Un pirate informatique réclame une rançon pour ne pas dévoiler la prochaine saison de la série Orange Is the New Black

Un pirate informatique réclame une rançon pour ne pas dévoiler la prochaine saison de la série Orange Is the New Black

Un pirate informatique affirme s'être procuré illégalement la prochaine saison de la série de Netflix Orange Is the New Black. Il réclame à la plateforme le paiement d'une rançon pour ne pas dévoiler le contenu des nouveaux épisodes de la fiction à succès.

L'auteur du chantage, qui se fait appeler The Dark Overlord, aurait déjà mis en ligne plusieurs épisodes sur un service de partage de fichiers illégal. The Associated Press n'a pas été en mesure de confirmer l'authenticité des fichiers en question. On ne connaît pas non plus le montant réclamé.
Les nouveaux épisodes de la cinquième saison de la série qui se déroule dans une prison pour femmes doivent être diffusés sur Netflix le 9 juin. La bande-annonce a été dévoilée le 8 février dernier.
Un éventuel piratage de l'une des séries à l'origine de la popularité de Netflix pourrait avoir des conséquences sur le nombre d'abonnés de la plateforme. La valeur financière de l'entreprise pourrait alors se trouver en danger…[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 : *Un pirate informatique réclame une rançon à Netflix | ICI.Radio-Canada.ca*

L’impossibilité de détecter la source d’une cyberattaque permet de désigner les coupables

L’impossibilité de détecter la source d’une cyberattaque permet de désigner les coupables

Se prononçant sur les accusations infondées concernant l'ingérence russe dans la politique d'autres pays, le chef de l'état-major général russe Valeri Guerassimov a fustigé les pays occidentaux pour avoir déclenché une guerre informationnelle.

L'impossibilité de détecter la source d'une cyberattaque permet de désigner les coupables, a déclaré le chef de l'état-major général russe Valeri Guerassimov lors d'une Conférence sur la sécurité internationale qui se déroule aujourd'hui à Moscou.
« L'Alliance a commencé à mettre au point l'application de l'article 5 du Traité de Washington (concernant la défense collective, ndlr.) dans le cas des cyberattaques sur les dispositifs matériels des systèmes étatiques et militaires des pays membres de l'Otan. Mais dans les conditions actuelles, il est presque impossible de détecter les sources réelles de ces attaques. À cet égard, il est possible de désigner les responsables sans avoir de preuve et d'agir sur eux par des moyens militaires », a déclaré le chef de l'état-major général russe.
« Les pays occidentaux intensifient la guerre informationnelle agressive déclenchée contre la Russie. Si on regarde les articles des médias européens et américains, il semble que presque tous les événements négatifs dans le monde soient orchestrés soit par les services spéciaux russes, soit par des hackers russes », a indiqué Valeri Guerassimov….[lire la suite]

Réagissez à cet article

Source : *L'impossibilité de détecter la source d'une*

cyberattaque permet de désigner les coupables

Est-ce que le vote électronique des élections Françaises est fiable ?

Le vote électronique : nouvelle preuve de manipulation des élites qui peuvent en deux temps trois mouvements truquer les votes comme bon leur semble …

Pendant les élections Françaises, les scellés appliqués sur la machine à voter et l'expertises des systèmes de votes électroniques réalisées par les experts indépendants respectant les **recommandations de la CNIL dans délibération n° 2010-371 du 21 octobre 2010 relative à la sécurité des systèmes de vote électronique** garantit le respect de l'intégrité et de la confidentialité des scrutins.
[block id="24761" title="Pied de page HAUT"]

A Lire aussi :
Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.
Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.
Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *LE VOTE ELECTRONIQUE = ESCROQUERIE ! – Agoravox TV*

Comment se protéger du smishing ?

Comment se protéger du smishing ?

Pour rappel Smishing est la contraction de SMS et de Phishing. On l'appelle également Hameçonnage par SMS.

Lorsque vous utilisez votre téléphone, appliquez des précautions de base, par exemple :
• Ne cliquez pas sur les liens que vous recevez sur le téléphone sauf si vous connaissez la personne qui vous les envoie.
• Même dans ce cas, si vous recevez d'un ami un SMS contenant un lien, avant de cliquer sur ce lien, assurez-vous que cet ami vous l'a bien envoyé.
• Les suites complètes de sécurité Internet ne sont pas réservées aux ordinateurs portables et aux PC. Elles trouvent également toute leur utilité sur votre téléphone mobile.
• Un VPN est également une possibilité à envisager pour vos appareils mobiles. Le VPN sécurisera et cryptera toutes les communications intervenant entre votre mobile et Internet.
• N'installez jamais d'applications à partir de SMS. Vous ne devez installer sur votre appareil que des applications en provenance directe de l'app store officiel. Ces programmes ont été testés de manière rigoureuse avant d'être autorisés sur le marché.
• Pratiquez le principe de précaution. En cas de doute sur la sécurité d'un SMS, ne l'ouvrez pas.

La quasi totalité des SMS que vous recevez est sans problèmes. Mais il suffit d'un mauvais SMS pour totalement compromettre votre sécurité. Un peu de bon sens vous évitera de vous faire dérober votre identité.

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 : *Qu'est-ce que le smishing ?*

Les présidentielles ne seront

pas affectés par une cyberattaque

Les résultats des présidentielles ne seront pas affectés par une cyberattaque

Le directeur de l'agence nationale de la sécurité des systèmes d'information a tenu à se montrer rassurant sur la solidité du système informatique qui sera utilisé lors de l'élection présidentielle pour collecter et remonter le vote des Français, alors que des craintes de piratage subsistent.

À quelques jours du premier tour de l'élection présidentielle française, faut-il craindre des résultats faussés par une attaque informatique venue de l'étranger pour favoriser tel ou tel candidat, ou au contraire nuire à l'un d'entre eux ? Cette perspective tout à fait inquiétante pour le bon fonctionnement de la démocratie est prise très sérieux à Paris, surtout depuis les incidents qui ont émaillé la campagne électorale américaine.

Guillaume Poupard

Mais pour Guillaume Poupard, directeur général de l'agence nationale de la sécurité des systèmes d'information (Anssi), il n'y a pas de raison de s'alarmer outre mesure. Si des menaces planent effectivement sur le scrutin, des mesures ont été prises tout au long de ces derniers mois pour éviter un scénario à l'américaine. Ou en tout cas en réduire la portée et la probabilité.

« *Le réseau propre du ministère de l'intérieur va être robuste pour être capable de travailler* », a-t-il confié jeudi 20 avril au micro de France Inter. « *On a fait un travail de qualité, je pense, de manière à résister à ces nouvelles menaces* » qui pourraient fausser la sincérité du vote. Tous les maillons de la chaîne informatique servant au processus ont ainsi été renforcés lorsque cela s'est avéré nécessaire.

« *Tous les réseaux informatiques qui vont notamment collecter les résultats, qui vont les additionner, pour au final donner dimanche soir les premières tendances puis les résultats définitifs, ces réseaux ont été durcis là où il le fallait* », a insisté M. Poupard. Et d'ajouter « *[qu'on s'est] assuré que les autres réseaux informatiques qui vont être impliqués dans l'élection seront bien opérationnels le jour de l'élection* »…[lire la suite]

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?
La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle
Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.
Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.
Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *Présidentielle : l'Anssi assure que les résultats ne seront pas affectés par une cyberattaque – Politique – Numerama*

Les données de santé des

Français désormais en libre accès

Les données de santé des Français désormais en libre accès

Dans un communiqué du 10 avril 2017, le gouvernement a indiqué qu'il ouvrait l'accès aux données issues du Système national des données de santé (SNDS) aux organismes exerçant une mission de service public pour toute étude, recherche et évaluation présentant un intérêt public. Ces organismes peuvent désormais consulter et exploiter les données du SNDS suivant certaines conditions détaillées dans le décret du 26 décembre 2016.

Ainsi, comme le précise le gouvernement :

• L'État, l'Assurance maladie, l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), la Haute Autorité de santé (HAS) ou encore Santé publique France peuvent accéder aux données du SNDS de manière permanente pour leur permettre d'assumer leurs missions

• Les équipes de recherche des centres hospitaliers universitaires (CHU), de l'Institut national de la santé et de la recherche médicale (INSERM) et des centres de lutte contre le cancer peuvent désormais consulter l'échantillon correspondant à 1/100ème de la population.

• Les autres organismes publics ou privés, à but lucratif ou non lucratif, auront eux aussi prochainement accès aux données issues de cette base pour toute étude, recherche et évaluation présentant un intérêt public. Ils seront, eux-aussi, soumis aux conditions précisées dans le décret du 26 décembre 2016

La loi interdit l'usage de ces informations pour deux finalités :

• La promotion commerciale des produits d'assurance santé

• La modulation des contrats d'assurance santé (évolution des primes, exclusions,…

Toutefois, cette annonce suscite des craintes et la réprobation, notamment chez certains acteurs de la santé.

Ainsi, la Fédération des Médecins de France – syndicat qui regroupe près de 3000 adhérents – s'oppose à cette mesure. *« Si la loi autorise des accès à cette vaste base de données au nom de la recherche et annonce la future possibilité à des entreprises lucratives de pouvoir y accéder également, la FMF rappelle que les données du SNDS ne seront pas anonymisées mais seulement pseudonymisées avec une possibilité d'identification. »* explique le syndicat dans un communiqué.

La FMF alerte :

– du risque élevé de perte de confidentialité de leurs données personnelles, soit en raison du piratage, soit en raison du nombre élevé de personnes potentiellement concernées par l'accès aux données du SNDS. La CNIL elle-même a estimé que « le niveau de sécurité envisagé ne sera pas atteint au lancement du traitement SNDS en mars 2017 »[1]. Bien que la loi prévoie un agrément très sévère pour les hébergeurs de données de santé, les mini serveurs de données, de radiologie ou de biologie, permettant un accès rapide aux résultats, ne sont pas tous agréés, et leur accès est très modérément protégé...[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 : *Les données de santé des Français désormais en accès libre –*

Est-ce que Linky aspire nos données personnelles ?

Est-ce que Linky aspire nos données personnelles ?

Linky, un compteur qui ne vous veut pas que du bien ! Ce boitier qui doit être installé dans tous les foyers relèvera en direct et à distance vos habitudes de consommation d'électricité.

Par ailleurs, des incidents ont lieu lors de la pose de ces compteurs, notamment lorsque des personnes s'y opposent : à Plouha et dans sa région récemment, plusieurs incidents ont été constatés, avec notamment une dame de 73 ans bousculée par un installateur alors qu'elle s'opposait à l'installation.
Avec le prétexte d'établir une facture plus précise, EDF prévoit de remplacer 90% des anciens compteurs en 4 ans. Un changement qui suscite de vives polémiques. En effet, de nombreuses communes s'opposent à l'installation de ce compteur dit intelligent. Si l'efficacité et le risque de surcoût sont remis en question, la menace d'intrusion dans la vie privée est également pointée du doigt.
En effet, par son système de collecte de données à distance, le compteur Linky est un véritable concentré d'informations personnelles. Il est techniquement capable de recueillir les index journaliers et la courbe de charge, c'est-à-dire un relevé précis de la consommation électrique de l'utilisateur. Ces données permettent de déduire des informations sur les habitudes de vie des consommateurs.
Des millions de Français seront concernés et des millions de données personnelles seront stockées par ERDF, qui souhaite entrer dans la danse du commerce d'informations, le Big Data. Pas étonnant, car cette mine d'or peut rapporter très gros. En effet, elle fait l'objet d'un véritable business, estimé à plusieurs milliers de milliards d'euros…[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 : *Linky, vendeur de données personnelles –*

Voyagez aux Etats-Unis et laissez vos données être espionnées

Voyagez aux Etats-Unis et laissez vos données être espionnées

---

L'administration Trump envisage de demander aux voyageurs arrivant aux Etats-Unis l'accès aux données de leur smartphone et à leurs comptes Twitter, Facebook ou LinkedIn. Une sévère menace pour la cybersécurité des entreprises européennes.

Cette fois-ci, la côte d'alerte est clairement franchie. Dans ses colonnes, le *Wall Street Journal* évoque un projet de l'administration Trump qui pourrait forcer les visiteurs arrivant aux Etats-Unis à communiquer aux autorités les contacts et contenus présents sur leur téléphone mobile ainsi que les mots de passe de leurs comptes de réseaux sociaux, permettant d'accéder aux messages privés envoyés sur ces canaux. Un projet qui ne serait pas limité aux pays soumis aux règles de sécurité les plus strictes – et dont les ressortissants doivent obtenir un visa -, mais concernerait aussi les pays considérés comme des alliés des États-Unis, dont la France.
Rappelons que, pour se rendre de façon temporaire sur le sol américain, pour affaires ou en tant que touriste, les Français doivent déjà solliciter une autorisation électronique (Esta), valable 2 ans. En février, le ministre de l'Intérieur américain (Homeland Security) avait déjà évoqué, lors d'une audition devant le Sénat, le fait que les voyageurs étrangers (notamment issus des 6 pays blacklistés par un décret de l'administration Trump) venant aux États-Unis seraient tenus de fournir leurs mots de passe sur les médias sociaux aux autorités d'immigration avant de rentrer sur le territoire américain.

La peur de l'espionnage économique

Selon le *Wall Street Journal,* cette mesure serait donc étendue à d'autres pays et aussi aux contacts téléphoniques. « *S'il existe un doute sur les intentions d'une personne venant aux États-Unis, elle devrait avoir à prouver la légitimité de ses motivations, vraiment et véritablement jusqu'à ce que cela nous satisfasse* », a expliqué le conseiller principal du Homeland Security, Gene Hamilton, cité par le quotidien économique.
Si la question ne manquera pas de soulever de vifs débats sur le sol américain et entre les États-Unis et ses partenaires et si une procédure de la sorte pose également quelques questions pratiques assez épineuses, la perspective risque d'échauder de nombreuses entreprises européennes. Car, les activités des services de renseignement US associent sans vergogne antiterrorisme et espionnage économique au profit des entreprises américaines. Une porosité d'ailleurs assumée, comme l'ont montré de nombreux documents dévoilés par Edward Snowden ou *Wikileaks* et révélant les activités de la NSA en matière d'espionnage économique. Les activités de cette nature ne sont d'ailleurs pas limitées à la seule agence de Fort Meade, mais s'étendent à toute la communauté du renseignement aux Etats-Unis.
Au passage, les mesures envisagées par l'administration Trump signeraient probablement l'arrêt de mort du Privacy Shield, l'accord transatlantique sur les transferts de données qui succède au Safe Harbor. Pour mémoire, ce dernier érige comme credo le fait que les données des citoyens européens exportées aux Etats-Unis bénéficient de la même protection que celle que leur accorde le droit européen. En février, les CNIL européennes s'étaient déjà inquiétées des conséquences possibles du décret sur l'immigration du Président Trump sur cet accord…[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 : *L'entrée aux Etats-Unis conditionnée par les données des smartphones ?*

Ce vibromasseur connecté muni d’une caméra est vraiment trop facile à hacker

Ce vibromasseur connecté muni d’une caméra est vraiment trop facile à hacker

Oui, évidemment on se demande bien qui voudrait hacker ce type d'objet, pour visionner ce type d'images. Mais ainsi va le monde : le Wi-fi de ce vibromasseur connecté se pirate en deux clics.

On ne le dira jamais assez, mais une connexion WiFi est une porte d'entrée royale pour n'importe quel hacker. Même fermée, elle est très simple à pirater. Ensuite, le pirate peut avoir accès à l'ensemble des données du trafic internet de l'objet connecté.

Photos, identifiants, mots de passe pour un téléphone, mais aussi flux *streaming* pour ce vibromasseur connecté. S'il vient à être piraté, c'est une tout autre intimité qui peut être violée.

Vibromasseur avec hot spot WiFi

Le vibromasseur Svakom Siime Eye (disponible au prix de 249 dollars) dispose du WiFi et d'une caméra intégrée pour procéder à des *livestreams*. Les chercheurs en sécurité de Pen Test Partners ont découvert que l'interface de l'objet connecté était très simple à hacker pour toute personne se trouvant à portée de la connexion WiFi (et pourvu d'un minimum de connaissance en la matière, cela s'entend).
Un piratage d'autant plus facilité que le mot de passe par défaut de ce point d'accès WiFi est « 88888888 », soit 8 fois le chiffre 8.

Un piratage enfantin

N'importe quelle personne à proximité du signal peut accéder au flux vidéo. Pire, en poussant leur investigation un peu plus loin, ces chercheurs sont parvenus à accéder au serveur web et à la racine de l'appareil pour configurer une connexion à distance.

Les utilisatrices qui voudraient partager ces instants intimes avec leur partenaire, pourraient se retrouver à faire de même avec leur voisin de palier. Une perspective peu réjouissante.
Le fondateur de Pen Test, Ken Munro, explique qu'il a tenté de contacter la compagnie pendant des mois avant de rendre publique ces informations.
Ce n'est pas la première fois que ce type d'objet connecté est mis au ban : le mois dernier, la société canadienne Standard Innovation a été condamnée à verser 3 millions de dollars à ses clientes pour avoir omis de mentionner qu'elle collectait leurs données personnelles via leur vibromasseur connecté et l'application dédiée.
Auteur : Elodie

Réagissez à cet article

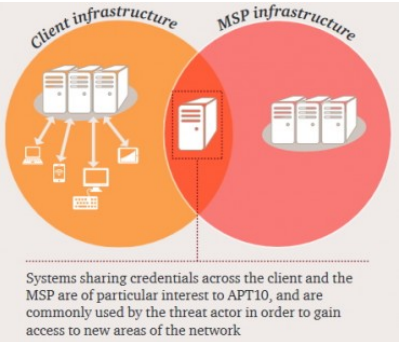
Source : *Ce vibromasseur connecté muni d'une caméra est vraiment trop facile à hacker*

Les services Cloud au centre d'attaques d'entreprises par APT10

Les services Cloud au centre d'attaques d'entreprises par APT10

Le groupe de pirates chinois APT10 a infiltré des services Cloud managés pour remonter aux serveurs des entreprises qui les utilisent.

La maturité des attaques ciblées contre les entreprises est montée d'un cran. *« Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience »*, a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme *« l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées »*. Pas moins.



De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. *« PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles »*, indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne…[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 : *Les services Cloud au centre d’attaques d’entreprises par APT10*