Communiqué de presse
Paris, le 21 décembre 2017

Les 10 cyberattaques qui ont marqué l'année 2017

Paris, le 21 décembre 2017 – A l'approche de la fin d'année, Hiscox, spécialiste de la cyberassurance, souhaite revenir sur les cyberattaques les plus frappantes de 2017.

1. **WannaCry / NSA – *Mai* –** Considérée comme la plus importante cyberattaque par *ransomware* de l'histoire, WannaCry a infecté en quelques heures plus de 300 000 ordinateurs, dans plus de 150 pays. Parmi ses victimes : FedEx, Renault, ou encore le ministère de l'intérieur russe. Cette attaque a été revendiquée par le groupe de hackers Shadow Brokers, ceux-là mêmes qui, au premier trimestre 2017, avaient réussi à s'introduire dans le réseau informatique de la NSA, et à y dérober un attirail considérable de failles, virus et autres outils informatiques, dont la faille exploitée par WannaCry, baptisée Eternal Blue. Il s'agissait d'une faille déjà identifiée par Microsoft, mais le patch correctif proposé n'avait pas été suffisamment massivement installé pour que l'attaque échoue. In fine, les coûts de WannaCry ont été évalués autour d'un milliard de dollars, sans compter bien évidemment toutes les conséquences indirectes qu'ont pu subir ses victimes.

2. **Petya / NotPetya – *Juin* –** Parmi les cyberattaques qui ont marqué l'année, il faut encore citer Petya / NotPetya. Petya, *ransomware* apparu en 2016, avait déjà réussi à contaminer des milliers d'ordinateurs, via la même faille de sécurité Windows, exigeant le paiement d'une rançon de 300 dollars (en bitcoins bien sûr) en échange de la récupération des fichiers. NotPetya, quant à lui, a vu le jour en juin 2017 : il s'agissait en réalité d'un virus déguisé en un *ransomware* ayant pour vocation de rappeler son prédécesseur Petya. Cette cyberattaque bien plus puissante, dont on ne connait pas l'origine, s'est propagée presque sans intervention humaine (contrairement à Petya qui requérait le téléchargement d'un spam envoyé par email) : il suffisait d'un seul poste non mis à jour sur un réseau pour que l'ensemble du réseau soit potentiellement compromis, sans compter que l'intégralité du disque dur était touchée (et non seulement, comme Wannacry, le système d'exploitation et les fichiers stockés). On estime à plus de 2 000 le nombre de sociétés qui ont été infectées par ce virus. Parmi elles, Saint-Gobain (coût de 220 millions d'euros) et la SNCF, mais aussi le publicitaire WPP ou encore le labo pharmaceutique Merck ; le système de surveillance des radiations de la centrale nucléaire ukrainienne de Tchernobyl a lui aussi été infecté. Les victimes ne pouvaient même pas payer la rançon pour récupérer la clé de décryptage, l'adresse mail associée à l'attaque étant invalide…

3. **Deloitte – *Septembre* –** Durant près de 6 mois, le prestigieux cabinet de conseil et d'audit a été victime d'une importante cyberattaque durant laquelle des pirates ont réussi à accéder à des informations privées, telles que des mails échangés entre le cabinet et ses clients. Les hackers ont utilisé l'identifiant et le mot de passe d'un compte administrateur, leur permettant ainsi d'accéder au Cloud Azure de Miscrosoft, plateforme hébergeant une partie des données de Deloitte.

4. **Equifax – *Septembre* –** La célèbre société de crédit américaine, également spécialisée dans la protection des données, a été victime d'un piratage informatique important au cours de l'année. Les informations de plus de 140 millions d'américains et plus de 200 000 numéros de cartes bancaires de consommateurs ont été consultés par les pirates, qui ont exploité une faille dans l'une des applications de la société, leur permettant ainsi d'accéder à certains fichiers. Quelques jours après l'attaque, le PDG de l'entreprise annonçait sa démission.

5. **Netflix – *Septembre* –** La plateforme de streaming Netflix a été victime d'un piratage d'envergure, plus précisément d'une campagne de *scam* visant directement ses utilisateurs des millions d'entre eux ont reçu des mails depuis l'adresse supportnetflix@checkinformation.com, les invitant à communiquer leurs coordonnées bancaires afin d'éviter que leur compte ne soit clôturé. Comme à l'accoutumée, tout avait soigneusement été pensé afin de tromper les victimes : site internet reprenant la charte graphique de la véritable plateforme, recours à un ton et à un design similaires à ceux employés par Netflix.

6. **DoubleLocker – *Octobre* –** Avec le *ransomware* DoubleLocker, ce ne sont pas les ordinateurs qui ont été touchés, mais les appareils mobiles fonctionnant sous Androïd. Pour la première fois, un virus a été capable de changer le code PIN des utilisateurs et de chiffrer les données de leur smartphone ou tablette. Ces derniers, alors dans l'incapacité de récupérer leurs fichiers ou d'utiliser leur appareil, n'ont eu d'autres choix que de payer la rançon demandée par les hackers.

7. **PowerShell – *Novembre* -** L'Arabie Saoudite fait régulièrement l'objet d'attaques informatiques, et 2017 n'a pas fait exception à cette règle : le NCSC (Centre national de sécurité saoudien) a signalé une campagne de « menaces persistantes avancées », menée via le logiciel Powershell (habituellement utilisée, en particulier, par le groupe MuddyWater), très difficile à détecter. Il semble que cette attaque se soit inscrite dans le cadre plus global d'une campagne massive de cyber-espionnage dirigée contre l'Arabie Saoudite.

8. **Imgur – *Novembre* –** Cette attaque informatique contre le site de partage d'images, qui a eu lieu en 2014, n'a pourtant été découverte qu'en 2017, et ce grâce à un signalement externe. En effet, les données de l'attaque ont été transmises à Troy Hunt, fondateur du site haveibeenpwned.com, qui a immédiatement alerté Imgur. Près de 1,7 millions d'utilisateurs du site d'hébergement d'images ont été victimes de cette cyberattaque, qui visait à dérober leurs données personnelles (adresses email et mots de passe, puisque la société ne demande pas les noms, adresses ou numéros de téléphones des utilisateurs). Utilisé par plus de 150 millions d'internautes, Imgur a tout de suite demandé à ses utilisateurs de changer leur mot de passe au plus vite, en utilisant des combinaisons différentes pour chaque site et application.

9. **Uber – *Novembre* –** Il y a un an environ, près de 57 millions de comptes utilisateurs de la plateforme Uber ont été piratés. L'entreprise américaine, leader mondial des VTC, aurait alors pris la décision de payer une rançon aux hackers de 100 000 dollars en échange de la destruction des données piratées, sans avoir l'assurance que celle-ci soit réellement effectuée. Cette affaire, contre-modèle de bonne communication sur le sujet, mise sous silence pendant une année, a éveillé les consciences en matière de cyber-sécurité, devenue un enjeu majeur pour les entreprises et pour les consommateurs. La Commission européenne a quant à elle jugé irresponsable la gestion par Uber des données de ses clients et de ses chauffeurs.

10. **NiceHash – *Décembre* –** Ces dernières semaines, l'envolée du Bitcoin a rythmé l'actualité, éveillant ainsi l'intérêt tout particulier des hackers. La célèbre plateforme slovène de minage de Bitcoins, NiceHash, a été victime d'une cyberattaque durant laquelle 4 700 bitcoins ont été dérobés, soit l'équivalant de près de 64 millions de dollars.

Rencontrez Astrid-Marie Pirson (Responsable de Marché Technologies / Médias / Télécoms / Cyber chez Hiscox), lors de la **10ème édition du Forum International de la Cybersécurité (FIC).**

Où et quand ?
Les 23 et 24 janvier / Lille Grand Palais

A propos de Hiscox

Hiscox est un spécialiste de l'assurance et de la réassurance qui compte 2200 salariés dans 13 pays. Fort de plus de 100 ans d'expérience, Hiscox travaille avec des professionnels et des particuliers pour offrir une couverture adaptée à des besoins d'assurance spécifiques.

Pour accompagner ses partenaires courtiers, notamment dans les défis liés à la digitalisation de leur métier, Hiscox a choisi de placer l'expérience client au centre de ses préoccupations tout en renforçant son approche conseil. C'est dans cette optique qu'Hiscox propose, depuis juin 2017 MyHISCOX, une nouvelle solution de souscription et de gestion en ligne complète et intuitive à destination de ses courtiers et partenaires.

https://www.hiscox.fr/courtage/

Contacts presse

Agence LEWIS
Robert Morel / Eléonore Ancel
01 85 65 86 33
hiscoxfrance@teamlewis.com