Les caméras de surveillance de Washington paralysées par le Ransomware again

Les caméras de surveillance de Washington paralysées par le Ransomware again

Selon le Washington Post, un ransomware aurait paralysé pendant plusieurs jours le réseau de cameras de surveillance municipale de Washington DC. Une réinitialisation générale a permis de se débarrasser du malware.

Quelques jours avant l'investiture de Donald Trump, la ville de Washington a fait face à une mauvaise surprise : selon le Washington Post, les cameras de la ville ont été victimes d'un malware de type ransomware qui les a rendus inutilisables, empêchant l'enregistrement d'image pendant plusieurs jours.

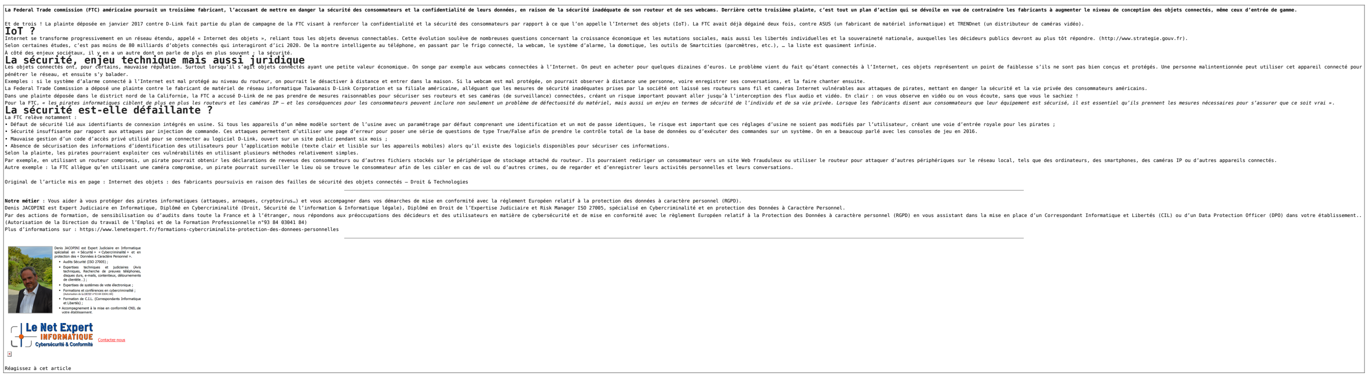
L'attaque a été détectée lorsque la police a réalisé que quatre caméras municipales ne fonctionnaient pas correctement et a contacté son prestataire informatique afin de résoudre le problème. La société a immédiatement détecté la présence de deux types de ransomware au sein des cameras, ce qui les a poussés à lancer une évaluation globale portant sur l'ensemble des appareils connectés au réseau de la ville. Au total, 123 caméras sur les 187 connectées au réseau présentaient des signes d'infection.
Les services municipaux n'ont néanmoins pas eu besoin de sortir leur porte-monnaie bitcoin pour remettre le système en route : une simple réinitialisation des cameras utilisées a permis de se débarrasser du malware et de relancer le fonctionnement. Le CTO de la ville a précisé qu'aucune rançon n'avait été payée par la ville et que le malware n'avait pas cherché à accéder au reste du réseau interne de la ville de Washington DC.
Washington s'en sort donc plutôt bien, contrairement à cet hôtel de luxe qui s'est vu contraint de payer les opérateurs d'un ransomware qui avaient bloqué l'ensemble du système de clef magnétique utilisé pour accéder aux chambres. Mais peu d'informations ont été diffusées par la ville sur la nature exacte de l'attaque, du ransomware ou même de la demande de rançon.

Réagissez à cet article

Original de l’article mis en page : Ransomware again : les caméras de surveillance de Washington paralysées – ZDNet

Des fabricants d’objets connectés poursuivis en raison de failles de sécurité

Des fabricants d’objets connectés poursuivis en raison de failles de sécurité



La Federal Trade commission (FTC) américaine poursuit un troisième fabricant, l'accusant de mettre en danger la sécurité des consommateurs et la confidentialité de leurs données, en raison de la sécurité inadéquate de son routeur et de ses webcams. Derrière cette troisième plainte, c'est tout un plan d'action qui se dévoile en vue de contraindre les fabricants à augmenter le niveau de conception des objets connectés, même ceux d'entrée de gamme.

Et de trois ! La plainte déposée en janvier 2017 contre D-Link fait partie du plan de campagne de la FTC visant à renforcer la confidentialité et la sécurité des consommateurs par rapport à ce que l'on appelle l'Internet des objets (IoT). La FTC avait déjà dégainé deux fois, contre ASUS (un fabricant de matériel informatique) et TRENDnet (un distributeur de caméras vidéo).

IoT ?

Internet se transforme progressivement en un réseau étendu, appelé « Internet des objets », reliant tous les objets devenus connectables. Cette évolution soulève de nombreuses questions concernant la croissance économique et les mutations sociales, mais aussi les libertés individuelles et la souveraineté nationale, auxquelles les décideurs publics devront au plus tôt répondre. (http://www.strategie.gouv.fr).
Selon certaines études, c'est pas moins de 80 milliards d'objets connectés qui interagiront d'ici 2020. De la montre intelligente au téléphone, en passant par le frigo connecté, la webcam, le système d'alarme, la domotique, les outils de Smartcities (parcmètres, etc.), … la liste est quasiment infinie.
À côté des enjeux sociétaux, il y en a un autre dont on parle de plus en plus souvent : la sécurité.

La sécurité, enjeu technique mais aussi juridique

Les objets connectés ont, pour certains, mauvaise réputation. Surtout lorsqu'il s'agit objets connectés ayant une petite valeur économique. On songe par exemple aux webcams connectées à l'Internet. On peut en acheter pour quelques dizaines d'euros. Le problème vient du fait qu'étant connectés à l'Internet, ces objets représentent un point de faiblesse s'ils ne sont pas bien conçus et protégés. Une personne malintentionnée peut utiliser cet appareil connecté pour pénétrer le réseau, et ensuite s'y balader.
Exemples : si le système d'alarme connecté à l'Internet est mal protégé au niveau du routeur, on pourrait le désactiver à distance et entrer dans la maison. Si la webcam est mal protégée, on pourrait observer à distance une personne, voire enregistrer ses conversations, et la faire chanter ensuite.
La Federal Trade Commission a déposé une plainte contre le fabricant de matériel de réseau informatique Taiwanais D-Link Corporation et sa filiale américaine, alléguant que les mesures de sécurité inadéquates prises par la société ont laissé ses routeurs sans fil et caméras Internet vulnérables aux attaques de pirates, mettant en danger la sécurité et la vie privée des consommateurs américains.
Dans une plainte déposée dans le district nord de la Californie, la FTC a accusé D-Link de ne pas prendre de mesures raisonnables pour sécuriser ses routeurs et ses caméras (de surveillance) connectées, créant un risque important pouvant aller jusqu'à l'interception des flux audio et vidéo. En clair : on vous observe en vidéo ou on vous écoute, sans que vous le sachiez !
Pour la FTC, *« les pirates informatiques ciblent de plus en plus les routeurs et les caméras IP – et les conséquences pour les consommateurs peuvent inclure non seulement un problème de défectuosité du matériel, mais aussi un enjeu en termes de sécurité de l'individu et de sa vie privée. Lorsque les fabricants disent aux consommateurs que leur équipement est sécurisé, il est essentiel qu'ils prennent les mesures nécessaires pour s'assurer que ce soit vrai ».*

La sécurité est-elle défaillante ?

La FTC relève notamment :
• Défaut de sécurité lié aux identifiants de connexion intégrés en usine. Si tous les appareils d'un même modèle sortent de l'usine avec un paramétrage par défaut comprenant une identification et un mot de passe identiques, le risque est important que ces réglages d'usine ne soient pas modifiés par l'utilisateur, créant une voie d'entrée royale pour les pirates ;
• Sécurité insuffisante par rapport aux attaques par injection de commande. Ces attaques permettent d'utiliser une page d'erreur pour poser une série de questions de type True/False afin de prendre le contrôle total de la base de données ou d'exécuter des commandes sur un système. On en a beaucoup parlé avec les consoles de jeu en 2016.
• Mauvaise gestion d'un code d'accès privé utilisé pour se connecter au logiciel D-Link, ouvert sur un site public pendant six mois ;
• Absence de sécurisation des informations d'identification des utilisateurs pour l'application mobile (texte clair et lisible sur les appareils mobiles) alors qu'il existe des logiciels disponibles pour sécuriser ces informations.
Selon la plainte, les pirates pourraient exploiter ces vulnérabilités en utilisant plusieurs méthodes relativement simples.
Par exemple, en utilisant un routeur compromis, un pirate pourrait obtenir les déclarations de revenus des consommateurs ou d'autres fichiers stockés sur le périphérique de stockage attaché du routeur. Ils pourraient rediriger un consommateur vers un site Web frauduleux ou utiliser le routeur pour attaquer d'autres périphériques sur le réseau local, tels que des ordinateurs, des smartphones, des caméras IP ou d'autres appareils connectés.
Autre exemple : la FTC allègue qu'en utilisant une caméra compromise, un pirate pourrait surveiller le lieu où se trouve le consommateur afin de les cibler en cas de vol ou d'autres crimes, ou de regarder et d'enregistrer leurs activités personnelles et leurs conversations.

Original de l'article mis en page : Internet des objets : des fabricants poursuivis en raison des failles de sécurité des objets connectés – Droit & Technologies

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits 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

Original de l'article mis en page : Internet des objets : des fabricants poursuivis en raison des failles de sécurité des objets connectés – Droit & Technologies

---

Comment rendre Internet plus sûr pour les jeunes ?

Comment rendre Internet plus sûr pour les jeunes ?

PartagerTwitterPartagerEnvoyer »Le Safer Internet Day est un événement mondial annuel organisé par le réseau européen Insafe, en février, pour promouvoir un Internet meilleur auprès des jeunes, de leurs parents et de la communauté éducative. »

Pour un internet plus sûr

Cette année, le **Safer Internet Day aura lieu le 7 février 2017** et se poursuivra tout au long du mois. L'objectif est de multiplier l'organisation – par les enseignants, les éducateurs, les associations de parents – d'actions de **sensibilisation sur la citoyenneté numérique** et le cyberharcèlement.

« Les cyberviolences et, plus spécifiquement, le **cyberharcèlement, sont parmi les risques les plus importants** auxquels peuvent être confrontés les jeunes internautes aujourd'hui. Alors que l'utilisation des réseaux sociaux explose, l'accent doit être mis sur la compréhension des enjeux de l'Internet, du fonctionnement de ces réseaux et de l'importance des données. »

Internet Sans Crainte est un « programme national de sensibilisation des jeunes aux enjeux de l'Internet.. Opéré par Tralalere depuis 2007, il est placé sous l'égide de l'Agence du numérique. Il fournit aux acteurs éducatifs les outils pour agir auprès du jeune public : comprendre ce qu'est Internet, **comment garder sa vie privée… privée, comment sécuriser ses recherches sur la toile,** comment se défendre en cas de cyber harcèlement…

Exemples d'actions qui vont être menées en BFC : du bon usage d'internet, le 14 février, à l'accueil periscolaire d'Esprels (70), internet sans crainte à Autun (71) le 14 mars, le Safe internet day le 7 février à Chaussin (39).

Les explications de Philippe Cayol, responsable du programme Internet Sans Crainte.

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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

Original de l’article mis en page : France 3 Bourgogne-Franche-Comté – Comment rendre Internet plus sûr pour les jeunes… tout un programme à découvrir à 9H50 le matin

---

Protéger son identité contre le vol sur Internet devrait être une priorité

Protéger son identité contre le vol sur Internet devrait être une priorité

Selon une étude concernant le vol d'identité et menée aux États-Unis par l'entreprise spécialisée dans la cybersécurité mobile Lookout auprès de 2000 clients, les délits concernant les données personnelles sont en pleine expansion. Ils constituent l'un des principaux soucis des usagers d'Internet et de la téléphonie mobile, qu'ils soient particuliers ou entreprises. Actuellement, le vol… Lire la suite

Actuellement, le vol d'identité est considéré comme un phénomène inéluctable d'après les enquêtes réalisées par Lookout. Les résultats démontrent que près de 35 % des sondées ont été victimes de vol d'identité. 41 % affirment que leurs données personnelles ne peuvent plus être sécurisées et, à un moment donné, elles seront inévitablement volées. D'ailleurs, aux États-Unis, le pourcentage d'infraction sur les identités des personnes a augmenté de près de 20 % depuis octobre 2015.

Internet : principal moyen de vol

Lookout affirme que le vol de données personnelles ne se passe plus par les méthodes classiques telles que la fouille des ordures dans les rues ou encore le vol de courrier dans les boîtes aux lettres ou il est très facile d'y trouver des informations permettant d'accéder aux numéros de carte de crédit ou de comptes divers. De nos jours, les criminels sont plus malins et bien plus discrets en usant de moyens sophistiqués et d'Internet comme les techniques de « phishing ».

Cette méthode profite de la faille humaine et non de l'informatique. Les voleurs se font passer pour une banque, un opérateur téléphonique ou une entreprise pour pousser la victime à se connecter sur leur site à travers un faux lien hypertexte. De cette manière, ils peuvent récolter des informations personnelles (des coordonnées bancaires surtout) qu'ils vont utiliser pour réaliser des achats ou des transferts d'argent vers leur compte.

En effet, l'étude menée par Lookout démontre que 60 % des Américains ont effectué à leur insu, des achats à de grandes entreprises de vente en ligne ou des transactions bancaires à cause d'une cyberattaque via de courriels frauduleux d'hameçonnage (phishing).

Les chiffres démontrés par l'étude de Lookout

D'autres chiffres révèlent aussi que les personnes ne se sentent pas en sécurité : 77 % craignent de perdre leur numéro de sécurité sociale, 74 % leurs données bancaires, 71 % leur code et carte de crédit et 56 % leurs données personnelles.

Par ailleurs, la plus grande peur des gens concerne le fait qu'ils ne soient pas immédiatement au courant du vol de leur identité au moment des actes de fraudes commises par les criminels. Selon l'enquête faite par Lookout, une personne victime d'un vol d'identité ne le découvrira que par une lettre postale (33 %), une information télévisée ou radio (31 %) ou un mail inattendu (31 %). Cela résulte du fait que les factures sur les crimes commis lui sont toujours renvoyées plus tard par mail ou par la poste.

Toujours d'après l'étude, 65 % des personnes ayant subi un vol ou une usurpation de leur identité via un site sur lequel elles se sont inscrites n'en seront averties qu'un mois après la cyberattaque. De même, 75 % des usurpés ne connaissent pas les actions à entreprendre dans de telles situations.

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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

Original de l’article mis en page : Le vol d’identité en nette progression : les données personnelles ne sont plus sécurisées

---

Des pirates informatiques demandes une rançon pour débloquer les serrures électroniques d’un hôtel de luxe

Des pirates informatiques demandes une rançon pour débloquer les serrures électroniques d’un hôtel de luxe

---

Des pirates informatiques ont utilisé un ransomware pour désactiver le système électronique d'un hôtel autrichien et demander une rançon de 1 500 euros. Il s'agit de la troisième attaque informatique qui cible l'établissement.

Des pirates informatiques ont transformé les vacances de plusieurs clients d'un hôtel autrichien en un véritable cauchemar. En effet, ils ont utilisé un ransomware qui a ciblé le système de sécurité et a désactivé les clés électroniques de l'établissement, en coinçant les touristes à l'extérieur de leurs chambres. La caisse, les ordinateurs et le système de réservation ont été également bloqués par l'attaque. L'affaire s'est déroulée au début de la dernière saison hivernale dans le Romantik Seehotel Jaegerwirt, situé près d'un lac idyllique au milieu des Alpes autrichiennes.

À vrai dire, les responsables de l'établissement affirment qu'il s'agit de la troisième attaque informatique menée par ces pirates informatiques, qui demandent chaque fois des rançons de plusieurs milliers d'euros. Cette fois, les propriétaires ont dû payer 1 500 euros en bitcoin pour pouvoir rétablir le système et réactiver les clés magnétiques.

L'ÉTABLISSEMENT AVAIT 180 CLIENTS, IL N'Y AVAIT PAS D'AUTRE CHOIX

Le directeur général de l'hôtel, Christoph Brandstaetter, explique : « L'établissement avait 180 clients, nous n'avions pas d'autre choix. Ni la police, ni l'assurance vous aide dans ce cas-là. » Payer la rançon était la solution la plus rapide et la plus efficace d'après le directeur.

Cependant, Brandstaetter ajoute avec frustration manifeste : « La réactivation de notre système, après la première attaque de cet été, nous a coûté plusieurs milliers d'euros. Nous n'avons reçu aucun remboursement de la part de l'assurance, parce que les coupables n'ont pas été trouvés. » Ainsi, l'hôtel devient malheureusement une double victime des nouvelles technologies et d'un système bureaucratique sans pitié.

Mais Brandstaetter avoue que son hôtel n'est pas un cas isolé : « Nous savons que d'autres collègues ont subi ces attaques, qui se sont déroulées de la même façon. »

Finalement, pour contraster efficacement les prochains attaques informatiques, l'équipe de l'hôtel a décidé de s'appuyer sur un système efficace. Après avoir remplacé les ordinateurs, l'établissement utilisera à nouveau des clés traditionnelles et des serrures. Et Brandstaetter de conclure : « Nous sommes en train de planifier la rénovation des chambres pour installer des serrures avec de véritables clés. Comme c'était au temps de nos arrière-grand-pères il y a 111 ans »…

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

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits 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

La CyberMenace jihadiste grandit

La CyberMenace jihadiste grandit

Un cyber-attentat de grande ampleur, qui causerait des dégâts physiques ou même des morts, n'est peut-être pas encore à la portée des groupes jihadistes mais cela pourrait changer sous peu et il faut s'y préparer, estiment des spécialistes.

D'autant qu'ils sont déjà en mesure de trouver, auprès de hackers et de mercenaires de l'ère digitale prêts à tout pour de l'argent, les capacités techniques qui leur manquent pour utiliser internet pour autre chose que de la propagande et du recrutement, ajoutent-ils.

« Daech (acronyme arabe du groupe État islamique), Al Qaïda, tous les groupes terroristes aujourd'hui : nous avons le sentiment que pour l'instant, ils ne disposent pas des compétences offensives cyber », déclare à l'AFP Guillaume Poupard, directeur de l'Agence nationale des systèmes d'information (ANSSI).

« Ces compétences sont compliquées à acquérir, même si ce n'est pas l'arme atomique. Avec quelques dizaines de personnes, un petit peu d'argent mais pas tant que ça, il y a la possibilité d'être efficace. Ils pourraient monter en compétence. Nous avons le sentiment que pour l'instant ils n'y sont pas. Ils ont d'autres soucis, et c'est compliqué pour eux », ajoute-t-il à Lille, où il a participé mercredi au 9e Forum international de la Cybersécurité.

« Les voir à court terme mener des attaques informatiques avec des impacts majeurs, on n'y croit pas trop. En revanche ça pourrait changer très vite. Notre vraie crainte, et on y est peut-être déjà, c'est qu'ils utilisent les services de mercenaires. Ce sont des gens qui feraient tout et n'importe quoi pour de l'argent », ajoute-t-il.

– Inscrit dans l'ADN –

Ce recours par des groupes jihadistes à des sous-traitants informatiques pour monter des cyber-attentats (mise en panne de réseaux électriques, paralysie de réseaux de transport ou de systèmes bancaires, prise de contrôle de sites ou de médias officiels, sabotage à distance de sites industriels critiques, par exemple), le directeur d'Europol, Rob Wainwright, l'évoquait le 17 janvier à Davos.

« Même s'il leur manque des savoir-faire, ils peuvent aisément les acheter sur le darknet (partie d'internet cryptée et non référencée dans les moteurs de recherche classiques qui offre un plus grand degré d'anonymat à ses utilisateurs, ndlr), où le commerce d'instruments de cyber-criminalité est florissant », estimait-il lors d'une table ronde intitulée « Terrorisme à l'âge digital »…[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 de formation, de sensibilisation ou d'audits 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

Nasty Android Malware that Infected Millions Returns to Google Play Store

HummingBad – an Android-based malware that infected over 10 million Android devices around the world last year and made its gang an estimated US$300,000 per month at its peak – has made a comeback.…[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 de formation, de sensibilisation ou d'audits 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 sur cette page.

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

---

80 % des entreprises françaises ont constaté au moins une cyberattaque dans

l’année

80 % des entreprises françaises ont constaté au moins une cyberattaque dans l’année

Dans son baromètre annuel fraîchement publié, le Club des experts de la sécurité de l'information et du numérique (CESIN) qui regroupe 280 responsables d'entreprises françaises, notamment celles du CAC 40, relate que 52% des responsables sécurité des systèmes d'information d'entreprises françaises (RSSI) avouent être optimistes dans la capacité de leur structure à faire obstacle aux risques d'intrusions en 2016, soit une hausse de 5% par rapport à 2015. Mais pourtant.

Le verre à moitié vide ou à moitié plein donc, puisque même si la moitié des RSSI se disent faire confiance à leur système de sécurité, la hausse perpétuelle des attaques ne fait aucun doute. D'après le CESIN, elles ont augmenté pour 46% des RSSI entre 2015 et 2016 alors que 53% s'estiment stables. Plus frappant encore, le pourcentage d'entreprises françaises recensant au moins une cyberattaque entrante dans leurs serveurs sur les 12 derniers mois, s'élève à 80%. Et c'est là que le bas blesse, il leur faut généralement en moyenne une à six heures pour détecter l'attaque et entre 3 jours et trois semaine pour corriger le système.

Des moyens de protection jugés peu efficaces

Afin d'assurer leur cyber-sécurité, 84% des entreprises vont acquérir de nouvelles solutions techniques, 55% jugeront utile d'augmenter leur budget et 44% vont accroître leur effectif, comme le rappelle La Tribune.

Si les pare-feux (91%), le VPN (89%) et le filtrage web (78%) sont jugées efficaces, les sondes de sécurité conseillées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sont jugées peu efficace (54%) ainsi que le chiffrement de base de données (60%). A ce propos, Olivier Ligneul, vice président du CESIN martèle : « Les RSSI ne peuvent plus se contenter d'être les ultra-spécialistes qui gérent les règles des pare-feux des entreprises .»

En résumé, 40% des entreprises affirment que les solutions techniques proposées par le marché ne sont pas adaptées aux différents types de menaces.

Les types d'attaques

Toujours selon le CESIN, l'attaque en tête de classement est de loin le « ransomware » soit la demande de rançon (80%), en seconde position arrive l'attaque par déni de service (40%), complète le podium les attaques virales générales (36%).

D'ailleurs à l'avenir et avec la transformation numérique, l'exposition aux attaques se multipliera notamment avec les mobiles, cloud et objets connectés, les entreprises devront ainsi revoir leur priorité en terme de protection et améliorer leur défense. Il y a du pain sur la planche.

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 de formation, de sensibilisation ou d'audits 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

Original de l'article mis en page : Baromètre CESIN : 80 % des entreprises françaises ont constaté au moins une cyberattaque dans l'année

---

GRIZZLY STEPPE – Russian Malicious Cyber Activity

On October 7, 2016, the Department Of Homeland Security (DHS) and the Office of the Director of National Intelligence (DNI) issued a joint statement on election security compromises.…[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 de formation, de sensibilisation ou d'audits 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 sur cette page.

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

GRIZZLY STEPPE – Russian

Malicious Cyber Activity

GRIZZLY STEPPE – Russian Malicious Cyber Activity

On October 7, 2016, the Department Of Homeland Security (DHS) and the Office of the Director of National Intelligence (DNI) issued a joint statement on election security compromises.…[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 de formation, de sensibilisation ou d'audits 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 sur cette page.

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