Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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

---

10 points à connaître sur l'attaques DDoS des États-unis

10 points à connaître sur l'attaques DDoS des États-unis

Le vendredi 21 Octobre, une série d'attaques par déni de service (DDoS) a provoqué une importante perturbation de l'accès aux sites Internet aux États-Unis. Les attaques ont ciblé les serveurs DNS (qui livrent les informations aux bonnes adresses), rendant de nombreux sites inaccessibles pendant plusieurs heures. Parmi eux figurent des sites permettant d'effectuer des achats en ligne, des réseaux sociaux, et d'écouter de la musique.

10 points à connaître sur l'attaque DDoS

ESET dresse un bilan des 10 points à retenir sur cette attaque. En voici un extrait, la version détaillée étant disponible sur WeLiveSecurity (version anglaise).

1. Les attaques ont ciblé la société Dyn, un important fournisseur de serveur DNS utilisé par de grands groupes comme Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, et le réseau Playstation.
2. Les attaquants ont piraté des milliers d'appareils connectés mal-protégés tels que les routeurs domestiques et les caméras de surveillance, pour former un réseau botnet.
3. L'attaque a été facilitée par la négligence des utilisateurs qui n'ont pas changé le mot de passe par défaut de leurs appareils.
4. L'exploitation d'appareils numériques par un code malveillant peut perturber l'activité économique d'un pays : il est probable que plusieurs millions de dollars de vente ligne soient perdus.
5. De nombreuses personnes malveillantes sont prêtes à nuire à l'activité économique d'un pays au moyen d'un code malveillant, et ce pour de multiples raisons.
6. L'information et l'éducation des utilisateurs sont primordiales.
7. La réduction du nombre d'appareils connectés vulnérables est un objectif réalisable et auquel les entreprises peuvent contribuer. Voici d'ailleurs 4 mesures recommandées par l'US CERT :

• Remplacer tous les mots de passe par défaut par des mots de passe forts ;
• Mettre à jour les objets connectés ;
• Désactiver l'UPnP (universal plug and play) des routeurs sauf en cas d'absolue nécessité ;
• Acheter des objets connectés auprès d'entreprises certifiant de fournir des dispositifs sécurisés.

1. Le code malveillant infectant les routeurs n'est pas nouveau et a déjà été repéré en mai 2015 par les équipe ESET.
2. Les nouvelles générations d'attaques DDos amplifient leur portée dans le fait qu'elles s'appuient sur de nombreux objets connectés.
3. Cette dernière attaque nous montre à quel point un pays peut être vulnérable en cas d'attaque de son système d'informations.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à 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 anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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

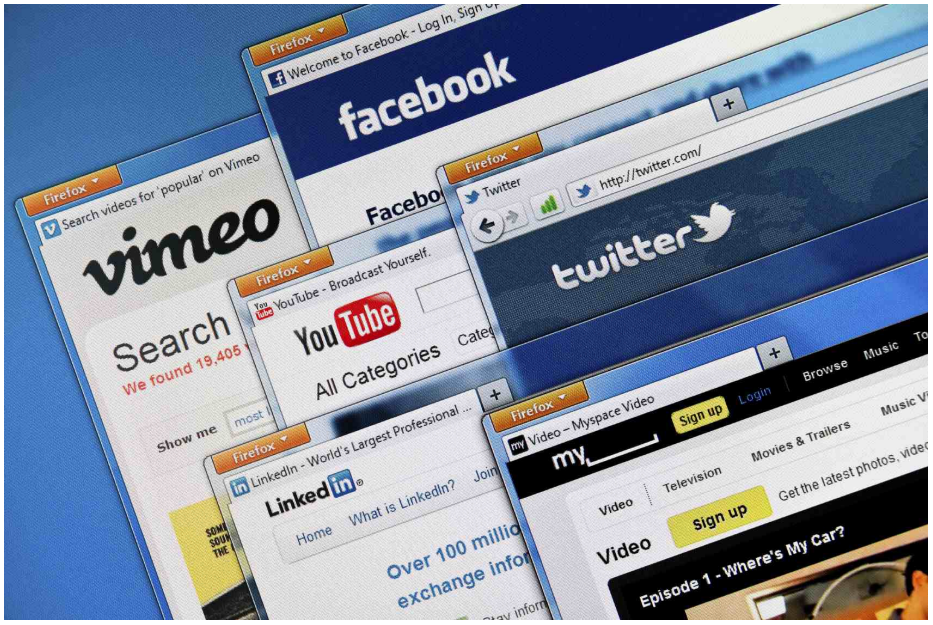
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : ESET livre les 10 points à connaître sur l’attaque DDoS – Global Security Mag Online

---

Six devoirs de cybersécurité pour la rentrée



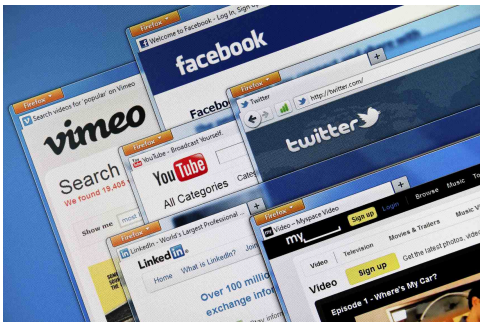
Six devoirs de cybersécurité pour la rentrée

La fin de l'été s'approche, ce qui implique le retour inévitable au travail. Après une période de repos est habituel que revenir à la routine ne soit pas facile, aussi quand il s'agit de mettre en pratique des mesures de sécurité et une précaution à nos dispositifs. Ces habitudes qui devraient déjà être acquises ne doivent pas s'abandonner et si elles n'existent toujours pas, c'est un bon moment pour commencer à se mettre à jour. La firme de sécurité Sophos Iberia propose ces conseils basiques pour une bonne routine de cybersécurité.

Des réseaux sociaux: publics ou privés ? À vous de choisir

Les réseaux sociaux ont déclenché un véritable phénomène international. Tout le monde s'y retrouve. Que l'on soit jeune ou plus vieux, tout le monde y est. Malgré le fait que ces soient des moyens intéressants pour se faire des amis, garder le contact, s'exprimer, partager ses émotions, ils présentent aussi une face cachée qui peut-être négative voire dangereuse car, parfois, **les réseaux sociaux peuvent donner une fausse sensation de sécurité.** Nous pensons que ce que nous publions peut seulement être vu par notre cercle plus proche d'amis, mais cela n'est pas toujours comme ça.

Il est nécessaire de configurer les **options de confidentialité** pour que les publications ne puissent pas être vues par n'importe quelle personne. Beaucoup d'utilisateurs ne comprennent pas cela et toute sa vie digitale est au découvert. Donc, comme première tâche, **accèdez aux options de confidentialité de vos réseaux sociaux (Facebook, Twitter, Instagram, et WhatsApp inclus) et décidez ce que vous voulez qu'il soit public**, et quoi est-ce que vous voulez maintenir dans le privé.



Sélectionnez bien vos contacts

Dans quelques réseaux sociaux, comme Twitter ou Linkedin, **il est habituel d'avoir beaucoup de contacts parmi lesquels nous ne connaissons pas tous personnellement.** Si nous maintenons un contrôle de ce que nous publions, il n'a pas de problème. Si nous sommes des utilisateurs qui partagent informations ou photographies plus personnelles, **nous devons être plus soigneux**: il est recommandable maintenir le profil privé (seulement à la vue des amis), et accepter comme contact seulement les personnes que nous connaissons. **Vous devez aussi penser à ce que vous partagez**, surtout quand il s'agit d'une information sensible comme la localisation.

Les mots de passe: différentes et privées

Il est très habituel entre les utilisateurs avoir un mot de passe unique pour quelques services. Avec la quantité de services que nous utilisons chaque jour, il est normal que nous ne puissions pas nous souvenir de toutes. **Mais il est recommandable avoir différents mots de passe dans chacun des comptes**, puisque **si quelqu'un réussit à accéder à l'une, il pourra accéder au reste.** Vous pouvez utiliser un gérant de mots de passe pour vous faciliter cette tâche.

Avant de déboucher, pensez deux fois

Les décharges, tant à travers des webs comme par courriers électroniques, sont la source de la plupart des infections des équipes, l'essor du ransomware est une bonne preuve de cela. C'est pourquoi, **il faut faire bien attention avant d'accéder à links**, des applications, des annonces ou webs qui peuvent être suspectes. Ah, et **cela ne s'applique pas seulement dans les Pcs aussi dans les smartphones.**

Fermez vos séances

Assurez-vous de fermer les séances de vos comptes quand vous aux dispositifs qui ne sont pas les vôtres, par exemple quand vous utiliserez un ordinateur public ou prêté. **Quelques services, comme Gmail ou Facebook, permettent de fermer les séances ouvertes de forme lointaine**, mais durant le temps qu'elles restent ouvertes et à la vue de n'importent qui **vos données sont exposés.**

Si vous le faites chez vous: pourquoi ne pas le faire en ligne?

Dans la porte de votre maison il y a une serrure: n'est pas? **Au réseau vous devez aussi mettre des empêchements pour que n'importe qui puisse accéder à vos informations**. Il est recommandable d'ajouter un mot de passe à votre ordinateur ou smartphone et aussi un code de déblocage. **Pour quelques utilisateurs il semble inconfortable, mais ces secondes extra peuvent vous éviter beaucoup de problèmes** comme que vos informations privées finissent aux mains étrangères.

…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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 : Six devoirs de cybersécurité pour la rentrée – Globb Security FR

Les protections de Windows complètement inefficaces à la technique AtomBombing !

Les protections de Windows complètement inefficaces à la technique AtomBombing !

Des chercheurs en sécurité ont découvert un mécanisme qui exploite une propriété propre à Windows pour en contourner tous les mécanismes de protection.

Une véritable bombe atomique pour l'intégrité de Windows. Une équipe de chercheurs de la société de sécurité israélienne Ensilo déclare avoir trouvé un moyen qui permet à un code malveillant de contourner toutes les barrières de sécurité possibles et inimaginables de l'OS de Microsoft. Et quelle que soit sa version. En l'occurrence, les experts ont effectué leurs travaux sur Windows 10.
La technique, qu'ils ont dénommée « AtomBombing » exploite les « Atom Tables ». Inhérentes au système d'exploitation, ces tables permettent aux applications de stocker les données et y accéder. Elles peuvent aussi être utilisées pour organiser le partage des informations entre les applications. *« Nous avons découvert qu'un attaquant pouvait écrire du code malveillant dans une table atom et forcer un programme légitime à récupérer ce code depuis la table*, explique le responsable de l'équipe de recherche Tal Liberman. *Nous avons également constaté que le programme légitime, maintenant infecté du code malveillant, peut être manipulé pour exécuter ce code. »* De plus amples détails sur la technique d'intrusion sont présentés sur cette page.

Pas de correctif possible

Ce n'est évidemment pas le premier cas connu de technique d'injection de code pour pénétrer le système et affaiblir son intégrité. Mais ces techniques s'appuient généralement sur des vulnérabilités de l'OS et la manipulation de son utilisateur amené, sans en avoir conscience, à déclencher l'exécution d'un code malveillant à travers un programme, comme un navigateur par exemple, pour contourner les barrières de sécurité.
Mais rien de tout cela dans le cas présent. *« AtomBombing est exécuté simplement en utilisant les mécanismes sous-jacents à Windows. Il n'est pas nécessaire d'exploiter les bugs ou les vulnérabilités du système d'exploitation*, assure le chercheur. *Comme la question ne peut être résolue, il n'y a pas de notion de correctif. Ainsi, la réponse pour atténuer [le risque] serait de plonger dans les appels des API et de surveiller les activités malveillantes. »* Autrement dit, pas de correctif possible mais du monitoring système en temps réel en quelque sorte (comme en propose au passage Ensilo). L'autre solution serait que Microsoft modifie l'architecture de Windows. Ce qui n'est pas prévu dans l'immédiat.
Ensilo reste discret – et c'est bien normal – sur la méthode pour injecter le code. A notre sens, l'exécution d'un tel script nécessite soit la complicité involontaire de son utilisateur (ce qui n'est pas nécessairement le plus compliqué), soit l'accès direct à une machine non protégée. En cas de succès, l'AtomBombing fait alors tomber toutes les barrières de protection selon les niveaux de restriction, peut accéder à des données spécifiques, y compris les mots de passe chiffrés, ou encore s'installer dans le navigateur pour en suivre toutes les opérations. Explosif !

Réagissez à cet article

Original de l’article mis en page : AtomBombing, le code insensible aux systèmes de protection de Windows

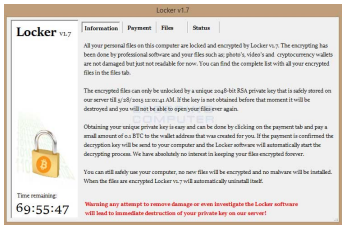
---

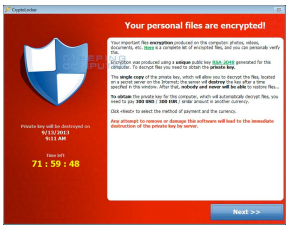
Comment vous protéger des Ransomwares ?

Comment vous protéger des Ransomwares ?

Cela n'est pas vraiment un scoop, les ransomwares sont en plein essor depuis quelques années. Comment concrètement protéger les utilisateurs d'un parc informatique contre ceux-ci ?

Il est d'abord crucial de rappeler que les utilisateurs sont le cœur du système d'information, ils en sont les principaux acteurs et représentent ainsi une ressource à protéger, en plus des données qu'ils manipulent et traitent, ils sont également le vecteur principal des attaques et des menaces.
Dans cet article nous allons passer en revu quelques points importants dans le but de protéger ses utilisateurs et son système d'information des infections de malware et notamment des ransomwares.
Pour rappel, un rançongiciel ou ransomware, est un malware (un programme, bout de code) qui va infecter un poste utilisateur, un serveur ou même un système informatique au complet, **pour chiffrer leur contenu de manière non définitive**. L'intérêt du pirate lors du déploiement d'un ransomware est de **prendre en otage les données de l'utilisateur**, qui n'y a plus accès puisqu'elles sont chiffrées. L'infection par un ransomware passe très souvent par l'affichage d'un message à l'utilisateur lui indiquant comment payer sa rançon afin, éventuellement, **d'obtenir une clé de déchiffrement lui permettant de récupérer ses données**.
Voici quelques exemple de ces messages :





Parmi les ransomwares les plus connus, et il y en a hélas beaucoup ces derniers temps, on retrouve :
• CryptoLocker : Ce cheval de Troie apparu en 2013 générait une pair de clé RSA 2048 bits et chiffrait certains documents en les repérant via leurs extension**s. Le malware demandait une rançon payable en Bitcoin et menaçait de supprimer les données au delà de 3 jours.** Ce délai n'était en réalité mis en place uniquement pour presser l'utilisateur et l'inciter à payer puisque les données étaient toujours récupérables, sous réserve d'en posséder la clé, après ce délai. Les gains de Evgeniy Bogachec, signalé comme responsable du déploiement du ransomware, ont été estimés à 3 millions de dollars.
• CryptoWall : Un cheval de Troie ciblant les OS Windows apparue en 2014, dérivé de CryptoLocker, **il se déployait notamment par l'intermédiaire de bannières publicitaires sur des sites web qui téléchargeaient et exécutaient le code malveillant**. La version 3.0 utilisait un payload écrit en Javascript, envoyé en pièce jointe des mails, qui était déguisé en image pour passer inaperçu auprès des utilisateurs. Environs 1 000 victimes de se ransomware on été constatée par le FBI en juin 2015, les rapports d'infection ont permis d'estimer une perte totale de 18 millions de dollars pour les victimes.
• Locky : Il s'agit d'un des ransomwares les plus actifs en 2016, il utilise le mail comme moyen d'infection avec un document word en pièce jointe. **Ce dernier contient des macros malicieuses et une partie de social engineering cherchant à convaincre les utilisateurs d'activer cette dernière**. La rançon demandée en échange de la clé de déchiffrement est généralement entre 0.5 et 1 bitcoins. Un fait marquant concernant ce ransomware est par exemple cas du Hollywood Presbyterian Medical Center qui a payé 17 000 dollars en bitcoin afin de récupérer ses données après une infection par le ransomware Locky
Il ne s'agit là que des plus connus, bien d'autres existent aujourd'hui.
Le scénario catastrophe est bien entendu celui présenté dans la série Mr Robot, **l'intégralité des postes utilisateurs et serveurs de l'entreprise E-corp se retrouvent infectés par un ransomware** et il est totalement impossible pour les administrateurs du parc informatique de retrouver une quelconque donnée, mis à part les backups restés offline. Ainsi, toutes les données de l'entreprise sont prises en otage.. A ce propos, avez vous des backups offline et mis à jour régulièrement ? 😉
Voici quelques points importants concernant la protection contre les ransomwares :

Garder un système d'information à jour

Qu'il s'agisse de la base anti-virus centralisée, des règles IDS/IPS ou de l'ensemble des applications métier, **les mises à jour permettent dans la plupart des cas d'éviter une infection qui souhaiterait se déployer en exploitant des vulnérabilités connues.** Il est en effet fort dommage d'être infecté par le biais d'une vulnérabilité connue et dont le correctif est disponible et aurait pu être appliqué. Ainsi, il est important d'avoir un processus de mise à jour réactif et bien organisé pour ces différents éléments. **Les anti-virus centralisés sont par exemple une bonne option** car le déploiement de la mise à jour des bases-virales et des signatures est directement intégré pour un déploiement sur tous les postes.
Également, des solutions comme WSUS permettent bien souvent de gérer finement les mises à jour, notamment celles de sécurité, afin d'évaluer l'impact sur une application métier par exemple.

La sensibilisation des utilisateurs

Il s'agit certainement du point le plus important, **à la fois le plus ardu mais aussi le plus efficace**. La sensibilisation de tous les acteurs du SI, et notamment des utilisateurs non technique, permet de mettre en place un comportement et une approche de la sécurité qui peut faire la différence. **Cela passe par des éléments aussi simple que de savoir évaluer la pertinence et la provenance exacte d'un mail reçu**, ainsi que du comportement à adopter en cas de doute. Mais également par des éléments techniques comme la possibilité de voir, dans la configuration par défaut des postes utilisateurs, les extensions de fichier afin d'y repérer un « *.pdf.exe* » par exemple.
La sensibilisation des utilisateurs est souvent **gérée par un l'équipe de sécurité ou les administrateurs systèmes**, cela requiert une compétence réelle en terme de pédagogie et certaines entreprises peuvent faire le choix d'externaliser ce point pour une meilleur efficacité. Pour commencer, il peut être mis en place dans un premier temps la diffusion d'une newsletter « *Informatique et sécurité* » diffusée une fois par mois aux utilisateurs et qui contiendrait les bonnes pratiques à adopter, les risques du moment, etc. Le tout en des termes non technique et de façon succincte pour que la newsletter soit lue.

Les backups

Cela a déjà été évoqué plus haut dans l'article, mais les backups sont votre seul recours en cas d'infection. En effet, même si la rançon est payée, il n'est pas toujours certains que les données soient retrouvées saines et sauves. Ainsi, **il vaut mieux opter pour une rétablissement des sauvegardes.** Dans ce cas, il faut que ces sauvegardes soient le plus à jour possible. Ainsi, il est important de mettre en place un processus de backup efface et régulier. **Ce point ne pose généralement pas de problème aux grandes entreprises qui en sont déjà munies** (qui n'a jamais supprimer un dossier important après une mauvaise manipulation ?), mais les entreprises en pleines croissances peines souvent à le mettre en place avant qu'un incident arrive.
Dans ce cas, il est important d'être proactif. Également, et dans les cas les plus avancés, la mise en place de backup offline est également vital. La fameuse sauvegarde sur cassette est alors une option à mettre en place en cas d'infection globale du SI.

Les filtres anti-spams et l'analyse des mails

Nous l'avons vu en détaillant les principes de fonctionnement de quelques ransomwares, le vecteur de transmission reste généralement le mail. Ainsi, disposer de bons filtres et anti-virus permet d'écarter la menace avant qu'elle n'arrive sur le poste de l'utilisateur.
Des solutions managées en mode SaaS peuvent ainsi être utilisés sans un processus trop lourd de mise en place et d'installation…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à 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 anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 : Ransomwares, des actions pour protéger ses utilisateurs – Information Security

---

Piratage de Dyn : l'attaque qui révèle le danger des objets connectés

L'attaque informatique qui a rendu inaccessible vendredi des géants du Web comme PayPal ou Twitter révèle les dangers en matière de sécurité informatique que représente l'engouement actuel pour les objets connectés. Explications.…[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

Nouvelles menaces informatiques et évolution des protection

Nouvelles menaces informatiques et évolution des protection

Destinés au grand public, ESET Internet Security et ESET Smart Security Premium apportent 5 nouvelles fonctions.

« Le tout nouveau produit ESET Internet Security vient s'ajouter à notre portefeuille de produits primés et offre aux utilisateurs les meilleures fonctionnalités en matière de détection, de vitesse et de convivialité. Ces nouveaux produits ajoutent à nos protections multi-couches existantes un ensemble de fonctionnalités centrées sur la protection de la vie privée » explique Eduard Kesely, Product Manager chez ESET.

ESET Internet Security, une protection optimale

ESET Internet Security s'adresse aux utilisateurs nécessitant une protection complète. Aux couches de sécurité déjà disponibles dans l'antivirus, s'ajoutent 3 nouvelles fonctionnalités :

• La protection contre les attaques par script.
• La protection Webcam qui signale les processus et les applications qui tentent d'accéder à la webcam de l'utilisateur et permet de les bloquer.
• La protection du réseau domestique qui permet à l'utilisateur de connaître l'identité des appareils connectés.

ESET Smart Security Premium, un produit haut de gamme

ESET propose un nouveau produit haut de gamme, ESET Smart Security Premium, destiné aux utilisateurs avancés et TPE. En plus des trois fonctionnalités ci-dessus, ESS Premium propose :

• Un gestionnaire de mots de passe.
• Le chiffrement des données pour les protéger en cas de vol ou de perte.

ESET cumule 3 récompenses prestigieuses : Pour la 98ème fois, ESET reçoit le prix VB100. De plus, il est le seul éditeur à avoir détecté 100% des menaces lors du test SE Labs (produits grand public) catégorie protection anti-malware. Enfin, le test réalisé par AV-Comparatives sur la protection anti-spam révèle qu'ESET est le N°1 haut la main.

La gamme ESET destinée aux particuliers, en plus de améliorations citées, couvre toujours macOS®, Android™ (antivirus et contrôle parental) afin de protéger l'intégralité de la famille.

Vous pouvez retrouver l'ensemble des fonctionnalités de nos produits sur https://www.eset.com/fr/

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à 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 anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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