Le Sénégal lutte toujours plus contre la cybercriminalité

	Le Sénégal lutte toujours plus contre la cybercriminalité

Le Sénégal veut se doter de moyens efficaces pour lutter contre la cybercriminalité. C'est ce qu'a déclaré ce matin, le ministre des Postes et des Télécommunications, lors de la cérémonie d'ouverture d'un panel dédié à ce fléau.

Cette rencontre contre intervient un an après que le Sénégal et le royaume des Pays-Bas ont lancé à la Haye, une initiative internationale sur la sensibilisation des Etats et des différents acteurs sur la question de la cybersécurité », a déclaré Yaya Abdoul Kane.

Selon lui, cette plateforme est venue à son heure puisqu'elle peut permettre de doter les pays africains et les experts, d'espace «pour échanger sur les expériences réussies et les bonnes pratiques en matière de cybersécurité. Nous pensons, après cette réflexion, pouvoir avoir des éléments sur lesquelles nous allons pouvoir nous baser pour affiner notre stratégie nationale sur la cybersécurité», révèle-t-il.

Pour avoir de bons résultats dans cette lutte, le Sénégal compte prendre les devants. Et c'est dans ce sens, informe le ministre des Postes et des Télécommunications, que « la formation des magistrats, mais également la création au niveau de la Police d'une brigade spécialisée en cybersécurité», a commencé.

Mais notre pays ne compte pas en rester là puisque : «qu'il est aujourd'hui opportun de renforcer ce dispositif et d'arriver à avoir une stratégie nationale sur la cybersécurité, mais aussi d'arriver à l'harmonisation d'un cadre juridique et règlementaire au niveau sous régional, voir international, pour une meilleure prise en charge de la question», conclut-il… [Lire la suite]

Source : *Lutte contre la cybercriminalité: Le Sénégal au premier rang*

Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable

	Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable par les anti-virus

Les attaques ransomwares ne baissent pas. Après avoir usurpé des avocats, des comptables, des PME, des mairies, FREE, voici le courriel piégé aux couleurs d'Orange. Ne cliquez surtout pas sur la pièce jointe.

Le courriel s'invite dans votre boites à mails avec comme objet : « ***Votre demande d'assistance*** » ; « ***Votre assistance Orange*** » ; « ***Votre assistance Orance Business***« . La missive pirate indique qu'une anomalie lors d'un prélèvement oblige le lecteur internaute à lire le fichier joint, un PDF piégé baptisé « ***Montant du mois*** » ou encore « ***Montant de la facture***« . Un piège qui, heureusement, est plutôt mal réalisé pour les internautes avertis. Il peut, cependant, piéger les plus curieux. La cible étant clairement les entreprises, une secrétaire, un comptable ou un responsable n'ayant pas vraiment le temps de lire autrement qu'en « Z » sera tenté de cliquer.

Au moment de l'analyse des fichiers, aucun antivirus n'avait la signature de la bestiole en mémoire. **A noter qu'un antivirus, face à ce genre d'attaque ne peut pas grand chose. Chaque mail et fichier joint portent en eux une signature (identification) unique et différente…** [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Attaques ransomwares aux couleurs d'Orange – ZATAZ*

Les établissements scolaires également victimes de ransomwares

Après les hôpitaux, les ransomwares s'attaquent de plus en plus aux établissements scolaires. Retour sur plusieurs cas aux Etats-Unis.

Les ransomwares sont devenus la plaie des responsables sécurité des entreprises ou des administrations. On peut se remémorer le témoignage du RSSI de l'AFP qui en a fait l'expérience. Le secteur hospitalier a été particulièrement touché avec différents exemples. Le plus symptomatique est le Hollywood Presbyterian Medical Center de Los Angeles qui a été obligé de payer 17 000 dollars en bitcoin pour retrouver l'usage de son réseau.

Certains payent la rançon

Après les hôpitaux, les ransomwares s'intéressent à une autre cible : les écoles. Plusieurs cas ont été recensés aux Etats-Unis. En février dernier, plusieurs écoles primaires du Horry County en Caroline du Sud ont été victimes d'un rançongiciel qui a bloqué 25 serveurs. Immédiatement après avoir été alertée par les enseignants, l'équipe IT a débranché les serveurs affectant ainsi les services en lignes des écoles. Après enquête, la porte d'entrée du malware était un vieux serveur non mis à jour. Toujours est-il que les responsables de l'école ont se sont vus réclamer 0,8 bitcoin par ordinateur soit un total de 20 bitcoins (environ 7600 euros). Malgré l'aide du FBI, le conseil d'administration du campus a décidé de payer la rançon demandée.

D'autres non

D'autres ont décidé de ne pas payer la rançon comme dans le cadre du Oxford School District dans le Mississipi. En février dernier aussi, ce réseau de 8 campus a été infecté par un rançongiciel réclamant environ 9000 dollars pour un retour à la normal. Le superintendant de l'établissement, Brian Harvey, a préféré ne pas payer et s'est concentré sur la récupération des données. Dans un entretien accordé à HottyDotty, il précise que « nous avons restauré à partir d'une sauvegarde ». Mais les dégâts étaient importants. « Je ne sais pas combien de données nous avons perdu. Je peux dire que nous avons perdu la plupart des serveurs Windows. La chose la plus importante a été de tout effacer et de tout réinstaller depuis la sauvegarde. » L'attaque a privé les établissements d'Internet pendant plus d'une journée. Les 4 premiers jours après l'attaque ont été focalisés sur la récupération du système des carnets de notes des élèves. D'autres applications ont souffert comme les reporting ou le recrutement des agents. Au final, deux semaines ont été nécessaires pour tout remettre à peu près d'aplomb : les sites web, la gestion de la cafeteria, ainsi que des plateformes pour l'éduction comme PowerSchool et Schoology.

Les parents d'élève s'inquiètent

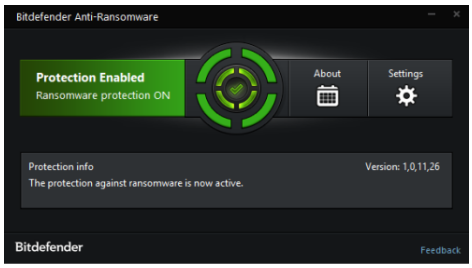
Autre affaire, le Texas School District qui gère une vingtaine d'établissements. Un ransomware a infecté le réseau, provoquant le blocage de plusieurs fichiers. La direction du district s'est voulue rassurante en expliquant que seule une petite partie des informations est concernée par le blocage. Ce dernier porte néanmoins sur un volume de 2,5 To de données. Les responsables ont choisi de ne pas payer la rançon demandée par les cybercriminels. « Nous avons réussi à effacer les fichiers chiffrés et à réinstaller données à partir d'une sauvegarde », précise un porte-parole du district. Un cas similaire à celui du Mississipi qui inquiète les parents d'élèves. « Ils [NDLR les établissements] détiennent des actes de naissance, des numéros de sécurité sociale ou des données médicales comme les vaccins », souligne une des parents d'élèves.

En France, aucun cas n'a été relevé ou publié sur des expositions à des ransomwares. Les écoles, universités et autres établissements scolaires font partie de cibles privilégiés par les cybercriminels. Obsolescence des parcs informatiques, système IT peu mis à jour, les pirates se ont trouvé un terrain de jeu grandeur nature pour tester et peaufiner leurs attaques. Les sommes demandées restent modestes, un signe selon les spécialistes pour reconnaître le degré de résistance des victimes à payer la rançon. En tout cas, les exemples américains doivent alerter les établissements bancaires européens et français sur les risques des ransomwares… [Lire la suite]

Réagissez à cet article

Source : *Les ransomwares prennent le chemin des écoliers*

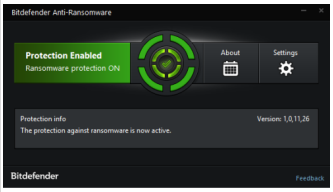
Bitdender met à disposition un outil gratuit de protection contre les Ransomwares



Bitdender met à disposition un outil gratuit de protection contre les Ransomwares

---

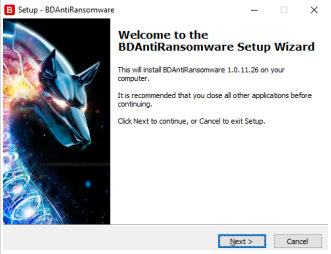
Bitdefender has just released a free tool that can protect against ransomeware viruses. Here is how to install it.



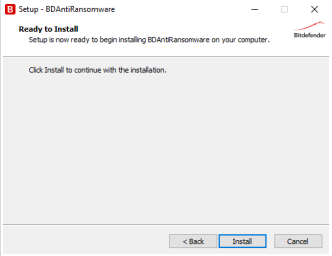
Hackers have been hitting everything from hospitals to police stations with Ransomeware viruses. Bitdefender has released a tool that could help fight it:
“Bitdefender anti-malware researchers have released a new vaccine tool which can protect against known and possible future versions of the CTB-Locker, Locky and TeslaCrypt crypto ransomware families.
“The new tool is an outgrowth of the Cryptowall vaccine program, in a way.” Chief Security Strategist Catalin Cosoi explained. “We had been looking at ways to prevent this ransomware from encrypting files even on computers that were not protected by Bitdefender antivirus and we realized we could extend the idea.”

Installation could not be easier

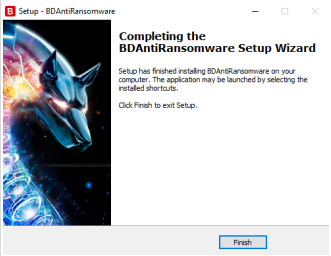
1. Download the file:
https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/
2. Run it:



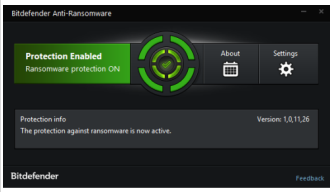
3. Click Next, and then install:



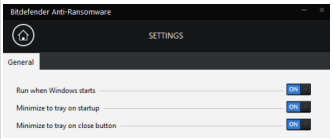
4. And then Finish



And that is it!



How easy was that?
If you want you can change the settings for the program. You may want to set it to “minimize on startup” and “minimize to tray on close”:

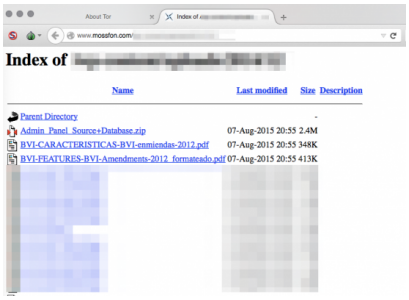


But it is pretty much an install and forget about it type app, no fuss, no muss.
Bitdefender has always been one of my favorite anti-virus programs, and this is a handy tool to have.
Check it out!

Réagissez à cet article

Source : *How to install Bitdender’s free Ransomware Protection Tool | CYBER ARMS – Computer Security*

#PanamaPapers : Les failles informatiques de Mossack Fonseca…

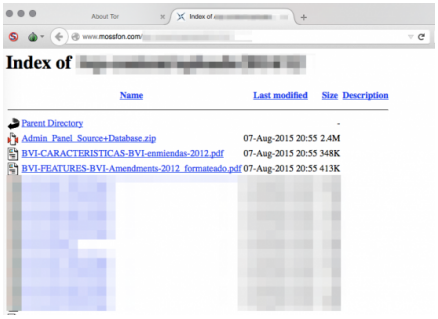


#PanamaPapers : Les failles informatiques de Mossack Fonseca…

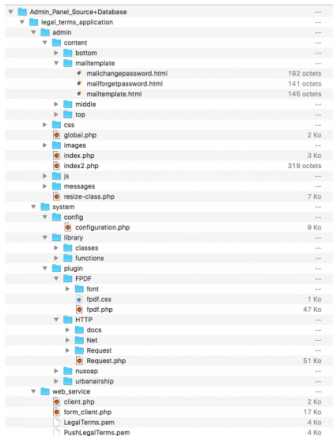
Un internaute vient de nous mettre sous le nez quelques éléments très, très … dur de trouver un qualificatif adapté. On se doutait bien en jetant un bref coup d'œil que le cabinet d'avocats panaméens avait une fâcheuse tendance à faire n'importe quoi, n'importe comment.
On peut également toujours spéculer sur l'origine de la fuite mais là n'est pas le problème, pour tout vous dire, l'origine de la fuite, on s'en fout, c'est la masse de données qui parle, et ce sont ces données qui sont importantes. Nous ne sommes évidemment toujours pas en mesure d'affirmer d'où vient la cette énorme fuite, mais comme nous le sentions, en collectionnant de si mauvaises pratiques, Mossack Fonseca s'assurait à plus ou moins long terme un drame.

Le WTF du jour

Aujourd'hui… la sauvegarde d'une application interne et d'un jeu de données, probablement sensibles, sauvegardés dans un répertoire public du site web vitrine de la société :

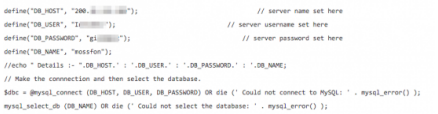


Et l'adresse IP internet du serveur de stockage des documents



La structure de l'application et son fichier de configuration
Et maintenant, admirez la complexité du password :

Rien de tel que de choisir le même mot de passe que le nom d'utilisateur et de base de données… et SURTOUT ne rien chiffrer, des fois qu'on oublierait un mot de passe si complexe.
… et évidemment



La base de données SQL est probablement un jeu de données tests qui est aussi sauvegardée au même endroit :

… oui tout ça accessible depuis un WordPress qui n'est pas à jour, installé sur un Apache mal configuré. …
… [Lire la suite]

Réagissez à cet article

Source : *PanamaPapers : Mossack Fonseca une incroyable bourde ? : Reflets*

WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

C'est peut-être l'absence de prise en compte de patchs de sécurité pour un plug-in WordPress et pour le CMS Drupal qui aurait permis de récupérer chez Mossack Fonseca les fameux Panama Papers qui font trembler le monde de la finance.

La fuite massive des documents de Mossack Fonseca, le cabinet panaméen qui gère des compagnies offshores, n'a pas fini de faire parler d'elle. Les 11,5 millions de documents contenus dans les 2,6 To de données – les fameux Panama Papers – ont déjà ébranlé de nombreuses sociétés et les sphères politiques, poussant par exemple le Premier ministre de l'Islande à démissionner. Mais comment ces données ont-elles été obtenues ?

NÉGLIGENCE INFORMATIQUE

De nombreuses questions demeurent concernant l'origine de la fuite qui provient d'une source anonyme. Mais beaucoup s'accordent sur le fait que la sécurité informatique a été négligée par Mossack Fonseca, ce que le cabinet avoue à demi mots en portant plainte pour piratage informatique.

Dans un mail qu'il ne fallait pas prendre pour un poisson d'avril, le cabinet avait expliqué à ses clients dès le 1er avril qu'il avait été victime d'une « brèche non autorisée de [son] serveur mail », comme le montre une copie publiée par Wikileaks le 3 avril. Bien sûr, les réactions sur Twitter ne se font pas fait attendre, amusées par la date d'envoi du mail et par l'absence de chiffrement des courriers électroniques de la part d'une entreprise qui met en avant « ses prestigieux services en ligne », comprenant « un compte sécurisé qui vous permet d'accéder n'importe où aux informations de votre société ».

DE L'IMPORTANCE DE METTRE À JOUR DRUPAL ET WORDPRESS

De récentes informations corroborent la thèse du piratage, qui aurait pu être facilitée par des vulnérabilités au sein des CMS utilisés par Mossack Fonseca, à savoir les gestionnaires de contenus Drupal et WordPress.

Comme le rapporte Forbes, le portail client du cabinet fait tourner une vieille version de Drupal (7.23). Or cette version est antérieure à un patch de sécurité qui corrigeait une énorme faille à partir de la version 7.32. Dans une notice de sécurité, Drupal allait jusqu'à recommander une nouvelle installation aux utilisateurs n'ayant pas mis à jour immédiatement après la sortie du correctif.

Il se peut donc qu'un attaquant ait exploité cette faille durant les deux années pendant lesquelles le cabinet n'a pas mis à jour sa version du CMS. Mais d'autres experts en informatiques ont découvert une autre porte qui aurait pu permettre à un hacker d'entrer dans le système.

Si le portail client du cabinet est sous Drupal, le site principal est lui sous WordPress. L'entreprise Wordfence, spécialisée dans la sécurité de l'omniprésent gestionnaire de contenus, a remarqué que l'installation WordPress utilisait une ancienne version du plugin Revolution Slider, connue pour présenter une faille sérieuse.

La version 3.0.95 de Revolution Slider (et les versions antérieures) contiennent en effet une vulnérabilité qui permet à un assaillant d'envoyer un fichier sur le serveur web sans avoir à s'identifier. L'entreprise note qu'un attaquant aurait donc pu prendre le contrôle du serveur sur lequel se trouvait l'installation WordPress… Le même serveur qui hébergeait les très précieux e-mails du cabinet.

En l'occurrence, rien ne prouve que les failles au sein des installations WordPress et Drupal du cabinet aient facilité la fuite des données. Dans la mesure où les journalistes n'ont pas rendu publics les documents, il sera d'ailleurs difficile de déterminer d'où ils proviennent. De son côté, le cabinet affirme qu'il s'agirait d'une attaque effectuée depuis l'étranger, écartant par la même toutes idées de fuites internes.

… [Lire la suite]

Source : *Panama Papers : des WordPress et Drupal mal gérés à l'origine d'un piratage ? – Tech – Numerama*

Adobe alerte sur une (nouvelle) faille critique dans Flash

Adobe alerte sur une (nouvelle) faille critique dans Flash

Adobe publie une notification de sécurité signalant la présence d'une vulnérabilité dans le format Flash. Une solution provisoire est proposée pour réduire les risques, en attendant la publication du patch.

Les raisons de détester Flash ne manquent pas. Depuis des années, le format conçu par Adobe fait l'objet de vives critiques tout à fait justifiées : de la lourdeur du logiciel à l'intégration médiocre avec le web, en passant par les soucis d'interopérabilité et le fait qu'il s'agisse d'une technologie propriétaire, Flash traîne une vilaine réputation. Pas étonnant que de nombreux acteurs souhaitent le voir disparaître.

Un format massivement utilisé mais bourré de défauts.

À cette liste déjà gratinée, il faut aussi inclure les problèmes de sécurité récurrents. Cela s'est encore vérifié récemment avec la découverte d'une vulnérabilité critique qui affecte toutes les versions du format, y compris la dernière disponible sur le site d'Adobe (numérotée 21.0.0.197). Et le pire, c'est que la brèche en question, identifiée sous le code CVE-2016-1019 est déjà exploitée.

« *Une vulnérabilité critique (CVE-2016-1019) existe dans Adobe Flash Player 21.0.0.197 et les versions précédentes dans Windows, Macintosh, Linux et Chrome OS. Une exploitation réussie pourrait provoquer un crash et permettre en théorie à un assaillant de prendre le contrôle du système affecté* », commente Adobe, qui confirme que la brèche est d'ores et déjà en cours d'utilisation.

Un correctif est attendu le 7 avril

« *Adobe est au courant des informations indiquant que CVE-2016-1019 est en train d'être activement exploité sur les systèmes utilisant Windows 7 et Windows XP avec Flash Player en version 20.0.0.306 et inférieur* ». Adobe explique qu'une solution permettant d'atténuer le problème est disponible avec la branche 21.0.0.182, de façon à empêcher l'exploitation de cette faille.

Les utilisateurs sont invités à mettre à jour sans tarder le logiciel Flash, même s'il n'existe pas encore de patch colmatant une bonne fois pour toutes cette brèche. En effet, l'usage d'une version réduisant l'exposition à un piratage à distance constitue déjà une protection supplémentaire. Adobe prévoit de publier dès demain, jeudi 7 avril, une mise à jour de sécurité qui réglera le problème … [Lire la suite]

Source : *Adobe alerte sur une faille critique dans Flash – Tech – Numerama*

Les terminaux de paiement cibles des pirates chasseurs de failles

	**Les terminaux de paiement cibles des pirates chasseurs de failles**

Avant le passage à des cartes à puce plus sécurisées, les cybercriminels sont à l'affût de failles dans les anciens systèmes de paiement aux États-Unis, pour continuer à voler des identifiants et des mots de passe. Vu les revenus qu'ils peuvent encore en tirer, l'enjeu reste assurément très attractif.

Selon FireEye, les cybercriminels redoublent d'efforts pour voler les informations des cartes de paiement sur les terminaux des détaillants américains avant la mise en place de nouveaux systèmes de défense.

L'an dernier, plus d'une douzaine de logiciels malveillants différents ciblant les TPV utilisés par de nombreux détaillants pour le traitement des paiements électroniques ont été découverts. Ces dernières années, les pirates ont réussi à pénétrer plusieurs fois dans ces systèmes, ciblant faiblesses ou vulnérabilités des logiciels afin d'extraire les informations qu'ils peuvent revendre sur le marché noir.

Depuis le mois d'octobre dernier, les détaillants endossent la responsabilité des transactions frauduleuses quand les paiements ne sont pas réalisés avec des cartes EMV. Celles-ci ont été dotées d'une puce électronique et bénéficient de meilleures sécurités pour protéger les données inscrites sur la puce. D'importants revendeurs qui ont été victimes de ces usurpations ces dernières années, comme le distributeur américain Target, ont amélioré leurs systèmes. Mais le coût et les retards de livraison des nouveaux systèmes certifiés ont ralenti la transition, laissant encore une marge d'action pour les cybercriminels. Au City Target sur Bush Street à San Francisco la semaine dernière, un achat de moins de 10$ effectué avec une carte à puce française n'a donné lieu à aucune vérification : ni code, ni signature et encore moins d'ID.

Des terminaux toujours très vulnérables aux Etats-Unis

Hier, un chercheur senior de FireEye spécialisé dans l'intelligence et les menaces, Nat Villeneuve, a écrit que plus d'une douzaine de logiciels malveillants de familles différentes ciblant les systèmes TP avaient été découverts l'an dernier. « Aux États-Unis, les criminels sont très actifs et cherchent par tous les moyens à infecter rapidement les systèmes de paiement avant que les détaillants américains n'achèvent la transition vers des systèmes plus sécurisés », a prévenu le chercheur. En réponse, les émetteurs de cartes et les banques ont amélioré leur capacité à identifier et à bloquer les transactions potentiellement frauduleuses. Mais la fraude reste suffisamment lucrative pour inciter les criminels à y consacrer encore beaucoup de ressources.

Nat Villeneuve parle d'un nouveau type de malware appelé POS Treasurehunt, qui vole les données des cartes de paiement à partir de la mémoire d'un ordinateur. « Le mode opératoire classique consiste à implanter Treasurehunt sur un système de TP, soit en utilisant des identifiants déjà volés, soit par force brute, c'est-à-dire en testant des séries de mots de passe courants pour accéder à des systèmes de paiement mal sécurisés », a-t-il écrit. Jusqu'ici, le champ d'action de Treasurehunt a été limité, signe que ses auteurs l'ont déployé sélectivement. Une chaîne de code du malware indique qu'il a été développé par un groupe dénommé Bears Inc. « Bears Inc. est très actif sur un forum dédié à la cybercriminalité souterraine liée à la fraude aux cartes de crédit », écrit le chercheur. « Sur ce forum, Bears Inc. a mis en vente des informations de carte de paiement volées ». Une autre chaîne de code comporte le message suivant : « Bonjour à Xylitol and Co ». Xylitol est le surnom d'un chercheur en malware bien connu, basé en France, qui anime un blog technique très suivi.

Une activité très rentable

Le piratage des TPV est toujours rentable pour les cybercriminels. On trouve facilement des forums de « carding » sur lesquels il est possible d'acheter des identifiants de carte de paiement. Le tarif de ces informations varie en fonction de la date limite d'utilisation de la carte et de la date où les données ont été volées. Les revenus tirés par les cybercriminels semblent tellement intéressants que les prix de ces informations ont même baissé.

Réagissez à cet article

Source : *Les pirates cherchent activement des failles dans les terminaux de paiement – Le Monde Informatique*

Des Box pourraient être piratées pour mener des attaques DDOS ?

Des Box pourraient être piratées pour mener des attaques DDOS ?

Eset a signalé l'activité d'un ver exploitant une faiblesse du protocole de gestion réseau distant Telnet implémenté dans les routeurs domestiques sous Linux. Des pirates peuvent s'en servir pour construire un botnet et lancer des attaques DDoS.

Construire des botnets à partir de routeurs, modems, points d'accès sans fil et autres terminaux réseaux ne nécessite pas d'exploits très sophistiqués. C'est le cas par exemple de Remaiten, un nouveau ver exploitant les routeurs domestiques sous Linux en tirant partie d'une faiblesse liée aux mots de passe du service de gestion réseau distant Telnet. Remaiten n'est autre que la dernière incarnation de bots Linux distribués spécialement conçus pour lancer des attaques par déni de service (DDoS). Lorsqu'il scanne des points d'entrée, Remaiten tente de se connecter à des adresses IP aléatoires sur le port 23 (Telnet) et, en cas de connexion fructueuse, il tente de s'authentifier en utilisant une combinaison de nom d'utilisateur et mot de passe en provenance d'une liste d'authentifiants communs, ont indiqué dans un billet de blog les chercheurs de l'éditeur en solutions de sécurité Eset. Ce n'est pas la première fois que les routeurs domestiques sont exposés à du piratage. On se souvient que l'année dernière 700 000 avaient été exposés à cause d'une faille NetUSB et plus récemment, des failles avaient été trouvées dans de nombreux routeurs WiFi Netgear et D-Link.

Scan de ports et fermeture du service Telnet pour se protéger

En cas de succès, le bot exécute plusieurs commandes pour déterminer l'architecture système avant de transférer un petit programme compilé pour permettre de télécharger l'ensemble des commandes de contrôle du botnet. Le ver dispose de versions pour jeux d'instructions mips, mipsel, armeabi et armebeabi. Une fois installé, il se connecte à un canal IRC et attend les commandes d'un pirate distant. Ce bot supporte une variété de commandes pour lancer différentes attaques DDoS et peut même scanner d'autres bots DDoS afin de les désinstaller.

Il est surprenant que de nombreux terminaux réseau utilisent encore Telnet pour la gestion réseau à distance plutôt que le protocole plus sécurisé SSH. Il est encore plus malheureux que de nombreux terminaux soient livrés avec le service Telnet ouvert par défaut. Afin de se protéger, il est recommandé d'utiliser un outil de scan de port en ligne et, dans le cas où le port 23 est ouvert, de fermer le service Telnet depuis la console d'administration web. Une possibilité qui n'est malheureusement pas offerte par tous les fournisseurs d'accès à leurs clients… [Lire la suite]

Réagissez à cet article

Utilisateurs de Tor

identifiés – Le FBI reste muet

Utilisateurs de Tor identifiés – Le FBI reste muet

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

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

Sceau FBI

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

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

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

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

Réagissez à cet article

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