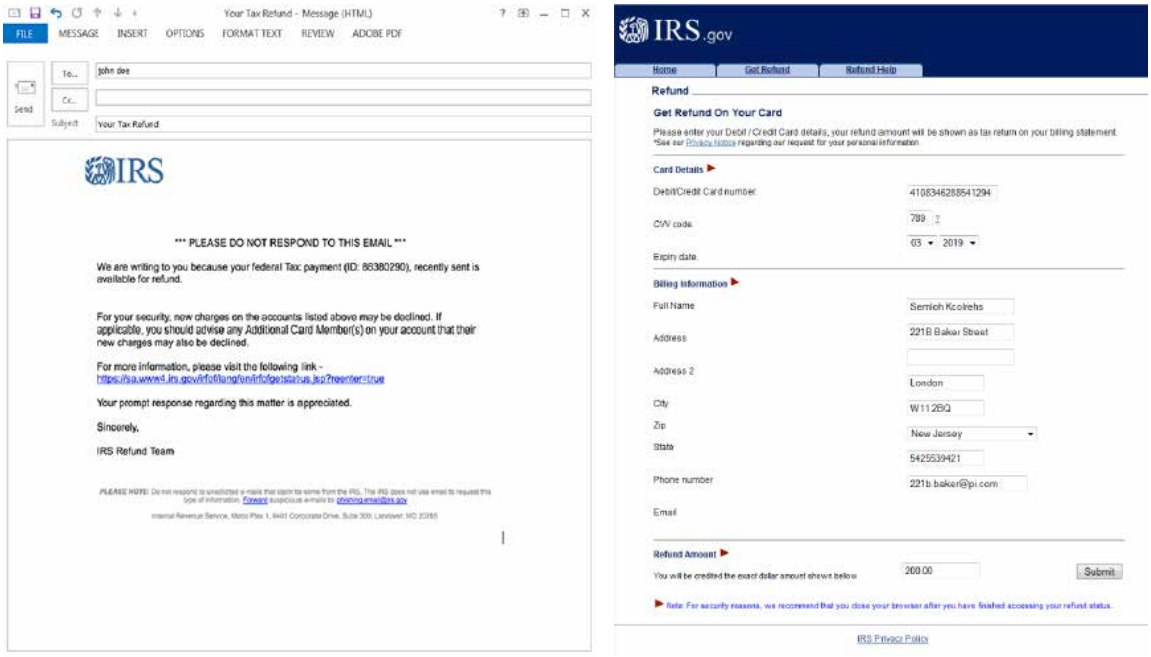
L'ESSOR DES ATTAQUES PAR MESSAGES DE SPEAR PHISHING

Les e-mails de phishing constituent des attaques exploratoires lancées dans le but d'inciter des internautes à révéler des données confidentielles, telles que des informations d'identification personnelle (PII) ou des identifiants réseau. Ces attaques ouvrent la voie à d'autres intrusions sur tout réseau auquel la victime a accès. Le phishing recourt généralement à l'ingénierie sociale et à des artifices techniques pour amener l'utilisateur à ouvrir des documents joints, cliquer sur des liens incorporés ou divulguer des informations confidentielles.

Les attaques de spear phishing sont plus ciblées. Les cyberpirates qui y ont recours segmentent leurs cibles, personnalisent les e-mails, usurpent l'identité d'expéditeurs soigneusement choisis et emploient diverses autres techniques pour contourner les systèmes de protection traditionnels. Leur objectif : inciter leurs cibles à cliquer sur un lien ou ouvrir une pièce jointe. Là où une attaque de phishing couvrira l'ensemble d'une base de données d'adresses électroniques, le spear phishing va viser des utilisateurs précis au sein d'entreprises triées sur le volet, avec une mission précise. Grâce aux informations personnelles recueillies sur les réseaux sociaux, les attaquants peuvent rédiger des messages très convaincants. Lorsque la cible clique sur le lien ou ouvre la pièce jointe, le pirate prend pied dans le réseau et peut mener à bien sa mission illicite.

Le spear phishing est le principal vecteur des menaces APT (Advanced Persistent Threats). À l'heure actuelle, des cybercriminels et certains États lancent des attaques ciblées au moyen de malwares sophistiqués et de campagnes nourries, multivectorielles et multiphases. Leur but consiste à obtenir un accès à long terme aux réseaux, données et ressources sensibles d'une organisation.

FIGURE 1 – TECHNIQUES COURANTES UTILISÉES DANS LES MESSAGES DE SPEAR PHISHING.

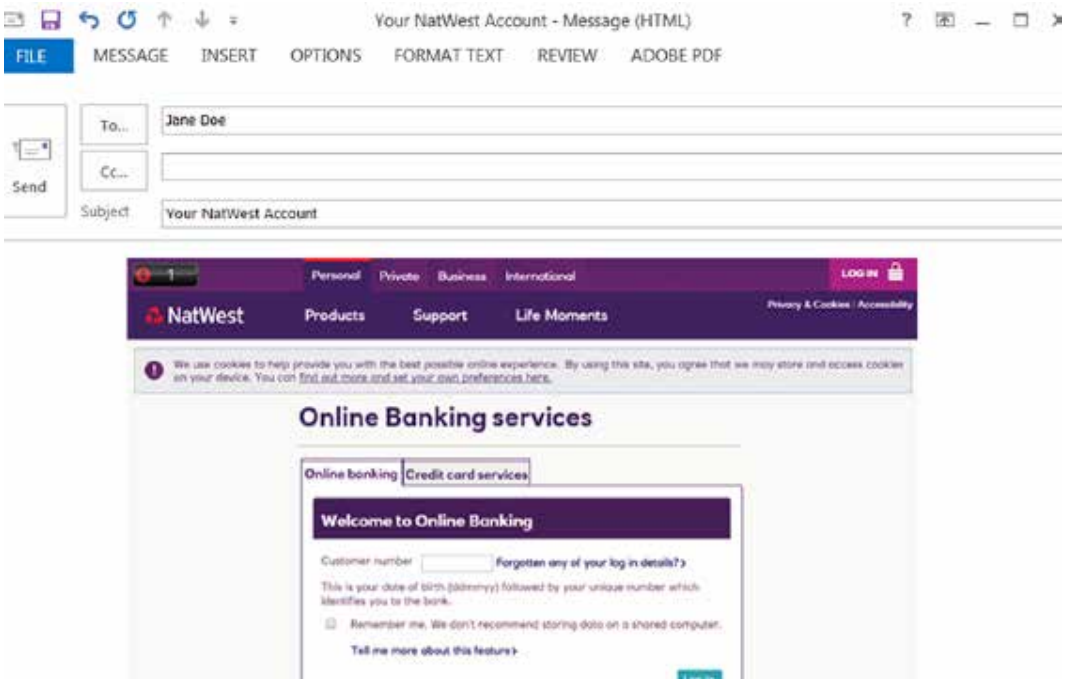


UNE EFFICACITÉ REDOUTABLE

Les attaques APT recourant au spear phishing reflètent une évolution radicale dans la stratégie des cyberpirates. Il n'est plus nécessaire de lancer des campagnes de spam à grande échelle. La rentabilité des attaques APT est bien supérieure moyennant une bonne préparation, un ciblage judicieux et des messages bien conçus, qui usurpent l'identité d'un expéditeur légitime de façon crédible (fig. 2).

84 % des entreprises interrogées lors d'une étude ont avoué avoir subi une attaque de spear phishing réussie en 2015. L'impact moyen d'une attaque de spear phishing fructueuse : 1,6 million de dollars. Les victimes ont vu le cours de leurs actions chuter de 15 %[1].

FIGURE 2 — SITE WEB FALSIFIÉ POUR INCITER LES UTILISATEURS À RÉVÉLER LEURS IDENTIFIANTS ET INFORMATIONS D'IDENTIFICATION PERSONNELLE (PII)



L'impact moyen d'une attaque de spear phishing fructueuse : 1,6 million de dollars.

[1] Vanson Bourne, « The Impact of Spear Phishing », 2016

Le spear phishing utilise une combinaison de mécanismes d'usurpation d'identité, d'URL dynamiques et de téléchargements drive-by pour contourner les défenses traditionnelles.

EXEMPLES ET CARACTÉRISTIQUES DE MESSAGES DE SPEAR PHISHING

Une attaque de spear phishing peut présenter une ou plusieurs des caractéristiques suivantes :

- **Menace combinée ou multivectorielle —** Le spear phishing utilise une combinaison de mécanismes d'usurpation d'identité, d'URL dynamiques et de téléchargements drive-by pour contourner les défenses traditionnelles.
- **Exploitation des vulnérabilités zero-day —** Les attaques avancées par spear phishing exploitent les vulnérabilités zero-day des navigateurs, des plug-ins et des applications pour poste de travail.
- **Attaque multiphase —** L'infiltration initiale constitue la première étape d'une attaque APT qui comprend plusieurs phases, telles que des communications sortantes initiées par les malwares, des téléchargements de fichiers binaires et l'exfiltration de données.
- **Des e-mails frauduleux bien conçus —** Les messages de spear phishing sont généralement rédigés de façon à cibler des individus précis. Ils ne ressemblent donc pas aux e-mails de spam diffusés en masse qui inondent Internet. Cela explique qu'ils ne soient pas détectés par les filtres de réputation et antispam, ce qui rend inopérants les dispositifs traditionnels de protection.

UNE AFFAIRE PERSONNELLE

L'année dernière, Mandiant, une entreprise FireEye, est intervenu sur plusieurs attaques ciblées lors desquelles des informations d'identification personnelle (PII) ont été volées par des cyberpirates liés à la Chine. Le volume des données dérobées laisse supposer que l'objectif était la collecte massive de données PII, et pas uniquement celles d'individus précis.

Mandiant n'avait jamais observé auparavant de tendance au vol de données PIII sans discrimination par des attaquants chinois. Les experts Mandiant avaient connaissance de quelques cas isolés de vols de données PII en marge de vols de données de plus grande envergure. Il peut arriver par exemple qu'un cybercriminel exfiltre toutes les données d'un serveur de fichiers, y compris des informations d'identification personnelle sans intérêt particulier pour l'attaquant.

L'année dernière, la situation a changé. Mandiant a en effet mené plusieurs investigations sur des vols d'énormes volumes de données PII, vraisemblablement orchestrés depuis la Chine. Plusieurs secteurs ont été touchés, dont les soins de santé, le tourisme, les services financiers et les organismes publics. Mandiant soupçonnait au départ que les pirates visaient en particulier les dossiers médicaux et informations de carte de crédit, mais n'avait pas trouvé de preuves pour étayer cette hypothèse. Les experts Mandiant ont cependant observé que les informations ciblées et exfiltrées pouvaient être utilisées pour vérifier les identités des personnes concernées : numéros de sécurité sociale, noms de jeune fille de la mère, dates de naissance, noms des anciens employeurs, associations de questions/réponses d'identification, etc.

UN CAS RÉEL

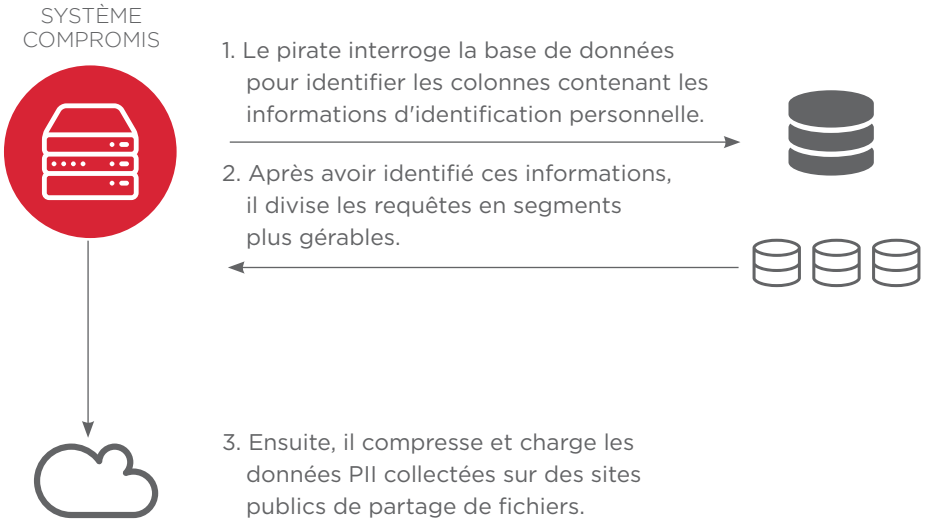
Un attaquant basé en Chine fait main basse sur une quantité massive d'informations d'identification personnelle (PII)

L'entrée en matière : un e-mail de spear phishing incitant un collaborateur à cliquer sur un lien vers du contenu malveillant. L'activation du lien a provoqué le téléchargement d'une backdoor, qui a octroyé aux attaquants un accès à l'environnement de la cible. Après s'être infiltrés, les pirates ont focalisé leurs activités de reconnaissance sur l'identification des bases de données contenant un maximum d'informations d'identification personnelle.

Ensuite, ils ont accédé aux bases de données en identifiant les DBA et leurs ordinateurs via l'annuaire Active Directory de la victime. Pour ce faire, ils ont recherché les appartenances aux groupes Active Directory avec le mot clé « database ». Ils se sont ensuite déplacés latéralement vers ces systèmes et ont extrait des documents leur permettant d'identifier les noms, serveurs et identifiants des bases de données.

Les attaquants maîtrisaient manifestement les systèmes de bases de données Microsoft, Teradata et Oracle, ainsi que les passerelles transactionnelles utilisées pour y accéder. Une fois en possession des informations nécessaires, ils ont systématiquement testé l'authentification et inventorié les bases de données. Ils ont ensuite recherché dans les tables des bases les colonnes dont les noms indiquaient des contenus sensibles, comme des numéros de sécurité sociale. Une fois ces informations identifiées, ils en ont extrait les champs pour chaque enregistrement dans les bases de données ciblées. Bilan des informations collectées : numéros de sécurité sociale, noms de jeune fille de la mère et dates de naissance. En raison du volume de données extraites, les pirates ont :

1. Extrait les informations par segments (entre 100 000 et 1 000 000 d'enregistrements à la fois)
2. Compressé les informations sous forme de fichiers archives scindés en plusieurs parties
3. Chargé les fichiers compressés contenant les données PII sur des sites de partage



UNE MEILLEURE SÉCURITÉ DE LA MESSAGERIE ÉLECTRONIQUE

À l'heure actuelle, les entreprises ont besoin d'une solution de sécurité de la messagerie électronique innovante, capable de détecter et bloquer automatiquement les attaques ciblées avancées qui ont recours au spear phishing, à la collecte d'identifiants ou à l'usurpation d'identité. La solution FireEye de sécurité de la messagerie électronique est plus efficace que les solutions standard et assure une protection proactive contre les attaques par e-mail.

Solution cohérente et intégrée contre tous les vecteurs de menaces

Pour combattre efficacement les cyberattaques actuelles, les entreprises ont besoin d'une protection multivectorielle. La messagerie électronique et les réseaux, par exemple, sont souvent utilisés de concert dans les attaques avancées. La solution doit pouvoir identifier en temps réel une attaque via le Web et remonter jusqu'au message à l'origine de l'attaque pour déterminer si d'autres utilisateurs ont été visés au sein de l'entreprise. Seul ce type de réponse défensive en temps réel permet de stopper efficacement les attaques ciblées avancées. Les entreprises peuvent protéger leurs réseaux plus efficacement avec des 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.

Protection dynamique pour neutraliser les exploits zero-day

Les solutions FireEye permettent d'analyser en temps réel les URL et les pièces jointes des e-mails ou encore les objets Web afin de déterminer s'ils sont malveillants. Cette fonctionnalité est essentielle pour bloquer les tentatives de spear phishing et autres attaques par e-mail dans la mesure où les techniques inédites échappent facilement aux dispositifs de sécurité basés sur la réputation ou les signatures. La détection de ces menaces permet à FireEye de neutraliser les malwares 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 le code d'exploits, FireEye peut identifier si des pièces jointes ou d'autres objets suspects sont malveillants. Toutes les communications de rappel sont inspectées, à la recherche d'activités malveillantes. 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 qu'en fonction 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 sont bloqués de façon à empêcher les transmissions de données sensibles. Cela empêche les attaquants de télécharger d'autres charges actives binaires malveillantes et stoppe ainsi la propagation de l'infection dans toute l'entreprise.

Cyberveille et analyse forensique pertinentes et exploitables

Les informations collectées par l'analyse minutieuse de malwares avancés peuvent être utilisés de diverses façons.

- Les systèmes FireEye peuvent prendre 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 analystes forensiques peuvent étudier les fichiers au moyen de tests hors ligne automatisés, afin de vérifier la nature malveillante du code et de le disséquer.
- Les experts et les entreprises peuvent se connecter à des systèmes de cyberveille unifiés pour obtenir des analyses critiques des menaces actuelles.

DÉTECTION ET BLOCAGE DU SPEAR PHISHING

Malgré les quelque 20 milliards de dollars investis chaque année dans la sécurité informatique, les attaques multivectorielles et multiphases ciblées parviennent à infiltrer les réseaux avec une efficacité redoutable. La majorité de ces attaques commencent par un e-mail malveillant. Les e-mails d'ingénierie sociale, tels que les messages de spear phishing, sont une arme de choix en raison de leur grande efficacité. Les criminels continueront à y avoir recours aussi longtemps que les entreprises conserveront les mêmes mécanismes de sécurité, incapables de les détecter. Seule une solution de protection contre les menaces globale, capable d'intervenir à chaque phase d'une attaque et de contrer de nombreux vecteurs de menaces, peut bloquer ces attaques ciblées avancées.

Les solutions FireEye de sécurité de la messagerie offrent des options de déploiement souples : sur site, dans le cloud et hybride. Elles assurent la protection globale de la messagerie électronique nécessaire pour bloquer les attaques ciblées avancées et préserver vos collaborateurs, données et ressources. La solution FireEye de sécurité de la messagerie électronique dispose d'un accès intégré à une cyberveille contextuelle mondiale — qui s'appuie sur des millions de capteurs et sur l'analyse de milliards d'événements. Ces nombreuses fonctionnalités font de la solution FireEye de sécurité de la messagerie électronique le meilleur moyen de détecter et bloquer efficacement des attaques par e-mail dévastatrices.

Pour en savoir plus sur FireEye, consultez notre site :
www.fireeye.fr/products/ex-email-security-products.html

FireEye, France | 4, place de la Défense, Paris La Défense Cedex 92974 | +33 1 58 58 01 76 | france@FireEye.com | www.FireEye.fr
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | www.FireEye.com

www.FireEye.fr