Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

Alerte : 6 millions d’iPhones victimes d’un Trojan qui exploite un bogue du DRM ?

D’après Palo Alto Networks, un nouveau malware baptisé AceDeceiver, a déjà infecté près de 6 millions d’appareils iOS non jailbreakés appartenant à des utilisateurs Chinois.

Comme ont pu le constater les chercheurs, ce trojan infecte les appareils mobiles via des ordinateurs Windows et exploite des erreurs commises par Apple dans le système de gestion des droits numériques (DRM). A l’heure actuelle, AceDeceiver circule uniquement sur le territoire chinois ; d’après Palo Alto, il s’agirait du premier malware capable d’infecter les gadgets d’Apple qui utilisent le système imparfait DRM FairPlay. Et il n’est pas nécessaire que l’appareil soit débridé pour garantir l’infection.

« D’abord, il y a eu XcodeGhost, puis ZergHelper, et maintenant AceDeceiver » a rappellé Ryan Olson, directeur des études sur les virus chez Palo Alto, alors qu’il commentait la dernière découverte aux journalistes de Threatpost. « Ils contribuent tous à l’érosion continue de la protection du magasin d’applications d’Apple ». D’après l’expert, AceDeceiver permet d’obtenir un accès « homme au milieu » à l’appareil iOS et de forcer l’utilisateur à communiquer son identifiant Apple aux attaquants.

Ce nouveau malware iOS se distingue de ses prédécesseurs par le fait qu’il n’utilise pas de certificats légitimes Apple pour s’introduire dans un appareil non débridé. Il opte pour la technique FairPlay Man-In-The-Middle, utilisée déjà depuis deux ans pour diffuser des applications pirates. D’après les conclusions de Palo Alto, le trojan AceDeceiver est le premier cas où ce genre de modification est utilisé pour installer des malwares sous iOS à l’insu de l’utilisateur.

L’analyse a démontré que les auteurs d’AceDeceiver ont préparé cette campagne malveillante pendant de nombreux mois. Au deuxième semestre de l’année dernière, ils ont réussi à introduire dans l’App Store trois versions différentes de l’application AceDeceiver avec une fonction d’économiseur d’écran. Cette opération s’imposait afin d’obtenir les codes d’autorisation d’Apple sollicités via iTunes. Par la suite, les individus malintentionnés ont exploité ces codes avec l’application Windows Aisi Helper spécialement développée à cette fin pour procéder à l’installation des malwares sur les appareils mobiles à l’insu de l’utilisateur.

Aisi Helper est vendu uniquement en Chine et se présente comme un outil pour iOS qui permet de créer des copies de sauvegarde, de restaurer le système, de débrider les appareils, d’administrer l’appareil et de le purger. Toutefois, dans ce cas l’existance d’un client de ce genre sur le poste de travail Windows simplifie également la tâche de l’attaquant car le malware peut être installé sur les appareils iOS lorsque ceux-ci sont connectés à l’ordinateur. AceDeceive réalise l’installation en substituant la poigné de main FairFlay par son propre serveur d’autorisation. Il s’agit d’une attaque FairPlay Man-In-The-Middle, appliquée pour la première fois en 2014.

AceDeceiver a été porté à l’attention d’Apple le mois dernier et la société a déjà retiré les trois faux économiseurs d’écran de son magasin d’applications. Palo Alto indique toutefois que l’attaque est toujours possible. « Tant que les attaquants disposent du code d’autorisation, ils ne doivent pas obligatoirement accéder à l’App Store pour diffuser ses applications » expliquent les chercheurs dans leur blog. Ryan Olson, de son côté, a confirmé aux journalistes que de telles utilisationsdétournées étaient possibles car les résultats de l’analyse réalisée par le mécanisme DRM d’Apple sont valides en dehors de l’écosystème iTunes.

Une fois installé sur un appareil iOS, AceDeceiver peut fonctionner comme un magasin d’applications alternatifs. Il fonctionne sous le contrôle des individus malintentionnés et offre un large choix de jeux et d’utilitaires. L’utilisateur est également invité à saisir son identifiant Apple et son mot de passe pour pouvoir accéder à toutes les fonctions de l’application pirate gratuite.

Ryan Olso explique qu’il est difficile d’éliminer les problèmes provoqués par AceDeceiver. Dans le cas de ZergHelper cité ci-dessus, Apple avait simplement supprimé le malware de son magasin. Le nouveau trojan se distingue par le fait qu’il compte sur un client Windows et utilise un code d’autorisation obtenu antérieurement, ainsi que des lacunes dans le projet FairPlay DRM.

Au moment de la publication de ce billet, Apple n’avait pas encore réagi aux questions de Threatpost…. [Lire la suite]

Réagissez à cet article

Source : *Un Trojan Exploite Un Bogue Du DRM Pour Charger Des Malwares Dans IOS – Securelist*

Alerte vigilance – Ransomware Lockyx

Alerte vigilance – #Ransomware Lockyx

Bonjour, Une vague d'attaques du ransomware Locky touche actuellement de nombreuses entreprises dans le monde et depuis peu en France.Voici nos conseils pour se protéger contre cette nouvelle menace :

CONSEIL N°1 : VIGILANCE UTILISATEUR

Informez vos collaborateurs de l'importance de ne pas ouvrir la pièce jointe d'un email envoyé par un expéditeur inconnu. Soyez très vigilant notamment avec les pièces jointes .zip, .doc, .xls : sources de propagation de Locky.

Les sensibiliser à l'utilisation des macros et/ou les désactiver, source de propagation de Locky.

CONSEIL N°2 : SOLUTION DE PRA

Assurez-vous que vos machines sont correctement sauvegardées, et les images externalisées pour une restauration rapide en cas d'attaque.

Les équipes ESET sont mobilisées à l'heure actuelle pour vous apporter une solution rapide et continue contre ce ransomware et ses multiples variantes quotidiennes.

Note : si vos machines sont déjà infectées, isolez-les des autres, initiez leur restauration et lancez une analyse complète de vos systèmes.

Cordialement,

L'équipe ESET

… [Lire la suite]

Réagissez à cet article

Source : *Alerte vigilance – Ransomware Lockyx*

Un malware soupconné d’être à l’origine d’une coupure de courant en Ukraine

Un malware soupconné d’être à l’origine d’une coupure de courant en Ukraine

---

Le 23 décembre, les habitants de la ville ukrainienne d'Ivano-Frankivsk ont subi une importante panne de courant. Celle-ci a été provoquée par une défaillance provenant de la centrale électrique régionale et a affecté plusieurs milliers de foyers de la région. Mais cette soudaine panne n'était pas un accident : en effet, la société chargée de l'exploitation de la centrale a précisé que celle-ci avait été causée par des « interférences » sur leurs systèmes.

Mais pour plusieurs médias locaux, la piste d'une cyberattaque visant les infrastructures énergétiques du pays est à privilégier. La société de cybersécurité ESET a d'ailleurs publié plusieurs informations en ce sens : la société explique avoir récupéré des samples de malware ayant affecté plusieurs centrales ukrainiennes, et explique que ceux-ci ont pu être utilisés dans le cadre d'une cyberattaque à l'encontre des équipements ukrainiens.

Des nouvelles du cyberfront

ESET se dit en mesure d'affirmer que plusieurs entreprises Ukrainiennes du secteur de l'énergie sont victimes de cyberattaques. Les attaquants ont notamment recours à une famille de malware baptisées BlackEnergy, dont les traces ont été détectées à plusieurs reprises en 2015 dans des entreprises ukrainiennes liées au secteur de l'énergie.
BlackEnergy est un malware connu, qui a déjà été repéré plusieurs fois par le passé. Celui-ci se présente sous la forme d'un malware modulaire : une fois la cible infectée, les attaquants peuvent exploiter la porte dérobée ainsi créée afin de télécharger des modules différents permettant au malware d'accomplir diverses actions sur la machine cible.
Parmi les modules identifiés de ce malware, l'un d'entre eux permet notamment de s'attaquer aux systèmes SCADA, des postes utilisés pour le contrôle et la surveillance des installations industrielles. BlackEnergy permet également le téléchargement d'un autre malware, baptisé cette fois killdisk, et dont l'objectif est la destruction de données. Un arsenal qui laisse ESET penser que ces outils ont pu être mis en œuvre dans l'attaque dont semble avoir été victime la centrale électrique d'Ivano-Franivsk.
Les services de sécurité ukrainiens accusent la Russie d'être à l'origine de l'attaque selon Reuters, mais ces derniers n'ont émis aucun commentaire venant confirmer ou infirmer cette théorie. Une enquête a été ouverte par les autorités nationales pour déterminer les circonstances exactes de cette coupure de courant.

Réagissez à cet article

Source : *Ukraine : un malware soupconné d'être à l'origine d'une coupure de courant*

URGENT : Phishing Free Mobile, ne vous faites pas avoir !

URGENT : #Phishing Free Mobile, ne vous faites pas avoir !

Réagissez à cet article

Source : *URGENT : Phishing Free Mobile, ne vous faites pas avoir ! – Le Blog du Hacker*

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi — metronews

Plus de 2 millions de personnes doivent recevoir ces jours-ci une prime de Noël de la part de la Caf et Pôle emploi. Des escrocs profitent de l'occasion pour envoyer de faux mail provenant soi-disant de ces organismes. Objectif : vous soutirer des données personnelles.

La prime de Noël est versée à partir de ce mercredi 16 décembre 2015. La période parfaite pour des cyber-escrocs de tenter de vous soutirer des informations personnelles en se faisant passer pour des administrations ou des grands organismes. Leur objectif : usurper votre identité voire se servir sur vos comptes bancaires.

La police nationale alerte en effet sur les faux mails prétendument envoyés par la Caf ou Pôle emploi, qui sont chargés de verser cette aide à plus de 2 millions de bénéficiaires. Cette technique est appelée phishing, ou hameçonnage. Pour mieux la reconnaître et donc ne pas tomber dans le piège, voici en quoi elle consiste et comment réagir :

Logos qui semblent vrais ⇒ Vous recevez un courrier électronique qui reprend les intitulés, les couleurs et les logos bien connus pour ne pas éveiller vos soupçons.

Liens vers des sites piégés ⇒ Ce mail mail comporte un lien ou une pièce jointe. En cliquant dessus, vous êtes redirigé sur un site piégé qui vous invite à saisir des données personnelles (login, mot de passe, numéro de compte client, coordonnées bancaires…) soi-disant pour confirmation ou une vérification.

Fautes d'orthographe ⇒ Ne cliquez pas si vous avez un doute. Un indice : ces faux messages comportent souvent des fautes d'orthographe. Sachez également qu'aucun opérateur ou organisme ne vous demande de venir vérifier sur leur site des informations confidentielles en vous les faisant retaper en ligne. Vous pouvez si vous le souhaitez signaler l'email douteux **ici** sur la plateforme Pharos.

Réagissez à cet article

Source : *Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews*

Le blog du journal The Independent victime de malvertising, la faute à Flash

Le blog du journal The Independent victime de malvertising, la faute à Flash

L'un des blogs du quotidien britannique The Independent a été victime d'un piratage et l'un de ses encarts publicitaires redirigeait les utilisateurs vers un logiciel malveillant. La meilleure parade pour l'internaute lambda ? Tenir Adobe Flash à jour.

La société Trend Micro alerte sur son blog d'une attaque visant l'un des blogs du quotidien britannique The Independent. Dans un post daté de mercredi, la société de cybersécurité fait état d'une cyberattaque ayant visé le blog du quotidien américain britannique The Independent. La source de l'infection provient selon Trend Micro de l'un des blogs WordPress du quotidien : les chercheurs de Trend Micro ont ainsi remarqué que celui-ci redirigeait les utilisateurs vers une page de l'Angler Exploit Kit. Celui-ci tentait par la suite d'exploiter une vulnérabilité au sein d'Adobe Flash afin d'installer un logiciel de type rançongiciel sur la machine des utilisateurs affectés.
Selon un porte-parole de The Independent interrogé par la BBC, l'infection était causée par une opération de malvertising : en conséquence, les administrateurs du site ont donc bloqué l'affichage de publicité sur la page incriminée en attendant que le problème soit résolu. Le quotidien britannique précise que rien ne laisse entendre que des utilisateurs du site ont pu être affectés par l'attaque.

Adobe Flash : usual suspect

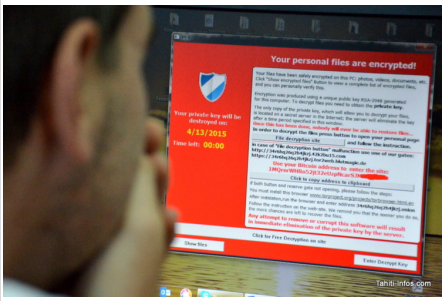
L'attaque n'a rien d'inhabituel : au contraire, on a plutôt affaire à un cas d'école assez représentatif des nouveaux moyens d'infections utilisés par les cybercriminels. D'une part, la technique du malvertising se démocratise : cette méthode consiste pour les cybercriminels à se faire passer pour des régies d'annonceurs publicitaires afin de pouvoir exploiter les outils de marketing programmatique pour faire apparaître leurs pages web malveillantes sur des sites à forte audience.
Dailymotion a ainsi été récemment victime de ce type d'attaque, qui gagne en popularité ces derniers mois. Les attaquants ont également eu recours à l'Angler Exploit Kit, le kit d'exploit le plus populaire actuellement parmi les cybercriminels. Véritables couteaux suisses des pirates, ces outils se présentent sous la forme de plateformes mises à jour afin d'exploiter facilement les vulnérabilités récemment découvertes dans les programmes populaires, Adobe Flash étant l'une des cibles favorites.
Enfin, le malware distribué appartient à la catégorie des ransomware, ou rançongiciel en français : le bien connu Cryptolocker. Celui-ci permet à l'attaquant de chiffrer l'ensemble des données sur le disque de la victime, données qui ne seront déchiffrées qu'en l'échange d'une rançon de 499$.
Pour l'utilisateur, la meilleure protection possible reste de veiller à conserver son navigateur et ses différents programmes à jour. Tout particulièrement Flash : on en profite pour signaler qu'une nouvelle mise à jour a été publiée par Adobe et corrige un peu plus de 70 failles de sécurités affectant le logiciel d'Adobe. Celui-ci étant la cible de choix des cybercriminels, on peut également envisager la suppression pure et simple du logiciel pour les plus paranoïaques.
Adobe annonçait d'ailleurs récemment amorcer la mise à la retraite de sa technologie, qui semble de moins en moins pertinente à l'heure de HTML5. Pour les victimes de ransomwares tels que cryptolocker, certaines sociétés de cybersécurité proposent des utilitaires permettant de decrypter les fichiers chiffrés par le logiciel malveillant, mais le fonctionnement n'est pas garanti.

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/le-blog-du-journal
-the-independent-vi
ctime-de-malvertising-la-faute-a-flash-39829632.htm

Attaque informatique importante contre les administrations et entreprises de Polynésie

Attaque informatique importante contre les administrations et entreprises de Polynésie

Depuis jeudi dernier, une attaque informatique de grande ampleur touche les services du Pays, de l'Etat et des entreprises de la Polynésie française. Le virus s'introduit sur les postes de travail par les mails, jeux flash et sites contaminés…



Les services informatiques du Territoire, de l'Etat et des entreprises sont en alerte rouge depuis bientôt une semaine : un virus s'est introduit sur de nombreux postes de travail et contamine même des serveurs au cœur de l'infrastructure des administrations et sociétés.

Un message de ce type peut accueillir les internautes imprudents

Ce virus est particulièrement vicieux, pour deux raisons. La première est qu'il est très évolué. Ce logiciel malveillant de dernière génération (une évolution de TeslaCrypt-2.0, détecté pour la première fois en juillet dernier) n'était pas encore identifié par les éditeurs d'anti-virus la semaine dernière. Kaspersky, la solution de sécurité du Pays et l'un des meilleurs du domaine, n'a mis à jour sa base de données virale contre cette nouvelle version qu'il y a deux jours.

La deuxième raison est le type d'attaques que commet ce virus : c'est un crypto-locker, aussi appelé « ransomware » pour « logiciel de rançon ». Une fois introduit sur les ordinateurs des victimes, il encrypte tous les fichiers du disque-dur puis demande une rançon pour rendre ses données à son propriétaire. Mais payer ne garantirait même pas le retour de toutes les données intactes…

NE PAS PAYER MAIS DEMANDER DE L'AIDE

Le conseil est de ne pas payer : « on ne peut pas décrypter les fichiers, mais des solutions existent pour récupérer les données. On peut essayer de revenir à des versions antérieures du fichier, sauvegardées automatiquement par Windows… Il y a aussi des façons de récupérer les fichiers originaux supprimés par le virus » nous explique un expert du CLUSIR (une association d'experts en informatique du Pays), qui assure qu'il ne faut pas céder à la panique. Il explique qu'en cas de contamination, il faut immédiatement éteindre le poste et le déconnecter du réseau, puis contacter son service informatique ou son prestataire informatique.

La situation semble désormais maitrisée dans les administrations après une sacrée frayeur. Nous avons ainsi appris que la direction de la Santé, l'Aviation civile, la direction des Ressources Marines et Minières, le palais de justice ou encore la clinique Paofai ont été attaqués. Certains serveurs auraient été contaminés et des bases de données rendues inaccessibles, par exemple celles de localisation des pêcheurs… Qui aurait été récupérée.

DES POSTES CONTAMINÉS VIA LES JEUX EN LIGNE

Les pirates utilisent des logiciels spéciaux pour infecter des sites web très populaires mais mal protégés. Ensuite, le « toolkit » essaiera de pénétrer les ordinateurs de tous les internautes qui visiteront ce site en testant les failles de sécurité connues. Pour vous protéger, gardez votre version de Windows, Flash, Javascript, votre navigateur etc. à jour.

On ne sait pas encore si c'est une attaque délibérée d'un groupe de pirates informatique – les mafias du monde entier se sont mises à ce nouveau modèle d'extorsion très juteux – ou s'il s'agit justes d'attaques aléatoires qui touchent particulièrement la Polynésie à cause de simples effets réseaux (un seul poste qui tombe et tout le réseau est contaminé ; un chef de service qui se fait avoir et tout son carnet d'adresses reçoit le virus par mail…). Les experts penchent pour la deuxième hypothèse, d'autant que le malware fait parler de lui dans le monde entier depuis quelques jours.

Les services informatiques qui luttent contre l'attaque en ce moment même nous confient que le principal point d'entrée du virus dans les réseaux était… Les sites de jeux en ligne contaminés par les pirates. Ensuite le virus a réussi à se répandre sur les réseaux des administrations puis des entreprises, jusqu'aux serveurs de fichiers du Pays par exemple, qui ont tous été passés en mode « lecture seule » ce mercredi pour essayer d'achever le virus.

L'autre mode de contamination : les fichiers attachés (particulièrement ceux ayant les extensions .js, .zip et .exe) et… les sites porno. Le meilleur conseil reste celui d'un informaticien contacté pour cet article : « Cette attaque c'est pour tout le monde, il est vraiment temps de faire vos sauvegarde. »

Les conseils de prudence du service informatique du Pays

Depuis le début de l'attaque contre les services du Pays, les informaticiens du Territoire sont sur le pied de guerre contre ce virus particulièrement sophistiqué. Plusieurs sources nous ont transmis les mails reçus dans toute l'administration territoriale, dont voici un extrait du dernier en date :

« Suite aux précédents courriels que nous vous avons envoyés, nous souhaitons vous tenir informés de l'évolution de l'infection virale. Elle touche aussi désormais d'autres sociétés de Polynésie française. La situation est inquiétante. (…)

Mise à jour de la définition virale

Nous vous demandons de vérifier que votre anti-virus Kaspersky est à jour. Pour cela, placer la souris sur l'icône « K » en bas à droite de votre bureau : la date d'édition des bases ne doit pas être antérieure à deux jours. Dans le cas contraire, merci de bien vouloir contacter le support du service informatique.

Sauvegarde de vos données personnelles

Nous vous rappelons aussi que vous devez faire des sauvegardes de vos données professionnelles se trouvant sur votre poste de travail. Les serveurs de fichiers étant en lecture seule, sauvegardez vos données professionnelles sur un support externe (disque USB, clé USB), ne pas oublier de le déconnecter à la fin de la sauvegarde.

Rappels sur des règles de sécurité

Afin de vous protéger des virus qui sévissent actuellement, nous vous demandons de suivre scrupuleusement les consignes de sécurité suivantes :

– ne pas ouvrir des courriels suspects (expéditeur inconnu, objet du courriel rédigé en anglais…)

– ne pas ouvrir les pièces jointes à un courriel suspect, en particulier, ne surtout pas ouvrir les fichiers se terminant par l'extension .js. »

Réagissez à cet article

Source : http://www.tahiti-infos.com/Attaque-informatique-importante-contre-les-administrations-et-entreprises-de-Polynesie_a141657.html

---

Un malware qui reste lors d'une réinstallation du

système d’exploitation

Un malware qui reste lors d’une réinstallation du système d’exploitation

Conçu en particulier pour dérober des données bancaires, l’écosystème Nemesis comporte un logiciel malveillant qui s’installe à très bas niveau sur le disque dur.

Les équipes de Mandiant (FireEye) ont découvert, en septembre dernier, un logiciel malveillant employant des méthodes de persistance peu communes : il s’immisce dans le processus d’initialisation de l’ordinateur infecté, avant même le chargement du système d’exploitation, afin de pouvoir compromettre celui-ci à coup sûr et, surtout, résister à une tentative de nettoyage de la machine par réinstallation de son système d’exploitation – « un moyen largement considéré comme le plus efficace pour éradiquer un logiciel malveillant », soulignent les chercheurs de FireEye dans un billet de blog.

Analyse comportementale : la clé de la sécurité ?

E-handbook : L’analyse comportementale joue un rôle non négligeable dans la sécurité de votre entreprise.

Ce logiciel malveillant fait partie de Nemesis, un ensemble d’outils malicieux utilisé par le groupe FIN1, qui semble « localisé en Russie, ou un pays russophone », spécialisé dans le vol de données de cartes bancaires et, plus généralement, d’informations « aisément monétisables en provenance d’organisations telles que banques, organismes de crédit, opérations de DAB », etc.

Comme le rappellent les chercheurs de FireEye, le secteur d’amorçage des disques durs, le fameux MBR (Master Boot Record), ne contient pas que des données inertes relatives aux partitions définies : il recèle également quelques éléments de code utilisés durant le processus de démarrage ; « ce code cherche la partition active principale et passe ensuite le contrôle au VBR (Volume Boot Record) de cette partition ». Ce dernier contient également du code exécutable « spécifique au système d’exploitation présent sur cette partition », et lui permettant de lancer son démarrage.

Baptisé Bootrash, le logiciel malveillant découvert par les équipes de Mandiant, pirate ce processus en remplaçant le code d’amorçage du VBR par son propre code malicieux chargé d’appeler le bootkit Nemesis. Celui-ci « intercepte certaines fonctions du processus de démarrage et injecte les composants Nemesis dans le noyau de Windows ».

Les chercheurs de FireEye soulignent que ce n’est pas une première, mais que l’utilisation d’un bootkit MBR ou VBR n’est pas courant. Une chance, peut-être, car la détection peut s’avérer particulièrement difficile : ces logiciels malveillants peuvent « être installés et s’exécuter presque complètement en dehors du système d’exploitation Windows », passant au travers des mécanismes de vérification de son intégrité ou encore des anti-virus – à moins d’examiner méticuleusement la mémoire vive.

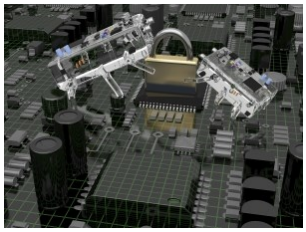
Réagissez à cet article

Source : http://www.lemagit.fr/actualites/4500260472/Un-malware-qui-reste-lors-dune-reinstallation-du-systeme-dexploitation

20% of cyber-attacks attributed to Conficker worm

20% of cyber-attacks attributed to #Conficker worm

Detected in everything from police body cameras to the business internet of things (IoT) landscape, now do you give a configuration fick?



The notorious Conficker worm has been gaining an ever-wider reputation for destruction. Last month SCMagazineUK.com reported on this comparatively old malware's presence as it started to appear pre-installed inside police body cameras.

Not content with infecting the security forces' use of Internet of Things devices, Conficker has continued to turn its venom towards the business landscape in general. October of this year saw Conficker ranked by security vendor Check Point as the most common malware used to attack British and international organisations.
Check Point suggests that as many as 20 percent of all attacks globally can be attributed to Conficker in the period identified.
Also known as by the name Downadup, Conficker was first identified as far back as 2008. It targets the Windows operating system and can form a botnet to infect a computer and spread itself to other machines across a network automatically, without human interaction.

Undead, still walking

As noted on The Register, networks belonging to the French Navy, the British House of Commons and Greater Manchester Police were all laid low by the malware. "Its recent resurgence hasn't caused anything like the same amounts of problems but still highlights the generally poor state of corporate security," wrote John Leyden.

How does the Conficker worm spread?

Microsoft's own advisory states that the Conficker worm spreads by copying itself to the Windows system folder. The firm notes, "It might also spread through file sharing and through removable drives, such as USB drives (also known as thumb drives), especially those with weak passwords."

What marks Conficker's resurgence now, in the dying days of 2015, is not only its brute-force attack ability on passwords but also its longer term ability to still cause impact. As botnets and remote control PC attacks now still grow, the prevalence of ransomware and data-stealing malware also continues to rank highly among the reported threats as measured by the security industry.

Common tools democratise hacking

Fraser Kyne, principal systems engineer at Bromium contacted SC to say that the use of common tools in this way democratises hacking, as it provides a framework for mounting similar attacks across a range of vectors.
"Re-purposing the tools of the past is a simple model for attackers, and one that is difficult to detect. We see some vendors claiming to be able to look for telltale signs of these models – but realistically they're playing a losing game where the attacker is always several steps ahead," said Kyne.
As a related note, Bromium Labs has recently blogged on the resurgence of malware that uses macros in Office documents, particularly Dridex. In this sense, malware is analogous to malaria. As vaccines become available, the disease morphs.
"The only practical (and sustainable) model for defending against malware is isolation. This needs to be done outside of the operating system. Modern hardware has the capability to do this securely, efficiently and invisibly for the user – and we're seeing proof of the success of this approach. In this model, the mosquito bites a crash test dummy, not the real user, and there's no impact to the business," he said.

Actually, you're failing miserably

Richard Cassidy, technical director EMEA, Alert Logic told SC that the proliferation of Conficker highlights organisations' continuing failure across the board to get it right when it comes to key security practices and policy enforcement.
"With the plethora of incredible security technologies today, from network access control to micro-visor security containers at the host process level, through to big data analytics platforms, all poised to detect advanced malware variants of C2C, botnet and remote control infection, it is a wonder therefore that organisations (including governments) are not only being successfully infected with malware, but also for inordinate periods of time before detection," said Cassidy.
He surmises that ultimately we have to assume that we will be infected, even if we manage to get all the required parts aligned.
"With this mindset, therefore, we will drive better protection of key data assets from being easily compromised and will work to ensure we are better poised to detect compromise activity, should a particular user not have adhered to a 'no-download' policy from untrusted sources," he said.
This article originally appeared on SC Magazine UK.

Réagissez à cet article
Source : http://www.scmagazine.com/20-of-cyber-attacks-attributed-to-conficker-worm/article/458392/

Le FBI et Microsoft font trembler le botnet DorkboOscar Barthe

Le FBI et Microsoft font trembler le botnet Dorkbot

En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.

Le botnet Dorkbot permet à ses utilisateurs de récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Twitter ou encore Steam.
En partenariat avec les forces de l'ordre de plusieurs pays comme le FBI et Interpol ainsi que d'autres acteurs IT et télécoms comme Eset, Microsoft a mené une attaque contre les infrastructures du botnet Dorkbot. Le but de l'attaque était, à défaut de l'éradiquer, de perturber son fonctionnement.
Microsoft a fait sa bonne action. La firme de Redmond a déclaré jeudi avoir collaboré avec les autorités de plusieurs régions pour perturber le fonctionnement du botnet Dorkbot.
Découvert il y a quatre ans, ce dernier a infecté aujourd'hui plus d'un millions de machine. Il est utilisée pour récupérer les identifiants de connexion de différents services comme Gmail, Facebook, Netflix, PayPal, Steam ou encore eBay. La firme de Redmond ne s'est toutefois pas lancée seule dans l'attaque contre Dorkbot, et a travaillé ainsi avec le fournisseur de solution de sécurité Eset, le Cert polonais Polska, la commission canadienne de Radio-télévision et de télécommunications, l'agence de sûreté américaine, le FBI, Interpol, Europol et la police montée du Canada.
Les utilisateurs sont pour la majeure partie d'entre eux infectés lors de leur navigation sur internet sur des sites pas forcément bien protégés. Dorkbot exploite la moindre faille logicielle via un exploit kit ou les spam. Il peut aussi utiliser un système de ver pour se diffuser à travers les réseaux sociaux, les services de messagerie ou les clés USB.

Une attaque efficace mais pas durable
Microsoft n'a toutefois pas détaillé comment il s'y était pris pour perturber les infrastructures de Dorkbot. Ce n'est d'ailleurs pas la première fois que la firme collabore avec les autorités dans ce genre de situation. Les actions coordonnées visant à déconnecter les serveurs hébergeant les botnet ont souvent un impact immédiat mais les bénéfices ne durent pas. Souvent, les cybercriminels remettent rapidement sur pied une nouvelle infrastructure et s'attaque à la reconstruction du botnet en infectant d'autres ordinateurs.
La situation autour de Dorkbot devenait critique. Ses créateurs ont diffusé un kit permettant d'utiliser le botnet comme base pour en construire d'autres, plus puissants. Baptisé NgrBot, il était en vente sur le deep web.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-le-fbi-et-microsoft-font-trembler-le-botnet-dorkbot-63185.html
Par Oscar Barthe