Comment les « ondes de choc digitales » vont intensifier la concurrence dans tous les secteurs

Comment les « ondes de choc digitales » vont intensifier la concurrence dans tous les secteurs

À mesure que 2020 approche, le rythme et l'impact des nouvelles technologies sur les entreprises et la société en général ne cessent de prendre de l'ampleur.
Thierry BRETON : Nous passons toujours plus de temps à interagir en ligne sur de nombreux appareils connectés. Les produits et services à destination des consommateurs ou des entreprises sont de plus en plus personnalisés, gourmands en données et sensibles au contexte. Parallèlement, **la confiance devient désintermédiée et transactionnelle** alors même que les objets interagissent directement entre eux et avec les utilisateurs en générant des flux de données de valeur.
Cependant, malgré la croissance exponentielle de nombreux développements de base dans les applications technologiques les plus innovantes, **le rythme du changement n'est pas toujours prévisible** : le progrès est hétérogène et peut même, dans certains cas, conduire à des impasses.
Parfois, **la combinaison de certaines compétences émergentes permet le développement d'innovations** telles que les véhicules entièrement autonomes, les diagnostics médicaux informatisés, les modifications génétiques ou les assistants virtuels intelligents. Dans d'autres cas, **des préoccupations autour du respect de la vie privée ou l'éthique ralentissent, voire font reculer la mise en œuvre de certaines technologies.**
Telles des ondulations à la surface d'un lac, les « ondes de choc digitales » émaneront de différentes sources et interagiront entre elles créant ainsi un environnement complexe et incertain…[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 : *Comment les « ondes de choc digitales » vont*

intensifier la concurrence dans tous les secteurs | Thierry Breton | Pulse | LinkedIn

---

Autopsie d’un virus qui se cache dans les pixels d’une publicité

Autopsie d’un virus qui se cache dans les pixels d’une publicité

Soyez prudents ! Les pirates informatiques sont très inventifs, et là, ils nous font, une fois de plus, la démonstration qu'ils sont de plus en plus malins. En effet, un laboratoire de sécurité a découvert un logiciel malveillant qui se cache dans les pixels composant l'image d'une publicité. Ce virus profite en fait d'une faille du navigateur Internet Explorer et de Flash Player, ce petit complément vous permettant notamment d'afficher des vidéos sur les pages que vous visitez.

Et parce qu'il s'intègre dans une photo, ce virus a été baptisé Stegano, en référence à la technique de la sténographie qui permet de dissimuler des informations secrètes dans des supports anodins. Très concrètement, vous ouvrez votre navigateur, quelques clics au cours d'une recherche et vous arrivez sur une page sur laquelle va aussi s'afficher une bannière publicitaire. Et du coup, le processus d'exécution du logiciel malveillant va se mettre en route. Il va d'abord vérifier si votre navigateur lui permet de s'installer et il va aussi récolter quelques informations au sujet de votre ordinateur.
Si ces informations sont favorables à la poursuite du processus, l'image de la publicité va être remplacée par une image similaire mais légèrement modifiée. Même en zoomant, la différence n'est pas facile à percevoir. Et c'est via cette image que l'installation va se poursuivre.
Durant cette seconde phase, le niveau de sécurité de votre ordinateur va être testé. Si la voie est libre, la dernière phase consistant à installer le logiciel malveillant va se déclencher. Ce dernier permettra, par exemple, aux pirates de collecter des données personnelles ou encore d'ouvrir une porte dérobée sur votre ordinateur pour en permettre l'accès et ceci, sans attirer votre attention.
Il est aussi possible que certains des internautes touchés voient leur ordinateur infecté par un logiciel qui va crypter les données, ce qui permet ensuite aux pirates de réclamer une rançon pour obtenir la clef permettant de les récupérer…[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 : *Virus informatique: attention Stegano se cache dans les pixels d'une publicité*

Rapport 2017 sur la Cyber Sécurité de F-Secure

Rapport 2017 sur la Cyber Sécurité de F-Secure

F-Secure vient de publier son Rapport 2017 sur la Cyber Sécurité qui décrit et analyse l'état actuel de la cyber sécurité dans le monde. Ce rapport s'attarde en particulier sur les problèmes que rencontrent les entreprises, dans un contexte où les pirates délaissent les malware conventionnels au profit d'attaques plus sophistiquées, et donc encore plus dangereuses.
« Les menaces actuelles peuvent déjouer les approches unilatérales classiques de la sécurité, même les plus efficaces. En ayant recours au phishing (avec désormais des listes, vendues en ligne, de comptes ou réseaux pré-exposés) ou via d'autres méthodes, les pirates peuvent beaucoup plus facilement viser un gouvernement ou une entreprise du Fortune 500 », explique Sean Sullivan, Security Advisor chez F-Secure. « Nous vivons dans un monde post-malware, où le piratage s'est industrialisé. Et les cyber criminels ne comptent plus seulement sur les malware les plus communs pour se faire de l'argent. »

Ce rapport offre une analyse détaillée des problèmes majeurs diagnostiqués par les chercheurs et experts sur le plan de la cyber sécurité. Parmi les principaux résultats :
• Une grande partie du trafic de reconnaissance active en 2016 était liée à des adresses IP majoritairement situées dans 10 pays, et notamment la Russie, les Pays-Bas, les États-Unis, la Chine ou encore l'Allemagne.
• Les versions obsolètes d'Android sont de plus en plus nombreuses et rendent les appareils mobiles particulièrement exposés. L'Indonésie possède le nombre le plus important d'appareils Android non mis à jour, la Norvège, le plus faible.
• La plupart des cyber attaques font appel à des techniques basiques et s'en prennent à des infrastructures peu robustes.
• 197 nouvelles familles de ransomware ont été découvertes en 2016, contre seulement 44 en 2015.
• Le recours aux exploit kits a diminué au cours de 2016.
Ce rapport relate également les évènements marquants et les tendances de l'année 2016. Au programme : des informations sur les botnets de type Mirai, sur les attaques préparées en amont, sur le cyber crime et sur les dernières tendances globales en matière de cyber menaces. Certaines organisations comme l'Autorité finlandaise de régulation des communication, le Virus Bulletin ou encore AV-Test, ont contribué à ce rapport à travers plusieurs articles…[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 : *Nouveau Rapport F-Secure sur la Cyber Sécurité : un monde « post-malware » – Global Security Mag Online*

Le site Internet de Donald Trump piraté par Iraqi Hacker

Le site Internet de Donald Trump piraté par Iraqi Hacker

During the 2016 presidential election campaign, we reported about how insecure was the mail servers operated by the Trump organization that anyone with little knowledge of computers can expose almost everything about Trump and his campaign.

Now, some unknown hackers calling themselves « Pro_Mast3r » managed to deface an official website associated with President Donald Trump's presidential campaign fundraising on Sunday.

The hacker, claiming to be from Iraq, reportedly defaced the server, secure2.donaldjtrump.com, which is behind CloudFlare's content management system and security platform.The server appears to be an official Trump campaign server, reported Ars, as the certificate of the server is legitimate, « *but a reference to an image on another site is insecure, prompting a warning on Chrome and Firefox that the connection is not secure.* »

The defaced website displayed an image of a black hat man and included a text message, which reads:

Hacked by Pro_Mast3r ~
Attacker Gov
Nothing Is Impossible
Peace From Iraq

…[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 : *President Donald Trump’s Website Hacked; Defaced By Iraqi Hacker*

Ransomwares : Pourquoi les entreprises préfèrent-elles payer ?

	**Ransomwares : Pourquoi les entreprises préfèrent-elles payer ?**

Le ransomware, 1ère menace informatique en Europe et « machine à cash » pour les cybercriminels : pourquoi les entreprises préfèrent-elles payer ? par Désirée Rodriguez

Pour Europol (Rapport annuel cybercriminalité 2016), le « *ransomware est devenu la première menace en Europe* » et les faits vont empirer dans les mois et années à venir. Régis Bénard, consultant technique du spécialiste français Vade Secure (leader mondial des solutions de protection des boîtes de messagerie contre ce type de menaces) confirme cette tendance qui n'est pas prête de laisser sa place puisqu'encore aujourd'hui, et malgré une hausse de la sensibilisation, les entreprises préfèrent souvent payer plutôt que de perdre du temps… et de l'argent. C'est tout le dilemme du ransomware.

« Pour maximiser leurs profits, les cybercriminels innovent en permanence »

Les cybercriminels sont organisés comme de vraies entreprises du crime numérique avec un accent très fort mis sur l'innovation pour maximiser leurs résultats.

Actuellement, Cerber est le ransomware le plus actif en France. Connu dans le monde entier, Cerber a notamment initié le concept du *ransomware-as-a-service*. L'idée est simple mais terriblement efficace : pour maximiser leurs profits, les cybercriminels proposent à des volontaires de diffuser le ransomware dans leur propre pays. Depuis 2016, Cerber est également une véritable entreprise du cybercrime avec un marketing quasi professionnel, un service après-vente qui propose d'accueillir les victimes pour les aider à payer leur rançon, etc.

« Locky, endormi ? Le ransomware le plus célèbre en France n'a pas fini de faire parler de lui »

Le ransomware le plus présent en France en 2016, marque une pause. Mais l'accalmie ne va malheureusement pas durer. L'année dernière, Locky avait déjà connu des périodes d'absence quasi totale. Plusieurs raisons peuvent expliquer ce ralentissement de l'activité de Locky mais la plus évidente est que les cybercriminels travaillent à des évolutions sur leur ransomware. Il va donc revenir prochainement sous une autre forme et donc encore plus fort. Deuxième explication possible : les réseaux de PC ou objets connectés piratés (botnets) pour diffuser en masse les attaques de Locky, ne sont pas disponibles car loués à d'autres cybercriminels ».

« L'humain : la protection la plus efficace contre les attaques de phishing et ransomware »

Les ransomware sont véhiculés par des emails de phishing ou spear phishing (D'après le Gartner 65 % des attaques informatiques étaient initiées par un phishing en 2015 alors qu'une étude récente de PhishMe souligne la montée en puissance du phishing puisque 91% des attaques informatiques commencent aujourd'hui par du phishing). L'email est donc le canal prioritaire utilisé par les cybercriminels pour piéger les entreprises. Le problème est que l'humain est loin d'être infaillible : plusieurs études le rappellent régulièrement.

Les failles humaines peuvent ainsi aller jusqu'à mettre en péril une entreprise. Alors que le nombre de victimes continue d'augmenter, il est temps d'accélérer la résistance pour ne plus tomber dans le piège. Et pour mieux se protéger, l'éducation et la formation des utilisateurs sont des axes primordiaux pour que chacun prenne conscience des enjeux et des risques.

Pour les entreprises tout comme pour les pouvoirs publics, il s'agit d'organiser des réunions d'information régulières sur la sécurité, des formations sur le phishing, des recommandations sur le bon usage des réseaux sociaux, sur des conseils de bon sens, ou sur des bonnes pratiques à mettre en place : n'ouvrir les pièces jointes suspectes que si l'expéditeur est confirmé, supprimer le message d'un expéditeur suspect inconnu sans y répondre, etc…[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 ransomware, 1ère menace informatique en Europe et « machine à cash » pour les cybercriminels : pourquoi les entreprises préfèrent-elles payer ? – Globb Security FR*

Cyberattaques des présidentielles. Qui serait responsable ?

Cyberattaques des présidentielles. Qui serait responsables ?

Les cyber-attaques que la Russie est soupçonnée de mener en France dans le cadre de la campagne présidentielle sont « une forme d'ingérence inacceptable », a estimé dimanche le ministre français des Affaires étrangères Jean-Marc Ayrault.

» Les cyberattaques russes, grande menace pour les États-Unis et l'Europe
Dans une interview au *Journal du Dimanche*, le chef de la diplomatie française a déclaré : « Il suffit de regarder pour quels candidats, à savoir Marine Le Pen ou François Fillon, la Russie exprime des préférences, dans la campagne électorale française, alors qu'Emmanuel Macron, qui développe un discours très européen, subit des cyberattaques. Cette forme d'ingérence dans la vie démocratique française est inacceptable et je la dénonce ».
« La Russie est la première à rappeler que la non-ingérence dans les affaires intérieures est un principe cardinal de la vie internationale. Et je la comprends. Et bien la France n'acceptera pas, les Français n'accepteront pas qu'on leur dicte leurs choix », a ajouté le ministre.

Quels éléments a-t-on pour de telles affirmations ?
Denis JACOPINI : Aujourd'hui la Russie, hier la Chine et demain qui ? Quels sont les éléments permettant d'affirmer de tels propos ?
L'adresse IP ?
Si c'est l'adresse IP qui est prise en compte, n'est-on nous pas en train de mélanger l'adresse IP ayant accédé aux systèmes informatiques et celle du commanditaire de l'attaque ?
Signatures et codages de caractères
Si ce sont les signatures présentes dans les codes ou les codages de caractères qui sont pris en compte, ne risque t-on pas de reproduire l'attribution hâtive de l'attaque de la chaîne TV5 monde à l'Etat islamique
alors même que très vite après l'attaque, de nombreux experts avaient mis en doute la crédibilité de la revendication.
A mon avis
En raison du refus de certains pays pour coopérer en matière de lutte contre la cybercriminalité, il devient très compliqué de remonter jusqu'aux ordinateurs utilisés pour mener de telles attaques, pire encore pour remonter jusqu'aux commanditaires des attaques informatiques. Les infos circulant encore ce matin font référence une fois de plus à des accusations qui sembleraient bien être sans preuve…
Malgré l'absence de preuve, Ayrault dénonce une «ingérence» de la Russie dans la présidentielle
Je serais bien intéressé
En tant qu'Expert judiciaire spécialisé en cybercriminalité, je serais bien intéressé pour expertiser les éléments concernés par cette affaire.
A bon entendeur…

Qu'en pensez-vous ? Merci de me laisser votre avis ou commentaire

---

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.

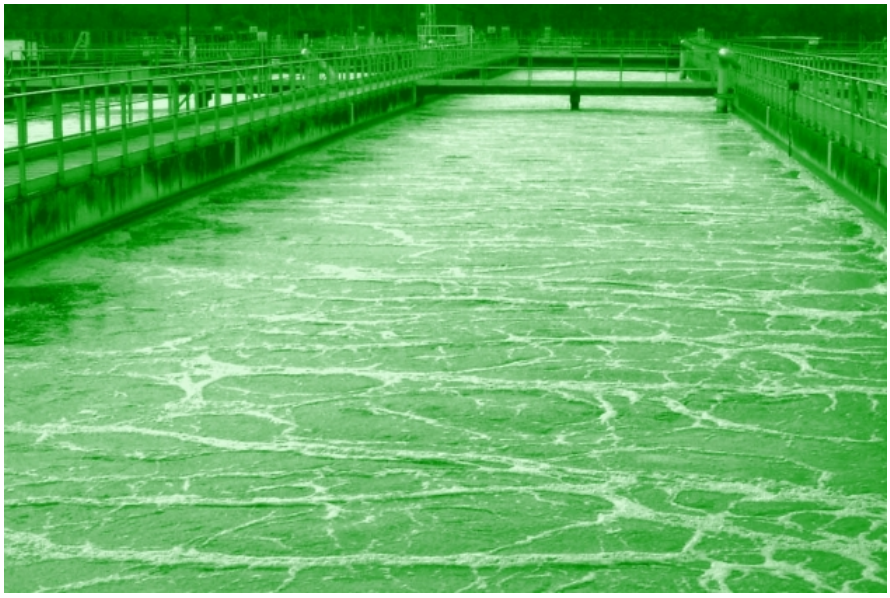
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Paris dénonce à nouveau les cyberattaques de Moscou*

Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière



Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière

---

Des chercheurs en sécurité ont créé LogicLocker, un logiciel malveillant capable de bloquer une station d'épuration d'eau dans le but d'extorquer des rançons. Ce type d'attaque serait la prochaine étape dans le domaine des ransomwares.

Les ransomwares cryptographiques, qui chiffrent les données des utilisateurs pour extorquer une rançon, vous font peur ? Alors attendez de voir les « ransomwares industriels », qui s'attaquent aux systèmes de contrôle des usines. Ils vous feront basculer en mode panique, car ils pourraient avoir des conséquences directes et néfastes sur notre environnement physique.
Pour l'instant, ce type de malware ne fait pas encore partie de l'arsenal des pirates, mais des chercheurs du Georgia Institute of Technology pensent que ce n'est qu'une question de temps, étant donné la faible sécurité des systèmes industriels. Pour montrer l'étendue de la menace, ils ont développé un prototype d'un tel ransomware et l'ont testé sur une maquette industrielle qui représente une station d'épuration d'eau d'une ville. Ils ont présenté leur travail cette semaine à l'occasion de la conférence RSA 2017, qui s'est tenue à San Francisco.

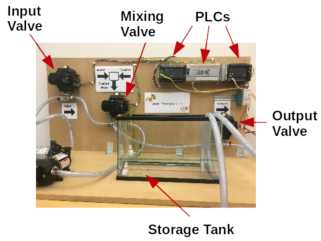


Fig. 2: Water Treatment Testbed

Baptisé LogicLocker, ce malware est capable d'infecter l'automate programmable industriel (programmable logic controller, PLC) qui régule la désinfection et le stockage de l'eau potable. L'attaque consiste à extraire le code exécutable de l'appareil et de le remplacer par un code malveillant, puis de changer le mot de passe d'accès. Ainsi, l'attaquant peut non seulement stopper le processus d'épuration, mais aussi empêcher les ingénieurs de réinstaller le code d'origine sur l'appareil. Le pirate peut alors envoyer aux responsables de la station d'épuration une demande de rançon doublée d'un ultimatum : s'ils ne payent pas au bout d'un certain temps, le code malveillant va surdoser le produit désinfectant et, du coup, rendre toute l'eau potable impropre à la consommation. Une fois la rançon payée, l'attaquant restitue le code volé.

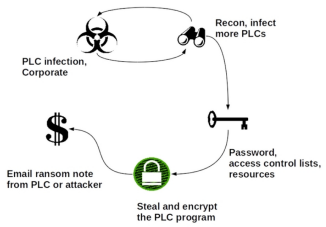


Fig. 3: General Flow of ICS Ransomware Attack

Un tel scénario est faisable dans n'importe quel domaine, à partir du moment où il y a des automates programmables connectées sur un réseau interne ou, carrément, sur Internet. Il suffit de se rendre sur le site Shodan.io pour constater qu'il existe d'ores et déjà des milliers de PLC accessibles par la Toile. Les chercheurs ont en trouvé d'emblée plus de 1400 de marque MicroLogix et 250 de marque Schneider Modicon.

Une question de profitabilité

Si les pirates n'ont pas encore exploité ce type d'attaque, ce n'est pas parce que ces automates sont bien sécurisés. Au contraire, leur manque de protection est notoire et connu depuis des années. *« La seule explication est que les cybercriminels n'ont pas encore trouvé le business model qui leur permet d'opérer de manière profitable dans ce type d'environnement »*, estiment les chercheurs dans leur étude. En effet, le ransomware industriel nécessite plus de recherche et de connaissance. Par ailleurs, son mode opératoire est très pointu et ne peut donc faire qu'un faible nombre de victimes. C'est donc exactement l'inverse des cryptoransomwares, qui sont diffusés en masse auprès d'un large parc d'utilisateurs…[lire la suite]

Source : *Ce malware pourrait empoisonner l'eau potable d'une ville entière*

Popcorn Time, un rançongiciel bien vicieux

Popcorn Time, un rançongiciel bien vicieux

Depuis peu, les rançongiciels (ou ransomware) constituent de véritables fléaux dans l'univers de l'informatique et du web. Ils touchent les données personnelles de millions de gens de par le monde. Les experts en sécurité se sont même mis à taxer 2016 comme étant « l'année des rançongiciels ».

Payez ou infectez vos amis

Sur cette année, il se peut que Popcorn Time soit le rançongiciel qui vienne clore la propagation de ces logiciels de chantage. Ce nouveau ransomware pose un gros dilemme à sa victime en lui imposant de payer une rançon ou d'infecter ses amis.

Pour commencer, il emprunte le nom d'une application de streaming vidéo ayant défrayé la chronique en 2015, ce qui incite au téléchargement de celle-ci. Ensuite, il infecte l'ordinateur de la victime par le biais d'un courriel piégé ou d'un lien malveillant, puis crypte ses données personnelles en usant d'un algorithme de chiffrement AES 256 bits.

Après que les données ont été cryptées, il impose à la victime de donner la valeur de 1 bitcoin (soit environ 700 €) ou de le transmettre sur l'ordinateur d'un ami. C'est une méthode toute nouvelle avec en plus une limite du nombre d'introductions de clé de déchiffrement. Entrer quatre fois la mauvaise clé ferait perdre définitivement ses données.

Les dossiers Windows sont les premières cibles

D'après la conclusion des enquêtes réalisées par le site Bleeping Computer sur ce rançongiciel, il ciblerait en premier les fichiers présents dans les dossiers Windows : Mes Documents, Images, Musiques et toutes les données sur le Bureau.

Afin de faire face à ce logiciel de rançon, la meilleure façon pour un utilisateur lambda est de prendre des précautions préventives basées sur les mesures de sécurité les plus basiques :

• faire des copies de ses données personnelles vers un support externe qui se débranche de l'ordinateur après chaque usage de ce dernier et sur les Clouds comme Dropbox, OneDrive, Google Drive, Mediafire, Mega, pCloud, Flipdrive… ;

• éviter d'ouvrir les mails aux destinateurs inconnus et contenant des liens ou des pièces jointes. Il est aussi possible que Popcorn Time provienne d'une personne de votre liste de contact. Prenez les mêmes réserves tant que le contenu n'a pas été formellement reconnu ;

• mettre à jour son système d'exploitation et son antimalware.

…[lire la suite]

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

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

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

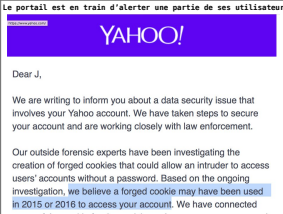
Original de l’article mis en page : Popcorn Time : le plus vicieux rançongiciel de cette année – @Sekurigi

---

Piratage de Yahoo. La technique des faux cookies a encore frappé

Piratage de Yahoo. La technique des faux cookies a encore frappé

Le portail est en train d'alerter une partie de ses utilisateurs sur des éventuelles intrusions en 2015 et 2016. Les pirates se sont appuyés sur des faux cookies d'authentification qui, depuis, ont été invalidés.



YAHOO!

Dear J,

We are writing to inform you about a data security issue that involves your Yahoo account. We have taken steps to secure your account and are working closely with law enforcement.

Our outside forensic experts have been investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, we believe a forged cookie may have been used in 2015 or 2016 to access your account. We have connected

Cette histoire de faux cookies n'est pas nouvelle. En décembre dernier, lorsque Yahoo avait révélé le vol d'un milliard de comptes utilisateur en 2013, l'entreprise avait déjà indiqué que des pirates avaient volé sur l'un de leurs serveurs un code source propriétaire utilisé pour créer les cookies d'authentification. Dès lors, il leur était possible de créer de faux cookies permettant de s'introduire dans des comptes d'utilisateurs sans même avoir besoin d'un mot de passe.
Ce qui est nouveau, en revanche, ce sont les dates. Yahoo n'a pas précisé quand ce code source a été volé. Il a juste indiqué qu'il a probablement été subtilisé par le même acteur gouvernemental qui lui a siphonné 500 millions d'identifiants fin 2014. Ce qui, visiblement, semble cohérent au regard des années mentionnées dans le message.
En d'autres termes, ce mystérieux groupe de pirates a été capable d'accéder potentiellement à n'importe quel compte utilisateur Yahoo, sans avoir à connaître de mot de passe, et cela pendant deux ans. Les utilisateurs ayant activé la procédure d'authentification forte n'étaient pas forcément mieux protégés, car le cookie d'authentification n'intervient qu'après avoir donné un login, un mot de passe et, éventuellement, un second facteur d'authentification. Le cookie est justement là pour maintenir la connexion pendant la durée d'une session, sans que l'utilisateur ne soit contraint de s'authentifier sans arrêt…[lire la suite]

Que pouvons-nous faire pour nous protéger ?
Denis JACOPINI : A notre niveau, pas grand chose. En effet, coté utilisateur, il n'y a pas grand chose à faire pour se protéger. En possession des codes sources permettant de générer les cookies ou disposant des cookies volés, mêmes si vous changez votre mot de passe, les pirates disposeront tout de même d'une clé spéciale qui ne nécessitera même pas votre identifiant et votre mot de passe pour accéder à votre compte . La solution doit venir de Yahoo, en changeant TOUS leur algorithme de sécurité rendant ainsi invalide TOUS les cookies volés ou générés avec l'ancien algorithme.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Des utilisateurs de Yahoo victimes d'attaques par faux cookies

---

Alerte ! Un virus informatique peut vider votre compte bancaire

Alerte ! Un virus informatique peut vider votre compte bancaire

---

77% des ménages possèdent un ordinateur et 75% une connexion internet. A l'heure ou le numérique gagne toujours plus de terrain, de nouvelles menaces s'invitent dans nos foyers, les virus.
Quand les nouvelles technologies veulent nous simplifier la vie en numérisant toutes nos informations, les hackers eux, redoublent d'ingéniosité pour créer des virus de plus en plus performants. Tous les jours des dizaines ne milliers de nouveaux virus sont créés, et si l'efficacité des antivirus est parfois relative, il reste que nous manquons aussi de vigilance.

Avertissement de la gendarmerie
« En consultant internet, une mise en garde indique que votre ordinateur est infecté par le virus « Zeus ». La page d'alerte vous oriente alors vers le numéro de téléphone d'un spécialiste de la sécurité informatique. […] L'escroc, homme ou femme, recommande alors le nettoyage de votre ordinateur et l'intégration à distance d'un antivirus, moyennant une somme d'argent variant entre 99 et 249 euros. »

C'est le message que la gendarmerie du Cher a fait paraître sur son Facebook afin de prévenir la population. Ce nouveau virus est d'autant plus dangereux que le hacker, télécharge et utilise vos données bancaires pendant que vous payez l'antivirus recommandé. Prudence donc si ce message apparaît sur votre écran, n'appelez surtout pas et confiez votre ordinateur à un spécialiste…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Certifié ISO 27005 Risk Manager, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : « Zeus » : un virus informatique qui peut vider votre compte bancaire !