Alerte à partager : Une faille sur Android à corriger d’urgence | Le Net Expert Informatique

	Alerte à partager : Une faille sur Android à corriger d’urgence

Si votre fournisseur de smartphone ou de tablette ne patche pas Stagefright de lui même, ce malware basé sur l'envoi de MMS peut être vraiment effrayant. Mais vous pouvez vous en protéger en respectant quelques étapes.

Franchement, la plupart des gens qui reçoivent les logiciels malveillants recherchent les ennuis. Ils ouvrent un fichier suspect envoyé par une personne qu'ils ne connaissent pas, vont sur un site Internet mal famé, voire téléchargent le dernier film ou jeu à la mode sur BitTorrent. Mais Stagefright, c'est différent. Ce logiciel malveillant basée sur une faille de sécurité se déclenche en recevant un MMS sur un appareil Android non patchées. Et bang, vous êtes piraté.
Stagefright peut attaquer tout smartphone Android, tablette, ou un autre dispositif fonctionnant sous Android 2.2 ou supérieur. Des approximativement quelque 1 milliard de gadgets Android présents sur le marché, Stagefright pourrait, en théorie, toucher 95% d'entre eux. Joshua J. Drake, le vice-président de Zimperium zLabs qui a découvert Stagefright prétend qu'il est parmi les « pires vulnérabilités Android découvertes à ce jour ».
Car la partie vraiment sournoise est qu'il n'est pas nécessaire de consulter le MMS pour être infecté. Si vous utilisez l'application Hangouts de Google , vous êtes infectés sans même consulter cette application de messagerie si l'on vous fait parvenir ce message.

Un malware pas comme les autres
Tout ce que l'attaquant a besoin de faire est d'envoyer ce paquet empoisonné à votre numéro de téléphone. Il allume alors votre appareil, et l'attaque commence. Cela peut arriver si vite que le temps que votre téléphone vous avertisse qu'un message est arrivé, vous avez déjà été piraté. Si par ailleurs vous utilisez l'application native de messagerie proposée avec Android, vous devez ouvrir le MMS, mais pas nécessairement déclencher la vidéo, pour être infecté.
Ce détournement de la sécurité d'Android fonctionne en profitant de la bibliothèque Stagefright incluse dans Android. Ce moteur de lecture multimedia est fourni avec des codecs basés sur des logiciels pour lire plusieurs formats de médias populaires. La faille de sécurité semble provenir du fait que pour réduire la latence de l'affichage vidéo Stagefright traite automatiquement la vidéo avant même que vous ne vouliez la regarder. Joshua J. Drake va révéler les détails de du fonctionnement de Stagefright au Black Hat début Août.

Google a été réactif…
Zimperium à informé Google du problème en Avril. Selon Drake, « Google a agi promptement et appliqué les correctifs à des branches de code interne sous 48 heures ». Une porte-parole de Google mentionne dans une réponse par e-mail : « Nous avons déjà répondu rapidement (…) en envoyant le correctif pour tous les appareils Android à nos partenaires ».

Elle ajoute :
La sécurité est renforcée dans Android : les applications Android sont exécutées dans ce que nous appelons une « sandbox d'application ». De la même manière qu'un bac à sable empêche le sable de sortir, chaque application est installée dans une « sandbox » virtuelle pour l'empêcher d'accéder à autre chose qu'à ses propres composants, ce qui signifie que même si un utilisateur devait installer accidentellement un morceau de malware, il lui est interdit d'accéder à d'autres parties du dispositif.
L'ouverture de l'écosystème améliore la sécurité et rend Android plus puissant. Comme Android est open source, tout le monde peut l'examiner pour comprendre comment il fonctionne et d'identifier les risques potentiels de sécurité. Toute personne peut mener des recherches et faire des contributions pour améliorer la sécurité d'Android.
Google encourage la recherche en matière de sécurité : le programme de récompenses de sécurité Android, lancé en 2015, et le programme Google Patch Rewards, lancé en 2014, récompensent les contributions de chercheurs en sécurité qui investissent leur temps et leurs efforts à aider à rendre les applications plus sûres.
Alors, avec toutes ces précautions, pourquoi une telle agitation? Oui, il s'agit d'une faille de sécurité particulièrement vicieuse, mais le correctif est là… n'est ce pas ?

…mais pas les fabricants
Euh, et bien en fait Android a un autre problème de sécurité bien plus important. À l'exception des appareils Nexus, Google fournit les correctifs de code source, mais ce sont les fabricants de smartphones et les opérateurs qui doivent les faire parvenir aux utilisateurs qui mettent à jour le firmware. Et au 27 Juillet aucun des principaux acteurs de l'écosystème Android n'a annoncé de plan pour fournir le patch. Pour des appareils anciens, les patches pourraient ne jamais être livrés.

Zimperium affirme que le Blackphone de SilentCircle est protégé contre cette attaque depuis la version 1.1.7 de PrivatOS. Firefox de Mozilla a également inclus un correctif pour ce problème depuis la version 38. Et bien sûr Zimperium propose sa propre protection contre les attaques Stagefright avec sa plate-forme de défense de la menace mobile, zIPS.

Voici comment se débrouiller sans patch
Mais ce que Zimperium ne mentionne pas, c'est qu'Android a déjà une excellente façon de bloquer la plupart des attaques de Stagefrights : bloquer tous les messages texte provenant d'expéditeurs inconnus.

Pour paramétrer cela avec Android Kitkat, la version la plus populaire d'Android, ouvrez l'application 'Messenger' et appuyez sur le menu dans le coin supérieur droit de l'écran (les trois points verticaux), puis appuyez sur 'Paramètres'. Une fois là, sélectionnez Bloquer les expéditeurs inconnus, et c'est tout.

Sur Lollipop, où Hangouts est l'application de messagerie par défaut, il n'y a aucun moyen par défaut de bloquer les expéditeurs inconnus. Vous pouvez toutefois sous 'Paramètres' aller aux 'messages multimédia' et désactivez 'Récupérer automatiquement les messages multimédias'.

Avec Lollipop et d'autres versions d'Android, je recommande de vous tourner vers des applications de blocage de SMS tierces. Pour Android 2.3 à 4.3, j'apprécie 'Blocage des Appels et SMS'. Si vous utilisez KitKat ou les versions au dessus, où une seule application de SMS peut être active au même moment, j'apprécie Postman, alias TEXT BLOCKER. Ce programme fonctionne en conjonction avec votre application préférée de textos pour bloquer les expéditeurs inconnus.

Rien de tout cela n'est parfait. Un ami peut toujours être infecté et propager des programmes malveillants. Mais c'est un bon début. La solution de court terme adviendra quand les fabricants et les opérateurs se magneront enfin le train et pousseront le correctif vers leurs clients. Mais compte tenu de leur historique, je ne vais pas attendre et je vais bloquer les MMS. La solution à long terme arrivera quand les entreprises qui utilisent Android commenceront à travailler avec Google pour fournir des correctifs de sécurité le plus rapidement possible, et tout le temps.

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

Source : http://www.zdnet.fr/actualites/stagefright-a-quel-point-les-utilisateurs-d-android-doivent-ils-etre-inquiets-39823010.htm
Par Steven J. Vaughan-Nichols

Microsoft trop lent à corriger quatre failles zero-day dans Internet Explorer | Le Net Expert Informatique

Microsoft trop lent à corriger quatre failles zero-day dans Internet Explorer

Alerté en janvier par TippingPoint (HP) de l'existence de 4 vulnérabilités d'Internet Explorer, Microsoft avait plus de 6 mois pour les corriger. Le délai écoulé et faute de correctifs, des détails sur ces vulnérabilités ont été divulgués.

Microsoft se montre une nouvelle fois trop lent à corriger des vulnérabilités dans ses logiciels. C'est Internet Explorer, son navigateur, qui est à présent pointé du doigt par la Zero Day Initiative de TippingPoint, une filiale d'HP.
Les spécialistes des failles logicielles accordent six mois aux éditeurs pour corriger des vulnérabilités signalées avant de dévoiler publiquement leur existence. Et c'est ce qui vient de se produire pour quatre failles d'Internet Explorer.

Interaction avec la cible requise
Faute de correctifs une fois le délai écoulé, la ZDI a donc communiqué sur ces vulnérabilités zero-day du navigateur. Ces failles avaient été signalées en janvier 2015 à Microsoft qui n'a pas fourni de correctifs et avait demandé, et obtenu, une extension jusqu'au 19 juillet.
Les chercheurs en sécurité de TippingPoint précise que ces vulnérabilités permettent à un attaquant d'exécuter du code à distance sur les installations vulnérables d'Internet Explorer.
Pour s'exécuter, l'attaque nécessite cependant une interaction avec l'utilisateur au travers d'une visite sur une page (lien transmis dans un email ou par messagerie instantanée) ou l'ouverture d'un fichier malveillant.
Microsoft se trouve à présent confronté à l'obligation de corriger quatre failles critiques dans Internet Explorer. ZDI ne précise pas quelles sont les versions du navigateur affectées.

Source : http://www.zdnet.fr/actualites/zdi-microsoft-trop-lent-a-corriger-quatre-failles-zero-day-dans-internet-explorer-39822812.htm

Alerte partagez ! Deux nouvelles failles zero-day dans le plugin Flash d'Adobe | Programmez! | Le Net Expert Informatique

Alerte partagez ! Deux nouvelles failles zero-day dans le plugin Flash d'Adobe

Il y en a des choses intéressantes dans les 400 Go de données récemment dérobées à la société The Hacking Team et publiées sur Pastebin

The Hacking Team est une société qui vit du cyber espionnage, mais qui en l'occurrence contribue pour le moment et à l'insu de son plein gré à la sécurité informatique. En effet le code source de son logiciel espion phare, DaVinci, fait partie des 400 Go volés. Et ce code source est riche d'enseignements.
Ainsi, il est apparu en fin de semaine dernière que DaVinci exploitait une faille zero-day dans le plugin Flash d'Adobe. Faille qu'Adobe a d'ailleurs rapidement corrigée.
Mais ce n'est pas tout. Après cette faille CVE-2015-5119, deux autres failles zero-day ont été identifiées grâce à The Hacking Team CVE-2015-5122 et CVE-2015-512 respectivement. Des failles dans le plugin Flash, encore et toujours… FireEye et Trend Micro détaillent quelques informations techniques à propos de ces failles, sur les pages citées.
Dans les deux cas, les failles consistent en des corruptions mémoire, dont l'exploit rend possible l'exécution d'un code arbitraire sur la machine attaquée. Il s'agit donc de failles hautement critiques, qui pour l'instant ne sont pas corrigées. En attendant les correctifs, les experts en sécurité recommandent très vivement la désactivation du plugin Flash, en raison de la gravité de ces failles.
Lire la suite….

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

Source : http://www.programmez.com/actualites/hacking-hacking-team-deux-nouvelles-failles-zero-day-dans-le-plugin-flash-dadobe-23012

Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team | Le Net Expert Informatique

	Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team

Les cybercriminels s'en frottent déjà les mains entre deux piratages. Deux jours après la mise en ligne de données piratées de l'éditeur de logiciels espions Hacking Team, les experts, qui ont épluché les 400 Go de documents, ont fait la découverte d'une faille de sécurité importante de Flash Player, un lecteur multimédia autonome utilisé par des sites commes Youtube, Dailymotion ou encore Facebook.

C'est l'éditeur d'antivirus Micro Trend qui a révélé sur son blog cette faille «zero-day», c'est à dire inconnue jusqu'à présent et sans correctif pour l'instant. Elle permet à un attaquant de prendre le contrôle à distance d'un ordinateur en exécutant un code arbitraire à distance ou dans le cas plus précis d'une entreprise de surveillance comme Hacking Team d'installer ses logiciels espions sans se faire remarquer.
Symantec a confirmé cette porte d'entrée dans votre ordinateur et conseille sur son blog (en anglais) de désactiver temporairement Flash Player sur les sites Internet douteux surtout sur Internet Explorer, le navigateur le plus exposé.
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) a lui aussi confirmé la faille et ses potentielles conséquences. Le CERT-FR précise que des «plusieurs kits d'exploitation (de pirates informatiques, NDLR) ont intégré cette vulnérabilité qui est activement exploitée».
Prise à défaut, l'entreprise américaine Adobe, à l'origine de Flash Player, a promis d'apporter un patch correcteur dans la journée de mercredi. D'autres failles de sécurité pourraient être révélées sur la masse de documents qui ont fuité. Mais les plus dangereuses restent celles dont seul un groupe d'initiés est au courant.

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

Source : http://www.leparisien.fr/high-tech/flash-player-une-faille-de-vulnerabilite-revelee-par-le-piratage-de-hacking-team-08-07-2015-4928849.php
Par Damien Licata Caruso

Grosse menace sur les mots de passe contenus dans le trousseau d'Apple | Le Net Expert Informatique

Grosse menace sur les mots de passe contenus dans le trousseau d'Apple

Peu importe que vous utilisiez iOS ou OS X, vos mots de passe sont en danger s'ils sont stockés dans le trousseau d'Apple.

Des chercheurs universitaires ont découvert une énorme faille de sécurité chez Apple, une faille suffisamment importante pour que la marque à la pomme n'ait pas encore réussi à la corrigé alors qu'elle a été signalée au mois d'octobre dernier. Pour causse, elle touche le mécanisme censé protéger les mots de passe : le trousseau.
L'idée du trousseau est simple : centraliser les identifiants et mots de passe pour que l'utilisateur n'ait pas à les ressaisir. Le problème, c'est que des chercheurs universitaires ont découvert toute une série de failles de sécurité.
Alors que le bac à sable est censé isoler les données pour qu'elles soient protégées, les chercheurs sont parvenus à percer le mécanisme.
Ils ont aussi créé un malware capable d'afficher tous les mots de passe de l'Apple's Keychain, c'est-à-dire ceux stocker dans le trousseau, ce qui expose tous les identifiants utilisés par les applications tierces : Facebook, Twitter, iCloud, Gmail, etc.
« Nous sommes parvenus à pirater tout le service Keychain, où Apple stocke les mots de passe et les autres paramètres de ses applis ainsi que les sandbox containers' dans OS X », explique Luyi Xing, responsable de cette recherche. « Nous avons découvert de nouvelles faiblesses dans les mécanismes de communication entre applis au sein d'OS X et d'iOS, qui pourraient être exploitées pour dérober des données confidentielles d'Evernote, Facebook et d'autres applis largement utilisées. »
Pour l'heure, le problème est énoncé, mais aucune solution n'est pour le moment encore disponible, le problème subsiste dans les versions actuelles d'iOS et d'OS X.

Alerte partage ! Les antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse | Le Net Expert Informatique

Alerte partage ! Les antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse

Un chercheur du Project Zero de Google a dévoilé une vulnérabilité critique affectant plusieurs produits et logiciels proposés par l'éditeur de sécurité ESET. La vulnerabilité est exploitable à distance et permet l'exécution de code malveillant sur la machine visée.

Les solutions de sécurité, comme n'importe quel autre logiciel, sont également exposées à des failles de sécurité qui peuvent permettre à un attaquant d'exécuter du code sur la machine. C'est d'ailleurs probablement l'une des raisons ayant poussé la NSA et le GCHQ à orienter leurs efforts de reverse engineering sur les produits de Kaspersky et d'autres éditeurs antivirus, afin de transformer ces obstacles en porte d'entrée au système de la cible.
La faille décrite par le chercheur Tavis Ormandy, qui avait déjà décelé une vulnérabilité affectant les logiciels de Sophos en 2012, porte plus précisément sur le moteur d'émulation utilisé par les produits de la société ESET. Cet outil est utilisé par l'antivirus pour faire tourner les instructions exécutées par la machine dans un environnement isolé, afin de détecter du code potentiellement malveillant pour l'utilisateur.

Même la version Linux est touchée
Malheureusement, celui-ci présente une vulnérabilité permettant à l'attaquant d'exécuter du code en disposant d'un haut niveau de privilège. Outre cet aspect, l'attaque est envisageable via un certain nombre de vecteurs : web, messagerie, ou périphérique de stockage, tous étant susceptibles d'être scannés par les programmes d'ESET à la recherche de code malveillant. La faille affecte les logiciels même dans leur configuration par défaut.
La vulnérabilité affecte de nombreux logiciels proposés par ESET : NOD32 Antivirus pour Windows, Cyber Security Pro pour OS X, NOD32 pour Linux Desktop, Endpoint Security et NOD32 Business Edition.
Un correctif est également proposé par ESET depuis le 22 juin, afin de corriger la faille de sécurité repérée par le chercheur. Le blog post détaille notamment divers moyen d'exploiter la faille, ainsi que des mesures d'atténuations : ainsi, couper l'analyse temps réel des outils d'ESET pourrait réduire le risque, en désactivant l'analyse automatique dans les outils proposés par la société slovaque. Mais la meilleure solution reste évidemment de patcher. Et vite.

Source : http://www.zdnet.fr/actualites/les-antivirus-eset-victimes-d-une-faille-de-securite-39821472.htm
Par Louis Adam

Les gouvernements occidentaux sous le feu des cyberattaques | Le Net Expert Informatique

24

Mercredi 17 juin, Tony Clement, le président du Conseil du Trésor (l'équivalent du ministre du Budget), a confirmé une cyberattaque en cours contre des sites gouvernementaux. À savoir, celui du Sénat, du ministère des Travaux Publics, du ministère de l'Industrie ou encore du service aux citoyens.

Cette attaque a entraîné le blocage de ces sites pendant plusieurs heures. Contrairement à l'attaque du Bundestag, cette cyberattaque a été revendiquée par le mouvement des Anonymous, qualifié de « groupe terroriste » par plusieurs médias canadiens.
Les Anonymous souhaitent « protester contre une nouvelle loi antiterroriste qui accroît significativement les pouvoirs des services secrets canadiens, mais sans aucun garde-fou autonome », nous précise Le Monde.
La loi antiterroriste C-51, adoptée le 6 mai dernier, porterait atteinte aux droits et libertés des Canadiens en ne visant que « les groupes minoritaires et les dissidents ». Elle donnerait en outre beaucoup plus de pouvoir au Service canadien du renseignement de sécurité (SCRS).
« Troque-t-on notre vie privée au nom de la sécurité ? », se demande la vidéo YouTube diffusée sur les réseaux sociaux. Une question très actuelle et surtout applicable à moult pays en guerre contre le terrorisme.
Néanmoins, le compte Anon_GovernmentWatch a assuré sur Twitter que « ce n'était pas nous cette fois-ci ».
La multitude de comptes se revendiquant des Anonymous rend difficile toute prise de position officielle. Mais au vu des messages qui suivent, le doute est de mise.
En revanche, il s'amuse du terme de « cyberattaque » employé pour une attaque en DDoS et encore plus du qualificatif de « terroriste ».

Encore une fois, ces attaques, contrastées dans leurs moyens et leur finalité, montrent à quel point les gouvernements sont exposés et vulnérables face aux cyberattaques, révélant des failles béantes en matière de cyberdéfense alors même que ces administrations prônent une surveillance toujours plus accrue et rendue possible par un déploiement de moyens ultra sophistiqués. Tragiquement ironique.

« On est un peu les cancres en ce qui a trait à la cybersécurité. On est les derniers élèves dans le fond de la classe », se désole Rosane Dorée Lefebre, porte-parole adjointe en matière de sécurité publique du NPD dans les colonnes de Radio Canada.

Quoi qu'il en soit, la classe de remplie de plus en plus de cancres… et les pirates ou « services étrangers » en profitent allègrement. Russes ? Chinois ? Accusations avérées ou non, le pacte de non-agression 2.0 signé récemment entre la Chine et la Russie apparaît donc très opportun…

Source : http://www.journaldugeek.com/2015/06/18/gouvernements-occidentaux-sous-le-feu-des-cyberattaques/

Montres connectées : vos données personnelles sont peut-être en danger | Le Net Expert Informatiquedc

Montres connectées : vos données personnelles sont peut-être en danger

Des chercheurs en sécurité n'ont pas eu trop de mal à récupérer des données personnelles à partir des montres connectées LG G Watch et Samsung Gear 2 Neo.

Les révélations sur les possibilités d'intrusion et de récupération de données personnelles dans les téléphones portables par les agences de renseignement américaines dévoilées dans les documents d'Edward Snowden ont conduit les éditeurs de plates-formes mobiles à relever les niveaux de sécurité, notamment par le chiffrement systématique des données personnelles et documents dans les appareils mobiles.
Et pour les montres connectées, ces gadgets qui fleurissent (ou aimeraient le faire) sur les poignets ? Une publication de chercheurs de l'Université de New Haven suggèrent que si des hackers ont besoin d'information, ils feraient bien de commencer par cette porte d'entrée.
Il n'ont pas rencontré énormément de difficultés pour obtenir différentes informations personnelles, que ce soit avec la LG G Watch (agenda, contacts, adresses email, données du podomètre) sous Android Wear ou la Samsung Gear 2 Neo (messages, emails, contacts, données de santé) sous Tizen OS….d'autant plus que ces données n'étaient pas chiffrées.
Avec la multiplication des objets connectés qui seront autant de points d'entrée théoriques à différents types de données personnelles, cette petite expérience a de quoi faire réfléchir, alors que des objets comme les montres connectées ont justement besoin d'un large accès aux données personnelles pour être pleinement efficaces, comme dans le cas de Google Now sur Android Wear.
Chiffrer les données sur les montres connectées (et les objets connectés en général) serait une bonne chose, mais encore faut-il que ce soit fait correctement, préviennent les chercheurs. Un certain nombre de failles exploitées par les agences de renseignement (mais aussi les méchants hackers) sont justement des attaques de type man-in-the-middle qui outrepassent ces protections sans même avoir à les casser.
A voir si la montre Apple Watch, en cours d'analyse à l'Université de New Haven, saura mieux préserver la vie privée de son possesseur. Il vaudrait mieux, étant donné les volumes de plusieurs dizaines de millions d'unités qui son censés être écoulés dès cette année…

Source : http://www.generation-nt.com/lg-watch-samsung-gear-montre-protection-donnees-actualite-1915829.html

Les attaques informatiques s’achètent sur le blackmarket | Le Net Expert Informatique

	Les attaques informatiques s’achètent sur le blackmarket

De 75 dollars le million d'adresses e-mail à plusieurs milliers de dollars pour une faille zero day exploitable… G Data a plongé dans le « blackmarket » pour en ressortir les principaux tarifs du marché de la cybercriminalité.

G Data s'est penché sur le marché de la cybercriminalité pour en étudier fonctionnement et offres de contenus. Baptisé « blackmarket », cet environnement construit autour de sites spécialisés, de forums privés, de structures d'anonymisation (proxy, VPN anonymes, réseau Tor…), de messageries protégées, de serveurs bulletproof (peu regardants sur la nature des fichiers stockés), de moteurs de recherche spécialisés et autres places de marchés de produits illicites, permet d'accéder à des montagnes de données personnelles, des kits de piratages en tout genre et de services d'attaques à la demande.
Au bout de son plongeon dans le blackmarket, les experts du SecurityLabs de l'éditeur allemand spécialisé en solutions de sécurité en a ressorti quelques informations éclairantes sur la vitalité du marché de la cybercriminalité. Un marché dont les tarifs évoluent entre une poignée de dollars et plusieurs centaines. La vente de données personnelles illégalement collectées se situe dans la zone basse des tarifs et, surtout, se commercialisent en volumes. Ainsi les accès aux comptes e-mails (adresse, nom d'utilisateur et mot de passe) se négocient 5 dollars le lot de 10 000. Les seules adresses e-mails, celles que se font notamment dérober les opérateurs et qui seront essentiellement exploitées pour des campagnes de phishing, ne se revendent pas plus de 10 dollars par poignées de 100 000, autour de 75 dollars le million. Les profils numériques qualifiés sont, eux, d'autant plus rentables qu'ils se revendent à l'unité : autour de 50 dollars pour une carte bancaire valide de type Gold ou Premier, un compte bancaire ou Paypal; 70 dollars l'identité complète dite Fullz (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires).

Plusieurs milliers de dollars la faille zero day exploitable
Les cybercriminels financièrement plus ambitieux orienteront leurs activités vers la vente de produits et services. L'installation d'un Bot, bien utile pour prendre le contrôle d'un réseau de PC infectés, se négocie autour de 50 dollars les 1000 machines à la soldes des cyberattaquants. Lesquels pourront également exploiter ces Bots pour organiser des attaques par déni de service distribué (DDoS). Un service proposé entre 10 et 200 dollars l'heure d'attaque. Le tarif pour une campagne de spam, non traçable (via un service de diffusion hébergé sur un serveur bulletproof) tombe en revanche autour de 5 dollars les 20 000 envois.
La création et l'hébergement (sur un serveur piraté) d'une page web infectieuse dans le cadre d'une campagne d'hameçonnage (phishing) se facture entre 10 et 30 dollars. Mais on trouve également des outils d'attaques plus onéreux (car censés être plus efficaces). Par exemple, le kit d'exploitation Nuclear, qui exploite les bannières publicitaires Google Ads pour dérouter l'utilisateur vers un site infectieux, est disponible autour de 1500 dollars. La palme revient aux outils capables d'exploiter les failles zero day de Windows à raison de plusieurs milliers, voire plusieurs dizaines de milliers de dollars, selon G Data.

Source : http://www.silicon.fr/besoin-dune-attaque-ddos-comptez-entre-10-200-dollars-de-lheure-118545.html
Par Christophe Lagane

De graves failles dans les NAS Synology à corriger | Le Net Expert Informatique

De graves failles dans les NAS Synology à corriger

Le fabricant de NAS Synology a corrigé plusieurs vulnérabilités dans son OS maison DSM (DiskStation Manager) – et ses composants associés – qui anime ses appliances de stockage, dont l'une pouvait permettre à des attaquants de compromettre les données stockées.

En effet, la vulnérabilité la plus sérieuse concerne donc Synology Photo Station, une fonction du DSM, le système d'exploitation basé sur Linux. Photo Station permet aux utilisateurs de créer des albums photo en ligne et des blogs accessibles à distance via l'adresse IP publique du périphérique. Mais des chercheurs en sécurité de l'entreprise néerlandaise Securify ont découvert que Photo Station n'effaçait pas correctement les entrées utilisateur, laissant à des attaquants la possibilité d'injecter des commandes système qui pourraient être exécutées avec les privilèges du serveur web.
De plus, Photo Station n'est pas protégé contre le cross-site request forgery (CSRF), une technique qui permet à un site web de forcer le navigateur d'un visiteur à exécuter des actions malveillantes sur un site différent de celui sur lequel il se connecte. Donc, même si Photo Station n'est pas configuré pour être accessible depuis Internet, un attaquant pourrait inciter un utilisateur situé sur le même réseau que le périphérique NAS à visiter une page web malveillante qui utiliserait le CSRF pour exploiter la vulnérabilité par commande d'injection sur le réseau LAN local. « En tirant parti de cette faille, des attaquants pourraient compromettre le périphérique NAS, et toutes les données qui y sont stockées », ont expliqué les chercheurs dans un avis qui comprend également une preuve de concept de l'exploit.

Des ransomwares s'attaquent à Synology
La version 6.3-2945 de Photo Station livrée la semaine dernière par Synology corrige cette vulnérabilité. Mais les notes de version font simplement état « d'améliorations de sécurité » sans donner de détails. La nouvelle version corrige aussi deux vulnérabilités cross-site scripting (XSS) identifiées par les chercheurs de Securify. Celles-ci pourraient être exploitées pour tromper les utilisateurs de Photo Station en les incitant à cliquer sur une URL malveillante qui exécute un code voyou dans leurs navigateurs. En cas de succès de ces attaques, des pirates pourraient voler les jetons de session ou les identifiants de connexion des utilisateurs de Photo Station ou exécuter des actions arbitraires en usurpant leur identité.
La semaine dernière Synology a corrigé une vulnérabilité similaire dans l'interface de gestion de DiskStation Manager. Les utilisateurs sont invités à mettre DSM à jour en version 5.2-5565 Update 1. Dans le passé, les boitiers NAS de Synology ont déjà été la cible de pirates. Ainsi, pas plus tard que l'an dernier, des attaquants ont exploité une vulnérabilité pour infecter plusieurs boitiers avec un ransomware destiné à crypter les fichiers stockés. Auparavant, les pirates avaient réussi à s'introduire dans les boitiers NAS de Synology pour faire tourner des programmes qui généraient de la crypto-monnaie pour leur compte.

Source : http://www.lemondeinformatique.fr/actualites/lire-synology-corrige-de-graves-failles-dans-son-os-dsm-61277.html
Par Jean Elyan