# Les 3 cyberattaques les plus nuisibles et comment les arrêter

**Un entretien avec Scott Plichta**

**Scott Plichta**

Responsable de la sécurité des systèmes d'information chez CSC

# Les 3 cyberattaques les plus nuisibles et comment les arrêter

## Un entretien avec Scott Plichta

Selon l'édition 2016 de l'enquête « Cost of Data Breach Study: Global Analysis », menée par le Ponemon Institute, la violation des données a été, en 2016, la plus grande menace pour la sécurité des entreprises dans le monde, entraînant une perte financière moyenne de 4 millions de dollars par entreprise touchée. Cela représente une augmentation de 29 % du coût total d'une violation de données depuis 2013.

Avec cette augmentation du nombre des attaques, la sécurisation des ressources en ligne de votre entreprise doit être la grande priorité de tout responsable informatique. En tant que partenaire de confiance des trois premières (et de plus de la moitié des 100 premières) marques mondiales répertoriées dans le classement Interbrand®, la société **CSC®** se doit bien évidemment de tout mettre en oeuvre pour assurer sa sécurité. Basée aux États-Unis, CSC propose à une clientèle internationale une gamme de services de gestion de noms de domaine, de protection des marques et de sécurité sur Internet. Afin d'élargir les perspectives, nous nous sommes entretenus avec Scott Plichta, responsable de la sécurité des systèmes d'information chez CSC, afin de profiter de ses recommandations sur les meilleures façons de protéger ses actifs numériques en 2015.

***Journaliste***

**Qui sont les principaux auteurs de cyberattaques ? Que ciblent-ils ? Comment s'y prennent-ils ?**

***Scott***

On compte en fait trois grandes catégories. Il y a tout d'abord les « hacktivistes », par exemple l'Armée électronique syrienne et Anonymous, qui lancent des attaques à travers le monde pour faire entendre des revendications politiques ou sociales. Il y a ensuite les cybercriminels, dont les actes sont motivés par l'appât du gain financier. Et il y a enfin les États-nations, dont les actions sont généralement liées à l'espionnage. Les États-nations ciblent certaines organisations ou industries spécifiques, en attirant des individus vers des sites Web à partir desquels des logiciels malveillants seront subrepticement téléchargés sur leurs ordinateurs. Les hacktivistes ont la particularité de ne pas avoir d'ennemi spécifiquement défini. Ces personnes cherchent avant tout à délivrer un message. Et un tel message peut nuire à la réputation d'une entreprise et avoir de sérieuses répercussions financières, selon le temps qu'il faudra à celleci pour reprendre le contrôle des systèmes dont la sécurité a été compromise.

Les cybercriminels tendent à se focaliser sur le vol pur et simple, recherchant notamment des informations de cartes de crédit pour faire ensuite des achats frauduleux. Ils visent plus particulièrement les consommateurs, ainsi que les entreprises qui proposent des biens de consommation. On sait enfin que certains États-nations emploient des tactiques telles que le « spear phishing » (harponnage) ou les attaques de type « watering hole » (attaque de point d'eau), en se faisant passer pour des personnes ou des sites Web de confiance pour infecter les ordinateurs des victimes au moyen de logiciels malveillants, une fois qu'elles ont visité un site Web ciblé.

« Il est vraiment important de tout mettre en oeuvre pour se prémunir contre de telles escroqueries. La bonne nouvelle, c'est que les entreprises ont pour cela beaucoup de moyens à leur disposition. »

### *Journaliste*

**À quels types de cyberattaques les entreprises sont-elles confrontées aujourd'hui ? Et comment les entreprises peuvent-elles protéger leur propre organisation ainsi que leurs clients ?**

### *Scott*

Les attaques de type « DNS Spoofing » (usurpation d'adresse IP) et DDoS constituent des menaces importantes pour les entreprises et leurs clients. Mais la plus grande menace, à l'heure actuelle, reste le phishing, et notamment le spear phishing, c'est-à-dire une tentative de phishing personnalisée qui utilise des informations collectées sur une personne ou une entreprise spécifique.

Les actes de phishing ont pour but d'infiltrer les organisations afin d'y voler des informations à des fins politiques ou financières. Ils existent déjà depuis un certain temps. Leur longévité s'explique en partie par le fait que la conception des e-mails frauduleux gagne sans cesse en sophistication ; les messages semblent donc de plus en plus convaincants aux personnes ciblées. Le spear phishing est particulièrement efficace dans la mesure où le consommateur peut penser que l'e-mail provient d'une personne qu'il connaît et en laquelle il a confiance. La disponibilité des informations sur les réseaux sociaux facilite fortement la recherche des informations nécessaires à la conception d'une attaque de spear phishing convaincante.

Les pratiques de phishing, début 2016, ont atteint le niveau le plus élevé observé par l'APWG (Anti Phishing Working Group), depuis le début de son activité de surveillance, en 2004.

Il est donc vraiment important de tout mettre en oeuvre pour se prémunir contre de telles escroqueries. La bonne nouvelle, c'est que les entreprises ont pour cela beaucoup de moyens à leur disposition. Je leur recommande tout d'abord d'avoir recours à la fois à l'authentification unique et à l'authentification à deux facteurs. CSC prend en charge l'authentification à deux facteurs avec le système Duo Security, que nous utilisons pour assurer la sécurité de nos systèmes internes. Les services d'authentification à deux facteurs renforcent la protection contre le phishing car ils aident à faire en sorte que seules les personnes autorisées puissent accéder à des ressources numériques spécifiques. S'il ne fallait retenir qu'un seul enseignement de cet entretien, ce serait que le déploiement de l'authentification à deux facteurs est la solution la plus simple et la plus rentable, et qui assure le meilleur retour sur investissement.

Un autre élément à prendre en compte est le fait que votre portefeuille de noms de domaine constitue une cible pour les hacktivistes, en particulier si votre marque est populaire ou controversée. Pour les noms de domaine critiques de votre entreprise, je recommande d'envisager les options de services de registrar et de verrouillage de registre, qui empêchent les transferts de domaines non autorisés vers des opérateurs de sites de phishing. CSC recommande à ses clients d'utiliser les deux services.

Nous proposons également des services de détection de phishing et de take down, qui permettent de mener une veille continue contre d'éventuelles attaques. La rapidité du service de neutralisation est essentielle pour minimiser les dommages potentiels. Voici d'ailleurs un autre enseignement important : les services de registrar et de verrouillage de registre offrent une solution simple et extrêmement rentable.

La formation de votre personnel et de vos clients concernant les techniques de phishing est également une mesure importante, dans la mesure où ces attaques exploitent précisément le manque de sensibilisation à ce risque. Nos employés sont formés et testés sur toutes ces questions, pour assurer à la fois notre propre sécurité et celle de nos clients. Si des moyens de contrôle appropriés ne sont pas mis en place, un simple clic sur un lien malveillant risque de compromettre la sécurité d'une organisation tout entière. L'association d'une technologie adaptée et de la sensibilisation des parties prenantes assurera une bonne défense contre un ennemi malheureusement implacable.

### *Journaliste*

**Vous venez de nous parler des plus grandes menaces auxquelles sont confrontées les entreprises. Pouvez-vous nous en présenter d'autres auxquelles il convient d'être attentif ?**

### *Scott*

Le DNS spoofing, qui est surtout utilisé par les cybercriminels, est une menace courante. Ce type d'attaque

n'est pas immédiatement destructeur, mais il orientera des utilisateurs légitimes vers des sites contrefaits, qui pourront entraîner de graves dommages en termes d'atteinte à la réputation et de perte d'activité. Il est important que votre plate-forme DNS soit suffisamment robuste pour résister à une telle attaque. La première action doit ici consister à consolider tous vos noms de domaine au sein d'une plate-forme unique : cela vous assurera une visibilité claire sur votre portefeuille et vous permettra de le gérer aisément et plus efficacement.

Nous observons toujours une menace constante d'attaques DDoS, qui congestionnent les réseaux en les encombrant de données malveillantes. Ces dernières années, la moyenne de l'amplitude des attaques DDoS a explosé ; dans son dernier rapport du 4ème trimestre 2016, "Quarterly Trends Report", Verisign signale une augmentation de 167 % de la dimension moyenne des pics d'attaques, comparés à ceux de 2015. CIO Insight estime qu'un temps d'arrêt d'une heure peut coûter plus de 100 000 dollars à une entreprise. Quand on sait que la durée moyenne d'une perturbation est de plus de 24 heures dans certains secteurs, on comprend que de telles attaques puissent rapidement avoir des implications qui se chiffrent en plusieurs millions de dollars.

La grande majorité des nouvelles attaques, dont la plupart sont lancées par les hacktivistes, visent les secteurs du Cloud, du SaaS et de l'IT, ainsi que les services financiers, les médias et le divertissement. Les entreprises doivent envisager avoir recours à un service de protection DDoS, qui permettra de détecter une attaque, et de filtrer et détourner efficacement le trafic malveillant, permettant ainsi au trafic légitime d'être acheminé à destination.

Un autre élément de protection important est l'utilisation des certificats SSL (Secure Sockets Layer), que l'on appelle parfois également certificats TLS (Transport Layer Security). Les certificats SSL/TLS sont un protocole établi assurant des communications sécurisées entre le client et le serveur. Ils constituent une ressource indispensable pour les sites Web, les e-mails, les sites intranet et les adresses IP.

Tous les sites web devraient être sécurisés avec de tels certificats aujourd'hui. Cela étant, même les protections SSL/TLS présentent des vulnérabilités, et il est donc important que les entreprises procèdent à un bilan de leurs suites de chiffrement SSL/TLS, deux fois par an ou dès qu'une vulnérabilité est publiée. L'une des sources de référence que j'utilise actuellement est bettercrypto.org.

### *Journaliste*

**En tant que responsable de la sécurité des systèmes d'information de CSC, quels conseils donneriez-vous aux entreprises qui souhaitent garantir la protection de leurs actifs numériques ?**

### *Scott*

La sécurité des actifs numériques exige deux éléments essentiels: une vigilance constante et une technologie performante. On peut à ce propos reprendre la boutade d'Andy Grove d'Intel : « Seuls les paranos survivront. »

Fort heureusement, l'évolution des processus et des technologies parviennent à tenir le rythme par rapport aux nouvelles menaces. Les marques ont à leur disposition un large choix en termes d'options de protection, avec notamment l'authentification supplémentaire, les solutions DNS, ou encore la surveillance et la réduction des attaques DDoS. Le choix du prestataire de services qui vous aidera à gérer vos actifs numériques est un élément important dans la protection générale de votre entreprise. Ce prestataire doit être capable d'analyser votre portefeuille d'actifs (cela incluant notamment les domaines, les applications et les réseaux sociaux), puis de vous conseiller sur les meilleures mesures à prendre pour les protéger en utilisant au mieux le budget numérique dont vous disposez. La cybercriminalité n'est pas près de disparaître, mais une compréhension solide des mesures à prendre pour protéger vos actifs contre tous les types d'attaques constituera un premier pas essentiel pour assurer la sécurité de votre entreprise et de vos clients.

# Renforcez votre sécurité

## Quatre mesures simples et rentables à prendre, dès aujourd'hui, pour renforcer votre sécurité :

- Mettre en oeuvre une authentification à deux facteurs. Cette mesure de sécurité supplémentaire est très abordable et constituera un investissement sûr. Veillez à ce que les noms d'utilisateur et mots de passe utilisés par vos employés ne permettent pas d'accéder à des ressources critiques.
- Ajouter un verrouillage de registre. L'ajout d'un système d'authentification de verrouillage de registre, qui permettra de vérifier les identifiants en entrant directement en contact avec une personne, permet d'éliminer pratiquement tout risque de modification non autorisée de serveurs de noms de domaine.
- Procéder à une évaluation des solutions DNS. Identifiez tous vos noms de domaine et consolidez-les au sein d'une plate-forme unique. Vous pouvez minimiser les dommages en mettant en place des solutions qui garantiront le maintien de la disponibilité des systèmes en cas d'attaque, en acheminant les requêtes vers différents serveurs ou vers des bases de données de sauvegarde si les sites de serveur sont inondés.
- Gérer les certificats SSL/TLS. Implémentez des certificats SSL/TLS sur tous vos sites Web, consolidez la gestion de ces certificats afin de vous assurer qu'aucun d'entre eux n'expirera à votre insu, puis mettez en place une procédure de contrôle continu de tous les certificats sur la base des normes en vigueur. Un bon prestataire sera normalement en mesure de vous aider sur tous ces points. Vous pouvez par ailleurs consulter bettercrypto.org, qui constitue actuellement une référence crédible.

« Le choix du prestataire de services qui vous aidera à gérer vos actifs numériques est un élément important dans la protection générale de votre entreprise. Ce prestataire doit être capable d'analyser votre portefeuille d'actifs puis de vous conseiller sur les meilleures mesures à prendre pour les protéger. »

## Sources

[1]http://www.ponemon.org/news-2/71

[2]http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

[3]https://blog.verisign.com/security/q4-2016-ddos-trends-report-167-percent-increase-average-peak-attack-size/

cscdigitalbrand.services/fr