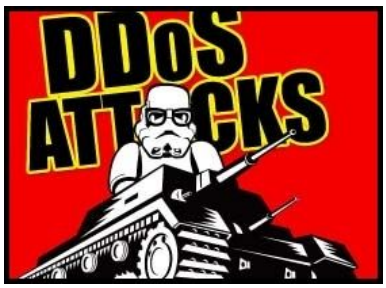
DDoS : les hébergeurs doivent prendre d’urgence des mesures pour défendre leurs clients

	DDoS : les hébergeurs doivent prendre d’urgence des mesures pour défendre leurs clients

Faisant chaque jour la une des journaux, les attaques par DDoS se multiplient. De ce fait, de nombreuses entreprises s'interrogent : leur stratégie de mitigation des DDoS les protège-t-elle suffisamment ? Aujourd'hui, elles se tournent vers leurs fournisseurs de cloud et leurs hébergeurs pour avoir la bonne réponse.

Malheureusement, l'hébergement procure aux hackers une surface d'attaque incroyablement attrayante. En effet, la taille et l'ampleur des infrastructures réseaux des data centers des opérateurs et l'importante base de clients que cela représente, présentent de multiples points d'entrée et se traduisent une énorme bande passante globale qui offre un véritable boulevard aux attaques DDoS perturbatrices et destructrices. En s'appuyant de plus en plus sur l'hébergement pour leurs services et leurs infrastructures critiques, les entreprises s'exposent elles-mêmes au risque de subir des cyber-menaces dévastatrices – même en tant que cibles indirectes.
L'aspect multi-tenant des centres de données du cloud peut expliquer la confiance relative des locataires. Une attaque DDoS volumétrique contre un des 'tenants' peut engendrer des répercussions désastreuses envers les autres : un effet « domino » de latence, de dégradation du service et d'interruption des activités de longue durée, avec de lourds dommages potentiels. Un trafic malveillant excessif qui bombarde un seul locataire au cours d'une attaque DDoS volumétrique, peut avoir des effets négatifs sur d'autres locataires et sur l'ensemble des opérations du centre de données. Il est en fait, de plus en plus fréquent qu'une attaque visant à l'origine un seul locataire ou un seul service, étouffe complètement les ressources partagées, en infrastructure et en bande passante. Ceci provoque de sévères ralentissements allant parfois jusqu'à la mise hors service du centre de données tout entier. En quelque sorte les effets secondaires du DDoS.

La technique du trou noir est un moyen de défense brut, utilisé couramment lors des attaques pour atténuer les effets secondaires des DDoS. Par cette technique, les fournisseurs de cloud et d'hébergement bloquent tous les paquets destinés à un domaine, le trafic étant re-routé vers un itinéraire nulL pour l'adresse (ou les adresses) IP sous attaque. Ce mode de défense contre les attaques DDoS pose un certain nombre de problèmes. En particulier, quand plusieurs locataires partagent une gamme d'adresses IP publiques. Dans ce cas, ils verront leur accès supprimé à l'ensemble des services, qu'ils soient ou non la cible spécifique de l'attaque. En pratiquant cette technique, l'opérateur du data center achève en fait lui-même le travail de l'attaquant en dosant complètement ses propres clients ! De plus, l'injection de routes nulL est un processus manuel qui nécessite des analystes humains, des processus workflow et des autorisations. On augmente alors les temps de réponse à l'attaque et on laisse tous les locataires du data center partagé en subir les conséquences sur des périodes pouvant atteindre plusieurs heures.
La dépendance croissante à Internet rend les effets – financiers ou autres – des attaques DDoS réussies de plus en plus douloureux pour les fournisseurs de services, les entreprises et les administrations. Et l'arrivée de nouveaux outils DDoS toujours plus puissants promettent le déclenchement d'attaques encore plus destructrices dans les mois et les années à venir.

Il est temps que les entreprises qui s'appuient sur des infrastructures ou des services hébergés commencent à se poser les bonnes questions, comme se demander si leurs fournisseurs d'hébergement ou de centres de données les protègent correctement quand une attaque DDoS frappe. Comme cela s'est vu à maintes reprises, les clients hébergés comptent en fait tout simplement sur leur fournisseur pour « s'occuper » des attaques quand elles surviennent, sans appréhender pleinement le danger et les conséquences de fermer les yeux face à ce type de comportement malveillant.

Voici trois étapes-clés pour que les fournisseurs protègent mieux leur propre infrastructure et celle de leurs clients.

1. Éliminer les délais entre le moment où les dispositifs de surveillance traditionnels détectent une menace et génèrent une alerte et le moment où un opérateur est en mesure d'y répondre. Initialement de quelques heures, l'effet de l'attaque sera réduit à quelques secondes. Ceci est possible par le déploiement d'appliances qui surveillent et atténuent automatiquement les menaces DDoS. La solution de mitigation doit pouvoir mettre à disposition des rapports d'alertes et d'événements en temps réel, avec une infrastructure de maintenance opérationnelle en arrière-plan pour des temps de réaction rapides, et fournir toute la visibilité indispensable pour comprendre l'état de la menace et améliorer pro-activement la défense anti-DDoS.

2. Déployer la mitigation DDoS inline. Si des périphériques out of band sont en place pour nettoyer le trafic, il convient de déployer rapidement des équipements de détection des menaces inline qui pourront inspecter, analyser et contrer les DDoS en temps réel.

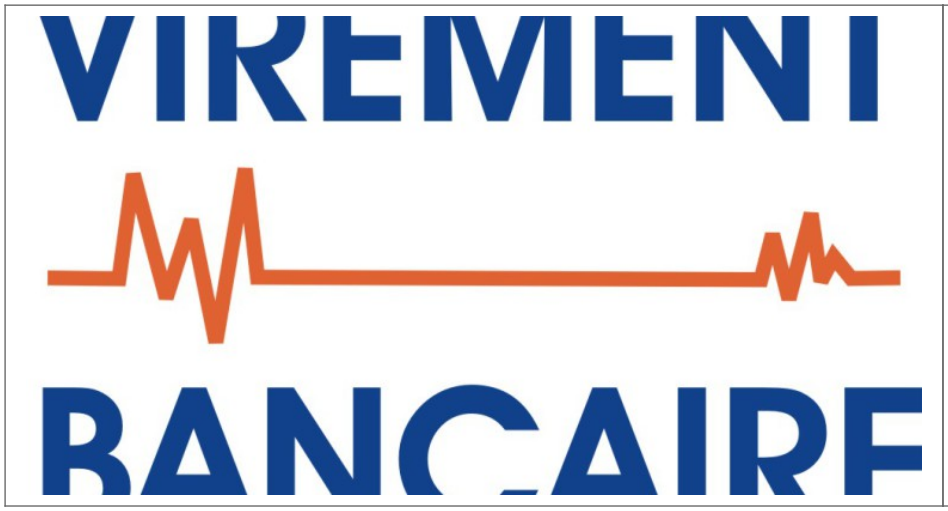
3. Investir dans une solution de mitigation DDoS architecturée pour ne jamais abandonner le bon trafic. Les prestataires de services hébergés doivent impérativement empêcher que l'équipement de sécurité ne devienne un goulot d'étranglement pour les services rendus et toujours permettre au trafic légitime de passer, sans aucune interruption ; voilà une approche de défense anti-DDoS réussie et sans dommage collatéral.

Les entreprises font confiance à leurs fournisseurs pour assurer la disponibilité de leurs services et, finalement, leur protection contre les cyber-menaces et les attaques par DDoS. Le déploiement d'une première ligne de défense complète contre les attaques DDoS permet de protéger pleinement les clients contre les menaces volumétriques dommageables, qu'elles soient dirigées vers les réseaux, qu'elles en proviennent ou qu'elles y transitent.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.programmez.com/avis-experts/ddos-les-hebergeurs-doivent-prendre-durgence-des-mesures-pour-defendre-leurs-clients-21827
par Adrian Bisaz

Virements bancaires frauduleux, découvrez les dernières techniques d’escroquerie



Virements bancaires frauduleux, découvrez les dernières techniques d’escroquerie

Les entreprises sont de plus en plus souvent victimes d'escroqueries bancaires, en particulier celles touchant les virements internationaux. C'est ainsi près de 250 millions d'Euros qui sont détournés, le plus souvent au profit d'organisations criminelles. 16% des entreprises reconnaissent ainsi avoir été touchées. A côté de la classique escroquerie qui consiste à usurper la signature d'un dirigeant de l'entreprise visée, puis à transmettre un ordre de virement falsifié à la banque, trois autres sont principalement utilisées.

Jean-Marc Souvira, commissaire principal à l'Office central de la répression de la grande délinquance financière révèle dans une vidéo (ci-dessous) destinée à sensibiliser les responsables d'entreprises sur les risques encourus qui sont chaque jours plus grands. Ces fraudes touchent tous les secteurs d'activité, elles visent majoritairement le commerce, en raison du très grand nombre de transactions réalisées dans ce secteur. Il faut rappeler aussi l'exposition des fraudes a la carte bancaire comme nous en parlions ici.

Prévenir les escroqueries aux ordres de virements internationaux dans les entreprises

Virements bancaires frauduleux : les nouvelles techniques des escrocs
La première d'entre elles est appelée «escroquerie à la nigériane»: L'escroquerie à la nigériane, ainsi appelée car les auteurs procèdent depuis l'Afrique de l'ouest, consiste à envoyer un mail informant la société destinataire d'un changement de coordonnées en raison de dysfonctionnements. Les auteurs y expliquent que le paiement des prochaines factures devra s'effectuer sur un nouveau compte bancaire, mieux sécurisé. Elle touche principalement les entreprises exerçant dans le secteur du commerce, les escrocs se faisant passer pour leurs sous-traitants asiatiques.

virements bancaires frauduleux
Une autre technique l'«escroquerie au président» : L'escroquerie au Président consiste à obtenir un virement en se faisant passer pour le PDG de l'entreprise, en arguant d'une quelconque urgence pour qu'il soit immédiat. Une personne de l'entreprise est appelée par le prétendu P-DG, qui explique qu'il est en déplacement et a besoin d'un virement pour une opération confidentielle, telle qu'une OPA ou un contrôle fiscal. Très compliquée puisqu'elle nécessite une bonne connaissance de l'entreprise et de ses codes, ainsi qu'un certain aplomb, cette escroquerie est très lucrative : les sommes détournées peuvent atteindre plus d'un million d'euros pour chaque ordre.
La dernière arnaque en vogue est celle qui profite de la norme Sepa : Plus récemment, une nouvelle escroquerie exploite les failles de la norme SEPA. Les escrocs contactent les entreprises, en se faisant passer pour un informaticien de leur banque, afin de les convaincre de se connecter sur un site pour des mises à jour ou des tests de sécurité. Ce faux site leur permet de prendre le contrôle à distance du réseau interne de l'entreprise. Des ordres de virement sont alors passés, sans surveillance puisque les banques ne vérifient plus si l'ordre émane bien de l'entreprise.

La Chine, principale plateforme de réception
Pour faire face à ces arnaques, il faut avant tout du « bon sens ». Mais il faut aussi ne pas tarder à se rendre compte de l'arnaque, car les opérations de virement ne peuvent être annulées après un délai, très court. Dans leur grande majorité c'est en Chine que l'on trouve l'origine des escrocs et vers ou l'argent est ensuite versé. La police et de la justice françaises doivent d'ailleurs très prochainement rencontrer leurs homologues chinois pour étudier ce problème qui ne touche pas seulement la France mais l'ensemble de l'Europe.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesnewseco.fr/techniques-escroquerie-virements-bancaires-01609.html

Smartphones : deux applis sur trois nous espionnent, révèle la Cnil

Smartphones : deux applis sur trois nous espionnent, révèle la Cnil

Pour savoir si les applications installées sur nos téléphones portables se montrent respectueuses de nos données personnelles, la Cnil a élaboré, avec l'aide de l'Inria, un logiciel de contrôle et l'a fait tourner sur 121 applications Android pour vérifier la collecte éventuelle d'informations de localisation, du carnet d'adresses, du calendrier ou même des numéros de téléphone.

Le résultat est édifiant, révèlent nos confrères d'Europe 1 : 66 % des applications communiquent sur le type de réseau Internet (Wi-Fi, 3G, 4G) auquel l'utilisateur est connecté, 24 % accèdent à la géolocalisation, le plus souvent à l'insu de l'utilisateur, cinq applis ont accédé au numéro de téléphone de l'utilisateur et deux ont été jusqu'à récupérer la liste des identifiants des points d'accès Wi-Fi présents autour de l'utilisateur.

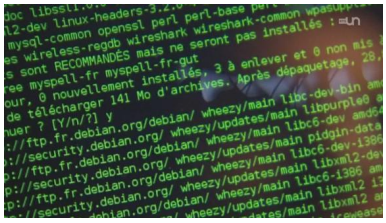
Une application qui n'est pourtant pas dédiée à la recherche d'itinéraire, Google Play, boutique de téléchargement d'applications pour Android, a même accédé à plus d'un million de fois à la géolocalisation d'un smartphone unique en trois mois !

La Cnil assortit ses conclusions de quelques conseils. La meilleure façon de se protéger consiste à éviter les téléchargements inutiles, et à faire régulièrement le tri dans celles qui sont installées sur son appareil. On peut également régler les paramètres de son téléphone (menu Paramètres Google, option « désactiver annonces par centres d'intérêt ».)

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.industrie-techno.com/smartphones-deux-applis-sur-trois-nous-espionnent-revele-la-cnil.35111
Par Muriel de Véricourt

Réseaux Wifi: gare aux pirates!

	**Réseaux Wifi: gare aux pirates!**

Aujourd'hui, on se déplace avec son Smartphone dans la poche, et de plus en plus souvent avec son ordinateur portable sous le bras. On veut pouvoir surfer sur le Net dans les gares, les aéroports, les cafés ou les chambres d'hôtel. Plusieurs grandes villes offrent même un accès wifi public et gratuit. Nos cartes bancaires sont aussi équipées de puces permettant le paiement sans contact. Mais attention, ce sont autant de nouvelles possibilités offertes aux pirates informatiques !

Le piratage informatique augmente
De l'aveu des experts, les antivirus ne savent pas s'adapter à toutes les nouvelles menaces. Il faut d'abord subir une attaque et ses conséquences avant de trouver la parade. Les criminels ont donc pratiquement toujours un temps d'avance. Et les portes d'entrée vers vos données confidentielles se multiplient. Les accès wifi « malicieux », ou encore les virus et autres applications permettant de récupérer vos données de carte de paiement sans contact (NFC)sont des méthodes récentes de piratage qui viennent s'ajouter à une liste déjà longue. Démonstrations.

Votre wifi peut vous rendre suspect
Un soir, madame T. a la mauvaise surprise d'être accueillie par des inspecteurs de la police judiciaire lors de son retour à son domicile. Des images pédopornographiques ont transité par son accès wifi! Bien que protégé, l'accès wifi a été piraté puis utilisé par un cybercriminel. Madame T a rapidement été mise hors de causes, mais reste choquée par cette aventure. Témoignage.

Wifi gratuits: Attention! Le point avec Luc Mariot, journaliste et producteur d'ABE

Les wifi gratuits contrôlés: CFF (en gare de Genève), Aéroport (GVA), Ville de Genève, Ville de Lausanne, Ville de Vevey, Starbucks, Mc Donald, Manor, Centre La Praille.

Vos données intéressent les cybercriminels
Les cybercriminels peuvent utiliser vos données de plusieurs manières. Certains rendent vos documents illisibles puis vous rançonnent en vous vendant la clé de décryptage. D'autres s'emparent tout simplement de vos coordonnées bancaires, pour ensuite les revendre ou consommer à vos frais sur la Toile. Enfin, certains s'invitent carrément chez vous ou à votre bureau, en suivant vos faits et gestes à travers votre micro et votre webcam intégrés. Comment se protéger?
Le Département du Trésor américain et l'Union Européenne annonçaient il y a 5 ans déjà que les profits générés par la cybercriminalité dépassent désormais ceux de la vente de drogue dans le monde ! Un phénomène qui ne va faire que s'amplifier dans les décennies à venir.

LE reportage qui vous dit tout

La principale faille dans les entreprises est le manque de connaissance de ces risques.
Au travers de conférences ou de formations, Denis JACOPINI vous propose de vous sensibiliser, responsable de la stratégie de l'entreprise qui DOIT désormais intégrer le risque informatique comme un fléau à combattre et à enrayer plutôt qu'une fatalité.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.rts.ch/emissions/abe/6205697-reseaux-wifi-gare-aux-pirates.html

Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

	Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

Lorsque des institutions gouvernementales ou des entreprises souhaitent stocker des informations confidentielles, elles utilisent le plus souvent un réseau en « air-wall », déconnecté d'internet, et isolé de toute connexion extérieure. Récemment pourtant, plusieurs chercheurs de l'université Ben-Gurion en Israël ont démontré qu'il était possible, une fois ce réseau contaminé par un virus spécifique, d'en récolter les données.

Les pirates informatiques peuvent voler les données de votre ordinateur même s'il est déconnecté et éteint.
Atlantico : Bien que les particuliers soient sans doute moins la cible de ce type d'attaque informatique, sont-ils tout aussi vulnérables ?
Michel Nesterenko : Tout ordinateur est potentiellement vulnérable. Mais les connaissances et la technologie nécessaire pour réussir un tel vol de données font que seules les ordinateurs dans lesquels sont stockés des données stratégiques ou des données commerciales de grande valeur sont vraiment à risque. Donc le consommateur normal n'a pas de grand souci à se faire.
Du temps de la Guerre Froide dans les années 60 les espions américains et russes pouvaient voler toutes les informations passant sur l'écran d'un ordinateur à partir du van stationné dans la rue.
C'est pour cela que certains ministères à Washington avaient blindés l'enveloppe extérieure des ordinateurs détenant des données sensibles de façon à empêcher toute émanation électromagnétique.

Jean-Paul Pinte : En tant que particulier, nous sommes encore plus vulnérables à ce type d'attaque ou d'infiltration qui, une fois installé sur une machine, permet d'y revenir et de se servir. Nous avons en effet moins pensé la sécurité de nos données par rapport à une entreprise par exemple, mais le risque demeure le même, il est même plus grand. Le ver installé sur un PC, il est en effet possible de faire ce que l'on veut, de s'installer confortablement et d'y revenir à sa guise. Une des seules façon de pirater un PC éteint serait d'être en rapport avec la C-MOS et nécessiterait donc un accès physique à la machine. Ce n'est donc à la portée du premier venu.
Comme pour votre Webcam éteinte, il est tout aussi possible d'en prendre la main à distance et certains vont même jusqu'à utiliser un cache ou collant qu'ils posent sur la Webcam pour s'en protéger. Un ordinateur quand il est éteint, c'est juste la boite d'alimentation qui est éteinte mais la carte mère continue à recevoir de l'énergie (un voyant lumineux au niveau de la carte mère est toujours présent). Il est donc toujours plus prudent de débrancher totalement son ordinateur et surtout de ne pas le laisser en mode veille ou veille prolongée. Il est également possible si l'on veut se protéger totalement de fermer son boîtier Wifi mais attention aux mises à jour qui se font parfois la nuit sur ces matériels.

Quelles données peuvent être récupérées ? Quelles sont les marges de manoeuvre des pirates informatiques avec pareil procédé ?
Michel Nesterenko : Potentiellement tout peut être récupéré à terme car le vol des données prends du temps, compte tenu des limitations de la bande passante. Ce type de procédé est fort utile dans un contexte militaire ou d'espionnage industriel. Les informations peuvent être revendues aux concurrents ou utilisées dans des manipulations boursières par exemple.

Jean-Paul Pinte : Une fois dans la machine, on peut tout faire avec quelques manipulations que connaissent bien ces hackers. A la base il y a quelques années, le but était simplement d'avoir pu infiltrer ou craquer une machine.
Aujourd'hui, ce sont tous vos contacts de messagerie, les fichiers stockés, les mots de passe qui peuvent être récupérés par exemple au même titre que tous les documents personnels. Il n'y a donc pas de limites.
Tous ces éléments pourraient se retrouver un jour sur la toile et servir par exemple dans le cas d'adresses de messagerie à des banques de données réutilisées par la suite pour faire des envois en masse comme cela se pratique dans le cas des mails nigérian.
Prendre la main sur votre machine revient à avoir la clé de votre domicile, le code de votre alarme et tout peut alors être envisagé en vue de vous voler des informations et des accès à des sites que vous utilisez et sur lesquels vous passez des actes d'achat par exemple.
Aujourd'hui, on parle même de vol de données qui pourraient vous faire chanter.

Comment savoir si notre ordinateur est infecté par ce type de virus ? Comment s'en apercevoir ?
Michel Nesterenko : Pour tout virus connu, il existe un antidote. Encore faut il que les anti-virus et parre-feu soient mis à jour constamment sur chacun des ordinateurs du réseau indépendamment.

Jean-Paul Pinte : Assurez-vous tout d'abord d'avoir la bonne dernière version officielle de vos logiciels et pensez à utiliser des solutions comme Anti Hacks qui détectera les problèmes de configuration et les logiciels obsolètes sur votre machine et qui, surtout, se chargera de configurer automatiquement les logiciels et vous aidera à les mettre à jour.
Ensuite un anti-virus que vous mettrez à jour tous les jours et pas à la petite semaine comme le font la plupart d'entre nous (beaucoup utilisent celui offert pour une période donnée par le fournisseur du PC mais oublient de le changer ou de l'actualiser dans le temps se retrouvant alors sans protection).

En attendant :
• surveillez vos barres d'outils et les liens que vous n'auriez pas ajouté personnellement ;
• contrôlez votre pointeur de souris qui à certains moments se déplacerait de façon inatendue ;
• regardez l'adresse URL du site que vous consultez car il pourrait changer lors d'une transaction financière par exemple ;
• veillez aux fenêtres intempestives qui s'affichent sur votre PC sans que vous n'interveniez et aux pages qui s'installent en arrière plan et que vous ne découvrez qu'une fois que vous fermez votre session Internet ou machine. Elles pourraient bien être la source d'un début d'installation d'une cyber-surveillance ;
• enfin si tout va plus lentement sur votre ordinateur; pensez à contrôler les fichiers qui se lancent au démarrage et surtout n'oubliez pas que le meilleur anti-virus est parfois de remettre à plat tous les six mois votre PC.

Quel est le niveau d'informatique nécessaire pour mettre en oeuvre correctement cette pratique ? Des solutions simples sont-elles mises à la disposition des amateurs ?
Michel Nesterenko : Le Hacking de haut niveau n'est pas une activité pour amateurs. Il faut des connaissances certaines pour mettre au point le virus adapté a une attaque particulière de même qu'il faut des informations précises obtenues par une opération de reconnaissance informatique et physique pour trouver l'ordinateur cible. Il s'agit d'un travail pour des spécialistes.

Jean-Paul Pinte : Dès que ces cybercriminels ont réussi à installer un virus ou un cheval de Troie (souvent aussi nommé malware ou logiciel malveillant) votre ordinateur devient une source potentielle de revenus. Ils auront accès à toutes vos données personnelles (messages, mails, documents bancaires, mots de passe, photos, vidéos, …) stockées sur votre disque dur et pourront surveiller votre activité sur Internet et sur votre machine.
Aujourd'hui, pas besoin d'être un grand expert sur le sujet en dehors de quelques types d'infiltrations spécifiques sur des sites dits plus sécurisés. En effet, malheureusement, beaucoup d'aide est apportée aux cyberdélinquants par Internet.. Des solutions contenus dans certains forums permettent à des petites mains de se lancer tout d'abord dans le cadre d'arrêt d'une machine en réseau dans une entreprise. Petit à petit, pirates, hackers ou encore crackers découvrent les modes opératoires des plus grands pour se les approprier et pour aller plus loin comme s'il y avait un concours entre eux.
Comment s'en prémunir ? Doit-on se résigner à avoir un ordinateur vierge de toute connexion à internet, avec des protocoles de sécurité stricts, comme par exemple ne pas utiliser de clé usb étrangère ou ne pas prêter les siennes ?
Michel Nesterenko : Absolument. Éviter de connecter à internet un ordinateur détenant des données critiques et stratégiques est la première étape. Interdire l'utilisation de toute clé USB non cryptées avec des codes particuliers est une deuxième étape.
Ensuite, il faudra songer à installer un blindage autour de l'écran pour éviter toute émanation électromagnétique. Surtout, il ne faut jamais oublier de tenir à jour les anti-virus et parre-feu sur chaque ordinateur et crypter toutes les données résidant sur le disque dur.
Le nombre de situations où cela sera vraiment recommandé reste fort restreint. Pour l'écrasante majorité des utilisateurs, cela ne sera jamais nécessaire heureusement.
Jean-Paul Pinte : De plus en plus, il faudra apprendre à se protéger et à avoir une culture sécuritaire en ce qui concerne les materiels que nous utilisons et que nous connectons à notre PC car ils seront autant de sources et de moyens d'attaque pour ces délinquants.
Tout ce qui est installé, introduit et (télé)chargé sur nos machines doit faire l'objet d'une sorte de scan ou contrôle si l'on veut rester dans une protection plus sereine.
Nous en sommes loin aujourd'hui quand nous validons la mise à jour d'un logiciel sans être sûr que l'envoi émane de la société en question. Certains internautes ont découvert tardivement que des exécutables s'étaient installés sur leur PC mais n'ont pu en mesurer l'impact sur leurs données, logiciels, etc.
L'objectif premier du hacker va être d'installer un virus ou un cheval de Troie sur votre ordinateur. Il se présente simplement sous la forme d'un exécutable (par exemple .exe), soit installé suite à l'attaque d'un de vos logiciels mal configurés ou obsolètes (la version installée n'est pas la dernière et contient donc des failles de sécurité). Ces failles sont en général la conséquence d'un bug de programmation dans l'application qu'un hacker saura mettre à profit pour prendre le contrôle de votre ordinateur. Ces logiciels sont très nombreux en voici quelques uns à titre d'exemple :
– Microsoft Windows ;
– Les suites bureautiques (Microsoft Office, OpenOffice) ;
– Les navigateurs (Internet Explorer, Firefox, Chrome, Opera, Safari) ;
– Les logiciels multimedia (Acrobat Reader, Flash, Shockwave, Windows Media Player, Quicktime, RealPlayer, WinAmp, iTunes, VLC) ;
– Les messageries instantanées (Windows Messenger, Pidgin) ;
– Java.

On a pu ainsi découvrir des cas de figure où les PC des internautes sont devenus des serveurs à leur insu se voyant alors stocker à des jours et des heures des données de personnes malveillantes qu'ils ne pouvaient alors contrôler sur leur propre machine.
De même d'autres ont accepté avec trop de simplicité et de naïveté une clé USB offerte avant l'entrée dans un salon ou symposium. Le but étant de garder la clé mais pas son contenu, ils ont ouvert cette dernière sans penser à l'exécutable qui allait s'installer sur la machine et qui allait devenir un moyen d'infiltration sans limite pour l'offreur.
Certaines applications sur ces clés vont même pendant qu'un tiers tente de recopier un fichier à partir de votre machine scruter votre PC pour lui sous-tirer tous vos contacts et ce que vous pouvez imaginer avec sans vous garantir qu'il n'aura pas pris la main sur votre PC pour y revenir ultérieurement.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.atlantico.fr/rdv/minute-tech/pirates-capables-voler-donnees-meme-votre-ordinateur-est-pas-connecte-internet-michel-nesterenko-1893142.html

---

Cryptolocker : quand un virus prend vos données en otage

contre rançon

	**Cryptolocker : quand un virus prend vos données en otage contre rançon**

Depuis quelques jours, une campagne d'attaque utilisant CryptoLocker (logiciel malveillant de type cheval de Troie) semblerait être en cours. La société d'antivirus Trend Micro a été alertée par de nombreux appels et messages de la part de ses clients et partenaires. Loïc Guézo, évangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro et administrateur du Clusif, livre quelques pistes pour lutter contre ce ransomeware (logiciel malveillant prenant les données personnelles de l'utilisateur en otage) particulièrement nuisible.

Vous cliquez sur le lien d'un e-mail reçu. Le fond d'écran change. Une fenêtre s'ouvre. Un avis apparaît, vous informant que vos fichiers importants sont cryptés. Vous tentez de cliquer ailleurs. Impossible de quitter la fenêtre. L'écran est verrouillé. Un cauchemar nommé « Cryptolocker ».
Ce « ransomware » (ou rançongiciel) est un logiciel malveillant qui piège l'ordinateur de ses victimes et prend en otage leurs données personnelles. Il est précisé que le chiffrage des données du disque par le logiciel malveillant les rend inutilisables jusqu'au versement de la rançon demandée. Le pirate promet de fournir la clé capable de déchiffrer les données en échange d'une somme de quelques centaines d'euros, à régler en ligne via Paypal ou un virement en bitcoins. Le tout avec un compteur de temps bien visible, qui signifie que la décision doit être prise rapidement.
Bien sûr une clé unique est utilisée pour chaque machine piégée. Si la rançon demandée n'est pas versée dans le temps imparti, la clé de chiffrement ne sera pas communiquée et les données chiffrées définitivement perdues. Et si la rançon est payée, rien ne garantit pour autant la suite des opérations…
Ce scénario digne d'un thriller a fait son apparition fin 2013 et revient en force depuis quelques semaines. S'il est encore trop tôt pour connaître précisément le nombre de systèmes infectés par le programme malveillant, Le Monde Informatique du 6 janvier 2014 rapporte que Cryptolocker 2.0 aurait infecté 200 à 300 000 PC et qu'environ 0,4 % des victimes ont probablement payé la rançon réclamée, même si payer ne garantit absolument pas le déblocage du système.
Ce banditisme virtuel est basé sur un chantage avec comme otage les données de la victime. Il a été jugé suffisamment grave pour que des policiers, spécialement formés, enquêtent pour retrouver ces malfaiteurs du Net et les poursuivent. Des unités spéciales américaines et européennes ont, par exemple, travaillé ensemble et uni leurs efforts pour démanteler le 2 juin dernier le réseau criminel GameOver Zeus qui, entre autres, pouvait distribuer Cryptolocker.

L'INGÉNIERIE SOCIALE, VECTEUR DE L'INFECTION
Les malfaiteurs s'appuient sur des techniques d'ingénierie sociale. Ils procèdent à l'envoi initial de leurres sous forme de vagues d'e-mails ciblés. D'où l'importance de vérifier la légitimité de chaque message. Il convient de toujours faire preuve d'une extrême prudence lorsque nous ouvrons la pièce jointe à un message électronique dont la source nous est inconnue.
Ce sont principalement aujourd'hui les utilisateurs de PC qui sont visés (des versions visant les mobiles apparaissent déjà). Mais le point de départ est bien le geste de l'utilisateur lui-même, piégé par un message avec pièce jointe. L'hameçon psychologique est celui de l'inquiétude naturelle, de la surprise ou de l'intérêt du destinataire du message. Il peut s'agir de faux courriers paraissant provenir d'un organisme social, d'une banque, d'une assurance, d'e-commerçants, de logisticiens ou de transporteurs, etc. La pièce jointe est censée être un document lié à un litige, une facture impayée, un avis de livraison en suspens, un remboursement sur trop-perçu…
L'éducation et la vigilance des utilisateurs isolés sont donc indispensables. Sur un réseau d'entreprise, l'information d'alerte doit être donnée et pourra plus facilement être souvent répétée : « n'ouvrez pas les mails de provenance inconnue sans vérification, ne cliquez jamais sur un lien si vous avez le moindre doute », etc.

COMMENT SE DÉFENDRE ET PRÉVENIR LE BLOCAGE ?
Il existe plusieurs moyens pour gérer cette menace, tant pour les particuliers que pour les entreprises. Il a été largement démontré que la sécurité basée sur les signatures a atteint ses limites, mais il existe cependant d'autres solutions avec des fonctions d'alerte plus évoluées. Ce sont par exemple des solutions basées sur les éléments environnementaux (comme la réputation d'adresses IP, les noms de domaine…). Un service de réputation va en particulier permettre de bloquer l'accès à certaines adresses IP correspondant à des C&C de botnets, empêchant tout simplement le Cryptolocker de s'initialiser et donc de chiffrer la cible !
Revoir la politique de sécurité des pièces jointes est urgent pour de nombreuses entreprises. L'adoption des bonnes pratiques permettra d'éviter une contamination très rapide.
Posons-nous les bonnes questions pour contrer Cryptolocker. Est-ce que l'entreprise dispose bien d'une politique de blocage des pièces jointes aux messages, empêchant par exemple le déclenchement d'un fichier exécutable ? Peut-on analyser « en amont » le comportement des pièces jointes ? Utilise-t-on un service avancé de réputation ? Surveille-t-on le comportement des pièces jointes sur la durée? A-t-on simplement le moyen de contrôler que la solution de sécurité reste activée ? Ces quelques premières précautions permettront d'éviter les catastrophes, en particulier pour les PME.
Il faut bien sûr toujours être sur ses gardes, ne pas négliger de mettre à jour les logiciels de sécurité installés et vérifier que le navigateur utilise la réputation de sites Web avant de cliquer sur un lien ou bien utiliser un service gratuit comme Trend Micro Site Safety Center.
Quant aux grandes entreprises, qu'elles se préparent à recevoir des attaques type Cryptolocker mais désormais ciblées. Et bien sûr, toujours communiquer en interne sur les risques, et communiquer, c'est répéter…

LES SYSTÈMES INFORMATIQUES DOIVENT ÊTRE PRÉPARÉS POUR RÉSISTER
On ne soulignera jamais assez que la formation des utilisateurs, la mise à jour régulière des logiciels et de bonnes pratiques d'utilisation de l'ordinateur individuel restent le socle de défense contre Cryptolocker ou toutes les nouvelles menaces similaires. Il est désormais nécessaire d'introduire des outils d'analyses plus complets (vision en temps réel de la menace ou exécution en environnement contrôlé – sandboxing – par exemple).
Si les cybercriminels perfectionnent chaque jour leurs logiciels malveillants qui deviennent ainsi de plus en plus sophistiqués, alors les systèmes informatiques doivent également être préparés pour résister mais surtout être cyber-résilients face à ces attaques. Cette lutte doit être globale pour non seulement réduire le taux de l'infection, mais également briser la chaîne de transmission des logiciels malveillants par une stratégie de défense en profondeur, y compris lors de son déroulement.
L'autre aspect fondamental reste la lutte policière et judiciaire contre ces nouvelles formes de criminalité dont les dernières semaines ont montré l'ampleur et le dynamisme.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.usine-digitale.fr/article/cryptolocker-quand-un-virus-prend-vos-donnees-en-otage-contre-rancon.N302748
par Loïc Guézo, Evangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro & Administrateur du Clusif

---

Kaspersky Lab prédit des attaques persistantes plus furtives et ultra ciblées

Kaspersky Lab prédit des attaques persistantes plus furtives et ultra ciblées

Les experts de l'éditeur de logiciels de sécurité informatique ont surveillé plus de 60 acteurs responsables de cyber-attaques à travers le monde. En observant de près ces menaces, Kaspersky Lab a pu dégager une liste des menaces émergentes dans le monde des APT (Advanced Persistent Threat ; Menaces persistantes avancées).

2015 sera l'année de la furtivité des cyber-menaces. © D.R.

Ces dernières années, Kaspersky Lab, un éditeur majeur de solutions de protection contre les cyber-attaques, a mis en lumière certaines des plus grosses campagnes d'attaques APT (Advanced Persistent Threats ; Menaces persistantes avancées), notamment RedOctober, Flame, NetTraveler, Miniduke, Epic Turla, Careto/ The Mask et d'autres. Les experts de l'équipe de recherche du GReAT (Global Research et Analysis Team) de Kaspersky Lab ont surveillé plus de 60 acteurs responsables de cyber-attaques à travers le monde. En observant de près ces menaces, Kaspersky Lab a pu dégager une liste des menaces émergentes dans le monde des APT.

Fragmentation des plus gros groupes APT

En 2015 il faudra s'attendre à ce que les plus gros et les plus importants groupes d'attaques APT se divisent en plusieurs unités plus petites, opérant de manière indépendante. Cela entrainera une base d'attaque plus étendue et, donc, plus d'entreprises seront touchées du fait que chaque petit groupe diversifiera ses attaques. Dans le même temps, cela signifie que les plus grosses entreprises précédemment infectées par deux ou trois groupes APT majeurs (par ex. Comments Crew et Wekby) connaîtront plus d'attaques, provenant d'un panel de sources élargi.

La méthode APT sera utilisée pour un cyber-crime plus vaste

Pendant nombre d'années, les cybercriminels se sont focalisés exclusivement sur le vol d'argent de l'utilisateur final. Une explosion des taux de vols de cartes de crédit, de piratages des comptes de paiement électronique ou des connexions de banque en ligne ont causé aux consommateurs la perte de millions d'euros. Cependant les experts de Kaspersky Lab observent une tendance plus intéressante qui deviendra prééminente en 2015 : les attaques ciblant directement les banques et qui utiliseront des méthodes tout droit sorties des stratégies APT.

Les réseaux d'hôtels deviendront des cibles privilégiées.

Le Groupe Darkhotel est ainsi l'un des acteurs APT connus pour avoir ciblé des visiteurs particuliers durant leur séjour dans les hôtels de certains pays. Actuellement, les hôtels fournissent un excellent moyen de cibler une certaine catégorie de personnes, comme des dirigeants d'entreprise. Cibler les hôtels est également très lucratif car cela fournit des renseignements sur les mouvements d'individus importants dans le monde. En 2015, ce type d'attaques pourra se multiplier à plus grande échelle.

Evolution des techniques d'attaques.

Aujourd'hui, nous voyons déjà des groupes APT déployer constamment des malwares de plus en plus évolués pour des systèmes informatiques qui se complexifient constamment (comme Turla et Regin). En 2015, nous nous attendons à voir des implantations de malwares encore plus sophistiquées qui tenteront de déjouer encore plus efficacement les outils de détections des attaques.

Nouvelles méthodes d'exfiltration des données. Les jours où les attaquants activaient simplement une backdoor dans un réseau d'entreprise pour voler des téraoctets d'informations depuis les serveurs FTP dans le monde sont révolus. Aujourd'hui, des groupes plus sophistiqués ont recours aux SSL de manière régulière en plus des protocoles de communication personnalisés. En 2015, plus de groupes d'attaquants feront usage des services cloud afin de rendre l'exfiltration plus discrète et plus difficile à remarquer.

Utilisation de fausses bannières lors des attaques

Les attaquants commettent des erreurs. Dans la vaste majorité des cas analysés, nous observons des artefacts qui fournissent des indices sur le langage utilisé par les attaquants. Par exemple, dans le cas de RedOctober et d'Epic Turla, nous avons conclu que les attaquants parlaient probablement couramment le russe. Dans le cas de NetTraveler, nous avons abouti à la conclusion que les attaquants parlaient couramment chinois. Cependant les attaquants commencent à réagir à cette situation. En 2014, nous avons observé plusieurs opérations « fausses bannières» où les attaquants ont introduits des malwares inactifs communément utilisés par d'autres groupes APT. En 2015, avec la propension croissante des gouvernements à « nommer et pointer du doigt » les attaquants, les groupes APT vont prudemment ajuster leurs opérations et placer de fausses bannières dans la partie.

« Si nous pouvons qualifier l'année 2014 de 'sophistiquée', alors 2015 sera sous le signe de la 'furtivité'

Nous pensons que les groupes d'attaques APT évolueront pour devenir plus sournois et seront encore plus difficile à traquer. Cette année, nous avons déjà découvert des attaques APT utilisant les vulnérabilités dites « zéro day » ainsi que d'autres techniques plus persistantes et plus insidieuses encore. A partir de ces découvertes, nous avons développé et déployer de nouveaux outils de défense pour nos utilisateurs », explique Costin Raiu, directeur du GReAT de Kaspersky Lab.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-f344b63add3ab82ad1ae1f0fc9ae7dc8.htm par Erick Haehnsen

Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

Des centaines de gigaoctets de fichiers ont déjà été diffusés par des pirates. Une situation catastrophique pour le géant du divertissement hollywoodien.

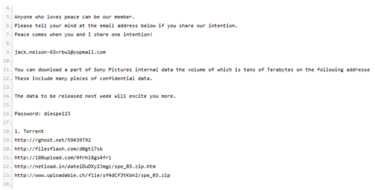
Imaginez que toutes les données – ou presque – qui transitent sur votre ordinateur de travail, stockées sur les disques durs et serveurs de votre entreprise, soient compilées et rendues accessibles à tous. Voilà la situation devant laquelle se retrouvent actuellement les employés et la direction de Sony Pictures Entertainment, après l'attaque informatique de grande ampleur subie le 24 novembre. Depuis, des milliers de gigaoctets de fichiers confidentiels du géant du divertissement hollywoodien, producteur et diffuseur de nombreux films, sont dispersés sur le Web.

Un mécanisme bien rodé

Les pirates, réfugiés derrière l'acronyme #GOP (pour Guardian of Peace), avaient au départ évoqué onze terabytes de documents (11 000 gigaoctets) subtilisés lors de leur attaque. Ils parlent maintenant de « dizaines de térabytes » de données – une centaine, disent les médias américains. Qu'un tel volume de données ait effectivement été volé semble de plus en plus probable.

Les documents internes de Sony Pictures publiés (fichiers Excel, Word, Powerpoint, PDF, etc.) se comptent déjà par centaines de milliers et en dizaine de gigaoctets, selon un décompte fiable établi par l'entreprise spécialisée en sécurité informatique Risk Based Security.

Le processus de diffusion est toujours le même. Des liens permettant de télécharger des fichiers RAR ou ZIP volumineux, par des sites de téléchargement direct ou grâce à des fichiers torrent, apparaissent sur l'éditeur de texte en ligne Pastebin, qui assure un certain anonymat à leurs auteurs. Les hackers envoient ensuite le lien du document Pastebin par e-mails à leurs contacts, soit n'importe qui ayant signifié son intérêt pour les documents Sony Pictures en écrivant aux adresses anonymes et temporaires que les membre de GOP diffusent régulièrement (journalistes, sympathisants des hackers, entreprises de sécurité informatique, enquêteurs, concurrents…).



```
Anyone who loves peace can be our member.
Please tell your mind at the email address below if you share our intention.
Peace comes when you and I share one intention!

jack.nelson-63vrbu1@yopmail.com

You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresse
These include many pieces of confidential data.

The data to be released next week will excite you more.

Password: diespe123

1. Torrent
http://rghost.net/59439792
http://filesflash.com/d0gti7sk
http://180upload.com/9frhl8gs4frl
http://netload.in/dateiDuDXy2Jmgc/spe_03.zip.htm
http://www.uploadable.ch/file/sf4dCf3tKWn2/spe_03.zip
```

Extrait d'un message donnant accès aux fichiers volés à Sony Pictures Entertainment. | Pastebin

Les données sont ensuite accessibles pendant quelques heures, avant la désactivation des liens de téléchargement par les hébergeurs et la suppression du document Pastebin – vraisemblablement sur requête des autorités ou de représentants légaux de Sony. Entre le 24 novembre et le 10 décembre, six « livraisons » de ce type ont eu lieu. Les pirates, maniant le sens du teasing, en promettent à chaque fois davantage : « les données que nous publierons la semaine prochaine vous exciteront encore plus », annonçait par exemple un document Pastebin publié le 5 décembre.

Un chantage pécuniaire ?

Les textes diffusés par les hackers qui accompagnent la publication de ces fichiers n'en disent en revanche que peu sur les motivations réelles justifiant cette fuite massive et organisée. La piste de la Corée du Nord, qui agirait en représailles au film The Interview parodiant le régime de Kim Jong-un, est accréditée par des similarités constatées entre l'attaque du 24 novembre et celle subie par la Corée du Sud en 2013. Mais l'un des cadres du FBI, officiellement chargé de l'enquête, a confié le 9 décembre qu'il n'était pour l'instant pas possible d'en attribuer la responsabilité à Pyongyang.

Dans un document publié le même jour, les membres proclamés des GOP demandent bien à Sony d'« arrêter immédiatement de diffuser un film sur le terrorisme qui peut mettre fin à la paix régionale et causer une guerre », sans nommer le film en question, et reprenant une rhétorique déjà servie auparavant à The Verge. Mais ils signalent également avoir « formulé une demande claire à l'équipe dirigeante de Sony », encore une fois sans préciser laquelle :

« Ils ont refusé de l'accepter. On dirait que vous pensez que tout se passera bien, si vous trouvez les attaquants et ne réagissez pas à notre demande. Nous vous avertissons à nouveau. Répondez à ce que nous vous demandons si vous voulez nous échapper. »

De quoi donner du crédit à l'hypothèse d'une tentative d'extorsion de fonds de la part des hackers de « Guardian of Peace ». Ce motif a d'ailleurs été clairement exposé dans un e-mail envoyé aux dirigeants de Sony Pictures quelques jours avant l'attaque : « Nous avons de quoi causer beaucoup de tort à Sony Pictures. (…) Nous voulons une compensation monétaire. Payez, ou Sony Pictures sera frappé dans son ensemble. »

La diffusion au compte-gouttes des documents confidentiels constituerait, dans ce contexte, un moyen de pression supplémentaire pour obtenir cette « compensation », de nature à alimenter un feuilleton médiatique dévastateur pour Sony Pictures. Les médias du monde entier ont ainsi repris :

Les données privées de célébrités

Des adresses postales, des numéros de téléphone, des adresses électroniques, ou encore le numéro de sécurité sociale de Sylvester Stallone, contenus dans les documents liés aux films et séries de Sony Pictures ont été rendus publics. Parmi ces informations, on trouve les pseudonymes utilisés par Tom Hanks, Natalie Portman ou encore Ice Cube pour conserver un peu de tranquillité (lors d'une réservation d'hôtel par exemple).

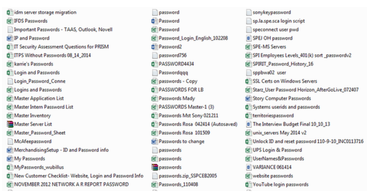
Ont également été publiés une cote de popularité des acteurs pays par pays, ou encore les sommes d'argent perçues par Seth Rogen et James Franco pour le film The Interview. Le premier aurait reçu 8,4 millions de dollars pour avoir coréalisé et interprété l'un des rôles principaux, le second 6,5 millions : des divulgations auxquelles ils ont réagi avec humour.

L'affiche de « The Interview ». | Sony Pictures

Les données privées des salariés et partenaires de Sony Pictures

Numéros de téléphone, CV, photos d'identité, montants de salaires, demandes d'augmentation, e-mails, planning de vacances, factures médicales… Autant d'éléments propres à la vie interne d'une structure qui emploie près de 7 000 personnes aux Etats-Unis, et qui a collaboré avec de très nombreuses personnes ces dernières années – stagiaires, prestataires ou partenaires directs au sein d'entreprises rachetées par Sony, comme Columbia Pictures. Ces détails apparaissent notamment dans un dossier intitulé « Ressources humaines », et se trouvent aussi dans des documents de travail liés aux tournages de films et de séries Sony.

Encore plus grave, de très nombreux mots de passe utilisés par les employés pour se connecter à tous types de services (propres à Sony Pictures, mais aussi ailleurs sur Internet) font partie des publications. Comme le note cruellement Gizmodo, ils étaient stockés sur les disques durs de Sony Pictures dans des fichiers Word et Excel sans protection, et dans un dossier appelé « Mot de passe ».



Les mots de passes de Sony Pictures. | Risk Biaised Security

De quoi pousser d'anciens employés à réfléchir à une plainte collective, arguant du manque flagrant de sécurité du réseau de l'entreprise. « Il y a des raisons de penser qu'il y a eu une grosse négligence de la part de [Sony Pictures]. Nous nous inquiétons tous concernant notre vie privée, et nos familles », a déclaré l'un d'entre eux à Fox News, après avoir vu diffuser son passeport, son visa, son numéro de sécurité sociale et ses contrats passés avec l'entreprise.

Des avocats californiens incitent également les salariés actuels à se lancer dans de telles procédures. Particulièrement exposés, ils se sont vus en plus directement menacés dans un e-mail leur étant adressé. « Tout le monde panique, et personne ne sait quoi faire », a témoigné l'un d'eux sur le site Fusion, décrivant une hostilité grandissante au sein de Sony Pictures à l'encontre du service informatique. Le FBI, chargé de l'enquête, devrait faire le point devant les employés sur le comportement à adopter face à cette situation le 12 décembre.

Les dirigeants de Sony Pictures ne sont pas épargnés. L'un des premiers documents diffusés par le site d'information Fusion dresse le détail des rémunérations des 17 salariés les mieux payés, à commencer par le dirigeant Michael Lynton (3 millions de dollars par an) – une seule femme dans ce palmarès. Parmi les fichiers publiés figurent des sauvegardes de plusieurs mois de conversations par courriels (professionnels et personnels) issues des messageries Outlook de cadres de l'entreprise : Amy Pascal, vice-présidente de Sony Pictures, Steve Mosko, à la tête de Sony Television, ou encore Leah Weill, conseiller juridique en chef.

Des révélations sur les films et les séries Sony

Dans son ensemble, cette masse de données fourmille d'informations sur la manière dont Sony Pictures gère son catalogue, ses productions et ses projets. Finances de l'entreprise, projets marketing, bilans comptables liés aux séries diffusées à la télévision américaine, rétrospectives annuelles, bases de contacts, documents préparatoires pour des négociations… Ces milliers de fichiers bruts s'accompagnent de visées stratégiques, comme en témoignent les points de vue exprimés par des employés (s'énervant par exemple contre l'omniprésence d'Adam Sandler à l'écran).

Dans ces documents se nichent ainsi, fatalement, des informations propres aux films et aux séries télévisées estampillées Sony. On y apprend par exemple comment les dirigeants de Sony Pictures ont fait modifier la fin du film The Interview (attention spoiler !), et négocié avec Marvel, qui souhaitait que Spiderman apparaisse dans le prochain Captain America. Plus problématique, des scripts inédits d'épisodes de séries, et même de films devant sortir en 2015, ont été repérés.

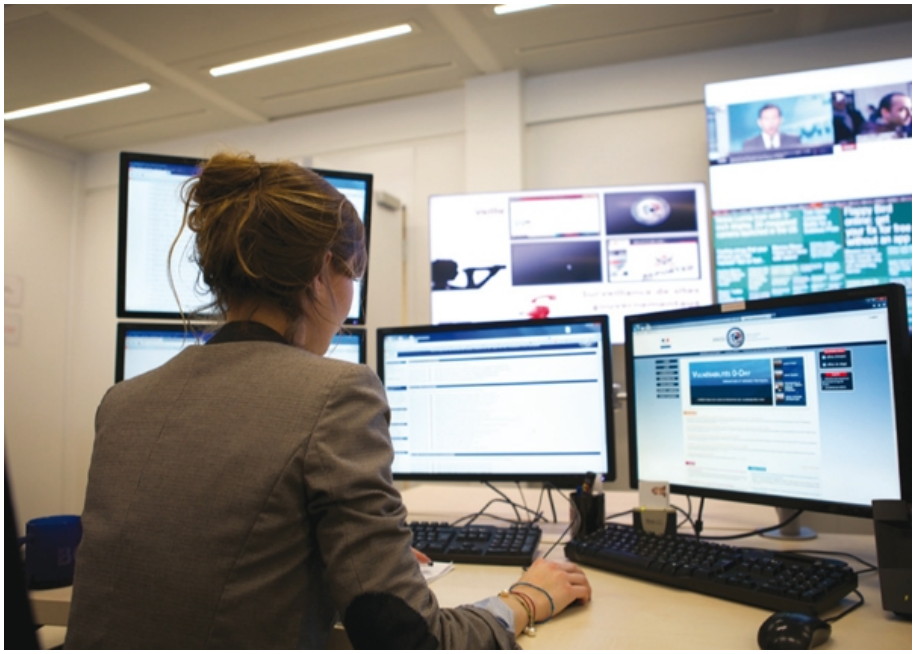
Plusieurs médias, comme le Wall Street Journal, ont également extrait diverses phrases chocs des e-mails échangés ces dernières années par la vice-présidente Amy Pascal avec le tout-Hollywood (réalisateurs, agents, stars, etc.). On y trouve quelques commentaires désobligeants sur des acteurs : Angelina Jolie et son « ego devastateur » en prennent pour leur grade. Ou encore, une chronique détaillée des négociations et conversations, parfois brutes de décoffrage, entourant le biopic sur Steve Jobs sur lequel Sony travaille depuis trois ans (notamment sur les choix de casting du scénariste Aaron Sorkin, qui avait songé à Tom Cruise pour incarner le fondateur d'Apple).

En savoir plus sur http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html#Ox8W3PwS6l8JJu0T.99
Par Michaël Szadkowski journaliste à Pixels

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html
par Par Michaël Szadkowski

Les cyber attaques dans le transport maritime



Les cyber attaques dans le transport maritime

La cyber-défense est classée au rang des priorités par le gouvernement. Un plan d'investissement d'un milliard d'euros sur 5 ans a été dévoilé au début de l'année pour faire face à cette nouvelle menace.

Des cyber-attaques qui inquiètent aussi le monde maritime.
« Le transport et la logistique maritimes sont le prochain terrain de jeux des pirates informatiques » : c'est le BMI, le Bureau Maritime International qui le dit..
L'organisme est spécialisé dans la lutte contre la criminalité envers le commerce maritime, notamment la piraterie et les fraudes commerciales ainsi que dans la protection des équipages. Dans un communiqué publié le 20 août 2014, le BMI a tiré la sonnette d'alarme en appelant l'ensemble de secteur à se protéger contre les cyber-attaques..
Si ces cyber-menaces inquiètent c'est parce qu'aujourd'hui dans un bateau, presque tout est informatisé. Tout est connecté à Internet entre la terre et la mer.
Aujourd'hui il est possible pour un hacker (voire un État) de détourner des informations, de prendre le contrôle d'un navire ou même de son système d'armement..
Au début c'était un jeu, c'est devenu une véritable guerre. Vous avez des menaces de ce type-là qui sont organisées comme des réseaux terroristes.

Trafic de drogue, vol de données, kidnapping
Les spécialistes en cyber-défense ont identifié deux menaces principales, comme l'espionnage et le sabotage.
Un « espion » peut par exemple « voler les données techniques » pour connaître avec précisions le trajet emprunté par un bateau. Cela « permet à un concurrent de voler le marché et de pratiquer des prix plus bas », raconte Dominique Riban, de l'ANSSI (Agence nationale de sécurité des systèmes d'information).
C'est elle qui surveille les sites internet de l'État français. Elle a été créée après la publication du Livre blanc de la Défense en 2008.

Télécharger l'intégralité du Livre blanc de la Défense

« Tout est potentiellement attaquable »
L'angoisse des experts en cyber-défense c'est aussi l'attaque des géants des mers, ces containers géants qui débarquent dans les ports européens.
Le plus gros au monde doit transporter 20 000 containers pour une valeur de deux à quatre milliards de dollars. On y trouve tout un tas de systèmes de cartographie, d'informations. Tous ces systèmes là sont potentiellement attaquables.
Patrick Hebrard est titulaire de la chaire Cyber-défense des systèmes navals à l'Ecole navale. Il s'occupe aussi de cyber-défense chez DCNS. « La passerelle peut ne plus avoir la maitrise de sa propulsion et de sa gouverne », poursuit-il. « Un hacker pourrait complètement bloquer la barre d'un bateau. »
En 2011, l'Agence européenne de cyber-sécurité (ENISA) a publié un premier rapport européen sur la cyber-sécurité maritime. Elle évoquait déjà les menaces qui s'amplifiaient. Elles mettaient en garde sur les conséquences désastreuses de ces cyber-attaques.
La même année, le port d'Anvers (dans lequel des milliers de containers sont débarqués chaque semaine sur les quais) avait été piraté par un cartel de la drogue. Ils avaient réussi à récupérer la marchandise avant que les douanes n'inspectent les containers.

Un yacht (volontairement) piraté et détourné
En 2013, un groupe d'étudiants en école d'ingénieurs a fait une expérience en pleine mer : ils ont piraté un yacht de luxe pour le détourner de son trajet initial, en utilisant le système GPS..
C'était en fait un test organisé avec l'accord des propriétaires du bateau. Naviguant de Monaco à l'île de Rhodes, le yacht a été piraté en pleine mer Ionienne. Grâce à un faux boîtier simulateur GPS, ils ont envoyé des signaux de localisation avec de fausses données, des signaux plus forts que ceux transmis par les satellites. Les « faux signaux » se sont donc substitués aux vrais, en les brouillant. Le yacht a alors viré de bord, en modifiant le pilote automatique.
« Les armateurs prennent de plus en plus en compte ces menaces », explique Eric Banel, secrétaire général d'Armateurs de France. « Les politiques d'entreprises contiennent quasiment toutes un chapitre sur la cyber-criminalité. »
Quand aux constructeurs navals, comme DCNS qui construisent des bateaux pour la Marine nationale notamment, ils développent des moyens pour faire face à cette cyber-criminalité maritime, avec aussi des experts présents à terre pour surveiller les flux qui transitent entre la terre et le bateau.
L'école navale, Telecom Bretagne, DCNS et Thales se sont associés pour créer, avec le soutien de la région Bretagne, une chaire de cyber-défense des systèmes navals. Le but est de mettre en œuvre toutes les techniques pour lutter contre les menaces du cyberespace. Cette chaire universitaire mais aussi industrielle ambitionne de stimuler la cyber-innovation. Des chercheurs qui devront trouver des parades à la vulnérabilité des navires en mer, du porte-container au méthanier en passant par les navires de guerre.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.franceinter.fr/emission-le-zoom-de-la-redaction-les-cyber-attaques-dans-le-transport-maritime

Panorama 2015 des menaces informatiques

	**Panorama 2015 des menaces informatiques**

McAfee, filiale d'Intel Security, publie son nouveau rapport annuel, intitulé '2015 Threats Prediction', qui met l'accent sur les principales menaces prévues pour l'année 2015. McAfee présente conjointement son rapport 'November 2014 Threat Report' relatif à l'analyse des menaces informatiques du dernier trimestre 2014.

Les prévisions 2015 de McAfee en matière de menaces :
1. Une fréquence accrue du cyber-espionnage. La fréquence des attaques de cyber-espionnage continuera d'augmenter. Les pirates actifs de longue date mettront en place des techniques de collecte des informations toujours plus furtives, tandis que les nouveaux venus chercheront des solutions pour subtiliser de l'argent et perturber les activités de leurs adversaires.
Les cyber-espions actifs de longue date travailleront à parfaire des méthodes toujours plus efficaces pour demeurer cachés sur les systèmes et les réseaux de leurs victimes. Les cybercriminels continueront à agir davantage comme des cyber-espions, en mettant l'accent sur les systèmes de surveillance et la collecte de renseignements sensibles relatifs aux individus, à la propriété intellectuelle et à l'intelligence opérationnelle. McAfee Labs prévoit que la cyberguerre sera davantage utilisée par les plus petits États et les groupes terroristes.

2. Attaques fréquentes, profitables et sévères envers l'Internet des objets. A moins d'intégrer le contrôle de la sécurité dès la conception des produits, le fort déploiement de l'IdO devrait dépasser les priorités de sécurité et de confidentialité. La valeur croissante des données pouvant être recueillies, traitées et partagées par ces dispositifs devrait attirer leurs premières attaques en 2015.
La prolifération croissante des appareils connectés dans des environnements tels que la santé pourrait également fournir aux logiciels malveillants un accès à des données personnelles plus sensibles que les données relatives aux cartes de crédit. En effet, selon le rapport de McAfee Labs intitulé « Cybercrime Exposed : Cybercrime-as-a-Service », chacune de ces données représenterait un gain d'environ 10 $ pour un cybercriminel, soit 10 à 20 fois la valeur d'un numéro de carte de crédit américaine volé.

3. Les débats autour de la vie privée s'intensifient. La confidentialité des données sera toujours menacée, dans la mesure où les pouvoirs publics et les entreprises peinent à déterminer ce qui constitue un accès équitable et autorisé à des « informations personnelles » mal définies.

En 2015, les discussions vont se poursuivre pour définir ce que sont les « informations personnelles » et dans quelle mesure elles peuvent être accessibles et partagées par des acteurs étatiques ou privés. Nous allons voir une évolution de la portée et du contenu des règles de la protection des données ainsi que des lois de réglementation de l'utilisation de l'ensemble de données préalablement anonymes. L'Union Européenne, les pays d'Amérique latine, ainsi que l'Australie, le Japon, la Corée du Sud, le Canada et bien d'autres pays adopteront des lois et des règlements de protection des données plus strictes.

4. Les ransomwares évoluent dans le Cloud. Les logiciels de demande de rançon (ransomware) connaîtront une évolution dans leurs méthodes de propagation, de chiffrement et de cibles visées. McAfee Labs prévoit également que de plus en plus de terminaux mobiles essuieront des attaques.

Une nouvelle variante de ransomware capable de contourner les logiciels de sécurité devrait aussi faire son apparition. Elle ciblera spécifiquement les terminaux dotés de solutions de stockage dans le Cloud. Une fois l'ordinateur infecté, le ransomware tentera d'exploiter les informations de connexion de l'utilisateur pour ensuite infecter ses données sauvegardées dans le Cloud. La technique de ciblage du ransomware touchera également les terminaux qui s'abonnent à des solutions de stockage dans le Cloud. Après avoir infecté ces terminaux, les logiciels de ransomware tenteront d'exploiter les informations de connexion au Cloud. McAfee Labs s'attend à une hausse continue des ransomwares mobile, utilisant la monnaie virtuelle comme moyen de paiement de la rançon.

5. De nouvelles surfaces d'attaque mobiles. Les attaques mobiles continueront d'augmenter rapidement dans la mesure où les nouvelles technologies mobiles élargissent la surface d'attaque.
L'émergence de kits de génération de logiciels malveillants sur PC et la distribution de code source malveillant pour mobile permettront aux cybercriminels de désormais cibler ces appareils. Les app stores frauduleux continueront d'être une source importante de malwares sur mobile. Le trafic engendré par ces boutiques d'applications sera notamment conduit par le 'malvertising', qui s'est rapidement développé sur les plateformes mobiles.

6. Les attaques dirigés contre les points de vente augmentent et évoluent avec les paiements en ligne. Les attaques dirigées contre les points de vente demeureront lucratives et l'adoption croissante par le grand public des systèmes de paiement numérique sur appareils mobiles offrira aux cybercriminels de nouvelles surfaces d'attaque à exploiter.

Malgré les efforts des commerçants de déployer des cartes à puce et à code PIN, McAfee Labs prévoit pour 2015 une hausse significative des failles de sécurité liés aux points de vente. Cette prédiction est notamment basée sur le nombre de dispositifs de points de vente devant être upgradés en Amérique du Nord. La technologie de paiement sans contact (NFC) devrait devenir un nouveau terrain propice à de nouveaux types d'attaques, à moins que les utilisateurs ne soient formés au contrôle des fonctions NFC sur leurs appareils mobiles.

7. Logiciels malveillants au-delà de Windows. Les attaques de logiciels malveillants ciblant des systèmes d'exploitation autres que Windows exploseront en 2015, stimulées par la vulnérabilité Shellshock.

McAfee Labs prévoit que les conséquences de la vulnérabilité Shellshock seront ressenties au cours des années à venir par les environnements Unix, Linux et OS X, notamment exécutés par des routeurs, des téléviseurs, des systèmes de contrôle industriels, des systèmes de vol et des infrastructures critiques. En 2015, McAfee Labs s'attend à une hausse significative des logiciels malveillants non-Windows dans la mesure où les hackers chercheront à exploiter cette vulnérabilité.

8. Exploitation croissante des failles logicielles. Le nombre de failles décelées dans des logiciels populaires continuant d'augmenter, les vulnérabilités enregistreront une forte hausse.

McAfee Labs prévoit que l'utilisation de nouvelles techniques d'exploitation telles que la falsification de pile (stack pivoting), la programmation orientée retour (RDP, Return Oriented Programming) et la programmation orientée saut (JOP, Jump-Oriented Programming), combinées à une meilleure connaissance des logiciels 64 bits, favorisera l'augmentation du nombre de vulnérabilités détectées, suivi en cela par le nombre de logiciels malveillants exploitant ces nouvelles fonctionnalités.

9. De nouvelles tactiques d'évasion pour le sandboxing. Le contournement du sandbox deviendra un problème de sécurité informatique majeur.

Des vulnérabilités ont été identifiées dans les technologies d'analyse en environnement restreint (sandboxing) mises en œuvre avec les applications critiques et populaires. McAfee Labs prévoit une croissance du nombre de techniques visant à l'exploitation de ces vulnérabilités ainsi que le contournement des applications de sandboxing. Aujourd'hui, un nombre significatif de familles de logiciels malveillants parviennent à identifier les systèmes de détection de type sandbox et à les contourner. A ce jour, aucun logiciel malveillant en circulation n'est parvenu à exploiter des vulnérabilités de l'hyperviseur pour échapper à un système de sandbox indépendant. Il pourrait en être autrement en 2015.

Pour lire le rapport 'McAfee Labs – Threat Report' dans son intégralité, cliquez ici : http://mcaf.ee/ojbsz

Retour sur 2014
Durant le troisième trimestre 2014, McAfee Labs a détecté plus de 307 nouvelles menaces par minute, soit plus de 5 chaque seconde, avec une croissance des logiciels malveillants sur mobile en hausse de 16 % sur le trimestre, soit une croissance annuelle de 76 %. Les chercheurs de McAfee Labs ont également identifié de nouvelles tentatives visant à tirer profit des protocoles de sécurité Internet, notamment les vulnérabilités de protocoles SSL tels que Heartbleed et BERserk, ainsi que l'abus répété des signatures numériques pour masquer les malwares comme étant légitimes.

Pour 2015, McAfee Labs alerte sur les techniques de cyber-espionnage des pirates informatiques et prévoit que les hackers actifs de longue date mettront en place des techniques de collecte de données confidentielles toujours plus furtives au travers d'attaques ciblées étendues. Les chercheurs du Labs prévoient ainsi de mettre davantage d'efforts sur les vulnérabilités liées à l'identification d'applications, de systèmes d'exploitation et au réseau, ainsi que sur les limites technologiques du sandboxing, dans la mesure où les hackers tentent de se soustraire à l'application de détection par hyperviseur.

« L'année 2014 restera dans les mémoires comme l'année où la confiance en matière de sécurité informatique a été ébranlée », déclare David Grout, directeur Europe du Sud de McAfee, filiale d'Intel Security. « Les nombreux vols et pertes de données ont altéré la confiance de l'industrie envers le modèle d'Internet ainsi que celle des consommateurs dans la capacité des entreprises à protéger leurs données. La confiance des entreprises, ainsi que celle des organisations, ont également étaient impactées et les a poussé à s'interroger sur leur capacité à détecter et à détourner les attaques dont elles ont été la cible », poursuit David Grout. « En 2015, l'industrie d'Internet devra se renforcer pour restaurer cette confiance, mettre en place de nouvelles normes pour s'adapter au nouveau paysage des menaces et adopter de nouvelles stratégies de sécurité qui requièrent de moins en moins de temps dans la détection des menaces. Ainsi, nous devons tendre à un modèle de sécurité intégrée dès la conception de chaque appareil. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/McAfee-Labs-dresse-le-panorama,20141210,49364.html