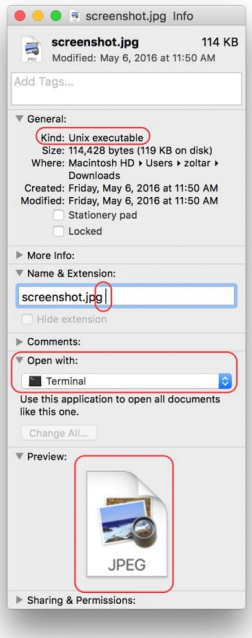
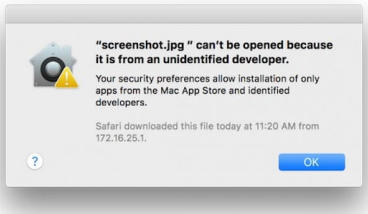
Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

	Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

Faut-il y voir la rançon du succès des Mac ? Toujours est-il qu'OSX/Keydnap est le deuxième malware de la semaine sur OS X, après Backdoor.MAC.Eleanor. Découvert par ESET, ce nouveau logiciel malveillant est pour le moment d'origine inconnue, mais on connait son mode de fonctionnement.
Téléchargé en pièce jointe ou depuis un site interlope, Keydnap se présente sous une forme bien innocente : une archive ZIP qui contient ce qui ressemble à une image (.jpg) ou un document texte (.txt). Sauf que le suffixe du document contient une espace, ce qui lance un Terminal, et non Aperçu ou TextEdit comme on peut s'y attendre.



En cliquant sur le document, un mécanisme se met en place qui fait prendre des vessies pour des lanternes. L'application attendue s'ouvre et présente le document qui va bien… sauf que dans l'intervalle, le fichier aura ouvert un Terminal (l'icône du Terminal apparait brièvement dans le dock avant d'être remplacée par celle de l'application standard). Une fois l'exécutable lancé, Gatekeeper prévient que le fichier provient d'un développeur non enregistré et qu'il ne peut pas ouvrir le document :



Ce message d'alerte intervient si et seulement si Gatekeeper n'autorise que les applications provenant du Mac App Store et des développeurs identifiés. Sur OS X El Capitan, on peut choisir de lancer une app téléchargée depuis « n'importe où », mais plus sous macOS Sierra.
Une fois lancé, le malware crée une porte dérobée et remplace le contenu de l'exécutable par un leurre téléchargé sur internet ou intégré dans le code du logiciel malveillant – il peut s'agir du document effectivement attendu, comme une image :

La porte dérobée créée par Keydnap est persistante, même si on multiplie les redémarrages du Mac. Il demandera aussi le mot de passe de la session, déguisé sous la forme d'icloudsyncd. Une fois en possession de cette information, il transforme le Mac en open-bar : l'objectif du malware est de récupérer les informations du Trousseau d'accès, qui contient les identifiants et mots de passe de vos logiciels et services en ligne.
À la lumière de cette nouvelle affaire, on comprend mieux pourquoi Apple exige maintenant des logiciels signés sur macOS Sierra.
Merci à Mickaël Bazoge pour son enquête et son article

Réagissez à cet article

Original de l’article mis en page : Nouveau malware sur OS X : OSX/Keydnap détrousse le Trousseau d’accès | MacGeneration

---

Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)

Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)

Le malware Keydnap exfiltre les mots de passe et les clés stockés dans le gestionnaire de mot de passe « KeyChain » de Mac OS X et crée une porte dérobée permanente.

Les chercheurs ESET se sont penchés sur OSX/Keydnap, un cheval de Troie qui vole les mots de passe et les clés stockées dans le gestionnaire de mot de passe « keychain », en créant une porte dérobée permanente.
Bien que la façon dont les victimes se trouvent exposées à cette menace ne soit pas très clair, nous pensons qu'elle pourrait se propager via des pièces jointes contenues dans les spams, des téléchargements à partir de sites non sécurisés ou d'autres vecteurs.
Le code malveillant Keydnap est distribué sous forme de fichier .zip avec le fichier exécutable imitant l'icône Finder habituellement appliqué aux fichiers texte ou JPEG. Cela augmente la probabilité que le destinataire double-clique sur le fichier. Une fois démarré, une fenêtre de terminal s'ouvre et la charge utile malveillante est exécutée.
À ce stade, la porte dérobée est configurée et le malware débute la collecte et l'exfiltration des informations de base figurant sur la machine Mac attaqué. À la demande de son serveur C&C, Keydnap peut obtenir les privilèges administratifs en ouvrant la fenêtre dédiée d'OS X.
Si la victime saisit ses identifiants, la porte dérobée fonctionne alors comme un root, avec le contenu exfiltré du porte-clés de la victime.
Bien qu'il existe des mécanismes de sécurité multiples en place au sein d'OS X pour réduire l'impact des logiciels malveillants, il est possible de tromper l'utilisateur.
Tous les utilisateurs d'OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées », rapporte Marc-Etienne M. Léveillé, Malware Researcher chez ESET.
Des détails supplémentaires sur Keydnap peuvent être trouvés dans notre article technique disponible sur WeLiveSecurity.com.

Réagissez à cet article
Source : ESET

Un nouveau malware s’attaque aux Mac

Un nouveau malware s’attaque aux Mac

BitDefender a découvert Backdoor.MAC.Eleanor, un malware qui permet aux attaquants de prendre le contrôle des machines Apple sous Mac OS et de les piloter à travers le réseau d'anonymisation Tor.

Selon l'éditeur de sécurité, Eleanor est distribué sous forme d'un logiciel que l'on peut télécharger depuis des sites web légitimes dédiés à l'univers Apple. Une fois installé, l'agent malveillant affiche une interface de conversion de fichiers par drag&drop, service supposément légitime qui, en toute opacité, installe des composants sur le système. A partir de là, l'attaquant peut prendre le contrôle complet de la machine, y compris capturer des images depuis la webcam du portable. Comme Eleanor n'est pas certifiée Apple, les utilisateurs sous El Capitan, la dernière version d'OS X verront s'afficher un message d'alerte de sécurité lors de l'installation de l'application infectieuse. Une barrière qui permettra d'éviter le pire.
Article original de Silicon

Réagissez à cet article

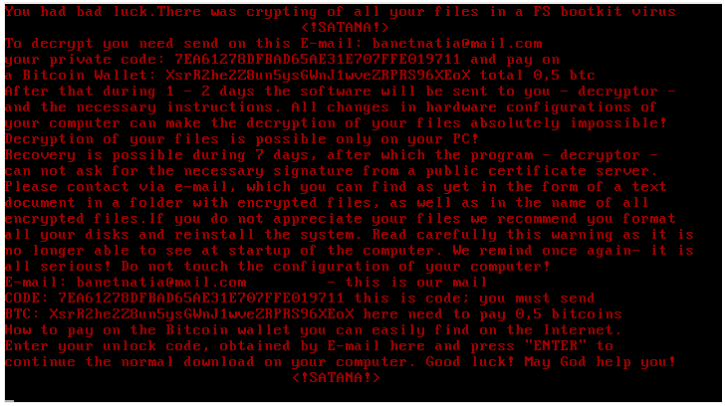
Original de l’article mis en page : Télégrammes :Darktrace; Google; e-Privacy; backdoor Mac

---

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

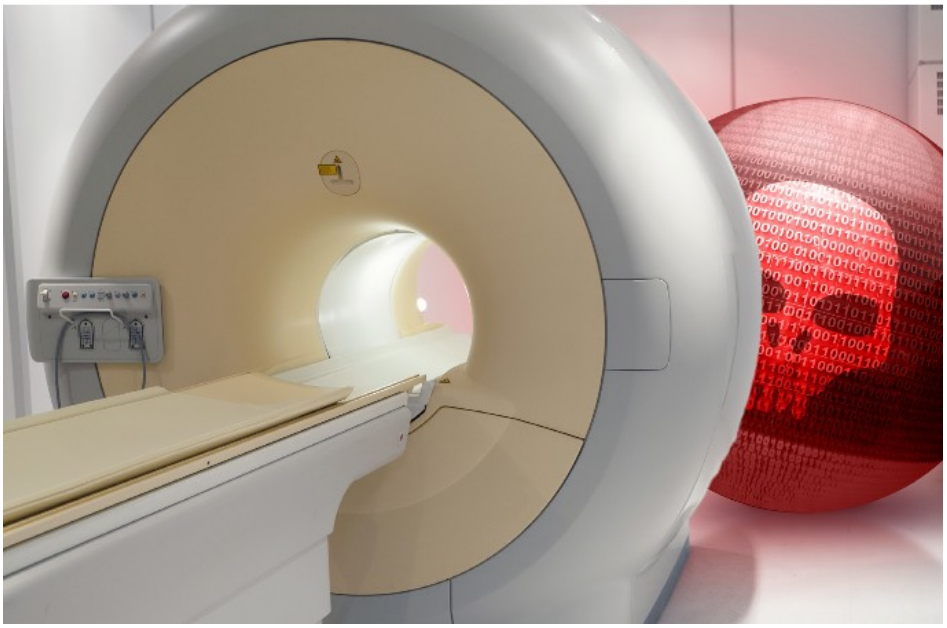
Ce n'est pas la seule bizarrerie que remarque le chercheur Hasherezade, auteur du billet. Il constate également que, le ransomware affiche toute la procédure de son déploiement, y compris la progression du chiffrement des fichiers. « *Habituellement les auteurs de logiciels malveillants ne veulent pas 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

---

Risques d’infection dans le médical des Objets Connectés



Risques d’infection dans le médical des Objets Connectés

La faible sécurité des équipements de santé connectés entraîne la résurgence des vieux virus comme Conficker.

Un des problèmes de la montée en puissance de l'Internet des objets ? La sécurité.
Spécialistes, constructeurs, éditeurs répètent à longueur de conférences qu'il faut absolument que l'IoT soit « secure by design ». Entendez par là que les capteurs, le protocole de communication, la plateforme de traitement de l'information, l'architecture soient sécurisés dès leur conception.
Oui mais voilà, c'est sans compter sur le fameux héritage technique. Le monde de la santé rentre typiquement dans ce cadre et tout particulièrement les outils médicaux connectés. On pense ici aux IRM, scanners, radios, ou pompes à insuline. Ces équipements sont de plus en plus ciblés par les cyberattaquants, car ils sont moins bien protégés que des PC ou des serveurs.
Conséquence de cette faible sécurité, les vieux virus se rappellent aux bons souvenirs des administrateurs et des RSSI. Un rapport de la société de sécurité TrapX Labs, disséquant une attaque baptisée MEDJACK.2, montre que les attaques utilisent des malwares comme networm32.kido.ib ou le ver Conficker en complément de menaces plus sophistiquées. Moshe Ben Simon, co-fondateur de TrapX, résume bien ce paradoxe : « *un loup intelligent déguisé avec des vieux habits de mouton* ».

Mise en place de backdoors

Premier constat, les équipements médicaux connectés à Internet fonctionnent avec des versions de Windows non corrigées allant de XP (qui n'est plus supporté par Microsoft) aux versions 7 et 8. Des cibles de choix pour les anciens virus. « *Ces vieux virus sont utilisés avec des malwares (en l'occurrence MEDJACK.2) plus élaborés pour installer des backdoors dans l'établissement de santé et ensuite mener une campagne par exfiltration de données, voire se transformer en #ransomware* », souligne le rapport.
Les échantillons de Conficker que les experts de la société de sécurité ont analysé, montrent que le ver a été modifié pour avoir une meilleure capacité à se déplacer dans un réseau. Pire, son évolution fait qu'il est devenu indétectable pour les équipements médicaux. Dans son enquête auprès de 3 hôpitaux, TrapX relève qu'aucune alerte n'a été remontée par les établissements sur la présence de Conficker. A son apogée en 2009, Conficker avait infecté entre 9 et 15 millions d'ordinateurs. Il avait, comme capacité, de casser les mots de passe, d'enrôler les PC dans des botnets, etc. La version actuelle est diffusée par phishing envoyé aux personnels de l'hôpital.

Les données patients : la ruée vers l'or

L'objectif de ces attaques : obtenir les dossiers patients. Des informations très demandées sur le Dark Web et affichant une forte valeur marchande au marché noir. « *Les cybercriminels peuvent voler l'identité d'un patient pour se faire rembourser par les assurances des traitements coûteux et, en plus, revendre ces traitements au marché noir* ». TrapX estime qu'un dossier médical se monnaye entre 10 et 20 dollars sur le marché, contre 5 dollars pour une information financière. En début de semaine, on apprenait le vol de 9,3 millions de données de santé de citoyens américains. Le calcul est vite fait…
Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Sécurité : Conficker revient infecter l’IoT médical

---

Nouvelle forme d’attaque informatique, les crypto-vers

Nouvelle forme d’#attaque informatique, les crypto-vers

Les cybercriminels ont trouvé une nouvelle manière de se faire de l'argent. Cela faisait longtemps qu'ils tentaient de prendre en otage des disques durs, mais les gens sont devenus plus vigilants et n'ouvrent plus n'importe quelle pièce jointe à un mail. Voilà pourquoi les cybercriminels se sont vu contraints d'inventer une nouvelle façon d'installer leur rançongiciel (#ransomware). Leur solution: le ver.

Le spécialiste de la sécurité Kaspersky lance donc une mise en garde. Le 'crypto-ver' est « une forme mixte dangereuse de maliciel (malware) et de rançongiciel qui se répand d'elle-même ». Elle peut se propager d'ordinateur à ordinateur, sans spam (pourriel) ou autre infection. Le malware se duplique simplement dans les appareils interconnectés.
Le premier ver, baptisé SamSam, s'est manifesté en avril. Et au cours des dernières semaines, des experts en sécurité ont découvert le ver ZCryptor. Ce dernier se présente sous la forme d'une simple mise à jour d'un programme largement utilisé tel Flash. Une fois en place, le ver commence à se propager, puis il crypte des dizaines d'extensions. Les victimes voient ensuite apparaître leur écran habituel, qui les informe que leurs fichiers ont été pris en otage et qu'ils doivent verser une rançon pour pouvoir y accéder de nouveau.
Les spécialistes des la sécurité n'ont pas encore trouvé une parade contre ZCryptor. Voilà pourquoi Kaspersky prodigue le conseil suivant: soyez sur vos gardes, veillez à disposer d'une bonne protection et effectuez régulièrement des sauvegardes (backups).

Réagissez à cet article

Original de l'article mis en page : Nouveau: le ver ravisseur – ICT actualité – Data News.be

Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

	Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

Particulièrement actif en Asie, ce malware est notamment parvenu à se frayer un chemin jusqu'au Google Play Store.

Android a pourtant initié depuis plusieurs années un grand nettoyage de son Google Play Store et a revu les règles et procédures d'accès des applications, mais certains malwares parviennent encore à contourner les garde-fous mis en place. Trend Micro alerte ainsi sur une famille de malware baptisés Godless, qui sont distribués entre autres via le Google Play Store et des applications malveillantes.

Trend Micro explique que Godless dispose de plusieurs exploits lui permettant d'affecter les appareils Android, ce qui le rend potentiellement dangereux pour tous les téléphones disposant d'une version antérieure à Android 5.1.
Le malware est généralement distribué via des applications proposées sur le Google Play store. La présence de celui-ci n'est pas détectée, car lorsque l'application est uploadée vers le playstore, elle ne contient aucun code malveillant à proprement parler. Mais une fois l'application installée, celle-ci va se mettre à jour et télécharger alors le « payload » contenant l'exploit de la vulnérabilité choisie par les cybercriminels.
Le malware tentera d'exploiter celle-ci pour acquérir les droits root sur la machine : il s'en sert par la suite pour installer des applications ou pour diffuser des publicités.
La France est relativement épargnée par ce malware, qui est principalement actif en Asie, notamment en Inde et en Indonésie. Mais Trend Micro estime que plus de 850.000 terminaux Android ont été infectés par ce malware à travers le monde. Outre les applications qui parviennent à le distribuer sur le Google Play Store officiel, celui-ci est évidemment diffusé sur les magasins d'application tiers.
Article original de Louis Adam

Réagissez à cet article

Original de l'article mis en page : Godless : un nouveau malware qui infecte plus de 850.000 terminaux Android – ZDNet

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Le ransomware RAA se propage à grande vitesse en Russie par le biais de campagnes de spams. Il prend la forme d'une pièce jointe en Javascript.

RAA, un ransomware entièrement écrit en Javascript

Si la plupart des logiciels malveillants qui ciblent des machines Windows est écrite en C++, voilà que RAA surprend puisque lui est intégralement écrit en Javascript, un langage destiné principalement à être interprété par les navigateurs web.

Pour les cybercriminels, le choix de ce langage n'est pas dû au hasard étant donné qu'ils tentent d'infecter les machines à distance via la diffusion de spams. Toutefois, tout utilisateur doit normalement agir avec méfiance avec les pièces jointes, d'autant plus si celles-ci sont dans un format Javascript. En effet, ce format doit inciter les utilisateurs à mettre le mail dans leur corbeille et surtout à ne pas ouvrir la pièce jointe.

Si tel est le cas, RAA peut faire des ravages puisqu'il est conçu pour chiffrer les documents disposant des extensions .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar et .csv comme le révèlent nos confrères du Monde Informatique.

Autant dire donc que le téléchargement de la pièce jointe n'est pas sans conséquences.

Pas de vaccin disponible pour déchiffrer les contenus

S'il existe parfois des vaccins contre les ransomwares, RAA n'a pas encore le sien si bien qu'une fois vos fichiers chiffrés, vous n'aurez aucune autre alternative que payer la rançon si vous voulez débloquer de nouveau l'accès à vos documents.

Pour l'heure, ce rançongiciel se propage principalement en Russie puisqu'il semble que c'est depuis ce pays qu'opèrent les cybercriminels. Toutefois, il y a fort à parier que la diffusion de RAA va s'étendre dans les prochains mois et qu'une version « internationale » du rançongiciel sera développée par ces spécialistes du genre.

Article original de Fabrice Dupuis

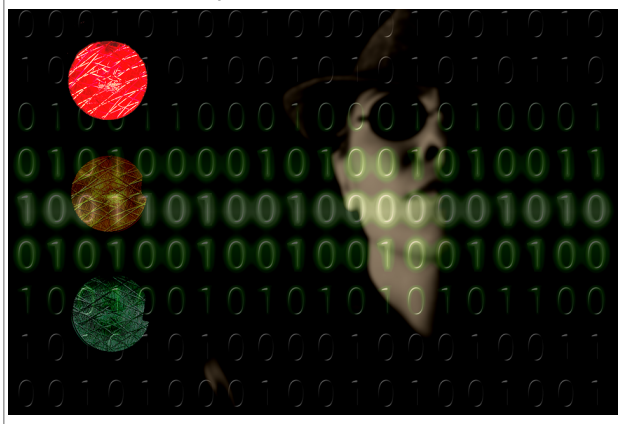
Réagissez à cet article

Original de l’article mis en page : RAA : un nouveau ransomware diffusé par spams

Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

Irongate, un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet

D'après les informations de FireEye, le malware Irongate, qui vise les systèmes de contrôle des procédés industriels ressemble en certains points au terrible ver Stuxnet. Cette découverte est une nouvelle source d'inquiétude pour les membres de la communauté de la sécurité de l'information et elle vient confirmer la nécessité du perfectionnement des systèmes de détection des malwares qui attaquent les infrastructures critiques.



Les chercheurs ont également signalé qu'Irongate ne constituait pas une menace sérieuse pour l'instant car il fonctionne uniquement dans des environnements simulés. Ceci étant dit, FireEye indique que ce malware est passé inaperçu pendant des années alors qu'il figurait pendant tout ce temps dans la base VirusTotal. « La compétence du secteur dans le domaine de l'identification et de la détection des menaces s'améliore, mais elle n'a pas encore atteint un niveau satisfaisant comme le montrent ces exemples » constate Rob Caldwell, directeur du groupe d'analyse FireEye Labs Advanced Reverse Engineering (FLARE). Il poursuit en expliquant qu'il faut absolument mieux comprendre ce que représentent les menaces pour les systèmes de contrôle des procédés industriels, comment les détecter et comment améliorer la protection contre celles-ci. »

D'après FireEye, le malware qu'elle a identifié se distingue par sa capacité à mener une attaque de type homme du milieu contre l'entrée et la sortie des procédés et à attaquer l'application qui exécute des opérations sur les processus dans les environnements simulés. Un système compromis par Irongate permet aux attaquants de substituer les contrôles industriels à l'insu de l'opérateur du système. Des techniques semblables ont déjà été utilisées par le passé pour mettre hors service des infrastructures critiques diverses, depuis des réseaux de distribution d'électricité jusqu'aux contrôleurs logiques de centrifugeuses dans le secteur nucléaire.

Les chercheurs ont découvert une exemplaire d'Irongate vers la fin de l'année 2015 sur VirusTotal alors qu'ils recherchaient des droppers compilés à l'aide PyInstaller. L'échantillon trouvé ressemblait très fort aux malwares qui visaient les systèmes d'automatisation industrielle et autres systèmes de contrôle des procédés industriels. Il se fait que ce modèle avait été chargé pour analyse en 2012, mais aucun logiciel antivirus ne l'avait reconnu.

L'analyse a démontré que le malware utilise une technique de l'homme du milieu qui permet de réaliser des attaques contre une application personnalisée de l'utilisateur qui fonctionne dans un milieu de modélisation des contrôleurs logiques programmables Step 7 de Simens Les experts ont découvert également une bibliothèque dynamique capable de masquer le comportement malveillant du code exécutable. Cette DLL est capable d'enregistrer cinq secondes du trafic « normal » provenant du contrôleur logique programmable modélisé ; l'attaquant peut reproduire ce fragment afin de masquer le transfert des données codées en dur vers l'équipement d'imitation.

Les chercheurs ont été surpris de voir que pour rendre l'analyse plus difficile, ce malware spécialisé se comporte comme un malware traditionnel : lorsqu'il est exécuté sur une machine virtuelle ou dans un bac à sable (Cuckoo), il passe en mode de veille et refuse de s'exécuter.

« Bien que Stuxnet soit plus complexe sur le plan technique, Irongate possède quelques traits similaires » a déclaré Sean McBride, analyste antivirus principal chez FireEye. Pour être plus précis, il a noté que ces deux malwares sont destinés à attaquer un système particulier de gestion et ils utilisent des outils de protection contre la détection : Stuxnet est capable de détecter la présence d'un logiciel antivirus et Irongate, celle d'une machine virtuelle. Toutefois, à la différence de ses rares confrères commeBlackEnergy, Havex, et même Stuxnet, Irongate n'est pas très répandu dans la pratique : il fonctionne seulement dans les environnements simulés orientés sur les systèmes Siemens.

Qui est donc à l'origine de ce malware et quel est son objectif ? FireEye avance trois hypothèses en réponse. Tout d'abord, les experts supposent que son auteur peut avoir nourri l'espoir que quelqu'un transfèrerait ce code depuis l'environnement simulé et commencerait à l'utiliser dans son environnement de travail. Il est également possible qu'Irongate soit un modèle expérimental et que son créateur a décidé de vérifier à quel point il était facile de le détecter via les services VirusTotal. La troisième hypothèse est celle considérée comme la plus probable par FireEye : un expert en sécurité de l'information a oublié qu'il avait soumis ce code à une vérification il y a un certain temps.

« Il convient de fournir de plus gros efforts dans le secteur pour détecter les menaces qui visent les systèmes de contrôle des procédés industriels » conclut Dan Scali, conseiller principal de la division conseil de FireEye sur les questions de sécurité des systèmes d'automatisation industrielle. « Globalement, il n'y a pas eu de gros progrès dans la résolution des problèmes posés par Irongate depuis Stuxnet. Dans la mesure où l'accès à de tels attaques se démocratise, le thème de l'adéquation des mesures de protection est source de préoccupation.

Réagissez à cet article

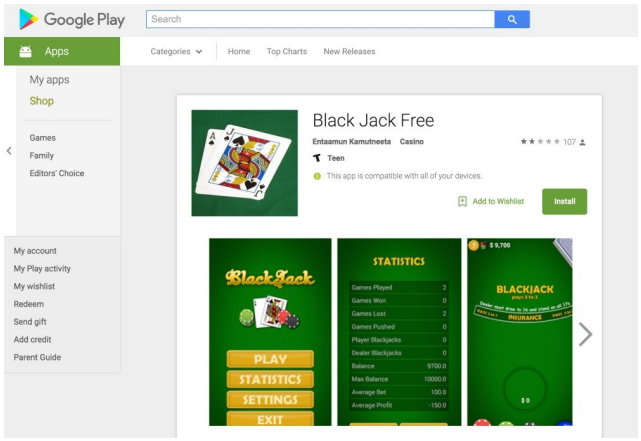
Original de l’article mis en page : Un malware qui vise les systèmes d’automatisation industrielle s’inspire de Stuxnet – Securelist

---

Alerte : Un Trojan détecté sur Google Play

Alerte : Un Trojan détecté sur Google Play

Lookout, spécialiste dans la sécurité mobile a détecté « Black Jack Free », un jeu gratuit sur Google Play qui appartient à la famille du Trojan Acecard.



S'il est de bon augure de se méfier des jeux d'argents, il faut les craindre d'autant plus lorsqu'ils sont sur internet. L'application Black Jack Free qui était en fait un Trojan a été téléchargée plus de 5000 fois avant d'être retirée du Google Play Store quatre jours plus tard. A première vue, il n'y avait rien à craindre de ce jeu de cartes qui permettait de jouer gratuitement tout en utilisant de l'argent fictif. Sauf que, dans l'arrière boutique l'application dérobait des données, mais aussi de l'argent sur les comptes en banque des utilisateurs. «Black Jack Free n'était pas directement le problème. Mais il installait une deuxième application, Play Store Update qui repérait les applications actives sur internet et imitait les pages d'accueil» explique Arnaud Simon, responsable technique Europe du sud chez Lookout.
Par ce stratagème, l'application superposait des fenêtres sur les applications bancaires, ou sur les réseaux sociaux comme Facebook ou Skype par exemple. Ensuite, les utilisateurs entraient leurs codes et identifiants sans se douter que des pirates les récupéraient. Play Store Update pouvait aussi intercepter des SMS, les envoyer vers un serveur malicieux, transférer des appels, verrouiller l'écran et effacer les données d'un terminal.

Un risque plus ou moins écarté

Il est donc fortement conseillé aux utilisateurs ayant téléchargé Black Jack Free de supprimer l'application de leurs terminaux Android et de se débarrasser de Play Store Update également. Ensuite, pour éviter les mauvaises surprises, Lookout invite les personnes concernées à modifier leurs codes d'accès.
A noter que « l'application était disponible sur Google Play car les pirates disposaient d'un accès potentiel à de nombreux terminaux. Mais les hackers ne se sont pas contentés de diffuser Black Jack Free sur cette seule et unique plateforme, elle est disponible ailleurs sur le web», ajoute Arnaud Simon. Comprendre que le Trojan court toujours et que la méfiance reste de mise.
Article original de Victor Mayet

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

Source : *Un Trojan détecté sur Google Play*