Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?

Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?

Pour exiger une rançon, des hackers pourraient pirater vos cafetières, télévisions, GPS connectés. Mais est-ce vraiment crédible ?

Les récentes attaques massives de « ransomwares », ces logiciels malveillants exigeant une rançon pour débloquer les ordinateurs qu'ils ont infectés, font craindre pour l'avenir des objets connectés, **des jouets aux téléviseurs en passant par le réfrigérateur ou la cafetière**, qui se multiplient dans nos foyers.
« Concernant l'attaque du week-end passé, il n'y a pas de risque pour les objets connectés. Elle touchait en particulier des systèmes avec Windows (…), et il n'y a pas d'objets connectés grand public aujourd'hui qui embarquent Windows pour fonctionner », assure Gérôme Billois, consultant chez Wavestone. « En revanche, il y a **déjà eu des attaques massives sur des objets connectés**« , rappelle-t-il.
Le malware (logiciel malveillant) Mirai a ainsi récemment infecté par centaines de milliers des objets connectés mal sécurisés, non pas pour les bloquer, mais **pour les transformer en zombies et créer des relais pour de futures cyberattaques**.

Transformer vos objets en mouchards

Mardi à La Haye, le jeune prodige Reuben Paul, 11 ans, a épaté une galerie d'experts en cybersécurité en piratant le bluetooth de leurs appareils électroniques pour prendre le contrôle d'un ours en peluche.
Les objets connectés sont donc des cibles tout à fait crédibles, qui peuvent aussi bien **siphonner des données** que se **transformer en mouchards**. Selon des documents révélés en mars par Wikileaks, les services de renseignement américains sont capables de « hacker » des smartphones, des ordinateurs et des télévisions intelligentes, notamment pour prendre **le contrôle de leurs micros et écouter ce qu'il se passe**.

« Tous les autres objets connectés sont piratables, ça a été démontré, que ce soit la cafetière, le réfrigérateur, le thermostat, la serrure électronique, le système d'éclairage… »Loïc Guézo stratégiste cybersécurité
…[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 : *Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ? – Sud Ouest.fr*

Cyberattaque mondiale : trois Français ont créé un logiciel anti WannaCry

Cyberattaque mondiale : trois Français ont créé un logiciel anti WannaCry

---

Il s'appelle WannaKiwi, et peut éviter le verrouillage de fichiers, mais il faut l'utiliser de tout urgence, selon ses inventeurs français

Cocorico ! Un groupe de trois Français, experts en sécurité informatique, a annoncé ce vendredi avoir mis au point un logiciel qu'ils ont nommé WannaKiwi permettant de récupérer les documents Windows cryptés par le virus informatique WannaCry, lors d'une cyberattaque massive.

« Rançongiciel », WannaCry a infecté quelque 300 000 ordinateurs dans plus de 150 pays la semaine dernière. En France, c'est principalement le groupe automobile Renault qui a été affecté, avec le blocage de chaînes de production. Une fois implanté, ce logiciel malveillant, qui utilise une faille de Windows, paralyse le système informatique en cryptant les données. Pour récupérer ces fichiers, il faut un code que les pirates fournissent (ou pas) en échange d'une rançon.

…/…

Pour télécharger WannaKiwi : https://github.com/gentilkiwi/wanakiwi/releases
Pour voir le blog d'informations (en anglais) : https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d

---

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

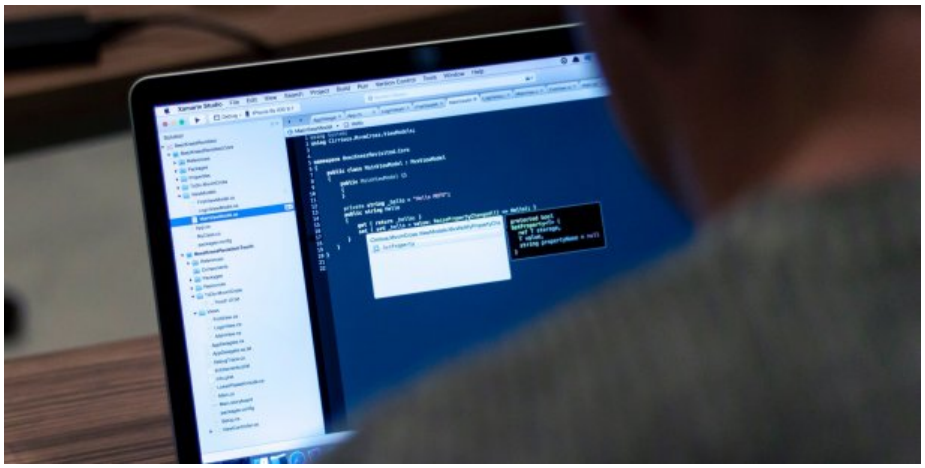
Contactez-nous

Réagissez à cet article

Source : *Cyberattaque : trois Français ont créé un logiciel*

anti WannaCry – Le Parisien

Adylkuzz, la nouvelle menace plus performante que WannaCry

	**Adylkuzz, la nouvelle menace plus performante que WannaCry**

Cette nouvelle cyberattaque, plus discrète que WannaCry serait en action depuis début mai 2017. Elle se servirait de la même faille dans le système informatique Windows pour s'infiltrer dans les données des ordinateurs.

Adylkuzz opère de façon plus invisible en créant une monnaie virtuelle dans l'ordinateur infecté avant d'envoyer cet argent à des adresses cryptées, volant les utilisateurs sans laisser de traces et sans qu'ils ne s'en aperçoivent.

« Bien que plus silencieuse et sans interface utilisateur, l'attaque d'Adylkuzz est plus rentable pour les cybercriminels. Elle transforme les utilisateurs infectés en participants involontaires au financement de leurs assaillants », explique Nicolas Godier, un expert en cyber sécurité de Proofpoint à l'AFP.

Le seul effet secondaire de ce virus est un ralentissement des performances de l'ordinateur infecté. Il est donc très difficile à diagnostiquer. Adylkuzz ferait aujourd'hui des centaines de milliers de victimes, et les sommes volées sont beaucoup plus importantes que celles de WannaCry.

***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 : *WannaCry: malgré un ralentissement de l'infection, la cyberattaque reste inquiétante*

Des hackers à l’origine de la cyber attaque mondiale menacent de divulguer d’autres failles

Des hackers à l’origine de la cyber attaque mondiale menacent de divulguer d’autres failles

Le groupe de pirates Shadow Brokers, qui avaient révélé la faille du système Windows à l'origine de la vaste opération de cyberattaque, affirme dans un message qu'il pourrait récidiver.

Le mystérieux groupe de pirates informatiques Shadow Brokers, qui a révélé en avril la faille exploitée pour mener une attaque informatique massive la semaine dernière dans le monde, a menacé d'en révéler d'autres le mois prochain.

Dans un message posté tard mardi soir sur internet, le groupe indique dans un très mauvais anglais qu'il acceptera à partir de début juin des paiements en échange desquels les souscripteurs recevront chaque mois des informations sur des techniques de piratage et des vulnérabilités informatiques…[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 : *Cyberattaque: des hackers menacent de divulguer d'autres failles*

Une intelligence artificielle pourrait comprendre la langue des dauphins d'ici 2021

Une intelligence artificielle pourrait comprendre la langue des dauphins d'ici 2021

La startup suédoise Gavagai AB développe une intelligence artificielle capable de comprendre une multitude de langues. Elle vient de lancer un projet d'une durée de quatre ans pour adapter son outil à la compréhension du langage des dauphins.…[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

WannaCrypt : une énorme épidémie de ransomwares perturbe les systèmes

informatiques du monde entier

WannaCrypt : une énorme épidémie de ransomwares perturbe les systèmes informatiques du monde entier

Une nouvelle vague de ransomwares connus sous le nom de « WannaCrypt » (détectée par ESET sous Win32 / Filecoder.WannaCryptor.D) s'est répandue dans le monde entier. Ce ransomware a infecté des dizaines de milliers d'ordinateurs. Il se propage en exploitant une vulnérabilité Microsoft® Windows dans des ordinateurs non patchés.

Touchant des centaines de milliers d'ordinateurs à travers le monde, la cyberattaque de vendredi est, de l'avis même d'Europol, « d'un niveau sans précédent ». A l'heure actuelle c'est plus de 75 000 victimes qui auraient été recensées dans le monde, parmi lesquelles le service public de santé britannique, le service de livraison FedEx, le ministère russe de l'Intérieur, des universités chinoises, l'opérateur télécom espagnol Telefonica, la compagnie ferroviaire allemande Deutsche Bahn ou encore Renault en France.

ESET® détecte et bloque la menace WannaCryptor.D et ses variantes. Le module de protection du réseau ESET bloque l'exploit au niveau du réseau. **ESET a alerté ses utilisateurs sur son site Internet. Toutes les instructions, étape par étape, sont renseignées pour qu'ils s'assurent d'être correctement protégés contre cette menace.**

Pour ESET, la sécurité du client a toujours été sa priorité. L'éditeur recommande aux utilisateurs de mettre à jour de manière proactive leurs systèmes d'exploitation, et de faire preuve de prudence lors de l'ouverture des pièces jointes. Dans ses solutions, ESET recommande d'activer LiveGrid.

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

Cyberattaque mondiale par le cryptovirus Wannacrypt. Pourquoi changer une équipe qui gagne ?

Cyberattaque mondiale. Pourquoi changer une équipe qui gagne ?

Des dizaines de milliers d'ordinateurs dans une centaine de pays ont été infectés depuis vendredi par un rançongiciel ou ransomware appelé Wannacry.
Denis JACOPINI Interviewé par RFI et propos personnels

De quoi s'agit-il ? comment ça marche ?
Depuis vendredi 12 mai 2017, une cyberattaque d'envergue mondiale a touché des dizaines de milliers d'ordinateurs. En fait, peut-être beaucoup plus d'ordinateurs on été infectés car il ne s'agit qu'un nombre estimatif…
Les ordinateur en question ont été infectés par un virus qui s'est introduit dans les systèmes informatiques au travers de la messagerie électronique et d'e-mails.
Ce type de virus, une fois introduit et activé bloque l'usage de votre ordinateur ou de votre système informatique en cryptant vos données. une fois vos données cryptées, un message vous invite à payer une somme d'argent en échange du code qui vous permettre de décrypter vos fichier et de les rendre à nouveau utilisables.
Le virus crypteur de données auquel nous avons à faire face s'appelle **WannaCry** (probablement un nom de ransomware qui est la contraction de Want a cryt).

Quelles suites peut-on donner à ce type d'attaques d'un point de vue judiciaire ?
Dans un monde idéal, il vous suffirait d'aller porter plainte à la Police ou à la Gendarmerie avec les preuves techniques à votre disposition pour qu'une enquête soit ouverte, que l'auteur du pirate soit recherché, retrouvé, arrêté, puis que son matériel saisi.
Des cas précédents ont montré que grâce à ça, des enquêteurs ont réussi à retrouver des clés de décryptage pour les mettre à disposition des victimes sur des sites internet spécialisés comme nomoreransom.org.
Malheureusement, la réalité bien différente. Il est essentiel de recueillir les preuves de cette attaque (ne serait-ce que pour votre assurance et porter plainte), mais une fois la plainte déposée il peut se passer plusieurs plusieurs mois ou plusieurs années avant de retrouver un pirate.

Dans ce grand désarrois certains décident de payer la rançon aux pirates pour récupérer l'accès à leurs données mais malheureusement peux nombreux seront qui auront satisfaction.
Dans le cas de cette cyber attaque mondiale, vu que le parquet de Paris se saisit de cette affaire, les choses devraient bouger plus vite.
Les chefs d'accusation qui peuvent être retenus contre les auteurs de cette d'attaque sont ;
• « accès et maintien frauduleux dans des systèmes de traitement automatisé de données », (deux ans d'emprisonnement et 30 000 euros d'amende et trois ans d'emprisonnement et 45 000 euros d'amende lorsque l'accès ou le maintien a entraîné une altération du système),
• « entraves au fonctionnement » d'un système de traitement automatisé de données (cinq ans d'emprisonnement et de 75 000 € d'amende);
• et « extorsions et tentatives d'extorsions ».

N'est-on pas protégé contre cette forme d'attaque ?
Depuis des dizaines d'années, pirates informatiques et forces de l'ordre jouent au chat et à la souris. La quasi totalité les victimes ayant fait les frais de telles attaques numériques se sont bien rendu compte qu'elle ne recevraient d'aide ni de la Police, ni de la Gendarmerie pour avoir réparation. Particuliers, entreprises, TPE, libéraux PME et même grandes entreprises ayant été piégées par de telles attaques informatiques devraient se poser des questions sur les compétences de leurs informaticiens.
Spécialisés pour être au service de leurs client pour gérer des parcs informatiques, ils assurent l'assistance, la maintenance, l'infogérance, mais pas la sécurité !
Assurer la sécurité informatique et plus particulièrement la sécurité de vos données est un métier à part entière et doit couvrir aussi bien des domaines techniques que pédagogiques pour amener les utilisateurs à faire évoluer leurs réflexes face aux usages du numériques.

Pourquoi changer une équipe qui gagne ?
Le premier virus qui a demandé une rançon date de 1989 et s'appelle PC Cyborg. Certes, il n'y avait pas encore l'Internet qu'on connaît aujourd'hui, mais déjà un mode opératoire habile destiné à tromper la vigilance de l'utilisateur était utilisé.
Depuis que l'internet s'est répandu, les techniques de propagation sont désormais différentes et peuvent s'adapter au support infecté (smartphone, tablette, PC, Mac et aussi objet connecté) mais la techniques pour s'introduire dans les réseau est depuis toujours la même dans la très grande majorité des cas. Même les virus, ransomwares (rançongiciels) les plus perfectionnés utilisent le bon vieil e-mail piégé ou le site Internet piégé pour s'introduire dans un réseau informatique. Les technique de camouflage, de dissimulation et de propagation vers les autres équipements du réseau peuvent par contre, elles, être extrêmement perfectionnées, mais les techniques pour pénétrer un système sont quant à elles quasiment systématiquement les mêmes.
Pourquoi faire autrement quand cette technique fonctionne encore !

Comment alors contrer de telles attaques ?

La solution n'est pas seulement technique. Certes il faut utiliser des logiciels de sécurité adaptés, mettre en place (et suivre !) des procédures de gestion de sécurité de parc rigoureuses mais ce qui nous paraît essentiel est le changement de comportement des utilisateurs.
C'est pour cela que nous proposons des formations dans le but de changer les réflexes des utilisateurs face à un e-mail, un site internet ou un appel téléphonique suspect. Nous apprenons à nos stagiaires à quoi ressemble le loup afin qu'ils évitent à l'avenir de le faire rentrer dans la bergerie.

Qui se trouve derrière ces attaques ?
Enquêteurs et experts informatiques internationaux sont lancés sur les traces des pirates informatiques à l'origine de cette cyberattaque. L'attaque est « d'un niveau sans précédent » et « exigera une enquête internationale complexe pour identifier les coupables », a indiqué l'Office européen des polices Europol, en précisant qu'une équipe dédiée au sein de son Centre européen sur la cybercriminalité avait été « spécialement montée pour aider dans cette enquête, et qu'elle jouera un rôle important ».
On évoque désormais « 200.000 victimes dans au moins 150 pays » (d'après Rob Wainwright, le directeur d'Europol) visés par les pirates informatiques et de nombreuses entreprises ou services publics reconnaissaient avoir été touchés ou avoir fait l'objet d'attaques. Mais il faudra attendre lundi et la réouverture des entreprises pour dresser un bilan plus complet de cette attaque, a-t-il prévenu.

Selon nous, si la vague de cyberattaques lancée vendredi semble marquer le pas, de nouvelles offensives sont à craindre. Une version encore plus redoutable de **WannaCry** risque bien d'arriver. En espérant que les OIV ne soient pas cette fois touchés.

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

Le facteur humain, clé de la cybersécurité

Le facteur humain, clé de la cybersécurité

La plupart des cyber-attaques exploitent le facteur humain pour s'introduire dans le système d'information des entreprises. L'envoi d'un email piégé (phishing) ou la distribution de clé USB infectée sont souvent beaucoup plus efficaces que nombre de techniques d'attaque dites « avancées ».

Par Matthieu Garin

Fort de ce constat, les grandes entreprises ont compris depuis longtemps l'enjeu que représente la sensibilisation de leurs employés. A quoi bon avoir les mécanismes de sécurité les plus robustes si les employés sont prêts à cliquer sur n'importe quoi

Des employés déjà très sensibilisés

Les plans d'actions de sensibilisation se sont multipliés pour traiter le problème : sessions plénières, campagnes d'affichage, pages dédiées sur l'Intranet… beaucoup d'initiatives, pour des résultats malheureusement décevants. Faites le test : il suffit de demander à un employé s'il sait qui contacter en cas de mail suspicieux pour mesurer le chemin qu'il reste à parcourir.

Mais alors comment peut-on améliorer la situation ? La réponse est dans la sémantique : **il ne s'agit plus de sensibiliser à la cybersécurité (les médias s'en chargent) mais de former les employés pour qu'ils acquièrent les réflexes qui sauvent…**[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.

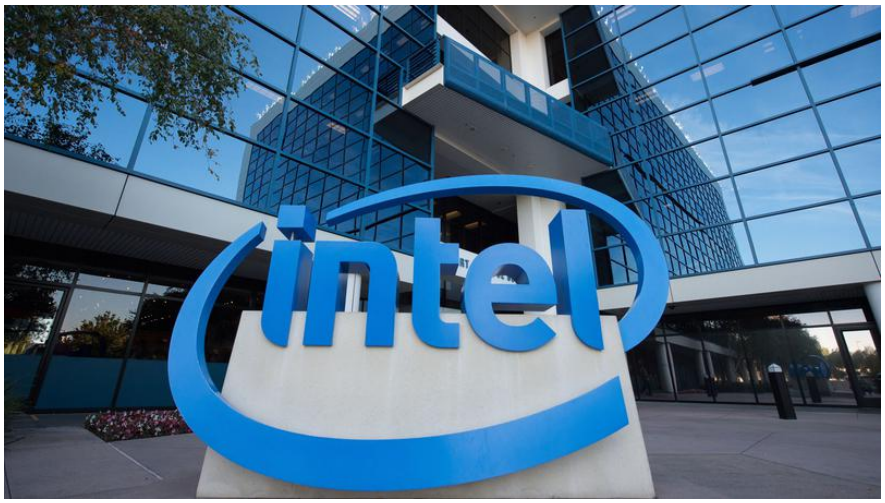
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Le facteur humain, clé de la cybersécurité – Le blog Expectra*

Faille de sécurité dans les processeurs Intel pour les ordinateurs professionnels



Faille de sécurité dans les processeurs Intel pour les ordinateurs professionnels

Une faille de sécurité majeure a été repérée sur les processeurs d'Intel. Elle permettrait la prise de contrôle de serveurs et d'ordinateurs d'entreprise.
Depuis 2008, les puces d'Intel comportaient une faille de sécurité. Le géant américain de l'électronique a publié lundi une annonce et une mise à jour afin de corriger le problème. Cette erreur de conception touche une grande partie des processeurs de la marque allant du Nehalem (2008) à Kaby Lake (2017), intégrés sur les PC professionnels. Les entreprises dotées de ces ordinateurs doivent, par contre, mettre à jour rapidement leur système.
La faille est située au niveau du programme «Active Management Technology». Il permet aux administrateurs accrédités d'accéder et de gérer des flottes d'ordinateurs à distance, ce qui explique pourquoi la faille touche les gammes professionnelles. Selon le site SemiAccurate, des hackers pourraient prendre le contrôle de l'intérieur et agir comme bon leur semble. Les informations présentes sur certains serveurs et les PC sont donc exposés à ces attaques. Les propriétaires d'ordinateurs équipés de puces Intel et issus de la grande consommation n'ont rien à craindre, selon Intel…[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 : *Intel révèle une faille de sécurité dans ses processeurs*

Nouvelle campagne mondiale de lutte contre le cyber-harcèlement de l’Organisation des Nations Unies

© Dariusz Sankowski

Nouvelle campagne mondiale de lutte contre le cyber-harcèlement. de l’Organisation des Nations Unies

Une réunion de parties prenantes sur la création d'une nouvelle campagne mondiale de lutte contre le cyber-harcèlement et d'un cadre pour un espace en ligne sûr s'est tenue à Londres les 26 et 27 mars 2017.

Partout dans le monde, les enfants et les adolescents se connectent de plus en plus par des moyens électroniques tels que téléphones, Internet, réseaux sociaux, applications et jeux en ligne. Pour la plupart, ces expériences en ligne sont positives, mais il arrive malheureusement que certaines soient négatives. De nombreux comportements négatifs qu'ils peuvent rencontrer dans le monde réel peuvent aussi se produire en ligne. Parmi les exemples de cyber-harcèlement figurent les messages de texte, les courriers électroniques, les images ou les vidéos malveillants, non voulus ou gênants et cela peut aussi prendre une forme plus subtile telle que l'exclusion.

Les jeunes sont les plus touchés par la violence en ligne

Une recherche de Microsoft réalisée en 2016 auprès d'adultes et d'adolescents de 14 pays montre que 65 % des répondants avaient été victimes d'au moins un risque en ligne, en particulier de contact non voulu…[lire la suite]

Réagissez à cet article

Source : *Nouvelle campagne mondiale de lutte contre le cyber-harcèlement | Organisation des Nations Unies pour l'éducation, la science et la culture*