Les meilleurs anti-malware gratuits du moment

	Les meilleurs anti-malware gratuits du moment

Les menaces sont omnipresentes sur internet. La performance des antivirus est alors remise en question. En effet, dans certains cas, ils ne sont pas assez puissants pour bloquer ces malwares. Le recours aux meilleurs logiciels anti-malware s'avère alors indispensable.

L'IObit Malware Fighter : fiable et s'adapte bien

Ce logiciel est gratuit pour repérer et lutter contre les malwares. Utilitaire efficace contre les adwares, chevaux de Troie, vers, keyloggers, etc, il se complète parfaitement avec un antivirus. Il offre une protection instantanée, une analyse heuristique, et le choix de recourir à un scan manuel. Il n'existe qu'en version anglaise et s'adapte à tous systèmes d'exploitation Microsoft, allant de Windows XP à Windows 10.

Le Spybot – Search& Destroy : l'anti-malware recherche et destruction par excellence

Celui-ci, également gratuit a la même capacité que le précédent. Il a deux sortes d'interface, l'une pour les néophytes et l'autre pour les professionnels. Ce logiciel protège les navigateurs contre les menaces et permet une analyse manuelle du système. Disponible seulement en anglais, il s'adapte sur les mêmes systèmes d'exploitation quel' L'IObit Malware Fighter .

L'AdwCleaner : le suppléant fiable

L'AdwCleaner est un logiciel gratuit qui détecte et supprime les malwares. Il est efficace contre les adwares, toolbars, PUP/LPI ethijackers. C'est un utilitaire qui fonctionne uniquement par analyse manuelle mais il faut disposer de la dernière version. L'AdwCleaner est un excellent complément d'un antivirus ou un autre logiciel anti-malwares. Il est disponible en langue française et dispose d'une même adaptabilité de système que les deux premiers logiciels.

Emsisoft Anti-Malware : le bilingue

A la différence des trois premiers logiciels, celui-ci est payant. Sa validité est de 30 jours pour épargner votre système contre les menaces de types cheval de Troie, vers, spywares, etc. Il se complète à 100 % avec un antivirus classique. Il offre la possibilité de scanner manuellement le système et permet une surveillance instantanée, de même qu'une analyse heuristique. Il est disponible à la fois en anglais et en français. Cet anti-malware s'adapte sur tous systèmes de Windows XP à Windows 10.

Le Malwarebytes Anti-Malware : bref, mais efficace

Ce logiciel possède un arsenal complet pour tenir éloignés tous les malwares. Il est efficace contre les spamgiciels, les chevaux de Troie, les spywares, etc. Son scanner manuel et analyse heuristique constituent un appui optimal pour un antivirus. Il est également disponible en bilingue. Sa validité n'est que de 14 jours.

TDSS Killer : le tueur de malware

Le TDSS Killer est un anti-malware de Kaspersky. Sa fonction majeure est de détecter et supprimer les infections de type rootkit. Son analyse se fait uniquement en mode manuelle. Le savoir-faire de Kaspersky est une garantie chez le TDSS Killer pour déceler les malwares dissimulés. Son point faible est sa seule disponibilité en anglais.

En somme, même si les antivirus classiques sont conçus pour se parer aux menaces, il arrive que les malwares les contournent. C'est pourquoi il est mieux de se doter d'un logiciel anti-malware efficace. Il est même prudent d'en recourir à plusieurs.
Article original de Sekurigi

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

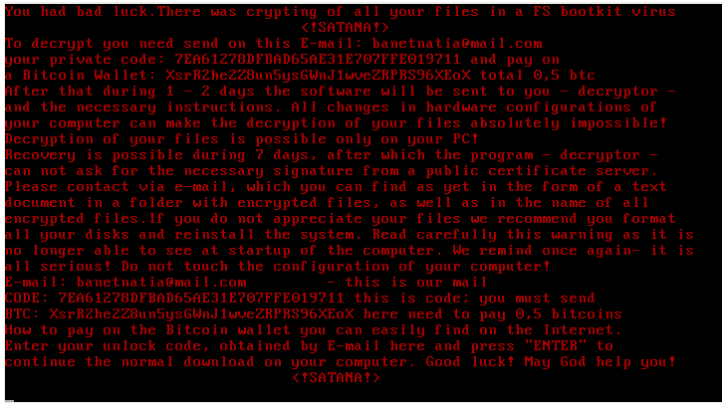
Original de l’article mis en page : Les meilleurs anti-malware gratuits du moment – @Sekurigi

---

Satana, un ransomware pire que Petya

Satana, un ransomware pire que Petya

Le nouveau rançomware Satana cumule chiffrement des fichiers et remplacement du secteur d'amorçage du disque.



Une nouvelle génération de ransomware est en train d'émerger. Satana, nom du nouveau malware, combine chiffrement des fichiers et écriture de code sur le secteur d'amorçage du disque, le MBR. Deux techniques inspirées de Petya et Mischa, note Malewarebytes qui constate la croissance du nouvel agent satanique ces dernières semaines.
« *Satana fonctionne en deux modes*, note la société de sécurité sur son blog. *Le premier se comporte comme Petya, un fichier exécutable (sous Windows, NDLR) [et] écrit au début du disque infecté un module de bas niveau, un bootloader avec un noyau personnalisé. Le deuxième mode se comporte comme un ransomware typique et chiffre les fichiers un par un (tout comme Mischa).* » Mais à la différence que les deux modes ne sont pas exploités alternativement mais bien appliqués ensemble, l'un après l'autre, pour s'attaquer à leurs victimes.

Payer ne garantit rien chez Satana

Malwarebytes ne le précise pas mais le mode de propagation de Satana reste probablement classique. A savoir par e-mail (et éventuellement d'un expéditeur en recherche de travail avec des liens vers les fichiers infectieux comme dans le cas de la première version de Petya). Une fois le MBR remplacé, le malware s'attaque au chiffrement des fichiers du disque (et des éventuels volumes reliés à l'ordinateur) et attend patiemment que le système soit redémarré. Quand c'est le cas, un message s'affiche sur l'écran expliquant la démarche à suivre pour récupérer l'accès à son PC, à savoir le paiement d'une rançon de 0,5 bitcoin (plus de 300 euros au cours du jour).
Si l'utilisateur parvient néanmoins à remplacer le MBR par un fichier d'amorçage sain (une manipulation manuelle qui est loin d'être à la portée de tout le monde), il se heurtera aux fichiers chiffrés sur le disque. Lesquels ont été renommés avec, en en-tête du nom, un e-mail aléatoirement choisi parmi ceux de l'équipe des développeurs de Satana, selon l'expert en sécurité (Gricakova@techmail.com, dans l'exemple présenté). Et les méthodes de chiffrement semblent suffisamment avancées pour rendre les fichiers piégés définitivement irrécupérables. D'autant que Malewarebytes pointe un bug pour le moins problématique pour la victime. De par le mécanisme de chiffrement/déchiffrement des fichiers, en cas de déconnexion au serveur de commandes et contrôle (C&C), la clé de décryptage (qui est la même que pour le cryptage) est perdue. Brisant tout espoir de la victime à pouvoir récupérer ses données (sauf à avoir fait préalablement des sauvegardes). « *Même les victimes qui paient peuvent ne pas récupérer leurs fichiers si elles (ou le C&C) sont hors ligne lorsque le chiffrement arrive* », prévient la société de sécurité.

Du code en cours de perfectionnement

Ce n'est pas la seule bizarrerie que remarque le chercheur Hasherezade, auteur du billet. Il constate également que, le ransomware affiche toute la procédure de son déploiement, y compris la progression du chiffrement des fichiers. « *Habituellement les auteurs de logiciels malveillants ne veulent pas laisser le code de débogage dans leur produit final* », écrit le chercheur. Lequel conclut que Satana est probablement encore en cours de développement et contient des failles. « *Le code d'attaque de bas niveau semble inachevée – mais les auteurs montrent un intérêt dans le développement du produit dans ce sens et nous pouvons nous attendre que la prochaine version sera améliorée.* » Une nouvelle génération de rançongiciel est bien en marche.
Article original de Christophe Lagane

Réagissez à cet article

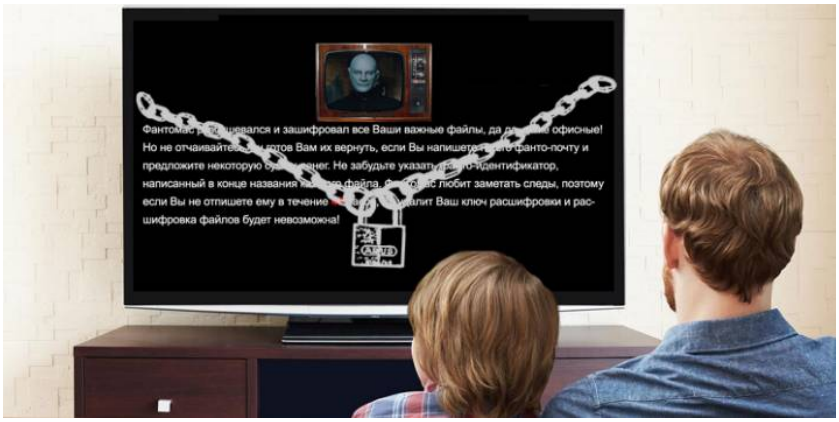
Original de l’article mis en page : Satana, un ransomware pire que Petya

---

Les Smart TV, nouvelle cible des ransomwares ?

Les Smart TV, nouvelle cible des ransomwares ?

Si les ransomwares sont chaque jour plus nombreux à venir « pourrir » le quotidien des particuliers comme des entreprises, voilà que ces derniers ne s'en prennent plus seulement aux ordinateurs et aux smartphones. En effet, Frantic Locker s'attaque également aux Smart TV.



Frantic Locker, le rançongiciel qui bloque les Smart TV

Alors que les ransomwares font de nombreuses victimes, le spécialiste de la sécurité informatique Trend Micro révèle que le rançongiciel Frantic Locker s'en prend désormais aux Smart TV.

Présent sur le marché depuis avril 2015, il n'a cessé d'évoluer et un grand nombre de variantes différentes ont développées lui permettant de s'ouvrir à de nouveaux horizons.

Ainsi, dernièrement, Frantic Locker, aussi connu sous le nom FLocker, est diffusé via des campagnes de spam par SMS ou bien par un site web préalablement piégé. Bien évidemment, l'objectif des cybercriminels est toujours le même : faire télécharger des applications malveillantes par l'intermédiaire de clics sur des liens frauduleux.

Mais là où le rançongiciel étonne, c'est qu'il ne bloque pas que les ordinateurs et les smartphones tournant sous Android. En effet, les cybercriminels ont fait des Smart TV leurs nouvelles victimes. Autrement dit, de nombreux téléspectateurs peuvent désormais vivre la mauvaise expérience de voir leur télévision laisser apparaître un message informant qu'une rançon de 200 dollars (en cartes-cadeaux iTunes) était nécessaire pour débloquer leur appareil.

Si tel n'est pas le cas, l'écran restera figé.

Un type d'attaque qui épargne encore certains pays

Depuis son lancement au printemps 2015, le rançongiciel Frantic Locker n'a cessé de se propager au point de cibler un nombre croissant de terminaux.

Concernant les Smart TV, toutes sont potentiellement vulnérables au ransomware FLocker mais selon Trend Micro, il s'autodétruirait en s'installant sur les Smart TV localisées dans plusieurs pays de l'Est de l'Europe comme la Russie, l'Ukraine, la Biélorussie, la Géorgie, la Bulgarie, l'Arménie, l'Azerbaïdjan, le Kazakhstan ou encore la Hongrie.

Article original de Jérôme DAJOUX

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 Smart TV, nouvelle cible des ransomwares ?