Le régulateur mondial d’internet victime d’une attaque informatique

Le régulateur mondial d’internet victime d’une attaque informatique

Le régulateur mondial d’internet, l’Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.

Une attaque par « hameçonnage » a en effet visé l’agence américaine et plusieurs de ses employés ont reçu des courriels destinés à ressembler à ceux envoyés par un de leurs collègues avec une adresse se terminant en « icann.org », selon le blog de l’Icann.

« Plusieurs employés ont vu leurs références dérobées », a précisé l’agence.
L’attaque a, semble-t-il, commencé en novembre. Typiquement, les attaques par hameçonnage sont destinées à duper les gens en les conduisant à cliquer sur des pages factices où ils rentrent leurs adresses et mots de passe, qui sont ainsi récupérés par les pirates informatiques.
Cette ruse a permis aux hackers de récupérer les adresses et mots de passe de plusieurs employés de l’Icann. Ils ont donc pu s’introduire plus avant au sein du système informatique de l’organisation.
Ils ont ainsi pu pénétrer dans des serveurs sécurisés où ils ont récupéré des dossiers sur des noms de domaines, des adresses et des mots de passe d’utilisateurs, a encore indiqué l’Icann.
Le blog et l’annuaire n’ont pas été trafiqués, a encore noté l’Icann sans préciser qui pourrait être à l’origine de l’attaque.
L’Icann, dont la mission est d’attribuer les noms de domaines des sites internet, devrait quitter le giron américain en fin d’année prochaine. Washington a en effet annoncé en mars qu’il pourrait ne pas renouveler son contrat avec la société basée à Los Angeles si un système de contrôle indépendant est en place pour assurer la fiabilité du système d’attribution des adresses.

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

Source : http://www.7sur7.be/7s7/fr/4134/Internet/article/detail/2156470/2014/12/18/Le-regulateur-mondial-d-internet-victime-d-une-attaque-informatique.dhtml

---

Live streaming illégal : un coût considérable pour

l’économie mondiale

	**Live streaming illégal : un coût considérable pour l’économie mondiale**

Une étude du Center for Strategic and Internationals Studies (CSIS) faisait grand bruit lors de sa sortie, en juin dernier. Elle évaluait à 445 milliards de dollars, soit 327 milliards d'euros, le coût global de la cybercriminalité sur l'économie mondiale. S'il semble compliqué de lutter contre ce fléau sans visage, la limitation de certains comportements à risque permettrait de réduire substantiellement la note pour les industries du secteur, mais aussi et surtout pour les internautes. Ainsi en va-t-il du live streaming illégal, plébiscité mais toxique.

Radiographie de la cybercriminalité mondiale

Sans surprise, les pays les plus exposés aux méfaits des cybercriminels sont les grandes puissances. A eux seuls, Etats-Unis, Chine et Allemagne concentrent 200 milliards de pertes dues à des piratages en tout genre, même si essentiellement par vol de propriété intellectuelle.

L'importance des dégâts commis par les hackers est inversement proportionnelle au nombre d'entre eux capables de conceptualiser des programmes permettant d'exploiter des failles logicielles connues (exploits). Selon le Centre de lutte contre la Cybercriminalité d'Europol, seule une centaine de personnes serait responsable de la cybercriminalité dans le monde. Autrement dit, si d'innombrables réseaux cybercriminels s'approprient les kits d'exploits et malwares créés par d'autres, ils ne sont qu'une poignée à pouvoir être considérés comme les cerveaux du hacking international.

Europol précise que ces kits et malwares sont à ce point élaborés qu'ils peuvent facilement être adaptés aux cibles spécifiques des cybercriminels. Des cibles qui sont souvent des entreprises dont les solutions de sécurité laissent à désirer, mais aussi des particuliers, notamment via leur utilisation du live-streaming illégal, véritables supermarchés pour les hackers, qui n'ont qu'à se pencher pour se servir.

Le live streaming illégal, tête de pont de la cybercriminalité mondiale

Début octobre, l'Association of Internet Security Professionals (AISP) se fendait d'un rapport alarmant. Intitulé « Illegal Streaming and Cyber Security Risks : a dangerous status quo ? » il montrait que 500 millions d'ordinateurs étaient infectés dans le monde, soit une infection toutes les 18 secondes.

Concernant les sites de live streaming illégaux, type retransmission de matchs de sport, le rapport de l'AISP se fait très précis. Selon lui, 80 % de ces plateformes hébergeraient des malwares, visant à subtiliser des données confidentielles aux personnes les fréquentant. Avec pour but, in fine, de bombarder leurs boites mails de spams, de subtiliser leurs codes bancaires ou encore d'usurper leur identité.

67 milliards de dollars sont dépensés par an en achat de services de sécurité sur Internet. Cette somme pourrait être considérablement réduite si les internautes prenaient conscience des risques encourus en surfant, par exemple, sur des sites de live streaming illégaux.

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

Source : http://www.actu-economie.com/2014/12/18/live-streaming-illegal-cout-considerable-leconomie-mondiale/
Par Christophe Fourrier

Détection d’une grande famille de malware et découverte de son mode opératoire

	Détection d’une grande famille de malware et découverte de son mode opératoire

La nouvelle variante de ransomware TorrentLocker atteint en 2014 plus de 40 000 systèmes informatiques européens.

Quelles sont les caractéristiques de cette nouvelle variante ?

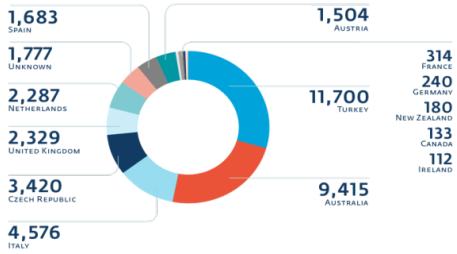
L'équipe de chercheurs canadienne ESET, spécialisée en menaces cybercriminelles, a découvert que depuis le début de l'année 2014, des attaques de ransomware du nom de TorrentLocker se propageaient partout en Europe. Cette variante identifiée par ESET comme Win32/Filecoder.Dl, appartient à la famille des ransomware. Il paraîtrait que les acteurs cachés derrière ce malware seraient de la même famille que le cheval de Troie bancaire : Hesperbot. Sa méthode change en revanche, puisque qu'il passe de la norme AES (Advanced Ecryption Standards) du chiffrement basé sur un compteur (CTR) au chiffrement d'enchaînement des blocs (Cipher Block Chaining, CBC)..

Le logiciel malveillant s'introduit malicieusement dans le système d'exploitation de sa victime, via des liens infiltrés eux-mêmes dans des e-mails frauduleux. Le logiciel crypte ensuite les données de l'ordinateur. Les documents, photographies et autres fichiers sont alors inutilisables pour le propriétaire. Le hacker peut aussitôt demander à la victime de payer une rançon si elle ne veut pas que ses données soient détruites. Les sommes demandées sont considérables, pouvant atteindre les 1200€. Pour déverrouiller ces données, la victime a besoin d'un code de déchiffrement que seul le pirate peut lui fournir et sans garantie.

Des techniques de persuasion toujours plus performantes

Les propriétaires de ces logiciels malveillants savent être de plus en plus convaincants en ciblant le message en fonction des pays qu'ils convoitent. Ils savent de mieux en mieux personnaliser et adapter leur message sur leurs cibles. Par conséquent, ils sont de plus en plus dangereux, car ces « faux » e-mails sont de plus en plus difficile à détecter pour les victimes.

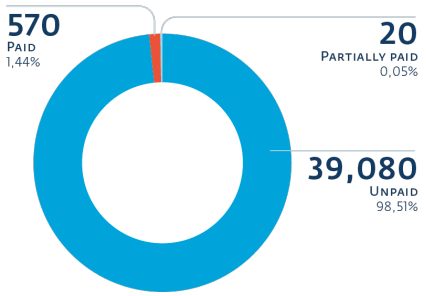
Les acteurs de ce logiciel malveillant utilisent de nombreuses ruses pour convaincre les internautes. Ils envoient des messages personnalisés, en mimant la provenance d'un organisme certifié. Ils en profitent ensuite pour réclamer le paiement d'une fausse facture. Ils arrivent même à troubler les internautes en allant jusqu'à insérer des images de CAPTCHA.



Nombre de victimes ayant payé les cybercriminels pour le logiciel

Des conséquences irrémédiables, attention à ne pas les encourager !

La dernière vague de TorrentLocker a atteint 40 000 ordinateurs, représentant 280 millions de documents chiffrés en Europe, Canada, Australie et Nouvelle-Zélande. Près de 600 victimes ont payé la rançon, ce qui a fait gagner 481 578€ aux malfaiteurs en Bitcoins! En France, Torrentlocker a intercepté 2 170 247 fichiers avec une demande de rançon d'au minimum 830€.



Nombre de victimes ayant payé les cybercriminels pour le logiciel

L'équipe de chercheurs canadiens ESET a su démanteler TorrentLocker en localisant le malware grâce aux serveurs C&C qui généraient des URL pour les pages d'échanges d'argent avec les victimes.

La première règle à prendre en considération est qu'il faut d'une part protéger ses appareils que ce soit un PC, un Mac, un smartphone ou une tablette sous Android. Ensuite il faut veiller à ne pas ouvrir des e-mails inconnus ou paraissant suspects et surtout ne pas cliquer sur un lien trop rapidement ni ouvrir la pièce jointe. Le conseil à retenir est de ne pas payer les rançons demandées, ce qui encourage les pirates et les entraîne à développer leurs logiciels malveillants.

Les actualités sur Torrentlocker

Le logiciel malveillant est en constante évolution, l'équipe de sécurité ESET a mis en place un livre blanc, où elle publie régulièrement leurs analyses et informe sur les nouvelles apparences que prend le logiciel au fil du temps, disponible sur www.welivesecurity.com.

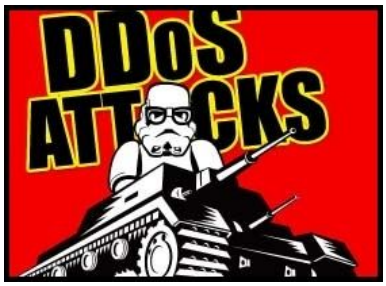
Pour plus d'informations sur TorrentLocker, vous pouvez consulter le livre blanc sur
http://presse.marketing-land.com/r/?F=23e5g9n2ctsdr5hy9tpgyh7gqgazh6hj3y38q6ds3xp5zm8q23sfj4q-5686679

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 : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a6329542c28f29

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.

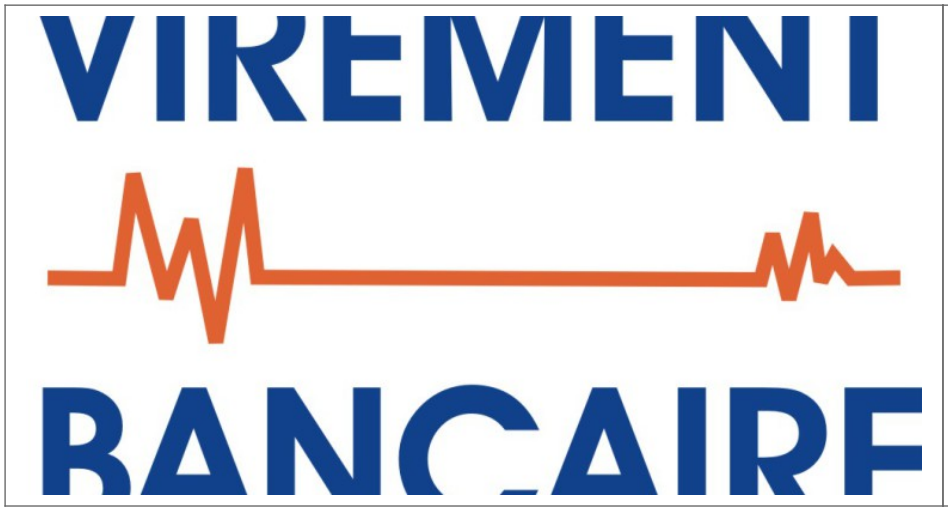
3. Investir dans une solution de mitigation DDoS architecturée pour ne jamais abandonner le bon trafic. Les prestataires de services hébergés doivent impérativement empêcher que l'équipement de sécurité ne devienne un goulot d'étranglement pour les services rendus et toujours permettre au trafic légitime 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

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

---

Fichiers pédopornographiques: un habitant de Peille arrêté

Fichiers pédopornographiques: un habitant de Peille arrêté

Un jeune homme de 21 ans, menuisier, inconnu de la justice, a été interpellé par le groupe « cybercriminalité », de la police judiciaire de Nice. Il est soupçonné d'avoir téléchargé pendant un an des centaines de fichiers (images et vidéos) de viols d'enfants.

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

Source : http://www.monacomatin.mc/nice/fichiers-pedopornographiques-un-habitant-de-peille-arrete.2023663.html

---

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.

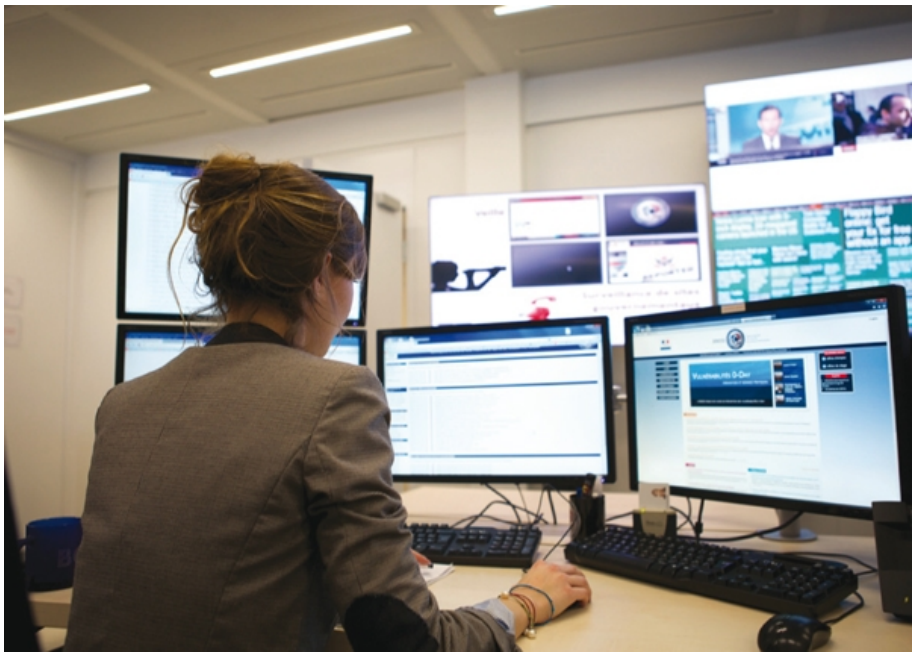
« Si nous pouvons qualifier l'année 2014 de 'sophistiquée', alors 2015 sera sous le signe de la 'furtivité'

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

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