Encore une faille 0-day sur Flash Player menaçant vos ordinateurs | Le Net Expert Informatique

Encore une faille 0-day sur Flash Player menaçant vos ordinateurs

Ces derniers mois, Flash Player a subi les foudres de grands noms de l'informatique suite à de nombreuses vulnérabilités découvertes en plus des innombrables précédentes corrigées auparavant. Déjà alors, certaines institutions comme Facebook réclamaient l'abandon du plug-in Flash alors cet aveu issu de la société de développement Adobe ne risque pas d'arranger le sort de son Flash Player.

Un rapport publié par la société Adobe a été publié mercredi et confirme la présence d'une faille critique au sein de la dernière version du Player mais aussi des précédentes. Celle-ci peut être employée « lors d'attaques limitées et ciblées ». Sont concernées les dernières versions,19.0.0.207 incluse mais également toutes les précédentes itérations sur Windows et Mac, Adobe Flash Player Extended Support Release pour l'intégralité des versions 18 ainsi que les versions pour Linux.

En plus des vulnérabilités 0-day employés par la Hacking Team, cette faille avait été décelée au cours de l'été par TrendMicro qui mettait alors au jour une attaque informatique de grande envergure orchestrée par le groupuscule Pawn Storm, pirates visant différents ministères des affaires étrangères à travers le monde ainsi que certains média.

Si cette attaque reposait principalement sur l'utilisation de malwares, des méthodes de phishing et exploitait une faille inhérente à Java (la première repérée depuis des années), le magazine spécialisé a par la suite découvert que les hackers s'appuyaient aussi sur une faille présente dans Flash Player.

Confirmée par Adobe, celui-ci a aussitôt assuré se mettre à l'élaboration d'un correctif. Initialement prévu pour une distribution au 16 octobre, ce patch devrait finalement être disponible vers le 19 du même mois. Reste que la plus sûre des solutions en attendant sa mise à jour consiste à désinstaller complètement le lecteur. Si la faille ne concerne pas directement la personne lambda mais principalement les hautes institutions, le principe d'action pourrait tout de même être repris par d'autres pirates et appliqués à une plus grande partie de la population. Prudence.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

http://www.phonandroid.com/flash-player-encore-faille-0-day-menacant-ordinateurs.html

Un nouveau virus découvert sur des distributeurs de billets | Le Net Expert Informatique

Un nouveau virus découvert sur des distributeurs de billets

Un nouveau malware a été en mesure d'attaquer des distributeurs automatiques de billets. Baptisé GreenDispenser, il entre dans la longue liste des outils informatiques permettant de vider le contenu d'une machine.

Après Suceful, Plotus ou encore Padpin, des experts en sécurité annoncent avoir découvert un nouveau malware informatique capable de s'attaquer aux distributeurs de billets. GreenDispenser agit comme un virus classique et permet de faire sauter les barrières de sécurité mises en place sur ce type d'appareil.

Le procédé d'attaque est classique. Les pirates doivent être en mesure d'accéder physiquement au distributeur. Le système peut alors être infecté par le biais du virus en se focalisant sur un middleware utilisé sur de nombreuses machines de ce type (utilisant la norme XFS). Ce logiciel, censé faire le lien entre la partie les périphériques (le clavier par exemple) fait fonctionner le distributeur ainsi que le reste de l'équipement va être le point faible.

Toujours est-il que le malware est capable d'agir sur le processus d'authentification à double facteurs des appareils. GreenDispenser permet également de mettre hors service un distributeur et dispose même d'un mécanisme d'autodestruction, le rendant particulièrement difficile à détecter par les éditeurs en sécurité ou d'éventuels enquêteurs.

A l'heure actuelle, GreenDispenser a principalement sévi au Mexique. Selon l'éditeur de sécurité Proofpoint, le malware pourrait toutefois facilement s'étendre à d'autres régions géographiques en dehors de l'Amérique latine. La société conseille aux professionnels détenant des distributeurs de vérifier la sécurité de leur dispositif et d'appliquer d'éventuelles mises à jour.

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

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-780740-virus-decouvert-distributeurs-billets.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1167429992#pid=22889469

Liste des applications iPhone et iPad infectées par le logiciel malveillant

XcodeGhost | Le Net Expert Informatique

	Liste des applications iPhone et iPad infectées par le #logiciel malveillant XcodeGhost

Des experts en sécurité ont récemment découvert sur un certain nombre d'applications dans l'App Store d'Apple un maliciel iOS appelé XcodeGhost. Les créateurs de XcodeGhost ont été en mesure d'intégrer un code malveillant dans ces applications à l'insu de leurs développeurs. Parmi les applications touchées, on retrouve les populaires WeChat et CamCard. Nous pouvons donc estimer que le nombre de victimes potentielles du logiciel malveillant XcodeGhost s'élèverait à de centaines de millions d'utilisateurs.

Voici une liste non exhaustive des applications détectées en tant que malveillantes :

CamCard Business
Action: Update to latest version
Current Status: Patched
Last version checked: 1.8.2

CamScanner Free| PDF Document Scanner and OCR
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

CamScanner +| PDF Document Scanner and OCR
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

Cam Scanner Pro
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

WeChat
Action: Update to latest version
Current Status: Patched
Last version checked: 6.2.6

WinZip – The leading zip unzip and cloud file management tool
Action: Update to the latest version
Current Status: Patched
Last version checked: 4.3

网易云音乐-好口碑,电台FM歌曲下载必备
Action: Update to latest version
Current Status: Patched
Last version checked: 2.9.0

OPlayerHD Lite
Action: Update to latest version
Current status: Patched
Last version checked: 2.1.03

网易公开课 — 教育视频平台，名校名师名课，TED演讲、优质纪录片
Action: Update to latest version
Current Status: Patched
Last version checked: 4.2.9

LifeSmart
Action: Uninstall immediately
Current status: Still malicious
Last version checked: 1.0.45

10000+ Wallpapers for iOS 8, iOS 7, iPhone, iPod and iPad
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.6

喜马拉雅FM (Podcasts) 儿童故事评书段子财经相声radio
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 4.3.8

开眼 — 精选视频推介，每天大开眼界
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.8.0

愤怒的小鸟2-李易峰至尊手游
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 2.1.1

爱推
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.1.5

电话号码归属地助手
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.6.5

自由之战-真·5V5(第一MOBA手游)
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.1.0

中国联通手机营业厅(官方版)
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.2

股市热点
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 2.40.01

Plus d'infos sur : https://blog.lookout.com/blog/2015/09/21/xcodeghost-apps

---

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

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

Source : https://blog.
lookout.com/fr/2015/09/23/xc
odeghost-apps/

Des hackers dupent Apple et infectent des millions d’iPhone | Le Net Expert Informatique

Des hackers dupent Apple et infectent des millions d’iPhone

Pour la première fois, des pirates ont réussi à diffuser des applications malveillantes sur le magasin AppStore, en trafiquant le langage de codage utilisé par les développeurs.

Après ses ordinateurs Mac, c'est au tour des iPhone et iPad d'Apple de se frotter aux virus. Le groupe à la pomme croquée a confirmé à Reuters que son magasin d'applications AppStore a été victime de sa toute première faille de sécurité majeure. Jusqu'à présent, l'AppStore était réputé comme ultra-sûr puisqu'Apple inspecte minutieusement chaque appli avant de la proposer aux téléchargements (à l'inverse du Play Store de Google), afin d'éviter les logiciels malveillants mais aussi imposer sa chape de plomb sur le sexe.

Sauf que des pirates malins ont trouvé une parade pour échapper à la vigilance de la pomme. Les hackers sont remontés jusqu'à la source de toutes les applis, le langage de codage Xcode, pour diffuser auprès des développeurs naïfs une version compromises (intitulée XcodeGhost). Toutes les applis créées avec cet outil pouvant dès lors de se transformer en logiciel malveillant. Un porte-parole d'Apple souligne auprès de Reuters :

Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps ».

La version compromise de Xcode a été identifiée comme hébergée sur un serveur chinois. Les développeurs ont préféré celle-ci puisqu'elle s'avérait beaucoup plus rapide à télécharger que le logiciel officiel hébergé sur le serveur d'Apple.

Des centaines de millions d'iPhone exposés

Selon la firme de sécurité Palo Alto Networks Inc, 39 applications malicieuses ont été découvertes et certaines sont particulièrement populaires, dont :

– l'incontournable appli de discussion instantanée WeChat,
– le très utilisé enregistreur de cartes de visites CamCard,
– Didi Chuxing, le concurrent chinois d'Uber,
– l'unique appli pour acheter des billets de train en Chine Railway 12306.

Au total, plusieurs centaines de millions d'utilisateurs pourraient avoir été victimes d'un vol de données tels que des mots de passe, estime l'entreprise, même si aucun cas n'a pour l'heure été constaté.

La firme de sécurité chinoise Qihoo360 affirme elle avoir détecté pas moins de 344 applis compromises. Plusieurs ont été retirées de l'AppStore par Apple, mais le groupe refuse de donner le nombre exact d'applications concernées. Un porte-parole affirme à « l'Obs » : *Nous prenons la sécurité très au sérieux et iOS [le système de l'iPhone et l'iPad, NDLR] est conçu pour être fiable et sécurisé. Pour protéger nos clients, nous avons supprimés les applications de l'AppStore que nous savons créées avec cet outil contrefait. »*

Sur son blog, WeChat affirme que seule la version de son appli antérieure au 10 septembre était affectée par la faille de sécurité. Une nouvelle version a depuis été diffusée pour remédier au problème.

Les iPhone, « des cibles de choix »

Selon Ryan Olson de Palo Alto Networks Inc, « l'information n'est toutefois pas à prendre à la légère », puisque cela montre que l'AppStore peut être compromis par des hackers qui ciblent les développeurs. Pis, cela pourrait donner des idées à d'autres et il sera difficile de s'en prémunir, estime-t-il.

L'iPhone ne serait-il plus aussi sûr qu'à ses débuts ? « Avec l'augmentation des parts de marché d'Apple, le nombre de cibles augmente et l'intérêt des cybercriminels augmente », pointe Laurent Heslault, responsable des stratégies de sécurité chez Symantec. Gérome Billois, administrateur du Club de la sécurité de l'information français (Clusif), renchérit :

Surtout que les utilisateurs d'Apple sont connus pour avoir des revenus plus élevés, faisant d'eux des cibles de choix ».

Surtout que les utilisateurs d'iPhone – et plus largement de smartphones – n'ont pas encore pris pleinement conscience des risques de piratage sur ces mini-ordinateurs. Rien que l'an dernier, l'entreprise de sécurité Symantec a découvert 6,3 millions d'appli malicieuses capables d'infecter les terminaux.

Apple n'est donc pas beaucoup plus sûr que ses concurrents. Le rapport annuel de Symantec pointe que 84% des vulnérabilités découvertes le sont sur iPhone (contre 11% pour Android). Le plus souvent, elles sont exploitées pour infecter l'appareil, dérober des informations personnelles (mots de passe, comptes bancaires…), afficher des publicités, ou encore envoyer des SMS surtaxés. Laurent Heslault interroge :

Il y a des centaines de milliers d'applications gratuites disponibles, croyez-vous qu'il y ait autant de philanthropes ? »

La vigilance est donc de rigueur avant de cliquer sur un lien, entrer ses identifiants sur un site, etc. Même prudence lorsqu'une fenêtre pop-up s'ouvre sur l'iPhone, réclamant l'identifiant et le mot de passe iCloud. Si elle n'a pas de raison de s'ouvrir (par exemple lors de la consultation de ses e-mails), alors il n'y a pas de raison de lui donner les informations.

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

Source : http://tempsreel.nouvelobs.com/tech/20150921.OBS6188/des-hackers-dupent-apple-et-infectent-des-millions-d-iphone.html
Par Boris Manenti

Savoir profiter des erreurs des Cybercriminels | Le Net Expert Informatique

Savoir profiter des erreurs des Cybercriminels

L'affaire Ashley Madison semble le prouver une fois de plus, les cybercriminels commettent des erreurs qui peuvent leur nuire. Détecter ces fautes et savoir les utiliser sont des éléments essentiels dans la gestion des crises cyber.

DES ATTAQUES DONT LES OBJECTIFS SONT SOUVENT DIFFICILES À CERNER

L'actualité le montre trop régulièrement, les actes cybercriminels se multiplient et visent tous types d'organisation. Certains sont revendiqués et leurs objectifs sont rapidement connus. C'est le cas pas exemple de l'attaque visant le site Ashley Madison où les motivations sont explicites.

Mais dans la plupart des cas, les objectifs de l'attaquant sont beaucoup plus difficiles à identifier ! Il est pourtant crucial de le faire pour pouvoir réagir au mieux et protéger rapidement ce qui n'a pas encore été touché par l'attaque.

Une des clés pour mieux comprendre une attaque consiste à exploiter les erreurs des attaquants. En effet, malgré leur niveau de compétences potentiellement élevé, les pirates restent des humains et commettent souvent des erreurs. Des fautes qu'il est possible d'exploiter pour mieux comprendre l'attaque et la contrer, mais aussi pour identifier ceux à son origine.

UTILISER LES ERREURS DES ATTAQUANTS POUR MIEUX LES COMPRENDRE

Le cas récent d'Ashley Madison semble être un bon exemple, même s'il faudra attendre les investigations complètes pour confirmer tous les éléments. Les attaquants auraient diffusé les données volées via BitTorrent en utilisant un serveur loué chez un hébergeur aux Pays Bas. Ils auraient cependant oublié de sécuriser ce serveur, en particulier ils n'ont pas mis de mot de passe sur les interfaces d'administration web. Même si cela ne permet pas de les identifier directement, il s'agit d'une piste de premier choix pour les forces de l'ordre en charge des investigations. Il faut cependant rester prudent car cela peut aussi être une forme de diversion réalisée par les attaquants. Affaire à suivre !

Autre exemple, le cas « Red October ». C'est l'affaire d'une vaste opération de cyber espionnage qui a commencé en mai 2007 et qui a été découverte par le cabinet Kaspersky quelques années plus tard. Le cabinet a réussi à identifier, bloquer et neutraliser le logiciel malveillant en utilisant une faille de l'attaque. En effet, les noms de domaines pour les serveurs d'exfiltration qui étaient utilisés dans le code malveillant n'avaient pas été réservés par les attaquants. Cela a permis à Kaspersky de simuler un de ces serveurs et de voir qui était infecté et quelles données étaient capturées.

Parfois, ces erreurs permettent même d'identifier les auteurs de l'attaque, comme ce fut le cas avec la traque de la personne derrière le malware PlugX.

Nos consultants ont d'ailleurs eux aussi rencontré ce genre de situation dans le cadre d'une attaque ciblée chez un de nos clients. Les pirates avaient en effet « oublié » la présence d'un keylogger sur les serveurs internes utilisés pour l'exfiltration des données, ce qui a permis à nos experts d'identifier quelles données étaient ciblées et où elles étaient envoyées. Nous avons même pu récupérer le login et le mot de passe utilisés par les attaquants. Le concept de « l'arroseur arrosé » remis au goût du jour.

SAVOIR TIRER PARTI DE CES INFORMATIONS POUR MIEUX GÉRER LA CRISE

Les informations obtenues grâce à ces erreurs sont très précieuses, elles permettent ensuite d'adapter la réponse à l'incident. D'autant plus que les attaquants utilisent parfois des mécanismes de diversion « bruyants » (redémarrage de machines, effacement de fichiers, forte activité CPU, voir déni de service…) afin de détourner l'attention des vrais données qu'ils visent. Une compréhension « métier » des objectifs de l'attaque permet d'éviter de se focaliser sur ces pièges.

Il est même souvent intéressant de laisser l'attaque se dérouler pour mieux la comprendre.

Les réflexes face aux incidents de sécurité « classiques » (déployer des signatures antivirales, réinstaller des serveurs…) sont donc aujourd'hui largement révolus. Il faut adopter une approche dynamique de la crise, s'intéresser à son objectif métier et utiliser les erreurs des attaquants pour être plus pertinent, en pouvant même envisager des réponses « actives » à l'attaque. Un challenge pour les équipes de réponses à incidents, qui doivent adapter leurs méthodologies et leurs réflexes, mais un objectif crucial pour lutter contre ces attaques

---

Source :

http://www.solucominsight.fr/2015/08/attaques-ciblees-profiter-des-erreurs-des-attaquants-pour-mieux-les-comprendre-et-les-contrer/

L’écran de verrouillage d’Android cède une nouvelle fois | Le Net Expert Informatique

L’écran de verrouillage d’Android cède une nouvelle fois

La méthode, assez simple, ne nécessite pas l'injection d'un malware. Elle concerne tous les terminaux sous Android 5.x et supérieurs.

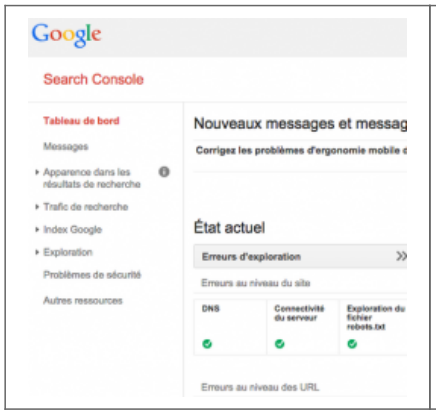
Contourner l'écran de verrouillage des smartphones Android n'est décidément pas très compliqué. Un spécialiste en fait une nouvelle fois la démonstration, utilisant une méthode assez simple qui n'exige pas de connaissances particulières ni l'injection d'un malware. Elle concerne tous les terminaux sous Android 5.x et supérieurs dont l'accès est protégé par un code (et pas un schéma).
La marche à suivre consiste d'abord à accéder aux appels d'urgence puis d'entrer une chaîne de caractères, les surligner (double-clic) et les copier. Il s'agit ensuite de copier et de coller autant de fois que c'est possible cette chaîne dans le champ mot de passe. Puis de se rendre dans l'appli photo, de faire apparaître la zone de notifications et de copier la chaîne de caractère lorsque l'appli demande à nouveau le mot de passe.
A ce moment, (après un moulinage plus ou moins long), l'appli Photo plante et le terminal se débloque comme par magie, permettant d'accéder à tout son contenu.
Prévenu de cette faille, Google n'a pas encore communiqué sur la question.

Source :
http://www.zdnet.fr/actualites/android-l-ecran-de-verrouillage-cede-une-nouvelle-fois-39824986.htm

---

Les pirates du SEO s'attaquent à Google Search Console | Le Net Expert

Informatique



Les pirates du SEO s'attaquent à Google Search ConsoleInformatique

Le spécialiste en sécurité Sucuri alerte sur la recrudescence d'attaquants qui se font passer pour les véritables propriétaires de sites web sur le service Google Search Console afin de détourner le trafic vers des pages et des sites infectés. Ces pirates vont jusqu'à supprimer les webmasters légitimes de la liste des propriétaires identifiés des sites.

Il arrive de plus en plus souvent que des pirates ayant compromis des sites web s'identifient eux-mêmes comme l'un des propriétaires de ces sites dans la Search Console de Google, constatent les chercheurs de la société Sucuri, spécialisée dans la sécurité sur Internet. Dans certaines circonstances, cela permet à ces attaquants d'agir plus longtemps sans être détectés. Précédemment connu sous le nom de Webmaster Tool, le service Search Console permet aux administrateurs de sites web de voir et comprendre où se situent leurs sites dans les résultats du moteur de recherche. Au-delà de ce type d'analyses, il permet aux webmasters de proposer de nouveaux contenus à indexer et de recevoir des alertes lorsque Google détecte des malwares ou des problèmes de spam sur leurs pages web (des mots-clés répétés abusivement). C'est particulièrement important car les infections entraînent des pertes de trafic et de réputation. Les utilisateurs qui cliquent sur des liens de résultats de recherche conduisant vers des sites hébergeant des malwares ou du contenu spammé reçoivent des avertissements inquiétants jusqu'à ce que ces sites soient nettoyés par leurs propriétaires.
Sur les comptes utilisateurs de la Search Console, Google permet en fait à plusieurs personnes de se dire propriétaires d'un site. Cela n'a rien d'inhabituel puisqu'il y a généralement plusieurs intervenants. Les spécialistes des outils de recherche, notamment, sont souvent distincts des administrateurs de sites et tous utilisent les données de la Search Console dans leurs rôles respectifs. Il y a plusieurs façons de se faire identifier comme propriétaire, mais la plus simple consiste à charger un fichier HTML avec un code unique pour chacun dans le dossier racine du site. Or, de nombreuses failles qui permettent aux attaquants d'injecter du code malveillant sur les pages web leur ouvrent aussi des portes pour créer des fichiers sur les serveurs web sous-jacents. Ces pirates peuvent notamment exploiter des vulnérabilités pour s'identifier comme l'un des propriétaires du site dans Search Console en créant les fichiers HTML requis.

Les attaquants exploitent des techniques de BHSEO

De tels abus deviennent de plus en plus courants. Sucuri cite pour preuve les multiples posts publiés à ce sujet sur les forums par les propriétaires de sites. Dans l'un des cas signalés, un webmaster a trouvé plus de 100 « utilisateurs vérifiés » dans sa console, note l'expert en sécurité Denis Sinegubko dans un billet. De nombreux pirates utilisent des sites compromis pour créer de fausses pages, tromper le classement des résultats de recherche et diriger le trafic vers d'autres pages à contenu dupliqué, ce qui permet aux attaquants d'exploiter des techniques d'optimisation de type BHSEO (black hat search engine optimization).

Devenus propriétaires vérifiés sur des sites compromis, les pirates peuvent alors suivre tranquillement les performances de leurs campagnes BHSEO sur le moteur de recherche de Google. Ils peuvent aussi soumettre de nouvelles pages de spams à indexer plus rapidement plutôt que de devoir attendre que ces pages soient naturellement découvertes par les robots de recherche. Ils peuvent aussi recevoir des alertes de Google si les sites sont identifiés comme étant compromis et, pire encore, ils peuvent éjecter les propriétaires légitimes des sites du service Search Console.

Des notifications qui passent entre les mailles

Lorsqu'un utilisateur est dit « vérifié » pour un site, les propriétaires de ce site vont recevoir une notification par email de Google. Cependant, ces messages peuvent facilement passer à travers les mailles du filet. Par exemple, s'ils sont envoyés vers une adresse mail qui n'est pas utilisée très souvent, ou bien s'ils sont noyés au milieu d'autres notifications reçues lors d'une journée très chargée en messages, ou encore s'ils arrivent pendant une période de congés. Dans ces cas-là, si les propriétaires légitimes n'ont pas consulté ces notifications et pris immédiatement des mesures, les attaquants peuvent alors les enlever de la liste de vérification du service Search Console en supprimant purement et simplement les fichiers de vérification HTML du serveur. Cela ne déclenchera aucune notification vers les véritables détenteurs du site, souligne Denis Sinegubko, de Sucuri.

Par la suite, si Google détecte un site web compromis et alerte automatiquement ses propriétaires identifiés comme tels, seuls les attaquants recevront cette notification. Ils pourront alors enlever temporairement du site les portes dirigeant vers leurs faux sites avant d'adresser à l'équipe antispam de Google une requête pour faire débloquer le site dans les résultats de recherche. Après quoi, ils pourront tranquillement remettre leur doorways vers différentes adresses URL, explique le chercheur de Sucuri.

Utiliser les méthodes alternatives de Google pour s'identifier

Si les véritables propriétaires ne sont plus identifiés comme tels, cela leur prendra un certain temps pour se rendre compte de ce qui s'est produit. Il est même possible qu'ils ne s'en aperçoivent pas. Pendant ce temps, les pirates continuent à exploiter leurs sites à leurs propres bénéfices. Et même si les administrateurs légitimes repèrent les faux propriétaires, il n'est pas toujours simple de s'en débarrasser. Les chercheurs de Sucuri ont vu de quelle façon les attaquants procédaient quelquefois en s'appuyant sur des règles de réécriture des URL dans le fichier de configuration htaccess et en générant dynamiquement des pages. Dans ces cas-là, les robots de vérification de Google détectent les fichiers HTML requis même si ceux-ci n'existent pas sur le serveur et si les vrais administrateurs ne peuvent pas les trouver.

Pour se préparer à de telles attaques, les webmasters peuvent prendre diverses mesures, indique Denis Sinegubko dans son billet. En premier lieu, ils doivent s'assurer qu'ils sont bien « vérifiés » comme propriétaires sur tous leurs sites web (en incluant les sous-domaines) dans la Search Console, même s'ils n'utilisent pas souvent ce service. Il existe trois méthodes alternatives de vérification acceptées par Google : à travers un fournisseur de noms de domaine, via un code de suivi Google Analytics ou, encore, avec une portion de code JavaScript à coller dans les pages. Cela évitera que des pirates suppriment leurs propres « vérifications » simplement en détruisant les fichiers correspondants sur le serveur. Enfin, à chaque fois qu'ils reçoivent des notifications de « new owners » de la part de Google, les webmasters doivent impérativement les contrôler en détail. « Dans la plupart des cas, cela signifie qu'ils ont un accès complet à votre site », avertit Denis Sinegubko. « Il faut alors intervenir sur toutes les failles de sécurité et supprimer tous les contenus malveillants que les attaquants auraient pu créer sur votre site », pointe le chercheur de Sucuri.

Source :
http://www.lemondeinformatique.fr/actualites/lire-les-pirates-du-seo-s-attaquent-a-google-search-console-62333.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Implantation de malwares dans les routeurs Cisco| Le Net Expert Informatique

	**Implantation de malwares dans les routeurs Cisco**

La firme de sécurité Mandiant, filiale de FireEye, a découvert que les firmwares de 14 routeurs d'entreprise de Cisco avaient été remplacés par des versions malveillantes permettant d'ouvrir des backdoors et de compromettre d'autres systèmes.

Remplacer le firmware d'un routeur par une version contaminée n'est plus du tout un risque théorique. Les chercheurs de la société Mandiant, spécialisée dans la sécurité informatique, ont détecté une véritable attaque ayant conduit à installer un faux firmware sur des routeurs d'entreprise dans quatre pays. Le logiciel implanté, désigné sous le nom de SYNful Knock, permet à des attaquants de disposer ainsi d'une porte dérobée, avec des accès à privilèges élevés, pour s'introduire dans les équipements affectés et y rester. La « backdoor » est en effet maintenue, même après un redémarrage du routeur. C'est un élément différentiant et inquiétant par rapport aux malwares que l'on trouve sur les routeurs grand public et qui disparaissent de la mémoire lorsque le périphérique est relancé.

SYNful Knock se présente comme une modification du système d'exploitation IOS (Internetwork Operating System) qui tourne sur les routeurs professionnels et les commutateurs de Cisco. A ce jour, les chercheurs de Mandiant l'ont découvert sur les routeurs ISR (Integrated Service Routeurs) modèles 1841, 8211 et 3825 que les entreprises placent en général dans leurs succursales ou qui sont utilisés par les fournisseurs de services réseaux managés.

Des experts de Mandiant mettent en garde contre de faux firmwares qui implantent des portes dérobées dans plusieurs modèles de routeurs Cisco : ISR 1841 (ci-dessus), 8211 et 3825. (crédit : D.R.)

Défaut ou vol de certificats d'administration

Filiale de la firme de cybersécurité FireEye, Mandiant a trouvé le faux firmware sur 14 routeurs, au Mexique, en Ukraine, en Inde et aux Philippines. Les modèles concernés ne sont plus vendus par Cisco, mais il n'y a aucune garantie que d'autres modèles ne seront pas ciblés à l'avenir ou qu'ils ne l'ont pas déjà été. Cisco a publié une alerte de sécurité en août avertissant ses clients sur de nouvelles attaques sur ses routeurs.

Dans les cas étudiés par Mandiant, SYNful Knock n'a pas été exploité en profitant d'une faille logicielle, mais plus probablement à cause d'un défaut de certificats d'administration ou via des certificats volés. Les modifications effectuées sur le firmware n'ont pas modifié sa taille d'origine. Le logiciel qui prend sa place installe une backdoor avec mot de passe ouvrant un accès Telnet à privilèges et permettant d'écouter les commandes contenues dans des packets TCP SYN (d'où le noom SYNful Knock). La procédure peut être utilisée pour indiquer au faux firware d'injecter des modules malveillants dans la mémoire du routeur. Toutefois, contrairement à la porte dérobée, ces modules ne résistent pas à un redémarrage du périphérique.

Des compromissions très dangereuses

Les compromissions de routeurs sont très dangereuses parce qu'elles permettent aux attaquants de surveiller et modifier le trafic réseau, de diriger les utilisateurs vers de faux sites et de lancer d'autres attaques contre des terminaux, serveurs et ordinateurs situés au sein de réseaux isolés. Généralement, les routeurs ne bénéficient pas du même degré d'attention que d'autres équipements, du point de vue de la sécurité, car ce sont plutôt les postes de travail des employés ou les serveurs d'applications que les entreprises s'attendent plutôt à voir attaqués. Les routeurs ne sont pas protégés par des utilitaires anti-malwares ni par des pare-feux.

« Découvrir que des backdoors ont été placées dans votre réseau peut se révéler très problématique et trouver un implant dans un routeur, encore plus », soulignent les experts en sécurité de Mandiant dans un billet. « Cette porte dérobée fournit à des attaquants d'énormes possibilités pour propager et compromettre d'autres hôtes et des données critiques en utilisant ainsi une tête de pont particulièrement furtive ». Dans un livre blanc, Mandiant livre des indicateurs pouvant être utilisés pour détecter des implants SYNful Knock, à la fois localement sur les routeurs et au niveau du réseau. « Il devrait être évident maintenant que ce vecteur d'attaque est vraiment une réalité et que sa prévalence et sa popularité ne feront qu'augmenter », préviennent les experts. A la suite de l'information diffusée par Mandiant, Cisco a lui aussi communiqué sur le sujet, en fournissant des explications complémentaires.

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-des-malwares-implantes-dans-les-routeurs-cisco-62359.html?utm_source=mail&utm_medium=email&utm_campaign=LeNetExpert.fr
Par Lucian Constantin / IDG News Service (adapté par Maryse Gros)

Alerte : Un ransomware qui verrouille votre appareil en changeant le code PIN Android | Le Net Expert Informatique

Alerte : Un ransomware qui verrouille votre appareil en changeant le code PIN Android

La société ESET a récemment publié un rapport alarmant sur la prolifération des ransomwares sur les appareils mobiles, aux États-Unis pour la plupart. Ces derniers se font passer pour des applis pornos réclamant des permissions quelque peu douteuses. Une fois ces dernières accordées, votre appareil est tout simplement verrouillé.

Nous vous parlions en début de semaine d'une application porno qui prenait ses utilisateurs en photo, puis leur demandait une rançon. Ce ransomware virulent se cachait derrière un fichier .apk que le détenteur du smartphone visé installait, sans le savoir, depuis un site pas très catholique.

Les chercheurs de la société ESET (qui édite des antivirus) viennent de pointer dans un billet de blog le fait que les ransomwares évoluent et se révèlent de plus en plus difficiles à contrer. Le dernier en date, Porn Droid, se présente comme souvent sous la forme d'un lecteur de contenus pour adultes. Ce dernier se télécharge au format .apk depuis un market alternatif, comme la plupart des applications du genre. Ce Porn Droid cache en vérité un ransomware qui va, en vous demandant les privilèges administrateur discrètement, bloquer votre appareil. Un message du FBI (classique) s'affichera et vous réclamera la modique somme de 500 $ à payer rapidement. Ce message stipule d'ailleurs (classique aussi) que vous avez hébergé du contenu pornographique interdit.

Une fois la menace passée, ce ransomware va bloquer votre appareil préféré par l'intermédiaire d'un Code Pin que vous ne connaissez évidemment pas. Pire encore, si vous avez l'habitude d'utiliser cette sécurité pour protéger votre smartphone, le ransomware est capable d'en modifier le code. ESET propose une solution si Porn Droid fait des siennes avec votre cher appareil Android. Pour ce faire, il faut employer l'invite de commande et la passerelle de débogage Android pour modifier le fichier chargé de traiter le code PIN de votre appareil. De plus, votre terminal doit être rooté, ce qui rajoute une condition supplémentaire. Notez que ce ransomware est tellement virulent qu'il est capable de fermer les antivirus installés sur votre mobile qui tournent en tâche de fond. En définitive, la meilleure solution reste la prévention. Méfiez-vous des portails proposant des applications à télécharger .apk et appliquez les 10 commandements de la sécurité pour garder son appareil à l'abri de toutes menaces. Si le porno mobile vous intéresse, consultez notre article qui lui est consacré.

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

Source : http://www.android-mt.com/news/porn-droid-ransomware-android-43752

Jusqu'à 200 000 utilisateurs WhatsApp touchés par une cyberattaque | Le Net Expert Informatique

Jusqu'à 200 000 utilisateurs WhatsApp touchés par une cyberattaque

Jusqu'à 200 000 utilisateurs du service de messagerie WhatsApp pourraient avoir été touchés par une cyberattaque permettant aux pirates de compromettre les données personnelles en utilisant simplement son numéro de téléphone.

Selon Checkpoint, une vulnérabilité dans la version web du service de messagerie WhatsApp aurait exposé jusqu'à 200 000 utilisateurs à une cyberattaque permettant aux pirates de compromettre les données personnelles. Pour cette attaque, les pirates ont simplement envoyé une vCard infectée à des numéros de téléphone au hasard.

Checkpoint précise que la faille dans la version web de WhatsApp pouvait être facilement exploitée par des personnes malveillantes, « sans aucun outil » spécifique.

Signalée à WhatsApp le 21 août dernier, la faille a été corrigée le 27 août. Ce n'est que maintenant que Checkpoint annonce sa découverte.

« Heureusement, WhatsApp a réagi rapidement et de manière responsable en déployant rapidement un correctif contre l'exploitation de cette faille dans le client web », écrit Oded Vanunu, gestionnaire de groupe de recherche de sécurité chez Checkpoint.

Source :
http://www.linformatique.org/whatsapp-jusqua-200-000-utilisateurs-touches-par-une-cyberattaque.html
Par Emilie Dubois