Quelques pistes en prévention ou en curation d’attaque par ransomwares

	Quelques pistes en prévention ou en curation d’attaque par ransomwares

Un de vos clients est victime d'un ransomware. Cryptolocker, Cryptowall, Supercrypt, TeslaCrypt, … Peut importe le malware, le résultat est à peu prêt le même. Ses fichiers sont cryptés, et l'impact est énorme. Dans l'urgence, il convient de procéder correctement, en prenant certaines précautions. Je vais donc ici vous donner quelques pistes (un peu en vrac) afin de traiter au mieux le problème.

Sauvegarde
J'imagine que si vous consultez cet article, aucune sauvegarde de votre client n'est exploitable. Sinon, vous l'auriez remontée.
Cependant, avant d'envisager toute action sur le/les systèmes infectés, pensez à procéder à une sauvegarde. Je recommande d'arrêter immédiatement ces systèmes infectés. Ensuite, qu'il s'agisse d'un serveur, ou d'un simple client, clonez le disque dur.
Pour cela, effectuez un clone en mode hors ligne, avec un de ces outils par exemple : Acronis, Veeam, AOMEI.
Ca vous permettra d'effectuer les tests que vous voulez sur le clone, sans aucun risque.

Lister les fichiers cryptés
Un outil bien pratique permet de lister les fichiers cryptés par Cryptowall. En effet, cette infection stocke la liste des fichiers qu'elle crypte dans le registre. L'outil ListCWall permet de localiser et utiliser ces infos afin de vous sortir une liste des fichiers, et permet aussi de les exporter afin de les stocker par exemple sur un média externe avant de formater la machine si besoin.

Utilitaires de décryptage
Ce qu'il faut retenir de ce paragraphe, ce n'est pas autant la liste des outils (non exhaustive) que je vous propose, mais que de tels outils voient le jour périodiquement. Pensez à regarder du côté des éditeurs d'antivirus (ou sur Tech2Tech!!), si un nouvel outil existe concernant l'infection que vous avez à traiter en particulier. En effet, suite à des enquêtes internationales, parfois, des réseaux tombent. Et lorsque les services en charge de ces enquêtes découvrent un lot de clés de cryptages, les éditeurs d'antivirus peuvent les exploiter afin de les intégrer dans des outils de décryptage. Pas sur que ca fonctionne donc (si la clé utilisée ne fait pas partie de celles qui ont été découvertes) mais vous pouvez le tenter…
On peut lister par exemple :
RectorDecryptor chez Kaspersky (pour le ransomware Rector)
XoristDecryptor chez Kaspersky (pour le ransomware Xorist/Vandev)
ScatterDecryptor chez Kaspersky (pour le ransomware Scatter)
ScraperDecryptor chez Kaspersky (pour le ransomware Scraper)
RakhniDecryptor chez Kaspersky (pour le ransomware Rakhni)
Ransomware Decryptor chez Kaspersky (pour le ransomware Coinvault/Bitcryptor)
Decryptor 0-1.3 chez Bitdefender (pour le ransomware Linux.Encoder.1)
DecryptCryptoLocker par FireEye et Fox IT (pour le ransomware CryptoLocker)
TeslaDecrypt par Cisco Talos Security Intelligence (pour le ransomware TeslaCrypt)

Récupérer les fichiers
A ma connaissance, si vous n'avez pas de sauvegardes, et que le ransomware n'a pas d'outil de décryptage dédié ayant été élaboré, il y a peu de chances de retrouver les fichiers.
Cependant, deux pistes peuvent s'avérer intéressantes :

Shadow Volume Copies
Les shadow copies (service de clichés instantanés), peuvent s'avérer utiles dans le cas d'un ransomware. Cependant, il faut déjà que le service soit activé et configurée correctement. Ensuite, la majorité des ransomware un peu élaborés et récents désactivent ce service, et vont effacer les snapshots déjà présents. S'ils s'avèrent utilisables, le logiciel Shadow Explorer sera pratique pour récupérer les fichiers.

Récupération de données
Il semblerait que, dans le cas de certains ransomware, les fichiers soient copiés, cryptés, puis supprimés. Il serait alors envisageable, si la machine est arrêtée au plus vite, de récupérer des fichiers à l'aide d'un utilitaire de récupération de données.
Pour cela, clonez d'abord le disque par précaution, en mode hors ligne (Live CD).

Se protéger des ransomwares
Plusieurs éditeurs de solutions de sécurité proposent des utilitaires plus ou moins élaborés afin de se protéger contre un cryptage de données.
Il y a d'abord une approche qui consiste à interdire le lancement d'exécutables situés dans %APPDATA%. C'est en effet un mode de fonctionnement courant de ce type de malwares. Cette fonction est proposée par Bitdefender à travers son outil gratuit Anti-Cryptowall. Personnellement cet utilitaire ne m'a pas vraiment convaincu lorsque je l'ai essayé, puisque j'ai pu lancé des exe situés dans %APPDATA%…
CryptoPrevent, utilitaire développé par Foolish IT permet de se prémunir d'une attaque par un CryptoLocker. Cependant, la version gratuite nécessite des mises à jours manuelles visiblement. Voyez plutôt vos besoins sur les différentes versions commerciales.
BitDefender a intégré dans sa version grand public 2016 un moteur d'analyse de cryptage. Le but est d'analyser en temps réel une éventuelle activité de cryptage sur la machine, et de la stopper. Cette fonction sera intégrée dans les antivirus pro maximum en début d'année 2017.
Pour ma part, je suis distributeur des solutions Panda Security Cloud. Et un outil a été mis au point durant l'été : Adaptive Defense 360. Venant en renfort de n'importe quel antivirus, ce produit permet de bloquer tous les logiciels que l'entreprise n'a pas décidé explicitement de laisser fonctionner sur son parc. Il en résulte une protection quasi parfaite, même si ca a un coût. Et comme il faut bien manger, je me fais au passage une petite pub : n'hésitez pas à me contacter si vous désirez vous équiper de cette solution!
Ce ne sont évidement que des exemples, non exhaustifs. Mais ils traduisent la diversité des solutions élaborées afin de contrer les ransomwares et cryptolockers, qui sévissent actuellement de manière dramatique.

Réagissez à cet article
Source : http://www.tech2tech.fr/ransomware-avec-cryptage-quelques-pistes/

Comment un cybercriminel peut infiltrer votre réseau

Comment un cybercriminel peut infiltrer votre réseau

La sécurité est plus que jamais une priorité pour les entreprises, contribuant activement à sa réussite. Les RSSI doivent désormais s'assurer que leurs projets en matière de sécurité IT sont en phase avec les objectifs de l'entreprise.

Nous sommes tous connectés à Internet, ce qui est très positif. Mais ce lien permanent implique que nous sommes tous au cœur d'un écosystème de grande envergure. Il est essentiel de comprendre que tout ce qui touche une organisation impactera également de nombreuses autres entreprises, et notamment ses partenaires. Ainsi, en cas de piratage d'une entreprise, ce sont des données personnelles identifiables qui sont détournées. Ces données peuvent être revendues à des spécialistes de l'usurpation d'identité ou constituer un terreau favorable aux attaques de phishing. Plus l'assaillant disposera d'informations sur vous, plus l'email qu'il vous enverra apparaîtra comme légitime et vous incitera à cliquer sur un lien malveillant.

Notons que les tactiques d'attaques actuelles sont similaires à celles d'il y a quelques années : récupération de mots de passe faibles, attaques de type phishing et téléchargement de logiciels malveillants à partir de sites web infectés ou de publicités malveillantes. Sauf qu'aujourd'hui, l'assaillant a gagné en furtivité et en efficacité lorsqu'il mène son attaque.

Penchons-nous, par exemple, sur les réseaux sociaux et les services en ligne. Nous sommes très nombreux à les utiliser, qu'il s'agisse de Facebook, de LinkedIn, ou encore des sites de rencontres en ligne. Les assaillants l'ont parfaitement compris et capitalisent sur la fibre émotionnelle de chacun. Ils établissent ainsi leur passerelle d'entrée vers les dispositifs des utilisateurs en s'aidant de ces sites et de techniques d'ingénierie sociale. Ainsi, si les méthodes d'ingénierie sociale restent les mêmes, les vecteurs et la surface d'attaque ont, en revanche, progressé. Parallèlement, ce sont les techniques de furtivité qui ont gagné en précision, avec des assaillants toujours plus aptes à se dissimuler. Se contenter d'utiliser les antivirus traditionnels n'est donc tout simplement plus suffisant.
Parmi les techniques utilisées, l'attaque de type phishing est la méthode principale pour s'immiscer au sein des réseaux d'entreprise.
Un email de phishing, conçu pour paraître le plus légitime possible, est envoyé avec un fichier joint ou une URL malveillante, et incitant l'utilisateur à ouvrir le fichier ou à cliquer sur l'URL.
L'attaque par téléchargement furtif (ou drive–by attack) est une autre technique utilisée par les assaillants. Ces derniers piratent un site Web et y installent un script java malveillant qui redirigera l'utilisateur vers un autre site hébergeant un logiciel malveillant téléchargé en arrière-plan vers l'équipement de l'utilisateur. Dans le cas d'une attaque ciblée, les assaillants peuvent passer des mois à identifier les sites Web les plus consultées par les organisations ciblées, pour ensuite les infecter.
Le malvertising (publicité malveillante) compte également parmi les techniques utilisées. Cette attaque emprunte les codes des attaques drive-by, mais l'assaillant se focalisera sur l'infection des sites de publicités. Il devient possible d'infecter un seul de ces sites qui, à son tour, pourra infecter jusqu'à 1 000 autres sites Web. Ou l'art d'industrialiser son attaque.
Enfin, n'oublions pas l'attaque mobile. Nombre de ces attaques sont similaires à celles mentionnées plus haut, mais elles ciblent les dispositifs mobiles. Notons qu'il est possible d'infecter un dispositif mobile via un message SMS, ou à l'aide d'un logiciel malveillant qui se présente en tant qu'application ludique ou de contenu pour adultes.
Lorsque l'assaillant est rentré dans un réseau et qu'il réside sur le dispositif d'un utilisateur (ordinateur de bureau ou portable, équipement mobile), il doit désormais injecter de nouveaux logiciels malveillants et outils pour mener à bien sa mission. Généralement, les informations de valeur ne sont pas stockées sur les postes de travail, mais plutôt sur les serveurs et des bases de données. Voici donc un aperçu des étapes supplémentaires pouvant être mises en œuvre par un cybercriminel déjà présent dans le réseau :

1. Téléchargement d'autres outils et logiciels malveillants pour compromettre davantage le réseau.
2. Exploration du réseau pour identifier les serveurs hébergeant les données ciblées. Recherche du serveur Active Directory contenant tous les identifiants d'authentification, dans l'objectif de pirater ces données, véritable sésame pour le cybercriminel.
3. Une fois les données ciblées identifiées, recherche d'un serveur provisoire pour y copier ces données. Le serveur idéal est un serveur stable, à savoir toujours disponible, et disposant d'un accès sortant vers Internet.
4. Exfiltration furtive et lente de ces données vers les serveurs des assaillants, généralement déployés dans le cloud, ce qui rend la neutralisation des communications plus complexe.

Les cybercriminels présents au sein du réseau sur une longue durée pourront obtenir tous types d'informations disponibles puisque les données d'entreprise, dans leur grande majorité, sont archivées sous format électronique. Plus le cybercriminel est présent sur le réseau, plus il en apprend sur les processus et les flux de données de votre entreprise. L'attaque Carbanak qui a ciblé de nombreuses banques dans le monde en est la parfaite illustration. Lors de cette exaction, les cybercriminels sont remontés jusqu'aux ordinateurs des administrateurs ayant accès aux caméras de vidéosurveillance. Ils ont ainsi pu surveiller de près le fonctionnement du personnel bancaire et enregistrer tous les processus dans le détail. Ces processus ont été reproduits par les cybercriminels pour transférer des fonds vers leurs propres systèmes.

Comme déjà souligné, une brèche dans le réseau s'initie généralement par un simple clic d'un utilisateur sur un lien malveillant. Après avoir investi le poste de l'utilisateur piraté, l'assaillant commence à explorer le réseau et à identifier les données qu'il souhaite détourner. C'est dans ce contexte que la notion de segmentation de réseau devient essentielle. Cette segmentation permet de maîtriser l'impact d'un piratage puisque l'entreprise victime peut isoler la faille et éviter tout impact sur le reste du réseau. D'autre part, elle permet de cloisonner les données sensibles au sein d'une zone hyper-sécurisée qui rendra la tâche bien plus complexe pour ceux qui souhaitent les exfiltrer.

Pour conclure, gardons à l'esprit qu'il est impossible de protéger et de surveiller le réseau dans sa totalité, compte tenu de son périmètre étendu et de sa complexité. Il s'agit donc d'identifier les données les plus sensibles, de les isoler et de porter son attention sur les chemins d'accès vers ces données.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/Comment-un-cybercriminel-peut,20151209,58191.html

---

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

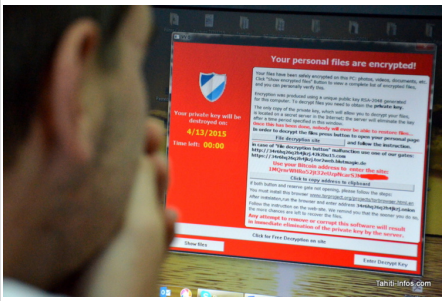
L'attaque n'a rien d'inhabituel : au contraire, on a plutôt affaire à un cas d'école assez représentatif des nouveaux moyens d'infections utilisés par les cybercriminels. D'une part, la technique du malvertising se démocratise : cette méthode consiste pour les cybercriminels à se faire passer pour des 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

---

CyberDélinquence ou CyberCriminalité ? Le terreau

de l’argent facile et des créatures de rêve

	**CyberDélinquence ou CyberCriminalité ? Le terreau de l’argent facile et des créatures de rêve**

La cybercriminalité ou la Cyberdélinquence est devenue un fléau des temps modernes. Mais facile à comprendre. Cependant, qui s'y frotte s'y pique. Tous ceux qui aiment l'argent facile, les belles filles, les sensations fortes, les Bon chics bon genre sont les principales victimes.

Internet est devenu incontournable avec certes des avantages et des inconvénients. Mais en face, il y a des hommes et des femmes prêts à tout, pour détourner les objectifs.

Phénomène de ces dernières années, la cybercriminalité est devenue un fléau.

Les réseaux sociaux attirent toutes ces personnes, souvent aveugles. Au bout du compte, on perd toutes ses plumes, ses économies, son prestige. Les forces de police, de gendarmerie comptent ainsi jouer un grand rôle pour mettre fin à cela. Mais comme l'a dit le Président Macky Sall, il faut mutualiser et partager les informations. Les gouvernements, les forces de sécurité essaient tant bien que mal, à mettre fin à cette forme de délinquance. Un phénomène de société.

Dans une société en mal de repères, on veut tout et tout de suite.

De l'argent, de belles filles, des Don Juan qui vous couvrent de millions, des voyages, mais en … rêve. Tout est fiction dans ce phénomène. En effet, les internautes ou les victimes mordent souvent trop vite à l'hameçon. Qui dans ce Sénégal n'aimerait pas recevoir des millions sans bouger ? Si cela existait, cela ne sortirait pas du cercle d'amis. Une utopie.

Aujourd'hui, nombre de compatriotes sont étranglés par les banques et les problèmes familiaux. Rien que pour l'obtention d'un crédit bancaire, l'on vous demande des « tonnes de paperasse », authentifiés. Ce sont donc des heures et des heures de connexion jamais gratuites. On surfe à longueur de journée. Et à tous les niveaux de notre haute administration. On se connecte pour des banalités, des futilités. Des conversations à vous donner des insomnies, des dettes.

Ils sont hommes d'affaires, étudiants, chômeurs, commerçants, dans toutes les catégories sociales. On « tchatte » et on oublie tout. On est en retard sur tout. Parce que la tête dans les nuages. Vous voyez souvent des personnes, rire, sourire pour un rien, c'est toujours la bonne humeur sur les visages. Jusqu'à ce que tout vous tombe sur la tête. On vous déplume en un temps record, comme devant ces faiseurs de miracles multiplicateurs de billets.

En effet, c'est la nouvelle version. Tout simplement. Comment se fait-il donc, que dans la clandestinité et dans l'illégalité, un inconnu vous détourne du système normal, sur un simple clic. Les victimes sont prises au piège après avoir été identifié. Sur le net, beaucoup de photos sont truquées. Des hommes se font passer pour des femmes, des femmes pour des hommes. Vous tombez toujours sur des personnages de rêve. Et dans votre subconscient, vous êtes prêts ou prêtes à tout. Pour oublier vos dettes, épouser cette perle rare, vous envoler sur une petite île, sans bruits ni tambours.

Loin de votre entourage, l'on vous propose toutes sortes de services jamais gratuits. Dès que l'argent commence à montrer son bout de nez, vous êtes pris comme une souris au piège. C'est d'abord les crédits téléphoniques, les virements, etc. Ce sont souvent des étrangers qui sont rois dans le phénomène. Mais de plus en plus, des Sénégalais y font légion.

Gagner de l'argent, épouser une belle fille, voyager, des dons… Ce qui est surprenant, c'est que beaucoup de victimes regrettent après avoir été dépouillé. Lors des mercredis de la police organisés cet été, le sujet sur la cybercriminalité avait été évoqué.

Devant les cadres, les hautes autorités de la police, la presse, entre autres, des panélistes avaient sonné l'alarme. Face à ce danger, des débats intéressants ont été organisé. Au Sénégal, il existe une entité qui s'occupe des données personnelles à « protéger » ? Et où il existe toujours selon les panélistes « un flou ». Dans un pays où il n'y a pas de textes juridiques spécifiques sur la cybercriminalité.

L'un des panélistes a évoqué un cas qui mérite attention. Celui d'une personne qui est tombée, par hasard sur un faux médecin. Ce dernier voulait à travers l'ordinateur, lui faire un check up. Imaginez un peu la suite. En lieu et place d'un toubib, ce fut un étranger qui après l'avoir photographié et non passé un « scanner », passe à l'acte deux. Le chantage. Mais la victime ne voulait pas que l'affaire s'ébruite. Déduire les frais et renvoyer la somme restante, une astuce payante

Autres faits importants.

Comment se fait-il que pour un « héritage », à recevoir, jamais dans un acte notarié, ou un « don » d'une personne anonyme, l'on puisse procéder à des virements d'argent… sans traces ? Les sociologues commencent à s'intéresser à l'affaire. Et souvent, leurs théories semblent incomprises de ces amateurs de sensations et de divertissements chèrement payés. Et le phénomène commence à devenir difficile à gérer. L'État du Sénégal a mis en place la brigade de lutte contre la cybercriminalité. Récemment, les gendarmeries africaines se sont rencontrées pour l'analyser. Surtout avec ces jeunes de plus en plus exposés. C'est pourquoi, le Président Macky Sall a demandé à toutes ces forces de défense : police, gendarmerie de mettre en place « des plateformes de partage ». Comme il l'a souligné lors cette rencontre, « les criminels ne connaissent pas les zones ». Souvent entre la gendarmerie et la police on parle « d'écoles ou de couleurs de tenue ».

Pour lui, ce qui importe « c'est le résultat ». Sinon, c'est « un éternel rattrapage ». En donnant comme exemple le ministère de l'Intérieur avec « Interpol ». Un phénomène selon lequel, il faut « une sensibilisation en direction de tous les citoyens.

Et pour ceux qui ont la responsabilité de gérer les systèmes informatiques ». Et le renforcement de la coopération internationale. La cybercriminalité n'a pas de frontières. Ou bien tout simplement être comme ce futé. Lorsqu'on lui a demandé une contrepartie, il a tout simplement demandé à son généreux donateur de lui envoyer l'argent, tout en y déduisant les soi-disant frais bancaires. Ce que le généreux « donateur » n'a pas voulu entendre.

Réagissez à cet article

Source : http://www.rewmi.com/cyberdelinquence-ou-cybercriminalite-le-terreau-de-largent-facile-et-de-creatures-de-reve.html

La face cachée du Web caché, le « dark Web »

	La face cachée du Web caché, le « dark Web »

Le «dark Web», dont les utilisateurs sont anonymes et intraçables, est utilisé, pour le pire et pour le meilleur, par des trafiquants d'armes autant que par des dissidents opprimés par les États totalitaire.

«Sur Internet, on peut acheter une kalachnikov en deux clics.» Pour qui n'y connaît rien, ce genre de phrases, entendues à la radio ou à la télévision, interroge.

Depuis les attentats de janvier notamment, Internet (1) est au cœur des préoccupations. «Dans quelle mesure, Internet et le Web profond sont-ils utilisés pour recruter, communiquer et préparer des actions criminelles?», interrogeait Nathalie Goulet, présidente de la commission d'enquête sénatoriale sur les réseaux djihadistes, lors d'une table ronde fin janvier.

Web profond, Web sombre ou dark Web… Tous ces termes renvoient à une même idée: il existerait un espace sombre, caché et donc suspect, dans lequel chacun pourrait, en quelques minutes, se procurer une arme ou de la drogue. De fait, à première vue, la chose n'est pas bien compliquée.

Pour commencer, il faut télécharger sur son ordinateur un navigateur personnalisé, libre et gratuit, comme TOR par exemple (pour The Onion Router). Ses paramètres permettent la connexion au réseau TOR. L'intérêt? Alors qu'habituellement, un utilisateur surfant sur Internet dispose d'une adresse IP, sorte de plaque d'immatriculation de son ordinateur, TOR brouille l'adresse IP de l'utilisateur.

«Les criminels ont recours à ce type de technologie pour anonymiser leurs échanges d'informations, ne pas être identifiés ni localisés, et de ce fait, ne pas être inquiétés par les forces de l'ordre, explique Solange Ghernaouti, directrice du Swiss Cybersecurity Advisory & Research Group, à l'Université de Lausanne. En rendant impossible la surveillance ou les filatures numériques, TOR permet l'anonymat et d'avancer masqué dans l'Internet.»

Une fois sur TOR, pas de moteur de recherche. Sur TOR, on ne trouve que ce que l'on sait chercher: il faut directement taper l'adresse du site souhaité dans la barre d'adresse. Pourquoi? Pour comprendre ce point, il faut s'imaginer Internet comme un iceberg. La partie immergée, la plus connue, est celle où nous avons l'habitude d'aller et dont les pages sont agrégées par des moteurs de recherche, comme Google. On y lit nos mails, on y achète des produits, on y fait des recherches… C'est l'Internet «surfacique», une petite partie d'Internet.

Sous la surface, on trouve le Web profond, qui contient les pages non indexées par les moteurs de recherche parce qu'elles sont mal conçues, non reliées, protégées par leur créateur… C'est le même Internet, mais en moins balisé.

Enfin vient le dark Web, ou plutôt les dark Nets, c'est-à-dire un ensemble de réseaux virtuels privés et décentralisés, constitués par des internautes qui se connectent entre eux.

Comment donc trouver une arme quand on n'y connaît rien? En récupérant des adresses de sites sur des forums, entre initiés. Ou grâce à des annuaires collaboratifs, référençant des adresses sous forme thématique, comme The Hidden Wiki (le «wiki» caché). Voulez-vous acheter un passeport? Rendez-vous à telle adresse. Des armes, de la drogue? Ce sera par là. Ainsi, on peut rapidement trouver un passeport français pour 600 € ou un pistolet SIG Sauer de calibre 9 mm pour 790 €.

Concrètement, pour acheter sur le dark Net, il a fallu à peine plus de deux clics: rechercher des adresses sur un annuaire, télécharger TOR, le lancer puis rentrer l'adresse dans la barre de navigation.

De là à acheter le produit, il reste encore quelques pas… Sur le dark Net en effet, les prix sont donnés en euros, mais les achats se font en bitcoins, une monnaie virtuelle et chiffrée, échangée entre deux ordinateurs. Datant de 2009, ce système fonctionne sans les États et sans les banques. Il est possible d'acheter ou de vendre des bitcoins contre des devises ayant cours légal, sur des plates-formes en ligne. Payer en bitcoin permet donc d'effectuer des transactions de personne à personne dans le monde entier, sans intermédiaire et à moindres frais. Ces échanges sont publics mais anonymes. Une fois son porte-monnaie approvisionné, il reste à se créer un compte client, comme sur eBay ou Amazon.

Mais attention, comme sur le Web surfacique, les escroqueries prolifèrent: sans régulation, ni contrôle, difficile de savoir si l'on peut faire «confiance» à un vendeur. De plus, les adresses changent sans arrêt, pour des raisons pratiques, techniques ou de sécurité, les rendant rapidement obsolètes.

Au final, le dark Web reste donc le domaine des initiés et des mafieux. D'ailleurs, alors qu'Internet compte cinq milliards d'utilisateurs, TOR en compterait deux millions quotidiens. Parmi eux, plusieurs profils. Il y a, bien sûr, les délinquants, trafiquants, hors-la-loi, parfois les mêmes que l'on retrouve dans le monde réel. Pour eux, Internet est un «facilitateur de la performance criminelle», selon Solange Ghernaouti: «Internet reflète notre réalité sociale, économique, politique et criminelle, poursuit-elle. Il n'est ni pire ni meilleur, mais contribue à faciliter certaines actions, y compris le passage à l'acte criminel du fait de la dématérialisation – on agit caché derrière un écran – à distance.»

Mais on trouve aussi sur le dark Net tous ceux qui veulent communiquer à l'abri des regards, les «internautes soucieux de préserver leur vie privée et leur intimité numérique ou les cyberdissidents à des régimes non démocratiques», poursuit le professeur. Tout un volet positif du dark Net, mais dont on parle beaucoup moins.

———

LES MOTS POUR COMPRENDRE

Internet représente un réseau de télécommunication international reliant des ordinateurs à l'aide du protocole TCP/IP. Il sert de support à la transmission de données: pages Web, courriels, fichiers informatiques.

Une adresse IP (Internet Protocol) est un numéro d'identification attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Une adresse IP est un numéro unique permettant à un ordinateur de communiquer dans un réseau.

Un moteur de recherche est un site Internet régi par une application sur lequel, en entrant des mots-clés, on obtient une liste de sites correspondant à la demande. Exemple: Google.

Un réseau virtuel privé est un passage ou un lien qui permet d'ouvrir un réseau local vers l'extérieur et de le connecter à un autre réseau local, grâce à une connexion Internet et avec une sécurité optimisée.

Le wiki est une application Web participative dont les internautes peuvent modifier les contenus.

Le terme bitcoin (de l'anglais « bit », unité d'information binaire, et « coin », pièce de monnaie) désigne à la fois un système de paiement virtuel et l'unité de compte utilisée par ce système.

Le chiffrement est une technique d'écriture en langage crypté ou codé. C'est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant de clés.

Réagissez à cet article

Source : http://www.la-croix.com/Ethique/Sciences-Ethique/Sciences/La-face-cachee-du-dark-Web-2015-12-08-1390141

L’agence météorologique australienne victime d’une cyber-attaque chinoise

L’agence météorologique australienne victime d’une cyber-attaque chinoise

---

L’équivalent australien de Météo France aurait été frappé par une cyber-attaque émanant de Chine. La faille serait très importante, impacterait jusqu’au ministère de la Défense australien, et coûterait plusieurs millions de dollars à réparer.

Le Bureau of Meteorology (BOM), l’agence nationale de météorologique australienne, a souffert d’une cyberattaque « massive »,rapporte la Australian Broadcasting Corporation le 2 décembre. D’une ampleur sans précédent en Australie, elle a été attribuée au gouvernement chinois par l’un des représentants gouvernementaux avec lequel la chaîne d’information s’est entretenue.

Le BOM héberge entre autres un centre de calcul à haute performance baptisé Solar, construit par Oracle sur la base d’une architecture Fujitsu. Outre le BOM, il est utilisé par de nombreuses agences gouvernementales australiennes, y compris le département de la Défense. D’après ce même représentant, sécuriser la faille de sécurité qui a permis cette attaque coûtera plusieurs millions de dollars.

Le gouvernement australien s’est refusé à confirmer l’information officiellement. La Chine de son côté nie toute responsabilité et juge les accusations sans fondement.

Réagissez à cet article

Source : http://www.usine-digitale.fr/article/l-agence-meteorologique-australienne-victime-d-une-cyber-attaque-chinoise.N368378

Les tendances 2016 en cyber-sécurité

Les tendances 2016 en cyber-sécurité

Comme la plupart des professionnels de la sécurité informatique, je souhaite vraiment que mes prédictions ne se réalisent pas. Je préférerais que les entreprises ne soient ni piratées ni victimes de failles. Mais en prédisant la prochaine vague de menaces, nous espérons aider les entreprises à rester au fait de l'évolution des tactiques et des méthodes que les criminels vont utiliser pour les cibler. Voici dix menaces et tendances que nous devrions constater au cours de 2016 en matière de sécurité informatique.

Si une semaine peut sembler longue en politique, comme l'a observé l'ancien Premier ministre britannique Harold Wilson, une année dans le domaine de la cyber-sécurité peut ressembler à une éternité. Malgré les changements rapides, beaucoup de choses restent cependant constantes. Les trois principales menaces prévues par Check Point pour 2015 étaient la croissance rapide des logiciels malveillants inconnus, les menaces mobiles et les vulnérabilités critiques dans les plates-formes couramment utilisées (Android, iOS et autres). Ces prédictions se sont pleinement réalisées et ces menaces continueront certainement de poser nombreux problèmes. Le jeu du chat et de la souris qui a caractérisé la cyber-sécurité au cours des dernières années se poursuit. Les pirates tentent de trouver sans cesse de nouvelles manières d'attaquer les réseaux, comme le montrent les failles de cette année chez Anthem, Experian, Carphone Warehouse, Ashley Madison et TalkTalk.

Logiciels malveillants « sniper »
Les plus grandes failles de 2016 seront le résultat de logiciels malveillants conçus sur mesure pour franchir les défenses d'entreprises spécifiques, telles que lors des attaques menées contre TV5 Monde. Les attaques génériques à champ large continueront de menacer les utilisateurs individuels et les petites entreprises, et les pirates amélioreront leurs méthodes d'attaque contre les grandes entreprises qui disposent de postures de sécurité plus sophistiquées. Ils utiliseront des méthodes de phishing plus approfondies et plus sophistiquées, et d'autres astuces d'ingénierie sociale pour accéder aux systèmes et aux données qu'ils souhaitent.

Les terminaux mobiles en 1ère ligne des attaques
Le nombre d'attaques mobiles continue d'augmenter à mesure que les appareils mobiles prennent place dans l'entreprise et offrent aux pirates un accès direct et potentiellement lucratif aux données personnelles et professionnelles. D'après une étude que nous avons menée en 2015, 42% des entreprises ont subi des incidents de sécurité mobile leur coûtant plus de 200 000 €, et 82% s'attendent à une augmentation du nombre d'incidents. Cette année a également été le témoin de l'émergence de plusieurs vulnérabilités mobiles critiques, notamment Certifigate impactant des centaines de millions d'appareils Android, et XcodeGhost – première infection malveillante à grande échelle ciblant des appareils Apple iOS non jailbreakés. Nous nous attendons à d'importantes vulnérabilités mobiles similaires l'année prochaine.

La bataille contre les menaces les plus dangereuses
Dans la bataille continue entre les pirates et les professionnels de la sécurité, les agresseurs déploient des variantes personnalisées de logiciels malveillants existants et d'attaques encore inconnues (« zero-day ») de plus en plus sophistiquées, capables de contourner la technologie de sécurité traditionnelle. Ces nouveaux vecteurs d'attaque exigent des solutions plus proactives et plus avancées pour stopper ces logiciels malveillants. Des innovations comme le sandboxing au niveau du CPU, capable d'identifier les menaces les plus dangereuses avant qu'elles ne parviennent à échapper à la détection des outils traditionnels et infecter les réseaux, seront plus que jamais nécessaires en 2016 pour faire face à ces nouvelles menaces.

Les infrastructures critiques plus que jamais en ligne de mire
En décembre 2014, une aciérie en Allemagne a été frappée par des pirates qui ont réussi à accéder au réseau de production de l'usine et causer des dommages « massifs ». Le département américain de la sécurité intérieure a découvert que le Trojan « Havex » était parvenu à compromettre les systèmes de contrôle industriel de plus de 1 000 entreprises du secteur de l'énergie en Europe et en Amérique du Nord. Les cyber-attaques menées contre des services publics et des processus industriels clés se poursuivront, à l'aide de logiciels malveillants ciblant les systèmes SCADA qui contrôlent ces processus. Comme ces systèmes de contrôle sont de plus en plus connectés et offrent une surface d'attaque plus étendue, une meilleure protection sera nécessaire pour les défendre. Ces risques sur les infrastructures critiques sont particulièrement sensibles dans un contexte de menaces terroristes accrues.

Les objets connectés : futur terrain de jeu des hackers ?
L'Internet des objets en est encore à ses balbutiements, et il est peu probable qu'il ait un fort impact en 2016. Néanmoins, les entreprises doivent réfléchir à la manière dont elles peuvent protéger les appareils intelligents et se préparer à une plus vaste adoption de l'IoT. Les utilisateurs doivent se demander « où leurs données sont transmises » et « ce qui se passerait si quelqu'un mettait la main sur ces données ». L'année dernière, nous avons découvert une faille dans des routeurs équipant des TPE dans le monde entier, qui pourrait permettre à des pirates de les détourner pour lancer des attaques sur tous les appareils qui leur sont connectés. Nous nous attendons à plus de vulnérabilités similaires dans les appareils connectés.

Les wearables c'est beau … mais pas très sécurisé !
Les wearables tels que les montres intelligentes font leur entrée dans l'entreprise, présentant de nouveaux risques et défis pour la sécurité. Les données stockées dans les montres intelligentes et les autres appareils personnels intelligents sont vulnérables et pourraient même être utilisées par des pirates pour capturer de l'audio et de la vidéo via des Trojans d'accès à distance. Les entreprises qui autorisent l'utilisation de ces appareils doivent assurer leur protection via des mots de passe et des technologies de chiffrement renforcées.
Trains, avions et véhicules connectés… autant de portes d'entrée pour les hackers !

2015 est l'année de l'émergence du piratage de véhicules : leurs logiciels embarqués sont détournés afin de prendre le contrôle des véhicules. En juillet, Fiat Chrysler a rappelé 1,4 millions de véhicules Jeep Cherokee aux États-Unis après que des chercheurs aient découvert qu'ils pouvaient être piratés via le système de divertissement connecté. Avec plus de gadgets et de systèmes connectés que jamais dans les véhicules modernes, nous devons protéger ces systèmes. Il en va de même pour les systèmes complexes des avions de ligne, des trains et autres formes de transport public.

Véritable sécurité pour les environnements virtuels
La virtualisation a été rapidement adoptée par les entreprises au cours des dernières années, que ce soit via SDN, NFV ou le Cloud. Les environnements virtualisés sont complexes et créent de nouvelles couches réseau. C'est seulement maintenant que nous comprenons réellement comment protéger ces environnements. Lorsque les entreprises migrent vers des environnements virtualisés, la sécurité doit être conçue dès le départ pour offrir une protection efficace.

Nouveaux environnements, nouvelles menaces
2015 était également l'année du lancement de plusieurs nouveaux systèmes d'exploitation, tels que Windows 10 et iOS 9. La majeure partie des attaques menées contre les entreprises ces dernières années ciblaient Windows 7, en raison de la faible adoption de Windows 8. Mais avec Windows 10 et son offre de téléchargement gratuit, les cybercriminels vont donc tenter d'exploiter ce nouveau système d'exploitation. Ses mises à jour sont plus fréquentes et les utilisateurs maîtrisent moins son environnement.

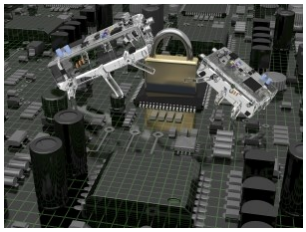
La consolidation de la sécurité pour la simplifier !
Pour se protéger contre les menaces multiformes, les professionnels de la sécurité sont susceptibles de se tourner vers des solutions d'administration centralisée de la sécurité. Les grandes entreprises qui possèdent pléthore de différents produits de sécurité sur leur réseau verront la consolidation comme un moyen de réduire à la fois coût et complexité. La multitude de solutions et de produits individuels devient rapidement ingérable et peut effectivement entraver la sécurité plutôt que l'améliorer. La consolidation de la sécurité fournit un moyen efficace de réduire la complexité afin que les nouvelles menaces ne s'égarent pas entre les mailles des différents systèmes.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-cyber-securite-en-2016-Check,20151204,58072.html

---

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