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

Faut-il avoir peur des ransomwares ?

	Faut-il avoir peur des ransomwares ?

Depuis le premier virus détecté en 1986, le nombre d'attaque n'a cessé d'augmenter, devenant la menace la plus importante pour les entreprises.

En effet, cette forme d'attaque profite aux cybercriminels qui ont trouvé le bon filon pour gagner de l'argent. En constante mouvance, les formes d'attaques sont de plus en plus redoutables et ont généré un trafic de données important : les informations détenues par les entreprises sont désormais toutes disponibles en environnement virtuel et constituent l'élément essentiel pour l'économie de la société (données sensibles, fichiers clients, etc). Leur perte est inconcevable et cela, les cybercriminels l'ont bien compris. Au fil des ans, leurs techniques ont changé jusqu'à l'arrivée des ransomwares. Ce type d'attaque se révèle être la plus rentable pour les attaquants qui multiplient les variantes. La tendance est d'ailleurs à l'augmentation sur tous types de support connecté.
Parce que la perte de données en entreprise peut avoir des conséquences irrémédiables sur son activité si l'on prend en compte les paramètres suivants : perte de productivité, perte de données et la réputation liée à ces deux pertes, le non-paiement de factures émises, perte de confiance des salariés dans leur entreprise ; l'impact d'un ransomware peut être catastrophique. Le succès et les méthodes pour obtenir un paiement rapide de la rançon ont permis aux cybercriminels d'attirer l'attention des médias et d'entretenir ce climat de tension.
Il y a quelques mois, ESET a averti les utilisateurs qu'un nombre impressionnant d'e-mails infectés propageaient des ransomwares, submergeant ainsi les boîtes de réception dans le monde entier. Feignant de ne contenir que des fichiers inoffensifs, JS/TrojanDownloader.Nemucod essayait en réalité de forcer les victimes à télécharger et à installer des ransomwares tels que TeslaCrypt ou Locky. Cette stratégie fut efficace puisque les cybercriminels l'ont répété plusieurs fois, multipliant également les variantes utilisées tels que CTBLocker ou Filecoder.DG.
Heureusement les ransomwares ne sont pas toujours aussi dangereux que ceux cités ci-dessus. Beaucoup de cybercriminels amateurs surfent sur cette tendance et développent leur propre ransomware dont l'exécutable, de faible qualité, est facile à contrer. Ceci fut le cas de Petya et Jigsaw qu'ESET a analysé : tous deux contenaient des défauts de mise en œuvre qui ont permis aux victimes touchées de récupérer leurs fichiers sans payer un centime.

Comment vaincre cette peur du ransomware ?
Avoir peur du ransomware ne vous en protègera pas pour autant et payer la rançon ne résoudra pas forcément vos problèmes. Si vous en arrivez à ce stade, c'est que vous n'avez pas appliqué toutes les précautions nécessaires.
La meilleure façon de ne plus avoir peur des ransomwares est de se protéger avec une solution efficace et reconnue, et de s'assurer de couvrir 3 domaines complémentaires : technologique, politique de sécurité et éducation des employés. Sous l'impulsion de l'Etat et des agences de sécurité, les entreprises sont encouragées à adopter des mesures de protection. Les textes, dont le RGPD, étant là pour cadrer l'utilisation et la sécurité des données détenues par les entreprises. En particulier, les investissements dans la recherche et le développement de nouvelles technologies nécessitent un plan de sécurité permettant d'évaluer et de décrire leur sécurité.
Par conséquent, avec des attaques de plus grande envergure et l'émergence de nouvelles vulnérabilités, le plus grand défi de 2016 est de mettre l'accent sur la protection des réseaux et l'accès aux données. Les meilleures pratiques de sécurité doivent donc être appliquées pour protéger les données, les informations et la vie privée. Il s'agit là d'un travail transversal qui exige une participation active des plus hautes fonctions de l'entreprise.
Faut-il avoir peur des ransomwares ? La réponse est non pour tout dirigeant préparé à cette éventualité.
Source : Benoît Grunemwald – Directeur des Opérations ESET France

---

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.

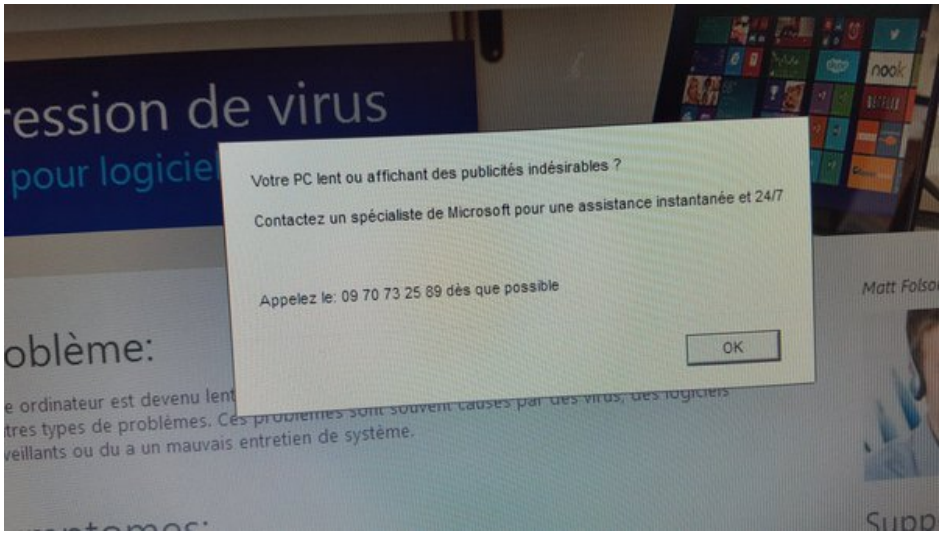
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Charts | ESET Virusradar

FakeAlert : Découverte d’une infection qui touche la France



FakeAlert : Découverte d’une infection qui touche la France

Détection d'une très forte augmentation du nombre d'échantillons du malware HTML / FakeAlert, à destination de la France.

HTML / FakeAlert est le nom générique donné par l'éditeur de solution de sécurité informatique ESET. Un terme qui nomme les fausses pages web hébergeant des messages d'alertes. Ces derniers indiquent à l'utilisateur qu'il est infecté par un virus ou qu'il a un autre problème susceptible de compromettre son ordinateur ou ses données. Pour stopper la soi-disant menace, l'utilisateur est invité à contacter par téléphone le faux support technique ou à télécharger une fausse solution de sécurité.
Le malware HTML / FakeAlert est généralement utilisé comme point de départ pour ce que l'on appelle les escroqueries de faux support. En conséquence, les victimes perdent de l'argent (en appelant des numéros surtaxés ou internationaux) ou sont infectés par un vrai malware installé sur leur ordinateur via les programmes « recommandés » figurant sur la page des fausses alertes…[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.

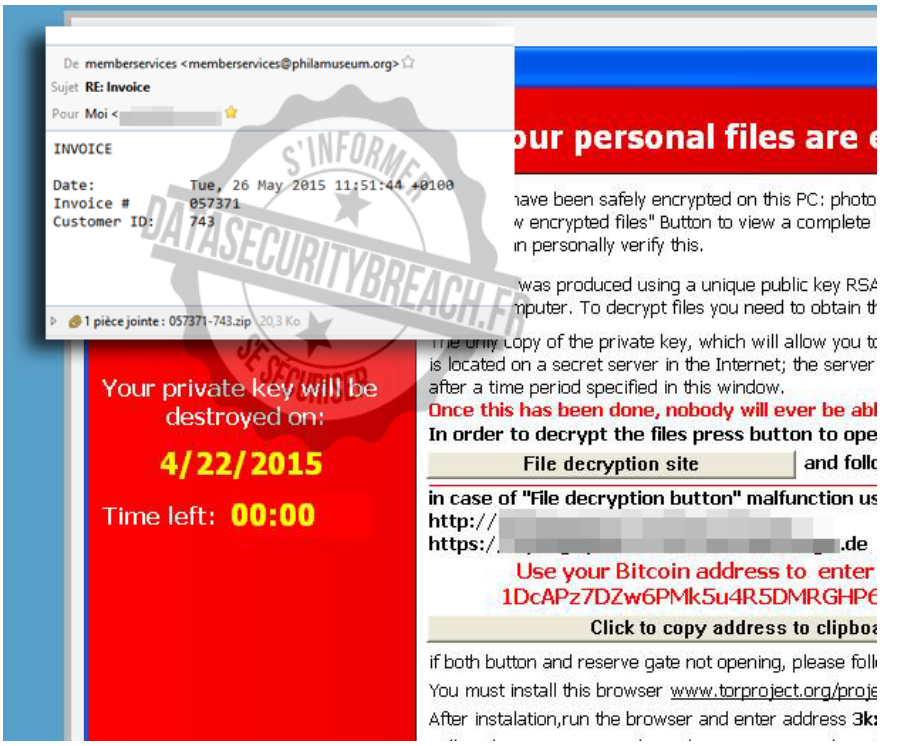
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : FakeAlert : Découverte d'une infection qui touche la France – ZATAZ

Mise à disposition de l’outil de déchiffrement contre le ransomware Polyglot



Mise à disposition de l’outil de déchiffrement contre le ransomware Polyglot

Les victimes du ransomware Polyglot, aussi connu sous le nom MarsJoke, peuvent maintenant récupérer leurs fichiers grâce à l'outil de déchiffrement développé par Kaspersky Lab.

Comment fonctionne Polyglot ? Il se propage via des emails de spam qui contiennent une pièce jointe malicieuse cachée dans une archive RAR. Durant le processus de chiffrement, il ne change pas le nom des fichiers infectés mais en bloque l'accès. Une fois le processus de chiffrement terminé, le wallpaper de bureau de la victime est remplacé par la demande de rançon. Les fraudeurs demandent que l'argent leur soit remis en bitcoins et si le paiement n'est pas fait dans les temps, le Trojan se détruit en laissant tous les fichiers chiffrés.

Lien avec CTB-Locker ?

Le fonctionnement et le design de ce nouveau ransomware sont proches de ceux de CTB-Locker, un autre ransomware découvert en 2014 qui compte de nombreuses victimes à travers le monde. Mais après analyse, les experts de Kaspersky Lab n'ont trouvé aucune similarité dans le code. En revanche, contrairement à CTB-Locker, le générateur de clés de chiffrement utilisé par Polyglot est faible. Les créateurs de Polyglot semblaient penser qu'en imitant CTB-Locker, ils pourraient piéger les utilisateurs en leur faisant croire qu'ils étaient victimes d'un grave malware, ne leur laissant d'autre option que de payer…[Téléchargez l'outil]

Article de Data Secutity Breach

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 : Outil de déchiffrement contre le ransomware Polyglot — Data Security BreachData Security Breach

Toutes les 4 secondes, un nouveau malware téléchargé

Toutes les 4 secondes, un nouveau malware est téléchargé

Selon Check Point, les téléchargements de logiciels malveillants inconnus ont été multipliés par 9 dans les entreprises. La faute aux employés ?

Dans leur rapport de sécurité 2016, les chercheurs de Check Point ont analysé plus de 31 000 incidents cyber touchant plusieurs milliers d'entreprises dans le monde. Résultat des courses : les téléchargements de logiciels malveillants explosent dans les entreprises.
L'an dernier, les téléchargements de malwares encore « inconnus » des systèmes de sécurité d'organisations ont été multipliés par 9, passant de 106 à plus de 970 téléchargements par heure, selon Check Point. En moyenne, un nouveau programme malveillant inconnu est téléchargé toutes les quatre secondes. Et les employés sont présentés comme le maillon faible dans ce domaine.

Maillon faible

Les malwares « connus » font également des dégâts (un téléchargement toutes les 81 secondes en moyenne) lorsque les systèmes sont irrégulièrement mis à jour et que les correctifs de sécurité font défaut. Une variante d'un programme malveillant peut aussi confondre un antivirus, au risque d'exposer les systèmes et réseaux d'une entreprise à l'espionnage et au vol de données…[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 : Un nouveau malware téléchargé toutes les 4 secondes

Les données de santé, la nouvelle cible des cybercriminels

	Les données de santé, la nouvelle cible des cybercriminels

Face au développement massif des nouvelles technologies, nos données personnelles sont aujourd'hui entièrement informatisées. De notre dossier médical jusqu'à nos données bancaires en passant par nos loisirs et notre consommation quotidienne, chaque minute de nos vies produit une trace numérique sans même que l'on s'en aperçoit.

Pendant des années nos données de santé étaient éparpillées entre médecins, laboratoire d'analyses, hôpitaux, dentistes dans des dossiers cartonnés qui s'accumulaient au coin d'un bureau ou sur une étagère. En 2012 la loi « hôpital numérique » avait permis un premier virage en obligeant la numérisation des données de santé par tous les professionnels pour une meilleure transmission inter-service. Depuis un an, la loi « santé 2015 » oblige à une unification et une centralisation des données de santé dans des serveurs hautement sécurisés constituant ainsi le Big Data.

Une centralisation des données qui n'est pas sans risque

Appliqué à la santé, le Big Data ouvre des perspectives réjouissantes dans le croisement et l'analyse de données permettant ainsi d'aboutir à de véritables progrès dans le domaine médical. Mais cela n'est pas sans risque.

Le statut strictement confidentiel et extrêmement protégé donne à ces données une très grande valeur. Nos données médicales deviennent ainsi la cible d'une nouvelle cybercriminalité, cotées sur le Dark Web.

Le Dark Web ou Deep Web est l'underground du net tel qu'on le connait. Il est une partie non référencée dans les moteurs de recherche, difficilement accessible où le cybertrafic y est une pratique généralisée. Sur le Dark Web les données personnelles sont cotées et prennent ou non de la valeur selon leur facilité d'accès et leur rendement.

Là où les données bancaires détournées sont de plus en plus difficiles à utiliser suite aux nombreuses sécurisations mise en place par les banques, l'usurpation d'identité et la récolte de données médicales prennent une valeur de plus en plus grande. Selon Vincent TRELY, président-fondateur de l'APSSIS, Association pour la Sécurité des Systèmes d'information, interviewer sur France Inter le 8 septembre 2016, le dossier médical d'une personne aurait une valeur actuelle qui peut varier entre 12 et 18 $.

Si l'on rapporte cette valeur unitaire au nombre de dossiers médicaux abrités par un hôpital parisien, on se rend compte que ceux-ci abritent une potentielle fortune pouvant aller jusqu'à des millions de dollars. Aussi pour protéger ces données, les organismes de santé se tournent vers des sociétés certifiées proposant un stockage dans des Datacenters surveillés, doublement sauvegardés, ventilés avec une maintenance 24h/24. Le stockage a donc un coût qui peut varier entre quelques centaines d'euros jusqu'à des centaines de milliers d'euros pour un grand hôpital. Le coût d'hébergement peut alors devenir un vrai frein pour des petites structures médicales où le personnel présent est rarement qualifié pour veiller à la sécurité numérique des données. Et c'est de cette façon que ces organismes deviennent des cibles potentielles pour les cybercriminels.

Des exemples il en existe à la Pelle. Le laboratoire Labio en 2015 s'est vu subtilisé une partie des résultats d'analyse de ses patients, pour ensuite devenir la victime d'un chantage. Les cybercriminels demandaient une rançon de 20 000 euros en échange de la non divulgation des données. Peu de temps après c'est le service de radiologie du centre Marie Curie à Valence qui s'est vu refuser l'accès à son dossier patients bloquant ainsi toute une journée les rendez-vous médicaux initialement fixés. Peu de temps avant, en janvier 2015, la Compagnie d'Assurance Américaine Anthem a reconnu s'être fait pirater. Toutes ses données clients ont été cryptées en l'échange d'une rançon.

Ces pratiques étant nouvelles, on peut s'attendre à une recrudescence de ce type de criminalité dans l'avenir selon les conclusions en décembre 2014 de la revue MIT Tech Review…[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 : Les données de santé, le nouvel El-Dorado de la cybercriminalité

Alerte : Le ransomware Locky passe en mode autopilote

Alerte : Le ransomware Locky passe en mode autopilote

Une nouvelle variante de Locky ajoute un mode autopilote qui proscrit les connexions aux serveurs de commandes et contrôles. Un mode toujours plus discret.
Il n'y a pas que les voitures autonomes qui se pilotent toutes seules (parfois avec des conséquences dramatiques). Les malwares aussi (avec des conséquences moins dramatiques humainement mais qui peuvent s'avérer aussi ennuyeuses qu'onéreuses). Locky, l'un des ransomwares les plus actif et tristement célèbre, connaît une nouvelle évolution. Il vient de passer en mode d'auto-pilotage. Autrement dit, l'agent malveillant n'a plus besoin de se connecter à un serveur distant de contrôle et commandes (C&C) pour engager le chiffrement des fichiers victimes de son attaque. C'est du moins ce qu'ont découvert les chercheurs en sécurité de l'éditeur Avira.

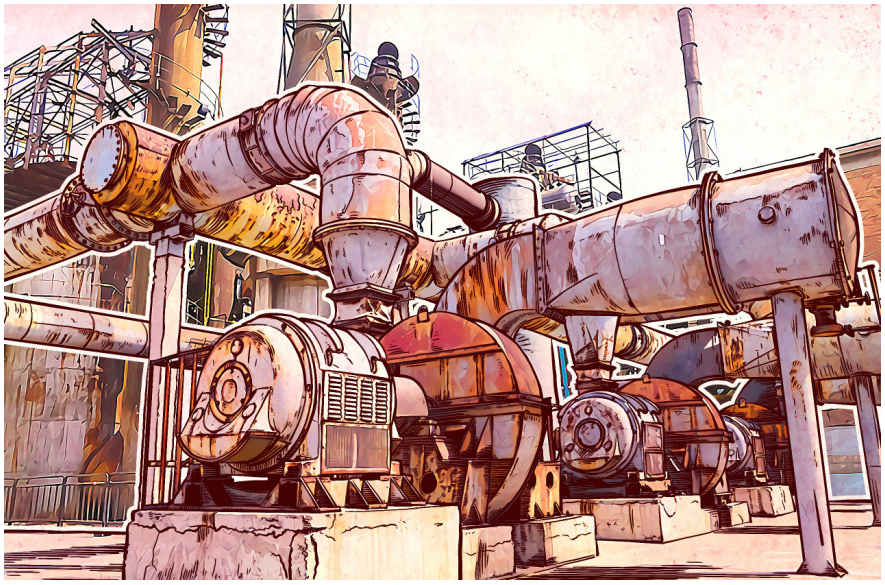
Locky en mode furtif
L'autopilotage permet désormais à Locky d'opérer en mode furtif. « Avec cette étape, [les attaquants] n'ont plus à jouer au chat et à la souris avec la mise en place incessante de nouveaux serveurs avant qu'ils ne soient blacklistés ou fermés », commente Moritz Kroll, spécialiste des logiciels malveillants au Protection Labs d'Avira. Il rappelle en effet que, précédemment, la configuration de Locky comprenait des URL pointant vers des serveurs de C&C ainsi qu'un algorithme de génération de domaines pour créer des liens supplémentaires vers des serveurs de commande et contrôle.
En se libérant de cette dépendance, le mode Autopilote du malware permet à ses auteurs (ou utilisateurs) d'économiser des coûts d'infrastructure et optimiser ainsi la rentabilité de leurs opérations. « Les cybercriminels affinent le mode d'infection 'hors-ligne', ajoute le chercheur d'Avira. En réduisant au minimum les activités en ligne de leur code, ils n'ont pas à payer pour autant de serveurs et de domaines supplémentaires. » Et si ce mode de fonctionnement déconnecté ne leur permet plus de remonter les statistique des infections en cours, il présente l'avantage de se montrer plus discret aux yeux des responsables du réseau. « Auparavant, les administrateurs systèmes pouvaient bloquer les connexions aux serveurs C&C et se prémunir des opérations de chiffrement de Locky. Ces jours sont désormais révolus, prévient Moritz Kroll. Locky a réduit les chances des victimes potentielles d'éviter une catastrophe de chiffrement. »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Ransomware : Locky active le mode pilotage automatique

---

Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

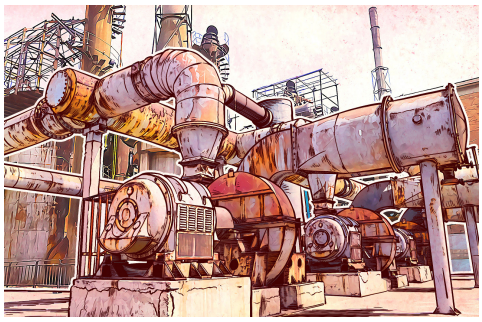


Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

---

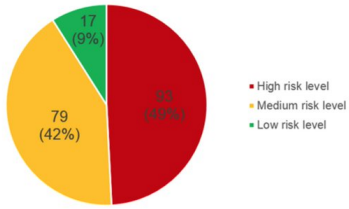
On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.

Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.



Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?

…[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 : Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Des serveurs Linux attaqués par le ransomware Fairware

Des serveurs Linux attaqués par le ransomware Fairware

Des exploitants de serveurs Linux signalent des attaques qui entraînent la disparition du dossier Internet du serveur et la non disponibilité des sites pendant une durée indéterminée.

Les participants aux forums de BleepingComputer se plaignent également de l'attaque : d'après la description fournie par une des victimes, cela ressemble plus à une attaque via force brute contre SSH. Notons qu'à chaque fois, le dossier Internet est supprimé et il ne reste que le fichier read_me qui contient un lien vers une page Pastebin où apparaît la demande de rançon.
Les individus malintentionnés promettent de rendre les fichiers contre 2 bitcoins et expliquent que le serveur de la victime a été infecté par le ransomware Fairware. Toutefois, à en croire Lawrence Abrams de chez Bleeping Computer, cette affirmation pourrait ne pas être tout à fait exacte.
« Si l'attaquant télécharge un programme ou un script pour réaliser « l'attaque », il s'agit alors bel et bien d'un [ransomware]. Malheureusement, nous ne disposons pas pour l'instant des informations suffisantes. Tous les rapports montrent que les serveurs ont été compromis, mais je n'ai pas encore eu l'occasion de le vérifier » a déclaré l'expert.
La demande de rançon contient l'adresse d'un portefeuille Bitcoin. La victime est invitée à réaliser le paiement dans les deux semaines, sans quoi les individus malintentionnés menacent d'écouler les fichiers sur le côté. Le message publié sur Pastebin possède le contenu suivant : « Nous sommes les seuls au monde qui pouvons vous rendre vos fichiers . Après l'attaque contre votre serveur, les fichiers ont été chiffrés et envoyés vers un serveur que nous contrôlons. »
Le message contient également une adresse email pour l'assistance technique, mais il est interdit à l'utilisateur d'y envoyer un message uniquement pour confirmer si les attaquants possèdent bien les fichiers perdus. Lawrence Abrams affirme que pour l'instant, il ne sait pas ce que les attaquants font avec les fichiers. Vu que les fichiers sont supprimés, il serait plus logique pour les conserver de les archiver et de les charger sur un serveur et non pas de les chiffrer et de gérer des clés individuelles.
En général, les ransomwares sont diffusés via l'exploitation de vulnérabilités ou par la victime elle-même qui est amenée, par la ruse, à exécuter le malware. Dans le cas qui nous occupe, rien ne trahit ce genre d'activité. Une des victimes indiquait sur le forum de Bleeping Computer que son serveur Linux avait été épargné en grande partie par l'attaque et que les fichiers de la base de données avaient été préservés. Ce commentaire indiquait également que les individus malintentionnés avaient laissé le fichier read_me dans le dossier racine.
La suppression de fichiers et le refus de confirmer leur vol sont des comportements inhabituels pour des individus malintentionnés qui travaillent avec des ransomwares. « Il est tout à fait possible qu'il s'agisse d'une escroquerie, mais dans ce cas c'est un mauvais business pour les attaquants » explique Lawrence Abrams. « Si l'escroc ne respecte pas sa promesse après le paiement de la rançon, il aura mauvaise réputation et plus personne ne le paiera. »
Toutefois, le message sur l'infection via le ransomware et la menace de publier les données volées sont en mesure de confondre la victime et de l'amener à répondre aux exigences des attaquants. Fairware n'est pas la première cybercampagne accompagnée d'une telle menace. L'année dernière, les exploitants du ransomware Chimera, avaient adopté une astuce similaire, même si leur malware n'était pas en mesure de voler les fichiers ou de les publier sur Internet.
Lawrence Abrams explique que les victimes de ransomwares devraient s'abstenir de payer la rançon, mais si elles décident d'agir ainsi, elles doivent au moins confirmer que le bénéficiaire du paiement possède bien les fichiers.
Article original de Securelist

Réagissez à cet article

Original de l’article mis en page : Fairware attaque des serveurs Linux – Securelist

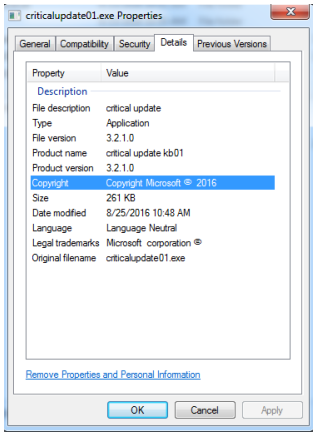
---

Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

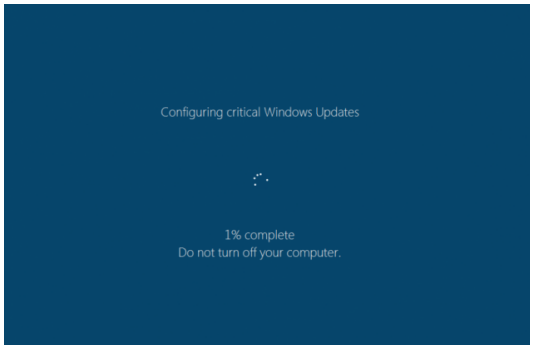
Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

Windows 10 lance automatiquement ses mises à jour, ainsi que tous les utilisateurs que ça importunent le savent. Une bonne opportunité pour les cybercriminels de sévir tranquillement.

C'est ainsi qu'un nouveau ransomware a été découvert par un analyste de chez AVG Technologies.
Un premier exécutable maquille ses propriétés afin de faire croire qu'il provient de Microsoft et qu'il s'agit d'une mise à jour critique.



Une fois ce malware installé, il en télécharge un autre dans le répertoire AppDataLocalTemp, sous le nom WindowsUpdate.exe. Puis il l'exécute.
Pour l'utilisateur, c'est une mise à jour qui s'est déclenchée, tant l'écran de cette seconde partie du malware est bien faite, avec les polices de Microsoft bien imitées.



L'utilisateur n'est pas surpris de voir que son disque dur tourne, tourne… Une 'expérience utilisateur' qu'il doit régulièrement supporter…
Sauf que là, le disque tourne parce que le malware en crypte toutes les données. Le méfait accomplit, un autre écran apparaît, moins habituel, avec une invitation à contacter les cybercriminels par mail, pour finalement devoir payer une rançon afin de récupérer les données.
Utilisateurs de Windows 10, la prochaine fois que vous verrez un écran de mise à jour, croisez les doigts !

Article original de fredericmazue

Denis JACOPINI vous recommande le logiciel de sécurité suivant :

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 : Fantom : un nouveau ransomware qui sévit sous Windows 10 | Programmez!