Antivirus software could make your company more vulnerable

	Antivirus software could make your company more vulnerable !

Security researchers are worried that critical vulnerabilities in antivirus products are too easy to find and exploit

Imagine getting a call from your company's IT department telling you your workstation has been compromised and you should stop what you're doing immediately.
You're stumped: You went through the company's security training and you're sure you didn't open any suspicious email attachments or click on any bad links; you know that your company has a solid patching policy and the software on your computer is up to date; you're also not the type of employee who visits non-work-related websites while on the job. So, how did this happen?

A few days later, an unexpected answer comes down from the security firm that your company hired to investigate the incident: Hackers got in by exploiting a flaw in the corporate antivirus program installed on your computer, the same program that's supposed to protect it from attacks. And all it took was for attackers to send you an email message that you didn't even open.
This scenario might sound far-fetched, but it's not. According to vulnerability researchers who have analyzed antivirus programs in the past, such attacks are quite likely, and may already have occurred. Some of them have tried to sound the alarm about the ease of finding and exploiting critical flaws in endpoint antivirus products for years.
Since June, researchers have found and reported several dozen serious flaws in antivirus products from vendors such as Kaspersky Lab, ESET, Avast, AVG Technologies, Intel Security (formerly McAfee) and Malwarebytes. Many of those vulnerabilities would have allowed attackers to remotely execute malicious code on computers, to abuse the functionality of the antivirus products themselves, to gain higher privileges on compromised systems and even to defeat the anti-exploitation defenses of third-party applications.
Exploiting some of those vulnerabilities required no user interaction and could have allowed the creation of computer worms – self-propagating malware programs. In many cases, attackers would have only needed to send specially crafted email messages to potential victims, to inject malicious code into legitimate websites visited by them, or to plug in USB drives with malformed files into their computers.

Attacks on the horizon

Evidence suggests that attacks against antivirus products, especially in corporate environments, are both possible and likely. Some researchers believe that such attacks have already occurred, even though antivirus vendors might not be aware of them because of the very small number of victims.
The intelligence agencies of various governments have long had an interest in antivirus flaws. News website The Intercept reported in June that the U.K. Government Communications Headquarters (GCHQ) filed requests in 2008 to renew a warrant that would have allowed the agency to reverse engineer antivirus products from Kaspersky Lab to find weaknesses. The U.S. National Security Agency also studied antivirus products to bypass their detection, according to secret files leaked by former NSA contractor Edward Snowden, the website said.

Réagissez à cet article

Source : *Antivirus software could make your company more vulnerable | Computerworld*

Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab

Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab

---

Avec Enigma, système de cryptage de données basé sur le blockchain, des informations confidentielles peuvent être stockées et partagées en ligne, sans intervention d'un tiers de confiance pour contrôler leur utilisation.

Enigma. Derrière ce nom mystérieux se cache l'une des dernières créations du MIT Media Lab, l'un des laboratoires de recherche du Massachusetts Institute of Technology. Ce système de cryptage de données est basé sur le blockchain, la technologie qui sous-tend le bitcoin (monnaie virtuelle mise en circulation en 2009). Elle fonctionne grâce au partage d'un registre d'informations par l'ensemble d'une communauté d'internautes.

Enigma, dont la version bêta sera lancée prochainement, permettra à des utilisateurs anonymes (particuliers, entreprises, associations…) de stocker dans le cloud et de partager des informations sensibles avec des tiers, de manière sécurisée. Pas besoin d'un intermédiaire de confiance, qui aurait accès à ces data pour contrôler leur utilisation et les crypter. Ces opérations sont effectuées par un réseau d'ordinateurs membres, grâce au système du blockchain. Les informations peuvent être traitées par des algorithmes, sans que le jeu de données brut ne soit jamais révélé dans sa totalité à l'une des parties.

DES RETOMBÉES DANS LE DOMAINE DU MACHINE LEARNING

Le registre blockchain, partagé par les ordinateurs membres du réseau, contrôle l'identité des utilisateurs d'Enigma (via un code, car ils sont anonymes) et leur donne accès ou non à tout ou partie des données. Il enregistre l'ensemble des opérations réalisées sur Enigma : enregistrement de nouvelles informations, consultation, opérations réalisées sur ces data…

Les données stockées par Enigma pourront être analysées par des applications et des logiciels extérieurs, tout en maintenant ces informations sous le contrôle de leur propriétaire. Le programme pourrait avoir des retombées intéressantes dans le domaine de la data science et du machine learning.

UN NOM DE BAPTÊME HISTORIQUE

Enigma pourrait également contribuer au développement d'un Internet des objets respectueux de la vie privée de ses utilisateurs, souligne le site spécialisé Bitcoin Magazine dans un article présentant le projet. Les propriétaires des données pourront, s'ils le souhaitent, les monétiser. Ils pourraient par exemple vendre à des laboratoires pharmaceutiques qui réalisent des recherches un accès partiel et contrôlé à leurs données de santé.

Guy Zyskind, étudiant au MIT, et Oz Nathan, entrepreneur qui a travaillé par le passé avec la défense israélienne, sont à l'origine de ce programme. Ils n'ont pas choisi son nom par hasard. Le système de cryptographie électro-mécanique utilisé par les Allemand pendant la deuxième guerre mondiale était baptisé Enigma. Un groupe de chercheurs, dont faisait notamment partie Alain Turing, a réussi à trouver la clef de ce code complexe.

Réagissez à cet article

Source : *Enigma, le système de cryptage de données basé sur le blockchain du MIT Media Lab*

Panne électrique en Ukraine : le malware aurait été aidé par l’humain

Panne électrique en Ukraine : le malware aurait été aidé par l’humain

---

 **Le mois dernier, une cyberattaque contre des fournisseurs d'énergie ukrainiens avait privé 80 000 clients d'électricité. D'après la signature du malware, l'attaque avait été imputée à un groupe de pirates ayant des liens avec la Russie. Mais, selon une nouvelle étude, le malware n'est pas directement à l'origine de la panne : les assaillants sont intervenus physiquement pour activer les disjoncteurs et provoquer la coupure de courant.**

Selon des informations publiées samedi par l'équipe du SANS Industrial Control Systems (ICS), une organisation spécialisée dans l'information et la formation des professionnels de la sécurité, le malware a bien servi aux pirates à s'introduire dans le réseau des fournisseurs d'électricité, mais ils sont ensuite intervenus sur les disjoncteurs pour couper l'alimentation. Depuis des années, les experts mettent en garde sur la vulnérabilité des systèmes de contrôle industriels. Les cyberattaques survenues le 23 décembre contre les installations ukrainiennes montrent que leurs craintes sont justifiées. Selon les experts du #SANS ICS, ces évènements sont aussi la preuve que de telles attaques sont planifiées et très coordonnées.
Depuis l'annexion de la Crimée par la Russie en 2014, les tensions entre la fédération et l'Ukraine restent fortes. « Pour masquer le piratage et l'intrusion dans les réseaux, les agresseurs sont intervenus physiquement sur la centrale électrique », a déclaré l'équipe du SANS ICS. « Les agresseurs ont également lancé en simultané une attaque DDoS par déni de service sur le réseau téléphonique afin de bloquer les appels des clients affectés par la panne », a encore déclaré l'organisation. Les attaques auraient visé les deux fournisseurs d'énergie Prykarpattyaoblenergo et Kyivoblenergo. Ce dernier a déclaré dans une mise à jour de service que 80 000 clients dépendant de 30 sous-stations avaient été déconnectés du réseau.

Des pannes provoquées par une action physique

Plusieurs entreprises de sécurité ont analysé le #malware Black Energy 3 et le #composant Killdisk utilisés pour les attaques. Jeudi dernier, l'entreprise de sécurité iSight Partners basée à Dallas a déclaré que ces logiciels malveillants avaient déjà été utilisés dans le passé par le #groupe de pirates Sandworm connu pour avoir de puissants intérêts russes. Mais, comme iSight, le SANS ICS pense que les pannes ne sont pas à mettre exclusivement sur le compte des malwares. « Autrement dit, de nouvelles preuves pourraient remettre en cause l'impact réel des composantes malveillantes impliquées dans l'attaque », a écrit Michael Assante, directeur du SANS ICS.
Le composant Killdisk écrase le Master Boot Record (MBR), premier secteur du disque dur chargé par le PC avant de monter le système d'exploitation, et empêche donc le PC de démarrer. Selon Symantec, Killdisk peut aussi écraser des fichiers en écrivant des données inutiles. Michael Assante avance que Killdisk n'était pas compatible avec le système SCADA de contrôle et d'acquisition de données utilisé par les deux opérateurs. Mais il a peut-être été utilisé pour effacer d'autres fichiers qui auraient permis la restauration des systèmes. « Il semble que les fournisseurs d'électricité ont rétabli leurs services en actionnant manuellement les disjoncteurs au bout de trois et six heures », a ajouté le directeur du SANS ICS. Selon lui, « il faudrait féliciter les opérateurs ukrainiens pour leur diligence et les efforts accomplis pour restaurer leurs services ».

Réagissez à cet article

Source : *Panne électrique en Ukraine : le malware n'est pas seul en cause – Le Monde Informatique*

Google corrige 5 failles critiques d’Android

Google corrige 5 failles critiques d’Android

Pratiquement tous les terminaux tournant sous une version récente d'Android sont affectés par au moins une des cinq failles critiques corrigées par Google dans l'OS mobile.

Google a remédié à une douzaine de vulnérabilités d'Android, dont cinq sont qualifiées de « critiques ».
Parmi les failles critiques identifiées et corrigées dans cette nouvelle série de correctifs, la firme de Mountain View signale qu'une des vulnérabilités pourrait permettre à un attaquant d'exécuter du code distant – comme un malware – en exploitant la manière dont Android traite certains fichiers médias.

Nexus, puis smartphones Samsung, LG et BlackBerry

Google précise par ailleurs qu'Android 5.0 et les versions ultérieures – dont « Marshmallow » 6.0 – sont affectées par ces différentes vulnérabilités.
Et si la nature de ces failles vous évoque quelque chose, ce n'est pas une coïncidence. Mois après mois, le service « mediaserver » reste le composant le plus problématique d'Android. Au point que Google a copié-collé le même message dans ses bulletins de sécurité à chaque fois que le composant a été affecté.
La vulnérabilité critique porte sur une partie centrale du logiciel Android et qui dispose de permissions auxquelles les applications tierces n'ont normalement pas accès. D'autres failles se situent elles dans la gestion du Bluetooth et du Wi-Fi, ou encore au niveau du kernel.
Les terminaux Nexus sont les premiers appareils Android à recevoir les correctifs de sécurité. D'autres fabricants, parmi lesquels Samsung, LG et BlackBerry, déploieront des mises à jour dans les prochains jours.

Réagissez à cet article

Source : *Google corrige 5 failles critiques d'Android*

50 attaques informatiques qui ont marqué le web Français en 2015

50 attaques informatiques qui ont marqué le web Français en 2015

Pendant qu'il est possible de lire un peu partout sur le web le « top 5 », le « top 7 » des attaques informatiques dans le monde, ZATAZ préfère regarder du côté de VOS ordinateurs avec le top 50 des attaques informatiques qui ont touché la France et les internautes francophones. Des cas traités par ZATAZ.

Madison, Hacking Team, Hôtels Trump, Madisson, Vtech… les cas de piratage et de fuites de par le monde ont été pléthoriques, encore une fois, cette année. Revenir sur ces cas, pourquoi pas, mais il suffit d'en parler aux internautes francophones croisés sur la toile pour se rendre compte qu'ils ne se sentent pas concernés, et considères ces actes comme « drôles », ou « insignifiants » pour leur vie 2.0. Bilan, sur 1 475 personnes interrogées par ZATAZ (Âgés de 18 à 55 ans – entre le 22 décembre et le 30 décembre – 71% d'hommes – 43% évoluant dans le monde de l'informatique) seules 96 personnes interrogées avaient pris soins de modifier leurs mots de passe, car utilisés plusieurs fois dans des comptes différents (webmails, forums, …). 27 des interviewés confirmaient qu'ils regardaient plus souvent leur compte en banque. 339 avaient décidé, cette année, de faire un backup mensuel de leurs données (Je vous conseille fortement de pratiquer une sauvegarde, chaque jour, ndr).

Opération Anti Charlie

Janvier 2015, les attentats contre la rédaction de Charlie Hebdo et une supérette parisienne met en émoi le monde et le web. Les Anonymous décident de s'attaquer aux sites de djihadistes. Les participants s'attaquent à tout et n'importe quoi, dont des commerces de produits Hallal. En réponse, de jeunes internautes musulmans et plus d'une centaine de pirates du Maghreb et d'Asie lancent l'Opération Anti Charlie. Plus de 20 000 sites en .fr sont modifiés et/ou infiltrés. A noter que certains sites piratés, mais aussi infiltrés sans que la moindre trace du piratage n'apparaisse publiquement, ne sont toujours corrigés 11 mois plus tard. Une attaque informatique qui, sous l'excuse d'une cyber manifestation, était surtout menée et manipulée par des commerçants officiant dans le blackmarket. Dans la liste des espaces touchés : plusieurs centaines de sites du CNRS et des Restaurants du cœur, ainsi que 167 établissements scolaires d'Aquitaine ou encore de vieux espaces du Ministère de l'Intérieur et de la Défense.

TV5 Monde

Avril, le piratage de TV5 Monde fait grand bruit dans un contexte politique tendu. Au début du mois d'avril, la chaîne fait face à une cyberattaque d'ampleur. Ses différents comptes de réseaux sociaux sont piratés et diffusent de la propagande de la secte de Daesh. La diffusion des émissions de la chaîne sont coupées de l'antenne par la direction. Trend Micro évoque l'implication possible d'un groupe d'APT d'origine russe, Pawn Storm. Les autorités restent discrètes sur les différents éléments de l'affaire, si bien qu'encore aujourd'hui, on peine à se faire une idée de ce qu'il s'est vraiment passé dans le SI de France TV5 Monde. C'est surtout l'impact médiatique de cette attaque que l'on retiendra. Cinq mois après l'attaque, ZATAZ alertera l'ANSSI et TV5 Monde pour corriger d'autres failles informatiques découvertes sur les serveurs de la chaîne. A noter qu'un internaute est arrêté au mois d'août en Bulgarie. Des documents retrouvés dans son ordinateur son signé CyberCaliphate, le pseudonyme utilisé lors de l'attaque de TV5 Monde.
Un piratage qui fait ressortir que les media Français sont totalement dépassés par les potentialités malveillantes qui planent au-dessus de leurs claviers. Pour preuves, les différentes fuites de données et autres failles remontées par ZATAZ auprès de France Télévision [Fuite de données de téléspectateurs] ; du journal telecablesat.fr et 13 833 comptes clients volés.

Infiltrations

Les banques, les grands groupes Français sont visés, chaque jour, par des tentatives de piratage. Des attaques réussies ou non. Les clients ne sont jamais informés. Pendant ce temps, des millions d'informations appartenant aux Français sont pillés, copiés, revendues sur la toile. Par exemples, avec trois espaces de filiales de la BNP Paribas. Des sites retrouvés dans un espace pirate. Les malveillants s'échangeant les failles donnant accès à des bases de données. ; le pétrolier Total, et sa boutique, attaquée et pillée en janvier 2015. 29.657 clients d'un espace commercial grand public du pétrolier. Les pirates m'avouaient avoir vendu pour 500€ des informations de Français collectés dans cette BDD. Des fuites de données accessibles directement, ou via des tiers commerciaux, comme ce fût le cas pour TF1 et 1,9 millions de clients Français, abonnés à des journaux papiers ; Le site Internet La Boutique Officielle, spécialisé dans la vente de vêtements « Urban », visité par des pirates informatiques. Données des clients volées. L'entreprise ferme son espace numérique plusieurs jours ; de son côté, la CNIL contrôle 13 sites de rencontres français, 8 sont mis en demeure de mieux contrôler les informations de leurs « clients » ; En Mars, une faille informatique permettait à un pirate informatique de mettre la main sur les données d'un espace Orange Business.
Juin 2015, le portail Associations Sportives, qui répertorie plus de 240.000 clubs et associations françaises est infiltré. Le pirate diffuse un extrait de la base de données. Même sanction pour l'enseigne King jouet qui corrigera une fuite de données visant ses clients. Quinze ans de factures disponibles sur le web d'un simple clic de souris ; Un pirate informatique annonçait, en septembre, le vol des données appartenant au laboratoire Santé Beauté. Le groupe Santé Beauté regroupe des marques telles que « Barbara Gould », « Linéance », « Email diamant », « Batiste », « Nair », « Poupina » et « Femfresh ».
En octobre, le piratage de plusieurs espaces de la marque de lingerie ETAM était annoncé. Le jeune pirate diffusait plusieurs captures écrans qui ne laissent rien présager de bon pour la marque de textile.

Ransomwares

La grande mode des logiciels dédiés au chantage 2.0 (blocage de disque dur, chiffrement de données, NDR) aura frappé très fort en cette année 2015. ZATAZ a reçu pas moins de 3.022 mails de personnes et de PME piégés par ce genre d'attaque informatique. J'ai pu référencer plusieurs dizaines de mairies ou entités publiques malmenées par un ransomware, comme GDF Suez.

Arnaques et autres fraudes

Des arnaques au ransomware qui oblige les « pirates » à payer pour récupérer leurs informations prises en otage. Des arnaques qui existent aussi sous d'autres formes, comme la fraude au président. KPMG, Michelin, le Printemps, LVMH, Vinci, Total, Brevini, Areva, le cabinet d'avocats Baker & McKenzie, Finder France, SAM, Abuba, Vallourec, Sonia Ryckiel, Dargaud, Seretram… quelques exemples d'entreprises qui ont versé de l'argent à des professionnels du social engineering. Des pirates qui avaient collecté un grand nombre d'informations sur l'entreprise. Des données qui vont permettre de convaincre les services comptables de verser des millions d'euros aux pirates. Ces derniers se faisant passer pour le patron, un client, un fournisseur. Les premières arrestations ont eu lieu en février 2015. Elles concernaient les pirates ayant jeté leurs dévolus sur le club de football de l'Olympique de Marseille (OM). Deux hommes (50 et 34 ans) seront été arrêtés à Tel-Aviv.
Autre chantage, autre arnaque, celle mise en place par Rex Mundi. Plus de 15 000 identités de patients d'un laboratoire de santé français diffusées par le pirate. Le maître chanteur réclamait 20.000€ contre son silence. Le laboratoire n'a pas payé. Les informations sensibles et privées des patients seront diffusées.
Des pirates informatiques qui se spécialisent, même dans les prénoms à l'image de cet arnaqueur qui ne visait que les « Jacquelines« . Un prénom que l'escroc considère comme étant celui de personnes âgées.
Le chômage et la « crise » économique profitent aux pirates. Comme avec le site Internet Crédit Financement Fiable qui cachait une escroquerie numérique ; ou encore avec plusieurs cas d'arnaques téléphoniques. Le pirate se faisant passer pour la FNAC, Conforama ou encore Darty ; Les hôteliers, les chambres d'hôtes ne sont malheureusement pas oubliés avec une vague massive de fausses réservations de séjours.

Universités et écoles

Piratage, spams massifs, infiltration par des pirates présumés Chinois et maintenant, la diffusion d'une base de données d'élèves. L'informatique de l'université de Lyon 3 était-elle devenue complétement folle en février 2015 ? Quelques mois plus tard, rebelote, avec de nouvelles fuites de données. D'autres grandes écoles seront visées par des fuites, comme l'extranet du groupe éducatif ESG fermé à la suite d'un piratage informatique ; ou encore le cas de milliers de documents privés, et pour certains sensibles, d'étudiants de l'EPITECH. Plus de 47 000 dossiers pour quatre ans de fuite.

Fuite de données d'adresses postales

En Mars 2015, via le site Internet Degrouptest, il était possible de trouver l'adresse postale collée à un numéro de téléphone. Même une ligne téléphonique sur liste rouge pouvait être démasquée ; Neuf mois plus tard, le même type de fuite touchait un site Bouygues Telecom. Ici aussi, il suffisait de rentrer un numéro de téléphone pour accéder aux adresses postales. Liste rouge comprise.
Des fuites de données que connaitra aussi la société Somfy (spécialiste de la domotique). Zataz.com a pu constater que l'un de ses espaces web, il était dédié au personnel de l'entreprise, avait été infiltré par de nombreux pirates informatiques. Des pirates qui s'étaient empressés d'installer des backdoors, des portes cachées, leur permettant de jouer, à loisir, avec le serveur et son contenu.
Fuite de données sous forme de CV aussi, comme ce fût le cas pour un site d'Ametix. Des milliers de CV sauvegardés directement dans un dossier du WordPress d'un site dédié à une opération marketing.

Viagra et baskets dans votre site web

Le Black Seo, l'utilisation malveillante du référencement de liens et pages pirates via un site légitime, aura permis à des escrocs d'installer de fausses pharmacies et autres boutiques de contrefaçons dans des centaines de sites Français. Des Mairies, des boutiques, des sites étatiques ; Sans parler des sites propres sur eux, capable d'attirer dans leurs filets des milliers de Français, comme la fausse boutique officielle Nike RBFIRM.
En juin, le site Internet officiel de la chambre des Huissiers de Justice de Paris est (le site diffuse toujours des liens malveillants, ndr) piraté et exploité par des vendeurs de viagra ; des attaques que zataz révélera aussi en août 2015 à l'encontre du site de la Haute Autorité de la Santé ; ou encore en septembre pour la Fédération nationale des associations d'accueil et de réinsertion sociale, pour le portail dédié à une étude médicale en France et l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (APRUS).

DDoS

Bloquer un site Internet, un serveur, un streamer (joueur en ligne) … la grande mode des petits pirates, en 2015. Des attaques qui ont eu pour mission de bloquer un site, d'empêcher son bon fonctionnement. Cette année, le groupe de presse belge Rossel (Le soir, La Voix du Nord, …), mais aussi NRJ, BFM, l'Académie de Grenoble ou encore l'UMP ont été attaqués de la sorte.
Des attaques faciles à mettre en place pour le premier idiot qui passe. Les boutiques vendant du DDoS poussent comme les champignons à l'automne. A noter que durant ce mois de décembre 2015, de très nombreux amateurs de jeux en ligne, des streamers, se sont retrouvés menacer par un maître chanteur demandant de l'argent pour stopper ses blocages.

Cartes Bancaires

La fraude à la carte bancaire se porte bien ! La police de Toulouse, et plus précisément la SRPJ, a mis la main sur trois cinéphiles pas comme les autres au mois d'avril 2015. Les individus avaient piégé un distributeur de billets installé dans le cinéma Gaumont Wilson ; En Juin, la banque postale déposé plainte après que des distributeurs de billets soient piégés par des skimmeur, du matériel pirate capable d'intercepter les données inscrites sur une carte bancaires ; Des cartes bancaires qui sont devenues causantes, en mode sans fil. Bilan, même le CNRS a tiré la sonnette d'alerte en indiquant que les cartes de paiement sans contact comportent de graves lacunes de sécurité ; du sans fil qui attire, en novembre, les Frotteurs 2.0 dans le bus, le métro et autres lieux publiques ; du matériel pirate que l'on a retrouvé, entre autre, au mois d'août 2015, dans un parking proche de la gare Montparnasse (Paris). Et les arrestations se succèdent, comme à Tours, et de la prison ferme (7 mois) pour l'un de ces pirates.

Objets connectés

En Mai, je vous expliquais que pour moins de 40 euros, des voleurs de voiture s'invitaient dans les véhicules que les propriétaires pensaient avoir fermé. Même le Ministère de l'Intérieur Français s'en inquiètera quelques jours plus tard ; des panneaux d'affichage seront attaqués, modifiés (Lille, Paris…). De la geek security attitude qui démontre aussi et surtout la faiblesse des villes connectées. La partie immergée d'un problème qui pourrait être bien plus dramatique.

Swatting

Le swatting, une mode venue des Etats-Unis. L'idée du pirate, envoyer les forces de l'ordre au domicile d'un joueur en ligne. En juillet, un second cas de swatting touchait la France. Domingo est un jeune Youtuber/Streamer. Un de ces jeunes professionnels du jeu en ligne qui diffuse ses parties, en direct. Il s'est retrouvé nez-à-nez avec la police après ce genre de mauvaise blague ; Le premier cas, en février 2015, BibixHD. L'action de la police, à son domicile, sera diffusé en directe alors qu'il était en train de jouer au jeu DayZ. Un inquiétant jeu qui amuse des adolescents en mal de repères. Certains vendant des possibilités de swatting pour quelques euros comme je le révélais au moins d'août !

Phreaking

Le piratage téléphonique, le phreaking, un acte numérique qui ne connait pas la crise. Mission du pirate, mettre la main sur une ligne téléphonique qu'il pourra commercialiser, surtout les minutes disponibles d'appels. Par exemples, en juillet, 5.288€ de détournement téléphonique pour la Maison de la Jeunesse de Nancy. En novembre, 43 000€ d'appels téléphoniques détournés pour le département des Deux-Sèvres.

Heartbleed

En juillet, la faille Heartbleed refaisait surface dans mes recherches. Une vulnérabilité datant d'avril 2014. Plusieurs centaines d'importants serveurs Français étaient toujours faillibles, 16 mois plus tard.

Scientologie

Des Anonymous se sont attaqués à plusieurs sites Français de la secte de la scientologie. Les manifestants 2.0 ont voulu rappeler l'affaire de Gloria Lopez, une ancienne scientologue retrouvée morte en 2006.

Box

Cette année, nous aurons connu chez ZATAZ cinq cas, dont deux considérés comme sérieux. Numéricâble, et Bouygues. Ce dernier avait son option Playin'TV particulièrement sensible. Plusieurs problèmes qui auraient pu servir à des actions malveillantes.

Réagissez à cet article

Source : *ZATAZ Magazine » Les 50 attaques informatiques qui ont marqué le web Français en 2015*

AVG dévoile ses prévisions d’attaques informatiques et technologiques pour 2016

AVG dévoile ses prévisions d’attaques informatiques et technologiques pour 2016

L'apparition de voitures autonomes n'est pas le seul élément prouvant que les systèmes logiciels « intelligents » vont améliorer notre sécurité. D'autres indicateurs sont également visibles sur Internet.
Chez AVG, il nous a fallu des années pour concevoir nos récents algorithmes de détection des brèches et de réputation des fichiers. Pour notre tout dernier moteur antivirus, nous avons utilisé des techniques sophistiquées d'apprentissage neuronal et de collecte de données dans le cloud, qui ont été conçues pour intercepter les logiciels malveillants plus en amont, et de manière plus systématique.

En 2016, de nouvelles solutions de sécurité fondées sur l'intelligence artificielle vont faire leur apparition.
On peut donc espérer que la bataille engagée contre les mauvais génies d'Internet va connaître un regain d'énergie très attendu, et que les menaces seront encore plus vite contrées et éliminées. Les progrès de l'intelligence artificielle et des systèmes d'apprentissage profond (ou « deep learning ») sont devenus bien plus accessibles. C'est ce que l'on a pu voir récemment, par exemple, lorsque Google a ouvert le code source de l'outil Tensorflow mis au point au sein de la division chargée de l'intelligence artificielle chez Google.

Autorités de certification : une disparition annoncée
La nécessité de sécuriser tout le trafic HTTPS des sites Web via un mode de chiffrement prend de l'ampleur. En 2016, avec l'apparition de nouvelles normes ouvertes et le fait que les propriétaires de sites pourront plus facilement faire des choix, il se pourrait que cette réalité devienne globale. Certaines autorités de certification, qui par comparaison commencent à paraître un peu dépassées, risquent de connaître des moments difficiles.
Ces dernières années, certains cas d'erreurs de gestion des certificats, des incidents de sécurité et des brèches de données les ont mis sur la sellette et ont fragilisé la puissance de ces géants. La confiance dans les certificats SSL a également été ébranlée, notamment par le fait que des organismes d'état pourraient infiltrer, dans certains cas, nos communications Web prétendument sûres.
Traditionnellement, le rôle d'une autorité de certification est de confirmer l'identité du propriétaire légitime d'un site Web avant d'émettre un certificat SSL signé. Cela reste une bonne idée pour les entreprises qui peuvent se le permettre, et certaines protections et indemnités d'assurance sont également prévues. En revanche, pour un blogueur ou un propriétaire de site professionnel lambda, il est à la fois laborieux et inutile de payer une autorité de certification et se soumettre à ce qui peut sembler un processus laborieux de vérification et de confirmation. Dans ce contexte, les alternatives techniques telles que Let's Encrypt (actuellement en phase bêta) devraient prospérer.
En outre, l'identification des faux certificats SSL va se poursuivre dans le cadre du programme de transparence des certificats de Google, grâce à des systèmes de détection intégrés dans les navigateurs Web modernes. Google continue à demander aux autorités de certification d'assumer leurs responsabilités, afin que nous soyons tous mieux protégés.
Enfin, avec l'annonce d'autres solutions telles que le protocole DANE proposé par Internet Society, qui offre la possibilité à n'importe quel propriétaire de site Web de valider son propre certificat SSL et donc de se passer totalement d'une autorité de certification, l'année 2016 va nous réserver des nouveautés intéressantes !

Malvertising et réseaux publicitaires : réagir ou disparaître
La publicité malveillante ou « malvertising » désigne ce qui se produit lorsque des visiteurs innocents sont la cible d'éléments malveillants, causés par des échanges avec des tiers douteux et une sécurité déficiente sur plusieurs réseaux publicitaires en ligne. En 2016, les réseaux publicitaires vont devoir réagir ou disparaître, avant qu'ils ne détruisent l'économie numérique qu'ils ont contribué à bâtir, et ne ruinent les résultats des sites Web dont la survie dépend des recettes publicitaires.
Ce problème a une cause principale : la « surface d'attaque » des scripts de publicité et de suivi toujours plus nombreux et complexes fournis par les réseaux publicitaires et intégrés par les éditeurs (souvent de façon transparente) sur leurs sites Web.
Sur mobile, plus de la moitié de la bande passante est utilisée pour la diffusion d'annonces publicitaires, beaucoup plus que pour le contenu même de la page !
S'il est associé avec des attaques réseau plus classiques, ce nouveau vecteur peut servir à infecter des milliers de victimes qui visitent des sites pourtant légitimes. Il faut aussi savoir que, même si beaucoup de grands réseaux publicitaires réagissent rapidement et arrêtent le flux de trafic lorsqu'un cas de malvertising se produit, quelques minutes suffisent pour toucher des centaines, voire des milliers de victimes. Toute personne ayant récemment installé un système de blocage publicitaire vous certifiera que ses sites Web préférés se chargent incroyablement plus vite, ce qui paradoxalement n'arrange rien.
Il faut malheureusement reconnaître qu'une grande partie des sites Web riches en contenu, pour qui les recettes publicitaires sont essentielles, se chargent lentement. En fait, une étude menée par le New York Times a montré que, pour la version mobile de nombreux sites d'actualité, plus de la moitié de la bande passante utilisée sert à la diffusion d'annonces publicitaires. Cela représente un volume de données (chargement des annonces, scripts et codes de suivi) supérieur au contenu effectivement affiché sur la page que vous lisez !
Toutefois, les systèmes de blocage de la publicité ne sont pas une solution à long terme à ce qui, finalement, est un problème de mise en œuvre. C'est encore plus vrai si vous convenez que la disparition du principe de monétisation actuellement en vigueur sur Internet pourrait avoir des conséquences économiques désastreuses. De plus, une récente déclaration de l'IAB (Interactive Advertising Bureau) confirme que les annonceurs « tiennent beaucoup moins compte de l'expérience utilisateur » dans leur manière d'élaborer des contenus.
Pour empêcher les systèmes de blocage d'annonces de se répandre, l'IAB a imaginé L.E.A.N. (de l'anglais Light, Encrypted, Ad Choice Supported and Non-Invasive), un programme basé sur des principes intervenant dans la prochaine phase des normes techniques publicitaires destinées à la chaîne d'approvisionnement publicitaire numérique globale. Quelle que soit la solution choisie, une chose est certaine : les réseaux publicitaires doivent réagir et régler les problèmes de sécurité, faute de quoi l'année 2016 pourrait bien être celle où la « vague scélérate » du malvertising aura emporté des millions d'entre nous.

Les mots de passe résistent
Les mots de passe sont un concept, pas une technologie, et la grande majorité d'entre nous va continuer à se servir de cet outil pour de nombreuses ressources, dans la vie privée comme dans la vie professionnelle. Alors certes, les mots de passe seront toujours utilisés en 2016, mais ils ne sont pas la panacée universelle, et vous avez donc intérêt à connaître certaines alternatives.
Cette année, Yahoo a annoncé le lancement d'une solution de sécurité qui utilise des périphériques mobiles plutôt qu'un mot de passe pour contrôler les accès, et nous avons même vu Google intégrer des fonctionnalités de verrouillage intelligent Smart Lock capables de déverrouiller votre smartphone en se servant des appareils présents à proximité.
Il existe des alternatives intéressantes aux mots de passe, même si ces derniers ont encore de beaux jours devant eux grâce à leur gratuité.
En matière de contrôle d'accès, la validation en deux étapes est un système efficace qui a tendance à se répandre et reste très utilisé chez de nombreux fournisseurs basés dans le cloud. Lorsqu'elle est proposée, vous avez tout intérêt à l'utiliser, surtout si vous n'êtes pas un spécialiste des mots de passe. Même s'il est interminable, le code de votre smartphone n'est pas inviolable, et le dispositif de lecture d'empreintes n'est peut-être pas si inutile.
Les mots de passe sont gratuits, et toutes les autres solutions ont généralement un coût, que ce soit sur le plan de la technologie ou de la complexité, ce qui explique que les mots de passe aient de beaux jours devant eux. Il est certain qu'en 2016, les problèmes liés aux mots de passe (réutilisation, stockage mal sécurisé, par exemple) ne risquent pas de disparaître. Espérons toutefois que nous saurons maintenir la vigilance des consommateurs et des entreprises !
L'Internet des objets : le principe de sécurité intégrée atteint le point d'ébullition Cela peut certes être amusant de posséder une de ces toutes nouvelles bouilloires WiFi, que vous pouvez allumer depuis votre smartphone, sans vous lever de votre fauteuil, mais ces objets normalement inoffensifs peuvent aussi révéler votre clé WiFi. Ceci n'est qu'un exemple de plus du problème existant au niveau de l'intégration de la sécurité.
S'ils ne sont pas protégés, chaque appareil périphérique, chaque téléviseur ou système stéréo intelligent, chaque système d'éclairage ou de sécurité domotique, et même ces nouveaux réfrigérateurs à la mode et ces voitures autonomes, bref tout ce qui est connecté à un réseau peut être la cible d'un hacker.
Les cybercriminels testent le matériel, analysent les ondes et recueillent mots de passe et autres données personnelles, quel que soit l'emplacement où ces informations sont conservées. Dans ce nouveau monde d'objets connectés, le danger augmente à mesure que la technologie vieillit.
Nous sommes nombreux à avoir paramétré nos ordinateurs et nos appareils mobiles de manière à ce qu'ils se mettent à jour automatiquement. En même temps, aucun d'entre nous ne pense à gérer la sécurité de ses appareils domestiques et à installer la dernière version logicielle.
Les objets connectés du quotidien peuvent réveler votre clé Wifi, et être la cible d'un hacker…Nous devons revoir notre façon de considérer ces appareils.
Dans certains cas, il est impossible de les mettre à jour. Nous devons considérer ces appareils et ces gadgets comme des ordinateurs déguisés, et les protéger aussi bien que nous le ferions pour notre PC et notre téléphone. Nous allons continuer à voir de nombreuses choses surprenantes connectées à Internet, et si aucun effort n'est fait pour y intégrer la sécurité, le problème risque d'empirer, car certains fabricants ne prennent pas le temps de mesurer les risques que courent les objets connectés au réseau.
Pour revenir un instant à l'analogie avec la bouilloire, rappelons que, dans une entreprise, si un employé achète une bouilloire intelligente, personne ne va s'en inquiéter et personne ne s'attendra à ce que le département informatique ait son mot à dire sur ce genre d'achat. Nous devons donc revoir entièrement notre façon de considérer ces appareils.

Mettre à jour : un élément vital !
Aujourd'hui plus que jamais, il est absolument essentiel que chaque logiciel, appareil, gadget ou équipement soit mis à jour.
Les constructeurs de voitures autonomes tels que Google annoncent déjà qu'ils assumeront la responsabilité des infractions au code de la route, et éventuellement des accidents ou des blessures corporelles dont leurs véhicules seraient responsables. Maigre consolation, avouons-le, si vous êtes victime d'un accident parce que vous avez oublié d'installer la dernière version du logiciel sur votre voiture … À mesure que les systèmes logiciels intelligents s'installent dans nos vies de multiples manières, ces mêmes logiciels pourraient décider de mettre votre vie en danger, il faut en être conscient.
Il va réellement devenir impératif que vous mettiez systématiquement vos logiciels à jour, en même temps que vos autres appareils. Un jour, cela vous sauvera peut-être la vie…

Réagissez à cet article

Source : *Cyber-Sécurité : AVG dévoile ses prévisions pour 2016 – Global Security Mag Online*

Apple contre le projet de loi britannique sur le renseignement !

Apple contre le projet de loi britannique sur le renseignement !

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Pour la firme de Cupertino, affaiblir les techniques de chiffrement, comme le souhaite le gouvernement britannique, reviendrait à diminuer la sécurité des « données personnelles de millions de citoyens respectueux des lois« . La création d'une porte dérobée présente, elle, un risque majeur : « une clef laissée sous le paillasson ne serait pas là uniquement pour les gentils. Les méchants sauraient la trouver également. » Voici en substance les points qu'Apple a voulu souligner à la commission en charge de ce projet de loi.

Autre point sensible : la modification du fonctionnement de iMessage pour pouvoir être écouté « placerait une entreprise comme Apple, dont la relation avec les clients est en partie construite sur un esprit de confiance quant à la confidentialité des données, dans une position très difficile« .

La commission saura-t-elle prendre en compte ce genre de considérations ? À suivre !

Réagissez à cet article

Source : *Apple contre le projet de loi britannique sur le renseignement !*

L’histoire interdite du piratage informatique (Documentaire)

L’histoire interdite du piratage informatique (Documentaire)

Hacker
C’est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd’hui ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

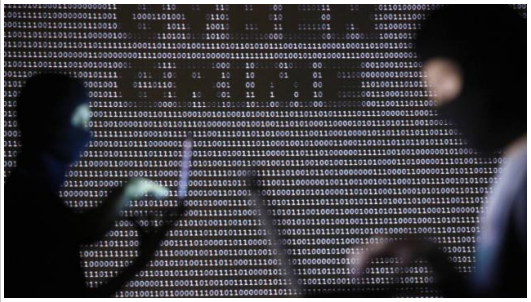
Réagissez à cet article

Source : *[Documentaire] L’histoire interdite du piratage informatique – TrLoad.net | Download Info | Video | Global Music Video | Top Videos, Artist, Songs, Free Mobile Music Download*

Crainte d’attentats pilotés à partir d’Internet en 2016

Crainte d’attentats pilotés à partir d’Internet en 2016

Les experts en cybercriminalité craignent beaucoup pour l'année à venir. Notamment des attentats déclenchés à distance.



Multiplication des demandes de rançons, perfectionnement des attaques par e-mail, détournement des objets connectés… 2016 ne devrait pas faire chômer les experts de la cybercriminalité, qui craignent de plus en plus un attentat déclenché à distance.

Demandez au bureau du Cercle européen de la sécurité et des systèmes d'information, qui fédère les professionnels du secteur quelle est la plus grande menace planant sur nos têtes, et la réponse sera unanime: « Le #cyber-sabotage, ou #cyber-terrorisme. L'attaque informatique d'un système lourd, qui aura des impacts environnementaux ou humains : polluer l'eau, faire exploser une usine, faire dérailler un train… » Les hackers – États, mafias ou groupes militants – utilisent des méthodes de plus en plus sophistiquées pour « casser » les systèmes informatiques de leurs cibles. À l'exemple de ce haut-fourneau allemand mis hors service il y a un an, on peut tout à fait envisager une cyberattaque contre un équipement vital.

L'éditeur américain Varonis envisage une variante retentissante, une cyberattaque contre la campagne présidentielle américaine. « Elle aura pour conséquence une violation importante des données qui exposera l'identité des donateurs, leurs numéros de carte de crédit et leurs affinités politiques confidentielles », prévoit-il. De quoi provoquer un joyeux désordre.

« Cheval de Troie »

Pour atteindre leurs cibles, les pirates informatiques apprécient particulièrement la technique du « cheval de Troie », qui consiste à faire pénétrer un « malware » (logiciel malveillant) sur les appareils des employés, d'où il pourra progresser vers les unités centrales. Et pour ce faire, une méthode prisée est le « spear phishing », l'envoi de courriels de plus en plus personnalisés, pour amener le destinataire à ouvrir un lien corrompu ou une pièce jointe infectée.

Cette méthode est également utilisée pour faire chanter les gens, chefs d'entreprise ou particuliers, après avoir dérobé et/ou crypter des données – de la comptabilité d'une société aux photos de vacances– qui ne sont rendues et/ou décryptées que contre rançon.

La même méthode peut aussi permettre à une entreprise d'espionner un concurrent. « L'année prochaine, ou dans les deux prochaines années, je pense qu'il va y avoir des vraies affaires qui vont sortir sur le sujet », estime Jérôme Robert, directeur du marketing de la société de conseil française Lexsi.

Smartphones peu protégés

« Il y a beaucoup d'entreprises qui ont déjà utilisé des détectives privés, il n'y a pas de raison qu'elles ne le fassent pas dans le cybermonde », remarque-t-il. Autre préoccupation des spécialistes: le glissement de la vie numérique vers des smartphones qui pèchent parfois par manque de protections.

« Il y a quasiment plus maintenant de smartphones qu'il y a d'ordinateurs, des smartphones qui sont allumés quasiment 24 heures sur 24, qui nous suivent partout », note Thierry Karsenti chez l'éditeur d'antivirus israélien Check Point. « Or, ils ont finalement beaucoup plus de connectivité que les équipements informatiques traditionnels. Ils ont même des oreilles puisqu'il y a un micro, ils ont même une caméra, et ils stockent tout un tas d'informations à la fois professionnelles et personnelles. C'est beaucoup plus embêtant de se faire pirater son smartphone que se faire pirater son ordinateur ! »

« Paradoxalement, si vous regardez la sécurité, vous avez beaucoup plus de sécurité sur un ordinateur », poursuit M. Karsenti. « Alors que les smartphones ou les tablettes n'ont absolument rien en termes de sécurité. » Et le développement des paiements par smartphone devrait allécher les hackers, généralement motivés par l'argent.

Objets connectés détournés

Même préoccupation pour les objets connectés, dont le nombre devrait exploser ces prochaines années. Ceux-ci sont, selon Lam Son Nguyen, expert en sécurité internet chez Intel Security, « souvent conçus sans tenir compte des aspects sécurité ». « Ils vont être susceptibles d'être attaqués par des personnes développant des solutions malveillantes », prévient-il.

Jusqu'à présent, on a surtout vu des hackers s'emparer de données d'utilisateurs stockées sur des serveurs distants des fabricants – dans le « cloud » -, et pas les objets eux-mêmes détournés à distance. « Pour les objets destinés aux consommateurs, il devrait y avoir des attaques qui seront plus des galops d'essai, des jeux, pour se faire plaisir. Je ne vois pas de grosse activité cybercriminelle sur les objets connectés », car il n'y aura sans doute pas d'argent à en tirer dans l'immédiat, juge Jérôme Robert chez Lexsi.

Réagissez à cet article

Source : *Cybercriminalité. Crainte d'attentats déclenchés à distance en 2016*

Les super cartes bancaires débarquent

	Les super cartes bancaires débarquent

Pour lutter contre la fraude, les banques misent sur la technologie. Demain, on paiera avec une carte à code éphémère ou un smartphone à reconnaissance faciale.

Cette révolution est à portée de main. Dans quelques mois, tout devrait changer… dans votre portefeuille. Votre carte bancaire va s'offrir une deuxième jeunesse. Un relooking qui porte un nom barbare : «cryptogramme dynamique». Ce qui, en français, signifie que les trois petits chiffres, situés au verso de votre carte, changeront au bout de quelques minutes.
Les plus grands fabricants de cartes bancaires au monde, Gemalto et Oberthur, ont lancé ces derniers mois la commercialisation de cette technologie. BNP Paribas, la Banque postale, la Société générale… La quasi-totalité des établissements financiers français sont en train de la tester auprès de leurs clients.

Qui va payer ?
Objectif affiché : mieux lutter contre la fraude à la carte bancaire. Un fléau dont la finance aimerait bien se débarrasser. Pas question de laisser les arnaques et les fraudes nuire à l'engouement des Français pour ce mode de paiement. Imaginez, le 5 décembre dernier, la France a battu un record : 42 millions de transactions par carte bancaire en un week-end. Soit 12 % de plus que lors du premier samedi de décembre 2014 !
Un effet logique du boom du commerce en ligne. Pourtant, les banques se laissent encore quelques mois pour un développement à grande échelle de cette carte bancaire plus sécurisée. Car un petit détail reste encore à trancher. Ce bout de plastique bourré de technologies coûte plus cher à produire que la carte à puce classique. Qui va payer ? La banque, les commerçants ou le client ? Les réponses du milieu bancaire restent floues. Les banques trancheront ces prochains mois. Mais elles n'ont plus vraiment le temps de tergiverser. Des start-up dénommées FinTech (technologie financière) commencent déjà à les bousculer, notamment en utilisant le smartphone pour lancer de nouveaux modes de paiement. Et comme d'autres secteurs l'ont appris à leurs dépens, l'immobilisme face aux nouvelles technologies ne paye pas.
«2016 sera l'année des nouveaux modes de paiements», pronostique donc un cadre de banque. Nombre d'établissements ont, dans les cartons, de nouveaux produits qui n'attendent plus qu'une autorisation de la Cnil (Commission nationale de l'informatique et des libertés) pour passer des simples tests à la commercialisation. C'est le cas des technologies de biométrie utilisant des éléments du corps (empreinte digitale, vocale, etc.). Les bons vieux codes bancaires bientôt périmés ?

Un cryptogramme valable 20 minutes
Même largeur, agilité, finesse, robustesse, touché… A priori, rien ne la distingue de sa prédécesseur. A un détail près : la carte bancaire de nouvelle génération est équipée d'un écran. Tout petit. Pas de quoi regarder un film en haute définition. Non, mais tout de même assez large pour afficher, en noir et blanc, les trois chiffres du fameux cryptogramme visuel. Ce code de sécurité réclamé à chaque achat sur la Toile devient «dynamique». «Cette carte est équipée d'une horloge interne. Le code de sécurité sur l'écran change toutes les vingt minutes», explique Frédérique Richert, marketing manageur chez Gemalto, le leadeur mondial de la carte à puce, qui commercialise depuis quelques semaines cette nouvelle technologie. «Cette carte lutte mieux contre la fraude», ajoute-t-elle.

Réduire le coût des fraudes
A priori, rien ne change pour l'utilisateur. Pour effectuer un achat en ligne, il doit toujours remplir les mêmes formulaires en indiquant son nom, son numéro de carte bancaire, la date de validité et le cryptogramme. La différence, c'est que ces coordonnées ont une durée de vie limitée. Si un pirate informatique les vole, il ne peut alors les utiliser que pendant une vingtaine de minutes. Un laps de temps, a priori, trop court pour multiplier les achats sur le Web ou revendre ces informations à d'autres escrocs.
La plupart des grands réseaux bancaires sont en train de tester auprès de leurs clients cette nouvelle technologie. Ainsi, BPCE a équipé depuis plusieurs semaines un millier de clients. BPCE utilise la technologie d'Oberthur, concurrent de Gemalto. Avec un avantage, celui de réduire le coût des fraudes. Car les banques assument une partie du coût de l'arnaque : indemnisation du client pour les achats réalisés frauduleusement, coût du changement du support, etc. «Nous regardons à la fois l'effet de cette nouvelle technologie sur le coût lié à la fraude mais aussi sur la confiance des utilisateurs dans le paiement en ligne, dans l'usage des cartes bancaires», explique Nicolas Chatillon, directeur du développement fonctions transverses du groupe BPCE. Un point stratégique. Car un possesseur de carte bancaire en confiance, c'est un consommateur qui dépense !

Réagissez à cet article

Source : *Les super cartes bancaires débarquent*