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

---

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]

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

---

Réagissez à cet article

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

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

---

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

---

Réagissez à cet article

Source : *Le nouveau Locky vise les entreprises françaises*

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

---

Réagissez à cet article

Source : *Que faire en premier en cas d’attaque informatique*

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

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	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.

Réagissez à cet article

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

---

Réagissez à cet article

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

Que sait de nous Google grâce à nos comportements sur Internet ?

	Que sait de nous Google grâce à nos comportements sur Internet ?

Mondialement connue, la firme américaine Google est utilisée par de nombreux internautes, pour son moteur de recherche, mais aussi pour ses nombreux services gratuits (Gmail, Drive, Youtube, Google Maps…). Seul petit hic ? Le revers de la médaille. Puisque Google exploite vos données sans que vous n'en ayez toujours conscience.

Tout le monde connaît Google pour son moteur de recherche ultra-performant. C'est d'ailleurs le moteur préféré des Français. Fin 2016, selon Netbooster, plus de 94 % d'entre eux l'ont utilisé pour effectuer leurs recherches en ligne. Pour apprécier la démesure de ce chiffre, il suffit de voir la part restante à ses principaux concurrents : moins de 4 % pour Bing (Microsoft) et à peine plus de 2 % pour Yahoo.

Plus de 200 services gratuits…

À travers sa maison mère « **Alphabet** », Google est l'une des premières capitalisations mondiales avec une valeur de 588 milliards de dollars, juste derrière Apple. La firme de Moutain View n'est pas la seule à analyser les données qui lui parviennent. Tous les géants du secteur (Apple, Amazon, Facebook…) le font en s'appuyant sur les traces que nous laissons chaque jour sur Internet. Ils engrangent des milliards de dollars grâce à ces informations personnelles.

Inutile donc d'être un financier avisé pour comprendre que la seule activité de moteur de recherche ne suffit pas à générer de telles entrées d'argent. Google est une pieuvre géante, dont les tentacules s'étendent dans des domaines aussi nombreux que variés. Le système d'exploitation Android, le navigateur Internet Chrome, les vidéos YouTube, la plateforme de téléchargement Google Play, la cartographie Google Maps, la suite bureautique Google Documents, le site de partage de photos Picasa…

Ce sont plus de 200 services proposés gratuitement par l'entreprise. Pour la plupart d'entre eux, la seule contrepartie demandée est l'ouverture d'un compte Gmail, le service de messagerie en ligne maison. L'adresse email et le mot de passe associé deviennent alors vos sésames pour vous identifier et entrer dans la sphère Google, depuis n'importe quel terminal à travers le monde.

… en échange de vos données personnelles

Toute cette gratuité a cependant une face cachée : l'exploitation commerciale de nos données personnelles. En effet, elles représentent une manne financière des plus importante. En acceptant les « **conditions générales d'utilisation** », que nous ne lisons quasiment jamais, nous donnons le droit à Google de tracer et d'utiliser tout ce que nous faisons sur Internet : les sites visités, les achats effectués, les lieux dans lesquels nous nous rendons, les films regardés, les livres lus, la musique écoutée…

L'ensemble de ces données est alors analysé par les puissants ordinateurs de la firme, dans le but créer une sorte de carte d'identité très précise de chaque utilisateur. Ces profils, compilant de très nombreuses données, se revendent à prix d'or aux marques désireuses de cibler au mieux leur publicité. C'est ce que l'on appelle le « **Big Data** ».

Pour profiter gratuitement des services de Google, comme ceux de nombreux autres acteurs des nouvelles technologies, nous devons donc rogner sur notre vie privée, en abandonnant la confidentialité de nos données personnelles. Il existe une formule qui résume parfaitement cette pratique : « **si c'est gratuit, c'est que le produit c'est vous** ! »…[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

---

Réagissez à cet article

Source : *Données personnelles. Voici ce que Google sait de vous*

Qu'est ce que le Smishing ?

Qu'est ce que le Smishing ?

Smishing est la contraction de SMS et de Phishing. On l’appelle également Hameçonnage par SMS.
Tout comme le phishing, un message à caractère urgent est envoyé à un utilisateur pour qu’il entreprenne une action. Lors d’un Smishing, c’est un message texte qui est envoyé à un utilisateur sur son téléphone. Le texte du message demande généralement à l’utilisateur d’appeler un numéro de téléphone ou de se rendre sur un site Internet pour effectuer une action précise. La plupart du temps, lorsque vous composez ce numéro de téléphone, vous êtes automatiquement redirigé vers un serveur vocal interactif. Il est demandé à l’utilisateur de fournir des informations personnelles (mot de passe) ou bancaires (numéro de carte bancaire).
Souvent, cette forme de phishing implique un message de texte dans un SMS ou dans un numéro de téléphone. Le numéro de téléphone comporte un message automatisé à partir duquel vos informations commencent à être réellement recueillies. Ce qui rend particulièrement effrayant le smishing, c’est que l’on a plutôt tendance à faire confiance à un SMS qu’à un e-mail. La plupart des gens sont conscients des risques encourus pour la sécurité lorsqu’on clique sur des liens contenus dans des e-mails. Mais c’est moins le cas lorsqu’il s’agit de SMS.

Ne cliquez jamais sur les liens contenus dans ces messages et ne rappelez jamais ces numéros.

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

---

Réagissez à cet article

Source : *Que sont le Smishing et le Vishing ? | Aide Homelidays*

Les présidentielles ne seront pas affectés par une cyberattaque

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	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]

Réagissez à cet article

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*