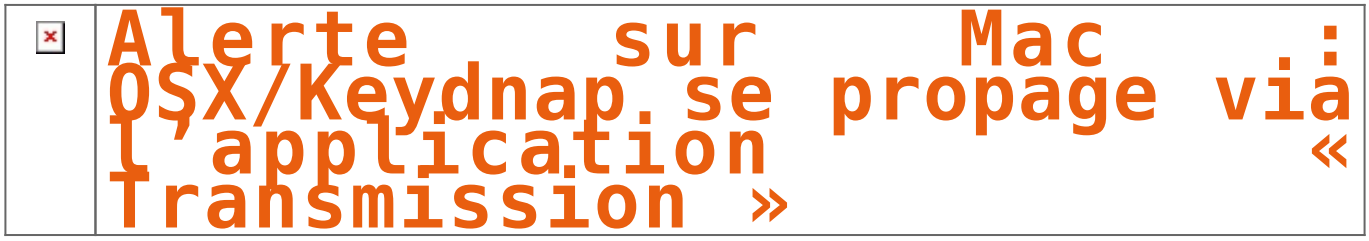
Alerte sur Mac : OSX/Keydnap se propage via l'application « Transmission »



Le mois dernier, les chercheurs d'ESET ont découvert un malware sur Mac OS X nommé OSX/Keydnap, qui exfiltre les mots de passe et clés stockés dans le gestionnaire de mots de passe « KeyChain » ; et qui crée une porte dérobée permanente.
Au moment de la découverte, notre Malware Researcher Marc-Etienne Léveillé expliquait que « 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 ».

Les équipes ESET viennent de découvrir que le malware OSX/Keydnap se distribue via une version compilée de l'application BitTorrent.

Une réponse instantanée de l'équipe de transmission

Suite à l'alerte donnée par ESET, l'équipe de transmission a supprimé le fichier malveillant de leur serveur Web et a lancé une enquête pour identifier le problème. Au moment de la diffusion de la première alerte, il était impossible de préciser depuis combien de temps le fichier malveillant a été mis à disposition en téléchargement.

Selon les informations de la signature, l'application a été signée le 28 août 2016, mais ne se serait répandue que le lendemain. Ainsi, les équipes ESET conseillent aux personnes qui ont téléchargé la transmission V2.92 entre le 28 et le 29 août 2016 de vérifier si leur système est compromis en testant la présence de l'un des fichiers ou répertoires suivant :

- /Applications/Transmission.app/Contents/Resources/-License.rtf
- /Volumes/Transmission/Transmission.app/Contents/-Resources/License.rtf
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/icloudsyncd
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/process.id
- $HOME/Library/LaunchAgents/com.apple.iCloud.sync.daemon.-plist
- /Library/Application Support/com.apple.iCloud.sync.-daemon/
- $HOME/Library/LaunchAgents/com.geticloud.icloud.photo.-plist

Si l'un d'eux est présent, cela signifie que l'application malveillante de « transmission » a été exécutée et que le malware Keydnap est probablement en cours d'exécution. Notez également que l'image malicieuse du disque se nomme Transmission 2.92.dmg tandis que l'original se nomme Transmission–2.92.dmg (trait d'union).

Article original de ESET

Pour protéger votre Mac, Denis JACOPINI recommande l'application suivante :

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

Ransomware : Locky se fait passer pour un fichier système Windows

	Alerte : le Ransomware Locky se fait passer pour un fichier système Windows

Une variante du ransomware Locky se fait passer pour un fichier DLL dans l'espoir de tromper les filtres de sécurité.

Toujours plus vicieux. Le ou les groupes de cybercriminels qui se cachent derrière le Locky ne cessent de faire évoluer l'un des plus populaires ransomware de la Toile. Objectif : déjouer les dernières mises à jour des solutions de protection et attraper toujours plus de victimes dans les filets. Victimes qui, rappelons-le, n'auront d'autre choix que de payer une rançon (généralement en bitcoin) pour récupérer leurs données si elles n'ont pas pris soin de faire des sauvegardes.
Aux dernières nouvelles, la dernière variante de Locky se distingue en se cachant derrière un fichier .DLL et non plus derrière un .EXE comme précédemment. Les DLL (Dynamic Link Library) sont des bibliothèques logicielles exploitées par Windows pour exécuter une application. « Ce que nous trouvons le plus intéressant dans cette dernière vague Locky est qu'au lieu de télécharger un binaire EXE, ce composant ransomware arrive maintenant en tant que binaire DLL, soulignent les chercheurs en sécurité de Cyren. Qui plus est, le fichier DLL ainsi téléchargé est personnalisé pour empêcher les scanners de virus de le détecter facilement. »

Attention au zip
Si le DLL parvient à passer les filtres de sécurité, son exécution reste identique à celle constatée jusqu'à présent, à savoir que le rançongiciel part à la recherche de fichiers à chiffrer avant de rediriger ses victimes vers une page affichant la facture (et la méthodologie du mode de paiement). Petite variante, le mécanisme d'attaque attribue l'extension .zepto aux fichiers devenus illisibles. « Comparé aux précédentes, cette nouvelle variante ajoute un autre niveau d'obscurcissement qui déchiffre et exécute le réel script chargé du téléchargement de Locky », constatent toutefois les chercheurs.
Le mode de distribution et d'infection de JS/Locky.AT!Eldorado, nom de cette nouvelle variante de Locky, n'a, lui, pas changé : il tente toujours de se propager par l'envoi d'un e-mail trompeur invitant à cliquer sur une pièce jointe au format ZIP renfermant le code Javascript qui va déclencher la décompression des fichiers et l'exécution des commandes de téléchargement de l'agent infectieux proprement dit. Etre doublement attentif lors de la réception de ce genre d'e-mail (et éviter de cliquer sur des fichiers ZIP sans être absolument certain de leur origine) reste le meilleur moyen d'éviter de l'infection.

Article original de Christophe Lagane

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 : Ransomware : Locky se fait passer pour un fichier système Windows

---

Alerte : un malware Android commandé par… Twitter

Alerte : un malware Android commandé par… Twitter

Les concepteurs du malware Android Twittor se servent du réseau social pour envoyer des instructions à la souche infectieuse. Une technique plus furtive que les classiques serveurs de commande et contrôle.

L'éditeur d'antivirus Eset affirme avoir découvert le premier malware commandé… par des tweets. Selon la société slovaque, Android/Twittor est une application Android malveillante, probablement diffusée par SMS ou via des URL piégées, qui masque sa présence et se connecte à un compte Twitter dans l'attente d'instructions. Ces dernières peuvent le conduire à télécharger une autre app malveillante ou à changer de compte Twitter de contrôle. Actuellement, selon Eset, Twittor sert à importer différentes versions d'un malware bancaire. Mais pourrait tout aussi bien passer au ransomware…

« *Utiliser Twitter plutôt que des serveurs de commande et contrôle (C&C) est plutôt innovant pour un botnet Android* », souligne Lukas Stefanko, le chercheur d'Eset qui a mis au jour cette nouvelle souche infectieuse. L'objectif des cybercriminels est, comme l'indique ce chercheur, de constituer un réseau de machines esclaves, soit un botnet. Le point faible des constructions de ce type réside souvent dans l'envoi régulier d'instructions aux éléments de ce réseau, des communications susceptibles de révéler l'existence du botnet. Par ailleurs, les serveurs C&C constituent le maillon faible des botnets : si les autorités les localisent et parviennent à les fermer, c'est tout le réseau criminel qui s'effondre.

Passer d'un compte Twitter à un autre

Autant de raisons qui pourraient avoir poussé les concepteurs de Twittor à complexifier les techniques de communication entre les machines esclaves et l'entité les contrôlant, selon Eset. En plus de l'emploi de Twitter, les cybercriminels chiffrent leurs messages et utilisent des topologies complexes pour leur architecture de C&C, avance l'éditeur. « *Ces canaux de communication sont difficiles à mettre au jour et encore plus difficiles à bloquer totalement*, reprend Lukas Stefanko. *De l'autre côté, il est très simple pour les escrocs de rediriger les communications vers un compte nouvellement créé.* » Et pas de risque de voir la police fermer purement et simplement Twitter pour ce motif…

Dans l'univers Windows, dès 2009, un botnet a eu recours à Twitter, fondé seulement 3 ans auparavant, pour envoyer des instructions. Mais Twittor est bien le premier malware créateur de bot commandé via le réseau social.

Article original de Reynald Fléchaux

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 : Inédit : un malware Android commandé par… Twitter

Alerte : Twitter pour Android infecté par un Cheval de Troie

Alerte : Twitter pour Android infecté par un Cheval de Troie

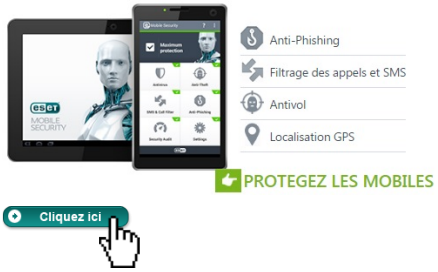
ESET découvre le premier botnet sous Android qui contrôle Twitter

Les chercheurs ESET ont découvert une porte dérobée sous Android qui contient un Cheval de Troie et qui est contrôlée par des tweets. Détecté par ESET comme étant Android/Twitoor, **il s'agit de la première application malveillante utilisant Twitter** au lieu d'une commande et d'un contrôle traditionnel de serveur (C&C).
Après son lancement, le Cheval de Troie cache sa présence sur le système et vérifie le compte Twitter défini par intervalle régulier pour les commandes. Sur la base des commandes reçues, il peut soit télécharger des applications malveillantes, soit basculer le serveur C&C d'un compte Twitter à un autre.
« L'utilisation de Twitter pour contrôler un botnet est une étape innovante pour une plateforme Android », explique Lukáš Štefanko, malware researcher chez ESET et qui a découvert cette application malicieuse.
Selon Lukáš Štefanko, les canaux de communication basés sur des réseaux sociaux sont difficiles à découvrir et impossible à bloquer entièrement – alors qu'il est extrêmement facile pour les escrocs de rediriger les communications vers un autre compte de façon simultanée.

Twitter a d'abord été utilisé pour contrôler les botnets de Windows en 2009. « En ce qui concerne l'espace Android, ce moyen de dissimulation est resté inexploité jusqu'à présent. Cependant, nous pouvons nous attendre à l'avenir à ce que les cybercriminels essayent de faire usage des statuts de Facebook ou de déployer leurs attaques sur LinkedIn et autres réseaux sociaux » , prévoit Lukáš Štefanko.
Android/Twitoor est actif depuis juillet 2016.Il ne peut pas être trouvé sur l'un des app store officiels d'Android (selon Lukáš Štefanko) mais il est probable qu'il se propage par SMS ou via des URL malveillantes. Il prend l'apparence d'une application mobile pour adulte ou d'une application MMS mais sans fonctionnalité. Plusieurs versions de services bancaires mobiles infectés par un malware ont été téléchargées. Cependant, les opérateurs de botnet peuvent commencer à distribuer d'autres logiciels malveillants à tout moment, y compris des ransomwares selon Lukáš Štefanko.

Twitoor est le parfait exemple de l'innovation des cybercriminels pour leur business. Les utilisateurs d'Internet devraient continuer à protéger leurs activités avec de bonnes solutions de sécurité valables pour les ordinateurs et les appareils mobiles », conclut Lukáš Štefanko.
Source : ESET

Pour protéger vos équipements, nous recommandons l'application suivante :



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

Attention à l'application

« Rio Olympics 2016 «

	Attention à l'application « Rio Olympics 2016 «

Avec l'approche des jeux Olympiques de Rio, le téléchargement d'applications thématiques va battre son plein. Gare aux applications dangereuses !
Rio Olympics 2016 Keyboard, un clavier publicitaire dangereux !

La société Lookout Mobile Security vient d'alerter ZATAZ de certains problèmes de confidentialité et des enjeux rencontrés par les utilisateurs et les entreprises avec l'application Rio Olympics 2016 Keyboard. Une APP disponible en version iOS et Android.
L'application officielle de l'entreprise américaine NBC Universal Media, Rio 2016 Olympics keyboard est en apparence une simple extension de clavier pour les personnes qui suivent les jeux Olympics. Cependant, il a identifié que cette application était capable de compiler plus d'information qu'initialement prévu par son développeur, exposant ainsi la confidentialité des données des amateurs des JO de RIO et possiblement des entreprises pour lesquelles ils travaillent.
Finalement, l'équipe de recherche a informé NBCUniversal des enjeux de confidentialité identifiés dans les versions Android et iOS de l'application officielle Rio 2016 Keyboard. NBCUniversal a réagi rapidement pour résoudre les problèmes identifiés et s'assurer que les versions disponibles seraient sécurisées avant l'ouverture des Jeux Olympiques d'été de Rio. Si vous avez téléchargé l'application, effacez là. A vous de décider, ensuite, si vous installez la nouvelle version.

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 : ZATAZ L'appli Rio Olympics 2016 Keyboard dangereuse – ZATAZ

Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Avant même la sortie sous Android de Prisma, une application populaire de retouche photos, Google Play Store s'était retrouvé inondé de fausses applications.

Les chercheurs d'ESET ont découvert de fausses applications imitant Prisma, dont plusieurs Chevaux de Troie dangereux. Dès l'avertissement d'ESET, le service sécurité de Google Play a retiré toutes les fausses applications du store officiel d'Android. Ces dernières auront tout de même atteint plus d'1,5 millions de téléchargements.
Prisma est un éditeur de photos unique publié par les laboratoires de Prisma. D'abord développé pour iOS, cette application a remporté d'excellents résultats de la part des utilisateurs d'iTunes et de l'App Store d'Apple. Les utilisateurs d'Android étaient à leurs tours impatients de la découvrir sur le Google Play (disponible depuis le 24 juillet 2016).
« La plupart des fausses applications de Prisma disponibles sur Google Play ne disposent pas d'une fonction retouche photo. A l'inverse, elles affichent uniquement des annonces, avertissements ou de faux sondages pour tromper l'utilisateur qui fournit des informations personnelles le concernant ; ou encore pour le faire souscrire à de faux services type SMS onéreux », commente Lukáš Štefanko, Malware Researcher chez ESET.
La plus dangereuse des fausses applications imitant Prisma et trouvée dans le Google Play est un Cheval de Troie téléchargeur détecté par ESET comme Android/TrojanDownloader.Agent.GY. Des informations sur les périphériques sont envoyées au serveur C&C, ce qui lui permet de télécharger sur demande des modules supplémentaires et de les exécuter afin de voler des données sensibles telles que le numéro de téléphone, l'opérateur, le pays, la langue etc.
A cause de ses capacités de téléchargement, la famille des malwares type Android/TrojanDownloader.-Agent.GY pose de sérieux risques pour les plus de 10.000 utilisateurs Android qui ont installé cette application dangereuse avant d'être retiré du Google Play Store.

Pour se protéger, Denis JACOPINI recommande l'application suivante :

Article original de Eset

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

Orange corrige un sérieux problème de sécurité dans l’une de ses boutiques en ligne

	Orange corrige un sérieux problème de sécurité dans l’une de ses boutiques en ligne

Alterte ! Plusieurs problèmes découverts dans le site orangeboutique.fr. L'un d'eux aurait pu permettre d'injecter un document piégé directement dans une boutique Orange.
Imaginez, vous visitiez le site orangeboutique.fr [espace fermé depuis le 19/07/16] et téléchargiez ce que vous pensiez être un document officiel de l'opérateur téléphonique Français. Un PDF vous proposant les dernières réductions et promotions. Sauf que dans ce fichier Adobe, un code malveillant orchestrant le téléchargement d'un logiciel espion dans votre ordinateur.
De la science-fiction ? Malheureusement, non ! Le protocole d'alerte de ZATAZ a permis la correction de plusieurs problèmes dans le site orangeboutique.fr. Parmi les « bugs » que je peux vous révéler aujourd'hui, la possibilité d'injecter dans l'espace 2.0 n'importe quel fichier à partir d'une page dédiée non verrouillée.
L'équipe sécurité d'Orange a très rapidement pris en main et corrigé le problème dès la réception du Protocole d'Alerte. D'autres failles et fuites concernées ce même site, avec par exemple l'accès à des documents internes. Des fichiers non sensibles [pas de données clients], sauf dans les mains de la concurrence pouvant ainsi découvrir les actions commerciales à venir dans les agences physiques Orange (Tarifs, produits, cibles clientèles…). Des accès sans aucune restriction, ni mot de passe. Le site a été fermé le 19 juillet 2016.
Article original de Damien Bancal

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 : ZATAZ Orange corrige un sérieux problème dans l'une de ses boutiques en ligne – ZATAZ

Attention aux versions piégées de Pokémon GO

Attention aux versions piégées de Pokémon GO

L'application Pokémon Go fait un carton dans les smartphones. Prudence, non encore officiel en Europe, installer le jeu via des boutiques hors de contrôle des auteurs met en danger votre vie privée.

Pas de doute, le phénomène Pokémon GO débarque en force en cet été 2016. L'application tirée du jeu éponyme de Nintendo permet de s'éclater à trouver des Pokemons un peu partout dans le monde. De la réalité virtuelle bien venue pour l'été.

Édité par Niantic, le créateur de Pokémon GO ne propose son appli qu'aux États-Unis, en Australie et en Nouvelle-Zélande. Un pré lancement pour tester les serveurs, très sollicités, et la stabilité du jeu. Bref, normalement, il n'est pas possible d'y jouer en Europe, et donc en France. Sauf qu'il y a toujours des possibilités, comme celle d'installer Pokémon GO vient l'APK (le programme) proposé par de nombreux sites Internet non officiels.

Attention ! des sites qui ne sont pas maîtrisés et contrôlés par les auteurs. Des espaces de téléchargements qui sont des limites du Play Store de Google et de l'App Store d'Apple. Bref, à vos risques et périls.

J'ai déjà pu repérer des APK piégés (ransomwares, cheval de Troie, …) proposés, je l'avoue, dans des lieux peu recommandables. Prenez l'avertissement très au sérieux. Pokemon GO ne vous demandera JAMAIS d'accéder à vos messages [SMS, MMS], à vos appels téléphoniques. Si l'APK que vous avez téléchargez vous propose ces « autorisations », ne l'installez surtout pas. Attendez la version officielle.

Je ne me voile pas la face, le phénomène attire beaucoup d'internautes, jeunes et moins jeunes. Et avec les vacances, une bonne occasion de sauter sur le jeu pour smartphone de l'été. Des milliers de Français l'ont fait. J'en croise beaucoup, dans la rue, comme le montre ma photographie, prise ce 13 juillet dans les rues de Paris. Je rentre de New York, l'engouement est… pire !

A noter que plusieurs éditeurs d'antivirus ont mis la main sur une version « malveillante » de Pokémon GO. Bitdefender, par exemple, parle de DroidJack. Ce cheval de Troie ouvre une backdoor et donne l'accès aux données des appareils mobiles infectés, permettant ainsi leur prise de contrôle à distance par les pirates. Ce malware disponible pour seulement 200 dollars sur certains sites Web, offre au pirate une interface de contrôle facile à utiliser lui permettant par exemple de surveiller l'activité des appareils corrompus, de passer des appels, d'envoyer des SMS, de localiser l'appareil, d'utiliser l'appareil photo ou le microphone ou même d'accéder aux dossiers.

La version iPhone malmenée par la version officielle

Autre mise en garde pour les joueurs de Pokémon GO : sur iOS, l'application semble demander plus d'autorisations que nécessaire. L'accès à l'application via un compte Google semble conférer au développeur Niantic (ex Start-up de Google), un accès complet aux comptes des utilisateurs. Ce problème est en cours de résolution et n'est pas présent dans les versions Android.

Article original de Damien Bancal

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 : ZATAZ Pokémon GO, prudence aux fichiers vérolés – ZATAZ

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

Le malware Nymaim s’attaque désormais aux institutions financières du Brésil

---

Après avoir contaminé l'Europe et l'Amérique du Nord en 2013, le malware Nymaim refait surface 3 ans plus tard et se propage désormais via une campagne de spearphising intensive, en utilisant un document Microsoft Word comme pièce jointe infectée

Lors de la découverte de la souche originale de Nymaim en 2013, notamment avec ses techniques de code modulaire (chaîne d'abattage et d'évasion), nous avions pu remarquer que plus de 2,8 millions d'infections s'étaient propagées. Sur le premier semestre 2016, ESET a de nouveau observé une augmentation significative de détections du malware Nymaim.

Infectant principalement la Pologne (54%), l'Allemagne (16%) et les Etats-Unis (12%), cette mutation du malware Nymaim a été détectée comme appartenant à la catégorie *Win32/TrojanDownloader.Nymaim.BA.* Elle utilise le spearphishing et une pièce jointe (type Word.doc) contenant une macro malveillante. Utilisée pour contourner les paramètres de sécurité par défaut de Microsoft Word via les techniques d'ingénierie sociale, l'approche est très dangereuse dans les versions anglaises de MS Word.

« Grâce à ses techniques d'évasion sophistiquées, l'anti-VM, l'anti-débogage et les flux de contrôle, cette fusée à deux étages sert à livrer le ransomware comme charge utile finale. Ce code que l'on peut nommer « Trojan modulaire » est impressionnant par sa faculté à voler les informations d'authentification de sites de banque électroniques dans les formulaires typiques en contournant la protection SSL. Ce code malveillant a évolué de façon à fournir des logiciels espions », explique Cassius de Oliveira Puodzius, Security Researcher chez ESET en Amérique Latine.

En avril 2016, la version précitée a été rejointe par une variante hybride de Nymaim (Gozi) qui avait pour cible les institutions financières d'Amérique du Nord, mais également en Amérique latine et principalement au Brésil. Cette variante fournit aux cybercriminels le contrôle à distance des ordinateurs compromis plutôt que de chiffrer les fichiers ou bloquer la machine – comme cela se fait habituellement.

En raison des similitudes entre les cibles visées dans chaque pays et les taux de détection, nous pouvons affirmer que les institutions financières restent au centre de cette campagne.

« L'étude complète de cette menace est toujours en cours. Toutefois, si vous pensez que votre ordinateur ou votre réseau a été compromis, nous vous recommandons de vérifier que les adresses IP et les URL que nous avons partagées dans l'article complet de WeLiveSecurity ne se trouvent pas dans votre pare-feu et dans le journal de votre proxy. Nous vous conseillons de mettre en place une stratégie de prévention en ajoutant une liste noire des des adresses IP contactées par ce malware au pare-feu et les URL à un proxy, aussi longtemps que votre réseau prendra en charge ce type de filtrage », conclut Cassius de Oliveira Puodzius.

Pour lire l'intégralité du rapport et ainsi obtenir des informations complémentaires sur le malware Nymaim, cliquez ici.

Cliquez ici

Article original de Lucie Fontaine

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

Eleanor, nouvelle menace sur la planète Mac

Eleanor, nouvelle menace sur la planète Mac

Alors que beaucoup d'utilisateurs de Mac se montrent parfois négligents en matière de sécurité, les équipes de BitDefender ont détecté un nouveau backdoor baptisé Eleanor qui ciblent les Mac et qui peut causer d'importants dégâts sur les machines. En effet, il offre la possibilité aux pirates de prendre le contrôle d'une machine à distance.

Le backdoor Eleanor à l'assaut des Mac

Comme souvent, c'est l'éditeur BitDefender qui a identifié la nouvelle menace qui pèse sur les Mac. Eh oui, même si les dangers sont généralement moindres sur Mac que sur PC, voilà que ceux qui ont choisi les ordinateurs d'Apple doivent se montrer vigilants.

En effet, dès lors que ce backdoor silencieux est parvenu à infecter une machine, il a la capacité de permettre à un attaquant de prendre le contrôle du Mac à distance. Ainsi, les hackers peuvent s'en servir pour voler des données présentes sur la machine piratée, télécharger des applis frauduleuses ou même pour détourner la webcam, une pratique de plus en plus courante.

Reste que l'infection du Mac ne se produit pas toute seule et qu'elle est l'une des conséquences du téléchargement de l'application malveillante Easy Doc Converter. En effet, lors du démarrage d'OS X, cette appli va installer sur le Mac trois composantes : un service Tor, un service web capable de faire tourner PHP et un logiciel dédié. Autrement dit le matériel indispensable pour que s'installe, sur Mac, un backdoor silencieux comme Eleanor.

L'intégralité des Mac concernée par Eleanor ?

Si BitDefender a tenu à alerter sur sa découverte, il semblerait tout de même que tous les Mac ne soient pas tous concernés par cette menace.

En effet, parce que le logiciel Easy Doc Converter n'est pas signé numériquement avec un certificat approuvé par Apple, les risques d'infection sont réduits. D'ailleurs, la marque à la pomme a tenu à le préciser en rappelant que tous les Mac dotés de la protection Gatekeeper n'avaient rien à craindre.

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 : Eleanor, nouvelle menace sur la planète Mac