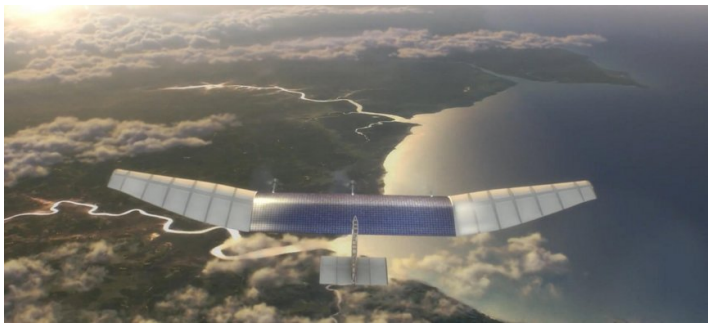
Boeing planche sur des drones capables de déployer des logiciels espions | Le Net Expert Informatique



Boeing planche sur des drones capables de déployer des logiciels espions

Le spécialiste de l'aéronautique Boeing travaille sur la production de drones capables d'infecter les ordinateurs et smartphones aux alentours.

En début de mois, nous apprenions que la société milanaise Hacking Team, qui propose des outils d'interception des communications entre internautes aux gouvernements ou aux pouvoirs publics, avait elle-même été hackée. Quelque 400 gigaoctets de données confidentielles ont été récupérés révélant la nature des relations entre Hacking Team et ses partenaires. Ces documents sont mis à disposition sur le site Wikileaks.
Parmi les informations révélées, la filiale Insitu de Boeing, spécialisée dans la production de drones, avait signé un partenariat avec Hacking Team afin de procéder à des hacks à distance. L'appareil serait ainsi en mesure de cibler un smartphone ou un ordinateur portable en particulier puis de l'infiltrer via un réseau Wi-Fi.
Selon le magazine The Intercept, qui rapporte l'information, le drone en question est prévu pour pouvoir accéder aux fichiers à distance, récupérer le journal des appels, l'historique des messageries instantanées ou encore les emails.
Au sein des emails aspirés sur les serveurs de Hacking team, nous trouvons notamment une feuille de route datant du mois de juin. Celle-ci fait mention d'un petit appareil pouvant être transporté par un drone et capable de récupérer les données transitant via les réseaux.
Le document explique que l'attaque devra prendre en charge Windows 10 ainsi que le navigateur Microsoft Edge et Skype Web. Sur OS X, Hacking Team a finalisé un dispositif scannant les sauvegardes locales d'iTunes et planchait sur la capture des certificats d'iCloud et des images de l'application Photos.
Retrouvez tous les détails de ce projet en italien sur cette page.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spyware-logiciel-espion/actualite-774222-boeing-planche-drones-capables-deployer-spyware.html

---

Alerte partagez – Nouvelle faille Android…| Le Net

Expert Informatique

	**Alerte partagez – Nouvelle faille Android…**

En début de semaine l'affaire Stagefright révélait une faille majeure sur Android. Trend Micro en remet aujourd'hui une couche dévoilant une nouvelle faille critique. Non patchée par Google assure l'expert en sécurité.

Dure semaine pour Android. Trend Micro annonce la découvre d'une nouvelle faille qui cette fois permet de rendre le téléphone non fonctionnel. En début de semaine, l'affaire Stagefright avait déjà ébranlé l'aura de Google. Aucun correctif n'est encore disponible.
Quand cette faille est exploitée avec succès, le téléphone équipé d'Android devient silencieux. Plus d'alertes sur les messages, plus de sonnerie d'appel. Rien. Puis le téléphone se grippe, peu à peu, et s'arrête. La faille « est causée par un débordement d'entier lorsque le service de mediaserver analyse un fichier MKV. Il lit la mémoire de tampon ou écrit des données à l'adresse NULL lors de l'analyse des données audio » analyse Trend Micro.

Jelly Bean et Lollipop touchés
« La vulnérabilité réside dans le service mediaserver, qui est utilisé par Android pour les index de fichiers multimédias qui sont situés sur le périphérique Android. Ce service ne peut pas traiter correctement un fichier vidéo malformé utilisant le conteneur Matroska (généralement avec l'extension. mkv). Lorsque le processus ouvre un fichier MKV malformé, le service peut se bloquer (et avec lui, le reste du système d'exploitation) » explique Trend Micro.
Cette faille de sécurité peut être exploitée en incitant un internaute à visiter un site infecté, ou en lui faisant télécharger une application vérolée. Les versions d'Android impactées par cette faille courent d'Android 4.3 (Jelly Bean) à Android 5.1.1 (Lollipop).
Trend Micro a informé discrètement Google en mai dernier, mais l'entreprise n'aurait pas classé cette faille autrement qu'une «vulnérabilité de faible priorité », selon Trend Micro. Conséquence : aucun patch n'a été publié. Trend Micro prend donc aujourd'hui les devants et rend public cette faille, espérant que Google ait la même réactivité qu'avec Stagefright. Et Trend Micro en profite bien sûr pour faire la publicité de ses solutions, qui évidemment, protègent des complications de Google.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/android-a-nouveau-victime-d-une-faille-39823130.htm

---

Des chercheurs développent une étonnante attaque web sur

la DRAM | Le Net Expert Informatique

Des chercheurs développent une étonnante attaque web sur la DRAM

Des chercheurs ont réussi à exploiter un défaut nommé « Rowhammer » qui inquiéte depuis longtemps les experts de la sécurité informatique. Leur attaque, menée depuis le web, s'appuie sur JavaScript et cible la DRAM des ordinateurs, exposant des millions d'internautes.

On sait depuis plusieurs années que les cellules mémoire des ordinateurs sont vulnérables à une interférence intentionnelle. Mais un récent document de recherche explique comment mener une attaque depuis le web qui augmente considérablement le danger pour les utilisateurs. Ce document, publié par des institutions autrichiennes et françaises – il a été coécrit par Daniel Gruss et Stefan Mangard de l'Université de Technologie de Graz en Autriche, et par Clémentine Maurice de Technicolor et Eurecom en France – pourrait obliger les fondeurs à trouver en urgence une solution qui résout le défaut connu sous le nom de « Rowhammer ».
Pour augmenter la densité de la DRAM, les concepteurs n'ont cessé de rapprocher les cellules, les rendant vulnérables aux interférences électriques. Une technique décrite sous le nom de « rowhammering » permet de changer la valeur binaire des cellules adjacentes en activant de manière répétée une rangée donnée de cellules de mémoire. Pendant longtemps, les concepteurs se sont préoccupés de la fiabilité posée par cette fuite électrique, sans considérer la question de la sécurité. Mais cette approche est en train de changer rapidement.

Une attaque à distance en JavaScript
Plus tôt cette année, des chercheurs de Google ont annoncé qu'ils avaient réussi à développer deux exploits opérationnels : le premier leur a permis de mener une attaque par escalade de privilège et l'autre utilise le changement de polarité induit par le défaut « Rowhammer » pour obtenir des privilèges au niveau du noyau. Mais, pour que l'attaque réussisse, ils avaient été obligés d'installer leurs exploits sur la machine de l'utilisateur. Ce qui est remarquable dans ce nouveau document, c'est qu'une telle attaque pourrait être menée depuis le web en s'appuyant sur JavaScript. Le code proof-of-concept Rowhammer.js a été testé dans Firefox 39, « mais notre technique d'attaque est générique et peut être appliquée avec tout type d'architecture, de langage de programmation et d'environnement runtime », ont-ils écrit. Elle ne nécessite pas un accès physique à un ordinateur, ce qui la rend beaucoup plus dangereuse.
Cela signifie également qu'un grand nombre de personnes pourraient être ciblées depuis le web, ce qui augmente le pool de victimes potentielles. « Étant donné que l'attaque peut être lancée simultanément et furtivement contre un nombre arbitraire de machines, elle représente une énorme menace pour la sécurité », ont-ils ajouté. De plus, un grand nombre d'ordinateurs sont vulnérables, puisque l'attaque est indépendante du système d'exploitation, et que le bug « Rowhammer » affecte de nombreux types d'architectures de puces. Les chercheurs essayent encore de savoir combien de systèmes seraient vulnérables à leur attaque. Jusqu'à présent, ils n'ont pas développé d'exploit qui permettrait d'obtenir un accès root à un ordinateur en exploitant le « rowhammering », mais ils pensent que des pirates pourraient éventuellement étendre les capacités de l'exploit qu'ils ont découvert.

Bloquer JavaScript avec NoScript
Tant que les fondeurs ne trouvent pas de solution à long terme pour résoudre le problème Rowhammer.js, les chercheurs proposent d'inclure dans les navigateurs web un test permettant de vérifier si l'ordinateur est vulnérable. Si le test est positif, « JavaScript doit être mis sous contrôle pour éliminer la possibilité d'un exploit. Même si le système est très probablement résistant, il faut laisser à l'utilisateur la possibilité d'activer explicitement JavaScript quand il visite une page web », écrivent-ils. Une autre alternative serait de désactiver complètement JavaScript en utilisant une extension comme NoScript. Mais de nombreux sites web reposent sur JavaScript et sans lui, la consultation de ces sites devient problématique.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemondeinformatique.fr/actualites/lire-des-chercheurs-developpent-une-etonnante-attaque-web-sur-la-dram-61920.html
Par Jean Elyan et IDG NS

Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité | Le Net Expert Informatique

Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité

Lors des Assises de la Sécurité MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation tout en préservant la confidentialité des données personnelles. Pour Sid-Ahmed Lazizi, Directeur Général France, MobileIron Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable.

Global Security Mag : Qu'allez-vous présenter à l'occasion des Assises de la Sécurité ?
Sid-Ahmed Lazizi : Lors des Assises de la Sécurité, MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation modernes dans le cadre d'une utilisation de terminaux divers et variés. Elle prend en compte l'identité, le contexte et les règles de confidentialité établies pour définir le niveau approprié d'accès aux données et services des entreprises. MobileIron sécurise les données statiques sur les terminaux, dans les applications et dans le cloud. Son action de sécurisation porte également sur les data-in-motion (données dynamiques) lorsqu'elles circulent entre le réseau d'une entreprise, les terminaux et les référentiels de stockage. Grâce à MobileIron, les services informatiques peuvent assurer la sécurité des données des entreprises où qu'elles soient, tout en préservant la confidentialité des données personnelles des employés. Cette plateforme se compose de trois produits :
MobileIron Core : serveur qui permet aux services informatiques de définir des règles de sécurité et de gestion sur les systèmes d'exploitation mobiles les plus répandus
MobileIron Client : logiciel qui réside sur les appareils afin d'y appliquer les règles définies par le service informatique
MobileIron Sentry : passerelle intelligente qui sécurise le trafic des données entre les appareils mobiles et les systèmes back-end de l'entreprise

GS Mag : Quelle va être le thème de votre conférence cette année ?
Sid-Ahmed Lazizi : Le thème de notre conférence qui aura lieu le 2 octobre à 11h est « Le nouveau modèle de sécurité en entreprise ». Les employés choisissent de plus en plus de travailler sur des terminaux mobiles dotés de systèmes d'exploitation modernes tels que Android, iOS ou Windows 10, et ce en lieu et place des ordinateurs de bureau traditionnels et des outils conçus pour Windows. Le défi engendré en termes de sécurité par ces nouveaux systèmes d'exploitation est bien différent de ceux de l'ancienne ère du PC, ce qui nécessite d'aborder la situation sous un autre angle et d'utiliser une technologie nouvelle.

GS Mag : Quel est votre message aux RSSI ?
Sid-Ahmed Lazizi : À mesure que les terminaux mobiles et objets connectés se multiplient, s'adaptent et intègrent le monde de l'entreprise, les services informatiques découvrent de nouvelles menaces qui pèsent sur les données et doivent relever de nouveaux défis pour les protéger. Ils doivent repenser leurs stratégies et infrastructures informatiques pour permettre une utilisation sûre et efficace de ces terminaux et objets, qui représentent une véritable opportunité d'augmenter la productivité des collaborateurs de l'entreprise.
Les technologies portables étant relativement récentes, elles se développent et s'améliorent constamment. Elles présentent le même défi que celui des smartphones quand ces derniers sont apparus. En effet, lorsque les technologies mobiles ont commencé à s'imposer, la réponse initiale des directions informatiques fut de réguler ou restreindre les accès mobiles. Cette approche s'est révélée majoritairement inefficace, les employés trouvant de plus en plus de solutions pour contourner les recommandations de leur département IT.
Liés aux smartphones, les technologies portables vont très rapidement débarquer en entreprise Etant donné que la restriction n'est pas toujours une option viable, reste le problème de la sécurité des données. Pour commencer, les départements informatiques devraient se concentrer sur les plateformes qui permettent de gérer et de sécuriser au niveau fichier, ce que certaines sociétés avancées font déjà sur mobile. Ces types de services garantissent la protection des données de l'entreprise même si le dépôt central de stockage des données est corrompu.
Les départements informatiques devront également travailler main dans la main avec les équipes RH et juridique pour définir un cadre d'utilisation clair de ces appareils mobiles au sein de l'entreprise, tout comme rappeler les risques de sécurité induits par l'accès aux données de l'entreprise sur des appareils portables ou similaires. Idéalement, ces règlements devraient être communiqués aux employés de façon positive pour valider le potentiel d'exploitation des appareils mobiles à la fois sur le plan professionnel et personnel.

Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable. Cela permettra de favoriser la relation de confiance entre les directions informatiques et les employés.

Source : https://www.globalsecuritymag.fr/Sid-Ahmed-Lazizi-MobileIron-Les,20150716,54434.html

---

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team | Le Net

Expert Informatique

	Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team

Anticipant sur les besoins de ses clients, Hacking Team s'est assuré d'être prêt au lancement de Windows 10. La société italienne a adapté ses outils pour être capable d'installer un backdoor sous Windows 10, et ainsi de pouvoir collecter à distance toutes les frappes de touches au clavier.

Windows 10 n'est pas encore officiellement sorti, mais les firmes qui fournissent aux autorités les outils permettant d'accéder à distance aux données sont déjà à pied d'oeuvre pour s'adapter au niveau système d'exploitation de Microsoft. Ainsi l'entreprise italienne Hacking Team, dont les e-mails ont fuité ce mois-ci, s'est assurée dès l'an dernier de pouvoir fournir à ses clients de quoi espionner des utilisateurs de Windows 10.

« Nous avons testé Windows 10 Preview et ça fonctionne », a ainsi expliqué Marco Valleri, le directeur de Hacking Team, dans un e-mail du 4 novembre 2014. Il répondait à l'ancien responsable des opérations à Singapour, Serge Woon, qui se demandait si « RCS 9.4 supporte Windows 8.2 » (en fait Windows 10). RCS est l'acronyme de « Remote Control System », le malware qui permet à Hacking Team de prendre à distance le contrôle d'un ordinateur pour accéder à ses données.

Un autre e-mail du 29 juin 2015 montre que deux employés de Hacking Team, Marco Fontana et Andrea Di Pasquale, ont testé avec succès l'installation hors ligne de plusieurs outils sur Windows 10 Enterprise Insider Preview. Ils disent avoir vérifié notamment « l'installation d'un backdoor », « l'exportation de preuves depuis le backdoor », et la « désinstallation du backdoor ».

« Super ! », s'enthousiasme le directeur technique Marco Valleri, qui propose aussitôt une réunion pour déployer la mise à jour dans un git, probablement celui de RCS.

La société Hacking Team dispose également d'un outil invisible pour Windows 10 permettant de collecter toutes les frappes de touches au clavier (un « keylogger »), comme le montre un courriel du 5 juin. Marco Fontana, qui semble être une petite star dans l'entreprise, y rend compte d'une réunion du mercredi 3 juin 2015, où « l'un des thèmes de la réunion était le test du mécanisme d'injection dans l'application Metro ».

Il explique que « le POC du keylogger pour Windows 10 est prêt et peut être testé pour vérifier sa « compatibilité » avec les antivirus ». Le POC (Proof-of-concept) est une démonstration de faisabilité.

Dans un e-mail du 15 juin, Marco Fontana précise à son équipe qu'il a testé une « technique d'injection dans l'application Metro de Windows 10 », et que « l'exécutable 'ExeLoader' injecte la DLL ApiHookDll dans un processeur notepad.exe et capture les touches ». Il s'agit d'un POC visant à collecter les touches tapées sous sur l'application « Bloc Notes » de Windows 10.

« Si tout fonctionne correctement, dans le dossier temporaire de Windows (%temp%) vous verrez un fichier texte créé qui contient les touches enfoncées dans notepad. Le fichier a un préfixe KBD_ et une valeur aléatoire (ex: KBD_000407E600C553CE.txt) ».

Tout l'objet du logiciel RCS de Hacking Team est justement d'installer à distance les backdoors qui permettent d'installer des outils tels que ce keylogger, lequel permet ensuite de récupérer, par exemple, les mots de passe saisis pour accéder à des comptes e-mail, ou des mots de passe de clés de chiffrement.

« On ne peut pas croire à la sécurité d'un OS pour le grand public », s'était amusé en novembre dernier David Vincenzetti, le président de Hacking Team, en lisant une actualité selon laquelle Windows 10 pourrait signer la fin des malwares.

Source : http://www.numerama.com/magazine/33727-deja-des-backdoors-et-keyloggers-pour-windows-10-chez-hacking-team.html
par Guillaume Champeau

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance | Le Net Expert Informatique

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance

De nouvelles informations émergent des centaines de milliers d'e-mails piratés au fabricant de logiciels espions Hacking Team. Des échanges ont montré que l'entreprise italienne a été contactée par Insitu, un fabricant de drones appartenant à Boeing, pour travailler sur un système qui permettrait aux engins de pirater des réseaux Wi-Fi à distance, a relevé le site The Intercept.

Un rapport daté du 1er juillet montre d'ailleurs qu'Hacking Team travaillait sur un système d'injection réseau utilisable par drone, c'est-à-dire « un équipement conçu pour insérer du code malicieux dans les communications d'un réseau Wi-Fi », explique le site spécialisé Ars Technica.

« Nous ne pouvons vendre nos produits qu'à des entités gouvernementales »

Selon un premier e-mail envoyé en avril, Insitu s'est montré intéressé par une présentation de Hacking Team à l'IDEX 2015, un salon de la défense qui s'est tenu aux Emirats arabes unis en février. « Nous aimerions potentiellement intégrer votre système de piratage de Wi-Fi à un système aérien et nous souhaiterions prendre contact avec un de vos ingénieurs qui pourrait nous expliquer, plus en détail, les capacités de l'outil, notamment la taille, le poids et les spécifications de votre système Galileo [un logiciel espion] », écrit alors Giuseppe Venneri, ingénieur mécanique en formation chez Insitu.

« Gardez à l'esprit que nous ne pouvons vendre nos produits qu'à des entités gouvernementales », répond un responsable de Hacking Team, sans fermer la porte à une collaboration. Selon un e-mail interne, le même responsable de Hacking Team indique qu'Insitu travaille avec des agences gouvernementales et demande quels produits seraient les plus adaptés à la demande du fabricant.

Aucun accord trouvé

La correspondance entre Insitu et Hacking Team s'est arrêtée en mai et a été fortement retardée par des discussions d'ordre légal, chaque entreprise souhaitant utiliser son propre accord de non-divulgation avant de démarrer les discussions commerciales. Les courriels les plus récents suggèrent que les négociations n'ont jamais commencé.

Le vendeur de logiciels espions italien Hacking Team est sous pression depuis un piratage qui a conduit à la publication de plus de 400 gigabits de données confidentielles début juillet. Certains documents indiquent notamment que l'entreprise pourrait avoir vendu des solutions de surveillance à des pays sous embargo comme le Soudan et la Russie.

Source : http://www.lemonde.fr/pixels/article/2015/07/20/hacking-team-a-travaille-sur-un-drone-capable-d-infecter-des-ordinateurs-a-distance_4691260_4408996.html
Par Florian Reynaud

Ashley Madison tente de rassurer ses clients infidèles | Le Net Expert Informatique

12	Ashley Madison tente de rassurer ses clients infidèles

Alors qu'un maître-chanteur menace de diffuser un fichier de près de 40 millions d'hommes et de femmes inscrits sur Ashley Madison pour tromper leur conjoint, l'éditeur affirme qu'il a trouvé la parade : la loi américaine de protection du droit d'auteur.

Ce matin, nous rapportions que l'éditeur canadien du site de rencontres adultères Ashley Madison s'était fait pirater une base de données avec les noms de quelques 37 millions d'utilisateurs du service qui promet discrétion et anonymat. Alors qu'ils n'en ont publié que des extraits, les hackers promettent de publier l'intégralité de la base de données sur internet si la société Avid Life Media basée à Toronto ne ferme pas Ashley Madison et deux autres sites internet qu'elle édite.
Mais l'entreprise n'entend visiblement pas céder aux pressions et essaye de rassurer tant bien que faire se peut ses clients. Dans un communiqué envoyé à Numerama, Avid Life Media explique les contre-mesures mises en place, qui pourraient toutefois s'avérer vaines si les hackers décidaient de mettre leurs menaces à exécution et de passer par un réseau P2P incontrôlable comme BitTorrent pour publier la base de données intégrale. La société mise sur la loi américaine sur le droit d'auteur sur internet (le DMCA) qui impose aux plateformes de supprimer les contenus publiés sans l'autorisation des ayants droit lorsqu'elles sont notifiés. Elle estime que sa base de données est couverte par le DMCA.
Jusqu'à présent, les extraits des bases communiqués à titre de preuve du piratage ont effectivement été mis en ligne sur des sites de téléchargement direct qui acceptent de retirer les liens illicites qui leur sont notifiés, et qui l'ont fait. Mais ce ne sera pas le cas si les hackers (ou « le » hacker si l'on en croit les soupçons que porte l'entreprise sur un ancien collaborateur) décident, par exemple, de publier un simple fichier .torrent, comme l'ont fait récemment les pirates de Hacking Team. Il n'y a alors personne à qui envoyer une demande de DMCA, et/ou beaucoup de sites de liens BitTorrent qui ne les respectent pas.

Voici le communiqué reçu :
Suite à une intrusion injustifiée et criminelle dans notre système samedi 18 juillet 2015, Avid Life Media a immédiatement engagé l'une des équipes de sécurité informatique les plus pointues au monde afin de prendre toutes les mesures possibles pour résoudre cette crise.
En utilisant la Digital Millennium Copyright Act (DMCA), notre équipe a supprimé avec succès tous les messages liés à cet incident ainsi que toutes les Informations Personnelles Identifiables (PII) publiées en ligne à propos de nos utilisateurs.
La confidentialité des informations concernant nos utilisateurs a toujours été notre plus grande priorité, et nous sommes rassurés que les dispositions contenues dans le DMCA aient permis de résoudre ce problème efficacement. Notre équipe de spécialistes et de professionnels sécurité informatique, en plus de faire appliquer la loi, continuent d'enquêter sur cet incident, et nous publierons de futurs bulletins dès que de nouveaux éléments verront le jour.

Source : http://www.numerama.com/magazine/33730-quand-ashley-madison-tente-de-rassurer-ses-clients-infideles.html
Par Guillaume Champeau

Le site de rencontre Madison Ashley piraté – l'analyse de Kaspersky Lab | Le Net Expert Informatique

Le site de rencontre Madison Ashley piraté – l'analyse de Kaspersky Lab

Le site de rencontres adultères canadien Ashley Madison, qui revendique plus de 37 millions d'inscrits, a été victime d'une attaque informatique ayant pour but de voler les données personnelles d'un grand nombre d'utilisateurs. Ces données ont été brièvement mises en ligne.

Marta Janus, chercheuse en sécurité au sein de l'équipe de recherche et d'analyse (GReAT) du spécialiste en sécurité Kaspersky Lab, revient sur cette attaque :
Marta Janus « L'attaque subie par Madison Ashley nous rappelle à quel point il est important pour toutes les entreprises de mettre en place des mesures de sécurité contre les cyberattaques, afin de protéger les données personnelles de leurs utilisateurs. Un internaute qui accepte de confier certaines de ses données privées à un site web devrait être assuré que ses informations seront conservées de la façon la plus sécurisée qui soit, et les entreprises concernées devraient pouvoir s'y engager.
Il faut également rappeler que toutes les failles de sécurité qui entrainent des fuites de données privées sont un problème, quelles que soit la nature du site visé, sa moralité et même sa légalité. Dans le cas de l'attaque contre Ashley Madison, l'affaire est très sérieuse car la fuite concerne des informations comme les noms, les adresses ou encore les données bancaires. Une fois rendues publiques, ces informations pourraient par exemple être utilisées pour voler de l'argent.
Les raisons pour lesquelles une entreprise peut être victime d'une cyber attaque sont nombreuses – argent, politique ou même éthique. N'importe quelle entreprise peut être la cible d'une attaque et même si les solutions de sécurité réduisent les risques que cette attaque soit fructueuse pour les criminels, d'autres mesures existent pour une protection renforcée. Je pense notamment aux mises à jour logicielles, encore trop souvent remises au lendemain, à la réalisation régulière d'audits de sécurité ou encore au test des infrastructures. Le meilleur moyen de lutter contre ce type de cyberattaques est de se protéger avant qu'elles ne frappent en disposant d'une stratégie de sécurité complète et efficace. »

Source : https://www.globalsecuritymag.fr/Site-de-rencontre-pirate-l-analyse,20150720,54540.html
par Kaspersky Lab

Les Etats Unis devraient avoir peur des prochaines cyber-attaques ? | Le Net Expert Informatique

Le nouvel Economiste	Les Etats Unis devraient avoir peur des prochaines cyber-attaques ?

Mercredi dernier, la Bourse de New York et United Airlines ont suspendu leurs activités pendant plusieurs heures en raison de problèmes informatiques mystérieux, tandis que le site Internet du 'Wall Street Journal' a brièvement disparu.

Tous trois ont insisté pour dire qu'il s'agissait de problèmes techniques, et non d'attaques malveillantes. Mais l'inquiétude monte après des agressions contre de puissantes entreprises et agences américaines.
En février dernier, la compagnie d'assurance Anthem révélait que des pirates informatiques avaient volé les données de plus de 80 millions de clients. L'Office of Personnel Management, basé à Washington, révélait que des hackers avaient subtilisé des données de millions d'employés fédéraux. Commerçants ou banques, plusieurs entreprises ont aussi été attaquées.
Mercredi, au moment où la Bourse de New York était suspendue, l'université de Cambridge et le groupe d'assurances Lloyds publiaient un rapport affirmant que si une cyber-attaque s'en prenait au réseau électrique américain, les dommages pourraient s'élever à mille milliards de dollars. Quelques minutes plus tard, le directeur du FBI, James Comey, déclarait devant le Congrès qu'il avait des difficultés à venir à bout des systèmes de chiffrage des djihadistes. En mai, M. Comey expliquait que les terroristes islamiques avaient adopté l'idée d'utiliser des logiciels malveillants contre les infrastructures stratégiques. La chose est plutôt effrayante.
La question clé que les investisseurs, les politiciens et les électeurs doivent se poser est non seulement d'envisager qui pourrait être la prochaine cible, mais aussi de savoir si Washington est capable de face à ces attaques. La réponse est certainement non.
Sur le papier, les ressources ne manquent pas. En début d'année, le président Barack Obama a par exemple affecté 14 milliards de dollars à la lutte contre le cyberterrorisme. Mais le principal problème n'est plus tant un manque d'argent que de coordination : alors que la peur se propage, un nombre ahurissant d'organismes et de groupes de travail différents se sont lancés dans la lutte contre le cyberterrorisme, souvent en collaborant très peu entre eux. L'institution censée être en charge des menaces est le Département de la Sécurité nationale, mais ses compétences laissent sceptiques les responsables militaires. Le Pentagone a son propre personnel affecté aux cyberattaques, tout comme les services secrets.
"Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur les défenses cybernétiques. Mais avec le tribalisme exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace"
La Maison-Blanche a tenté d'obliger ces organismes à travailler ensemble. De leur côté, des organismes civils comme la Commission de réglementation nucléaire ont aussi commencé à tenir des réunions discrètes avec d'autres organismes cet automne sur ces questions. Mais la collaboration entre les secteurs reste inégale. "Le niveau de préparation des différents organismes varie énormément" admet un haut responsable de Washington au centre de cette mission. De plus, y ajouter des organismes du secteur privé entraînera une dégradation plus profonde de la situation : non seulement le Pentagone se méfie du partage de données avec d'autres institutions, mais les entreprises sont souvent terrifiées à l'idée de révéler les attaques dont elles ont fait l'objet.
Existe-t-il une solution ? Une réponse sensée pourrait être de créer une nouvelle entité qui serait l'entité centrale de lutte contre le cyberterrorisme. Il existe des précédents, la plupart des régulateurs de Washington ayant été créés pour répondre à une nouvelle menace. La Securities and Exchange Commission, par exemple, a été créée après le krach de 1929 ; la Food and Drug Administration, après des scandales concernant des médicaments dangereux. Une deuxième option serait de relancer le DHS (Department of Homeland Security) afin que celui-ci se focalise sur la lutte contre les cyberattaques. Il pourrait, par exemple, s'appeler ministère de la Sécurité Intérieure et Cybernétique.
Quoi qu'il en soit, Washington a besoin de répondre à la question qu'Henry Kissinger posait pour l'Europe : en temps de crise, "Qui dois-je appeler ?" Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur la défense cybernétique. Mais avec l'esprit de clan exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace. Il faut juste espérer que ce "quelque chose" ne sera pas trop dévastateur, comme une attaque réelle des transports ou des marchés.

Source : http://www.lenouveleconomiste.fr/financial-times/les-prochaines-cyber-attaques-contres-les-etats-unis-seront-terribles-27703/
Par David Pilling

Les entreprises attendraient-elles gentiment les attaques ? | Le Net Expert Informatique

Les entreprises attendraient-elles gentiment les attaques ?

Qu’on se le dise : n’importe qui peut se faire attaquer, qu’il s’agisse d’une petite comme d’une grande entreprise.

En 2013, le New York Times a subit une cyberattaque de l’armée électronique syrienne ; un groupe d’activistes soutenant Bachard El Assad. Les auteurs ont ciblé la partie la moins sécurisée du réseau, les serveurs DNS alors qu’ils sont devenus la pierre angulaire de toute applications internes ou externes.
En juin dernier, l’US Army s’est faite attaquée par les mêmes hackers. Et ce, alors même que l’Etat--Major américain avait fait de la cyberdéfense une priorité en investissant fortement. Pourtant, ces deux attaques démontrent qu’ils sont faiblement protégés et que, quelque soit leur taille, toutes les entreprises ou organismes sont des cibles potentielles. Les services informatiques n’ont donc pas su s’adapter à ces nouvelles menaces.
En France, le 1er semestre fut dense en matière de cyberattaques : TV5 Monde, Charlie Hebdo et Thales ont fait l’objet de sévères attaques de leur système informatique. On se souvient que des documents présentés comme des pièces d’identité et des CV de proches des militaires français impliqués dans les opérations contre l’EI avaient été postés sur le compte Facebook de TV5Monde par les pirates.
L’attaque avait été initialement revendiquée par des inconnus se réclamant de Daech (Etat Islamique). L’enquête s’oriente en juin vers des hackeurs russes. Le vol de données semble être le principal objectif des hackers.
Quelques semaines plus tôt, Manuel Valls annonçait que la défense française allait intégrer des community managers et hackers, plus à même de contrer les attaques. Une méthode innovante…. mais est--ce suffisant pour protéger une infrastructure réseau ?

Les entreprises françaises en mal d’inspiration ?
En général, les entreprises ne communiquent pas ou très peu sur leurs attaques. En effet, en regardant de plus près les cyberattaques subies en France, on s’aperçoit que les informaticiens n’ont pas su anticiper les nouvelles menaces. Ils ont préféré sécuriser leurs réseaux grâce à des méthodes utilisées depuis des décennies. Malheureusement, cela ne s’avère plus suffisant pour contrer les nouvelles menaces et les nouvelles techniques utilisées par les hackers.
En parallèle, cela met en exergue les problèmes d’investissement que les entreprises rencontrent et leurs manques de réactions.
Selon une étude menée par IDC [1], si la plupart des organisations sont conscientes des risques de sécurité liés aux serveurs DNS (82 % des répondants étaient conscients des menaces, qu’ils ont reconnues), l’essentiel des budgets en sécurité réseau est encore consacré à des solutions de sécurité plus traditionnelles telles que les pare--feu (68 %).
L’étude d’IDC a également révélé que même si 85 % des répondants disposent des fonctions de sécurité du DNS de base, les entreprises restent vulnérables, car ces fonctions sont généralement inefficaces en cas d’attaque.
Enfin, 73% des entreprises françaises ont subies des attaques sur leurs serveurs DNS mais elles ne sont que 7% à les considérer comme une très grande menace contre 27% aux Etats-- Unis, alors que les dégâts subies lors de ces attaques ont été très importants (vol de données, interruption de service, …).
Sans prise de conscience des responsables informatiques français, les cyberattaques ne cesseront de s’intensifier. Avec la multiplication des appareils connectés à internet, dans tous les domaines d’activités (hôpitaux, grandes administrations ou petites entreprises, dans la banque, l’énergie, la défense,), les données continueront d’avoir de la valeur aux yeux des pirates informatiques si les RSI ne changent pas leurs méthodes de protection.

[1] Enquête IDC sur la sécurité des serveurs DNS, avril 2014

Source : https://www.globalsecuritymag.fr/Les-entreprises-attendraient-elles,20150715,54386.html
par Hervé Dhelin, Directeur Marketing d’EfficientIP