Utilisateurs de Tor identifiés – Le FBI reste muet

Utilisateurs de Tor identifiés – Le FBI reste muet

Le FBI soppose à une demande de la justice qui exige de la police américaine quelle présente sa méthode lui ayant permis didentifier des utilisateurs d'un site pédopornographique, en les piratant.

Le FBI n'a absolument aucune envie de dévoiler la méthode secrète qu'il a employé pour pirater plus d'un millier de membres d'un site pédopornographique. Et cela, même si c'est la justice américaine qui lui demande.
C'est en effet ce qu'est en train de révéler le procès visant une personne accusée d'avoir fréquenté cet espace, dont l'accès ne pouvait se faire qu'à travers le réseau d'anonymisation TOR.
Dans cette affaire, les avocats du prévenu souhaitent connaître la technique utilisée par la police fédérale pour infecter les ordinateurs de ceux qui visitaient Playpen – le nom de ce site pédopornographique – lorsqu'il était encore en ligne.
Pour la défense, il s'agit de tenter de démontrer que le FBI a outrepassé ses prérogatives au cours de l'enquête, en débordant du cadre de son mandat.

Sceau FBI

L'approche du FBI dans l'affaire PlayPen fait polémique outre-Atlantique.
En février, le magistrat a donné suite à cette demande et exigé du FBI qu'il communique à la partie adverse tous les détails de sa méthode de piratage. Mais comme le pointe la BBC, le service de police est particulièrement hostile à cette demande. Un courrier a été adressé cette semaine au juge afin de l'inviter à reconsidérer sa position, estimant que la défense dispose déjà de suffisamment de pièces pour travailler.
En réalité, l'opposition du FBI vise avant tout à préserver l'intérêt de sa technique. En effet, il se pourrait qu'une communication des détails à la partie adverse affaiblisse l'efficacité de cette méthode. Si celle-ci devient publiquement connue, les failles qu'elle exploite seraient tôt ou tard colmatées par TOR, les navigateurs et les serveurs hébergeant des sites web. De même, les utilisateurs se montreraient aussi plus prudents.

LE FBI VEUT PRÉSERVER L'EFFICACITÉ DE SA MÉTHODE EN LA GARDANT SECRÈTE

C'est sans doute ce scénario que le FBI veut éviter, afin de pouvoir l'appliquer de nouveau à l'avenir si le besoin s'en fait sentir. Et si la position de la police fédérale se défend, celle de la défense, qui agit dans l'intérêt de son client, est tout aussi audible : le FBI a-t-il enfreint son mandat au nom de la loi ? Et la méthode employée est-elle vraiment fiable ? Une erreur au niveau de l'identification de l'internaute est toujours possible.
L'affaire Playpen remonte au tout début de l'année 2015, lorsque le FBI réussit à prendre le contrôle des serveurs du site pédopornographique. Plutôt que de le fermer immédiatement, ce qui a aussi provoqué son lot de critiques lorsque l'information a été révélée publiquement, la police opte pour une autre approche, celle du honeypot : le site est demeuré actif pendant près de deux semaines, en utilisant ses propres serveurs, de façon à voir qui se connecte sur Playpen.

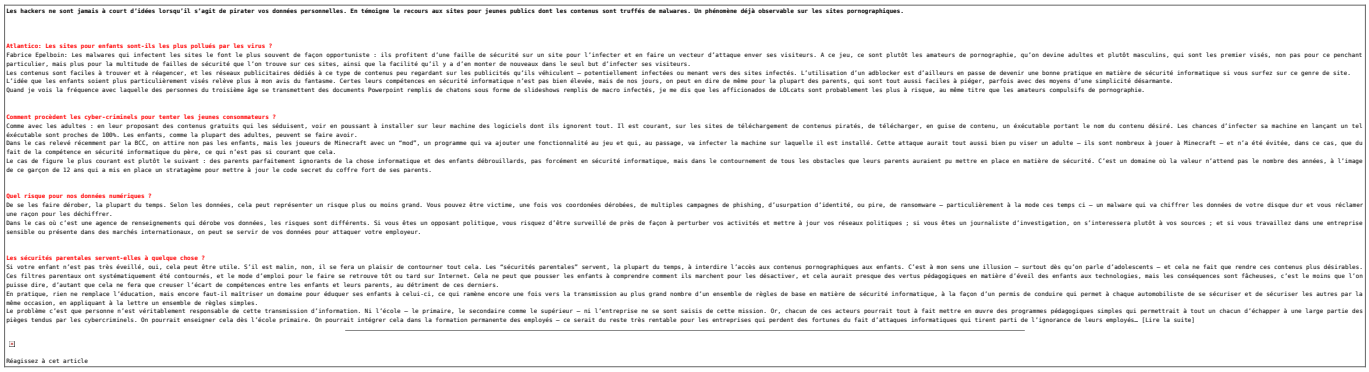
Le principe du réseau TOR rappelle celui des couches de l'oignon qui masquent le cœur de la plante.
C'est à ce moment-là que le FBI a utilisé sa fameuse technique pour contaminer le poste informatique des visiteurs, afin, notamment, de récupérer leur véritable adresse IP, qui est habituellement cachée avec le réseau d'anonymisation TOR, puisque la connexion passe par une succession de relais afin de camoufler la géolocalisation du PC d'origine.
Une fois l'adresse IP en main, il a suffit de contacter les fournisseurs d'accès à Internet – en tout cas ceux aux USA – pour avoir l'identité des internautes. Au total, la technique du FBI a permis de collecter pas moins de 1 300 adresses IP… [Lire la suite]

Réagissez à cet article

Source : *Le FBI refuse de dire comment il identifie des utilisateurs de Tor – Politique – Numerama*

Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?



Les hackers ne sont jamais à court d'idées lorsqu'il s'agit de pirater vos données personnelles. En témoigne le recours aux sites pour jeunes publics dont les contenus sont truffés de malwares. Un phénomène déjà observable sur les sites pornographiques.

Atlantico: Les sites pour enfants sont-ils les plus pollués par les virus ?

Fabrice Epelboin: Les malwares qui infectent les sites le font le plus souvent de façon opportuniste : ils profitent d'une faille de sécurité sur un site pour l'infecter et en faire un vecteur d'attaque enver ses visiteurs. A ce jeu, ce sont plutôt les amateurs de pornographie, qu'on devine adultes et plutôt masculins, qui sont les premier visés, non pas pour ce penchant particulier, mais plus pour la multitude de failles de sécurité que l'on trouve sur ces sites, ainsi que la facilité qu'il y a d'en monter de nouveaux dans le seul but d'infecter ses visiteurs.
Les contenus sont faciles à trouver et à réagencer, et les réseaux publicitaires dédiés à ce type de contenus peu regardant sur les publicités qu'ils véhiculent – potentiellement infectées ou menant vers des sites infectés. L'utilisation d'un adblocker est d'ailleurs en passe de devenir une bonne pratique en matière de sécurité informatique si vous surfez sur ce genre de site.
L'idée que les enfants soient plus particulièrement visés relève plus à mon avis du fantasme. Certes leurs compétences en sécurité informatique n'est pas bien élevée, mais de nos jours, on peut en dire de même pour la plupart des parents, qui sont tout aussi faciles à piéger, parfois avec des moyens d'une simplicité désarmante.
Quand je vois la fréquence avec laquelle des personnes du troisième âge se transmettent des documents Powerpoint remplis de chatons sous forme de slideshows remplis de macro infectés, je me dis que les afficionados de LOLcats sont probablement les plus à risque, au même titre que les amateurs compulsifs de pornographie.

Comment procèdent les cyber-criminels pour tenter les jeunes consommateurs ?

Comme avec les adultes : en leur proposant des contenus gratuits qui les séduisent, voir en poussant à installer sur leur machine des logiciels dont ils ignorent tout. Il est courant, sur les sites de téléchargement de contenus piratés, de télécharger, en guise de contenu, un éxécutable portant le nom du contenu désiré. Les chances d'infecter sa machine en lançant un tel éxécutable sont proches de 100%. Les enfants, comme la plupart des adultes, peuvent se faire avoir.
Dans le cas relevé récemment par la BCC, on attire non pas les enfants, mais les joueurs de Minecraft avec un "mod", un programme qui va ajouter une fonctionnalité au jeu et qui, au passage, va infecter la machine sur laquelle il est installé. Cette attaque aurait tout aussi bien pu viser un adulte – ils sont nombreux à jouer à Minecraft – et n'a été évitée, dans ce cas, que du fait de la compétence en sécurité informatique du père, ce qui n'est pas si courant que cela.
Le cas de figure le plus courant est plutôt le suivant : des parents parfaitement ignorants de la chose informatique et des enfants débrouillards, pas forcément en sécurité informatique, mais dans le contournement de tous les obstacles que leurs parents auraient pu mettre en place en matière de sécurité. C'est un domaine où la valeur n'attend pas le nombre des années, à l'image de ce garçon de 12 ans qui a mis en place un stratagème pour mettre à jour le code secret du coffre fort de ses parents.

Quel risque pour nos données numériques ?

De se les faire dérober, la plupart du temps. Selon les données, cela peut représenter un risque plus ou moins grand. Vous pouvez être victime, une fois vos coordonnées dérobées, de multiples campagnes de phishing, d'usurpation d'identité, ou pire, de ransomware – particulièrement à la mode ces temps ci – un malware qui va chiffrer les données de votre disque dur et vous réclamer une rançon pour les déchiffrer.
Dans le cas où c'est une agence de renseignements qui dérobe vos données, les risques sont différents. Si vous êtes un opposant politique, vous risquez d'être surveillé de près de façon à perturber vos activités et mettre à jour vos réseaux politiques ; si vous êtes un journaliste d'investigation, on s'interessera plutôt à vos sources ; et si vous travaillez dans une entreprise sensible ou présente dans des marchés internationaux, on peut se servir de vos données pour attaquer votre employeur.

Les sécurités parentales servent-elles à quelque chose ?

Si votre enfant n'est pas très éveillé, oui, cela peut être utile. S'il est malin, non, il se fera un plaisir de contourner tout cela. Les "sécurités parentales" servent, la plupart du temps, à interdire l'accès aux contenus pornographiques aux enfants. C'est à mon sens une illusion – surtout dès qu'on parle d'adolescents – et cela ne fait que rendre ces contenus plus désirables. Ces filtres parentaux ont systématiquement été contournés, et le mode d'emploi pour le faire se retrouve tôt ou tard sur Internet. Cela ne peut que pousser les enfants à comprendre comment ils marchent pour les désactiver, et cela aurait presque des vertus pédagogiques en matière d'éveil des enfants aux technologies, mais les conséquences sont fâcheuses, c'est le moins que l'on puisse dire, d'autant que cela ne fera que creuser l'écart de compétences entre les enfants et leurs parents, au détriment de ces derniers.
En pratique, rien ne remplace l'éducation, mais encore faut-il maîtriser un domaine pour éduquer ses enfants à celui-ci, ce qui ramène encore une fois vers la transmission au plus grand nombre d'un ensemble de règles de base en matière de sécurité informatique, à la façon d'un permis de conduire qui permet à chaque automobiliste de se sécuriser et de sécuriser les autres par la même occasion, en appliquant à la lettre un ensemble de règles simples.
Le problème c'est que personne n'est véritablement responsable de cette transmission d'information. Ni l'école – le primaire, le secondaire comme le supérieur – ni l'entreprise ne se sont saisis de cette mission. Or, chacun de ces acteurs pourrait tout à fait mettre en œuvre des programmes pédagogiques simples qui permettrait à tout un chacun d'échapper à une large partie des pièges tendus par les cybercriminels. On pourrait enseigner cela dès l'école primaire. On pourrait intégrer cela dans la formation permanente des employés – ce serait du reste très rentable pour les entreprises qui perdent des fortunes du fait d'attaques informatiques qui tirent parti de l'ignorance de leurs employés… [Lire la suite]

Réagissez à cet article

Fabrice Epelboin est enseignant à Sciences Po et cofondateur de Yogosha, une startup à la croisée de la sécurité informatique et de l'économie collaborative.

Source : *Quand les sites pour enfants se transforment en pièges pour voler les données personnelles de leurs parents | Atlantico.fr*

Mise à jour urgente Java. Patch d'une vulnérabilité critique de 2013

Mise à jour urgente Java. Patch d'une vulnérabilité critique de 2013

Oracle vient de livrer un correctif de sécurité pour combler une faille critique dans Java remontant à 2013. Cette dernière avait été découverte seulement en début d'année.

Oracle a publié une mise à jour de sécurité **urgente** pour corriger une vulnérabilité critique dans Java permettant à des attaquants de compromettre les ordinateurs d'internautes se rendant sur des sites web spécialement conçus pour les piéger. L'identifiant de cette vulnérabilité est CVE-2016-0636, suggérant qu'il s'agit d'une nouvelle mais cela n'est pas vraiment le cas. Dans un mail, la société de sécurité polonaise Security Explorations a confirmé que cette mise à jour patche une faille originellement rapportée à Oracle en 2013.
En début de mois, cette même société avait indiqué qu'un correctif publié par Oracle en octobre 2013 pour une vulnérabilité critique, portant l'identifiant CVE-2013-5838, s'était révélé inefficace et pouvait être contourné en changeant seulement 4 caractères de l'exploit original. Cela signifie que la vulnérabilité était toujours exploitable dans les dernières versions de Java. Or, dans son dernier bulletin, Oracle n'a fait aucune mention à l'ancienne faille trouvée par Security Explorations. Etrange renvoi d'ascenseur, non ?

L'update 77 pour Java SE 8 indispensable

Oracle recommande d'installer dès que possible cette nouvelle mise à jour Java, compte-tenu du degré de sévérité de la vulnérabilité et des détails techniques de contournement désormais rendus publics. Les utilisateurs de Java SE 8 sont prévenus d'installer l'update 77 (8u77), sachant que pour les possesseurs de Java 6 et 7, la mise à jour n'est proposée qu'en cas de support long terme, ces versions n'étant plus supportées … [Lire la suite]

Réagissez à cet article

Source : *Une vulnérabilité critique de 2013 patchée dans Java – Le Monde Informatique*

Daech prend le contrôle d'une centrale nucléaire – Futuriste ?

	**Daech prend le contrôle d'une centrale nucléaire. Futuriste ?**

Le coordinateur de l'UE pour la lutte contre le terrorisme estime que les djihadistes seront bientôt capables de cyberattaques contre des sites sensibles.

La prise de contrôle d'une centrale nucléaire par des mouvements djihadistes pourrait devenir une réalité « avant cinq ans », a admis samedi le coordinateur de l'Union européenne pour la lutte contre le terrorisme alors que la sécurité des sites nucléaires belges est pointée du doigt.
« Je ne serais pas étonné qu'avant cinq ans il y ait des tentatives d'utiliser l'Internet pour commettre des attentats », notamment en prenant le contrôle du « centre de gestion d'une centrale nucléaire, d'un centre de contrôle aérien ou l'aiguillage des chemins de fer », estime Gilles de Kerchove dans une interview au quotidien La Libre Belgique.
« À un moment donné, il y aura bien un gars » au sein de l'organisation djihadiste État islamique « avec un doctorat en technologie de l'information qui sera capable d'entrer dans un système », a-t-il estimé.

La miniaturisation des explosifs mais également la connaissance accrue des combattants de l'État islamique dans les biotechnologies constituent de réelles menaces pour l'avenir, selon lui. « Que se passera-t-il quand on en sera à comment élaborer un virus dans la cuisine de sa mère ? » s'est-il demandé.
En revanche, M. de Kerchove a estimé que le département belge de la Défense était « assez bon » en matière de cybersécurité. « Ils n'ont, bien sûr, pas les capacités de représailles des Français, des Anglais ou des Américains, mais en cas d'attaque, je pense que notre département de la Défense est assez bon », a-t-il dit, précisant cependant qu'il ne savait pas « si le gouvernement » belge était « capable d'anticiper et de résoudre de grosses attaques ».

Sécurité renforcée
Des médias belges et internationaux ont rapporté vendredi que la cellule terroriste bruxelloise responsable des attentats de mardi avait prévu une attaque à l'arme de guerre dans les rues de Bruxelles, type 13 novembre à Paris, et la fabrication d'une « bombe sale » radioactive après une surveillance vidéo par deux des kamikazes, les frères El Bakraoui, d'un « expert nucléaire » belge.
À la suite des attaques survenues mardi à Bruxelles qui ont fait 31 morts, la sécurité avait été renforcée autour des deux centrales nucléaires de Belgique.
C'est dans ce contexte de suspicion sur la sécurité des sites nucléaires qu'un agent de sécurité dans le nucléaire a été abattu et son badge volé jeudi soir dans la région de Charleroi, dans le sud de la Belgique, selon le journal La Dernière Heure. Samedi, la piste terroriste a été écartée, par la justice belge. La piste terroriste est formellement démentie, rapporte l'agence de presse Belga, citant le parquet de Charleroi, dans le sud du pays. Le juge d'instruction spécialisé dans les matières terroristes n'a pas été saisi. Les raisons de la mort de la victime, abattue, tout comme son chien, de plusieurs balles à son domicile, ne sont pas encore connues mais les enquêteurs pensent à un cambriolage qui aurait mal tourné ou à un crime pour des raisons privées.
Le parquet de Charleroi a démenti le vol de son badge d'accès de centrale nucléaire… [Lire la suite]

-

Réagissez à cet article

Source : *Quand Daech prendra le contrôle d'une centrale nucléaire – Le Point*

Des chercheurs trouvent une faille dans le chiffrement d’Apple

	Des chercheurs trouvent une faille dans le chiffrement d’Apple

Des chercheurs de l'université Johns Hopkins révèlent une faille dans le chiffrement de l'application iMessage. Celle-là pourrait permettre à des pirates d'accéder aux photos et vidéos envoyées.

Issu du *Washington Post*, l'article aurait été retiré juste après sa publication ce matin, selon certains blogueurs qui réussissent néanmoins à retrouver sur Google des bribes de l'article. De nouveau visible sur le site du journal, la nouvelle pourrait faire grand bruit. Car ce matin des universitaires américains prétendent avoir décelé une faille dans le chiffrement d'iMessage, l'application de messagerie instantanée d'Apple.

La compagnie vante justement sa capacité de chiffrement « de bout en bout », qui chiffre le message au moment même de son envoi, et garantit normalement qu'aucun tiers (y compris Apple) ne puisse obtenir la clé de déchiffrement du message. Pourtant le chercheur Matthew D. Green qui a dirigé l'équipe universitaire affirme qu'une faille permettrait d'intercepter les images et vidéos. « *Cela n'aurait en rien aidé le FBI à débloquer l'iPhone du tueur de San Bernardino* », affirme-t-il, « *mais cela démontre que la notion selon laquelle ce type d'application serait infaillible est erronée.* »

Selon Green, il était insensé de demander à une société comme Apple de créer des versions modifiées de leurs produits, puisque des failles peuvent d'ores et déjà être trouvées : « *Même Apple, qui compte dans ses rangs les meilleurs cryptographes du monde, ne sont pas en mesure de créer un chiffrement 100% fiable. C'est bien ce qui me rend inquiet quand j'entends qu'en plus on parle de créer des failles volontaires dans leurs produits alors que nous ne sommes déjà pas capables de créer des sécurités imparables.* »

Le professeur Matthew D. Green, de l'université Johns Hopkins

Pour intercepter le fichier, les étudiants auraient conçu un logiciel qui imite les serveurs d'Apple. La communication qu'ils ont attaquée par la suite contenait selon eux un lien vers une photo stockée sur l'iCloud d'Apple, ainsi que sa clé de déchiffrement de 64 bits.

Matthew D. Green et son équipe ont fait savoir qu'ils publieront les détails de leur attaque dès qu'Apple aura trouvé un remède à la faille découverte. Ils affirment aussi que des attaques similaires sont régulièrement pratiquées par les services de renseignement américains… [Lire la suite]

Réagissez à cet article

Source : *Des chercheurs trouvent une faille dans le chiffrement d'Apple*

Alerte : Faille Java à corriger d'urgence. Oui encore…

Alerte : Faille Java à corriger d'urgence. Oui encore…

Oracle a publié un patch en urgence pour son logiciel Java. Celui-ci corrige une faille critique dans Java permettant d'exécuter du code à distance sur une machine vulnérable.Dans une alerte de sécurité, Oracle confirme que la faille (CVE-2016-0636) est sévère avec une note de 9.3 sur une échelle qui grimpe jusqu'à 10 (Common Vulnerability Scoring System)… [Lire la suite]

Réagissez à cet article

Source : *Oracle corrige en urgence Java. Oui encore… – ZDNet*

Des millions de smartphones Android touchés par une faille critique

Des millions de smartphones Android touchés par une faille critique

Une faille figurant dans un nombre considérable de smartphones Android permet à des applications d'accéder au contrôle total du système d'exploitation.

La sécurité du système d'exploitation Android est une source régulière d'inquiétude et mobilise constamment l'attention des spécialistes, qui scrutent sans relâche l'OS open source porté par Google afin d'y déceler des vulnérabilités.
Si celles-ci ne manquent pas – les récents correctifs publiés par la firme de Mountain View sont là pour le prouver –, elles sont néanmoins corrigées avec une relative célérité. Toutefois, une faille repérée depuis un certain temps est parvenue à passer entre les mailles du filet. Et pour ne rien arranger, celle-ci s'avère très sérieuse.

TOUTE LA GAMME NEXUS EST CONCERNÉE

Depuis 2014, une vulnérabilité permettait à une application d'accéder aux privilèges root sur un grand nombre de téléphones Android, dont toute la gamme Nexus. Sur un téléphone rooté, il est possible d'accéder au contrôle total du système d'exploitation et ainsi effectuer des actions normalement bloquées par le constructeur pour des raisons de sécurité.
En l'occurrence, avec cette brèche, une application pouvait accéder à des fonctionnalités bloquées de l'OS et installer du code malveillant. « Une vulnérabilité du noyau qui permet l'élévation des privilèges pourrait permettre à une application nuisible d'exécuter du code arbitraire [sans l'accord du propriétaire, nlr] dans le noyau », explique Google.
Les noyaux Linux 3.4, 3.10 et 3.14 sont touchés, mais ceux plus récents (à partir de 3.18) sont hors de danger.
Cette faille a été identifiée depuis février 2015 sous la référence CVE-2015-180 et un patch est en préparation depuis le mois dernier, après la notification envoyée à Google par la CORE Team, un regroupement d'experts en sécurité informatique. En mars, Zimperium, une startup également spécialisée dans ce domaine, a notifié Google de la présence d'une application profitant de cette faille sur le Google Play.

Dans son bulletin de sécurité, Google explique que l'application en question a été retirée du Google Play. « Les clients qui installent une application qui cherche à exploiter cette faille prennent des risques.
Les applications de root sont interdites sur le Google Play et nous allons bloquer l'installation de cette application en dehors du Google Play grâce à la vérification d'applications », tranche l'entreprise.
Cela étant dit, un utilisateur qui aurait désactivé la vérification d'application peut toujours installer manuellement une application profitant de l'exploit sur son appareil via le fichier APK ou sur un magasin d'application alternatif.
Pour corriger ce problème, Google va déployer un patch sur l'ensemble de la gamme Nexus dans les prochains jours. Celui-ci a été transmis aux différents constructeurs, mais à cause de la fragmentation d'Android, il pourrait se passer plusieurs semaines, voire mois, avant que les fabricants n'appliquent le correctif sur leurs appareils… [Lire la suite]

Réagissez à cet article

Source : *Une faille de sécurité critique touche des millions de smartphones Android – Tech – Numerama*

Toutes les versions de Windows touchées par une faille critique

Toutes les versions de Windows touchées par une faille critique

Toutes les versions de Windows, dont Windows 10, sont affectées par une faille critique pour laquelle un correctif est disponible. La vulnérabilité permet d'exécuter arbitrairement du code.

Le dernier Patch Tuesday de Microsoft est léger en correctifs critiques, mais une faille majeure cependant affecte l'ensemble des versions supportées de Windows.

Dans son bulletin de sécurité mensuel, Microsoft informe les utilisateurs de la nécessité de patcher immédiatement une vulnérabilité sérieuse au niveau de la façon dont le système d'exploitation gère certains fichiers. Toutes les versions de Windows sous support sont concernées, de Windows Vista à Windows 10.

La faille (MS16-013) pourrait permettre à un attaquant d'exécuter arbitrairement du code comme l'utilisateur authentifié sur la session Windows. Les risques sont donc accrus pour les utilisateurs avec un compte doté des droits administrateur.

Autres vulnérabilités dans Office, IE et Edge

Pour réaliser l'attaque, le pirate doit amener l'utilisateur à ouvrir un fichier Journal spécialement forgé. Il pourra ainsi exécuter des programmes, supprimer des données et même créer de nouveaux comptes avec tous les droits sur le poste Windows.

Windows Server 2016 Tech Preview 4 est également affecté par la vulnérabilité et le correctif doit donc aussi être déployé sur ces configurations. Microsoft précise toutefois n'avoir à ce jour détecté aucune exploitation de cette faille Windows.

A noter que l'éditeur a publié trois autres correctifs pour des vulnérabilités critiques de Windows et Office.

MS16-012 corrige une faille permettant à un attaquant d'exécuter du code en exploitant un fichier PDF compromis. Les utilisateurs de Windows 8.1 et Windows 10 sont principalement touchés. Le problème de sécurité a été signalé à l'éditeur par un tiers et ne ferait pas l'objet d'attaques.

MS16-015 remédie à plusieurs failles de corruption mémoire dans Microsoft Office. Elles autorisent des attaques par le biais de fichiers Office malveillants. Leur exploitation permet d'obtenir des droits équivalents à ceux de l'utilisateur de la session ouverte.

MS16-022 corrige enfin de nombreuses vulnérabilités d'Adobe Flash Player dans Windows 8.1 et versions suivantes de l'OS Microsoft.

L'éditeur diffuse par ailleurs un patch cumulatif pour Internet Explorer (MS16-009) et le nouveau navigateur de Windows 10, Microsoft Edge (MS16-011). Les différentes failles ne feraient l'objet d'aucune exploitation avant la diffusion des correctifs, toujours selon la firme de Redmond… [Lire la suite]

Réagissez à cet article

Source : *Toutes les versions de Windows touchées par une faille critique*

---

20 vulnérabilités critiques corrigées dans Magento

20 vulnérabilités critiques corrigées dans Magento

Magento, fournisseur de solutions e-commerce open source, a patché plusieurs vulnérabilités présentant un risque d'attaques dont certaines de type XSS. Plusieurs éditions des versions communautaire et entreprise sont concernées.

Les administrateurs de sites e-commerce sous Magento ont tout intérêt à faire preuve de grande vigilance. L'éditeur vient en effet de lancer plusieurs correctifs pour combler des vulnérabilités critiques dans plusieurs versions de ses produits. Parmi les failles recensées, l'une permet d'injecter du code Javascript dans un champ de mail pour mener des attaques de type cross-site scripting (XSS). Considérée par Magento comme critique, cette vulnérabilité permet de pirater le compte administrateur de la session. Elle affecte l'édition communautaire de Magento (antérieure à la v1.9.2.3), ainsi que l'édition entreprise (antérieure à la v1.14.2.3) de la solution e-commerce open source.

La salve de correctifs permet également de combler 19 autres failles (relatives notamment aux formulaires de commandes, headers des adresses IP client, téléchargement de fichiers, deni de service newsletter, contournement de captcha…) dont certaines concernent également les v2.x des versions communautaire et entreprise de Magento. Il s'agit des premières vulnérabilités de taille que Magento a rencontrées cette année. En 2015, l'éditeur avait dû faire face à plusieurs problèmes dont une vulnérabilité critique exploitée ayant affecté un grand nombre de sites e-commerce.

Réagissez à cet article

Un phishing et Lastpass s’en est allé

Un phishing et Lastpass s’en est allé

Lors de la conférence Shmoocon, un chercheur a présenté une attaque de phishing particulièrement convaincante visant les services du gestionnaire de mot de passe Lastpass. En réaction, les mesures de sécurité ont été rehaussées par l'éditeur du service.

Le phishing n'est pas toujours un problème situé entre le clavier et la chaise. C'est en tout cas la thèse défendue par le chercheur Sean Cassidy, qui a présenté ce week-end lors de la conférence Shmoocon une attaque de cette catégorie particulièrement convaincante et capable de tromper les utilisateurs les plus aguerris du gestionnaire de mot de passe Lastpass.

L'attaque, baptisée « Lostpass » exploite plusieurs vulnérabilités présentes sur le service de gestion des mots de passe : il s'agit tout d'abord pour l'attaquant d'attirer l'utilisateur sur un site malicieux, puis d'afficher une notification indiquant à l'utilisateur que celui-ci a été déconnecté de Lastpass. Une fois celle-ci affichée, l'utilisateur est ensuite redirigé vers une page de login quasi identique à celle affichée par Lastpass en cas de déconnexion. L'attaquant peut exploiter un bug notamment présent dans Chromium afin de disposer d'un nom de domaine quasi similaire à celui utilisé pour les extensions chrome du même type que celles utilisées par Lastpass.

L'attaquant peut ensuite exploiter l'API ouverte de Lastpass pour vérifier si les identifiants entrés par l'utilisateur sont valides et pour savoir si celui-ci a activé un système d'identification à double facteur : si tel est le cas, l'attaquant peut également présenter une invite copiée sur celle proposée par le service de gestion de mot de passe et qui lui permet de récupérer par la même occasion le token généré par la double authentification. Une fois les identifiants récupérés, l'attaquant peut accéder au reste des mots de passe stockés par l'utilisateur, ou modifier les paramètres de sécurité du compte afin de faciliter d'éventuelles futures attaques.

Un problème entre la chaise et le clavier ?

Les équipes de Lastpass ont été mises au courant de ce scénario d'attaque au cours de l'été 2015 et ont depuis mis en place plusieurs mesures afin de protéger les utilisateurs. La société a ainsi mis en place un système de vérification par mail lorsque l'utilisateur se connecte depuis un appareil inconnu, ce qui permet selon Lastpass de réduire considérablement les attaques de ce type.

La société précise également revoir le fonctionnement de son extension :
celle-ci s'appuie en effet sur des notifications Viewport pour informer ses utilisateurs, une technique facile à imiter pour un attaquant qui souhaiterait tromper un utilisateur. Un comportement que Lastpass entend corriger afin de réduire un peu plus le risque de confusion entre véritables notifications et notifications malicieuses émanant du site visité.
Pour Sean Cassidy, le problème souligné par ce scénario est tout aussi critique qu'une vulnérabilité classique, mais celui-ci regrette que les attaques de type phishing soient trop souvent reléguées au simple rang des problèmes liés à l'utilisateur. Dans sa démonstration en effet, la différence entre les pages légitimes et les pages malicieuses utilisées par un attaquant est minime. Seule une infime différence de trois caractères dans une url et quelques différences typographiques séparent ici le vrai du faux, ce qui rend l'attaque bien plus inquiétante.

Réagissez à cet article

Source : *Lastpass : un phishing presque parfait*