Université Lyon 3 : 88.000 contacts ont été dérobés par les pirates informatiques

Université Lyon 3 : 88.000 contacts ont été dérobés par les pirates informatiques

Les services de l'université Lyon 3 avait d'abord parlé d'une fuite d'environ 5000 contacts pour la plupart étudiants, cependant depuis une plus récente information du site lepoint.fr, l'université aurait reconnu avoir fait fuité par erreur, 88 000 contacts. Un cas plus grave que le premier dont on vous avez fait écho au début du mois de février. Pour rappel, les fichiers dérobés contenaient les noms, prénoms, date de naissance, informations sur le cursus suivis, adresses personnelles postale et électronique, numéros d'étudiants fixe et mobile, mais aussi des conversations échangées par e-mail entre les étudiants et le personnel de l'université ou encore les coordonnées d'entreprises partenaires de l'université.

Des mesures contre les cyberattaques prises en décembre
Contactée par lepoint, l'université « a regretté un cafouillage de communication », avant qu'Yves Condemine, le directeur des systèmes d'informations (DSI), explique que « la base de données piratées concerne 88 000 contacts ». Bien qu'aujourd'hui « les problèmes sont réglés », il affirme néanmoins que « des mesures avaient été prises dès décembre », après des alertes envoyées par un des étudiants de l'université. Le directeur des services d'informations reste cependant « encore prudent » dans la surveillance du réseau même si « rien ne permet aujourd'hui de penser que (l')infrastructure soit compromise », affirme t-il.

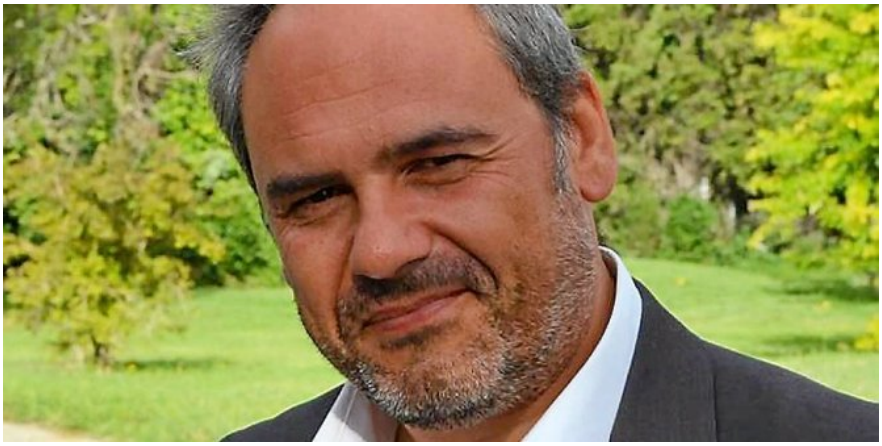
L'agence de cyberdéfense n'analysera pas le réseau de l'université
Cependant, l'université n'a pas souhaité l'intervention de l'agence de cyberdéfense. Malgré l'urgence de la situation et la charge de travail nécessaire pour analyser la totalité du réseau, l'université a souhaité s'occuper seule de cette tâche. L'incident à néanmoins était signalé à son ministère de tutelle qui a contacté l'Anssi, l'agence nationale de cyberdéfense, sans pour autant la saisir. « Nous sommes restés en contact avec l'Anssi, via le ministère de l'Enseignement supérieur », affirme Yves Condemine à lepoint. Pas très rassurant si l'agence de cyberdéfense ne peut ni analyser, ni trouver d'éventuelles portes dérobées dans le réseau, ni même remonter jusqu'aux pirates pour comprendre leurs intentions en piratant la base de données d'une université.

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

Source : http://www.digischool.fr/a-la-une/universite-lyon-3-contacts-derobes-pirates-informatiques-26701.php

---

Cyber-attaques : Denis Jacopini, expert, alerte – Article dans Midi Libre Gard…



Cyber-attaques : Denis Jacopini, expert, alerte – Article dans Midi Libre Gard…

Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.Après les attentats du 7 janvier, de nombreux sites internet d'institutions locales ou religieuses en France ont été piratés par des groupes de hackers se présentant comme des islamistes, dont celui du palais des Papes à Avignon, victime d'un défaçage (remplacement de la page d'accueil du site) par un groupe dénommé Fallaga team . Ces phénomènes de piratage ne sont pas nouveaux et s'accentuent. Ils sont imputables à différents types de malfaiteurs et se matérialisent de manière très différente. Décryptage des cyber-attaques avec Denis Jacopini, expert judiciaire près la cour d'appel de Nîmes et des juridictions du Gard, du Vaucluse, de l'Ardèche et de la Drôme. Denis Jacopini : « Les chefs d'entreprise ne sont pas assez sensibilisés. » DR Qu'est-ce qu'une cyber-attaque ? C'est une attaque informatique utilisant les réseaux de télécommunication et cela existe depuis qu'Internet s'est répandu dans le…


Bagnols

Midi Libre | midilibre.fr
MERCREDI 11 FÉVRIER 2015

3

Cyber-attaques : « Les sociétés ne se protègent pas »

Entretien | Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.

Contexte

GROS PLAN

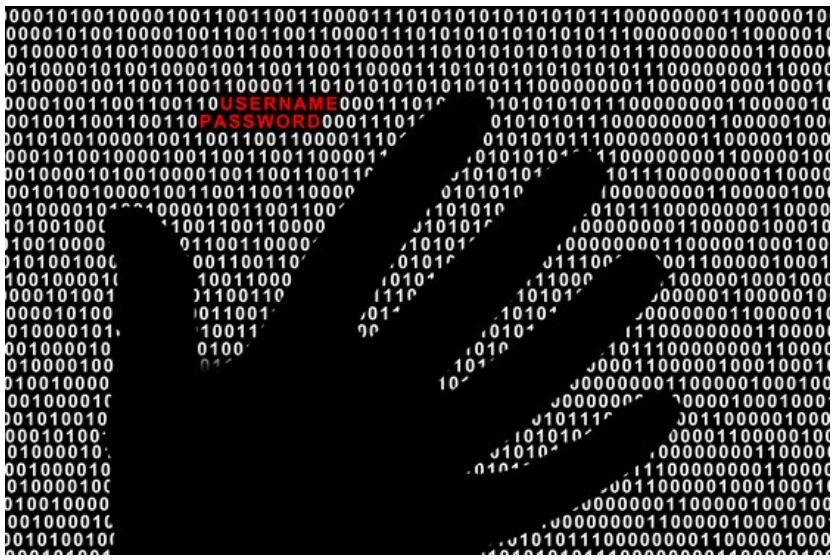
La e-reputation

Gard : 20 faits de piratage de sites en 2014 et cinq en 2015

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

Source : http://www.midilibre.fr/2015/02/11/cyber-attaques-les-societes-ne-se-protegent-pas,1123222.php

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…



Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Des pirates se sont infiltrés dans les systèmes d'information d'une centaine de banques en 2013, ont dérobé au moins 300 millions de dollars, et agissent encore aujourd'hui, apprend Kaspersky.

C'est l'une des cyberattaques les plus sophistiquées jamais identifiées par Kaspersky. L'éditeur de solutions antivirus russe a dévoilé auprès du New York Times, lundi, les résultats d'une enquête menée depuis 2013 en partenariat avec Interpol et Europol. Conclusions : de 300 millions à 1 milliard de dollars ont été dérobés à une centaine de banques dans trente pays. Active depuis près de deux ans, la cyberattaque a toujours cours.

Pour ces raisons, l'éditeur reste volontairement imprécis sur les informations divulguées, ne fournissant pas, par exemple, le nom des établissements concernés. Les institutions sont basées principalement en Russie, au Japon, aux Etats-Unis et en Suisse. D'après le quotidien américain, JP Morgan Chase figure parmi les cibles.
Ce cybergang basé en Russie, Chine et Ukraine, « a franchi un nouveau cap » dans la méthode employée, souligne Kaspersky, en dérobant des fonds aux banques sans avoir à passer par les clients. L'attaque aurait débuté avec des infections classiques par hameçonnage, quand des employés de banque téléchargeaient malgré eux sur leur poste le malware nommé « Carbanak » – c'est également le nom de ce groupe de pirates.

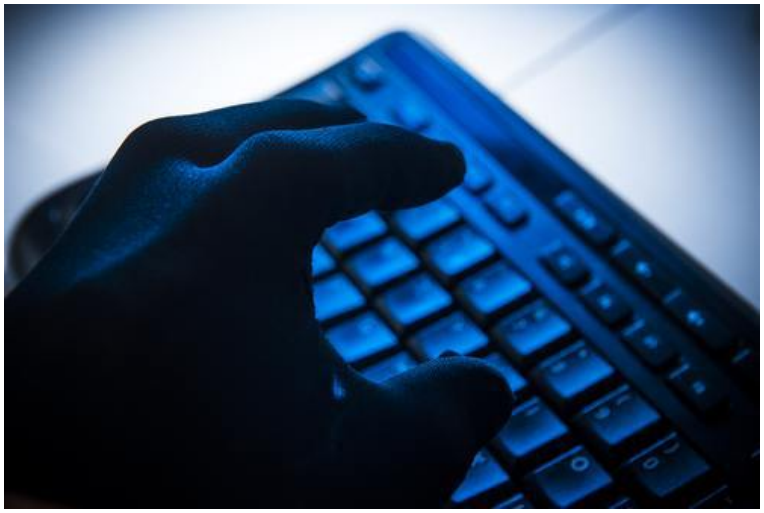
Observer et imiter les transferts d'argent
Une fois bien installés sur les ordinateurs chargés des transferts de fonds ou de la compatibilité, il peuvent observer discrètement et patiemment les routines des employés et les processus des banques. Les pirates remontent ensuite sur les machines des responsables des transferts et des comptes, où ils installent un outil d'administration à distance (RAT) afin d'en prendre le contrôle et « d'imiter les activités normales ».
Ainsi, les assaillants peuvent créer de faux comptes pour y transférer de l'argent, a priori sans éveiller de soupçons. Si le hameçonnage n'a rien d'exceptionnel en soi, c'est l'aspect méthodique et la patience des pirates que Kaspersky pointe du doigt dans son rapport. De quoi leur avoir évité de s'être fait pincer à ce jour.
Ce qui a déclenché l'enquête remonte à la fin 2013 lorsqu'un distributeur s'est mis à émettre des billets en plein Kiev, en Ukraine. Alertée, la banque concernée a alors missionné Kaspersky. Lequel découvrira assez tôt que cette avarie allait en fait devenir, comparé à l'ampleur de la cyberattaque, le dernier souci de la banque.

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

S o u r c e
http://pro.clubic.com/it-business/securite-et-donnees/actualite-754433-kaspersky-cyber-attaque-banques.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_17/02/2015&partner=-&svc_position=86524329&svc_misc=-&crmID=639453874_86524329&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-754433-kaspersky-cyber-attaque-banques.html

---

Cybercrime : la fraude à un milliard de dollars



Cybercrime : la fraude à un milliard de dollars

La fraude est inédite par son ampleur : une centaine d'établissements financiers et de banques ont été victimes d'une cyberattaque encore jamais vue.(c) Shutterstock/EconomieMatin

La société de sécurité informatique Kaspersky Labs a mis au jour le pot aux roses, qui touche une trentaine de pays parmi lesquels la Russie, les États-Unis, l'Allemagne, la Chine, l'Ukraine ou encore le Canada. En tout et pour tout, c'est un milliard de dollars qui s'est évaporée des comptes de ces banques !

Interpol, sur le coup, reçoit l'aide des fins limiers de Kaspersky pour débusquer les pirates qui ont mis la main sur ce pactole. Il s'agirait, d'après les premiers renseignements, d'un groupe de hackers provenant de l'est de l'Europe (Russie et Ukraine), ainsi que de Chine.

Les méthodes employés, rapporte Interpol, marquent un tournant pour ce type d'infraction. Le processus mis en œuvre par les pirates relèvent d'une grande sophistication, qui leur permet de subtiliser l'argent « directement dans les banques », mais « sans avoir à viser ceux qui, au final, vont utiliser cet argent ».

Des méthodes redoutables donc, et transparentes, qui exploitent de nouvelles failles de sécurité et autres brèches dans les systèmes utilisés par les établissements bancaires. Et l'attaque se poursuit à l'heure actuelle.

Lire la suite….

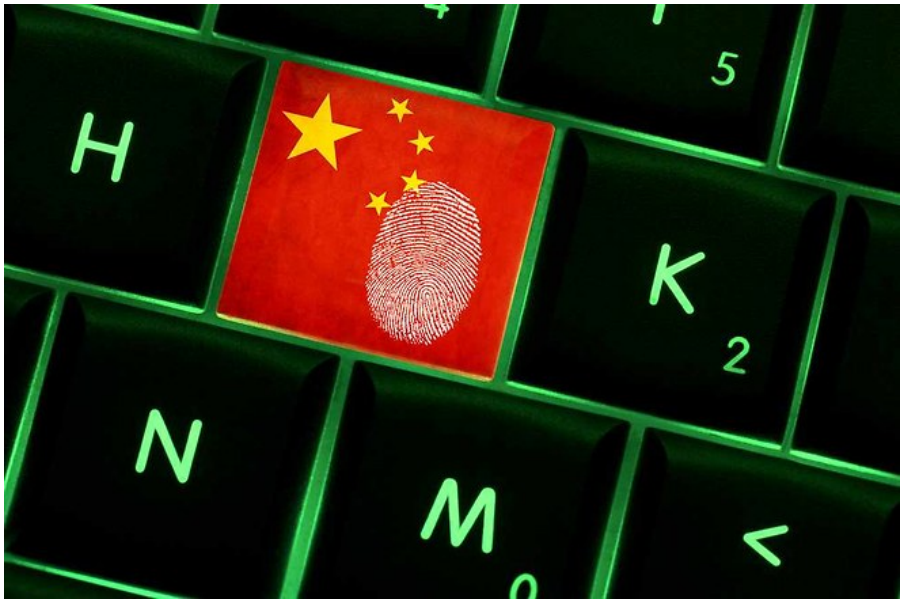
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.journaldeleconomie.fr/Cybercrime-la-fraude-a-un-milliard-de-dollars_a1994.html

---

Forbes victime d'une vaste

cyber-attaque chinoise



Forbes victime d'une vaste cyber-attaque chinoise

Les pirates traquaient tout spécialement des experts en défense et des sociétés financières grâce à la technique de hacking dite de « point d'eau ».

Un groupe de pirates informatiques basés en Chine a piégé fin 2014 le site internet du magazine américain Forbes, profitant notamment de failles d'un navigateur populaire pour transmettre des virus aux visiteurs, ont indiqué mardi des experts en cyber-sécurité. Selon les sociétés Invincea et iSight Partners, les pirates traquaient tout spécialement des experts en défense et des sociétés financières grâce à la technique de hacking dite de « point d'eau ».
Cette technique consiste généralement à infiltrer un site internet populaire, puis à le piéger avec des virus qui vont ensuite infecter les visiteurs. Lors de cette campagne de piratage menée en fin d'année dernière, Forbes et d'autres sites ont été visés, ont indiqué les experts. « Une menace chinoise avancée a compromis Forbes.com pour mettre en place une attaque de style +point d'eau+ visant la défense américaine et des sociétés de services financiers fin novembre 2014 », a expliqué Invincea dans un rapport publié sur son site, qualifiant cette attaque d' »éhontée ».

Vaste portée
Les pirates ont notamment exploité les failles du navigateur Internet explorer et du programme Adobe Flash, qui ont depuis été réparées, a précisé la société. Cette campagne de cyber-espionnage n'aurait duré que quelques jours. De son côté, la société ISight a avancé que le groupe de pirates chinois Codoso, aussi appelé Sunshop, était à l'origine de cette attaque informatique concoctée pour cibler certains profils parmi les milliers de visiteurs du site.
Il aurait déjà à son actif des campagnes contre la défense américaine, des centres de réflexion, des services financiers, des entreprises énergétiques et des dissidents politiques, ont ajouté ces experts. Forbes.com est classé 61e site internet le plus populaire aux Etats-Unis et 168e mondial ; par conséquent la portée de la campagne de piratage pourrait être très vaste, estiment les experts.

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

Source : http://www.lesechos.fr/tech-medias/hightech/0204150910405-forbes-victime-dune-vaste-cyber-attaque-chinoise-1092213.php par AFP

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 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 ».

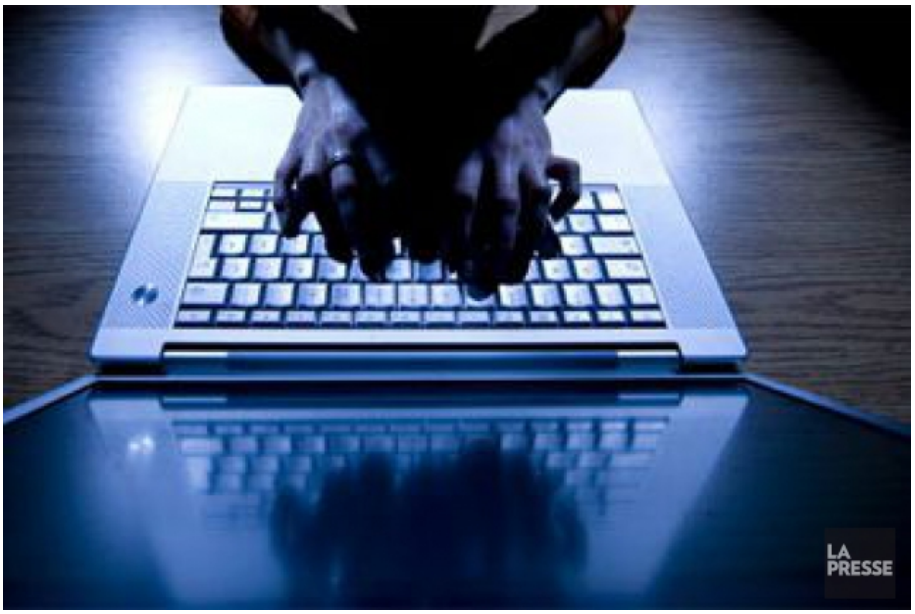
Chiffrer les serveurs SSH et désactiver le démarrage de comptes à distance
L'objectif de ce rootkit est de cacher des processus, des fichiers, et des ports associés avec XOR.DDoS. « Contrairement à des attaques DDoS typiques de robots, XOR.DDoS est l'une des familles de malware les plus sophistiquées 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

Attaque informatique à la Ville de Montréal | Pierre-

André Normandin | Matériel informatique

	**Attaque informatique à la Ville de Montréal**

Une attaque informatique a frappé la Ville de Montréal, hier après-midi. Près d'une vingtaine de postes de travail ont été infectés par un nouveau logiciel malveillant reçu par courriel.

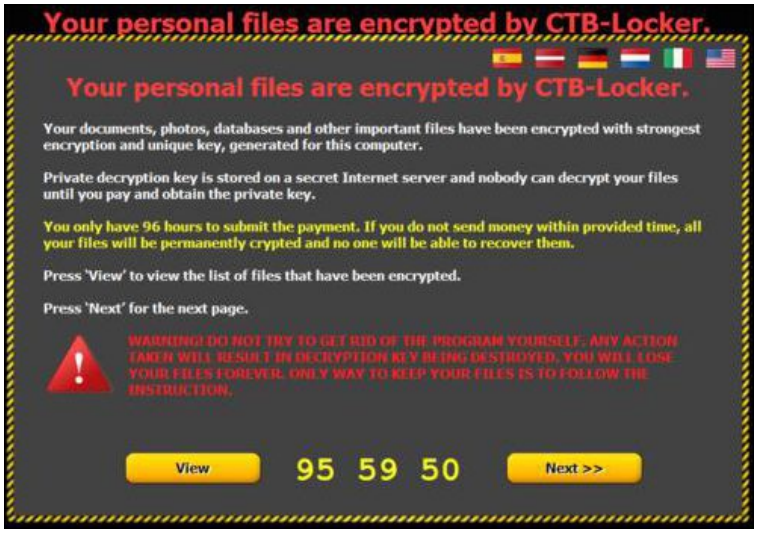
« Au cours des dernières heures, plusieurs postes de travail ont été infectés par un logiciel malveillant », prévenait hier un message envoyé aux 28 000 employés de Montréal. L'avis précisait que le virus crypte les données du poste de travail infecté et des répertoires réseau connectés au poste. Du coup, les employés perdent l'accès à tous leurs fichiers informatiques.
L'ampleur des dommages causés par l'attaque n'est pas claire. Il n'a pas été possible de savoir si des données ont été volées. Le message de la Ville précisait simplement que le service des technologies s'affairait à récupérer les informations perdues et à enrayer la propagation du logiciel malveillant.
Le virus a touché « moins de 20 postes de travail répartis dans 4 édifices », a indiqué un porte-parole de la Ville, Gonzalo Nunez. Plusieurs d'entre eux se trouvaient à l'hôtel de ville, selon une source.
Les employés dont le poste de travail a été infecté ont reçu un courriel qui leur indiquait qu'ils avaient reçu une télécopie. Le fichier, identifié à leur nom afin de déjouer leur vigilance et portant une extension.zip, contenait toutefois un nouveau logiciel malveillant de type « cryptolocker ». Celui-ci bloque l'accès aux fichiers informatiques de l'ordinateur.
Les logiciels antivirus des ordinateurs infectés étaient à jour, assure la Ville, mais ils n'ont pu bloquer ce nouveau logiciel malveillant. Le fournisseur de la Ville, Symantec, a transmis en après-midi une mise à jour pour contrer le virus.
« Le service des technologies de l'information est en contrôle de la situation. », a affirmé M. Nunez.
Les informaticiens de la Ville ont invité leurs collègues à la prudence. « Pour éviter toute perte de données et préserver l'intégrité de nos infrastructures, nous vous demandons de ne pas cliquer sur les fichiers portant une extension.zip que vous recevez par courriel, peu importe que le courriel provienne de l'interne ou de l'externe. »
Il ne s'agit donc pas du même type d'attaque que celle qui avait ciblé la municipalité de Terrasse-Vaudreuil en janvier, quand son site internet avait été piraté par des sympathisants du groupe État islamique. Le service des technologies de l'information de Montréal croit d'ailleurs que la Ville de Montréal n'était pas délibérément ciblée. « Ce virus semble n'avoir aucun rapport avec la moindre organisation qui fait les manchettes actuellement », a indiqué M. Nunez.

Attaques fréquentes
Les attaques par des logiciels malveillants sont fréquentes, dit Jean-Philippe Nantel, agent de recherche senior au Centre de recherche informatique de Montréal (CRIM). « Ce type d'attaque profite d'une faille d'un programme utilisé par la Ville », résume-t-il.
Le vol de données est possible avec ce type de virus, mais il est principalement utilisé dans des tentatives d'hameçonnage, ajoute M. Nantel. Généralement, après avoir crypté les données d'un ordinateur, un pirate prend contact avec le propriétaire en demandant de l'argent pour déverrouiller les données. Une source a confirmé à La Presse que ce type de message a été reçu.
« Les organisations comme Montréal ont beaucoup de moyens pour contourner ces logiciels malveillants. En théorie, elles sont protégées. Les employés ne perdront pas des années de travail. Ils vont peut-être perdre la journée ou au pire la semaine. C'est plus un désagrément que du vol de données », dit M. Nantel.

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

Source : http://techno.lapresse.ca/nouvelles/materiel-informatique/201502/05/01-4841461-attaque-informatique-a-la-ville-de-montreal.php
Par Pierre-André NORMANDIN

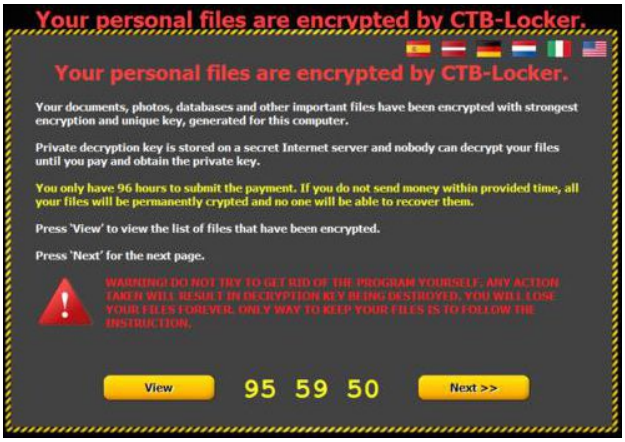
Plusieurs entreprises visées par des hackers



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

Piratage d’un gros assureur-santé visant les données d’un quart des Américains

Piratage d’un gros assureur-santé visant les données d’un quart des Américains

L’un des plus gros assureurs-santé américain, Anthem, a été victime d’une attaque informatique qui visait une base de données relatives à un quart des Américains, selon le groupe.« Des cyber-pirates ont réalisé une attaque très sophistiquée pour obtenir un accès non autorisé à l’un des systèmes informatiques d’Anthem, et ont obtenu des informations personnelles sur des clients et des salariés d’Anthem », a indiqué l’assureur dans un communiqué mercredi soir.
« La base de données affectée contient des informations d’environ 80 millions de personnes et des dizaines de millions » d’entre elles ont pu être volées, a précisé une porte-parole, Cindy Wakefield, confirmant une information du Wall Street Journal.

Aucune carte de crédit affectée
Les données compromises incluent des noms, dates de naissance, numéros de sécurité sociale (qui sont un élément important d’identification aux Etats-Unis), adresses physiques ou électroniques, ainsi que des informations liées à l’emploi des personnes, y compris sur leurs revenus.
Anthem affirme en revanche qu’aucune donnée de carte de crédit n’est affectée, et dit ne pas avoir de preuve à cette date que les pirates aient accédé à des informations médicales.
Selon les experts en cyber-sécurité, les données médicales peuvent être plus lucratives pour les pirates que les cartes de crédit, parce qu’elles permettent de créer de fausses identités pour se faire prescrire des médicaments qui seront ensuite revendus, ou bien de remplir de fausses déclarations d’assurance santé.

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

Source : http://www.20minutes.fr/monde/1534579-20150205-piratage-gros-assureur-sante-visant-donnees-quart-americains