Le pire des ransomwares vous fait perdre vos données à vie

Le pire des ransomwares vous fait perdre vos données à vie

Dans la famille des logiciels malveillants, on trouve de tout : les virus, les trojans, les rootkits, les spywares… Et puis il a aussi les ransomwares, aussi appelés rançongiciels, qui consistent à chiffrer les données d'un utilisateur, et à lui réclamer une certaine somme en échange de la clé de déchiffrage.

Mais récemment est apparu un nouveau ransomware appelé Power Worm.
Sa particularité ? Être tellement mal codé qu'il est impossible de déchiffrer ensuite les données corrompues, même en mettant la main au porte-monnaie.
Power Worm s'en prend aux fichiers Word et Excel en les chiffrant sans que l'utilisateur ne s'en aperçoive.
En théorie, lorsqu'il souhaite ensuite accéder à ces données, celui-ci est alors contraint de payer la coquette somme de 700 euros pour les récupérer. Mais dans sa toute dernière version, Power Worm détruit littéralement l'une des clés qui permettraient de déchiffrer les données.
En conséquence, il est totalement impossible d'accéder au contenu des fichiers chiffrés. Inutile donc de payer les 700 euros réclamés par l'auteur de ce malware, cela ne sert à rien. Le chercheur Lawrence Abrams, expert en malwares, explique sur le site Bleeping Computer qu'il « n'y a malheureusement rien qui puisse être fait pour les victimes de cette infection. Si vous avez été infecté par ce ransomware, votre seule option est de restaurer une sauvegarde de vos données ».

C'est visiblement une carence dans le code la part de l'auteur qui est à l'origine de ce gros bug : ça n'était pas volontaire d'après le chercheur Nathan Scott, qui a découvert ce défaut de conception. L'unique moyen de se préserver d'une telle situation reste de laisser constamment en place un antivirus sur sa machine. Ici, peu importe qu'ils soient gratuits ou payants : ils devraient tous remplir leur office et empêcher n'importe quel ransomware de s'installer, et en particulier interdire Power Worm de chiffrer les données de l'utilisateur.

Source : http://www.tomsguide.fr/actualite/power-worm-ransomware,49134.html

Un outil gratuit pour immuniser les ordinateurs et bloquer les menaces du ransomware CryptoWall 4.0

Un outil gratuit pour immuniser les ordinateurs et bloquer les menaces du ransomware CryptoWall 4.0

Les chercheurs spécialistes en malwares et experts en cyber-sécurité de Bitdefender ont développé un outil gratuit afin de stopper la propagation du malware CryptoWall 4.0. Ce logiciel permet aux utilisateurs d'immuniser leurs ordinateurs et de bloquer les tentatives de chiffrement de fichiers.

L'outil peut être installé et utilisé en tant que mesure préventive, comme un vaccin, exclusivement contre cette variante spécifique de ransomware. Si l'ordinateur est déjà infecté par CryptoWall 4.0, ce vaccin n'aidera pas à désinfecter la machine.

Les pays ciblés jusqu'ici, identifiés par Bitdefender, incluent : la France, l'Italie, l'Allemagne, l'Inde, la Roumanie, l'Espagne, les États-Unis, la Chine, le Kenya, l'Afrique du Sud, le Koweït et les Philippines.

Les serveurs de spam de CryptoWall 4.0 sont situés en Russie et le malware écrit en Javascript, télécharge le composant de ce ransomware depuis un serveur russe. Les investigations de Bitdefender révèlent aussi que l'algorithme de chiffrement utilisé est de l'AES 256. Seule la clef est chiffrée en RSA 2048, qui est un algorithme impossible à déchiffrer du fait de sa complexité, mais qui demande beaucoup de ressources. Les utilisateurs russes semblent être à l'abri.

Le malware ne poursuit pas le chiffrement s'il détecte que la langue du clavier est le russe.

Dans la lignée de ses prédécesseurs, CryptoWall est rapidement devenu un succès financier pour ses créateurs. De récents chiffres montrent que les dommages liés à CryptoWall 3.0 s'élèvent à 325 millions de dollars, uniquement aux États-Unis. Ce succès a incité d'autres groupes de cybercriminels à écrire un nouveau code qui utilise des algorithmes de chiffrage plus sophistiqués. Par conséquent, il devient de plus en plus difficile pour les éditeurs d'antivirus de déchiffrer le code et de proposer une solution.

Bitdefender rappelle aux utilisateurs que cet outil agit comme une couche supplémentaire de protection, qui intervient en complément d'une solution antimalware.

Les utilisateurs des solutions de sécurité Bitdefender 2016 sont d'ores et déjà protégés contre le chiffrement de CryptoWall. La nouvelle technologie anti-ransomware de Bitdefender, unique sur le marché, empêche le chiffrement de fichiers et documents personnels et protège ainsi contre tous les rançongiciels, même nouveaux et inconnus.

Téléchargez gratuitement ICI le vaccin de Bitdefender contre CryptoWall 4.0
http://labs.bitdefender.com/projects/cryptowall-vaccine-2/bitdefender-offers-cryptowall-vaccine/

Les chercheurs en malwares de Bitdefender ont analysé un échantillon de nouvelles souches du malware et ont observé de nettes différences entre CryptoWall 4.0 et ses prédécesseurs.

Source : http://www.globalsecuritymag.fr/Bitdefender-a-developpe-un-outil,20151110,57433.html

Le pire des ransomwares vous fait perdre vos données à vie

Le pire des ransomwares vous fait perdre vos données à vie

Recrudescence de l’hacktivisme et des extorsions en ligne en 2016 | Le Net Expert Informatique

Recrudescence de l’hacktivisme et des extorsions en ligne en 2016

Trend Micro publie son rapport annuel de prédictions de sécurité 2016 : “The Fine Line : 2016 Security Predictions”. L’an prochain, les extorsions, l’hacktivisme et les malware mobiles devraient continuer de se développer. En parallèle, les administrations et les entreprises adopteront une posture plus offensive en matière de cyber-sécurité.

« Nous pensons que 2016 sera une année majeure, tant pour les cybercriminels que pour ceux qui souhaitent s’en protéger », explique Raimund Genes, CTO de Trend Micro. « Les administrations, au même titre que les entreprises, prendront conscience des bénéfices qu’apporte l’anticipation dans le domaine de la cyber-sécurité, avec une évolution attendue du cadre réglementaire et une augmentation des recrutements de responsables cyber-sécurité au sein des organisations. Parallèlement, alors que les utilisateurs sont de plus informés sur les menaces en ligne, les cyber-pirates s’adapteront en concevant des schémas sophistiqués et personnalisés pour cibler les particuliers comme les entreprises. »

Selon ce rapport, 2016 marquera un tournant significatif dans le domaine de la publicité malveillante (malvertising). Rien qu’aux États-Unis cette année, 48 % des internautes utilisent déjà des logiciels permettant de bloquer les publicités. Alors que l’utilisation de ces logiciels a bondi de 41% en 2015 dans le monde, les annonceurs vont modifier leur approche de la publicité en ligne, tandis que les cybercriminels tenteront d’identifier de nouveaux moyens pour obtenir les informations personnelles des internautes.

L’extorsion en ligne devrait croître rapidement, en faisant la part belle à l’analyse psychologique des victimes et aux techniques d’ingénierie sociale. Les hacktivistes seront amenés à divulguer des informations toujours plus incriminantes, impactant fortement leurs cibles et encourageant les infections secondaires.

« Les hackers évoluent en permanence pour s’adapter à leur environnement et, alors que la publicité en ligne décline, nous assistons à une progression des ransomware », constate Tom Kellermann, Chief Cybersecurity Officer, Trend Micro. « Face à des investissements croissants en sécurité et une réglementation qui se durcit, ce sont précisément ces évolutions qui aboutiront à de nouveaux vecteurs et méthodes d’attaques toujours plus sophistiqués ».

Parmi les principales prédictions de Trend Micro pour 2016 :

Les cybercriminels devraient utiliser de nouvelles méthodes pour personnaliser leurs attaques, faisant certainement de 2016 une année historique en matière d’extorsion en ligne

Le nombre de malware mobiles devrait franchir la barre des 20 millions, affectant notamment la Chine, tandis que les nouveaux moyens de paiement en ligne deviendront les principales cibles à l’échelle mondiale

Les objets et équipements intelligents étant de plus en plus utilisés au quotidien par le grand public, au moins une faille de sécurité sur ces derniers devrait s’avérer mortelle

Les hacktivistes vont faire évoluer leurs méthodes d’attaque de façon à détruire systématiquement leurs cibles par des fuites de données de très haut niveau

Moins de 50% des organisations devraient disposer d’experts en cyber-sécurité au sein de leurs équipes d’ici à fin 2016

La croissance des solutions et services de blocage de publicités devrait inciter les cybercriminels à trouver de nouvelles méthodes pour cibler leurs victimes, entraînant ainsi un recul des publicités malveillantes

La réglementation va évoluer vers un modèle de cyber-sécurité mondiale, permettant des poursuites, des arrestations et des condamnations de cybercriminels plus efficaces

Pour en savoir davantage sur les prévisions de sécurité en 2016 de Trend Micro, rendez-vous sur : http://www.trendmicro.fr/renseignem…

Source : http://www.globalsecuritymag.fr/Predictions-2016-Trend-Micro,20151106,57314.html

Je Suis Paris | Le Net Expert Informatique

Je
Suis
Paris

Loin des spams, des arnaque et de tous les actes illicites que nous suivons sur Internet depuis plusieurs années, nous partageons notre peine avec les victimes des attentats de Paris de ce Vendredi 13 Novembre 2015.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

Une grosse panne à l'aéroport d'Orly provoquée par un système tournant sous… Windows 3.1 | Le Net Expert Informatique

Une grosse panne à l'aéroport d'Orly provoquée par un système tournant sous… Windows 3.1

Le 7 novembre, soit samedi dernier, une énorme panne a cloué les avions au sol pendant plusieurs heures à l'aéroport d'Orly. Une panne provoquée par une panne informatique d'une des tours de contrôle qui scrute les données météo. Après plusieurs heures, le trafic a repris et l'histoire aurait pu s'arrêter là. Mais le Canard Enchaîné a révélé la vraie nature de cet incident.

L'hebdomadaire revient en effet sur cette panne. Selon lui, elle concernait le système Decor (qui fourni les données météo) tournant sous… Windows 3.1. Un OS sorti en 1992, tout de même. C'est à cause d'une défaillance de ce système que des milliers de passagers se sont retrouvés bloqués. Dans le Canard, un ingénieur de l'aéroport donne d'ailleurs son avis sur la situation :

Samedi matin, le trafic n'était pas vraiment dense. Mais imaginez, pendant la COP21, le ballet des chefs d'Etat perturbé à cause d'un logiciel informatique qui date de la préhistoire. De quoi aura-t-on l'air ?

C'est vrai que l'histoire est tout de même étonnante, voire pathétique. Mais comme l'affirme l'hebdomadaire, le ministre des transports prévoit de renouveler le parc informatique de l'aéroport à partir de 2017.

Source :
http://www.journaldugeek.com/2015/11/12/une-grosse-panne-a-laeroport-dorly-provoquee-par-un-systeme-tournant-sous-windows-3-1/

Une faille dans un composant expose des milliers d’applications Java | Le Net Expert Informatique

Une faille dans un composant expose des milliers d’applications Java

Découverte il y a 9 mois, une vulnérabilité non corrigée dans le composant Apache Commons Collections expose les serveurs d'applications Java à un sérieux risque d'exécution de code à distance.

La dernière faille critique Java en date a été découverte dans la bibliothèque Apache Commons qui regroupe un ensemble de composants Java dont la maintenance est assurée par l'Apache Software Foundation. La bibliothèque est utilisée par défaut dans plusieurs serveurs d'applications Java et dans des produits comme Oracle WebLogic, IBM WebSphere, JBoss, Jenkins et OpenNMS.

La vulnérabilité, précisément localisée dans le composant Collections d'Apache Commons, résulte directement de la désérialisation des objets Java. Dans les langages de programmation, la sérialisation désigne le processus de conversion des données en format binaire. Cette conversion permet le stockage des données dans un fichier ou dans la mémoire, ou leur envoi sur le réseau. La désérialisation est le processus inverse.

La vulnérabilité, signalée par les chercheurs Chris Frohoff et Gabriel Lawrence en janvier 2015 pendant une conférence sur la sécurité, n'a pas suscité beaucoup d'attention. Sans doute que la plupart des gens estiment que la responsabilité de la prévention des attaques exploitant le processus de désérialisation incombe aux développeurs d'applications Java et non aux créateurs de la bibliothèque.

« Je ne pense pas qu'il faut incriminer la bibliothèque, même si elle peut certainement être améliorée », a déclaré par courriel Carsten Eiram, responsable de la recherche dans l'entreprise de sécurité Risk Based Security.

« En définitive, une entrée non fiable ne devrait jamais être désérialisée aveuglément. Les développeurs devraient comprendre comment fonctionne une bibliothèque et valider chaque entrée au lieu de lui faire confiance ou espérer qu'elle effectue à leur place ce travail de sécurisation ».

Un correctif bientôt disponible

Vendredi dernier, la faille est revenue dans l'actualité : les chercheurs de l'entreprise de sécurité FoxGLove ont livré des exploits proof-of-concept pour WebLogic, WebSphere, JBoss, Jenkins et OpenNMS basés sur la vulnérabilité. Mardi, Oracle a publié un avis de sécurité comportant des instructions d'atténuation temporaires pour WebLogic Server en attendant le correctif permanent que l'éditeur est en train de mettre au point. Les développeurs d'Apache Commons Collections ont également commencé à travailler sur un correctif.

Apache Commons Collections contient une classe InvokerTransformer. La faille utilise la sérialisation Java et une méthode d'appel dynamique dite de réflexion sur la classe InvokerTransformer pour exécuter du code distant. Un attaquant pourrait fabriquer un objet sérialisé avec un contenu malveillant pour qu'il soit exécuté au moment de sa désérialisation par une application Java avec l'aide de la bibliothèque Apache Commons. « Prises séparément, la classe InvokerTransformer et la sérialisation ne sont pas en cause, mais dès qu'elles sont combinées, la question de sécurité apparaît », a déclaré Joshua Corman, CTO de Sonatype, une entreprise d'automatisation de la chaîne d'approvisionnement des logiciels qui aide les développeurs à suivre et à gérer les composants qu'ils utilisent dans leurs applications.

D'autres composants Apache Commons vulnérables

Joshua Corman et Bruce Mayhew, un autre chercheur en sécurité de Sonatype, pensent que le problème ne concerne pas uniquement le composant Collections d'Apache Commons. Selon eux, d'autres composants Java pourraient poser un problème identique. « Je peux vous assurer qu'aujourd'hui, un tas de gens passent les composants les plus courants au peigne fin pour identifier d'autres classes sérialisables qui pourraient permettre l'exécution de commandes à distance », a déclaré Bruce Mayhew. « Et parmi eux, il y a des gens bien intentionnés, mais probablement aussi des gens mal intentionnés ». Si l'on en croit les discussions en cours sur la recherche de bogues, InvokerTransformer n'est sans doute pas la seule classe vulnérable de l'environnement Apache Commons Collections. Trois autres classes pourraient présenter le même problème. Les chercheurs de FoxGLove Security se sont intéressés de près à des projets de logiciels publics utilisables en « commons-collection » hébergés sur GitHub et ils ont identifié 1300 sources possibles. Et il faut aussi prendre en compte les milliers d'applications Java qui utilisent la bibliothèque dans les environnements d'entreprise.

Même s'il y a une forte probabilité que le problème dépasse le composant Collections, les développeurs devraient essayer de retirer les commons-collections du classpath ou de supprimer la classe InvokerTransformer du fichier jar concerné tant qu'il n'y a pas de correctif disponible pour la vulnérabilité. Mais tous ces changements doivent être appliqués avec précaution, car ils peuvent rendre les applications inopérantes.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-faille-dans-un-composant-expose-des-milliers-d-applications-java-62956.html
Par Lucian Constantin, IDG NS (adaptation Jean Elyan)

Une plateforme en ligne pour combattre le Phishing | Le

Net Expert Informatique

	**Une plateforme en ligne pour combattre le Phishing**

Face à l'expansion du hameçonnage (phishing), la police judiciaire française a décidé de s'allier au privé. Une initiative « exceptionnelle », relate l'AFP, présente lors de la signature, le 4 novembre, d'une convention avec l'association privée Phishing Initiative. Cette plateforme, fondée par Microsoft, PayPal et Lexsi, offre aux internautes la possibilité de lutter contre ces menaces en dénonçant l'adresse d'un site – mais pas de mails.

Pour la PJ, il s'agit d'abord de mettre l'accent sur la prévention. C'est, d'un point de vue réaliste, sa seule façon d'agir contre ce phénomène trop complexe à appréhender. Catherine Chambon, sous-directrice de la lutte contre la cybercriminalité à la direction centrale de la PJ, a expliqué à l'agence de presse que les faits étaient le plus souvent « générés par un seul auteur, de l'étranger » ce qui rend les enquêtes « longues ».

Une menace grave

En 2014, 137 000 signalements ont été effectués sur la plateforme gouvernementale Pharos, dont un tiers concernait le phishing. Depuis le début 2015, Phishing Initiative a récolté pour sa part 60 000 signalements dont 35 000 relevaient du hameçonnage. Derrière ces faux e-mails envoyés par des usurpateurs se cachent parfois des attaques hypersophistiquées comme celle menée en février à l'encontre de cent grandes banques.

Pour la société dont l'identité a été volée (une banque, un assureur, un service en ligne…), les dégâts sont d'une autre nature. Elle, qui investit énormément en communication et en marketing, peut voir ruinée sa réputation en quelques heures à peine, selon l'expert Return Path, en raison d'une campagne de phishing.

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-785286-police-phishing.html

Phishing : Lexsi et Microsoft s’allient à la plateforme Pharos | Le Net Expert Informatique

	Phishing : Lexsi et Microsoft s’allient à la plateforme Pharos

Le phishing a la cote : cette technique de social engineering consiste, via l'envoi de mail frauduleux ou la création de faux sites web arborant les couleurs d'un service ou d'une administration, à soutirer des identifiants aux victimes qui pensent se connecter sur le site légitime. Simple, facile à automatiser, le phishing est une attaque de plus en plus courante comme le soulignent les chiffres de la plateforme : en 2015, la Phishing Initiative a ainsi repéré plus de 35.000 URL jugées malveillantes.

La plateforme Phishing Initiative a été lancée par des sociétés privées (Lexsi et Microsoft notamment, mais Google est aussi partenaire du projet) et annonce aujourd'hui un partenariat avec Pharos, la plateforme de signalement mise en place par l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.)

« C'est un partenariat qui porte sur deux volets principaux » explique à ZDNet.fr Jérôme Robert, responsable marketing du groupe Lexsi « D'une part, le partenariat permettra de mettre en place un échange de données : quand un site de phishing sera signalé chez Pharos, ils nous transmettront leurs informations. A l'inverse, on leur transmettra également les informations que nous avons, bien que notre dispositif seul ne permette pas l'ouverture d'une plainte. D'autre part, on espère également pouvoir bénéficier d'une certaine visibilité à travers ce partenariat. »

Lutter contre le hameçonnage des particuliers

La plateforme Phishing Initiative s'adresse avant tout aux particuliers et permet de communiquer une URL jugée suspicieuse par l'utilisateur. Une fois l'URL transmise, des experts de Lexsi analysent le site afin d'écarter d'éventuels faux positifs. Si celle-ci est jugée malveillante, elle est transmise à Microsoft et Google qui peuvent l'ajouter à leurs listes noires de sites web, présentant un avertissement aux utilisateurs qui tentent de s'y connecter.

Des listes noires qui sont partagées par les principaux éditeurs de navigateur et qui permettent donc d'assurer une plus grande sécurité des internautes. En parallèle de cela, Lexsi se charge également de prendre des mesures afin de signaler le site et de le faire fermer.

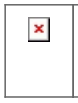
Le service est entièrement gratuit, destiné aux particuliers qui ont été redirigés ou confronté à un site malveillant. « On a remarqué que pas mal d'entreprises avaient également recours à notre service pour signaler des tentatives de phishing » poursuit Jérôme Robert « Ça ne nous dérange pas et on n'entend pas du tout limiter cela. Mais on permet aux entreprises qui le désirent de sponsoriser l'initiative à hauteur de 5000 euros par an, et on envisage de proposer des services additionnels aux entreprises, tels que la possibilité de soumettre des URL en masse pour 1500 euros. »

L'effort permettra également au groupe Phishing Initiative de nourrir différents rapports sur les tendances des la cybercriminalité en ligne.

Source :

http://www.zdnet.fr/actualites/phishing-lexsi-et-microsoft-s-allient-a-la-plateforme-pharos-39827758.htm

La surveillance des communications internationales validée | Le Net Expert Informatique



La surveillance des communications internationales validée

Le Parlement a adopté un texte comblant un vide laissé par la loi renseignement. La surveillance des communications internationales impliquera moins de contrôles que celle des interceptions effectuées dans l'Hexagone.

Le débat est clos. Le Parlement a adopté définitivement jeudi 5 novembre par un dernier vote de l'Assemblée la proposition de loi destinée à légaliser la surveillance des communications internationales, qui resteront soumises à moins de contrôles que les interceptions effectuées en France.

Les députés ont voté le texte dans les mêmes termes que les sénateurs un peu plus tôt dans la journée.

Le législateur compétent

La proposition de loi a pour objet de pallier un vide juridique résultant de la censure par le Conseil constitutionnel d'une disposition de la loi renseignement. Celle-ci, qui légalise et encadre l'activité des services en France, était restée floue pour leurs activités à l'étranger, renvoyant cela à un décret en Conseil d'État.

Mais le Conseil constitutionnel a jugé que c'était au législateur d'agir dès lors que des libertés publiques étaient concernées.

Une autorisation du Premier ministre

Les auteurs du texte, les députés socialistes Patricia Adam et Philippe Nauche, respectivement présidente et vice-président de la commission de la Défense à l'Assemblée, ont proposé un cadre juridique spécifique en introduisant un nouveau chapitre dans le code de la sécurité intérieure.

Dès lors que « la défense et la promotion des intérêts fondamentaux de la Nation », qui comprennent notamment « les intérêts économiques, industriels et scientifiques majeurs » de la France, sont concernées, « la surveillance des communications qui sont émises ou reçues de l'étranger » est autorisée et le Premier ministre pourra « désigner les zones géographiques, les organisations ou les personnes objets de cette surveillance ».

Moins de contrôles

Ces interceptions à l'étranger seront nettement moins encadrées que celles effectuées en France. Le Premier ministre n'aura pas besoin de solliciter l'avis préalable de la nouvelle Commission nationale de contrôle des techniques de renseignement (CNCTR).

Sur proposition du Sénat, la commission mixte paritaire a retiré au Premier ministre la faculté de déléguer à un collaborateur la désignation des réseaux de communications électroniques internationales sur lesquels l'interception est autorisée.

Source :
http://www.latribune.fr/economie/france/la-surveillance-des-communications-internationales-validee-par-le-parlement-520191.html