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

Allocab condamné par la Cnil

	Allocab condamné par la Cnil

---

La police de protection des données personnelles en ligne vient de condamner la société Allocab à verser une amende de 15 000 euros. L'entreprise de VTC aurait mal protégé et conservé certaines données bancaires de ses utilisateurs sans tenir compte des avertissements de la Cnil, dont le verdict est tombé ce 25 avril.

Les données des utilisateurs frauduleusement conservées

La société de VTC (Voiture avec chauffeur) Allocab propose des chauffeurs privés aux utilisateurs de son application. En réponse aux demandes des clients, la Cnil (Commission nationale de l'informatique et des libertés) a effectué un contrôle des activités de la firme dans le cadre de la loi « Informatique et Libertés ». L'enquête a révélé qu'Allocab commettait plusieurs manquements à ce texte : elle rapporte notamment que « des données relatives à des comptes inactifs et des cryptogrammes de cartes bancaires étaient encore présents dans le système d'information et la sécurité des données n'était pas suffisamment assurée » et que les mots de passe à un seul caractère étaient par ailleurs admis, ce qui ne garantit aucune sécurité aux données des utilisateurs. Il ne s'agit pourtant pas du premier faux pas de cette entreprise, déjà sanctionnée en 2015.

Des avertissements ignorés

Le 10 novembre 2015, Allocab se voyait mise en demeure par la Cnil suite à la plainte d'un utilisateur. L'institution ordonnait à l'entreprise de détruire les données des anciens clients et de « prendre toute mesure nécessaire pour garantir la sécurité et la confidentialité des données des utilisateurs du site », notamment en limitant la durée de conservation des cryptogrammes de cartes bancaires et de toutes les données des utilisateurs. Suite à cette première condamnation s'est déroulée une longue correspondance dans laquelle Allocab prétextait des dysfonctionnements techniques et certifiait mettre en place des mesures nécessaires. Ces affirmations ont incité la Cnil à mener un deuxième contrôle. Au cours de cette seconde investigation fin 2016, elle découvre que plusieurs de ses injonctions ne sont pas respectées : de nombreux comptes inactifs existent encore sur la plateforme, tout comme les données et cryptogrammes des cartes bancaires de nombreux utilisateurs.

15 000 euros d'amende

Les fameux dysfonctionnements invoqués par Allocab n'ont pas convaincu la commission, dont un comité restreint l'a condamné le 13 avril dernier au versement d'une amende de 15 000 euros…[lire la suite]

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

Notre métier : Vous accompagner 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

Source : *Allocab condamné par la Cnil*

600.000 serveurs Windows en danger, Microsoft ne patchera pas la faille

600.000 serveurs Windows en danger, Microsoft ne patchera pas la faille

---

Un défaut de sécurité dans un ancien serveur Web Windows ne sera pas corrigé, même si des centaines de milliers de machines continuent d'exécuter le logiciel obsolète de Microsoft.
Un 0Day pour des serveurs Web sous Windows Internet Information Services (IIS 6) a été exploité à outrance par les pirates informatiques depuis juillet 2016. Un défaut de sécurité qui ne sera pas corrigé. Deux chercheurs en sécurité de l'Université de technologie de la Chine du Sud ont expliqué que cette faille est dorénavant connue par Microsoft, mais qu'elle ne sera pas patchée. La version affectée d'IIS 6 a été publiée pour la première fois avec Windows Server 2003. Elle n'est plus prise en charge depuis 2015…[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 : *ZATAZ Défaut de sécurité : 600.000 serveurs Windows en danger, Microsoft ne patchera pas la faille – ZATAZ*

La nouvelle version du virus Locky vise les entreprises françaises

La nouvelle version du virus Locky vise les entreprises françaises

La nouvelle charge de propagation du ransomware Locky s'est particulièrement concentré sur la France ces derniers jours, selon Vade Secure.

La nouvelle campagne de propagation de Locky qui se répand ces derniers jours a particulièrement frappé la France lundi 24 avril. Vade Secure annonce avoir bloqué, à lui seul, 369 000 exemplaires de l'email contenant le ransomware. *« Dont 200 000 chez nos partenaires clients et opérateurs et 169 000 sur notre Cloud »*, précise Sébastien Gest, Tech évangéliste chez l'éditeur français de sécurisation des boîtes emails. Qui ajoute avoir constaté un nouveau pic de 25 000 envois, ce mardi 25 avril, lors d'une courte attaque autour de 12h. Signalons, à titre personnel, que les équipes de NetMediaEurope, éditeur de *Silicon.fr*, ont elles-mêmes reçu un avertissement de son prestataire technique sur l'existence de cette nouvelle campagne. Une alerte relativement rare dans nos services.

Certes, le volume constaté depuis hier peut sembler insignifiant en regard des 1,4 million d'emails infectieux Locky que Vade Secure bloquait chaque jour en juillet 2016. Un taux qui s'était affaibli au fil des mois pour tomber à 600 000 fin décembre. Mais la nouvelle campagne de tentative d'infection semble se distinguer par des attaques ciblant des zones géographiques précises. *« Plus de 95% des e-mails bloqués hier se destinaient à des entreprises françaises »*, confirme l'expert qui rappelle que sa société protège quelques 400 millions de boîtes électroniques de 76 pays dans le monde dont les Etats-Unis et le Japon. En revanche, Vade Secure n'a pas constaté de profil particulier des entreprises ciblées. *« Tous les types d'entreprises sont concernés, du grand compte à la petite PME »*, assure le technicien. Rappelons que Locky est un crypto-ransomware qui, s'il est exécuté, va chiffrer tous les fichiers rencontrés sur son passage et réclamer une rançon, généralement en bitcoin, pour que la victime retrouve l'usage de ses documents…[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 nouveau Locky vise les entreprises françaises*

Beware! New Android Malware Infected 2 Million Google Play Store Users

Initially thought to be 600,000 users, the number of Android users who have mistakenly downloaded and installed malware on their devices straight from Google Play Store has reached 2 Million.…[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

Que faire en priorité en cas d'attaque informatique

Que faire en priorité en cas d'attaque informatique

Quelles sont les premières mesures à prendre lorsque l'on suspecte d'avoir été la victime d'un incident de sécurité informatique ?

A un moment ou l'autre, votre entreprise devra faire face à un incident de cybersécurité. Mais sous la pression, l'effet du stress, on fait des erreurs. Trop reporter la prise de décisions critiques peut renforcer l'impact de l'incident, mais inversement, prendre des décisions trop hâtives peut causer d'autres dommages à l'entreprise ou entraver une réponse complète.
Il existe de nombreuses façons de soupçonner qu'un incident de sécurité s'est produit, de la détection d'activités inhabituelles par le suivi proactif des systèmes critiques jusqu'aux audits, en passant par la notification externe par les forces de l'ordre ou la découverte de données compromises perdues dans la nature.
Toutefois, des indicateurs tels que la consommation inhabituelle de ressources CPU ou réseau sur un serveur peut avoir plusieurs origines différentes, dont beaucoup n'ont rien à voir avec des incidents de sécurité. Il est là essentiel d'enquêter davantage avant de tirer des conclusions.
Disposez-vous des d'indices cohérents ? Par exemple, si l'IDS détecte une attaque de force brute contre le site Web, les journaux Web le confirment-ils ? Ou, si un utilisateur signale une attaque suspectée de hameçonnage, d'autres utilisateurs ont-ils été visé ? Et quelqu'un a-t-il cliqué sur des liens ou des documents joints ?
Vous devez également réfléchir à des questions relatives à la nature de l'incident. S'agit-il d'une infection par un logiciel malveillant générique ou un piratage de système ciblé ? Y'a-t-il une attaque intentionnelle en déni de service (DoS) en cours ?…[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 : *Que faire en premier en cas d'attaque informatique*

Est-ce que la campagne présidentielle d'Emmanuel Macron a été vraiment piratée par les Russes ?

Est-ce que la campagne présidentielle d'Emmanuel Macron a été vraiment piratée par les Russes ?

Une société de cybersécurité affirme qu'un groupe de hackers russes a tenté de déstabiliser la campagne d'Emmanuel Macron, confirmant les dires de l'équipe du candidat.

L'équipe d'Emmanuel Macron dénonçait, en février, « *plusieurs milliers d'attaques* » contre ses structures informatiques. Dans un rapport consulté par *Libération* et *20 Minutes*, lundi 24 avril, la société de cybersécurité Trend Micro confirme que le mouvement En marche ! a été la cible, pendant les derniers mois de la campagne présidentielle, de pirates informatiques identifiés comme appartenant au groupe de hackers russes Fancy Bear.

Que sait-on de ces tentatives de piratage ?

Entre le 15 mars et le 17 avril, selon *Libération*, la société Trend Micro « *a repéré quatre sites web reproduisant des pages d'accueil de services en ligne Microsoft, avec des adresses destinées à tromper les utilisateurs* ». Les noms de domaine suivants ont été créés : onedrive-en-marche.fr, mail-en-marche.fr, portal-office.fr et accounts-office.fr. L'objectif de ces noms, dont deux imitent le nom du site officiel d'Emmanuel Macron (en-marche.fr), est d'inciter les destinataires d'un mail frauduleux à se connecter et renseigner identifiant et mot de passe…

Connaît-on les conséquences de ce piratage ?

L'équipe d'Emmanuel Macron affirme que ces manœuvres n'ont pas eu d'effet. Contacté par *20 Minutes*, Mounir Mahjoubi, responsable numérique de la campagne En marche !, assure qu'« *aucune de ces boîtes mail n'a été hackée* ». « *Nous avions détecté ces noms de domaine et plusieurs autres*, poursuit Mounir Mahjoubi. *Certaines personnes ont cliqué sur les liens, mais n'ont renseigné ni identifiant ni mot de passe* », explique-t-il encore à *Libération*, et aucune donnée n'a été volée…[lire la suite]

« En général on ne sait pas qui attaque », explique le directeur général de l'ANSSI. « Les attaques peuvent venir d'absolument partout. Mieux vaut se demander comment faire pour se protéger ».

Denis JACOPINI : A ce jour, nous n'avons aucune certitude sur les auteurs de l'attaque de TV5 monde en avril 2015. Bientôt 2 ans plus tard, les preuves recueillies ne sont pas suffisantes pour accuser Russes, Chinois ou d'autres états. Alors quelques jours ou quelques semaines à la suite des élections Françaises ne suffiront pas à nous assurer de l'identité des auteurs de ces ingérences. On peut avoir des doutes, mais nous auront difficilement des certitudes.

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 : *Présidentielle : trois questions sur les soupçons de piratage informatique ciblant En marche !*

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*

Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs

Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs

---

Script kiddies and online criminals around the world have reportedly started exploiting NSA hacking tools leaked last weekend to compromise hundreds of thousands of vulnerable Windows computers exposed on the Internet.

Last week, the mysterious hacking group known as Shadow Brokers leaked a set of Windows hacking tools targeting Windows XP, Windows Server 2003, Windows 7 and 8, and Windows 2012, allegedly belonged to the NSA's Equation Group.

What's Worse?

Microsoft quickly downplayed the security risks by releasing patches for all exploited vulnerabilities, but there are still risks in the wild with unsupported systems as well as with those who haven't yet installed the patches.

Multiple security researchers have performed mass Internet scans over the past few days and found tens of thousands of Windows computers worldwide infected with **DoublePulsar**, a suspected NSA spying implant, as a result of a free tool released on GitHub for anyone to use.

Security researchers from Switzerland-based security firm Binary Edge performed an Internet scan and detected more than 107,000 Windows computers infected with DoublePulsar.

A separate scan done by Errata Security CEO Rob Graham detected roughly 41,000 infected machines, while another by researchers from Below0day detected more than 30,000 infected machines, a majority of which were located in the United States.

The impact ?

DoublePulsar is a backdoor used to inject and run malicious code on already infected systems, and is installed using the **EternalBlue** exploit that targets SMB file-sharing services on Microsoft's Windows XP to Server 2008 R2.

Therefore, to compromise a machine, it must be running a vulnerable version of Windows OS with an SMB service expose to the attacker.

Both DoublePulsar and EternalBlue are suspected as Equation Group tools and are now available for any script kiddie to download and use against vulnerable computers.

Once installed, DoublePulsar used hijacked computers to sling malware, spam online users, and launch further cyber attacks on other victims. To remain stealthy, the backdoor doesn't write any files to the PCs it infects, preventing it from persisting after an infected PC is rebooted….[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 : *Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs*