Furtim, le malware qui détruit les solutions de sécurité.

	Furtim, le malware qui détruit les solutions de sécurité

Alors que de nouveaux malwares sont découverts quasiment chaque jour, voilà que l'un d'entre eux fait beaucoup parler. Il s'agit de Furtim, un #logiciel malveillant qui se caractérise par sa faculté à détruire les solutions de sécurité présentes sur le PC infecté.

Si l'on en croit nos confrères de Silicon, un nouveau malware a été découvert par les équipes d'EnSilo. Comme son nom l'indique, Furtim est capable de passer inaperçu sur les machines qu'il a réussi à infecter.

Probablement crée par des hackers d'Europe de l'Est, ce malware se compose d'un driver qui scanne le PC infecté, d'un module downloader, d'un gestionnaire d'alimentation, d'un voleur de mots de passe et d'un module de communication serveur.

Toutefois, avec une telle composition, impossible de comprendre comment fonctionne réellement ce malware. Pour l'heure, Furtim apparait seulement comme un logiciel malveillant très sophistiqué et capable d'analyser son environnement avant de s'exécuter. Pour cela, il va scanner la machine infectée pour détecter les solutions de sécurité et les outils de filtrage DNS.

Preuve que les pirates ont pensé à tout, Furtim bloque l'accès à de nombreuses sites spécialisés dans la sécurité informatique et à des forums d'aide à la désinfection et désactive les notifications Windows, le gestionnaire des tâches et diverses autres fonctionnalités.

Furtim, un éclaireur en vue de futures attaques

Selon les premières recherches menées par les équipes d'EnSilo, Furtim n'aurait probablement pas vocation à agir seul puisqu'il pourrait bien uniquement jouer un rôle d'éclaireur.

En effet, puisqu'il est capable de déjouer les outils de sécurité, il pourrait être utilisé pour introduire des menaces sur des PC sans que cela ne soit décelable… [Lire la suite]

Réagissez à cet article

Source : *Furtim, le malware qui détruit les solutions de*

sécurité

Auteur : Fabrice Dupuis

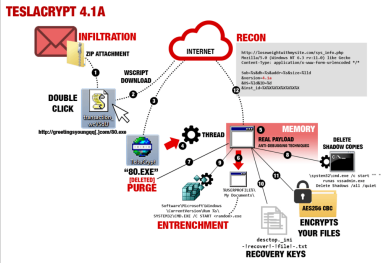
Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

---

Ces nouveaux exemplaires de TeslaCrypt sont diffusés massivement en tant que pièce jointe dans des spams qui imitent les avis de réception de colis des courriers express. D'après Endgame, la version 4.1A est apparue il y a environ une semaine ; outre les extensions déjà ciblées, elle attaque également les fichiers suivants .7z, .apk, .asset, .avi, .bak, .bik, .bsa, .csv, .d3dbsp, .das, .forge, .iwi, .lbf, .litemod, .litesql, .ltx, .m4a, .mp4, .rar, .re4, .sav, .slm, .sql,

La diffusion de TeslaCryp via le spam constitue également un changement : lors des campagnes récentes de TeslaCrypt, le ransomware avait été propagé via des kits d'exploitation et des redirections depuis des sites WordPress et Joomla. Dans ce cas, la victime doit ouvrir le fichier ZIP en pièce jointe afin d'activer un downloader JavaScript qui utilise Wscript (un composant de Windows) pour télécharger le fichier binaire de TeslaCrypt depuis le domaine greetingsyoungqq[.]com.
D'après notre interlocutrice, l'analyse de la version actualisée du ransomware fut complexe car elle lance de nombreux flux d'application et d'opérations de débogage afin de compliquer la tâche des outils de protection. Comme l'explique Amanda Rousseau, « il semblerait qu'il essaie de dissimuler les lignes dans la mémoire. Il est plus difficile pour l'Antivirus de les détecter s'il n'analyse pas la mémoire. »



Le recours à Wscript rend également la détection plus compliquée car le trafic ressemble à des communications légitimes de Windows. Selon Amanda Rousseau, il aura fallu quatre jours aux outils de détection pour identifier la technique et l'ajouter aux signatures. La durée de service des serveurs de commande sur lesquels se trouve TeslaCrypt a été limitée. A l'issue de celle-ci, les individus malintentionnés changent d'hébergement.
La version actualisée du ransomware utilise également un objet COM pour dissimuler les lignes de code extraites et élimine les identifiants de zone afin qu'ils ne soient pas découverts. De plus, pour éviter la surveillance, le malware arrête plusieurs processus Windows : Task Manager, Registry Editor, SysInternals Process Explorer, System Configuration et Command Shell. Pour garantir sa présence permanente, il se copie sur le disque et crée le paramètre correspondant dans la base de registres.
Vous trouverez une description technique détaillée de TeslaCrypt, y compris de ses méthodes de chiffrement et de ses techniques de lutte contre le débogage sur le blog d'Endgame.
Amanda Rousseau a indiqué dans ses commentaires que lors des essais, les nouveaux échantillons ont atteint les disques réseau connectés et ont tenté de chiffrer les fichiers qui s'y trouvaient. Ils tentent également de supprimer le cliché instantané du volume afin de priver la victime de toute chance de récupération.
Mais il y a malgré tout une bonne nouvelle : la version actualisée de TeslaCrypt chiffre les fichiers à l'aide d'une clé AES 256 et non pas à l'aide d'une clé RSA de 4 096 bits comme indiqué dans la demande de rançon et qui plus est, les informations indispensables au déchiffrement restent sur la machine infectée. « Nous avons trouvé l'algorithme de chiffrement : il fonctionne correctement, mais laisse le fichier de restauration dans le système » a confirmé Amanda Rousseau. « Si l'on part du programme de déchiffrement antérieur de TeslaCrypt et que son code est actualisé conformément aux [découvertes], il sera possible de réaliser le déchiffrement. » Il y a un an environ, Cisco a diffusé un utilitaire de ligne de commande capable de déchiffrer les fichiers touchés par TeslaCrypt.
Amanda Rousseau a également signalé que les auteurs de la version actualisée du ransomware avait emprunté beaucoup de code aux versions antérieures, notamment l'utilisation des objets COM et certaines techniques de débogage. « On dirait que les individus malintentionnés suivent les chercheurs à la trace en surveillant le code [de déchiffrement] publié sur Github en open source » explique le président d'Endgame en montrant les modifications introduites au cours du dernier mois depuis la version 4.0 jusqu'à la version 4 1A. – De petites modifications sont introduites dans chaque version et à la sortie de chaque nouveau décrypteur. Il prenne le meilleur de ce qui était utilisé il y a deux mois et l'appliquent aujourd'hui. »… [Lire la suite]

Source : *TeslaCrypt s'attaque à de nouveaux fichiers et améliore sa protection – Securelist*

Jigsaw, un rançongiciel avec compte à rebours destructeur

Jigsaw, un rançongiciel avec compte à rebours destructeur

Une heure… C'est le délai que laisse à sa victime le rançongiciel Jigsaw pour verser sa rançon. Passé ce délai, il commence à détruire les fichiers de l'ordinateur en accélérant son rythme toutes les heures. Des experts en sécurité ont trouvé le moyen de s'en débarrasser. Pour l'instant.

Apparemment, le versement d'une rançon en bitcoins ne suffit plus à certaines cyber-fripouilles, auteurs de ransomwares, pour fournir à leurs victimes la clé qui leur permettra de déchiffrer les fichiers de leur ordinateur. Il s'en trouve maintenant pour exiger des utilisateurs attaqués qu'ils s'en acquittent en moins d'une heure. Un nouveau programme dénommé Jigsaw chiffre les fichiers et commence à les détruire petit à petit jusqu'à ce que le malheureux utilisateur verse l'équivalent de 150 dollars en monnaie virtuelle Bitcoin. Après une heure, le ransomware détruit l'un après l'autre les fichiers, puis, après chaque cycle de 60 minutes, augmente le nombre de fichiers supprimés. Si aucun paiement n'est effectué dans un délai de 72 heures, tous les fichiers restants disparaissent. « Essayez de tenter quelque chose d'amusant et l'ordinateur appliquera certaines mesures de sécurité pour détruire vos fichiers », prévient un message du pirate accompagnée du masque du personnage de tueur Jigsaw, de la série de films d'horreur Saw.

Et ce n'est pas une menace en l'air.

Le malware est tout sauf inactif. Selon certains experts du forum de support technique BleepingComputer.com, ce rançongiciel détruit un millier de programmes à chaque fois que l'ordinateur redémarre ou que son processus est relancé. Dans un billet, Lawrence Abrams, fondateur du site, constate que c'est la première fois que l'on voit ce type de menaces propagées par le biais d'une infection par ransomware. La bonne nouvelle, pour l'instant, c'est que les experts ont élaboré une méthode pour déchiffrer les fichiers affectés par Jigsaw sans avoir à payer la rançon.

Inactiver Jigsaw puis déchiffrer les fichiers à l'aide d'un utilitaire

La première chose à faire, c'est d'ouvrir le gestionnaire de tâches de Windows et de terminer tous les processus appelés firefox.exe ou drpbx.exe qui ont été créés par le ransomware, indique Lawrence Abrams. Puis, il faut lancer l'utilitaire Windows MSConfig et supprimer l'entrée de démarrage pointant vers %UserProfile%AppDataRoamingFrfxfirefox.exe. Cela arrêtera le processus de destruction des fichiers et empêchera le malware de se relancer au redémarrage du système. Les utilisateurs pourront alors télécharger l'utilitaire Jigsaw Decrypter hébergé par BleepingComputer.com afin de déchiffrer leurs fichiers. Lorsque ce sera fait, il est hautement recommandé de télécharger un logiciel anti-malware à jour et de lancer un scan complet de son ordinateur pour désinstaller entièrement le ransomware.
En novembre, un précédent programme d'attaque dénommé Chimera menaçait de diffuser les fichiers des utilisateurs sur Internet. Toutefois, rien n'a prouvé qu'il était en mesure de le faire. Par comparaison, Jigsaw met ses menaces à exécution et révèle une évolution inquiétante sur ce terrain. Si les experts en sécurité ont trouvé un moyen de déchiffrer les fichiers cette fois, rien ne garantit qu'ils pourront le faire avec les prochaines versions. Les pourvoyeurs de ransomware sont généralement prompts à corriger leurs erreurs… [Lire la suite]

Pour info, en plus des technologies indispensables comme l'**anti-phishing** (pour **se protéger des e-mails de phishing**) et l'**anti-malware** (pour **se protéger des malwares cachés dans des e-mails ou des sites internet infectés**) qui protègent les clients contre les menaces d'Internet, ESET Smart Security 9 contient une toute nouvelle protection des transactions bancaires. Cette fonction met à disposition l'ouverture d'un navigateur sécurisé pour veiller à ce que toutes les transactions financières en ligne soient effectuées en toute sécurité. L'utilisateur peut également paramétrer lui-même tous les sites bancaires de paiement en ligne qu'il consulte le plus fréquemment.

Réagissez à cet article

Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable

	Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable par les anti-virus

Les attaques ransomwares ne baissent pas. Après avoir usurpé des avocats, des comptables, des PME, des mairies, FREE, voici le courriel piégé aux couleurs d'Orange. Ne cliquez surtout pas sur la pièce jointe.

Le courriel s'invite dans votre boites à mails avec comme objet : « ***Votre demande d'assistance*** » ; « ***Votre assistance Orange*** » ; « ***Votre assistance Orance Business***« . La missive pirate indique qu'une anomalie lors d'un prélèvement oblige le lecteur internaute à lire le fichier joint, un PDF piégé baptisé « ***Montant du mois*** » ou encore « ***Montant de la facture***« . Un piège qui, heureusement, est plutôt mal réalisé pour les internautes avertis. Il peut, cependant, piéger les plus curieux. La cible étant clairement les entreprises, une secrétaire, un comptable ou un responsable n'ayant pas vraiment le temps de lire autrement qu'en « Z » sera tenté de cliquer.

Au moment de l'analyse des fichiers, aucun antivirus n'avait la signature de la bestiole en mémoire. **A noter qu'un antivirus, face à ce genre d'attaque ne peut pas grand chose. Chaque mail et fichier joint portent en eux une signature (identification) unique et différente…** [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Attaques ransomwares aux couleurs d'Orange – ZATAZ*

Les établissements scolaires également victimes de ransomwares

Après les hôpitaux, les ransomwares s'attaquent de plus en plus aux établissements scolaires. Retour sur plusieurs cas aux Etats-Unis.

Les ransomwares sont devenus la plaie des responsables sécurité des entreprises ou des administrations. On peut se remémorer le témoignage du RSSI de l'AFP qui en a fait l'expérience. Le secteur hospitalier a été particulièrement touché avec différents exemples. Le plus symptomatique est le Hollywood Presbyterian Medical Center de Los Angeles qui a été obligé de payer 17 000 dollars en bitcoin pour retrouver l'usage de son réseau.

Certains payent la rançon

Après les hôpitaux, les ransomwares s'intéressent à une autre cible : les écoles. Plusieurs cas ont été recensés aux Etats-Unis. En février dernier, plusieurs écoles primaires du Horry County en Caroline du Sud ont été victimes d'un rançongiciel qui a bloqué 25 serveurs. Immédiatement après avoir été alertée par les enseignants, l'équipe IT a débranché les serveurs affectant ainsi les services en lignes des écoles. Après enquête, la porte d'entrée du malware était un vieux serveur non mis à jour. Toujours est-il que les responsables de l'école ont se sont vus réclamer 0,8 bitcoin par ordinateur soit un total de 20 bitcoins (environ 7600 euros). Malgré l'aide du FBI, le conseil d'administration du campus a décidé de payer la rançon demandée.

D'autres non

D'autres ont décidé de ne pas payer la rançon comme dans le cadre du Oxford School District dans le Mississipi. En février dernier aussi, ce réseau de 8 campus a été infecté par un rançongiciel réclamant environ 9000 dollars pour un retour à la normal. Le superintendant de l'établissement, Brian Harvey, a préféré ne pas payer et s'est concentré sur la récupération des données. Dans un entretien accordé à HottyDotty, il précise que « nous avons restauré à partir d'une sauvegarde ». Mais les dégâts étaient importants. « Je ne sais pas combien de données nous avons perdu. Je peux dire que nous avons perdu la plupart des serveurs Windows. La chose la plus importante a été de tout effacer et de tout réinstaller depuis la sauvegarde. » L'attaque a privé les établissements d'Internet pendant plus d'une journée. Les 4 premiers jours après l'attaque ont été focalisés sur la récupération du système des carnets de notes des élèves. D'autres applications ont souffert comme les reporting ou le recrutement des agents. Au final, deux semaines ont été nécessaires pour tout remettre à peu près d'aplomb : les sites web, la gestion de la cafeteria, ainsi que des plateformes pour l'éduction comme PowerSchool et Schoology.

Les parents d'élève s'inquiètent

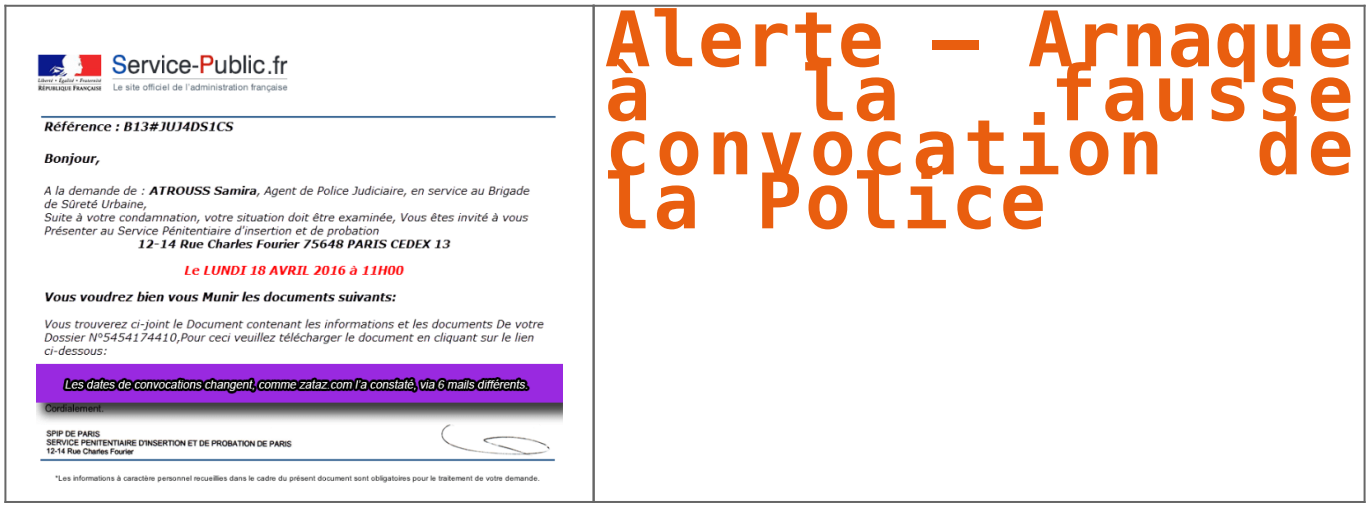
Autre affaire, le Texas School District qui gère une vingtaine d'établissements. Un ransomware a infecté le réseau, provoquant le blocage de plusieurs fichiers. La direction du district s'est voulue rassurante en expliquant que seule une petite partie des informations est concernée par le blocage. Ce dernier porte néanmoins sur un volume de 2,5 To de données. Les responsables ont choisi de ne pas payer la rançon demandée par les cybercriminels. « Nous avons réussi à effacer les fichiers chiffrés et à réinstaller données à partir d'une sauvegarde », précise un porte-parole du district. Un cas similaire à celui du Mississipi qui inquiète les parents d'élèves. « Ils [NDLR les établissements] détiennent des actes de naissance, des numéros de sécurité sociale ou des données médicales comme les vaccins », souligne une des parents d'élèves.

En France, aucun cas n'a été relevé ou publié sur des expositions à des ransomwares. Les écoles, universités et autres établissements scolaires font partie de cibles privilégiés par les cybercriminels. Obsolescence des parcs informatiques, système IT peu mis à jour, les pirates se ont trouvé un terrain de jeu grandeur nature pour tester et peaufiner leurs attaques. Les sommes demandées restent modestes, un signe selon les spécialistes pour reconnaître le degré de résistance des victimes à payer la rançon. En tout cas, les exemples américains doivent alerter les établissements bancaires européens et français sur les risques des ransomwares… [Lire la suite]

Réagissez à cet article

Source : *Les ransomwares prennent le chemin des écoliers*

Alerte – Arnaque à la fausse convocation de la Police



C'est derrière un document présumé aux couleurs de la Police Judiciaire que des centaines de Français sont piégés, depuis quelques jours, par un courriel malveillant aux couleurs du Service Pénitentiaire d'insertion et de probation de Paris.


Service-Public.fr
Le site officiel de l'administration française

Référence : B13#JUJ4DS1CS

Bonjour,

*A la demande de : **ATROUSS Samira**, Agent de Police Judiciaire, en service au Brigade de Sûreté Urbaine,*
Suite à votre condamnation, votre situation doit être examinée, Vous êtes invité à vous Présenter au Service Pénitentiaire d'insertion et de probation
12-14 Rue Charles Fourier 75648 PARIS CEDEX 13

Le LUNDI 18 AVRIL 2016 à 11H00

Vous voudrez bien vous Munir les documents suivants:

Vous trouverez ci-joint le Document contenant les informations et les documents De votre Dossier N°5454174410,Pour ceci veuillez télécharger le document en cliquant sur le lien ci-dessous:

Les dates de convocations changent, comme zataz.com l'a constaté, via 6 mails différents.

Cordialement.

SPIP DE PARIS
SERVICE PENITENTIAIRE D'INSERTION ET DE PROBATION DE PARIS
12-14 Rue Charles Fourier

*Les informations à caractère personnel recueillies dans le cadre du présent document sont obligatoires pour le traitement de votre demande.

Êtes-vous un dangereux criminel ? Normalement, non ! Avez-vous oublié de payer une année de contraventions ? Si tout va bien, non ! Avez-vous oublié votre séjour en prison ? Bref, le courriel communiqué ce week-end au nom d'un « ***Agent de police Judiciaire, en service en Brigade de Sureté Urbaine*** » vous n'avez rien à craindre de cette missive.
Depuis quelques jours, un étonnant mail aux couleurs de l'administration judiciaire Française s'invite dans les boites mails de nombreux, très nombreux lecteurs de ZATAZ.COM. La missive indique, en objet, être une « ***Convocation par Officier de Police Judiciaire (C.O.P.J)***« . Un titre suffisamment inquiétant, mais le pirate a rajouté en bonus « ***Obligation*** » histoire de renforce son social engineering.

Bonjour,

*A la demande de : **ATROUSS Samira**, Agent de Police Judiciaire, en service au Brigade de Sûreté Urbaine,*
Suite à votre condamnation, votre situation doit être examinée, Vous êtes invité à vous Présenter au Service Pénitentiaire d'insertion et de probation
12-14 Rue Charles Fourier 75648 PARIS CEDEX 13

Le LUNDI 18 AVRIL 2016 à 11H00

Vous voudrez bien vous Munir les documents suivants:

Vous trouverez ci-joint le Document contenant les informations et les documents De votre Dossier N°5454174410,Pour ceci veuillez télécharger le document en cliquant sur le lien ci-dessous:

Le courriel informe le lecteur qu' »***à la demande de*** [identité d'une personne], ***Agent de police Judiciaire, en service en Brigade de Sureté Urbaine.*** » vous êtes convoqués à la suite de votre condamnation et que « ***votre situation doit être examinée***« . La missive se termine par une date et une adresse postale. Une adresse officielle du *Service Pénitentiaire d'insertion et de probation de Paris (SPIP)*.
Le bot pirate [robot informatique], derrière cette diffusion malveillante, propose des rendez-vous, les lundis (11, 18 avril…). Comme vous l'aurez compris, une pièce jointe est proposée dans cette arnaque. Un PDF qui cache surtout une malveillance informatique. Attention, ne mettez pas en automatique, dans les options de votre logiciel de correspondance, la confirmation de lecture. L'attaque pirate demande, justement, que soit confirmé la lecture du courrier. Évitez de confirmer à l'escroc votre existence.
Bien entendu, ne cliquez surtout pas sur ce genre de fichier (ici, il ne s'agit pas d'un ransomware), surtout si vous n'êtes pas attirés par le chiffrement de vos données et l'obligation de payer une « rançon » pour récupérer vos documents privés, ou vous retrouver avec un logiciel espion dans votre machine. Ne rappelez pas, non plus, les numéros de téléphones qui peuvent être fournis.

Réagissez à cet article

Source : *ZATAZ Piège informatique à partir d'une fausse convocation de la Police – ZATAZ*

Et si la publicité cachait des Malwares ?

Et si la publicité cachait des Malwares ?

Alors que plusieurs sites d'information ont récemment mené une action pour dénoncer l'utilisation des bloqueurs publicitaires rappelant que la publicité était le principal revenu pour les sites web, il est également bon de savoir qu'elle tend à devenir un véritable vecteur d'attaque pour les pirates informatiques.

Des ransomwares cachés dans les publicités en ligne

Depuis plusieurs jours maintenant, de nombreux internautes se retrouvent piégés par des rançongiciels sans réellement comprendre comment ces derniers ont pu infecter leur ordinateur.

En effet, alors que beaucoup ont bien compris qu'ils devaient accorder la plus grande attention aux pièces jointes adressées par mail ainsi qu'aux fichiers qu'ils téléchargent sur la Toile, ils sont également nombreux à ne pas savoir que les publicités en ligne peuvent être à l'origine de l'infection.

Eh oui, de plus en plus de pirates informatiques parviennent à compromettre des réseaux d'annonces publicitaires en se faisant passer pour des personnes fiables. Ils adressent alors à la régie des bannières à faire afficher par des sites web, certaines intégrant un malware qui pourra infecter les ordinateurs des milliers d'internautes qui verront la publicité.

Cette forme de piratage est d'autant plus « sournoise » que le malware utilisé et baptisé Angler détecte l'existence de logiciel de sécurité et n'est réellement actif que si l'ordinateur ne dispose pas de sécurité. Autant qu'il est très complexe à détecter.

Les bloqueurs de publicité, finalement utiles pour sécuriser un ordinateur ?

Quelques heures seulement après que plusieurs sites d'informations français aient dénoncé le recours de plus en plus fréquent des internautes aux bloqueurs publicitaires, ces derniers viennent d'avoir un joli coup de publicité.

En effet, les bloqueurs de publicité peuvent être une solution pour sécuriser un ordinateur et tout du moins se protéger contre le malvertising.

Le développement de ce phénomène devrait en tout cas complexifier un peu plus encore la tâche des webmasters puisque l'image de la publicité, déjà jugée intrusive et gênante, devrait être davantage écornée en devenant une menace en matière de sécurité… [Lire la suite]

Réagissez à cet article

Source : *Quand la publicité devient un vecteur d'attaque*

Protégez-vous gratuitement du Virus Locky avant qu'il ne soit trop tard !

Protégez-vous gratuitement du Virus Locky avant qu'il ne soit trop tard !

Voici une solution rapide et pratique et efficace uniquement avec les versions actuelles de Locky pour s'en protéger.
Rien ne garantit qu'une version ultérieure de Locky ne contournera pas le souci.

Comme Locky essaye de créer la clé **HKCUSoftwareLocky** dans la base de registre (regedit), il suffit de la créer avant lui…

et de refuser tous les droits d'accès sur celle-ci:

Et voilà ! Ainsi, en se lançant sur votre système, Locky se crashera comme une station Mir dans le jardin de Paco. Les autres solutions proposées par Lexsi sont un poil plus complexes, mais vraiment intéressantes. Je vous invite à les lire, ne serait-ce que pour votre culture personnelle.
Merci Korben d'avoir relayé et à Olivier pour le partage.

Réagissez à cet article

Source : *Locky – La solution pour s'en protéger – Korben*

Petya, le nouveau ransomware qui chiffre l'ensemble du disque

Petya, le nouveau ransomware qui chiffre l'ensemble du disque

---

Le G DATA Security Labs a détecté les premiers fichiers ce jeudi 24 mars, en Allemagne, d'un nouveau type de ransomware nommé Petya.

A la différence des codes actuels, tels que Locky, CryptoWall ou TeslaCrypt, qui chiffrent certains fichiers du système, Petya chiffre l'ensemble des disques durs installés.

.

La campagne actuellement en cours vise les entreprises

Dans un email au service des ressources humaines, il y a une référence à un CV se trouvant dans Dropbox. Le fichier stocké dans le partage Dropbox est un exécutable. Dès son exécution, l'ordinateur plante avec un écran bleu et redémarre. Mais avant cela, le MBR est manipulé afin que Petya prenne le contrôle sur le processus d'amorçage. Le système démarre à nouveau avec un message MS-Dos qui annonce une vérification CheckDisk. A défaut d'être vérifié, le système est chiffré et plus aucun accès n'est possible.

Le message est clair : le disque est chiffré et la victime doit payer une rançon en se connectant à une adresse disponible sur le réseau anonyme TOR. Sur la page concernée, il est affirmé que le disque dur est chiffré avec un algorithme fort. Après 7 jours, le prix de la rançon est doublé. Il n'y a pour le moment aucune certitude sur le fait que les données soient irrécupérables.

Il est donc recommandé aux entreprises et particuliers de redoubler de vigilance quant aux emails reçus… [Lire la suite]

Réagissez à cet article

Source : *Petya : un nouveau ransomware qui chiffre l'ensemble du disque*

Alerte : Faille Java à corriger d'urgence. Oui encore…

Alerte : Faille Java à corriger d'urgence. Oui encore…

Oracle a publié un patch en urgence pour son logiciel Java. Celui-ci corrige une faille critique dans Java permettant d'exécuter du code à distance sur une machine vulnérable.Dans une alerte de sécurité, Oracle confirme que la faille (CVE-2016-0636) est sévère avec une note de 9.3 sur une échelle qui grimpe jusqu'à 10 (Common Vulnerability Scoring System)… [Lire la suite]

Réagissez à cet article

Source : *Oracle corrige en urgence Java. Oui encore… – ZDNet*