Après 3 semaines d’insistance de ZATAZ, la CNIL fait corriger une fuite de données sur le site du PS en quelque heures

	Après 3 semaines d’insistance de ZATAZ, la CNIL fait corriger une fuite de données sur le site du PS en quelque heures

Pendant trois semaines, j'ai tenté de faire corriger une fuite de données découverte sur le site du Parti Socialiste. J'ai dû faire appel à la CNIL pour qu'un sympathique communicant de ce parti politique français daigne écouter !

Pendant trois semaines, j'ai tenté de faire corriger une fuite de données découverte sur le site du Parti Socialiste. J'ai dû faire appel à la CNIL pour qu'un sympathique communicant de ce parti politique français daigne écouter !

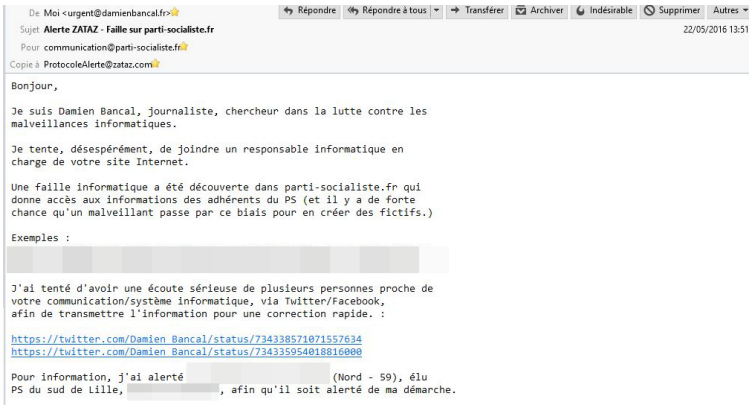
Des fuites de données, j'en croise des dizaines par mois, des centaines par années. Depuis la création de mon blog, voilà plus de trente ans (sur disquette, puis papier) et bientôt 20 ans sur le web, ZATAZ a pu aider plus de 60.000 entreprises, associations, particuliers à se protéger des malveillants du web. Bref, permettre de corriger une fuite de données, une faille, un problème de piratage via le protocole d'alerte ZATAZ.

Dans 99,9% des cas, cela se passe bien, voire très très bien. Pour les cas étatiques, par exemple, l'ANSSI me répond dans la minute, même un dimanche, à 3h du matin. La CNIL ne met pas plus de temps. Seulement, il y a ce 0,1 % de … J'ai un mot en tête, mais n'étant pas grossier de nature, je vous laisse l'imaginer.

Allô ! le Parti Socialiste ? vous avez une fuite de données !

Il y a trois semaines, je constatais une étonnante fuite de données visant un sous domaine du site Internet du Parti Socialiste. Je passerai le côté technique de la chose. Il suffisait de cliquer sur un lien particulièrement formulé vers le sous dossier « Archive » pour que s'ouvre un espace d'administration du portail politique du PS.

Le « oueb » de ce groupe politique fait parti du 0,1 % de cette froideur intellectuelle et de « je-m'en-foutisme » qui pourraient coûter très chers si un interlocuteur moins impliqué que moi avait eu en main l'accès à cette fuite de données. Car fuite de données il y avait. Il était possible d'accéder aux noms, prénoms, adresses physiques, mails des adhérents, montant des cotisations, code dossier, département … de l'espace adhésion (en attente de traitement, transmise, non finalisée et effective).



De Moi <urgent@damienbancal.fr>
Répondre | Répondre à tous | Transférer | Archiver | Indésirable | Supprimer | Autres
Sujet **Alerte ZATAZ - Faille sur parti-socialiste.fr** 22/05/2016 13:51
Pour communication@parti-socialiste.fr
Copie à ProtocoleAlerte@zataz.com

Bonjour,

Je suis Damien Bancal, journaliste, chercheur dans la lutte contre les malveillances informatiques.

Je tente, désespérément, de joindre un responsable informatique en charge de votre site Internet.

Une faille informatique a été découverte dans parti-socialiste.fr qui donne accès aux informations des adhérents du PS (et il y a de forte chance qu'un malveillant passe par ce biais pour en créer des fictifs.)

Exemples :

J'ai tenté d'avoir une écoute sérieuse de plusieurs personnes proche de votre communication/système informatique, via Twitter/Facebook, afin de transmettre l'information pour une correction rapide. :

https://twitter.com/Damien_Bancal/status/734338571071557634
https://twitter.com/Damien_Bancal/status/734335954018816000

Pour information, j'ai alerté (Nord - 59), élu PS du sud de Lille, , afin qu'il soit alerté de ma démarche.

Bref, après deux mails au service presse (sans réponse) ; deux mails aux DSI BS et JW (sans réponse) ; plusieurs Tweets dont une discussion hallucinante avec l'un des DSI que je tentais de contacter, autant dire qu'au bout de trois semaines, j'ai beau faire cela bénévolement, la moutarde commençait à me monter au nez, surtout après la lecture de plusieurs articles indiquant que d'étonnantes adhésions au PS étaient apparues dans plusieurs circonscriptions (Metz, …). Je me suis résolu à contacter des élus du PS officiant dans ma région, ainsi que la CNIL. Autant dire qu'avec la prestigieuse dame, cela n'aura pas pris trois semaines. Deux heures après mon alerte à la Commission Informatique et des Libertés, l'étonnant accès disparaissait du web… [Lire la suite]

Article de Damien Bancal

Réagissez à cet article

Source : *ZATAZ La CNIL fait corriger une fuite de données sur le site du PS – ZATAZ*

Plusieurs millions de comptes MySpace en vente en ligne sur le marché noir

Plusieurs millions de comptes MySpace en vente en ligne sur le marché noir

---

Un fichier comportant des informations sur plusieurs centaines de millions de comptes MySpace, dont 427 millions de mots de passe, a été mis en vente sur un site spécialisé, a révélé le site LeakedSource. Selon des tests effectués par Motherboard, les mots de passe figurant dans les documents correspondent bien à des comptes existant ou ayant existé.

Selon LeakedSource, les mots de passe de la base de données étaient chiffrés, mais protégés par une technologie aisément contournable avec du temps et de la puissance de calcul. L'intégralité de la base de donnée a été mise en vente pour environ 2 500 euros sur un site spécialisé dans le recel de données volées.

Un milliard d'inscrits

MySpace, considéré il y a dix ans comme le site le plus populaire pour les adolescents et les étudiants, n'est aujourd'hui plus que l'ombre de ce qu'il était. Le service, qui permet de créer sa page personnelle, avait notamment construit sa popularité en attirant de nombreux groupes de musique populaires. Le service existe toujours, et annonçait à la fin de 2015 avoir dépassé le seuil symbolique du milliard d'inscrits au cours de son existence. Les données contenues dans les fichiers volés restent cependant sensibles – de nombreux internautes réutilisent le même mot de passe pour plusieurs applications ou services. Il est conseillé aux utilisateurs ayant détenu ou détenant un compte MySpace de changer leur mot de passe s'ils l'ont réutilisé sur d'autres services… [Lire la suite]

Réagissez à cet article

Source : *Les informations de millions de comptes MySpace en vente en ligne*

Et si charger la batterie de son smartphone via un port USB était dangereux ?

Et si charger la batterie de son smartphone via un port USB était dangereux ?

On s'est tous probablement retrouvés un jour ou l'autre dans une situation où il nous restait peu de batterie sur notre téléphone et que nous n'avions pas de chargeur à portée de main. Le pire, c'est ce que ça nous est arrivé au moment même où on en avait le plus besoin, comme attendre un appel important, un message ou un e-mail, etc.

Il parait donc tout à fait normal de chercher une source d'électricité à proximité lors d'une telle situation, par exemple utiliser un port USB. Mais est-ce bien sûr ? Non, en réalité cela peut s'avérer dangereux. Via une connexion USB, n'importe qui peut s'emparer de vos fichiers, infecter votre smartphone d'un virus ou même le rendre inutilisable.

Chevaucher la foudre

Avant d'aborder le problème des hackers, il est important de préciser que toute les sources d'électricité ne sont pas forcément bonnes pour votre téléphone. Il existe beaucoup de plaintes sur Internet, principalement d'utilisateurs tentant de charger leur téléphone dernier cri en les connectant à des adaptateurs ou des chargeurs d'occasion (ou non originaux). Dans certains cas, les téléphones ont été rendus inutilisables. Dans certains cas encore plus étranges, des personnes prenant leur téléphone alors qu'ils étaient en charge ont été sérieusement blessées ou même tuées.

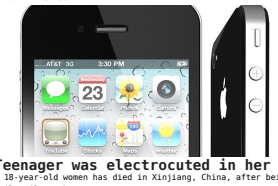
Follow

Daily Mail Online

@MailOnline

Teen dies after being electrocuted in her sleep while charging her iPhone http://dailym.ai/1o7Eia5

2:10 PM – 31 Jul 2014



Teenager was electrocuted in her sleep while charging her iPhone

A 18-year-old women has died in Xinjiang, China, after being electrocuted in her sleep while charging her iPhone 4s. It is not known if she was using an authentic Apple phone charger.

dailymail.co.uk

•

•

140140 Retweets

•

2424 likes

Malheureusement, il s'agit plus que de simples accidents. Par exemple, l'année dernière un appareil a été baptisé à juste titre : le tueur USB. Il contenait un impressionnant ensemble de condensateurs hébergés dans une carte mémoire flash USB, qui déchargeait 220 V dans le port USB auquel il était connecté. Une telle décharge pourrait dans le meilleur des cas détruire le port USB et dans le pire sans doute la carte mère de tout l'ordinateur. Nous doutons que vous souhaitiez tester la durabilité de votre téléphone de cette façon.

Montrez-moi vos fichiers

Deuxièmement, les ports USB n'ont pas été conçus uniquement pour la charge, mais aussi pour transférer des données. Les téléphones consommant le plus de données sont ceux conçus sur la plateforme Android 4 *x* et les versions antérieures, ils se connectent sur le mode MTP (Media Transfer Protocol) par défaut, exposant tous les fichiers de l'appareil.

En moyenne, il faut plus d'une centaine de kilo octets de données rien que pour le système hôte des fichiers et dossiers du téléphone. Pour vous donner une idée, il s'agit de la taille d'une copie de l'e-book d'*Alice au pays des merveilles*.

Bloquer votre téléphone vous éviterait de courir un tel risque mais honnêtement seriez-vous prêt à vous passer de votre téléphone pendant qu'il est en charge ? Et à toujours le débrancher du port USB lorsque vous recevez un message par exemple ?

A présent, jetons un coup d'œil de plus près aux données qui sont transmises du port USB même lorsque le mobile est en mode (bloqué) « charge seule ». La taille de ces données varie, dépendant de la plateforme du mobile et du système d'exploitation de l'hôte. Mais dans tous les cas, il s'agit plus que d'une « simple charge ». Comme nous l'avons découvert, ces données incluent le nom du mobile, le nom du fournisseur et le numéro de série.

Accès complet et au-delà

Vous devez sûrement penser que vous ne voyez pas où est le problème, seulement il y en a un, puisque nous avons trouvé en cherchant des informations accessibles au public qu'un fournisseur en particulier autorise beaucoup plus que ce qui est spécifié par le système.

Comment est-ce possible ?

Cela est rendu possible via un ancien système de commandes appelées commandes AT. Ces dernières ont été développées il y a quelques dizaines d'années afin de permettre les communications des modems et ordinateurs. Plus tard, elles ont été intégrées au standard du GSM et désormais sont toujours utilisées sur les smartphones.

Pour vous donner une idée de l'usage des commandes AT, laissez-moi vous donner quelques exemples que nous avons été en mesure de découvrir à la surface d'Internet : elles permettent à un hacker d'obtenir votre numéro de téléphone et de télécharger les contacts enregistrés dans la carte SIM. Ces commandes permettent d'établir un appel à n'importe quel numéro, et ce à vos frais, bien entendu. Et si vous êtes en roaming, de tels appels inattendus peuvent vite faire grimper la facture. Dépendant du vendeur, le mode du roaming peut faciliter l'accès à un hacker d'installer n'importe quel type d'applications, y compris malveillantes.

Tout ce qu'on vient de mentionner est possible, même si votre smartphone est bloqué !

En résumé, ne vous fiez pas aux apparences d'un port USB car il pourrait bien « cacher des choses ». Il s'agit d'un système qui collecte les données des appareils auxquels il est connecté, peu importe les raisons. C'est une source d'énergie bancale, tel un puissant condensateur ou un ordinateur qui installe une porte dérobée sur votre appareil. Une chose que vous ignorez jusqu'à ce que vous le branchiez.

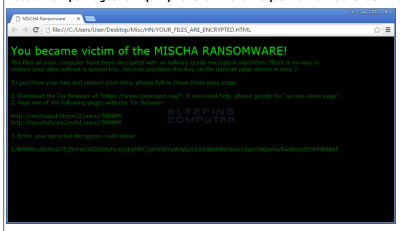
Article de Alexey Komarov

Source : *Les dangers de charger la batterie de son smartphone via un port USB – Kaspersky Daily – | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.*

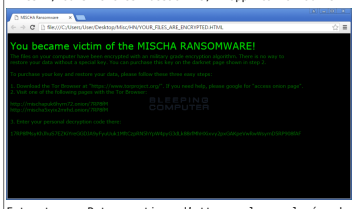
Mischa, le ransomware successeur de Petya

Mischa, le ransomware successeur de Petya

Apparu au mois de mars, le ransomware Petya a ouvert une nouvelle voie dans le développement des ransomwares. Il s'agissait du premier cas d'un malware qui allait au-delà du chiffrement des fichiers sur les disques locaux et partagés et qui préférait s'attaquer à la table de fichiers principale



Ceci étant dit, Petya n'était pas infaillible et les chercheurs ont été rapidement en mesure de créer un outil de restauration de certains des fichiers chiffrés par ce malware. Les individus malintentionnés n'ont pas perdu leur temps et ils ont trouvé le moyen de contourner une autre lacune de Petya : sa dépendance vis-à-vis de la volonté de la victime qui doit octroyer au malware les autorisations d'administrateur pour accéder à la table de fichiers principale (MFT).
Un nouveau programme d'installation de Petya a été détecté la semaine dernière. Celui-ci utilise un scénario de réserve. Si le malware n'obtient pas les autorisations d'administrateur au lancement, c'est un autre ransomware qui sera installé sur la machine infectée, en l'occurrence Mischa.
D'après les explications de Lawrence Abrams, de chez Bleeping Computer, les autorisations d'administrateur indispensables au fonctionnement de Petya figurent dans le manifeste de la version originale. Dans les commentaires envoyés à Threatpost, Lawrence Abrams explique « qu'avant l'exécution du code, Windows affiche la boîte de dialogue UAC qui sollicite ces autorisations. Si le service UAC est désactivé, l'application est exécutée automatiquement avec [les autorisations d'administrateur]. Si l'utilisateur clique sur « No » dans la fenêtre UAC, l'application n'est pas exécutée et, par conséquent, l'installation de Petya n'a pas lieu ».
Pour les exploitants de Petya, ces échecs représentent un gaspillage de ressources d'après Lawrence Abrams. Pour rectifier le tir, ils ont empaqueté un autre ransomware avec le programme d'installation. Il s'agit de Mischa qui sera exécuté si l'option « Petya » n'a pas pu être mise en œuvre.
Le manifeste de la nouvelle version indique que le fonctionnement requiert les données du compte utilisateur. Dans ce cas, Windows autorise le lancement de l'application sans afficher d'avertissement UAC. Comme l'explique Lawrence Abrams, « au lancement du programme d'installation, il sollicite les autorisations d'administrateur conformément à ses paramètres. La boîte de dialogue UAC s'affiche et si l'utilisateur choisit « Yes », ou si UAC est désactivé, l'application obtient les autorisations d'administrateur et installe Petya. Dans le cas contraire, c'est Mischa qui sera installé. Cette méthode est très intelligente ».



Entre temps, Petya continue d'attaquer les employées des services des ressources humaines allemands à l'aide de messages non sollicités qui contiennent des liens vers un fichier malveillant dans le cloud. Au début, les individus malintentionnés utilisaient Dropbox, mais depuis le blocage des liens Dropbox malveillants, ils se sont rabattus sur le service allemand TelekomCloud. Le fichier exécutable se dissimule sous les traits d'un fichier PDF qui serait un prétendu CV d'un candidat à un poste libre. Il contient même une photo.
« Lorsque l'utilisateur télécharge le fichier exécutable, l'icône PDF s'affiche, ce qui laisse penser qu'il s'agit bien d'un CV au format PDF » explique Lawrence Abrams. Toutefois, lorsque ce fichier est ouvert, il tente d'installer Petya. Et si cela ne marche pas, il installe le ransomware Mischa.
Le comportement de Mischa est identique à celui des autres ransomwares standard. Il analyse le disque local à la recherche de fichiers portant certaines extensions. Il chiffre les fichiers à l'aide d'une clé AES et ajoute à leur nom une extension de 4 caractères, par exemple 7GP3. Lawrence Abrams explique que « lorsque Mischa chiffre le fichier, il conserve la clé de chiffrement à la fin du fichier obtenu. Il convient de noter qu'il ne chiffre pas uniquement les fichiers traditionnels dans ce genre d'attaque (PNG, JPG, DOCX, etc.), mais également les fichiers EXE. »
Une fois qu'il a chiffré les fichiers, Mischa exige le versement d'une rançon de 1,93 bitcoins (environ 875 dollars américains) pour le déchiffrement. La somme doit être payée via le site Tor. Il n'existe pas encore d'outil de déchiffrement pour ce ransomware. « Nous conseillons aux victimes de vérifier avant tout la conservation des clichés instantanés à l'aide de Shadow Explorer. Ils pourraient être utile pour restaurer une ancienne version des fichiers chiffrés » conclut Lawrence Abrams.

Article du Kaspersky Lab

Réagissez à cet article

Source : *Petya possède un suppléant : Mischa – Securelist*

Forte hausse des applications Android malveillantes

Forte hausse des applications Android malveillantes

Les applications Android malveillantes et les ransomwares dominent le paysage des menaces au 1er trimestre 2016.

La société Proofpoint a publie son Rapport trimestriel sur les menaces, qui analyse les menaces, les tendances et les transformations observées au sein de notre clientèle et sur le marché de la sécurité dans son ensemble au cours des trois derniers mois. Chaque jour, plus d'un milliard de courriels sont analysés, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malwares afin de protéger les utilisateurs, les données et les marques contre les menaces avancées. On apprend, entre autres, que 98 % des applications mobiles malveillantes examinées au 1er trimestre 2016 ont ciblé des appareils Android. Cela demeure vrai en dépit de la découverte médiatisée d'un cheval de Troie pour iOS et de la présence persistante d'applications iOS ou officieuses dangereuses. Les applications Android malveillantes sont de plus en plus nombreuses.

75 % des attaques de phishing véhiculées par des e-mails imposteurs comportent une adresse «répondre à » usurpée afin de faire croire aux destinataires que l'expéditeur est une personne représentant une autorité. Ce type de menaces est de plus en plus mature et spécialisé, et c'est l'un des principaux ciblant les entreprises aujourd'hui, qui leur auraient coûté 2,6 milliards de dollars au cours des deux dernièresannées selon les estimations.

Applications Android malveillantes

Les ransomwares se sont hissés aux premiers rangs des malwares privilégiés par les cybercriminels. Au 1er trimestre, 24 % des attaques par e-mail reposant sur des pièces jointes contenaient le nouveau ransomware Locky. Seul le malware Dridex a été plus fréquent.

L'e-mail reste le principal vecteur de menaces : le volume de messages malveillants a fortement augmenté au 1er trimestre 2016, de 66 % par rapport au 4ème trimestre 2015 et de plus de 800 % comparé au 1er trimestre 2015. Dridex représente 74 % des pièces jointes malveillantes.

Chaque grande marque analysée a augmenté ses publications sur les réseaux sociaux d'au moins 30 %. L'accroissement du volume des contenus générés par les marques et leurs fans va de pair une accentuation des risques. Les entreprises sont constamment confrontées au défi de protéger la réputation de leurs marques et d'empêcher le spam, la pornographie et un langage grossier de polluer leur message.

Les failles de Java et Flash Player continuent de rapporter gros aux cybercriminels. Angler est le kit d'exploitation de vulnérabilités le plus utilisé, représentant 60 % du trafic total imputable à ce type d'outil. Les kits Neutrino et RIG sont également en progression, respectivement de 86 % et 136 %. (ProofPoint)… [Lire la suite]

Article 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

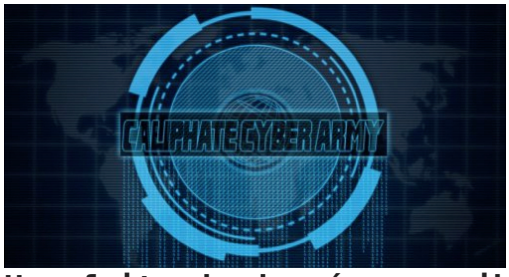
Réagissez à cet article

Source : *Forte hausse des applications Android malveillantes – Data Security BreachData Security Breach*

La France visée par une nouvelle cyberattaque de l’EI

La France visée par une nouvelle cyberattaque de l’EI

Les équipes CybelAngel ont repéré lundi 16 mai une base de coordonnées de citoyens français et américains publiée sur le site justepaste.it. L'utilisateur à l'origine de la publication se revendique de la Caliphate Cyber Army (#CCA).



Une fuite de données sensibles mais accessibles depuis 6 mois

Le message commence par une représentation de la basmala, un verset leitmotiv du Coran à la gloire de Dieu. Des mots-dièse "CCA #CyberCaliphate #UCC" et un logo de la Caliphate Cyber Army viennent compléter la revendication introductive.

Vient ensuite une liste de 77 emails, mots de passe, numéros de téléphone, adresses, comptes Paypal et soldes de compte Paypal. La liste concerne 38 adresses françaises, 31 américaines, 6 australiennes, 1 philippine et 1 néerlandaise. Les coordonnées semblent être uniquement personnelles et non professionnelles.

Après analyse, il semblerait que les données exposées ici étaient déjà présentes sur le Dark Web avant cette publication. En effet, un message publié le 12 janvier dernier sur le site pastebin.com reprenait 35 paires d'emails/mots de passe correspondant exactement à ceux publiés le 16 mai par la Cyber Caliphate Army. A l'aune de cette troublante similarité entre le 12 janvier et le 16 mai, la CCA reprendrait à son compte des adresses en libre accès sur le Dark Web ; ce qui ne serait pas la première fois.

Une Cyber Armée aux attaques peu techniques mais à fort impact médiatique

La Cyber Caliphate Army est issue de la volonté de l'Etat Islamique de projeter son action dans l'espace virtuel en 2014. Elle est dans un premier temps dirigée, et probablement entièrement constituée par Junaid Hussain, un hacker anglais.

De son lancement pendant l'été 2014 jusqu'à l'assassinat de Hussain par un drône américain en août 2015, la CCA a revendiqué une série de cyberattaques peu sophistiquées mais très médiatiques : plusieurs défacements de comptes Twitter du Commandement Central des Armées américaines (CENTCOM), de Newsweek, de chaînes de télévisions américaines, l'arrêt des retransmissions des 11 chaînes de TV5 Monde (action dont la parenté est mise en doute par de nombreux experts).

Cette nouvelle fuite souligne les faiblesses de la Cyber Armée du Califat

Depuis la mort de Husain, la CCA a mené des actions nettement moins symboliques : des défacements indiscriminés de milliers de sites et des actions à la parenté douteuse dont des fermetures de systèmes informatiques revendiquées ex-post et des diffusions de données en réalité déjà en ligne, comme celle détectée ce 16 mai par CybelAngel.

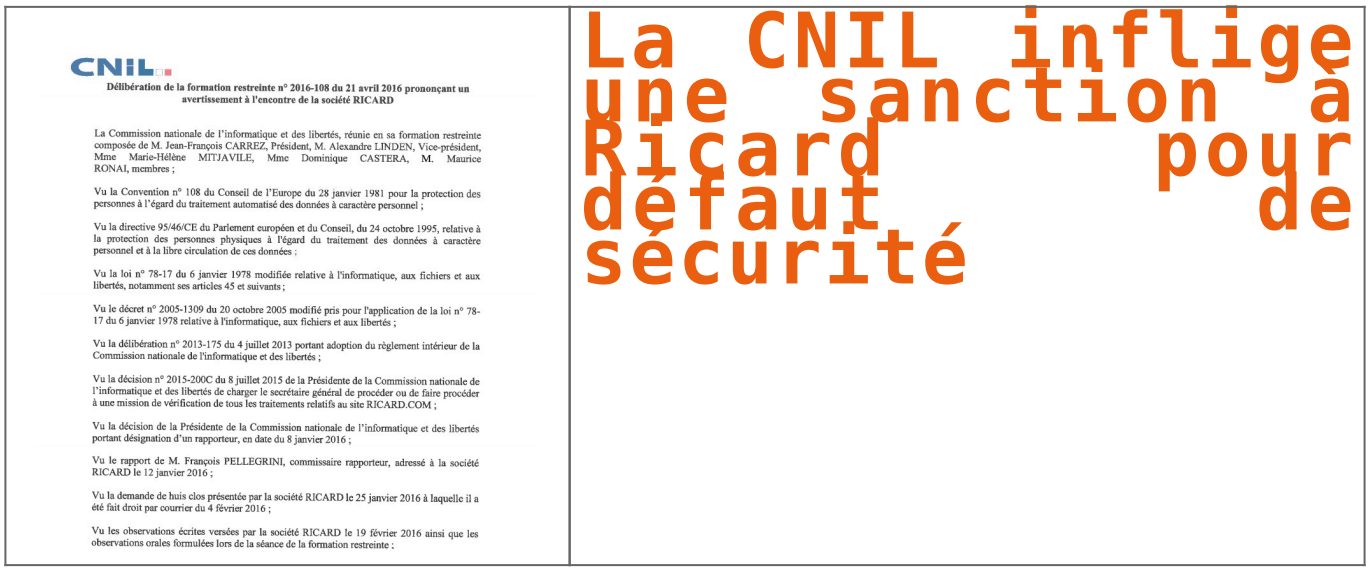
Face à ce potentiel de nuisance visiblement réduit, 4 groupuscules d'hacktivistes islamistes dont la Cyber Caliphate Army ont proclamé leur union en un United Cyber Caliphate en avril ainsi que nous vous le rapportions la semaine dernière. Quelques semaines plus tard, le groupuscule Cyber Caliphate Army revendique pourtant en son nom propre une action et ne mentionne le United Cyber Caliphate qu'en un hashtag UCC. Il semblerait que l'intégration des différents groupes hacktivistes islamistes prenne plus de temps que prévu.

Article de CybelAngel Analyst Team

Réagissez à cet article

Source : *La France visée par une nouvelle cyberattaque de l'EI*

La CNIL inflige une sanction à Ricard pour défaut de sécurité – Le Monde Informatique



CNIL

Délibération de la formation restreinte n° 2016-108 du 21 avril 2016 prononçant un avertissement à l'encontre de la société RICARD

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, M. Alexandre LINDEN, Vice-président, Mme Marie-Hélène MITJAVILE, Mme Dominique CASTERA, M. Maurice RONAI, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2015-200C du 8 juillet 2015 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tous les traitements relatifs au site RICARD.COM ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur, en date du 8 janvier 2016 ;

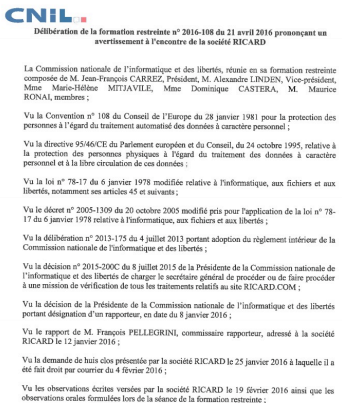
Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé à la société RICARD le 12 janvier 2016 ;

Vu la demande de huis clos présentée par la société RICARD le 25 janvier 2016 à laquelle il a été fait droit par courrier du 4 février 2016 ;

Vu les observations écrites versées par la société RICARD le 19 février 2016 ainsi que les observations orales formulées lors de la séance de la formation restreinte :

La CNIL inflige une sanction à Ricard pour défaut de sécurité

La CNIL vient de publier un avertissement public contre Ricard pour défaut de sécurisation des données d'un programme de fidélité accessible sur le web.



CNIL.

Délibération de la formation restreinte n° 2016-108 du 21 avril 2016 prononçant un avertissement à l'encontre de la société RICARD

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, M. Alexandre LINDEN, Vice-président, Mme Marie-Hélène MITTAVILLE, Mme Dominique CASTERA, M. Maurice RONAI, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2015-200C du 8 juillet 2015 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tous les traitements relatifs au site RICARD.COM ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur, en date du 8 janvier 2016 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé à la société RICARD le 12 janvier 2016 ;

Vu la demande de huis clos présentée par la société RICARD le 25 janvier 2016 à laquelle il a été fait droit par courrier du 4 février 2016 ;

Vu les observations écrites versées par la société RICARD le 19 février 2016 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Voilà une publicité dont Ricard se serait bien passé mais la sanction est cependant bien légère. La CNIL vient en effet de sanctionner le distributeur de produits alcoolisés pour un programme de fidélité présenté sur son site web. Les données personnelles des membres de ce programme n'étaient en effet pas protégées. L'autorité administrative indépendante, constatant l'absence de préjudice réel et la correction du problème, n'a cependant pas sanctionné très durement l'entreprise puisqu'elle lui a juste infligé un avertissement public par une décision du 21 avril 2016 publiée le 24 mai.

Concrètement, les données personnelles (noms, prénoms, dates de naissance, moyens de paiements, achats opérés, adresses électroniques, téléphones…) étaient stockées dans un répertoire du site web qui n'était ni bloqué en accès (par un *.htaccess* par exemple) ni crypté. La seule précaution prise était une demande de désindexation du répertoire dans les moteurs de recherche via une instruction dans le *robot.txt*. Donc, une simple lecture du*robot.txt*, par nature en clair, permettait de savoir où chercher des informations intéressantes…

Incompétence du prestataire, indifférence du responsable de traitement

Après un premier contrôle opéré le 8 juillet 2015, la CNIL prévient Ricard du problème. La société déclare avoir effectué le nécessaire en le commandant à son prestataire, information confirmée par un courrier du 23 juillet. Or, le 27 novembre 2015, un nouveau contrôle aboutit au constat que, certes, l'affichage du contenu du répertoire indiqué dans le*robot.txt* n'est plus possible mais l'accès en lecture aux URL directes des fichiers l'est toujours ! Un nouveau procès-verbal d'infraction lui est donc adressé le 4 décembre 2015, notification à l'origine de la procédure dont nous parlons ici. Le site web a finalement été refondu pour être à l'état de l'art en matière de sécurité.

Cette affaire est l'occasion de plusieurs rappels intéressants. Tout d'abord, pour la CNIL, le seul et unique responsable est et demeure l'entreprise qui ordonne la création et maîtrise le traitement de données. Cette entreprise ne peut en aucun cas se défausser sur un prestataire. C'est au commanditaire de bien vérifier la mise en place des mesures obligatoires. Mais, et c'est induit, le commanditaire, responsable du traitement, doit effectivement commander et vérifier la mise en place des telles mesures.

Une mise en cause du prestataire délicate

La délibération de la CNIL ne mentionne pas le sous-traitant en cause. Une porte-parole de la CNIL précise : « pour l'instant, le seul responsable pour nous est Ricard en tant que responsable du traitement même si, avec le nouveau Règlement Européen, la place du prestataire va évoluer. » Le groupe Pernod-Ricard, sollicité par la rédaction, n'a pas encore officialisé une réaction ni précisé quel était le prestataire en cause.

Cela dit, dans l'absolu, le prestataire pourrait être poursuivi civilement par Ricard. Le producteur de pastis pourrait lui demander une indemnisation pour le préjudice subi de son fait, notamment le préjudice d'image.

Mais encore faudrait-il que la faute puisse être caractérisée et prouvée. En effet, les attentes en matière de sécurité doivent être spécifiées contractuellement pour qu'un manquement soit caractérisé. Et les instructions du commanditaire, Ricard en l'occurrence, ne doivent pas être contraires directement ou indirectement aux bonnes pratiques. En général, ce genre d'affaires se règle discrètement dans les bureaux des entreprises concernées et il est peu probable que le résultat de ces palabres ne soit un jour connu.

MISE À JOUR : COMMUNIQUÉ DE RICARD

En réponse à notre sollicitation, Ricard nous a fait parvenir un communiqué laconique, sans citer le prestataire mis en cause, mais insistant sur les limites du manquement relevé par la CNIL. « Suite à la délibération de la CNIL du 21 avril 2016 prononçant un avertissement à l'encontre de la société Ricard pour son site internet Ricard.com, la société Ricard prend acte de cette décision et précise, comme le rappelle la CNIL, que la faille de sécurité identifiée a été corrigée sur le site existant. La société Ricard entend préciser que les données étaient exclues d'une indexation sur Internet et n'ont donc jamais été accessibles par des moteurs de recherche. La société Ricard confirme en outre avoir développé un nouveau site Ricard.com qui sera mis en ligne début juin et qui répond également aux normes de sécurité ».

Article de Bertrand Lemaire

Réagissez à cet article

Source : *La CNIL inflige une sanction à Ricard pour défaut de sécurité – Le Monde Informatique*

Un vague massive de spams JavaScript distribue le ransomware Locky

Un vague massive de spams JavaScript distribue le ransomware Locky

Les pays européens sont aujourd'hui victimes d'une vague de spams essayant d'exécuter un code JavaScript installant le redoutable ransomware Locky.

Au cours de la semaine écoulée, un grand nombre d'ordinateurs à travers l'Europe – et d'autres endroits dans le monde dont les Etats-Unis et le Canada – ont été touchés par une campagne massive de spams transportant des pièces jointes JavaScript malveillantes qui installent le ransomware Locky. Les pièces jointes sont généralement des fichiers d'archives .zip qui contiennent .js ou fichiers .jse intérieur. Ces fichiers s'exécutent directement sous Windows sans avoir besoin d'applications supplémentaires.

L'éditeur spécialisé dans la sécurité ESET a observé un pic dans les détections de JS / Danger.ScriptAttachment, un téléchargeur malware écrit en JavaScript qui a démarré le 22 mai et a atteint son sommet le 25 mai. JS / Danger.ScriptAttachment permet de télécharger divers programmes malveillants à l'insu des internautes, mais il a récemment été adapté pour distribuer Locky, un programme malveillant répandu qui utilise un chiffrement fort pour crypter les fichiers des utilisateurs. Cependant, il est très rare que des gens envoient des applications légitimes écrites en JavaScript par email. Les utilisateurs devraient éviter d'ouvrir ce type de fichiers.

La France touchée à 36%

De nombreux pays en Europe ont été touchés. Les taux de détection les plus élevés ont été observés au Luxembourg (67%), en République tchèque (60%), en Autriche (57%), aux Pays-Bas (54%), au Royaume Unie (51%) et en France 36%. Les données de télémétrie de l'éditeur ont également montré des taux de détection importants pour cette menace au Canada et aux États-Unis. Bien que Locky n'a pas de défauts connus qui permettraient aux utilisateurs de déchiffrer leurs fichiers gratuitement, les chercheurs en sécurité de Bitdefender ont développé un outil gratuit qui peut prévenir les infections Locky. L'outil trompe le ransomware en lui indiquant que l'ordinateur est déjà infecté.
L'utilisation de fichiers JavaScript pour distribuer Locky a commencé un peu plus tôt cette année, ce qui a incité Microsoft à publier une alerte à ce sujet en avril dernier.
Article de Lucas Mearian/ IDG NS (adaptation SL)

Réagissez à cet article

Source : *Un vague massive de spams JavaScript distribue le ransomware Locky – Le Monde Informatique*

L’adoption de l’analyse comportementale appelée à s’étendre

L’adoption de l’analyse comportementale appelée à s’étendre

Selon Gartner, les entreprises se tournent de plus en plus vers l'analyse comportementale pour améliorer la détection des incidents et renforcer l'efficacité de leurs SOC. De quoi pousser à une inéluctable consolidation du marché.

L'analyse comportementale – des utilisateurs comme des flux réseau ou des entités connectées à l'infrastructure – a fait une entrée remarquée sur le marché de la sécurité l'an passé. Mais selon Gartner, les solutions isolées actuellement proposées vont être rapidement appelées à s'intégrer, au point d'encourager à une consolidation des acteurs.

Dans une note d'analyse, Avivah Litan et Eric Ahlm résument la situation : « les besoins des acheteurs pour détecter les brèches de tout type vont pousser à la consolidation des systèmes de détection basés sur le comportement, tels que les systèmes d'analyse du comportement des utilisateurs et des entités (UEBA), de détection et de réponse sur les points de terminaison (EDR), et d'analyse du trafic réseau (NTA) ».

Des catégories bien distinctes

Dans la première catégorie, le cabinet mentionne par exemple Securonix, LightCyber, Exabeam et Gurucul. Le premier étant notamment utilisé par HP au sein du système de gestion des informations et des événements de sécurité (SIEM) ArcSight. Pour l'EDR, il prend pour exemples Hexis et Ziften, mais pourrait également évoquer SentinelOne, notamment. En matière de NTA, le cabinet fait référence à SS8 et Niara, mais il faut également compter avec Vectra Networks ou encore Darktrace, entre autres.

Mais voilà, comme le relèvent les deux analystes, les acheteurs de solutions de sécurité ne veulent pas seulement détecter les brèches, « mais aussi y répondre rapidement et efficacement ». S'il le fallait, l'édition 2016 de RSA Conference a fait la démonstration de cette tendance. Ce besoin doit conduire à une « collision du marché entre systèmes de détection basés sur le comportement et systèmes d'orchestration et de réaction ». Et cela parce que ni UEBA, ni EDR, ni NTA ne semble en mesure d'apporter, seul, une réponse complète aux besoins des entreprises.

Des capacités différentes

Ainsi, Avivah Litan et Eric Ahlm soulignent que la première catégorie est efficace pour identifier des compromissions de comptes utilisateurs ou des acteurs internes malveillants, mais peut montrer ses limites dans la détection des incidents impliquant des logiciels malveillants. De son côté, « l'EDR peut être efficace pour trouver les comportements mauvais sur un hôte et identifier les objets malicieux », mais plus faible lorsqu'il s'agit de mettre le doigt sur une menace interne. Enfin, les outils de NTA « peuvent être capables de trouver les conséquences de deux types d'événements, mais n'ont pas les données relatives aux utilisateurs ou aux hôtes nécessaires pour confirmer l'incident ».

Analyse comportementale : la clé de la sécurité ?

D'autres outils peuvent venir en outre compléter l'édifice, qu'il s'agisse des SIEM ou des systèmes de gestion du renseignement sur les menaces comme ceux d'Anomali, de ThreatConnect ou encore de ThreatQuotient. Au final, pour les analystes de Gartner, le marché s'avère « bruyant, chaotique et encombré », pollué notamment par des discours marketing qui s'articulent « autour des mêmes thèmes clés tels que analytique, machine learning, automatisation, et autres termes similaires, bien que leur application de ces fonctionnalités soit largement différente en ce qui concerne ce qu'ils peuvent faire dans leurs rôles spécifiques ». Bref, la confusion règne.

Des performances à démontrer

Et cela d'autant plus que, selon Gartner, les spécialistes de l'analytique appliquée à la sécurité peinent encore à faire la démonstration de la valeur de leurs solutions. Lors d'échanges, ceux-ci cherchent surtout à se différentier en évoquant l'étendue ou le volume de leurs échantillons de données, le framework analytique utilisé ou encore la technologie analytique employée – apprentissage machine, deep learning, et intelligence artificielle sont là largement mis à contribution. Las, si le cabinet voit là des « facteurs importants et des sujets de discussions divertissants », tous « échouent à constituer un différentiateur majeur » car, pour Avivah Litan et Eric Alhm, « les éditeurs devraient d'abord se concentrer sur la manière dont le recours à l'analytique rend leur technologie meilleure en termes de résultats, de manière mesurable. Par exemple, dans quelle mesure trouver des attaques inconnues est plus efficace en pourcentage avec l'analytique que chercher à trouver un logiciel malveillant inconnu sans ».

Une inéluctable consolidation

Pour autant, les deux analystes ne contestent pas la valeur intrinsèque que l'analytique apporte à la détection de brèches. Mais ils soulignent l'importance des étapes suivant la détection. D'où la convergence anticipée entre acteurs de la détection basée sur l'analytique et de l'orchestration/réaction. Et c'est peut-être là que le SIEM est appelé à jouer une nouvelle carte, pour dépasser des limites bien connues. Dès lors, pour Gartner, les acteurs de détection devaient « soit prévoir de nouer formellement des partenariats avec des acteurs du SIEM […] ou se préparer à reprendre des fonctions clés du SIEM ».

Le cabinet s'attend donc clairement à une consolidation prochaine de systèmes de détection de menaces basés sur les comportements, mais il n'exclue pas l'émergence de solutions de type plateforme dédiées à l'investigation et à la réponse aux incidents. Des solutions sur lesquelles les composant de détection et de réponse viendraient se greffer. Et n'est-ce pas justement ce que cherche à proposer un Phantom Cyber ?

Article de Valéry Marchive

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

Source : *L'adoption de l'analyse comportementale appelée à s'étendre*

Deux applications accusées d'espionner les coureurs

Deux applications accusées d'espionner les coureurs

Les applications Runkeeper et Tinder viennent d'être dénoncées par le conseil des consommateurs norvégien. En effet, elles exploiteraient illégalement les données des utilisateurs.

Si vous ne le savez pas encore, Runkeeper est une application qui permet de mesurer ses performances sportives. Si on parle d'elle aujourd'hui, ce n'est pas vraiment pour les fonctionnalités qu'elles proposent, mais plutôt pour un sujet plus serré. En effet, cette application qui est la possession de la société FitnessKeeper violerait les règles de confidentialité des données personnelles. D'après le NCC (conseil des consommateurs norvégien), afin de pouvoir évaluer l'état de l'utilisateur, elle doit d'abord accéder à des fonctionnalités stratégiques telles que la géolocalisation.
Et le comble dans tout cela, c'est le fait que les données de l'utilisateur ayant été collectées seraient ensuite utilisées pour des finalités commerciales. En effet, elles seraient revendues à des entreprises de publicité et seraient même sauvegardées même après la suppression du compte. En tout cas, c'est ce qu'avance un rapport qui date du 10 mai. Interrogé sur cette question, le fondateur de Runkeeper a indiqué que le problème vient d'un bug. « Nous sommes en train de sortir une nouvelle version de notre application qui élimine ce bug… Nous prenons au sérieux la confidentialité des données des utilisateurs… », a-t-il indiqué. Par ailleurs, outre l'application Runkeeper, le NCC pointe aussi du doigt l'application Tinder, laquelle est une application pour les fans de rencontre amoureuse. Elle, aussi, conserverait les données des utilisateurs, notamment, les photos et les conversations… [Lire la suite]

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

Source : *Runkeeper et Tinder : les deux applications accusées d’espionner les coureurs – MeilleurActu*