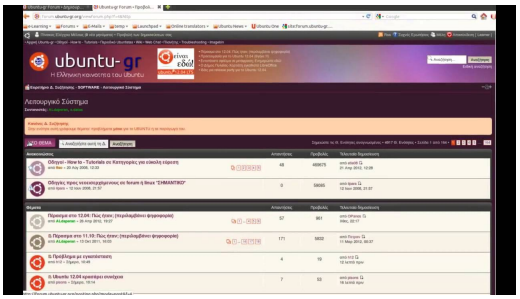
Deux millions de données d’utilisateurs Ubuntu dérobées



Deux millions de données d’utilisateurs Ubuntu dérobées

Le forum de la distribution Ubuntu a été victime d'une grave attaque informatique. Deux millions d'utilisateurs se sont fait voler leurs données.

Le butin du pirate est plus qu'impressionnant. Noms, mots de passe, adresse mails et IP, les données de deux millions d'utilisateurs du forum d'Ubuntu se sont envolées. La nouvelle a été annoncée jeudi dans un communiqué par Canonical l'éditeur d'Ubuntu. *« A 20h33 UTC le 14 Juillet 2016, Canonical et l'équipe ont été informés par un membre du Conseil Ubuntu que quelqu'un prétendait avoir une copie de la base de données des forums. Après enquête initiale, nous avons été en mesure de confirmer qu'il y avait bien eu une exposition des données et nous avons fermé les forums par mesure de précaution. »*

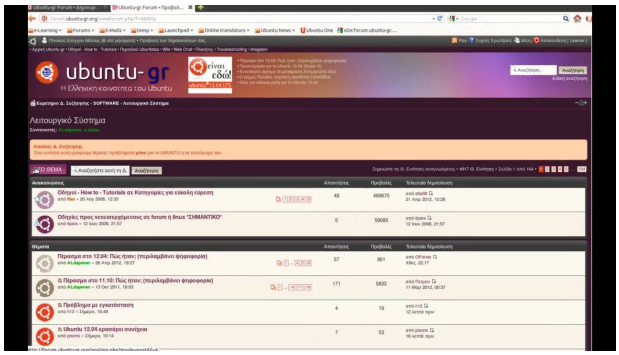
Une attaque par injection SQL

Une enquête plus poussée a révélé que la méthode employée est une injection SQL. Le pirate a pu injecter des requêtes SQL formatées dans la base de données des forums pour ensuite télécharger les datas.

Cependant, le communiqué précise que le hacker n'a pas pu accéder aux mots de passe utilisateur valides ni au référentiel de code Ubuntu ou au mécanisme de mise à jour. Moins certain, le rapport précise que normalement les services Canonical ou Ubuntu en sortent indemnes, comme certains forums.

Tout est plus ou moins rentré dans l'ordre

Des mesures correctives ont été prises et les forums restaurés. Les mots de passe du système et de la base de données ont été réinitialisés et ModSecurity, une Web Application Firewall vient renforcer le dispositif de sécurité. Selon Canonical, ça va mieux, même si après ce genre de vol il est légitime de penser que le mal est fait.



Article original de Victor Miget

Réagissez à cet article

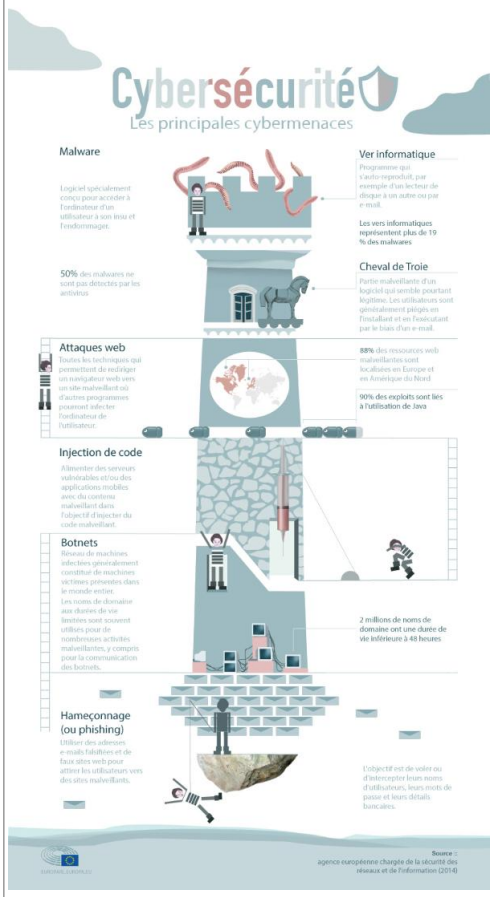
Original de l'article mis en page : Ubuntu : les données de

deux millions d’utilisateurs dérobées

Directive sur la sécurité des réseaux et des systèmes d’information

Directive sur la sécurité des réseaux et des systèmes d’information

Nos sociétés digitalisées reposent de plus en plus sur des réseaux électroniques qui peuvent faire l'objet de cyberattaques aux conséquences importantes. Afin de mieux faire face à ce type de menaces en ligne, le Parlement et le Conseil ont conclu en décembre dernier un accord sur les premières règles européennes en matière de cybersécurité. Celles-ci ont été soutenues par l'ensemble du Parlement réuni en session plénière ce mercredi 6 juillet.



Vols d'identité, faux sites web de banques, espionnage industriel ou inondation de données qui rendent un serveur incapable de répondre : les menaces en ligne sont nombreuses et visent tant les particuliers que les entreprises et les autorités publiques.
Les incidents et les attaques des systèmes d'information des entreprises et des citoyens pourraient représenter un coût de 260 à 340 milliards d'euros par an, selon les estimations de l'Agence européenne chargée de la sécurité des réseaux et de l'information.
Les cyberattaques menées contre certaines infrastructures clés de nos sociétés, comme les services bancaires, les réseaux d'électricité ou le secteur du contrôle aérien, peuvent avoir des conséquences particulièrement importantes sur notre quotidien.
Dans le cadre d'un Eurobaromètre publié en février 2015, les citoyens européens ont exprimé de fortes inquiétudes à propos de la cybersécurité : 89 % des internautes évitent de diffuser des informations personnelles en ligne. Selon 85 % des sondés, le risque d'être victime de cybercriminalité est de plus en plus important.

Vote en plénière
Les députés ont approuvé la directive sur la sécurité des réseaux et de l'information dans l'Union, qui définit une approche commune autour de la question de la cybersécurité.
Le texte prévoit une liste de secteurs dans lesquels les entreprises qui fournissent des services essentiels, liés par exemple à l'énergie, aux transports ou au secteur de la banque, devront être en mesure de résister aux cyberattaques.
La directive les oblige notamment à signaler les incidents de sécurité graves aux autorités nationales. Les fournisseurs de services numériques tels qu'Amazon ou Google devront également notifier les attaques majeures aux autorités nationales.
Ces nouvelles règles sur la cybersécurité visent également à renforcer la coopération entre États membres en cas d'incidents.

Téléchargez la directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil :
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Article original du Parlement Européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité : mieux faire face aux attaques en ligne

---

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.

Combien y a-t-il d'attaques par rançongiciel en France ?
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
Avez-vous quand même une idée de l'évolution du phénomène ?
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
Les victimes ont-elles le réflexe de porter plainte ?
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
Qu'est-ce qui pousse à porter plainte ?
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
Qui sont les victimes ?
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
Quel est votre rôle dans la lutte contre les rançongiciels ?
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
Quel rapport entretenez-vous avec les entreprises ?
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
Parvenez-vous, dans vos enquêtes, à identifier les responsables ?
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
Parvenez-vous à collaborer avec vos homologues à l'étranger ?
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

---

Sans utiliser la moindre carte de crédit, deux hommes ont volé 1,7 millions d'euros à la First Commercial Bank de Taïwan.

Les « casses du siècles » deviennent de plus en plus cocasses et subtiles à l'ère du tout numérique. Chaque mois ou presque, on peut trouver un exemple de vol de banque, qui mêle développement logiciel et matériel. Cette fois le crime n'implique pas le vol ou la copie de cartes de crédit : à Taïwan, deux pirates ont réussi à retirer l'argent de 30 distributeurs sans se faire prendre. La somme volée s'élève à 70 millions de dollars taïwanais.
Leur méthode était particulièrement rodée. En moins de 10 minutes, les voleurs ont exécuté un programme dans le système du distributeur de billet qui, bien gentiment, a offert ses devises sans demander de compte. Le logiciel a ensuite pris soin d'effacer toute trace du larcin. Et les voleurs sont repartis, à 30 reprises, avec le gros lot. Les enquêteurs ne savent toujours pas comment les pirates ont fait pour déployer leur code aussi rapidement sur les distributeurs, ni quel moyen a été utilisé pour se connecter aux machines – un smartphone est évoqué.

LES VOLEURS SONT REPARTIS, À 30 REPRISES, AVEC LE GROS LOT
Les deux hommes seraient des étrangers : l'un d'eux a été identifié comme étant un citoyen russe qui s'est enfui de l'île dimanche et est recherché par Interpol. L'identité et la nationalité de l'autre homme ne sont pas connues. En attendant les experts de la compagnie allemande qui fournit les distributeurs à la banque taïwanaise qui a été prise pour cible, la décision de bloquer tous les distributeurs du même fournisseur a été prise par les autorités. 400 distributeurs de billet ont donc été rendus inactifs.
Article original de Julien Cadot

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet – Tech – Numerama

---

Huit bonnes pratiques pour bien sécuriser les objets connectés

Huit bonnes pratiques pour bien sécuriser les objets connectés

---

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Le point.

Gartner prédit 26 milliards d'objets connectés d'ici 2020. En 2016 ce sont 4,9 milliards de dispositifs connectés qui devraient être déployés. Des objets qui seront potentiellement confrontés à un grand nombre d'attaques. En effet, le volume des cyber-attaques recensé par l'étude The Global State of Information Security® Survey 2016, réalisée par le cabinet d'audit et de conseil PwC en collaboration avec CIO et CSO, a progressé de 38 % dans le monde en 2015. Comment alors sécuriser au mieux ses objets connectés ?

En appliquant quelques bonnes pratiques.

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Plusieurs zones « sensibles » sont donc à surveiller au sein des objets connectés notamment au niveau du capteur et au niveau du transfert des données.

Pour le capteur, l'un des moyens les plus efficaces pour se protéger consiste à sécuriser le hardware grâce à un Secure Element, qui empêche tout accès à l'information lorsqu'on se connecte au capteur. Un élément sécurisé repose sur une plate-forme matérielle inviolable qui héberge des données, cryptées ou non, en toute sécurité et en conformité avec les règles de sécurité fixées par les autorités de confiance. Certains de ces éléments, comme les cartes microSD, peuvent même être amovibles.

Pour sécuriser les données, il est indispensable d'utiliser des technologies de chiffrement robustes afin de lutter contre le piratage ou les interceptions. En effet, le chiffrement rend les données impossibles à lire pour qui ne possède pas la clé de déchiffrement de 128 bits ! Efficace pour repousser les hackers même les plus coriaces.

Une fois le capteur protégé et les données chiffrées, il est important d'assurer la sécurité de l'information lors de son transfert de bout en bout : du capteur jusqu'au portail client.

L'utilisation d'un système de clés multiples géré par un tiers de confiance tel que le propose le protocole LoRa s'avère une solution des plus fiables.

Un tiers de confiance fournit un système de gestion de clé – Key Management System (KMS) – qui permet de générer une AppKey unique pour chaque capteur. A chaque nouvelle session, une AppSKey – Application Session Key – dérivée de l'AppKey sert au chiffrement des données du client. L'opérateur n'a pas accès à ces 2 clés, elles ne sont connues que du tiers de confiance dans le KMS et du client bien sûr pour déchiffrer les données.

Une fois les données récupérées, l'utilisation d'un VPN est bien sûr conseillé.

En agissant à ces différents niveaux, vous appliquez une sécurité optimale à vos objets connectés. De plus, vous pouvez appliquer quelques conseils pour assurer une sécurité de bout en bout des processus :

1. Évaluez le bon degré de sécurité sur le capteur en fonction de la criticité de la donnée : selon l'information concernée, il n'est pas forcément nécessaire d'insérer un Secure Element dans le capteur.
2. Utilisez une technologie avec un protocole de chiffrement robuste de type AES128 par exemple.
3. Mettez en place des infrastructures intégrant l'état de l'art en termes de chiffrement.
4. N'écrivez pas vos clés de cryptage sur disque dur : privilégiez les éléments de sécurité non stockés et volatiles. Calculées « à la demande » par un algorithme, elles ne peuvent donc pas être piratées en cas d'attaque sur la base de données.
5. Optez pour un renouvellement de la clé de chiffrement à chaque connexion du capteur sur le réseau. Une clé renouvelée régulièrement à moins de risque d'être piratée.
6. Utilisez un portail sécurisé pour accéder à vos données applicatives chiffrées : vous avez ainsi, seul, la possibilité de déchiffrer les données. Toutefois, si vous choisissez de ne pas les déchiffrer vous-même, assurez-vous que votre prestataire le fasse sur un cloud sécurisé.
7. Choisissez des technologies en perpétuelle évolution : au sein de la LoRa Alliance, un groupe dédié fait évoluer en permanence le protocole afin d'être toujours à la pointe de la sécurité.
8. Optez pour un opérateur qui intègre les processus de sécurité recommandés par l'ANSSI dans la conception et l'exploitation de son réseau.

Article original de Franck Moine

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

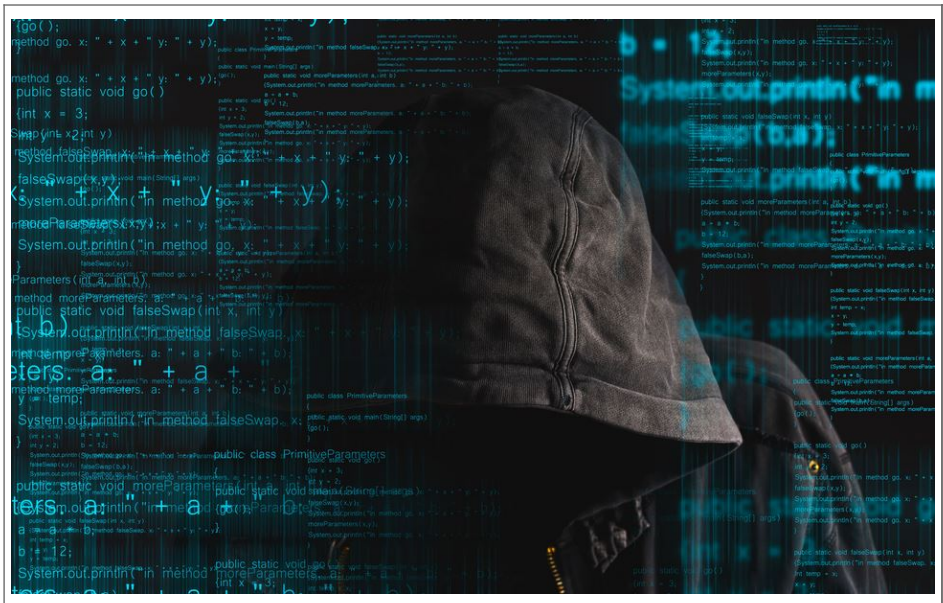
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Huit bonnes pratiques pour bien sécuriser les objets connectés – JDN

Un cousin du malware Furtim cible les énergéticiens européens



Un cousin du malware Furtim cible les énergéticiens européens

---

SentinelOne a découvert une variante du malware Furtim qui vise les sociétés européennes dans le domaine de l'énergie.

En mai dernier, des chercheurs la société EnSilo ont découvert un malware baptisé Furtim qui devait son nom à une obsession virant à la paranoïa de ne pas être détecté par les outils de sécurité. De la préparation à son installation jusqu'à son implémentation, le malware scrute, analyse et bloque tout ce qui touche de près ou de loin à la sécurité IT.

Il semble que ce malware revienne sous une autre forme pour s'attaquer au système industriel des entreprises énergétiques européennes. Des chercheurs de SentinelOne l'ont détecté au sein du réseau d'un énergéticien européen. Cette menace a un nom, SFG, et a été trouvée à la fois par une remontée d'information des logiciels de SentinelOne, mais aussi sur des forums privés. Les experts ont travaillé sur les échantillons pour comprendre son fonctionnement. Les résultats de cette analyse montrent que le comportement, la sophistication et la furtivité du malware sont l'œuvre d'un Etat ou pour le moins d'une organisation soutenue par un gouvernement. Les experts penchent pour une initiative provenant de l'Europe de l'Est.

Jusqu'au sabotage du réseau énergétique

Dans le détail, le cousin de Furtim s'appuie sur les mêmes exploits pour éviter d'être repéré par les outils de sécurité (antivirus, firewall next gen, solution endpoint, sandboxing). Plusieurs développeurs de haut niveau ont mis la main à la pâte pour perfectionner SFG. L'objectif est multiple, extraire des données ou faire tomber le réseau d'énergie, sans laisser de traces. Le malware affecte toutes les versions de Windows, précise SentinelOne dans un blog. Il situe ses débuts au mois de mai dernier et il est encore actif.

Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque s'appuyant sur le malware Blackenergy. Ce type de menaces est pris très au sérieux par les gouvernements au point de forcer les entreprises à remonter leurs niveaux de sécurité. En France, l'ANSSI peaufine les arrêtés sectoriels sur la sécurité des OIV (opérateurs d'importance vitale) notamment dans le domaine de l'énergie.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Malware : un cousin de Furtim cible les énergéticiens européens

Un concessionnaire Lamborghini de Mulhouse piraté

Un concessionnaire Lamborghini de Mulhouse piraté

Le vol de données peut souvent cacher des arnaques et attaques informatiques plus vicieuses encore. Exemple avec le piratage d'un concessionnaire de Lamborghini de l'Est de la France.

Derrière un piratage informatique, 99 fois sur 100, se cache le vol des données que le malveillant à pu rencontrer dans son infiltration. Des données qui se retrouvent, dans l'heure, quand ce n'est pas dans les minutes qui suivent la pénétration du site dans des forums et autres boutiques dédiés à l'achat et revente d'informations subtilisées.Un concessionnaire de Lamborghini, à Mulhouse, vient d'en faire les frais.

Une fois les contenus dérobés exploités (phishing, escroqueries…) le pirate s'en débarrasse en les diffusant sur la toile. C'est ce qui vient d'arriver à un concessionnaire automobile de l'Est de la France. Ici, nous ne parlons pas de la voiture de monsieur et madame tout le monde, mais de Lamborghini.

Prend son site web par dessus la jambe et finir piraté !

Le concessionnaire se retrouve avec l'ensemble des pousses bouton de la planète aux fesses. De petits pirates en mal de reconnaissance qui profitent d'une idiote injection SQL aussi grosse que l'ego surdimensionné de ces « piratins ». Bilan, le premier pirate a vidé le site, revendu/exploité les données. Il a ensuite tout balancé sur la toile. Les « suiveurs » se sont jetés sur la faille et les données. J'ai pu constater des identifiants de connexion (logins, mots de passe) ou encore des adresses électroniques lâchées en pâture. Des courriels internes (webmaster, responsables du site…).

Article original de Damien Bancal

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ

Le Maroc peut-il créer une Silicon Valley au Maghreb ?

Le Maroc peut-il créer une Silicon Valley au Maghreb ?

Le Maroc a-t-il les capacités de se transformer en « Silicon Valley » du Maghreb? Hamza Hraoui, conseiller en communication d'influence pour les entreprises et les dirigeants, estime que »oui ».

Dans un entretien paru jeudi 7 juillet au HuffpostMaroc, cet expert estime que le Maroc a toutes les potentialités pour cet objectif, à condition de revoir le fonctionnement de l'Agence nationale de réglementation des télécommunications (ANRT). »Nous sommes en tout cas crédibles et légitimes pour être le spot technologique de la région », souligne t-il. »Le taux de pénétration d'internet dépasse 56% chez nous alors qu'en Tunisie c'est 44%, en Algérie c'est moins de 20%. En plus d'avoir la population la plus connectée du Maghreb, le Maroc connaît également le plus fort dynamisme de ses médias en ligne. » En outre, le Maroc a pris de l'avance sur le plan des infrastructures de TIC, selon lui: » quand l'Algérie a introduit la 3G qu'en 2013, nous avons aujourd'hui la couverture 4G la plus large du Maghreb. » Mais, tempère l'expert, le pays accuse déjà un retard dans ce domaine.

Le »Hic »

»Au Maroc on est au point mort », affirme t-il, avant d'expliquer que »si la stratégie industrielle (du Ministre de l'Industrie et de l'Economie numérique) a esquissé les grandes lignes de l'économie numérique du pays, la structuration des écosystèmes numériques tarde à venir », même si »le potentiel est là. » Pour Hamza Hraoui, »il faut enclencher maintenant notre transformation et prendre le train de la nouvelle économie en misant sur notre tissu entrepreneurial. » Car »les Marocains attendent un vrai plan du numérique, conquérant et volontariste qui permettra d'accompagner les projets structurants des entreprises sur les marchés, où le Maroc peut acquérir d'ici 3 à 5 ans, un leadership continental: fabrication additive comme les imprimantes 3D, les objets connectés, la réalité augmentée, les villes intelligentes, les écoles du numérique… » Pour cela, il faut que bien des barrières tombent, et que les opérateurs du secteur rattrapent le retard accusé par le Maroc dans le digital et l'économie numérique.

Faire sauter les barrières

Et, surtout, libérer le secteur des »interdits » et des blocages. Il estime ainsi que la Maroc, en interdiction de la VoiP, »donne un mauvais signal aux acteurs de la nouvelle économie suite à cette interdiction. » »Et ses répercussions se feront sentir à moyen et à long terme », ajoute cet expert en communication, qui appelle l'ANRT à faire »son update ». Plus direct, il accuse l'ANRT de cloisonner le secteur des TIC et empêcher l'économie numérique de se développer. »A l'heure du décloisonnement de l'information, de l'explosion de la data et de l'émergence de l'économie collaborative, l'ANRT poussée et pressée par les opérateurs télécom, nous a montré qu'elle vit encore à l'âge de pierre en enlevant aux jeunes étudiants, aux chercheurs, aux start-upers qui créent de la richesse dans ce pays l'essence même du progrès: le droit à la mobilité. » Pour lui, »cela nous montre à quel point nos institutions ont du mal à admettre que la relation public-autorité et l'ordre établi sont profondément bouleversés par le digital, obligeant les hommes politiques à revoir en profondeur leurs messages, décisions et façons de faire. » A fin décembre 2015, le Maroc comptait 13,89 millions d'abonnés à l'Internet fixe, soit un taux de pénétration de 41,1 %, alors que le parc de l'internet mobile compte 12,81 millions d'abonnés avec une progression de 69,58% par an.

Article original de Amin Fassi-Fihri

Réagissez à cet article

Original de l'article mis en page : TIC: Le Maroc peut créer une Silicon Valley au Maghreb, mais…(Expert) – Maghreb Emergent

Secret des conversations, Facebook Messenger bientôt chiffré

	Secret des conversations, Facebook Messenger bientôt chiffré

Non, tous les échanges sur Messenger ne sont pas chiffrés de bout en bout. Pas encore du moins. Facebook teste le procédé à travers une nouvelle fonctionnalité, #Secret Conversations. En y ajoutant un petit côté messages éphémères à la Snapchat.

Facebook chantre du chiffrement de bout en bout ? L'entreprise vient de lancer une nouvelle option pour Messenger permettant de démarrer une conversation sécurisée. Baptisée Secret Conversations, celle-ci permet de créer, via la fiche d'un contact, une conversation chiffrée entre deux utilisateurs. Derrière, on retrouve le protocole Signal, également utilisé par WhatsApp.
Mais, contrairement à #WhatsApp, Secret Conversations se veut optionnel, pour ne pas dire ponctuel. Car il s'agit là de préférer la sécurité au confort, un choix auquel Facebook n'entend pas contraindre ses utilisateurs. Ainsi, via cette fonctionnalité, on ne peut envoyer que du texte et des photos à un unique destinataire. Pas de vidéo, de GIF, de paiement ou de discussion de groupe.

Ce message s'autodétruira automatiquement dans 4…3…

Cette sobriété se conjugue avec l'absence de synchronisation entre les appareils d'un même utilisateur. Impossible donc de commencer une conversation chiffrée avec son iPhone et de passer ensuite à sa tablette : la discussion est uniquement rattachée au terminal avec lequel elle a été initiée. En outre, preuve que Mark Zuckerberg n'a toujours pas digéré le refus de son offre de rachat sur Snapchat, il est possible de définir à l'aide d'un minuteur la durée de vie d'un message. Qui s'autodétruira une fois le délai écoulé.
L'option est intégrée à l'application Messenger pour Android et iOS. Déjà disponible pour certains, elle sera déployée plus largement au cours de l'été. Pour l'heure, il semble que rien ne soit prévu pour les versions navigateur du service.

Article original de Guillaume Périssat

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Secret Conversations : Facebook Messenger en mode chiffré

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

Après avoir contaminé l'Europe et l'Amérique du Nord en 2013, le malware Nymaim refait surface 3 ans plus tard et se propage désormais via une campagne de spearphising intensive, en utilisant un document Microsoft Word comme pièce jointe infectée

Lors de la découverte de la souche originale de Nymaim en 2013, notamment avec ses techniques de code modulaire (chaîne d'abattage et d'évasion), nous avions pu remarquer que plus de 2,8 millions d'infections s'étaient propagées. Sur le premier semestre 2016, ESET a de nouveau observé une augmentation significative de détections du malware Nymaim.

Infectant principalement la Pologne (54%), l'Allemagne (16%) et les Etats-Unis (12%), cette mutation du malware Nymaim a été détectée comme appartenant à la catégorie *Win32/TrojanDownloader.Nymaim.BA.* Elle utilise le spearphishing et une pièce jointe (type Word.doc) contenant une macro malveillante. Utilisée pour contourner les paramètres de sécurité par défaut de Microsoft Word via les techniques d'ingénierie sociale, l'approche est très dangereuse dans les versions anglaises de MS Word.

« Grâce à ses techniques d'évasion sophistiquées, l'anti-VM, l'anti-débogage et les flux de contrôle, cette fusée à deux étages sert à livrer le ransomware comme charge utile finale. Ce code que l'on peut nommer « Trojan modulaire » est impressionnant par sa faculté à voler les informations d'authentification de sites de banque électroniques dans les formulaires typiques en contournant la protection SSL. Ce code malveillant a évolué de façon à fournir des logiciels espions », explique Cassius de Oliveira Puodzius, Security Researcher chez ESET en Amérique Latine.

En avril 2016, la version précitée a été rejointe par une variante hybride de Nymaim (Gozi) qui avait pour cible les institutions financières d'Amérique du Nord, mais également en Amérique latine et principalement au Brésil. Cette variante fournit aux cybercriminels le contrôle à distance des ordinateurs compromis plutôt que de chiffrer les fichiers ou bloquer la machine – comme cela se fait habituellement.

En raison des similitudes entre les cibles visées dans chaque pays et les taux de détection, nous pouvons affirmer que les institutions financières restent au centre de cette campagne.

« L'étude complète de cette menace est toujours en cours. Toutefois, si vous pensez que votre ordinateur ou votre réseau a été compromis, nous vous recommandons de vérifier que les adresses IP et les URL que nous avons partagées dans l'article complet de WeLiveSecurity ne se trouvent pas dans votre pare-feu et dans le journal de votre proxy. Nous vous conseillons de mettre en place une stratégie de prévention en ajoutant une liste noire des des adresses IP contactées par ce malware au pare-feu et les URL à un proxy, aussi longtemps que votre réseau prendra en charge ce type de filtrage », conclut Cassius de Oliveira Puodzius.

Pour lire l'intégralité du rapport et ainsi obtenir des informations complémentaires sur le malware Nymaim, cliquez ici.

Réagissez à cet article