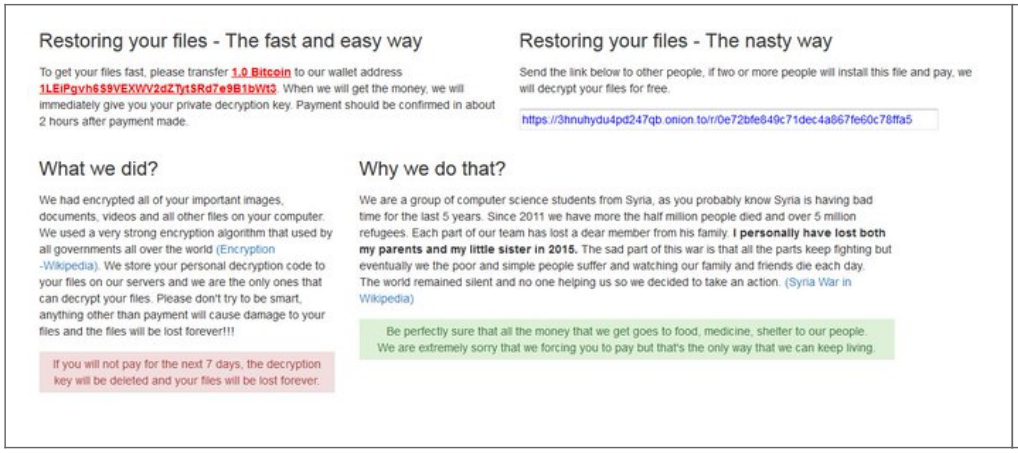
Pour récupérer vos données, ce ransomware vous demande d’infecter d’autres victimes



Restoring your files - The fast and easy way

To get your files fast, please transfer 1.0 Bitcoin to our wallet address 1LEiPgvh6S9VEXWV2dZTyt5Rd7e9B1bWt3. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5

What we did?

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world (Encryption -Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.

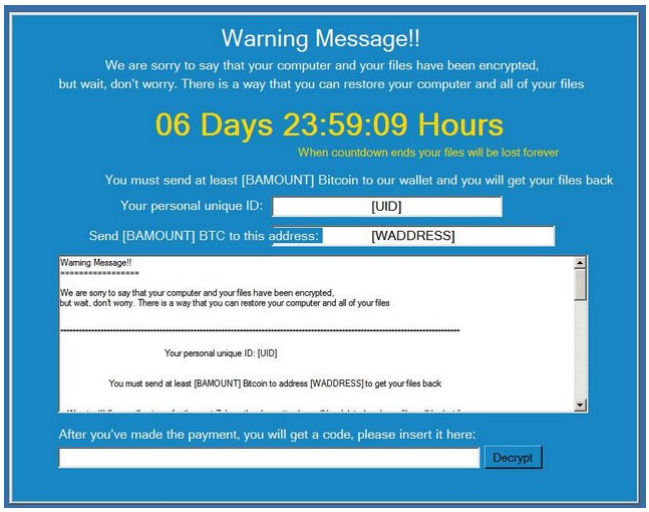
Why we do that?

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2015.** The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia)

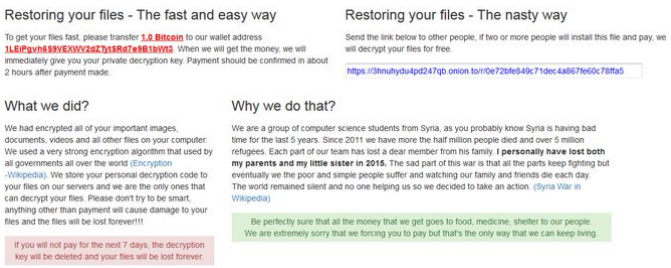
Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

Pour récupérer vos données, ce ransomware vous demande d’infecter d’autres victimes

Un nouveau logiciel de rançon contraint ses victimes à participer à sa propagation, sous peine de perdre leurs données.



L'idée semble tout droit sortie d'un épisode de *Black Mirror*. Il y a quelques jours, l'équipe de MalwareHunterTeam a mis la main sur un *malware* en cours de développement, baptisé Popcorn Time – aucun lien avec l'application de streaming du même nom. Comme de nombreux logiciels de rançon, il demande à ses victimes de payer pour pouvoir déchiffrer leurs données. Le tarif est fixé à un Bitcoin, soit 730 euros au cours actuel. Mais l'équipe de Popcorn Time laisse une possibilité moins coûteuse, qu'elle qualifie elle-même de «sale»: propager le logiciel en infectant deux autres personnes. Les données sont déverrouillées après le paiement des nouvelles victimes.



Pour vous aider à choisir la méthode sale, les auteurs de Popcorn Time fournissent le lien sur lequel devront cliquer les cibles. Il redirige vers un fichier hébergé sur un serveur Tor – actuellement hors-service. Une fois exécuté, Popcorn Time prétend installer un logiciel, tout en exécutant le chiffrement. Comme le relève le site Bleeping Computer, il s'attaque à de nombreux dossiers, parmi lesquels Mes Documents, Mes Photos, Ma Musique ou le Bureau. Chaque fichier est chiffré en AES (*Advanced Encryption Standard*). Il affiche ensuite une page d'avertissement incluant l'ensemble des instructions, un décompte d'une semaine et un champ permettant d'inscrire la clé de déchiffrement.

Réagissez à cet article

Original de l’article mis en page : Pour récupérer vos données, ce ransomware vous demande d’infecter d’autres victimes

---

Les jouets connectés s’amusent avec nos données personnelles

	Les jouets connectés s’amusent avec nos données personnelles

---

Une étude technique menée par plusieurs associations de défense des consommateurs dénonce les failles de sécurité et les CGU de plusieurs jouets connectés.

À seulement quelques semaines de Noël, l'association de défense des consommateurs UFC-Que Choisir part en croisade contre les jouets connectés. Cette étude, faite de concert avec l'association norvégienne Forbrukerradet s'attarde sur deux jouets en particulier : la poupée Cayla et le robot i-Que.

Une connexion Bluetooth vulnérable

Sont tout d'abord dénoncées des failles de sécurité qui entourent le protocole Bluetooth. La connexion entre les jouets et le smartphone se fait sans aucun code d'accès. Étant donné qu'ils sont munis d'un micro, un tiers se situant à moins de 20 mètres peut s'y connecter et entendre les échanges avec l'enfant. Il pourrait même prendre le contrôle total du jouet.

La protection des données personnelles passe à la trappe

L'UFC-Que choisir s'en prend aussi la sécurité des données personnelles. Malgré la loi « Informatique et libertés », les conditions contractuelles autorisent la collecte des données vocales. « *Ces données peuvent ensuite être transmises, notamment à des fins commerciales, à des tiers non identifiés. Les données sont aussi transférées hors de l'Union européenne, sans le consentement des parents* » explique l'UFC.

Enfin pour couronner le tout, ces jouets font du placement produit : »*l'étude a ainsi révélé que Cayla et i-Que prononcent régulièrement des phrases préprogrammées, faisant la promotion de certains produits – notamment des produits Disney ou des références aux dessins animés de Nickelodeon*« . L'association de consommateur a donc décidé de saisir la CNIL afin qu'elle contrôle le respect de la protection de données personnelles, ainsi que la DGCCRF pour qu'elle sanctionne les manquements aux dispositions légales et réglementaires sur la sécurité.

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 : 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 : L'UFC-Que Choisir épingle les jouets connectés sur la sécurité des données personnelles – CNET France

---

Naissance de l'intelligence artificielle idiote

La course à la maîtrise de l'intelligence artificielle s'accélère. Cette semaine Uber a acquis Geometric Intelligence, une start-up qui va lui permettre d'atteindre une nouvelle dimension dans cette discipline.…[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

Alerte ! Des publicités Internet contaminées par des

malwares

	**Alerte ! Des publicités Internet contaminées par des malwares**

De très nombreux sites Internet à forte notoriété ayant des millions de visiteurs quotidiens sont touchés. Les systèmes de détection ESET montrent qu'au cours des deux derniers mois, Stegano a été affiché auprès de plus d'un million d'utilisateurs. Stegano se cache dans les images publicitaires affichées sur les pages d'accueil des sites Internet.

Bonjour,
Depuis le début du mois d'octobre 2016, des cybercriminels ciblent les utilisateurs d'Internet Explorer et analysent leur ordinateur pour détecter les vulnérabilités dans Flash Player. En exploitant leurs failles, ils tentent de télécharger et d'exécuter à distance différents types de malwares.
Ces attaques se rangent dans la catégorie des publicités malveillantes, c'est-à-dire que des codes malicieux sont distribués via des bannières publicitaires. **La victime n'a même pas besoin de cliquer sur la publicité** : il suffit qu'elle visite un site Internet l'affichant pour être infecté. Elle est alors renvoyée automatiquement vers un kit d'exploitation invisible **permettant aux cybercriminels d'installer à distance des malwares sur son ordinateur.** Vous trouverez ci-joint notre infographie expliquant la technique utilisée par Stegano pour infecter les ordinateurs.
« **Certaines des charges utiles que nous avons analysées comprennent des chevaux de Troie, des portes dérobées et des logiciels espions, mais nous pouvons tout aussi bien imaginer que la victime se retrouve confrontée à une attaque par ransomware,** » explique Robert Lipovsky, senior malware researcher chez ESET. « Cette menace montre combien il est important d'avoir un logiciel entièrement patché et d'être protégé par une solution de sécurité efficace et reconnue. Si l'utilisateur applique ces recommandations, il sera protégé contre ce genre d'attaque, » poursuit Robert Lipovsky.
« Stegano » fait référence à la sténographie, une technique utilisée par les cybercriminels pour cacher une partie de leur code malveillant dans les pixels d'images présents dans les bannières publicitaires. Ceux-ci sont masqués dans les paramètres contrôlant la transparence de chaque pixel. Cela entraîne un changement mineur des tons de l'image, rendant ces derniers invisibles à l'œil nu pour la victime potentielle.
Afin d'éviter de se retrouver infecté par le malware Stegano, ESET recommande aux utilisateurs de protéger leurs machines avec une solution de sécurité fiable et de mettre à jour les applications et le système d'exploitation.
Pour plus d'informations sur Stegano, nous vous invitons à consulter les deux articles suivants venant de WeliveSecurity. Le premier est l'analyse technique détaillée de Stegano, le second est une interview de Robert Lipovksy, Senior malware researcher chez ESET, expliquant la menace pour le grand public. Nous nous tenons à votre disposition pour plus de détails.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : Le malware Stegano infecte les machines à l'insu de ses victimes

---

Sony retire une backdoor dans ses caméras connectées

Sony retire une backdoor dans ses caméras connectées

Sony a corrigé le code source utilisé dans plusieurs de ses modèles de caméra de surveillance. Une porte dérobée avait été découverte par une société de sécurité informatique. En cette fin d'année, les caméras de surveillance ne sont pas à la fête.…[Lire la suite]

Denis JACOPINI Expert en cybercriminalité et en protection des données personnelles réalise des audits sécurité, vous explique comment vous protéger des pirates informatiques et vous aide à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (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

Piratage de ses comptes de réseaux sociaux. Comment réagir ?

Piratage de ses comptes de réseaux sociaux. Comment réagir ?

Vos comptes sociaux abritent une somme considérable de données personnelles. Veillez à bien les sécuriser pour éviter les piratages d'individus malveillants.

Prévenir un piratage

1.
Choisissez des mots de passe complexes, différents et non-signifiants !
Aucune personne ou ordinateur ne doit être en mesure de le deviner. La CNIL publie des conseils pour créer un mot de passe efficace, le retenir et le stocker dans une base.

2.
Ne communiquez pas votre mot de passe
Il est vivement déconseillé de communiquer votre mot de passe à une tierce personne, de l'enregistrer dans un navigateur si vous n'avez pas défini de mot de passe maître ou dans une application non sécurisée.

3.
Activez un dispositif d'alerte en cas d'intrusion
La double authentification est une option activable sur la plupart des réseaux sociaux. Lorsque vous vous connectez depuis un poste informatique inconnu, le réseau social vous demandera de confirmer l'accès en entrant un code que vous aurez reçu par sms ou par courrier électronique. D'autres fonctions proposent simplement de vous alerter si une personne extérieure tente de se connecter à votre compte depuis un terminal inconnu (PC, smartphone, tablette, mac).

4.
Déconnectez à distance les terminaux encore liés à votre compte
Là encore, cette option disponible sur la plupart des réseaux sociaux vous permet d'identifier l'ensemble des terminaux avec lesquels vous vous êtes connectés à votre compte. Lorsque cela est possible, il est conseillé de désactiver le lien avec les terminaux dont vous ne vous servez plus. Une connexion identifiée depuis un navigateur inconnu ou une ville inconnue pourra vous mettre la puce à l'oreille.

5.
Désactivez les applications tierces connectées à votre compte
Il arrive que les applications tierces connectées à votre compte soient vulnérables à une attaque extérieure. Il est conseillé de désactiver les applications tierces dont vous avez autorisés l'accès par le passé et qui ne vous servent plus.

6.
Réglez vos paramètres de confidentialité
En devinant votre nom, votre fonction, votre liste d'amis, une personne mal intentionnée pourrait facilement déduire des informations qui servent à réinitialiser votre compte ou simplement à usurper votre identité afin de changer votre mot de passe par exemple.

Repérer un piratage
- votre mot de passe est invalide
- des tweets/posts imprévus sont envoyés depuis votre compte
- des messages privés sont envoyés de façon non volontaires
- des comportements inhabituels ont lieu sur votre compte sans consentement (comme suivre, se désabonner, ou bloquer)
- une notification de la part du réseau social vous informe que « Vous avez récemment changé l'adresse électronique associée à votre compte. »

Réagir en cas de piratage
1. Signalez le compte piraté auprès du réseau social
2. Demandez une réinitialisation de votre mot de passe
3. Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques « sécurité » proposées par ces réseaux sociaux

---

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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
Cybersécurité & Conformité RGPD/CNIL
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Prévenir, repérer et réagir face au piratage de ses comptes sociaux | CNIL

Que contient la nouvelle doctrine de cybersécurité russe?

Que contient la nouvelle doctrine de cybersécurité russe?

Selon la nouvelle doctrine de cybersécurité nationale signée le 6 décembre par le président Vladimir Poutine, l'une des principales menaces à la cybersécurité russe est le « développement par de nombreux pays étrangers de leurs possibilités d'action sur l'infrastructure informatiqu…[Lire la suite]

Denis JACOPINI Expert en cybercriminalité et en protection des données personnelles réalise des audits sécurité, vous explique comment vous protéger des pirates informatiques et vous aide à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (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

Les « robots-avocats » : quand l’intelligence artificielle facilite les démarches juridiques

Les « robots-avocats » : quand l’intelligence artificielle facilite les démarches juridiques

Jump to Navigation -A+A Revue de presse6 décembre 2016 AVOCAT www.franceinfo.fr, 5 déc.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (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

Explosion de la cybercriminalité en 2016

Explosion de la cybercriminalité en 2016

En 2016, les peur des attentats s'est multipliée par six, selon une étude sur l'insécurité en France. Autre donnée importante : en cinq ans, les personnes victimes de retraits frauduleux sur leurs comptes bancaires ont doublé.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.

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

---

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

Original de l'article mis en page : Explosion de la cybercriminalité en 2016 — Fdesouche

Et si la publicité sur Internet était aussi infectée par des malwares ?

Et si la publicité sur Internet était aussi infectée par des malwares ?

Les chercheurs ESET viennent de découvrir Stegano, un nouveau kit d'exploitation se propageant via des campagnes publicitaires. De très nombreux sites Internet à forte notoriété ayant des millions de visiteurs quotidiens sont touchés.

Les systèmes de détection ESET montrent qu'au cours des deux derniers mois, Stegano a été affiché auprès de plus d'un million d'utilisateurs. Stegano se cache dans les images publicitaires affichées sur les pages d'accueil des sites Internet.
Depuis le début du mois d'octobre 2016, des cybercriminels ciblent les utilisateurs d'Internet Explorer et analysent leur ordinateur pour détecter les vulnérabilités dans Flash Player. En exploitant leurs failles, ils tentent de télécharger et d'exécuter à distance différents types de malwares.
Ces attaques se rangent dans la catégorie des publicités malveillantes, c'est-à-dire que des codes malicieux sont distribués via des bannières publicitaires. **La victime n'a même pas besoin de cliquer sur la publicité** : il suffit qu'elle visite un site Internet l'affichant pour être infecté. Elle est alors renvoyée automatiquement vers un kit d'exploitation invisible **permettant aux cybercriminels d'installer à distance des malwares sur son ordinateur**.
« **Certaines des charges utiles que nous avons analysées comprennent des chevaux de Troie, des portes dérobées et des logiciels espions, mais nous pouvons tout aussi bien imaginer que la victime se retrouve confrontée à une attaque par ransomware**, » explique Robert Lipovsky, senior malware researcher chez ESET. « Cette menace montre combien il est important d'avoir un logiciel entièrement patché et d'être protégé par une solution de sécurité efficace et reconnue. Si l'utilisateur applique ces recommandations, il sera protégé contre ce genre d'attaque, » poursuit Robert Lipovsky.
« Stegano » fait référence à la sténographie, une technique utilisée par les cybercriminels pour cacher une partie de leur code malveillant dans les pixels d'images présents dans les bannières publicitaires. Ceux-ci sont masqués dans les paramètres contrôlant la transparence de chaque pixel. Cela entraîne un changement mineur des tons de l'image, rendant ces derniers invisibles à l'œil nu pour la victime potentielle.
Afin d'éviter de se retrouver infecté par le malware Stegano, ESET recommande aux utilisateurs de protéger leurs machines avec une solution de sécurité fiable et de mettre à jour les applications et le système d'exploitation.
Pour plus d'informations sur Stegano, nous vous invitons à consulter les deux articles suivants venant de WeliveSecurity. Le premier est l'analyse technique détaillée de Stegano, le second est une interview de Robert Lipovksy, Senior malware researcher chez ESET, expliquant la menace pour le grand public. Nous nous tenons à votre disposition pour plus de détails.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Original de l'article mis en page : Boîte de réception (31) – denis.jacopini@gmail.com – Gmail