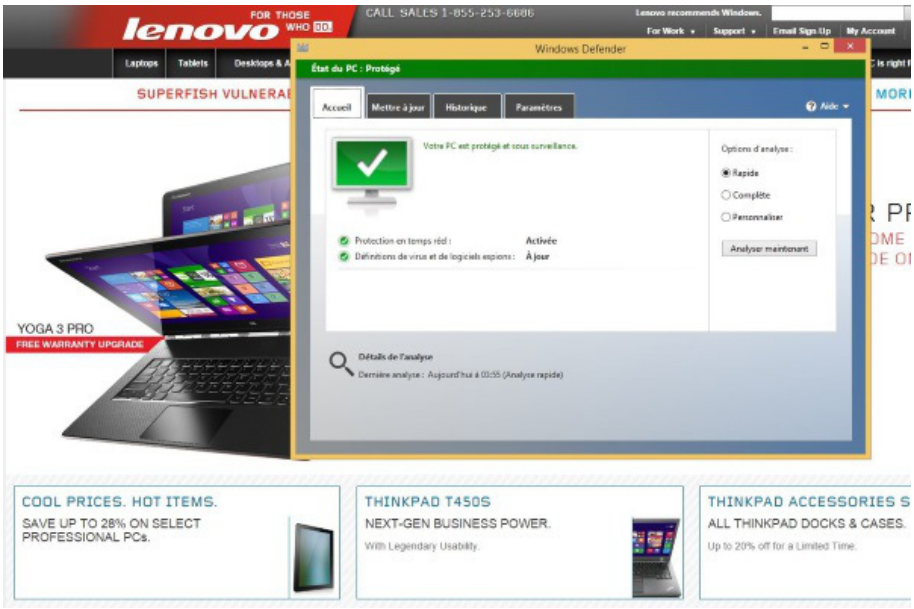
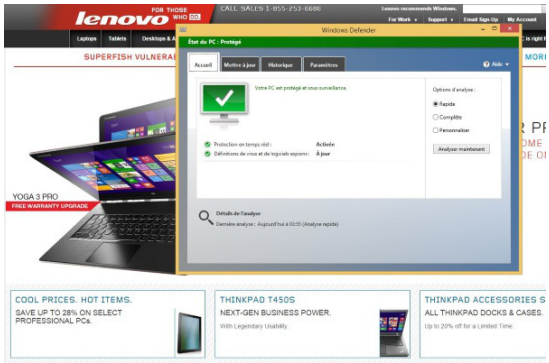
Les ordinateurs Lenovo contaminés d’usine…



Les ordinateurs Lenovo contaminés d’usine…

Possédez-vous un ordinateur grand public récent vendu par Lenovo? Si oui, il y a de fortes chances pour que votre appareil ait été livré avec Superfish, un logiciel publicitaire dangereux, qui pourrait notamment permettre à des pirates malintentionnés d'accéder à vos connexions web sécurisées. S'il était jusqu'ici difficile de se prémunir contre cette faille, Microsoft et Lenovo viennent de simplifier la chose, grâce à une mise à jour rapide de l'antivirus Windows Defender et à la mise en ligne d'un outil pour enlever le logiciel.C'est une semaine difficile qui se termine pour Lenovo, qui a volontairement équipé tous ses ordinateurs grand public vendus entre septembre 2014 et janvier 2015 de ce logiciel. Superfish n'a toutefois jamais été installé sur les ordinateurs ThinkPad et les ordinateurs pour entreprises de la compagnie.Pire, même si Lenovo a publié hier sur son site web un tutoriel pour expliquer comment enlever Superfish de ses ordinateurs, ce processus manuel ne corrige pas complètement le problème pour les ordinateurs déjà infectés.
C'est plutôt Microsoft qui a pris la chose en mains en premier aujourd'hui, avec une mise à jour de son antivirus Windows Defender, qui permet de désinstaller Superfish, en plus de mettre à jour les certificats SSL de l'ordinateur. Il suffit donc de mettre à jour Windows Defender et d'analyser son appareil pour s'en débarrasser.



Lenovo a finalement aussi publié un outil vendredi en soirée pour enlever convenablement Superfish. Celui-ci peut être télécharger automatiquement ici.
Les propriétaires d'un ordinateur Lenovo qui souhaitent savoir si leur appareil est affecté par Superfish peuvent suivre ce lien directement.
Voici la liste complète, mais peut-être pas exhaustive, des ordinateurs Lenovo livrés avec Superfish :
E-Series:
E10-30
Flex-Series:
Flex2 14, Flex2 15
Flex2 14D, Flex2 15D
Flex2 14 (BTM), Flex2 15 (BTM)
Flex 10
G-Series:
G410
G510
G40-70, G40-30, G40-45
G50-70, G50-30, G50-45
M-Series:
Miix2 – 8
Miix2 – 10
Miix2 – 11
S-Series:
S310
S410
S415; S415 Touch
S20-30, S20-30 Touch
S40-70
U-Series:
U330P
U430P
U330Touch
U430Touch
U540Touch
Y-Series:
Y430P
Y40-70
Y50-70
Yoga-Series:
Yoga2-11BTM
Yoga2-11HSW
Yoga2-13
Yoga2Pro-13
Z-Series:
Z40-70
Z40-75
Z50-70
Z50-75

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

Source : http://journalmetro.com/opinions/vie-numerique/724584/securite-informatique-microsoft-sattaque-a-superfish/
Par Maxime Johnson

Le ministre de la Poste et des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Le ministre de la Poste et des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Abidjan – Le ministre de la Poste et des Technologies de l'information et de la communication, Bruno Nabagné Koné, appelle au développement d' »une culture nationale » autour de la question de la sécurisation des réseaux et services numériques qui, estime-t-il, est essentielle pour lutter efficacement contre la cybercriminalité en Côte d'Ivoire.

Pour le ministre Nabagné Koné qui procédait lundi à l'ouverture d'un séminaire sur la cyber-sécurité organisé par l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI) autour du thème principal « Développement d'une stratégie nationale en matière de cyber sécurité », il s'agit notamment d'élever la question au rang de celles relevant de la sécurité nationale.
Le séminaire qui s'étendra sur deux jours se veut, selon le DG de l'ARTCI, Bilé Diéméléou, une lucarne d'échanges et de partage d'expériences afin de présenter les actions entreprises par sa structure dans l'accomplissement de sa mission visant à développer la cyber-sécurité.
La rencontre sera également l'occasion d'établir les bases du développement d'un partenariat public/privé fort en matière de cyber-sécurité avec la centaine de structures conviées, a-t-il ajouté.
Le ministre Nabagné Koné déplorait, à l'occasion, le fait que le traitement de la question de la sécurisation des réseaux et services numériques, « considérée comme la 5ème roue du carrosse dont on peut se passer », n'a pas toujours suivi le niveau d'évolution enregistré ces dernières années en Côte d'Ivoire en matière de TIC et même dans le monde.
C'est pourquoi, il appelle à une culture nationale en la matière et qui, selon lui, permettra de faire du souci de la sécurisation du cyber espace ivoirien une question de sécurité nationale.
Le ministre des TIC rappelait auparavant le danger que laisse planer la cybercriminalité sur le développement global de la Côte d'Ivoire, un phénomène qui, a-t-il reprécisé, va au-delà de la perception commune l'assimilant abusivement aux petites escroqueries commises au moyen des outils de moderne de communication.
La cybercriminalité est plutôt le fait pour une personne de s'introduire de façon malveillante dans des systèmes d'information, a-t-il fait comprendre, relevant que c'est cet aspect des choses qui rend le phénomène si préoccupant.
« Que des personnes entrent dans nos systèmes, c'est de cela que nous avons peur et c'est face à cela que nous devons prendre des mesures », a fait remarquer M. Nabagné Koné.
Il a notamment relevé le fait que le phénomène, s'il n'est pas efficacement combattu, pourrait consacrer un recul de l'usage des TICS qui partirait d'une méfiance légitime des populations vis-à-vis des solutions offertes.
« Sans confiance, la réaction des utilisateurs sera le rejet et c'est notre société qui recule », a laissé entendre le ministre.
« Les personnes malveillantes dans le cyberespace ou en ligne sont nombreuses, organisées et leurs motivations sont très diverses: politiques, criminelles, terroristes ou activistes. La cyber-sécurité doit faire partie intégrante du progrès technologique », a-t-il, pour ce faire, appelé.

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

Source : http://news.abidjan.net/h/526302.html

Voitures connectées faciles à hacker

Voitures connectées faciles à hacker

Les promesses de la voiture connectée font rêver : sans conducteur, intelligente,… mais visiblement, elle est aussi facile à pirater. Un hackeur en prend ici le contrôle, faisant du véhicule un danger pour ses passagers. Dans son émission « 60 minutes », CBS News consacre un dossier aux voitures connectées et à leurs failles de sécurité. Kathleen Fisher, experte de la DARPA (Defense Advanced Research Projects Agency) présente la voiture connectée comme un « ordinateur sur roues », soulignant de fait la possibilité de hacker le véhicule.

Démonstration à l'appui : il est en effet possible de contrôler la voiture à distance, à l'aide d'un simple ordinateur portable. Si déclencher les essuie-glaces ou le klaxon peut sembler « inoffensif », quand le hackeur prend contrôle des freins, c'est tout de suite plus inquiétant. Ici, il ne s'agit que de plots en plastique, mais on imagine rapidement les dégâts si une voiture connectée perdait les pédales « dans la vraie vie ».

Plus tôt cette semaine, le sénateur américain Edward J. Markey a sorti un rapport sur les dangers des voitures connectées. Il y compile les données fournies par 16 constructeurs automobiles dont BMW, Fiat Chrysler, Ford, General Motors, Nissan, Mitsubishi ou Mercedes-Benz après qu'il leur ait adressé une lettre et un questionnaire en décembre 2013. Certains constructeurs dont Tesla ont cependant refusé de lui répondre… Selon ses résultats, aucune mesure ne serait mise en place pour détecter et empêcher les tentatives de piratage ou les vols de données. Par ailleurs, outre la sécurité, le rapport revient aussi sur les problèmes de confidentialité des données : les propriétaires de voitures connectés ne seraient pas au courant de tout ce qui est enregistré à leur propos… De quoi faire réfléchir avant d'investir dans la voiture du futur.

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

Source : http://www.ladn.eu/actualites/pop-insight,voitures-connectees-faciles-hacker,74,24953.html

---

Cybercriminalité : un milliard de données volées en 2014 !

Cybercriminalité : un milliard de données volées en 2014 !

Selon l'étude Breach Level Index publié par le leader mondial de la sécurité numérique plus de 1 500 failles de données ont été enregistrées en 2014, entraînant le vol d'un milliard d'enregistrements de données. Par rapport à 2013, ces chiffres représentent une augmentation de 49 % du nombre de failles de données et de 78 % des enregistrements de données volées ou perdues.

Selon les données recensées dans l'indice BLI initialement réalisé par SafeNet pour l'année 2014, les cybercriminels sont principalement intéressés par le vol d'identité, 54 % des failles y étant rattachées, soit davantage que toute autre catégorie de failles y compris l'accès aux données financières. De plus, les infractions concernant les vols d'identité représentent également un tiers des failles de données les plus graves selon la notation du BLI (« catastrophique » pour une note comprise entre 9,0 et 10, ou « sévère » pour une note comprise entre 7,0 à 8,9). Les failles sécurisées, c'est-à-dire les failles de sécurité périmétrique où les données sont totalement ou partiellement cryptées, ont progressé de 1 % à 4 %.
« Nous assistons sans l'ombre d'un doute à un tournant dans la tactique abordée par les cybercriminels, le vol d'identité à long terme se substituant de plus en plus à l'immédiateté qui caractérise le vol des numéros de cartes de crédit », affirme Tsion Gonen, Vice-président en charge de la stratégie, Identity & Data Protection, Gemalto. « Le vol d'identité peut entraîner l'ouverture de nouveaux comptes de crédit frauduleux, la création de fausses identités à des fins criminelles, ainsi que d'autres activités d'une grande gravité. Les failles de données sont de plus en plus personnalisées, et il apparaît que pour l'utilisateur lambda, l'exposition aux risques est de plus en plus forte ».
Outre cette évolution vers le vol d'identité, les failles ont également augmenté en gravité en 2014, deux tiers des 50 failles les plus importantes selon leur score BLI ayant eu lieu l'année dernière. De plus, le nombre de failles de données impliquant plus de 100 millions d'enregistrements de données a doublé par rapport à 2013.
« Non seulement le volume des failles de données est en hausse, mais leur gravité est également de plus en plus importante. La question n'est plus de savoir « si » vous allez être victime d'un vol de données, mais « quand ». ajoute Tsion Gonen. La prévention des failles et la surveillance des menaces s'arrêtent là et ne sont pas toujours suffisantes pour repousser les cybercriminels. Les entreprises doivent adopter une vision des menaces numériques « centrée sur les données » en commençant par la mise en œuvre de meilleures techniques de gestion des identités et de contrôle d'accès, telles que l'authentification multi-facteurs, le chiffrement ou la gestion des clés pour sécuriser les données sensibles. Ces outils rendent les données subtilisées par les voleurs parfaitement inutilisables », précice-t-il.
En ce qui concerne les secteurs touchés, les services financiers et la grande distribution ont connu en 2014 les évolutions les plus significatives par rapport à d'autres segments industriels. La grande distribution est en légère augmentation par rapport à l'an dernier, avec 11 % de l'ensemble des failles de données enregistrées en 2014. Cependant, par le nombre d'enregistrements de données touchées, ce secteur est passé de 29 % en 2013 à 55 % en 2014 et ce, en raison de l'augmentation du nombre d'attaques visant les terminaux point de vente (TPV). Pour le secteur des services financiers, si le nombre de failles de données est resté relativement stable d'une année sur l'autre, le nombre moyen de dossiers perdus par faille a été multiplié par dix, passant de 112 000 en 2013 à 1,1 million en 2014.

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

Source : http://afriqueinside.com/cybercriminalite-milliard-donnees-volees-en-2014-12022015/

Un virus s’attaque au système informatique de la Ville de La Malbaie

	**Un virus s’attaque au système informatique de la Ville de La Malbaie**

Un virus provenant d'un fichier PDF qui semblait inoffensif s'est attaqué au système informatique de la Ville de La Malbaie, ralentissant considérablement le travail de certains de ses employés depuis une dizaine de jours.

«C'est un fichier PDF qui a été ouvert qui a ensuite contaminé le réseau et touché nos serveurs», relate le maire de la municipalité, Michel Couturier.

«Ça ne paralyse pas toutes les opérations, mais disons que ça les ralentit depuis 10 jours, puisque l'accès à certains logiciels est présentement impossible», explique-t-il, mentionnant que certains employés, notamment à la comptabilité, ont le temps ces jours-ci d'effectuer certaines tâches qu'ils n'avaient pas le temps de faire habituellement.

Vieux système

Par ailleurs, il souligne qu'aucun document n'a été perdu ou affecté par le virus, précisant qu'il ne s'agissait pas d'un acte de piratage. Alors que des experts en informatique s'affairent à régler le problème, M. Couturier admet que cet épisode risque d'accélérer la mise à jour du parc informatique de la ville. «On a quand même un vieux système de serveurs, on savait qu'il était à remplacer, mentionne-t-il. On avait prévu investir quelque part en 2015, mais disons que ça accélère un peu le tout.»

Selon le maire, le coût des opérations pour rétablir le système informatique à court terme à la suite du virus pourrait s'élever à 30 000$. «Il y a l'équipe de sous-traitants à payer et l'acquisition d'équipements, énumère-t-il, mais il y a aussi la perte de productivité. Ça aussi, ça a un coût.»

M. Couturier indique que tout devrait rentrer dans l'ordre d'ici la fin de la semaine. Selon lui, les services aux citoyens ne sont pas directement touchés par ces problèmes informatiques.

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

Source : http://www.journaldequebec.com/2015/02/10/virus-malbaie

Le groupe Capgemini lance une nouvelle ligne de services mondiale dédiée à la cybersécurité

	Le groupe Capgemini lance une nouvelle ligne de services mondiale dédiée à la cybersécurité

Capgemini lance sa nouvelle ligne de services mondiale dédiée à la cybersécurité. Celle-ci repose sur l'expertise de 2 500 professionnels de la cybersécurité, notamment des consultants, des auditeurs, des architectes, des spécialistes de la Recherche & Développement et des hackers éthiques , ainsi qu'un réseau mondial de 5 Centres Opérationnels de Sécurité (SOC, Security Operations Centers) et un large écosystème de partenaires technologiques. Capgemini prévoit une croissance élevée à deux chiffres de sa nouvelle ligne de services au cours des douze prochains mois. Elle doit permettre aux entreprises de mettre en œuvre un programme de transformation digitale en toute sécurité et de tirer parti des technologies du « SMACT » (Social, Mobile, Analytics, Cloud and Internet of Things) en toute confiance.

L'évolution rapide de la cybercriminalité a placé la sécurité au cœur des préoccupations des dirigeants. En effet, **entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120%** dans le monde et **le coût estimé de la cybercriminalité pour les entreprises s'élève en moyenne à 7,6 millions de dollars par an**, soit une augmentation de 10%. En outre, les hackers ont considérablement accru leurs connaissances des systèmes ciblés. De ce fait, les conséquences de leurs attaques sont de plus en plus importantes. Pour les entreprises du secteur de l'industrie, ces conséquences ne sont pas seulement financières ou réputationnelles mais peuvent également être matérielles ou humaines.
La nouvelle ligne de services mondiale dédiée à la cybersécurité de Capgemini répond aux problématiques de sécurité des systèmes IT, des systèmes industriels (OT), ainsi que des objets connectés (IoT- Internet Of Things). Selon la récente étude menée par Capgemini Consulting auprès de fournisseurs de technologies d'objets connectés, **les entreprises doivent être mieux préparées à faire face aux menaces qui pèsent sur la sécurité et sur la confidentialité des données** : seules 33% d'entre elles pensent que leurs objets connectés sont « très résistants » aux futures menaces de cybersécurité et 70% considèrent que « les questions de sécurité influencent les décisions d'achat des clients relatives aux objets connectés » .
La nouvelle ligne de services développera des services packagés et industrialisés qui peuvent être répliqués dans tous les pays. Ces offres de services packagés répondent aux besoins de sécurité de l'IT de nouvelle génération tels que la sécurité des infrastructures Hadoop, la sécurité des SDDC (Software-Defined Data Centers), ainsi que la sécurité des Clouds hybrides privés et publics. De nouvelles offres seront également lancées, telles que des tests de sécurité des applications « as-a-service » et des solutions de gestion des identités et des accès « as-a-service », pour permettre aux entreprises de tirer parti de l'approche Cloud et faciliter le déploiement de solutions de sécurité.
Selon Forrester Research , « L'importance de la protection de la vie privée, la recrudescence des cyberattaques et l'éclatement du périmètre de l'entreprise digitale ont obligé les professionnels de la sécurité et de la gestion des risques à renforcer la protection des données elles-mêmes. Dans la bataille pour recruter, servir et fidéliser ses clients, la protection de la vie privée et la sécurité des données sont devenues des avantages concurrentiels, et de ce fait une priorité business et technologique. »

La ligne de services mondiale dédiée à la cybersécurité de Capgemini permettra aux entreprises d'adopter une approche globale et pragmatique de leur stratégie de sécurité. Elle consolide l'expertise de Capgemini en tant qu'intégrateur de systèmes et fournisseur de services. Elle repose également sur sa connaissance approfondie de la cybersécurité, acquise dans le cadre des nombreuses missions réalisées auprès de ses clients au cours des dix dernières années dont celles menées pour le ministère du Travail et des Retraites (DWP) au Royaume-Uni, l'Agence spatiale française (CNES), Alstom Transport et Foyer (le plus important groupe d'assurance au Luxembourg).

Capgemini a conçu une gamme de services de cybersécurité assurant la protection des utilisateurs (identité numérique et contrôle d'accès), des applications, des terminaux (les terminaux de bureau, smartphones, tablettes, capteurs et autres objets connectés), des infrastructures (stockage, réseaux, serveurs, virtualisation et orchestration) et des données.

Les services proposés sont les suivants :

• Le conseil en sécurité et l'audit de sécurité
o Cela inclut l'évaluation des systèmes de sécurité, la définition de feuilles de route, les conseils opérationnels de sécurité et les audits de sécurité, tels que les tests d'intrusion et les investigations numériques.
o En janvier 2015, lors du Forum international de la cybersécurité (FIC), le prix « Label France Cybersecurity » a été décerné à Sogeti France, filiale du groupe Capgemini, par Axelle Lemaire, Secrétaire d'Etat chargée du numérique pour ses services d'audit de sécurité.
o Capgemini a aussi récemment conduit plusieurs missions de conseil comme pour Alstom Transport, incluant une analyse de risques, l'identification des cibles de sécurité et des recommandations d'architecture afin d'assurer la cybersécurité des trains et du système de signalisation.

• La conception et le développement de solutions pour protéger les systèmes informatiques, les systèmes industriels et les systèmes intelligents (objets connectés) :
o Grâce à l'acquisition d'Euriware, société française de services informatiques, Capgemini propose des services pour sécuriser les systèmes SCADA (systèmes de contrôle et d'acquisition de données). En outre, Sogeti High Tech offre des services qui permettent d'intégrer la sécurité dans le processus de développement des objets connectés.
o En outre, en partenariat avec Pivotal, Capgemini a récemment lancé une offre de Détection de Comportements Anormaux (Anomalous Behavior Detection) pour permettre aux entreprises d'identifier et de répondre aux menaces informatiques internes et externes les plus sophistiquées.

• Surveillance de la sécurité 24h/24 et 7j/7 :
o Aujourd'hui, Capgemini exploite cinq Centres Opérationnels de Sécurité (SOC, Security Operation Centers) mutualisés, qui sont les yeux et les oreilles permettant de détecter et de réagir aux cyberattaques. Ils sont situés en France, au Royaume-Uni, au Luxembourg et en Inde – où il y en a deux. Ces centres bénéficient de l'aide d'équipes de Recherche & Développement spécialisées en identification de vulnérabilités et en investigations numériques. Capgemini construit actuellement un sixième SOC en Belgique. Il conçoit et met également en place des SOC ad hoc pour ses clients.

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

Source : http://www.globalsecuritymag.fr/Le-groupe-Capgemini-lance-une,20150212,50774.html
Par Marc Jacob

En 2015, vous serez la première cible visée par la cybercriminalité

13

En 2015, vous serez la première cible visée par la cybercriminalité

ESET®, pionnier globale en protection proactive depuis plus de deux décennies, vient de publier un rapport très complet sur les principales tendances pour 2015 en cybercriminalité. Ce rapport est gratuit et peut être télécharger sur in the white paper section on WeLiveSecurity.com.

Alors que l'an dernier tout se concentrait autour de la protection de la vie privée sur Internet et le malware sur Android, de nouveaux secteurs de risques en sécurité informatique émergent en 2015. Le rapport gratuit Trends for 2015, est axé sur les cinq principaux domaines sur lesquelles les entreprises doivent se concentrer pour combattre les attaques. Il explique pourquoi les entreprises doivent être sur leurs gardes, commente l'évolution des menaces et leur donne des conseils pour protéger au mieux leurs actifs.
"Alors que les organisations améliorent continuellement leurs connexions digitales, de nouvelles pistes s'ouvrent aux cybercrime, " explique Marc Mutelet, CEO de MGK Technologies, distributeur exclusif des produits ESET sur la Belgique et le Luxembourg. L'astuce est de faire en sorte que vos défenses soient plus impénétrables que celles des entreprises qui vous entourent. En comprenant mieux le paysage des menaces vous êtes bien mieux préparé pour contrer les choses indésirables qui se cachent autour de vous. "

Le rapport est axé sur les principaux risques :
1. L'évolution of des APTs
2. Malware au point de vente
3. Fuite de l'information
4. Vulnérabilités
5. Internet des objets …. ou Internet des menaces?

"Nous pouvons tous imaginer combien il est frustrant pour les entreprises de devoir continuellement protéger leurs actifs contre les pirates et les criminels, c'est pour cela que nous avons voulu leur fournir de l'aide avec ce rapport, " commente Marc Mutelet. "Nous avons demandé à nos experts en sécurité de nous fournir une analyse détaillée de ce qu'ils pensent être des menaces émergeantes. Ce rapport est destiné à fournir des informations supplémentaires aux organisations, à les aider à revoir leurs technologies et processus de sécurité et à mettre en place les ressources nécessaires aux endroits stratégiques. "

Le rapport détaillé peut être téléchargé sur :
http://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf.

Vous êtes un chef d'entreprise, un élu, vous souhaitez sensibiliser votre personnel au risque informatique et le sensibiliser aux bonnes pratiques, n'hésitez pas à nous contacter.

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

Source :
http://www.informaticien.be/articles_item-17148-En_2015__les_entreprises_sont_la_premiere_cible_visee_par_la_cybercriminali.html

---

Le malware XOR.DDoS utilise la force brute pour contrôler les systèmes Linux

Le malware XOR.DDoS utilise la force brute pour contrôler les systèmes Linux

L'éditeur de sécurité FireEye a identifié deux autres versions du malware XOR.DDoS découvert en septembre 2014. Faisant partie d'une famille de logiciels malveillants particulièrement sophistiqués, il a la particularité de cibler différents systèmes Linux sous architectures x86 et ARM.

Les systèmes Linux sont toujours sous pression. Une dizaine de jours après l'alerte de Qualys portant sur la découverte de la faille « Ghost » relative à la librairie GNU C (http://www.lenetexpert.fr/une-faille-critique-permet-de-prendre-le-controle-des-routeurs-des-nas-des-systemes-linux), c'est au tour du spécialiste en sécurité FireEye de tirer la sonnette d'alarme. Cette fois au sujet d'un malware conçu pour cibler les systèmes Linux, incluant les terminaux à base d'architecture ARM et utilisant un noyau rootkit sophistiqué qui présente une grande menace.
Connu sous l'appellation XOR.DDoS et découvert une première fois en septembre par des chercheurs de Malware Must Die, ce cheval de Troie a depuis évolué et de nouvelles versions se sont retrouvées dans la nature depuis le 20 janvier selon un rapport publié vendredi par FireEye qui a analysé en détail cette menace.
XOR.DDOS est installé sur des systèmes cibles via des attaques SSH par force de brute lancées principalement depuis des adresses IP émanant d'une société hong-kongaise appelée Hee Thai Limited. Ces attaques essaient de deviner le mot de passe de démarrage en usant de différentes techniques basées sur des dictionnaires et des listes de mots de passe issues de précédentes violations de données. FireEye a observé plus de 20 000 tentatives de login SSH par serveur visé en 24 heures et plus d'1 million par serveur entre mi-novembre 2014 et fin janvier 2015.
Lorsque les attaquants tentent de deviner le mot de passe de démarrage, ils envoient une commande SSH complexe à distance pouvant parfois atteindre plus de 6 000 caractères, qui se compose de plusieurs commandes shell séparées. Ces commandes téléchargent et exécutent différents scripts dans le cadre d'une chaîne d'infection sophistiquée s'appuyant sur un système de construction de malware à la demande. L'utilisation de commandes SSH distantes est significative car OpenSSH ne liste pas de telles commandes « même lorsque la connexion est configurée dans la plus verbeuse de ses configurations », ont indiqué les chercheurs de FireEye. « Comme une commande distante ne créé par de terminal session, les systèmes de connexion TTY ne retiennent pas non plus ces événements, pas plus que les dernières commandes de logs ».
Cette infrastructure à la demande de construction sophistiquée d'automatisation de création de rootkits LKM s'appuie sur différents noyaux et architectures, sachant que les architectures de chaque Loadable Kernel Modules (LKM) doivent être compilées pour le noyau particulier sur lesquel il est prévu de tourner. « Contrairement à Windows qui dispose d'une API noyau stable permettant de créer du code qui est portable entre différentes versions de noyaux, le noyau Linux ne dispose pas d'une telle API », expliquent les chercheurs de FireEye. « Comme les changements internes de noyau changent d'une version à une autre, un LKM doit être binairement compatible avec le noyau ».

Chiffrer les serveurs SSH et désactiver le démarrage de comptes à distance

L'objectif de ce rootkit est de cacher des processus, des fichiers, et des ports associés avec XOR.DDoS. « Contrairement à des attaques DDoS typiques de robots, XOR.DDoS est l'une des familles de malware les plus sophistiquées ciblant les OS Linux », a précisé FireEye. « Il est également multi-plateformes avec du code source C/C++ pouvant être compilé pour cibler x86, ARM et d'autres plateformes ».
XOR.DDoS peut également télécharger et exécuter des fichiers binaires arbitraires lui donnant la capacité de se mettre tout seul à jour.
FireEye a identifié jusqu'à présent deux versions majeures de XOR.DDoS, le second ayant été repéré fin décembre. Le nombre de systèmes accessibles via SSH et utilisant des mots de passe faibles pouvant être vulnérables à des attaques par force brute complexe comme celles utilisées par les pirates derrière XOR.DDoS, pourrait être très élevé. Pour éviter d'être une cible trop facile, il faut absolument veiller à ce que les serveurs SSH soient configurés pour utiliser des clés de chiffrement au lieu de mots de passe pour l'authentification, et la connexion à distance pour démarrer des comptes devrait être désactivée, a précisé FireEye. « Particuliers et utilisateurs en PME peuvent installer l'utilitaire fail2ban qui fonctionne avec iptables pour détecter et bloquer les attaques par force brute ».

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

Source : http://www.lemondeinformatique.fr/actualites/lire-le-malware-xorddos-utilise-la-force-brute-pour-controler-les-systemes-linux-60175.html
Par Dominique Filippone avec IDG News Service

Paiement sans contact : votre carte bancaire risque-t-elle de se faire pirater

Paiement sans contact : votre carte bancaire risque-t-elle de se faire pirater ?

Près de la moitié des cartes bancaires sont désormais équipées de la technologie de paiement sans contact. Un développement à marche forcée qui alimente les craintes de fraude chez les consommateurs.

Une envolée… en toute discrétion. En un an, le nombre de cartes de paiement sans contact en circulation en France a bondi de 50%, pout atteindre 30,3 millions en octobre 2014, selon les derniers chiffres de l'Observatoire du NFC et du sans contact. Elles représentent désormais 47,4% de l'ensemble des cartes bancaires, contre 31% douze mois plus tôt.
Pour savoir si votre carte est dotée de cette technologie, c'est très simple : elle comporte alors un petit logo représentant des ondes se propageant. Si vous ne le saviez pas, rien d'étonnant : les banques ont en effet assez peu communiqué sur le sujet, équipant le plus souvent leurs clients lors d'un renouvellement de carte sans forcément les en informer.

La généralisation de ce nouvel outil de paiement est-elle pour autant synonyme de risque pour consommateurs ? Plusieurs experts en sécurité informatique ont déjà pointé du doigt les potentielles failles de ce système. « Les informations contenues sur cette carte ne sont pas cryptées et peuvent être récupérées très facilement grâce à un smartphone », prévient Thomas Livet, de la société Sifaris.
Nous l'avons testé, le procédé est en effet d'une simplicité enfantine : il suffit de télécharger l'une des multiples applications dédiées disponibles sur la plate-forme d'Android avec un smartphone compatible avec la technologie « NFC », puis de diriger ce téléphone vers une carte bancaire pour obtenir en quelques secondes les 16 numéros inscrits au recto, la date d'expiration et le nom de la banque (voir la capture plus bas). Inquiétant.
Reste que certaines données essentielles ne peuvent pas être aspirées : en particulier le cryptogramme, c'est-à-dire les 3 chiffres inscrits au dos de la carte faisant office de code de sécurité lors d'un paiement en ligne, ainsi que le nom de l'utilisateur. Ce qui complique de fait la tâche des escrocs, puisque la plupart des grands sites de e-commerce français et étrangers demandent ces informations pour valider un paiement. « Evidemment on pourrait concevoir un logiciel pour générer les 999 combinaisons possibles de cryptogramme, mais cela paraît bien compliqué pour ce genre de petites escroqueries », relativise Maxime Chipoy, de l'association de défense des consommateurs, UFC Que Choisir.

Même si la possibilité de se faire escroquer par ce biais n'est pas nulle, le risque de fraude paraît donc limité. Aucune arnaque liée au système de paiement sans contact n'est d'ailleurs pour le moment remontée aux oreilles de l'UFC. Même son de cloche chez CLCV : « Nous avons eu des plaintes relatives au paiement sans contact, mais uniquement concernant le manque de communication des banques sur le sujet, et non en raison d'escroqueries », explique Olivier Gayraud, de l'association.
Certes, la technologie sans contact facilite aussi la tâche des fraudeurs qui arrivent à subtiliser une de ces cartes : ils peuvent en effet l'utiliser sans avoir à taper le code pin, dans n'importe quel magasin équipé de la technologie sans contact. Mais le montant de chaque transaction est limité à 20 euros, et vous devez retaper le code pin une fois dépassé un certain plafond, défini généralement entre 80 et 100 euros selon les banques.
Si vous craignez tout de même de vous faire hacker votre carte, vous avez le droit de demander à votre banque la désactivation de la fonctionnalité de paiement sans contact, voire une nouvelle carte bancaire non équipée de cette technologie. Même si les établissements sont parfois réticents à le faire, n'hésitez pas à insister : « Si votre conseiller s'y oppose, exigez un refus par écrit. Cela devrait suffire à débloquer la situation », conseille Olivier Gayraud. Certaines banques peuvent aussi fournir gratuitement des étuis de protection, faisant office de « cage de Faraday », permettant d'isoler complètement la carte bancaire des ondes extérieures. Il est aussi possible d'acheter ces étuis dans le commerce pour quelques euros, voire des portefeuilles « anti-NFC » moyennant entre 10 et 30 euros.

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

Source : http://www.capital.fr/finances-perso/actualites/paiement-sans-contact-votre-carte-bancaire-risque-t-elle-de-se-faire-pirater-1010288
Par Thomas Le Bars

Plusieurs entreprises visées par des hackers

Plusieurs entreprises visées par des hackers

La prudence doit être de mise lorsque vous ouvrez vos e-mails. Une dizaine de cas de «ransomware», une arnaque informatique qui tente de soutirer une rançon aux victimes, ont été recensés cette semaine par le CIRCL, le Computer Incident Response Center Luxembourg. Ce type d'attaque est «techniquement très avancé depuis quelques semaines», a indiqué le CIRCL.

Ces piratages prennent la forme d'un e-mail dans lequel un lien ou une pièce jointe contient un logiciel malveillant qui prend en otage les données personnelles contenues sur l'ordinateur. Une fois les fichiers bloqués, les hackers invitent les victimes à payer de 500 à 1 000 euros pour, soi-disant, résoudre le problème.

Restaurer ses fichiers
Parmi les cas recensés ces derniers jours au Luxembourg, ce sont principalement des entreprises qui ont été touchées. Un ordinateur infecté peut alors bloquer les fichiers de tous les ordinateurs connectés au réseau de l'entreprise. Les données sont ensuite quasiment impossibles à récupérer vu la complexité du code utilisé actuellement par les hackers.
Le CIRCL suggère à toutes les entreprises de bien vérifier leur back-up. «Souvent les entreprises sauvegardent leurs fichiers mais ne vérifient pas que leur back-up est bien fait», explique-t-on au CIRCL. Il faut donc vérifier que les fichiers sauvegardés peuvent bien être restaurés et qu'ils disposent d'une période de conservation adéquate. Du côté des particuliers, sauvegarder ses données personnelles sur un disque dur externe est un bon réflexe. «Mais il ne faut pas laisser le disque dur branché à l'ordinateur», insiste-t-on encore au CIRCL, faute de quoi les fichiers contenus sur le disque dur externe seront aussi accessibles aux hackers

Comment reconnaître un «ransomware»?
Ce type d'attaque informatique circule via les liens ou les pièces jointes d'un e-mail. Souvent, il s'agit de courriers électroniques demandant de payer une facture. L'adresse du destinataire ne paraît à première vue pas suspecte.

Comment les éviter?
Pour éviter de se faire hacker, il faut donc garder en tête les précautions de base. Par exemple, ne pas cliquer sur un lien ou ouvrir un fichier .pdf, .zip ou .doc de la «Deutsche Telekom» si vous n'avez pas de facture à recevoir de cet opérateur. De même avec un e-mail pour un colis que vous n'attendez par, par exemple.
Le CIRCL recommande aussi de mettre à jour vos logiciels, y compris les plug-ins des navigateurs (comme Flash, Java, Silverlight, etc.) et de vous assurer que votre anti-virus est bien à jour.

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

Source : http://www.lessentiel.lu/fr/news/story/15460014