500 000 PC infectés à cause d’une faille Windows XP

500 000 PC infectés à cause d’une faille Windows XP

Selon les chercheurs en sécurité de Proofpoint, 52% des PC infectés par le botnet Qbot font tourner Windows XP. Exploitant une faille de Windows XP mais également de Seven et Vista, un groupe de cybercriminels russe a réussi à activer le botnet Qbot fort 500 000 PC zombies, essentiellement localisés aux Etats-Unis. Son objectif : Aspirer les identifiants bancaires des utilisateurs de ces PC corrompus.

Des pirates russes à l’origine du botnet Qbot ont construit une impressionnante armée de 500 000 PC zombies en exploitant des failles non corrigées dans des ordinateurs tournant sous Windows XP mais également Windows 7 et Vista. Des PC localisés principalement aux Etats-Unis, a fait savoir la société Proofpoint. Ces derniers temps, les hackers russes ont fait monter la pression avec des incursions sérieuses telle que l’attaque qui a visé la banque américaine JPMorgan Chase. Avec ce botnet, baptisé Qbot, les chercheurs de Proofpoint ont fait ressortir que le groupe qui est à l’origine de sa création l’a élaboré de façon méticuleuse à travers le temps, sans faire de vague, au point de rester sous les radars des sociétés de sécurité et donc de ne pas avoir attiré leur attention.

Selon Proofpoint, 75% des 500 000 PC infectés par le botnet Qbot sont situés aux Etats-Unis, sachant que parmi eux, 52% font tourner Windows XP, 39% Windows 7 et 7% Windows Vista. En Grande-Bretagne, la proportion de PC infectés est bien moindre, 15 000 postes environ. « Avec 500 000 clients infectés volant les identifiants des comptes bancaires en ligne des utilisateurs, le groupe de cybercriminels a le potentiel pour réaliser des bénéfices vertigineux », ont indiqué les chercheurs de la société de conseil en sécurité. Mais le botnet Qbot ne s’attaque pas seulement aux comptes bancaires, il compromet également les sites WordPress, soit en infectant le site lui-même ou bien en injectant des contenus corrompus dans leurs newsletters.
Article de Dominique Filippone

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemondeinformatique.fr/actualites/lire-500-000-pc-infectes-a-cause-d-une-faille-windows-xp-58878.html

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Selon la firme russe Dr.Web un malware visant spécifiquement les possesseurs de Mac serait actuellement actif, affectant plus de 17.000 machines à travers le monde. Pas une première, mais ce malware possède quelques spécificités amusantes.

Pas la peine de se mentir, les produits Apple eux aussi sont parfois victimes de malwares. En 2011, le Trojan Flashback avait ainsi infecté des centaines de milliers d'ordinateurs Apple. Le malware détecté par Dr Web est en revanche bien moins diffusé : 17.000 utilisateurs seulement seraient infectés.
Ce malware se range sous la catégorie des Botnets, infectant l'ordinateur de l'utilisateur afin de permettre à l'attaquant de l'exploiter pour d'autres fonctions à l'insu de son utilisateur. Le malware a été baptisé, un peu rapidement, iWorm par Doctor Web, bien que le mode exact de propagation du virus reste encore peu clair.
La particularité qui a retenu l'attention des chercheurs, c'est la façon dont les ordinateurs infectés récupèrent les adresses IP des serveurs de command&control. Les machines du botnet vont ainsi chercher sur Reddit les adresses de leurs centre de command&control : celles-ci sont postées à intervalles régulier dans la section commentaire d'un sujet destiné à recenser des serveurs Minecraft via un compte tenu par les individus responsables de la propagation du malware.

Reddit est innocent !
Reddit n'a rien à se reprocher, le site n'a pas été altéré ou son utilisation n'a pas été techniquement détournée, mais cette approche originale mérite d'être notée. Comme le relève le chercheur Graham Cluley, même en supprimant le compte utilisé pour router vers ces adresses IP, cela n'empêcherait pas les pirates de recréer un compte et de continuer leur activité.
Comme souvent néanmoins, il convient de rester prudent avec les alertes lancées par les firmes spécialisées dans la vente d'antivirus. Dr.Web annonce ainsi 17.000 ordinateurs infectés à travers le monde, mais ne précise pas du tout quel mode de diffusion a été choisi pour propager le malware. Selon des sources anonymes, le principal mode d'infection se ferait via le téléchargement de logiciels Adobe et Microsoft piratés sur les plateformes de partage en P2P.
De la même manière, peu d'informations sont disponibles pour ceux qui souhaitent se prémunir de ce malware, si ce n'est la solution vendue par Dr.Web… Mais selon MacRumors, l'outil de protection maison proposé par Apple à ses clients Xprotect, a été mis à jour pour détecter et empêcher la propagation de cette menace.
Attention Livo !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/un-nouveau-malware-vise-les-mac-17000-machines-affectees-39807339.htm
Par Louis Adam | Lundi 06 Octobre 2014

Attaque informatique contre les fournisseurs d'énergie – Dragonfly lance la cyberguerre froide…

Attaque informatique contre les fournisseurs d'énergie – Dragonfly lance la cyberguerre froide…
Le scénario du pire. Ou presque. Un groupe de hackers, baptisé Dragonfly, est parvenu à corrompre certains systèmes de contrôle des opérateurs d'énergie. Notamment en France. Les pirates avaient alors la possibilité de saboter la distribution d'énergie de certains pays.

Les clients de 12 banques suisses attaqués par des cybercriminels

Les clients de 12 banques suisses attaqués par des cybercriminels

Des pirates informatiques se sont lancés, depuis peu, dans une attaque d'envergure contre les comptes e-banking de douze banques suisses. Leurs méthodes sont perfides et laissent peu de traces, avertit Switch.

Le virus, de type cheval de Troie, a été nommé Retefe, a indiqué mardi Serge Droz, expert en sécurité auprès de l'organisme qui administre les noms de domaines en Suisse. Il confirmait une information parue sur le site Internet de la Handelszeitung. C'est l'entreprise de sécurité informatique Trend Mikro qui a rendu publique l'information sur l'attaque.

Le client de banque ouvre un spam – un courrier électronique indésirable – qui libère le virus. Le programme malicieux s'efface, une fois que l'infection a réussi. Aussitôt que le client ouvre une session e-banking, il est redirigé sur un mauvais serveur, sur lequel apparaît une copie de page Internet de sa banque. Le client entre alors ses informations de sécurité, qui sont désormais en main des malfaiteurs.

Lire la suite…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.lematin.ch/economie/hackers-s-attaquent-clients-12-banques-suisses/story/16520131

Alerte vigilance Simplocker – L’ère des malwares 2.0 sur les mobiles a sonné : Simplocker un cryptolocker sur Android

Alerte vigilance – Simplocker un cryptolocker sur Android

Les experts savaient depuis un moment que les cybercriminels tenteraient de s’attaquer à la flotte mobile, une cible très en vogue dans un monde où le nombre d’utilisateurs frôle les 7 milliards en 2014

Alerte HeartBleed Acte II – Nom de code Cupid

Alerte HeartBleed Acte II – Nom de code Cupid
Cupid, nouvel exploit qui utilise la Heartbleed, ébranle les connexions Wi-Fi.

Pour l’instant, à l’état de preuve de concept, cette faille n’est sans doute que le premier écho du coup de tonnerre qui a fait trembler le Net en avril dernier.

Une victime du virus Windigo témoigne

Le 19 mars dernier, je vous informais au travers d'un article (http://www.lenetexpert.fr/alerte-virus-windigo) de la découverte du virus Windigo par une équipe de spécialistes en sécurité.

Quelques semaines après les premières attaques, le gérant d'une entreprise internationale touché par ce virus témoigne sur les dégâts qu'il a subit.

Alerte VIRUS « Windigo »

	**Alerte Virus « Windigo »** sur des serveurs Internet

Après des mois d'enquête, les experts en sécurité d'ESET viennent de découvrir **une vaste campagne d'attaques cybercriminelles touchant 25 000 serveurs UNIX**, infectant plus de 500 000 ordinateurs chaque jour et ayant généré plus de**35 millions de spams**.

Surnommée « **Windigo** », cette opération cybercriminelle de grande ampleur vise essentiellement les Etats-Unis, l'Allemagne, le Royaume-Uni et la France. Les serveurs à faible niveau de protection (absence d'antivirus ou d'authentification forte) sont principalement visés.

Nous vous recommandons la plus grande vigilance et vous invitons dès maintenant à procéder à une **vérification de l'intégrité de vos serveurs** en éxécutant **la ligne de commande suivante (sur une seule ligne) :**

ssh -G 2>&1 | grep -e illegal -e unknown > /dev/null && echo « System clean » || echo « System infected »

Dans le cas où vos serveurs sont intacts, nous vous recommandons fortement de **considérer la mise en place d'une solution d'authentification forte** afin de protéger vos identifiants administrateur et clés privées.

Dans le cas où votre serveur est infecté, la sécurité de vos accès et de vos données doit être considérée comme compromise. C'est pourquoi nous vous recommandons de procéder à un formatage et une réinstallation système.

source : WeLiveSecurity.com

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Alerte VIRUS – Recrudescence d’attaques du ransomware Cryptolocker

	**Alerte niveau 1 – Recrudescence d’attaques du ransomware Cryptolocker**

Alerte niveau 1 – Recrudescence d’attaques du ransomware Cryptolocker

Les caractéristiques de ce malware

- Le plus souvent sous la forme d’un e-mail contenant une pièce jointe malveillante.
- Si la pièce jointe est ouverte, le programme s’installe sur l’ordinateur et chiffre les données.
- Dès lors, le cybercriminel débute son chantage en demandant de verser une rançon.
- D’une valeur moyenne de 700€, elle peut atteindre 4000€ lorsque l’attaque cible un serveur.
- Les serveurs sont la cible préférée des pirates
- Le pirate tente de pénétrer la machine via des accès

externes, ouvert sur internet
- Les mots de passe faibles sont facilement découverts par attaques dites « brut force par dictionnaire »
- Le pirate peut ensuite prendre la main sur le serveur, désactiver l'antivirus, et lancer le chiffrement de tous les fichiers de données
- Attention CryptoLocker chiffre également les sauvegardes et lecteurs réseau

Mise en garde, comment se prémunir ?

Voici un rappel des bonnes pratiques élémentaires

- Etre équipé d'un logiciel antivirus performant. ESET permet d'avertir l'utilisateur du danger. Malgré le message d'avertissement, l'utilisateur peut décider d'exécuter le fichier infecté. Il faut donc prendre en compte les messages des antivirus
- Sauvegarder ses données. Le guide édité par l'ANSSI va au-delà de la simple sauvegarde de fichiers et préconise la mise en place de Plan de Reprise d'Activité
- Mettre à jour les logiciels installés sur ses machines et serveurs : navigateur(s), outils Adobe, java, système d'exploitation, antivirus
- Bloquer les fichiers exécutables. Une protection en amont, par exemple sur serveur de messagerie ou passerelle. exemple : ESET Mail Security Exchange
- Répliquer ses sauvegardes locales sur un support externe.
- Appliquer des politiques de restrictions logicielles (PRS). Afin d'empêcher des programmes comme CryptoLocker de s'exécuter dans des répertoires tels que « %AppData% » ou « %LocalAppData% ». (règle qui peut être mise en place via le HIPS d'ESET)
- Utiliser les objets de stratégie de groupe (GPO) pour créer et restreindre les autorisations sur les clés de registre utilisées par CryptoLocker, comme HKCU \ SOFTWARE \ CryptoLocker (et variantes). Si le malware ne

peut pas ouvrir et écrire dans ces clés de registre, il sera incapable de chiffrer les fichiers

- Restreindre les autorisations sur les lecteurs réseau partagés pour empêcher les utilisateurs de modifier des fichiers
- Eviter d’utiliser les ports par défaut. Exemple : faille sur le port TSE TCP 3389 (Windows Terminal server)
- Utiliser des mots de passe forts, et mettre en œuvre une authentification multi-facteurs. Outil conseillé : ESET Secure Authentication

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)