Communiqué de presse
Paris, le 20 décembre 2018

Les 10 failles de cyber sécurité qui ont marqué l'année 2018

Paris, le 20 décembre 2018 – A l'approche de la fin d'année, Hiscox, spécialiste de la cyberassurance, souhaite revenir sur les failles de cyber sécurité les plus frappantes de 2018.

1. Meltdown et Spectre / Janvier

Ces deux failles de sécurité découvertes au début de l'année n'ont pas ciblé le web, ni même un logiciel, mais des processeurs. Si Meltdown concernait uniquement les processeurs Intel, Spectre touchait, en revanche, tous les processeurs en vente depuis dix ans, y compris les ARM composant les smartphones. La correction de ces failles historiques permettant à des logiciels et scripts malveillants d'accéder à des informations non chiffrées a impliqué plusieurs acteurs de l'industrie tels que des spécialistes des systèmes d'exploitation, des développeurs de navigateurs et des fabricants de processeurs.

2. JO de Pyeongchang / Février

Ciblant les organisateurs des Jeux Olympiques d'hiver, ce malware, à la provenance encore incertaine, avait pour vocation de perturber le bon déroulement de la cérémonie d'ouverture. Le logiciel « Olympic Destroy » a affecté la télévision, les accès internet et le site des Jeux, empêchant même les participants d'imprimer leurs billets d'entrée. A noter que cela n'a pas été la seule attaque menée contre les JO de Pyeongchang : le mois précédent son lancement, des hackers avaient déjà tenté de s'introduire dans les ordinateurs de l'organisation afin de dérober des mots de passe et des informations financières.

3. Ministères allemands / Mars

Cette cyberattaque inédite, soupçonnée d'avoir été menée par le groupe de hackers russes Fancy Bears, aurait débuté un an avant sa révélation. Visant à s'introduire dans des systèmes informatiques fédéraux, cette cyberattaque aurait permis aux hackers d'accéder à des données provenant du ministère de la Défense et du ministère des Affaires Étrangères. L'intrusion se serait produite via le réseau IVBB, utilisé pour les échanges entre les ministères de Bonn et Berlin, qui est pourtant totalement séparé de l'Internet public

4. Atlanta / Mars

La ville d'Atlanta a essuyé en début d'année une attaque massive de ransomwares. L'attaque « SamSam », qui aurait été menée à l'aide d'un logiciel piraté élaboré par la NSA, a permis aux hackers de prendre le contrôle des ordinateurs de la ville. En échange, une rançon de 51 000 $ en bitcoins a été réclamée. Les hackers ont pu, entre autres, reporter les dates de comparution au tribunal, geler les offres d'emploi de la ville, et interrompre les systèmes informatiques pendant près d'une semaine. Le coût de cette attaque est estimé à près de 10 millions de dollars.

5. TSB / Avril

TSB, une banque de détail britannique, a vu ses systèmes paralysés après une importante panne informatique. Pendant plus d'une semaine, les clients de la banque ont rencontré de grandes difficultés à accéder à leurs comptes en ligne et ont ainsi été dans l'incapacité de régler leurs factures ou de transférer de l'argent. L'un des clients s'est même retrouvé avec un découvert s'élevant à 1 million de livres. Depuis cet incident, la banque TSB a connu d'autres pannes, faisant ainsi ressortir la

fragilité des systèmes informatiques financiers qui peut impacter leur réputation et leurs bénéfices de manière significative.

6. TicketMaster / Juin

Le site de billetterie britannique a été victime d'une cyberattaque visant à dérober les données d'une partie de ses utilisateurs, telles que leurs informations personnelles et de paiement. La faille proviendrait d'un chatbot développé par la société Inbenta Technologies : les hackers seraient parvenus à modifier un code JavaScript utilisé par ce bot, leur permettant ainsi de mettre la main sur certaines données confidentielles.

7. Système de santé de Singapour / Juillet

Ville ultra connectée, Singapour a subi en milieu d'année la pire cyberattaque de son histoire. Ciblant le système de santé de la ville, des hackers auraient réussi à s'introduire dans les ordinateurs du réseau de SingHealth, l'une des principales entreprises médicales singapouriennes. Les dossiers médicaux d'un quart de la population de la ville, soit 1,5 millions de personnes, ont été dérobés, permettant ainsi aux pirates d'avoir accès à des informations personnelles telles que les numéros d'identification nationale et adresses des patients.

8. Ports de San Diego et de Barcelone / Septembre

Les ports de Barcelone et de San Diego ont chacun été victimes d'une cyberattaque à quelques jours d'intervalle. Bien que la première n'ait perturbé que légèrement certaines opérations terrestres, la seconde a affecté la capacité de travail des employés, en touchant les départements de permis, de services commerciaux et des documents publics. Les attaques subies par ces deux ports internationaux de manière quasi simultanée et leurs similitudes laissent à penser qu'il s'agit d'une action coordonnée, même si rien n'a été confirmé.

9. Facebook / Septembre

Le réseau social aux 2,2 milliards d'utilisateurs a essuyé une attaque d'ampleur à la rentrée. Des hackers auraient profité d'une faille technique afin de dérober des outils d'accès permettant de se connecter aux comptes Facebook de près de 50 millions de personnes. Cette cyberattaque, qui est la plus importante subie par le réseau social, a fait chuter son action de 3% dans les heures suivant l'annonce.

10. Bloomberg / Octobre

A la rentrée, Bloomberg, chaine de télévision américaine, a rendu publique une enquête visant la Chine. Cette dernière a été accusée par les États-Unis d'avoir mis au point un programme d'espionnage informatique ciblé contre des services américains et quelques grandes entreprises telles que Apple ou Amazon. Des espions chinois auraient infiltré la chaine logistique de Supermicro et inséré des puces dans du matériel informatique utilisé par ces entreprises et agences fédérales américaines, donnant ainsi accès à Pékin à leurs réseaux internes.

A propos de Hiscox

Hiscox est un groupe international d'assurances spécialisées coté sur le London Stock Exchange (LSE:HSX). Hiscox a pour ambition de devenir un assureur spécialiste reconnu en présentant un portefolio d'offres diversifié en termes de produits et de présence géographique. Ce portfolio est équilibré entre des entreprises fortement exposées aux catastrophes et d'autres confrontées à des risques spéciaux moins volatiles, lui donnant des opportunités de croissance tout au long du cycle d'assurance. Le Groupe Hiscox emploie plus de 2 200 collaborateurs dans 13 pays pour répondre aux besoins de ses clients à travers le monde. En Europe, au Royaume-Uni et aux Etats-Unis, Hiscox offre une gamme de solutions spécialisées pour les professionnels et particuliers à travers un canal direct. En France, Hiscox dispose de bureaux à Paris, Lyon et Bordeaux. Hiscox France s'appuie sur ses 100

collaborateurs et sur son réseau de courtiers pour proposer une large gamme d'assurances à destination des particuliers, des professionnels et des collectivités. Plus d'info : http://www.hiscox.fr/

Contacts presse
Agence LEWIS
Eléonore Ancel / Anaïs Sarrassat
01 85 65 86 32
hiscoxfrance@teamlewis.com