Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr

Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr

Yahoo donne les détails des hacks qui ont touché plus d'un milliard de comptes, et en révèle un nouveau. Et la patronne se serait fait sucrer ses primes.

La crucifixion de **Yahoo** continue, et si ce n'est pas déjà fait, on ne peut que vous recommander à ce stade de supprimer votre éventuel compte Yahoo. Dans un communiqué, l'entreprise est revenue par le menu sur toutes les attaques qui ont gravement entaché la réputation de l'entreprise depuis 2014. On y apprend en prime que dernièrement, des hackers ont obtenu du code propriétaire de Yahoo et ont pu fabriquer de faux cookies.
Cela leur aurait permis d'accéder à 32 millions de comptes entre 2015 et décembre 2016. Sur cette masse, seuls 26 utilisateurs auraient été prévenus. L'entreprise explique également collaborer avec les autorités depuis que son enquête a révélé la possible implication de **hackers** soutenus par un état dans ces piratages. En tout, plus d'un milliard de comptes Yahoo ont été compromis depuis 2014…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Yahoo subit un énième hack embarrassant, la patronne du groupe se justifie sur Tumblr*

1,2 million de francs détournés d’une entreprise Bernoise

1,2 million de francs détournés d’une entreprise Bernoise

CYBERCRIMINALITÉ – Une société bernoise a été victime de piratage informatique. En tout, 1,2 million de francs ont été détournés. Le patron ne décolère pas, s'étonnant du manque de réactivité des banques.

Des cyber-criminels sont parvenus à détourner 1,2 million de francs des comptes de la société bernoise Küng Holding. Mis à part 160'000 francs, l'argent a pu être récupéré, mais le patron de l'entreprise Christoph Küng ne décolère pas.

Ce dernier s'étonne d'une part que trois banques aient déclenché sans demande d'éclaircissements des paiements vers d'obscures adresses. Dans un cas, 785'000 francs ont notamment été versés à un individu au Kirghizistan. D'autre part, M. Küng estime que le logiciel de paiement utilisé comporte de sérieux problèmes de sécurité.

Ces failles ont rendu possibles les ordres de paiement du pirate informatique, a confié jeudi Christoph Küng à l'ats. Il confirmait des informations publiées par le site internet Inside Paradeplatz, le Bund et la Berner Zeitung.

Cheval de Troie

Les cyber-criminels ont agi en utilisant le cheval de Troie Gozi, qui s'introduit dans les ordinateurs par le biais d'une pièce-jointe dans un courriel. Ces ordres de paiement ont seulement éveillé les soupçons de PostFinance, qui a considéré une demande de virement de 49'000 francs comme « inhabituelle ».

Les trois banques ont en revanche autorisé ces paiements sans difficulté. Ce n'est que par la suite que Christoph Küng a pu péniblement stopper une grande partie de ces virements et récupérer l'argent.

La société informatique suisse qui a développé le logiciel se défend des accusations, estimant que Küng Holding n'a pas installé une mise à jour importante. Christoph Küng nie toutefois cette affirmation…[lire la suite]

NDLR : Denis JACOPINI souhaiterai bien être Expert judiciaire désigné sur cette affaire. Analyser le moyen utilisé par le pirate informatique pour modifier le comportement du logiciel de comptabilité devrait être très instructif !

La responsabilité de l'éditeur va t-elle être recherchée en raison de l'existence d'une faille de sécurité sans son logiciel et en raison de sa possible négligence pour ne pas avoir mis en place des mesures de sécurité adapté au coté sensible de la fonction de virement automatique ?

La responsabilité du dirigeant qui n'a pas appliqué la mise à jour recommandée est elle engagée ?

Peut-être bien que l'expertise permettra d'aboutir à une toute autre cause .

Si nous le pouvons, nous suivrons cette affaire.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Piratage informatique dans une entreprise bernoise: 1,2 million de francs détournés*

Les dangers des jouets connectés | Denis JACOPINI

Les dangers des jouets connectés | Denis JACOPINI

La gamme Cloudpets de Spiral Toys a été piratée. Plus de 800000 comptes ont été piratés avec les informations qui y sont liées et plus de 2,2 millions de messages vocaux se retrouvent également sur la toile. Les peluches connectées de la marque permettait en effet aux parents et aux enfants de s'échanger des messages par le biais d'une application téléphonique, à travers l'ours en peluche.

Denis JACOPINI a été Interviewé par la revue Atlantico à ce sujet :

Atlantico : Une société d'ours en peluche connectés a été récemment piratée, les messages laissés par les parents à leurs enfants sont désormais hackable. Ce n'est pas la première fois que ce type de piratage arrive, pour protéger nos enfants, devrions-nous les éloigner de ce type de jouets connectés ?
Denis JACOPINI : En effet, au-delà du risque relatif à la protection des données personnelles des enfants et de leurs parents, la revue Que choisir avait déjà alerté les consommateurs en fin 2016 sur des risques inhérents au connexions non sécurisée de plusieurs jouets connectés.
Qui a tenu compte du résultat de cette étude pour revoir la liste des jouets qui seraient présents dans la hotte légendaire ?
La relation entre les enfants et les jouets va bien au-delà de la technologie et des risques qu'elle peut représente.
Les jouets bénéficie également de phénomènes de mode et l'engouement, sauf erreur, se fout bien de la qualité des produits et encore moins de leur sécurité.
Manque de connaissance, inconscience, crédulité ou trop de confiance de la part des parents ? Il est vrai qu'on peut facilement croire que si des jouets se trouvent sur nos rayons, c'est qu'ils ont forcément dû passer avec succès toute une batterie de tests rassurant pour le consommateur.
Pour la part des jouets à usage familial testés, même si les normes EN71 et EN62115 ont été récemment révisées pour répondre aux exigences de la nouvelle directive 2009/48/CE, les validations se reposeront sur des niveaux satisfaisants en terme de propriétés physiques et mécaniques, d'inflammabilité, de propriétés chimiques, électriques ou bien relatives à l'hygiène et à la radioactivité.
Vous l'aurez remarqué, aucun test n'est prévu pour répondre à des mesures ne serait-ce que préventive en terme de protection des données personnelles et encore moins en matière se sécurité numérique.
Alors finalement, pour répondre à votre question : « devrions-nous éloigner les enfants de ce type de jouets connectés ? »
A mon avis, en l'absence de normes protectrices existantes, la prudence devrait être de mise. Certes, il est impossible de se protéger de tout. Cependant, il serait à minima essentiel que les parents soient informés des risques existants et des conséquences possibles que pourraient provoquer des piratages par des personnes mal intentionnées pour prendre des mesures qu'ils jugent utiles.

Atlantico : Comment pouvons-nous restreindre la possibilité de piratage de données pour ce type d'objet ?
D.J. : La situation confortable serait que le consommateur soit vigilant pour ce qui concerne les mesures de sécurité couvertes par l'appareil et celles qui ne le sont pas. Malheureusement, ces gardes-fous ne sont qu'à l'état d'étude.
Sauf à vous retrouver dans un environnement ou le voisin le plus proche se trouve à plusieurs dizaines de mètres, être prudent dans l'usage de ces objets pourrait par exemple consister à :
– Si le jouet le permet, changer le mot de passe par défaut et mettre en place un mot de passe complexe pour accéder à sa configuration ;
– Si le jouet le permet, activer les connexions sécurisées par cryptage ;
– Si le jouet le permet, désactiver les connexions à partir d'une certaine heure ;
– N'utiliser les jouets connectés que dans des environnements protégés, en raison de la portée limitée des communications Bluetooth (par des distances suffisantes entre le jouet et des pirates éventuels) ;
– Pour les jouets utilisant le Wifi,
– Mettre en place des protections physiques contre les rayonnements électromagnétiques dans certaines directions ;
– Cacher les caméras si elles ne sont pas utilisées ;
– En fin d'utilisation du jouet, ne pas se satisfaire d'éteindre l'appareil qui ne sera peut-être seulement en veille, mais retirer les piles ou placer le jouet dans un espace protégé (fabriquez une cage de Faraday) ;
Enfin, compte tenu que le bon fonctionnement du jouet est lié à l'acceptation des conditions contractuelles d'utilisation des donnés personnelles ne respectent pas les règles européennes relative à la protection de ces données et de la vie privée car les fabricants sont généralement situés hors Europe, ne pas accepter ces conditions reviendrait à être privé de l'usage des fonctions du jouet.

Atlantico : Concrètement, les objets connectés sont une porte ouverte à notre intimité, quels sont les dangers liés à ce type d'objets ?
A défaut d'information de la part des fabricants et d'alerte de la part des médias, il serait, à mon avis, adapté que le consommateur reconsidère les objets numériques et particulièrement les objets connectés comme étant des équipements dont les fonctions et conséquences induites risquent de se retourner contre son utilisateur.
L'année dernière, l'association de consommateurs UFC-Que choisir a mis en garde les consommateurs sur le stockage des données. Elle a d'ailleurs saisi sur le sujet la Commission nationale de l'informatique et des libertés et la Direction générale de la concurrence, de la consommation et de la répression des fraudes.
En effet, tout ce que disent les enfants à la poupée testée est enregistré et mystérieusement stocké sur des serveurs à l'étranger et géré par la société Nuance Communications. L'Association européenne de défense des consommateurs a déclaré : « Tout ce que l'enfant raconte à sa poupée est transmis à l'entreprise, basée aux États-Unis, Nuance Communications, spécialisée dans la technologie de reconnaissance vocale ».
Quelles sont les conséquences d'un tel usage de nos données ?
L'objectif évident est le matraquage publicitaire des enfants, car certains jouets ont une certaine tendance à faire souvent allusion à l'univers de Disney ou à Nickelodeon par exemple.
Enfin, des tests ont montré qu'un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans même que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom Bluetooth par défaut du jouet connecté, permet très simplement de les identifier.
Plus grave encore… Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet.
Que ça soit en en terme d'écoute et d'espionnage à distance de l'environnement de l'enfant et de celui des parents, ou en terme de prise de contrôle à distance de l'appareil risquant de terroriser ou pire, traumatiser l'enfant, la prudence doit d'abord rester de mise.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

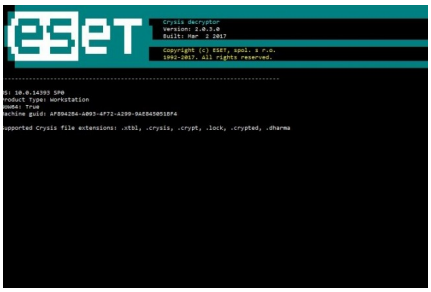
Réagissez à cet article

Source : *Jouet connecté : après un piratage, les données de 800000 familles fuitent sur le web*

Le Ransomware Dharma enfin décrypté

	Le Ransomware Dharma enfin décrypté

Les clés de déchiffrement du ransomware Dharma ainsi que toutes ses variantes ont été mises en ligne par un utilisateur. Kaspersky et Eset ont mis à jour leurs outils de lutte contre les ransomwares pour permettre à toute personne ou entreprise de déchiffrer gratuitement leurs fichiers chiffrés.



Les fournisseurs de sécurité dont Kaspersky et Eset ont mis à jour leurs outils pour permettre de déchiffrer les fichiers piégés par le ransomware Dharma. (crédit : D.R.)

C'est une belle victoire qui vient d'être remportée contre le diabolique ransomware Dharma. Les personnes ayant des fichiers chiffrés par ce programme peuvent en effet souffler car ils peuvent désormais avoir accès à des clés de déchiffrement pour pouvoir les retrouver. Apparu pour la première fois en novembre, Dharma est basé sur l'ancien programme de ransomware Crysis. Il est facile de le reconnaitre par l'ajout aux fichiers chiffrés de l'extension .[email_address].dharma. , l'adresse mail correspondant à celle utilisée par le pirate pour tenter d'extorquer sa victime.
Mercredi, un utilisateur sous le pseudonyme de gektar a publié un lien vers un post Pastbin sur le forum du support technique de BleepingComputer.com. Un post indiquant contenir les clés de déchiffrement du ransomware Dharma et de toutes ses variantes. Etrangement, la même chose s'est produite en novembre avec les clés de son prédécesseur, Crysis ce qui a permis à des chercheurs de créer des outils de déchiffrement. Aucune autre motivation que celle de mettre à disposition ces clés n'a été enregistrée concernant gektar. La bonne nouvelle est que ce leak a permis aux chercheurs de Kaspersky et d'Eset de vérifier son travail. Bingo : les deux sociétés ont mis à jour leurs outils de déchiffrement respectifs à savoir RakniDecryptor et CrysisDecryptor.

Une guerre des gangs dans les ransomwares

Cette situation devrait résonner à l'oreille des personnes touchées par des ransomwares qui ne devraient pas oublier de conserver une copie de leurs fichiers chiffrés à leur insu. Les chercheurs trouvent en effet parfois des failles dans les implémentations du chiffrement des ransomwares leur permettant de casser le chiffrement des clés. Dans d'autres cas, les autorités judiciaires et de police saisissent les serveurs de commande et de contrôle utilisés par les gangs de ransomware et publient ces clés.
Dans d'autres cas comme ici, les clés arrivent à la surface par d'autres moyens inexpliqués. Peut être parce que le développeur du ransomware a décidé de fermer boutique et décide de lâcher les clés, ou alors a-t-on à faire à une rivalité entre deux gangs de hackers qui se mettent des bâtons dans les roues pour court-circuiter l'activité des uns et des autres. Dans tous les cas, il est également recommandé de jeter un oeil sur le site NoMoreRansom.org, régulièrement mis à jour et proposant aussi bien des outils que des conseils pour lutter contre ces fichus ransomwares.

Article rédigé par Lucian Constantin / IDG News Service

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

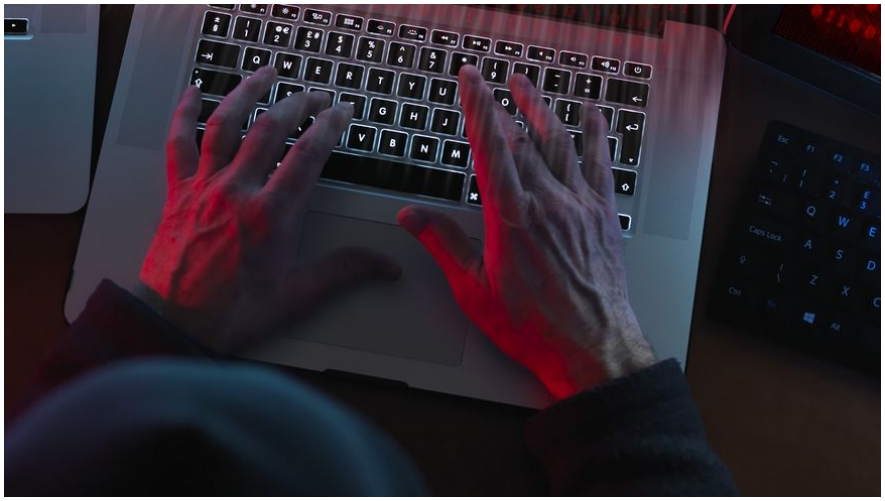
Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Un ransomware piège les Mac*

Comptes bidons, « fake news », vol de données : ces manipulations informatiques

qui pourraient perturber la Présidentielle

	Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle

Elles ont beaucoup fait parler d'elles durant la campagne présidentielle américaine : certaines pratiques malveillantes sur Internet pourraient aussi peser sur l'élection en France. Voici en quoi elles consistent.
Interview par Marina Cabiten (France Bleu)

Des pirates informatiques qui œuvrent contre Hillary Clinton, et donc en faveur de Donald Trump, le tout commandité par le Kremlin : il ne s'agit pas d'un scénario de film mais d'une accusation très sérieuse formulée par les autorités américaines lors de la campagne présidentielle. Internet est un outil puissant pour les manipulations informatiques, à différents degrés. Et la France est, selon plusieurs acteurs de la cybercriminalité, très mal préparée à ces usages détournés. Voici comment des personnes mal intentionnées pourraient perturber la campagne.

Inonder les réseaux sociaux de faux utilisateurs : l'astroturfing

Tout un chacun peut utiliser son compte Facebook ou Twitter pour s'exprimer, et éventuellement partager ses opinions politiques. Mais cette utilisation des réseaux sociaux peut être bidonnée. Ce phénomène est appelé astroturfing, du nom d'une marque de pelouse synthétique pour les stades : Astroturf. Autrement dit, il s'agit de faire prendre aux internautes du faux gazon pour de l'herbe naturelle… Comment ? **En inondant les réseaux sociaux de faux comptes automatisés, les "bots"**, qui diffusent des messages rédigés par les initiateurs de cette technique de "marketing politique" qui ne dit pas son nom, et garantit l'anonymat.
N'importe quel internaute peut créer et animer des faux comptes. Avec un peu plus de moyens financiers, il peut payer pour qu'un réseau social comme Facebook donne plus de visibilité à une page ou à un post via un algorithme qui fera apparaître le message sur davantage de "murs" d'utilisateurs, qui n'ont rien demandé. Sur Twitter, il peut acheter des "followers" (personnes qui suivent le compte) pour donner une fausse légitimité à ses comptes artificiels. Le degré ultime est de se payer un logiciel qui fait ça tout seul, voire d'employer quelqu'un pour l'exploiter. Cela existe, au sein d'entreprises privées mais parfois aussi de partis politiques. **C'est une forme de propagande de plus en plus répandue.** Le gouvernement français a annoncé récemment son intention de surveiller les réseaux sociaux pour éventuellement repérer des "mouvements" suspects de ce type.

Quand des sites partisans se font passer pour des organes de presse : les « fake news »

L'expression "Fake news", qui se traduit littéralement par « fausses informations », est très en vogue depuis la présidentielle américaine et vient de la diffusion sur Internet de prétendus articles de presse, qui ne sont en réalité pas rédigés par des journalistes. Des articles contenant des informations non vérifiées, parfois erronées, voire carrément mensongères dans le but bien précis de manipuler l'opinion.
La mécanique est la même que pour l'astroturfing, tout faire pour que ces "fake news" soient largement vues sur Facebook et les autres réseaux sociaux ou forums. Selon les calculs du site Buzzfeed, les articles relayant de fausses informations **(comme le faux soutien du pape François à Donald Trump, ou la révélation imaginaire de ventes d'armes par Hillary Clinton à l'organisation Etat islamique)** ont suscité 8,7 millions d'interactions sur Facebook durant la campagne américaine, contre 7,3 millions pour les articles de la presse traditionnelle.
En France récemment, plusieurs médias ont fait part de leur volonté de lutter contre ce phénomène, allant même pour certains jusqu'à nouer un partenariat avec Facebook et Google. ***"Le problème c'est que la rumeur court toujours beaucoup plus vite que la rectification ou la suppression du contenu"***, objecte Denis Jacopini, diplômé en cybercriminalité et sécurité de l'information, ***"laissant s'installer dans l'esprit de l'électeur ces fausses affirmations."***

De vrais contenus, mais dérobés et diffusés sans autorisation : le vol de données

La menace la plus sophistiquée reste le vol d'informations numériques. C'est l'exemple des pirates informatiques (hackers) qui ont récupéré près de 20.000 courriels de responsables du parti d'Hillary Clinton. Ils sont entrés dans les serveurs du parti démocrate dès l'été 2015, accumulant ces données parfois embarrassantes sans que personne ne s'en aperçoive, pour les publier au moment opportun pour déstabiliser le camp démocrate. Une cyberattaque venue de Russie pour aider Donald Trump à gagner l'élection, affirme la CIA dans un rapport révélé par la presse américaine. ***"Aucun parti politique français n'est actuellement protégé contre une telle malveillance"***, assure Denis Jacopini.
Selon le Canard Enchaîné (numéro du 8 février 2017), **les services secrets français s'inquiètent de cyberattaques russes** durant la Présidentielle, qui auraient pour but d'aider la campagne de Marine Le Pen. De son côté, le secrétaire général du mouvement « En Marche ! » Richard Ferrand a affirmé publiquement que les pirates russes visent particulièrement Emmanuel Macron et ont déjà attaqué à plusieurs reprises son site web.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle*

Cybersécurité dans le monde : à quoi peut-on s'attendre ?

Cybersécurité dans le monde : à quoi peut-on s'attendre ?

L'année 2016 a démontré que les mesures de sécurité traditionnelles ne suffisaient plus et que de nouvelles stratégies devaient être mises en place. 2017 va donc s'inscrire dans la continuité de ce qui a déjà été amorcé l'année passée, à savoir : toujours plus de sécurité pour toujours une protection maximisée. Les experts de NTT Security ont fait ressortir les tendances et les prévisions pour cette année qui débute.

Selon Garry Sidaway, Vice-Président Senior de la Stratégie de Sécurité

1. L'identité restera au cœur des enjeux

Au risque de nous répéter, les mots de passe fournissent aujourd'hui des garanties insuffisantes. À l'ère du digital et de la mobilité, commodité et sécurité ne font pas bon ménage. Certes, les mots de passe sont bien pratiques, mais ils sont de moins en moins perçus comme une preuve d'identité irréfutable. Devant l'utilisation croissante des smartphones et les exigences de simplicité des consommateurs et des professionnels, les solutions d'identité resteront donc au cœur des préoccupations en 2017. C'est ainsi que le mot de passe traditionnel cèdera du terrain face à la poussée du « multi-facteurs », une méthode combinant plusieurs facteurs d'authentification (localisation, possession d'un objet, d'une information, etc.). Cette association entre physique et digital, avec en toile de fond l'émergence de méthodes d'authentification avancées, favorisera le développement de nouvelles solutions de gestion des identités.

2. Le mobile sera omniprésent

Au royaume du digital, le mobile est roi. Un roi qui bouscule l'ordre établi dans de nombreux domaines, des méthodes de paiement jusqu'aux interactions sociales. Véritables hubs digitaux, nos smartphones constituent désormais non seulement une fenêtre de contrôle et d'interaction avec le monde mais aussi une interface d'identification et d'authentification. Dans un tel contexte, 2017 verra le curseur de la menace se déplacer des ordinateurs portables vers les appareils mobiles. Si, traditionnellement, les acteurs de la sécurité se sont concentrés sur les systèmes back-end et les conteneurs, ils devront revoir leur approche pour placer le mobile au cœur de leur dispositif.

3. Les entreprises surveilleront la menace interne

Le problème des menaces internes ne date pas d'hier. Côté défense, les progrès réalisés dans les domaines de l'analytique et de la détection des anomalies devraient se poursuivre en 2017. Dans un milieu de l'entreprise de plus en plus dynamique, définir les critères d'un comportement utilisateur « normal » restera un défi de taille. Toutefois, avec le développement de nouvelles techniques de machine learning, nous verrons l'analyse comportementale s'opérer directement au niveau des terminaux.

4. Fin de la détection basée sur les signatures

Antivirus nouvelle génération, solutions de sécurité des terminaux, solutions de détection et de réponse aux incidents… Peu importe leur nom, les solutions de protection des terminaux se projetteront bien au-delà de la détection basée sur des signatures statiques, à commencer par les outils d'analyses avancées que l'on retrouvera systématiquement sur ces solutions. Leur force résidera notamment dans leur capacité à exploiter la puissance du cloud pour partager l'information sur les menaces connues. La diversité et le volume sans précédent des malwares engendreront l'émergence d'une nouvelle approche. Destinée à enrayer le syndrome dit du « patient zéro », cette démarche reposera à la fois sur une collaboration internationale et l'utilisation d'une cyberveille prédictive et proactive pour libérer toute la force du collectif.

5. Le tout-en-un fera de plus en plus d'adeptes

Alors que le marché de la cybersécurité se consolide, les entreprises se tournent vers des solutions de sécurité couvrant l'intégralité des environnements TIC. Traditionnellement, la force des prestataires de sécurité managée (MSS) s'est située dans leur capacité à intégrer un maillage d'outils complexes et pointus. Aujourd'hui, la situation a changé. Tout l'enjeu consiste à intégrer le facteur sécurité à tous les échelons du cycle opérationnel de l'entreprise. Les clients chercheront donc un partenaire capable d'agir sur tous les fronts : applications métiers, infrastructure réseau, services cloud et de data center autour d'une console de gestion centralisée. En 2017, les solutions multifournisseurs apparaîtront comme datées. Les acteurs de la sécurité devront ainsi coordonner un service complet de bout en bout pour répondre aux enjeux de l'espace de travail digital.

Selon Stuart Reed, Directeur Senior Product Marketing

6. Les consommateurs exigeront plus de transparence

Une étude récente de NTT Security a mis en lumière les attentes croissantes des cyberconsommateurs en matière de transparence, tant sur le plan des pratiques que de la gestion des incidents. Ces conclusions traduisent notamment une sensibilisation accrue des consommateurs sur les questions de sécurité suite aux scandales de violations à répétition. La tendance est appelée à se poursuivre en 2017 et au-delà. Notons enfin que les entreprises dotées de politiques de sécurité et de plans d'intervention efficaces diminueront leur exposition au risque, tout en profitant d'un puissant levier de compétitivité.

7. L'innovation en moteur de consolidation

Du point de vue de l'offre comme des fournisseurs de cybersécurité, 2016 a été placée sous le signe de la consolidation. Au rang des plus grosses opérations, on citera l'acquisition de BlueCoat par Symantec, la série de rachats par Cisco et, plus proche de nous, la création de NTT Security autour de trois piliers : analytique de pointe, cyberveille avancée et conseils d'experts en sécurité. Derrière ce phénomène de consolidation, on retrouve une constante : l'innovation. Concrètement, les grandes entreprises ont racheté des spécialistes pour accéder à leurs compétences et les englober dans une offre plus aboutie. Ces grands acteurs profitent enfin d'économies d'échelle considérables – et de l'expertise et de l'efficacité qui en découlent – pour mener des programmes d'incubation qui viendront à leur tour stimuler l'innovation. Cette tendance de fond souligne bien l'importance de l'innovation pour évoluer au rythme des besoins de sécurité des clients.

8. L'identité des objets

Avec l'essor de l'IoT, la frontière entre physique et digital s'estompe peu à peu pour créer des expériences clients plus pratiques, rapides et efficaces. Seulement voilà, les cybercriminels ont eux aussi investi la sphère de l'IoT à l'affût de la moindre vulnérabilité. On a ainsi recensé des cyberattaques se servant d'objets connectés (caméras de vidéosurveillance, imprimantes…) pour lancer des attaques DDoS qui sont parvenues à paralyser des sites comme Twitter et Spotify. L'année 2017 verra sans doute une recrudescence des attaques perpétrées à l'encontre des objets connectés. D'où le besoin impérieux d'intégrer ces appareils à une politique de sécurité plus complète, notamment pour mieux contrôler l'identité et la légitimité de leurs utilisateurs.

9. L'analytique changera la donn

L'un des grands défis de la cybersécurité pourrait se résumer par cette question : comment produire une information cohérente à partir d'une avalanche de données issues de dispositifs multiples ? Si l'analyse de données a pour fonction première de « donner du sens », l'évolution des menaces doit nous inciter à revoir nos méthodes d'interprétation et de contextualisation de l'information. Dans cette optique, les outils avancés d'analyse du risque vous permettront de prendre les bonnes décisions. Au-delà des événements présents, ces outils ont pour fonction de décortiquer les données historiques pour faire ressortir des tendances, mais aussi d'utiliser l'intelligence artificielle pour identifier les schémas comportementaux annonciateurs d'une attaque. Fondées sur des technologies avancées de machine learning, des outils d'analyse automatiques et des experts en astreinte permanente, les solutions d'analytique de pointe promettent de changer la donne dans le secteur des MSS.

Selon Kai Grunwitz, Vice-Président Senior Europe Centrale

10. La cybersécurité va s'imposer comme un facteur clé de succès

Pour être reconnue comme tel par tous les acteurs concernés, la cybersécurité doit s'intégrer en amont à l'ensemble des processus métiers de l'entreprise. Dans un monde connecté où le digital gagne chaque jour en importance, les entreprises veulent pouvoir compter sur une sécurité parfaitement incorporée à leurs stratégies métiers et IT. Outre son rôle indispensable de gardienne des données sensibles, du capital intellectuel et des environnements de production, la cybersécurité sera également partie intégrante de l'innovation et de la transformation de l'entreprise.

La sécurité ne sera plus seulement le problème des DSI, mais s'invitera au cœur des processus métiers et constituera l'un des ressorts de la chaîne de valeur. Enfin, la gestion du cycle de sécurité constituera un différenciateur clé autant qu'une priorité essentielle dans le cadre d'une stratégie de sécurité orientée métiers. Elle procurera aux entreprises un avantage concurrentiel et un réel levier de valeur ajoutée.

Selon Chris Knowles, Directeur solutions

11. Le RGPD sera partout !

Si vous pensiez que le Règlement général sur la protection des données (RGPD) a été l'un des grands thèmes de 2016, attendez de voir ce que 2017 vous réserve. Alors que les fournisseurs proclameront les avantages de leurs technologies et que les équipes juridiques plancheront sur la définition d'une sécurité réellement irréprochable, les clients, eux, se lanceront dans les préparatifs.

12. Au royaume des aveugles, les borgnes sont rois… mais plus pour très longtemps !

Pour beaucoup d'entreprises, la sécurité se résume à la protection d'un périmètre au moyen de périphériques inline censés analyser l'intégralité du trafic et intervenir sur la base d'éléments visibles. Toutefois, la mobilité croissante des collaborateurs, associée à l'explosion du nombre d'applications cloud en entreprise, créent des « angles morts ». À commencer par le transit d'informations via des tunnels cryptés, le stockage et le traitement de données à l'extérieur de data centers sécurisés, ou encore les communications entre machines virtuelles qui échappent totalement à la surveillance des dispositifs de sécurité existants. En 2017, les entreprises se pencheront sur ce phénomène afin d'éliminer les angles morts et de reprendre le contrôle de leur sécurité.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Cybersécurité dans le monde : à quoi peut-on s'attendre ?*

Le piratage informatique aussi risqué pour les animaux

Le piratage informatique aussi risqué pour les animaux

Pas évident d'y penser quand on n'est pas du milieu, mais au 21ème siècle, le braconnage se joue de plus en plus sur le terrain du numérique.

Le GPS, pour le meilleur comme pour le pire

Le balisage des animaux est une pratique qui date du début du XXe siècle. **Après la pose de bagues sur les oiseaux au début du siècle, les scientifiques se sont tournés vers les transmetteurs radio dans les années 1950, avant de passer au système de suivi par satellite Argos dans les années 1970.** Aujourd'hui, c'est un autre système de suivi qu'utilisent les chercheurs : le GPS.

Cigogne équipée d'un GPS© Vasileios Karafillidis Shutterstock

Le GPS, tout le monde l'a dans son smartphone. Il nous facilite beaucoup la vie en nous aidant à nous retrouver dans une ville inconnue, en nous permettant d'appeler un taxi ou encore en nous rassurant lorsque nos enfants, rentrant seuls de l'école, utilisent leur smartphone pour partager avec nous leur localisation.

Mais au-delà de ces usages pratiques, s'en cache un plus obscur. Les balises GPS que les chercheurs placent sur les animaux ne sont pas des smartphones sophistiqués, il est donc assez facile de les pirater pour recevoir de manière indue ces données. Une faille que les braconniers exploitent à volonté, en mettant en danger la vie des animaux.

*Lire aussi : **la lutte contre le commerce en ligne de faune sauvage est engagée***

Le cyber-braconnage, un problème qui ne sera pas résolu du jour au lendemain

Le phénomène est encore trop peu connu et réservé au milieu des chercheurs…[lire la suite]

***Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.*

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

*Plus d'informations sur : **https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles***

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Le piratage informatique, un risque pour les animaux*

Les collectivités territoriales cibles des Pirates Informatiques

Les collectivités territoriales cibles des Pirates Informatiques

Si elles n'en ont pas toujours conscience, les collectivités territoriales peuvent bel et bien être victimes de cyberattaques. Et ce, pour de multiples raisons. En cas de faute avérée, les sanctions encourues peuvent devenir particulièrement difficiles à assumer.

Par Pierre-Alexandre Conte

Une République numérique. C'est ainsi qu'a été baptisée la loi portée par l'actuelle secrétaire d'Etat chargée du numérique, Axelle Lemaire, parue le 8 octobre 2016 au « Journal officiel ». Un nom ô combien symbolique et révélateur de la profondeur de la transformation vécue par l'ensemble de la société.

Celle-ci touche naturellement les collectivités territoriales, qui bénéficient des multiples avantages qu'elle génère, mais qui doivent, dans le même temps, composer avec de nouvelles obligations. Parmi elles, figure en tête de liste la sécurisation de leur système d'information.

En préambule de son rapport d'activité annuel paru en 2016, l'Agence nationale de la sécurité des systèmes d'information (Anssi) introduisait le sujet comme suit : « Les technologies numériques procurent des gains de productivité et sont donc source de richesse et de compétitivité pour notre pays, mais elles induisent également des vulnérabilités nouvelles. La cybersécurité est devenue, de ce fait, une condition structurante, non seulement de la sauvegarde de notre patrimoine économique et intellectuel, mais aussi de la protection physique de nos concitoyens. » Des propos signés Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

FOCUS

Dans son rapport d'activité concernant l'année 2015, l'Anssi explique avoir reçu 4 000 signalements, soit 50 % de plus qu'en 2014. L'Agence a aussi dû traiter une vingtaine d'incidents de sécurité majeurs.

Les sites web en première ligne

La première erreur en matière de sécurité informatique consiste à penser qu'une collectivité, quelle que soit sa nature, n'a aucune raison d'être la cible d'une attaque. C'est pourtant un raisonnement fréquemment rencontré au sein des petites et moyennes communes, qui considèrent parfois qu'elles ne détiennent rien qui puisse intéresser d'hypothétiques assaillants. « Comme tout un chacun qui dispose d'une visibilité sur internet, les collectivités territoriales peuvent faire partie des victimes d'une vague d'attaques, précise Guy Flament, référent de l'Anssi au sein de la région Nouvelle Aquitaine.

Leur présence sur internet, notamment par le biais de leurs sites web, offre des surfaces pour les attaquants, qui peuvent leur permettre d'afficher des messages de revendication ou de propagande. Ensuite, les collectivités subissent des attaques par des « rançongiciels » qui prennent en otage leur système d'information et offrent de le libérer contre une rançon. En ce qui concerne les autres menaces informatiques que peuvent être le sabotage ou l'espionnage, elles ne sont pas, pour le moment, particulièrement visées. Mais elles pourraient le devenir, notamment à cause du nombre de données à caractère personnel qu'elles hébergent. »

À LIRE AUSSI
• Plusieurs milliers de sites Internet de communes mal sécurisés

Les collectivités territoriales brassent en effet de plus en plus de données, dont certaines s'avèrent particulièrement sensibles. Elles sont au cœur de toutes les préoccupations, comme en témoignent les nombreux articles qui leur sont consacrés au sein de la loi pour une République numérique. Il convient donc de les protéger.

« Les collectivités détiennent notamment l'état civil. Il ne faudrait pas qu'un jour ces fichiers puissent être modifiés par des attaquants. Les comptes de la commune intéressent aussi les gens et tout ce qui touche aux dossiers de consultation publique », lance Guy Flament.

À LIRE AUSSI
Notre dossier : Données personnelles, un gisement sous haute protection

Sanctions pénales

La protection des données du citoyen est garantie par la loi « informatique et libertés ». C'est évidemment la Commission nationale de l'informatique et des libertés (Cnil) qui veille au respect de cette dernière. Ses compétences ont été élargies par la loi pour une République numérique.

Sur le plan financier, les collectivités encourent une amende pouvant s'élever jusqu'à 3 millions d'euros ; ce n'est pas rien ! La Cnil peut aussi ordonner que l'organisme sanctionné informe à ses frais les victimes. La loi prévoit par ailleurs la possibilité de sanctionner pénalement les maires, les présidents de conseils régionaux et de conseils généraux en cas de manquement grave, comme le fait de ne pas prendre les mesures nécessaires pour garantir la confidentialité des informations ou l'utilisation de ces dernières à d'autres fins.

A partir du mois de mai 2018, les collectivités devront appliquer le règlement européen sur le sujet. Concernant ce dernier, selon Pierre Deprez, avocat du cabinet DS avocats dans le département « droit de la propriété intellectuelle, technologies numériques et data », on parle d'un « changement de paradigme ». Cela signifie le passage « d'un régime de déclaration et d'autorisation des traitements à un régime d'accountability, d'autoresponsabilité ».

Les communes devront conserver « une trace des moyens techniques et organisationnels qu'elles auront mis en œuvre pour assurer la sécurité des données », dans le but de montrer patte blanche en cas de contrôle.

Mais les données ne sont pas l'unique préoccupation des collectivités. D'autres domaines requièrent leur attention, à l'image des objets connectés. Ce sont de formidables outils, mais ils peuvent aussi se retourner contre ceux qui les utilisent.

« Les objets connectés, comme les smartphones il y a quelques années, représentent une augmentation de la surface d'attaque puisqu'ils sont, par nature, connectés à internet. Si ces objets ne sont pas correctement configurés et sécurisés, ils offrent une porte d'entrée à d'éventuels attaquants », précise Guy Flament.

Des risques divers

« L'émergence des outils connectés implique de prendre ses précautions, déclare de son côté Olivier Fouqueau, directeur général des services d'Infocom94, syndicat intercommunal informatique du Val-de-Marne. Quand une direction générale des services techniques, voire un élu, décide que c'est super d'équiper toutes les places de parking d'un capteur pour permettre de savoir, à distance, par le biais de son téléphone portable, s'il y a une place pour se garer, mais qu'il n'y a pas de sécurité autour, cela peut très vite devenir difficile à gérer. »

Les rapports affirmant que la cybercriminalité est en constante augmentation sont rendus publics de manière quasi quotidienne. Pour autant, il n'est pas si évident de trouver une collectivité territoriale qui accepte de faire part d'une mauvaise expérience. La raison est simple : elle relève de la peur de voir son image se détériorer. C'est là l'un des principaux risques encourus, notamment par les villes.

« Il ne se passe pas une journée sans qu'il y ait un site internet défiguré dans la région », déplore le référent de l'Anssi en Nouvelle Aquitaine. En cas de pertes de données et de responsabilité avérée, le règlement européen demandera également aux collectivités, en 2018, d'informer le public quant à ses failles de sécurité. Si les communes sont concernées par leur image, elles doivent en plus composer avec l'inaccessibilité de leur site. Ce qui peut altérer de manière plus ou moins grave la mission de service public.

La perte peut aussi être financière, notamment s'il y a demande de rançon, les sommes demandées étant, la plupart du temps, élevées.

« Le sujet de la sécurité est souvent diabolisé, regrette Frank Mosser, expert dans le domaine de la cybersécurité et président de MGDIS, société éditrice de services logiciels de pilotage et de valorisation de l'action publique, basée à Vannes. Quand ça fait trop peur, on a tendance à mettre la tête dans le sac et à faire l'autruche. Il y a quelques années, ce n'était pas si grave que cela. Là, ça le devient un peu plus. »

FOCUS

Le « rançongiciel », fléau international en pleine expansion

Extorsion Tout le monde ou presque a entendu parler de Locky. Ce « ransomware » – « rançongiciel » en français – s'est rendu populaire en faisant de nombreuses victimes au cours de l'année passée. Une fois activé sur l'ordinateur de la personne visée, ce dernier chiffre les données et demande une somme d'argent en échange de leur restitution. S'il reste l'exemple le plus connu, Locky n'est pas un cas unique. Loin de là.

290 millions de dollars – Le FBI estime que durant le premier trimestre de l'année 2016, environ 209 millions de dollars ont été extorqués par le biais de « rançongiciels ». Aux Etats-Unis, le Hollywood Presbyterian Medical Center a fait partie des victimes au mois de février 2016. Paralysé pendant plus d'une semaine, il avait fini par débourser la somme de 17 000 dollars pour reprendre une activité normale. Et ce, après avoir dû envoyer de nombreux patients vers d'autres établissements.

Une mésaventure similaire est arrivée trois mois plus tard au Kansas Heart Hospital. Mais cette fois, après avoir payé la rançon, l'hôpital n'a pas pu récupérer ses fichiers. Pire, une seconde somme d'argent lui a été demandée. Fin janvier, c'est la police de Washington qui s'est aperçue que le réseau de vidéosurveillance de la ville ne fonctionnait plus correctement. Avant de prendre connaissance du problème : depuis le 12 janvier, un « ransomware » avait commencé à faire son œuvre, paralysant 123 des 187 caméras utilisées. En cherchant la source du dysfonctionnement, des enquêteurs sont tombés un peu plus tard sur un message les invitant à payer une somme. Ce qui n'a pas été fait. Le réseau a été réinstallé dans l'urgence.

FOCUS

L'expérience traumatisante d'une commune piratée

Chaque jour ou presque, des collectivités découvrent qu'elles ont été victimes d'une attaque informatique. Mais difficile de témoigner à visage découvert. Voici ce qu'une victime raconte, sous couvert d'anonymat : « Nous sommes arrivés un matin et nos postes informatiques étaient bloqués, explique cette directrice générale des services. Impossible de travailler dans ces conditions. Sur les écrans était affiché un message énigmatique et surtout, une demande de rançon. »

Si la police a rapidement été prévenue, la commune a dû se résoudre à trouver une solution au plus vite pour reprendre une activité normale. « Nous ne pouvions pas payer la somme, explique-t-elle. Nous avons appelé notre prestataire informatique qui a fait le déplacement et nous a indiqué qu'une grande partie de nos données, notamment les plus récentes, étaient perdues.

Personne n'avait anticipé le problème. Cela a créé beaucoup de remous au sein de la collectivité, dans la mesure où nous ne savons pas qui est responsable de l'attaque. L'enquête est toujours en cours. Plusieurs pistes ont été évoquées, dont des personnes hostiles à certaines décisions locales. C'est une expérience qui reste encore assez traumatisante pour nous. »

Si le prestataire informatique a fourni une solution d'appoint pour que les données soient plus fréquemment sauvegardées, aucun changement en profondeur, en termes de sécurité, n'a été apporté à ce jour.

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

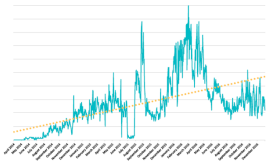
Réagissez à cet article

Source : *Cybersécurité : les collectivités territoriales, des cibles potentielles sous surveillance*

En 2016, les ransomwares sous Android ont augmenté de plus de 50%

En 2016, les ransomwarés sous Android ont augmenté de plus de 50%

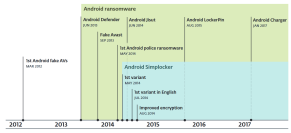
Basé sur sa technologie LiveGrid®, ESET© publie un rapport sur les menaces Android™ : sur l'ensemble des logiciels malveillants détectés en 2016, la catégorie ransomware a augmenté de plus de 50% par rapport à 2015, le plus fort taux de menaces enregistré.



Android ransomware detection trend, according to ESET LiveGrid®

« Au total, nous avons constaté **une augmentation de près de 20% des logiciels malveillants** (tous confondus) **sous Android en un an.** Sur cette plateforme, les ransomwares sont ceux qui se sont le plus développés. Selon le FBI (1), cette menace aurait rapporté jusqu'à 1 milliard de dollars aux cybercriminels l'année dernière. Avec une forte augmentation au cours du premier semestre 2016, nous pensons que cette menace ne disparaîtra pas de sitôt », déclare Juraj MALCHO, Chief Technology Officer chez ESET et qui abordera ce sujet lors du Mobile World Congress 2017.

ANDROID RANSOMWARE CHRONOLOGY



Au cours des 12 derniers mois, **les cybercriminels ont reproduit des techniques identiques à celles utilisées pour la conception de malwares infectant des ordinateurs**, afin de concevoir leurs propres logiciels malveillants sur Android : écran de verrouillage, cyrpto-ransomwares… Ainsi, ils ont réussi à développer des méthodes sophistiquées permettant de cibler uniquement les utilisateurs des différentes versions de cette plateforme.
En plus d'utiliser des techniques d'intimidation comme le « Police ransomware (2) », les cybercriminels chiffrent et cachent la charge utile malveillante sous l'application compromise, afin de rendre sa présence indétectable.
D'après les observations d'ESET, les ransomwares sous Android se concentraient sur l'Europe de l'EST puis sur les Etats-Unis en 2015, avant de migrer vers le continent asiatique en 2016. « Ces résultats montrent la vitesse de propagation de cette menace, active à l'échelle mondiale », ajoute Juraj MALCHO.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

=

Réagissez à cet article

Source : *Boîte de réception (252) – denis.jacopini@gmail.com – Gmail*

Autopsie d'un virus qui se cache dans les pixels d'une publicité

Autopsie d'un virus qui se cache dans les pixels d'une publicité

Soyez prudents ! Les pirates informatiques sont très inventifs, et là, ils nous font, une fois de plus, la démonstration qu'ils sont de plus en plus malins. En effet, un laboratoire de sécurité a découvert un logiciel malveillant qui se cache dans les pixels composant l'image d'une publicité. Ce virus profite en fait d'une faille du navigateur Internet Explorer et de Flash Player, ce petit complément vous permettant notamment d'afficher des vidéos sur les pages que vous visitez.

Et parce qu'il s'intègre dans une photo, ce virus a été baptisé Stegano, en référence à la technique de la sténographie qui permet de dissimuler des informations secrètes dans des supports anodins. Très concrètement, vous ouvrez votre navigateur, quelques clics au cours d'une recherche et vous arrivez sur une page sur laquelle va aussi s'afficher une bannière publicitaire. Et du coup, le processus d'exécution du logiciel malveillant va se mettre en route. Il va d'abord vérifier si votre navigateur lui permet de s'installer et il va aussi récolter quelques informations au sujet de votre ordinateur.
Si ces informations sont favorables à la poursuite du processus, l'image de la publicité va être remplacée par une image similaire mais légèrement modifiée. Même en zoomant, la différence n'est pas facile à percevoir. Et c'est via cette image que l'installation va se poursuivre.
Durant cette seconde phase, le niveau de sécurité de votre ordinateur va être testé. Si la voie est libre, la dernière phase consistant à installer le logiciel malveillant va se déclencher. Ce dernier permettra, par exemple, aux pirates de collecter des données personnelles ou encore d'ouvrir une porte dérobée sur votre ordinateur pour en permettre l'accès et ceci, sans attirer votre attention.
Il est aussi possible que certains des internautes touchés voient leur ordinateur infecté par un logiciel qui va crypter les données, ce qui permet ensuite aux pirates de réclamer une rançon pour obtenir la clef permettant de les récupérer…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Virus informatique: attention Stegano se cache dans les pixels d’une publicité*