Un Russe plaide coupable aux États-Unis pour plusieurs cyberattaques | Le Net Expert Informatique

Arrêté en 2012, un jeune homme de nationalité russe, âgé de 34 ans, a plaidé coupable de fraudes informatiques contre plusieurs grosses entreprises financières pour le vol massif de données bancaires et la perte de millions de dollars.

Vladimir Drinkman a plaidé coupable devant la Cour fédérale du New Jersey mardi 15 septembre et admis son implication dans ce que les autorités qualifient de plus grand système de piratage d'ordinateur jamais poursuivi aux États-Unis. Ces attaques ont compromis plus de 160 millions de numéros de carte bancaire et causé 300 millions de dollars de pertes.

Les faits remontent au moins à 2003 et selon la plainte du Département de la Justice, accompagné de 4 autres accusés, toujours en fuite, le jeune homme s'est introduit frauduleusement dans les ordinateurs de plusieurs entreprises, 16 au total, qu'ils surveillaient depuis des mois, dont celles du NASDAQ, du Dow Jones, de Visa, mais également de Carrefour SA.

Vladimir Drikman lors de sa première audience en février 2015
au cours de laquelle il a plaidé non coupable

Ils ont profité des vulnérabilités de la base de données SQL pour s'infiltrer dans les différents réseaux. Dans la plupart des cas, ils ont même laissé une porte dérobée ouverte (backdoor) derrière eux pour, au besoin, se réintroduire dans le réseau ultérieurement. Ils ont alors utilisé une faille de sécurité pour y glisser des « renifleurs » (analyseurs de paquets), des logiciels malveillants (malwares) qui collectaient et subtilisaient les données clients comme les numéros de sécurité sociale et autres informations d'identification en plus de celles des cartes bancaires trouvées dans les ordinateurs.

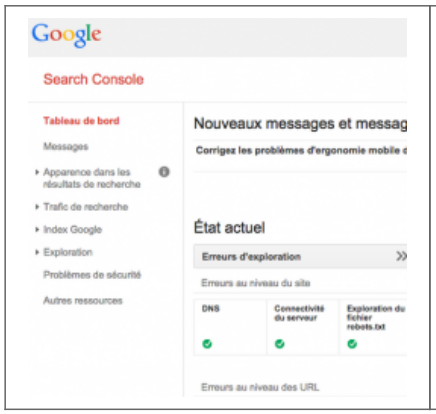
Afin de monétiser leur attaque, ils ont stocké l'ensemble des données volées dans des serveurs à l'étranger pour pouvoir les vendre ensuite au marché noir sur différents forums. Un souci d'anonymat rencontré jusque dans leur moyen de communication, chiffré, au cours de leurs opérations afin de brouiller les pistes pour qu'on ne remonte pas jusqu'à eux.

Pour le procureur une personne comme « Vladimir Drinkman, qui a les compétences pour s'introduire dans nos réseaux informatiques et l'envie de le faire, représente une menace pour le bien être de nos économie, notre vie privée et notre sécurité nationale ».

Arrêté en juin 2012 à Amsterdam puis extradé vers les États-Unis, Drinkman était depuis incarcéré dans l'attente de son procès. Si le jeune homme a plaidé non coupable dans un premier temps, il s'est ravisé depuis. Bien que 9 autres chefs d'accusation ont été rejetés, il encoure 30 ans de prison pour fraude électronique, mais son récent plaidé coupable pourrait atténuer la sentence. Sentence qui ne sera pas connue avant le 15 janvier 2016.

Source : http://www.journaldugeek.com/2015/09/16/russe-plaide-coupable-etats-unis-cyberattaques/
Par Elodie

Les pirates du SEO s’attaquent à Google Search Console | Le Net Expert Informatique



Les pirates du SEO s’attaquent à Google Search ConsoleInformatique

Le spécialiste en sécurité Sucuri alerte sur la recrudescence d'attaquants qui se font passer pour les véritables propriétaires de sites web sur le service Google Search Console afin de détourner le trafic vers des pages et des sites infectés. Ces pirates vont jusqu'à supprimer les webmasters légitimes de la liste des propriétaires identifiés des sites.

Il arrive de plus en plus souvent que des pirates ayant compromis des sites web s'identifient eux-mêmes comme l'un des propriétaires de ces sites dans la Search Console de Google, constatent les chercheurs de la société Sucuri, spécialisée dans la sécurité sur Internet. Dans certaines circonstances, cela permet à ces attaquants d'agir plus longtemps sans être détectés. Précédemment connu sous le nom de Webmaster Tool, le service Search Console permet aux administrateurs de sites web de voir et comprendre où se situent leurs sites dans les résultats du moteur de recherche. Au-delà de ce type d'analyses, il permet aux webmasters de proposer de nouveaux contenus à indexer et de recevoir des alertes lorsque Google détecte des malwares ou des problèmes de spam sur leurs pages web (des mots-clés répétés abusivement). C'est particulièrement important car les infections entraînent des pertes de trafic et de réputation. Les utilisateurs qui cliquent sur des liens de résultats de recherche conduisant vers des sites hébergeant des malwares ou du contenu spammé reçoivent des avertissements inquiétants jusqu'à ce que ces sites soient nettoyés par leurs propriétaires.
Sur les comptes utilisateurs de la Search Console, Google permet en fait à plusieurs personnes de se dire propriétaires d'un site. Cela n'a rien d'inhabituel puisqu'il y a généralement plusieurs intervenants. Les spécialistes des outils de recherche, notamment, sont souvent distincts des administrateurs de sites et tous utilisent les données de la Search Console dans leurs rôles respectifs. Il y a plusieurs façons de se faire identifier comme propriétaire, mais la plus simple consiste à charger un fichier HTML avec un code unique pour chacun dans le dossier racine du site. Or, de nombreuses failles qui permettent aux attaquants d'injecter du code malveillant sur les pages web leur ouvrent aussi des portes pour créer des fichiers sur les serveurs web sous-jacents. Ces pirates peuvent notamment exploiter des vulnérabilités pour s'identifier comme l'un des propriétaires du site dans Search Console en créant les fichiers HTML requis.

Les attaquants exploitent des techniques de BHSEO

De tels abus deviennent de plus en plus courants. Sucuri cite pour preuve les multiples posts publiés à ce sujet sur les forums par les propriétaires de sites. Dans l'un des cas signalés, un webmaster a trouvé plus de 100 « utilisateurs vérifiés » dans sa console, note l'expert en sécurité Denis Sinegubko dans un billet. De nombreux pirates utilisent des sites compromis pour créer de fausses pages, tromper le classement des résultats de recherche et diriger le trafic vers d'autres pages à contenu dupliqué, ce qui permet aux attaquants d'exploiter des techniques d'optimisation de type BHSEO (black hat search engine optimization).

Devenus propriétaires vérifiés sur des sites compromis, les pirates peuvent alors suivre tranquillement les performances de leurs campagnes BHSEO sur le moteur de recherche de Google. Ils peuvent aussi soumettre de nouvelles pages de spams à indexer plus rapidement plutôt que de devoir attendre que ces pages soient naturellement découvertes par les robots de recherche. Ils peuvent aussi recevoir des alertes de Google si les sites sont identifiés comme étant compromis et, pire encore, ils peuvent éjecter les propriétaires légitimes des sites du service Search Console.

Des notifications qui passent entre les mailles

Lorsqu'un utilisateur est dit « vérifié » pour un site, les propriétaires de ce site vont recevoir une notification par email de Google. Cependant, ces messages peuvent facilement passer à travers les mailles du filet. Par exemple, s'ils sont envoyés vers une adresse mail qui n'est pas utilisée très souvent, ou bien s'ils sont noyés au milieu d'autres notifications reçues lors d'une journée très chargée en messages, ou encore s'ils arrivent pendant une période de congés. Dans ces cas-là, si les propriétaires légitimes n'ont pas consulté ces notifications et pris immédiatement des mesures, les attaquants peuvent alors les enlever de la liste de vérification du service Search Console en supprimant purement et simplement les fichiers de vérification HTML du serveur. Cela ne déclenchera aucune notification vers les véritables détenteurs du site, souligne Denis Sinegubko, de Sucuri.

Par la suite, si Google détecte un site web compromis et alerte automatiquement ses propriétaires identifiés comme tels, seuls les attaquants recevront cette notification. Ils pourront alors enlever temporairement du site les portes dirigeant vers leurs faux sites avant d'adresser à l'équipe antispam de Google une requête pour faire débloquer le site dans les résultats de recherche. Après quoi, ils pourront tranquillement remettre leur doorways vers différentes adresses URL, explique le chercheur de Sucuri.

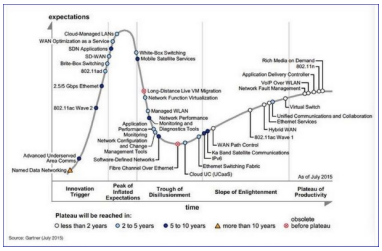
Utiliser les méthodes alternatives de Google pour s'identifier

Si les véritables propriétaires ne sont plus identifiés comme tels, cela leur prendra un certain temps pour se rendre compte de ce qui s'est produit. Il est même possible qu'ils ne s'en aperçoivent pas. Pendant ce temps, les pirates continuent à exploiter leurs sites à leurs propres bénéfices. Et même si les administrateurs légitimes repèrent les faux propriétaires, il n'est pas toujours simple de s'en débarrasser. Les chercheurs de Sucuri ont vu de quelle façon les attaquants procédaient quelquefois en s'appuyant sur des règles de réécriture des URL dans le fichier de configuration htaccess et en générant dynamiquement des pages. Dans ces cas-là, les robots de vérification de Google détectent les fichiers HTML requis même si ceux-ci n'existent pas sur le serveur et si les vrais administrateurs ne peuvent pas les trouver.

Pour se préparer à de telles attaques, les webmasters peuvent prendre diverses mesures, indique Denis Sinegubko dans son billet. En premier lieu, ils doivent s'assurer qu'ils sont bien « vérifiés » comme propriétaires sur tous leurs sites web (en incluant les sous-domaines) dans la Search Console, même s'ils n'utilisent pas souvent ce service. Il existe trois méthodes alternatives de vérification acceptées par Google : à travers un fournisseur de noms de domaine, via un code de suivi Google Analytics ou, encore, avec une portion de code JavaScript à coller dans les pages. Cela évitera que des pirates suppriment leurs propres « vérifications » simplement en détruisant les fichiers correspondants sur le serveur. Enfin, à chaque fois qu'ils reçoivent des notifications de « new owners » de la part de Google, les webmasters doivent impérativement les contrôler en détail. « Dans la plupart des cas, cela signifie qu'ils ont un accès complet à votre site », avertit Denis Sinegubko. « Il faut alors intervenir sur toutes les failles de sécurité et supprimer tous les contenus malveillants que les attaquants auraient pu créer sur votre site », pointe le chercheur de Sucuri.

Source :
http://www.lemondeinformatique.fr/actualites/lire-les-pirates-du-seo-s-attaquent-a-google-search-console-62333.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

2 à 3 ans nécessaires pour contrer les cyber-attaques | Le Net Expert Informatique



2 à 3 ans nécessaires pour contrer les cyber-attaques

La prévention des attaques sur les réseaux, jusqu'au cœur des entreprises, doit-elle redevenir une priorité dans les investissements ? Selon une récente étude du cabinet Gartner (*), seulement 40% des grandes organisations disposeront, en 2018, de plans de sécurité formels pour se prémunir contre les cyber-attaques particulièrement agressives. A ce jour, pratiquement aucune organisation n'aurait mis en place de dispositifs réellement efficaces.

Le 'Hypercycle' des tendances Networking et sécurité (Source : Gartner 07-2015)

La série récente d'attaques sur les réseaux (dont celle visant Sony) a mis en alerte les responsables IT, les incitant à se préoccuper désormais de détecter et de riposter plutôt que de bloquer puis de traiter les cyber-attaques.

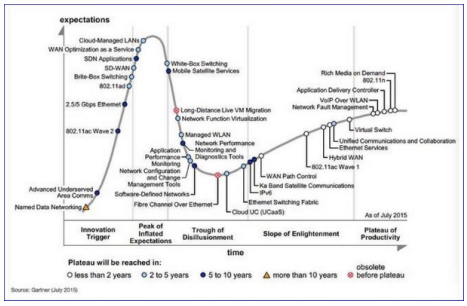
« Ce type d'attaques particulièrement virulent impose d'instituer de nouvelles priorités, de la part des 'CISO' (Chief information security officers – ou RSSI, responsables sécurité du système d'information) mais également de la part des responsables BCM (Business continuity management) », observe le rapport Gartner. De telles attaques, à ce point agressives, « peuvent causer des interruptions d'activité prolongées, capables de perturber gravement les opérations 'métier' ».

Des attaques très ciblées

Gartner définit ces attaques agressives comme étant des attaques ciblées de telle sorte qu'elles affectent de façon critique les opérations 'métier' internes. « Le but délibéré est de provoquer des graves dommages dans les activités de l'entreprise», explique un analyste. « Les serveurs peuvent être complètement arrêtés ou pilotés à distance, les données peuvent être effacées et la propriété intellectuelle peut être détournée via Internet par des 'hackers' malintentionnés ».

Les organisations victimes de tels assauts peuvent se retrouver sous la pression des médias en quête d'informations sur le sinistre. Et la réaction des autorités publiques ainsi que la diffusion de notes d'information rendue obligatoire vont accroître la visibilité d'une situation de chaos causée par de telles attaques.

Ces attaques peuvent exposer des informations internes critiques sur les médias sociaux, avec un enchaînement de conséquences bien plus embarrassantes que le vol de données personnelles ou la saisie de numéros de cartes bancaires. Les salariés peuvent ne plus être en mesure d'exercer normalement sur leur lieu de travail habituel, et cela, parfois pour une période de plusieurs jours voire de plusieurs mois.



Détecter d'abord puis riposter

Pour lutter contre ce type d'attaques, les RSSI devraient donc adopter une démarche non plus de blocage puis de détection des attaques, mais l'inverse: détecter d'abord puis répondre aux attaques.

« Éviter entièrement toute attaque dans une grande organisation complexe n'est tout simplement pas possible. C'est pourquoi, depuis quelques années, on met plus l'accent sur la détection et la riposte, car il se confirme que les nouveaux modèles d'attaque, avec des preuves d'impact évidentes, peuvent occasionner de graves sinistres », explique le rapport Gartner.

Des contrôles préventifs, à partir des pare-feu, logiciels anti-virus et solutions de gestion des vulnérabilités, ne suffisent plus comme objectif d'un plan de sécurité: « La réalité actuelle impose désormais de bien répartir les investissements entre les outils de détection et les dispositifs de riposte », constate Gartner.

Un nouvel examen des risques

La prolifération des terminaux mobiles connectés et l'internet des objets élargit le champ des cyber-attaques, ce qui exige plus de vigilance encore, plus de budget et un nouvel examen plus approfondi des risques. Il convient donc, en priorité, se défaire de ces dépendances technologiques, et d'annihiler sinon réduire l'impact de tels incidents techniques sur les process métier et sur le chiffre d'affaires.

Autre suggestion : les détenteurs d'informations doivent être responsabilisés sur la protection de leurs ressources ; ils doivent s'engager à prendre en considération les risques résultant des solutions 'métier'.

Avec l'arrivée des objets connectés, supposés toujours disponibles, de nouveaux incidents pourraient interrompre des transactions commerciales et à entamer la fidélité des clients.

Construire de nouveaux cas d'usage

L'heure est venue, estime Gartner, de construire de nouveaux cas d'usage sans oublier d'investir dans des dispositifs proactifs afin de prévenir ces nouvelles menaces.

« Il faut se projeter sur de nouvelles solutions assurant la gestion de la continuité d'activité ». Et le rapport de conclure: « La sécurité n'est pas un problème technique, traité par des spécialistes cachés quelque part dans le service informatique… Il faut dès aujourd'hui solutionner les problèmes qui peuvent arriver ».

La sécurité prédictive

Les grands fournisseurs du monde IT ont commencé à investir dans cette dimension prédictive de la sécurité. Ainsi, HP a fait l'acquisition de plusieurs sociétés spécialisées, comme ArcSight, Fortify, TippingPoint, Attala… Grâce aux technologies Big Data, il devient possible d'analyser en quasi temps réel les événements ou incidents qui peuvent s'amorcer, avant même qu'ils ne se propagent. C'est la phase de prévention de menaces potentielles, avant leur manifestation. Les nouveaux dispositifs sont le fruit de la synergie désormais possible entre des plateforme SIEM (Security information and event management) telles qu'ArcSight et la technologie IDOL d'Automy intégrant un moteur d'analyse Big data en temps réel. Les données de sécurité brutes peuvent être suivies en permanence et analysé à travers des modèles de comportement. Ceci permet de rendre visibles des menaces généralement perçues trop tardivement.

Depuis quelques mois, quantités d'autre solutions et services tirent parti de ces nouvelles possibilités technologiques, que le Gartner conseille d'examiner de près.

_ _ _

(*) Etude Gartner « Formal plans to address aggressive cyber-security business disruption attacks (02/2015, présentée à Londres ce 14/09/2015)

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/securite-2-a-3-ans-necessaires-pour-contrer-les-cyber-attaques-39825020.htm

La cybersécurité devrait devenir le point d’orgue de la coopération sino-américaine | Le Net Expert Informatique

La cybersécurité devrait devenir le point d’orgue de la coopération sino-américaine

Dans le cadre de la prochaine visite du président chinois Xi Jinping aux Etats-Unis, il est quasiment certain que la cybersécurité sera un sujet brûlant. En fait, en matière de protection de la cybersécurité, la Chine et les Etats-Unis, deux acteurs importants dans ce domaine, ont beaucoup à gagner à coopérer.

Il y a quelques jours, le représentant spécial de M. Xi, Meng Jianzhu, s'est rendu aux Etats-Unis. Les deux pays ont alors atteint un consensus important pour la lutte contre les crimes sur Internet. Les deux pays peuvent désormais coopérer davantage dans ce domaine.

La Chine et les Etats-Unis sont deux pays dotés de technologies Internet très développées, a indiqué M. Meng, ajoutant que dans le contexte des incidents fréquents et des menaces sécuritaires croissantes dans le cyberespace, il est très important que les deux pays renforcent la confiance mutuelle et la coopération dans la sphère de la cybersécurité.

Le consensus a envoyé un bon message: la cybersécurité peut devenir un domaine de coopération sino-américain au lieu d'une source de frictions.

Mais certaines agences américaines ainsi que certains médias ne cessent de parler des soi-disantes attaques chinoises sur Internet.

Le directeur des Renseignements nationaux américains, James Clapper, a déclaré que la Chine et la Russie représentent les menaces sur Internet les plus sophistiquées et que le cyber-espionnage chinois continue de viser un vaste domaine des intérêts américains. Des médias américains ont même dit que des entreprises et des individus chinois pourraient être sanctionnés pour leurs cyberattaques contre des cibles commerciales américaines.

Il est évident que ces remarques irresponsables et ces accusations sans fondement ne sont pas favorables aux relations bilatérales et empêcheront de trouver des solutions à ce problème.

La Chine ne cesse de dire qu'elle est contre toutes formes de cyberattaques et qu'elle les éliminera, car elle a été pendant longtemps une victime de ces activités illégales.

Face à la cybersécurité, nouveau problème touchant pratiquement le monde entier, la Chine a également prôné la coopération avec la partie américaine et tout autre pays afin de protéger la sécurité et son ordre pacifique.

La Chine a montré qu'elle était prête à exploiter le potentiel de la gouvernance d'Internet avec les autres pays, mais tout progrès majeur dans ce domaine dépend de l'action de Washington.

Si les Etats-Unis pouvaient faire preuve de sincérité et prendre d'autres vraies mesures concrètes pour protéger la cybersécurité aux côtés de la Chine, au lieu de porter des accusations sans fondement contre la Chine, les conséquences pour les relations bilatérales seraient positives et l'Internet serait meilleur.

Source : http://french.xinhuanet.com/2015-09/15/c_134627069.htm

Le Mali prépare la riposte face à la montée de la cybercriminalité | Le Net Expert Informatique

Le Mali prépare la riposte face à la montée de la cybercriminalité

Qu'il s'agisse de groupes étatiques ou non-étatiques, l'Internet représente aujourd'hui beaucoup plus de menaces sur la sécurité comme en témoignent les faux mails, les vols de numéros de cartes bancaires, la pédopornographie, le blanchiment d'argent, le trafic de stupéfiants, voire, les activités à des fins criminelles et terroristes. Les cyberattaques se jouent des frontières et des distances, sont anonymes, et il est très difficile d'identifier formellement le véritable attaquant.

Ces attaques peuvent être réalisées facilement, à bas coût et à très faible risque pour l'attaquant. Elles visent à mettre en péril le bon fonctionnement des systèmes d'information et de communication utilisés par les citoyens, les entreprises et les administrations, voire l'intégrité physique d'infrastructures essentielles à la sécurité nationale. D'où la nécessité d'une stratégie concertée de lutte contre le phénomène.
Avec l'organisation de ce colloque dont le maitre d'œuvre est l''Autorité Malienne de Régulation des Télécommunications/TIC et des Postes (AMRTP) accompagnée par l'Agetic, la Sotelma et Africa ITCs consulting, les autorités entendent apporter une réponse et une approche globale de lutte contre le phénomène. L'objectif du colloque est d'une part, d'informer et de sensibiliser les décideurs politiques et administratifs, les acteurs de télécommunication et des TIC, la société civile ainsi les médias sur l'impérieuse nécessité de la mise en place des dispositifs en matière de cyber sécurité et des mesures de lutte contre la cybercriminalité et d'autre part, d'apporter des réponses adéquates aux menaces.
A l'ouverture des travaux, le ministre Choguel Maïga a noté que les actions à mener pour enrayer les cybers menaces sont particulièrement difficiles, dans la mesure où l'on se trouve dans le domaine de l'immatériel, avec des techniques en constante et rapide évolution et que les sites Internet et les données auxquelles l'on accède proviennent souvent de serveurs hébergés dans d'autres pays. « Toutefois, malgré ces difficultés, une impérieuse nécessité d'agir nous incombe et notre action au Mali repose sur une conviction très forte : la liberté a, comme fondement, la sécurité. Cela suppose que, face à la cybercriminalité, nous ne pourrons pas garantir le plein exercice de la liberté des usagers et des citoyens qu'en nous en donnant les moyens adaptés », a indiqué le ministre qui a formulé le vœu que, lors du colloque, les décideurs politiques et administratifs, les acteurs des secteurs de télécommunications et des TIC, les acteurs de la société civile et les médias saisissent l'occasion pour se familiariser davantage avec le concept de cyber-menace et développer à travers des plans d'activités, une stratégie de cyber-sécurité.
Durant deux jours, les acteurs échangeront, avec les experts sur plusieurs thématiques comme le cyber crime de masse, le cyber crime ciblé, le terrorisme internet. Aussi, les participants vont passer au peigne le rôle du citoyen, des institutions et de l'Etat dans la lutte contre la cybercriminalité, l'état des lieux de la cybercriminalité au Mali ainsi le cadre réglementaire et opérationnel.
Rappelons que la cyber sécurité recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre les attaques. L'augmentation spectaculaire du niveau de sophistication et d'intensité des cyberattaques a conduit ces dernières années la plupart des pays développés à renforcer leur résilience et à adopter des stratégies nationales de cyber sécurité. Dans plusieurs pays, la prévention et la réaction aux cyberattaques ont été identifiées comme une priorité majeure dans l'organisation de la sécurité nationale.

Source : http://maliactu.net/mali-face-a-la-montee-de-la-cybercriminalite-le-mali-prepare-la-riposte-a-la-taille-des-enjeux/
Par Daniel KOURIBA

Implantation de malwares dans

les routeurs Cisco| Le Net Expert Informatique

	**Implantation de malwares dans les routeurs Cisco**

La firme de sécurité Mandiant, filiale de FireEye, a découvert que les firmwares de 14 routeurs d'entreprise de Cisco avaient été remplacés par des versions malveillantes permettant d'ouvrir des backdoors et de compromettre d'autres systèmes.

Remplacer le firmware d'un routeur par une version contaminée n'est plus du tout un risque théorique. Les chercheurs de la société Mandiant, spécialisée dans la sécurité informatique, ont détecté une véritable attaque ayant conduit à installer un faux firmware sur des routeurs d'entreprise dans quatre pays. Le logiciel implanté, désigné sous le nom de SYNful Knock, permet à des attaquants de disposer ainsi d'une porte dérobée, avec des accès à privilèges élevés, pour s'introduire dans les équipements affectés et y rester. La « backdoor » est en effet maintenue, même après un redémarrage du routeur. C'est un élément différentiant et inquiétant par rapport aux malwares que l'on trouve sur les routeurs grand public et qui disparaissent de la mémoire lorsque le périphérique est relancé.

SYNful Knock se présente comme une modification du système d'exploitation IOS (Internetwork Operating System) qui tourne sur les routeurs professionnels et les commutateurs de Cisco. A ce jour, les chercheurs de Mandiant l'ont découvert sur les routeurs ISR (Integrated Service Routeurs) modèles 1841, 8211 et 3825 que les entreprises placent en général dans leurs succursales ou qui sont utilisés par les fournisseurs de services réseaux managés.

Des experts de Mandiant mettent en garde contre de faux firmwares qui implantent des portes dérobées dans plusieurs modèles de routeurs Cisco : ISR 1841 (ci-dessus), 8211 et 3825. (crédit : D.R.)

Défaut ou vol de certificats d'administration

Filiale de la firme de cybersécurité FireEye, Mandiant a trouvé le faux firmware sur 14 routeurs, au Mexique, en Ukraine, en Inde et aux Philippines. Les modèles concernés ne sont plus vendus par Cisco, mais il n'y a aucune garantie que d'autres modèles ne seront pas ciblés à l'avenir ou qu'ils ne l'ont pas déjà été. Cisco a publié une alerte de sécurité en août avertissant ses clients sur de nouvelles attaques sur ses routeurs.

Dans les cas étudiés par Mandiant, SYNful Knock n'a pas été exploité en profitant d'une faille logicielle, mais plus probablement à cause d'un défaut de certificats d'administration ou via des certificats volés. Les modifications effectuées sur le firmware n'ont pas modifié sa taille d'origine. Le logiciel qui prend sa place installe une backdoor avec mot de passe ouvrant un accès Telnet à privilèges et permettant d'écouter les commandes contenues dans des packets TCP SYN (d'où le noom SYNful Knock). La procédure peut être utilisée pour indiquer au faux firware d'injecter des modules malveillants dans la mémoire du routeur. Toutefois, contrairement à la porte dérobée, ces modules ne résistent pas à un redémarrage du périphérique.

Des compromissions très dangereuses

Les compromissions de routeurs sont très dangereuses parce qu'elles permettent aux attaquants de surveiller et modifier le trafic réseau, de diriger les utilisateurs vers de faux sites et de lancer d'autres attaques contre des terminaux, serveurs et ordinateurs situés au sein de réseaux isolés. Généralement, les routeurs ne bénéficient pas du même degré d'attention que d'autres équipements, du point de vue de la sécurité, car ce sont plutôt les postes de travail des employés ou les serveurs d'applications que les entreprises s'attendent plutôt à voir attaqués. Les routeurs ne sont pas protégés par des utilitaires anti-malwares ni par des pare-feux.

« Découvrir que des backdoors ont été placées dans votre réseau peut se révéler très problématique et trouver un implant dans un routeur, encore plus », soulignent les experts en sécurité de Mandiant dans un billet. « Cette porte dérobée fournit à des attaquants d'énormes possibilités pour propager et compromettre d'autres hôtes et des données critiques en utilisant ainsi une tête de pont particulièrement furtive ». Dans un livre blanc, Mandiant livre des indicateurs pouvant être utilisés pour détecter des implants SYNful Knock, à la fois localement sur les routeurs et au niveau du réseau. « Il devrait être évident maintenant que ce vecteur d'attaque est vraiment une réalité et que sa prévalence et sa popularité ne feront qu'augmenter », préviennent les experts. A la suite de l'information diffusée par Mandiant, Cisco a lui aussi communiqué sur le sujet, en fournissant des explications complémentaires.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lemondeinformatique.fr/actualites/lire-des-malwares-implantes-dans-les-routeurs-cisco-62359.html?utm_source=mail&utm_medium=email&utm_campaign=LeNetExpert.fr
Par Lucian Constantin / IDG News Service (adapté par Maryse Gros)

Le Maroc abritera l’Africa Security Forum 2015 | Le Net Expert Informatique

	Le Maroc abritera l’Africa Security Forum 2015

Le Maroc accueillera les 12 et 13 octobre 2015, l'Africa Security Forum (Forum africain de sécurité). Il verra la participation de nombreux experts, de chercheurs, de spécialistes de la Défense et de la Sécurité africains, ainsi que leurs pairs, notamment européens et américains.

Organisée par le Think Tank Atlantis, en partenariat avec le Forum international des technologies de sécurité (FITS), basé à Paris, la rencontre, qui se tiendra à Casablanca, sera l'occasion pour les experts, de se pencher sur des problématiques liées à la sécurité, et ceci autour d'une plateforme de débats et d'échanges.
L'objectif d'Africa Security Forum est de mettre en présence les grands opérateurs publics et privés de 16 pays africains, les entreprises les plus innovantes et les experts des secteurs concernés par les thématiques génériques retenues pour cette édition 2015.
Le forum, offrira un cadre idéal pour discuter des questions relatives à la sûreté-sécurité, avec de larges champs d'expertise comme ceux de la défense, de la cyber-défense, de l'intelligence stratégique et de la sécurité industrielle. Selon le président d'Atlantis, Driss Benomar, le développement affiché par nombre de pays dans le monde est immanquablement confronté à des problèmes de terrorisme. Ce qui justifie l'urgence de renforcer la sécurité au niveau des frontières et de durcir les contrôles des flux commerciaux et des transports. « Nous sommes dans une conjoncture très importante et nous pensons que ce forum est une initiative nouvelle pour pouvoir échanger les expériences réussies des uns et des autres pour être efficaces à l'avenir », a-t-il estimé lors d'une conférence de presse, tenue ce vendredi 11 septembre à Casablanca et destinée à la présentation du programme d'Africa Security Forum.

Source :
http://www.financialafrik.com/2015/09/14/le-maroc-abritera-lafrica-security-forum-2015/

Russie: la Commission électorale attaquée par des hackers US | Le Net Expert Informatique

Russie: la Commission électorale attaquée par des hackers US

Le site officiel de la Commission électorale centrale (CEC) de Russie a repoussé une attaque informatique provenant d'une compagnie basée à San Francisco, annoncent les médias russes. Des élections de différent niveau se sont tenues dimanche 13 septembre en Russie.

Piratage massif: sanctions US imminentes contre des compagnies chinoises

La tentative de piratage a été enregistrée samedi soir, selon le chef de la CEC, Vladimir Tchourov. « Quelqu'un a essayé de pirater notre site et de substituer son contenu, avec un intensité de 50.000 requêtes par minute », a-t-il déclaré. Selon lui, cette tentative aurait rapidement été neutralisée.

La CEC a demandé aux organes compétents des Etats-Unis d'identifier et de punir les coupables.

Des élections régionales et locales se sont tenues dimanche 13 septembre en Russie. Près de la moitié des électeurs étaient appelés aux urnes. Les chefs de 24 régions russes, les députés de 11 parlements régionaux et 25 conseils municipaux ont notamment été élus.

Source : http://fr.sputniknews.com/russie/20150914/1016708817.html

Alerte : Un ransomware qui verrouille votre appareil en changeant le code PIN Android | Le Net Expert Informatique

Alerte : Un ransomware qui verrouille votre appareil en changeant le code PIN Android

La société ESET a récemment publié un rapport alarmant sur la prolifération des ransomwares sur les appareils mobiles, aux États-Unis pour la plupart. Ces derniers se font passer pour des applis pornos réclamant des permissions quelque peu douteuses. Une fois ces dernières accordées, votre appareil est tout simplement verrouillé.

Nous vous parlions en début de semaine d'une application porno qui prenait ses utilisateurs en photo, puis leur demandait une rançon. Ce ransomware virulent se cachait derrière un fichier .apk que le détenteur du smartphone visé installait, sans le savoir, depuis un site pas très catholique.

Les chercheurs de la société ESET (qui édite des antivirus) viennent de pointer dans un billet de blog le fait que les ransomwares évoluent et se révèlent de plus en plus difficiles à contrer. Le dernier en date, Porn Droid, se présente comme souvent sous la forme d'un lecteur de contenus pour adultes. Ce dernier se télécharge au format .apk depuis un market alternatif, comme la plupart des applications du genre. Ce Porn Droid cache en vérité un ransomware qui va, en vous demandant les privilèges administrateur discrètement, bloquer votre appareil. Un message du FBI (classique) s'affichera et vous réclamera la modique somme de 500 $ à payer rapidement. Ce message stipule d'ailleurs (classique aussi) que vous avez hébergé du contenu pornographique interdit.

Une fois la menace passée, ce ransomware va bloquer votre appareil préféré par l'intermédiaire d'un Code Pin que vous ne connaissez évidemment pas. Pire encore, si vous avez l'habitude d'utiliser cette sécurité pour protéger votre smartphone, le ransomware est capable d'en modifier le code. ESET propose une solution si Porn Droid fait des siennes avec votre cher appareil Android. Pour ce faire, il faut employer l'invite de commande et la passerelle de débogage Android pour modifier le fichier chargé de traiter le code PIN de votre appareil. De plus, votre terminal doit être rooté, ce qui rajoute une condition supplémentaire. Notez que ce ransomware est tellement virulent qu'il est capable de fermer les antivirus installés sur votre mobile qui tournent en tâche de fond. En définitive, la meilleure solution reste la prévention. Méfiez-vous des portails proposant des applications à télécharger .apk et appliquez les 10 commandements de la sécurité pour garder son appareil à l'abri de toutes menaces. Si le porno mobile vous intéresse, consultez notre article qui lui est consacré.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.android-mt.com/news/porn-droid-ransomware-android-43752

100% des montres connectées présentent des failles de sécurité | Le Net Expert Informatique

100% des montres connectées présentent des failles de sécurité

Les montres équipées de connexion réseau et de fonctions de communication représentent une nouvelle cible pour les cyberattaques. Tel est le principal résultat de l'étude, menée par HP Fortify, qui révèle que 100% des montres testées recèlent d'importantes vulnérabilités, comme par exemple des fonctions d'authentification insuffisantes, un manque de capacités de chiffrement, et des soucis dans la protection des données personnelles1. Dans ce rapport, HP recommande un certain nombre d'actions pour améliorer la sécurité dans la conception et l'utilisation des montres, à la maison ou dans son environnement de travail.

Avec le déploiement de l'Internet des Objets, les smartwatches gagnent en popularité en raison de leur côté pratique et des nouvelles fonctionnalités qu'elles proposent. En devenant des objets usuels, ces montres vont collecter de plus en plus d'informations personnelles sensibles, comme des données de santé. La possibilité de les connecter avec des applications disponibles sur smartphone risquent prochainement de leur donner accès à encore plus d'informations, comme par exemple les codes permettant d'ouvrir votre maison ou votre véhicule.
« Les montres connectées commencent à peine à entrer dans nos vies. Elles offrent déjà de nouvelles fonctionnalités innovantes qui pourraient ouvrir la voie à de nouvelles menaces sur des informations et des activités sensibles », a déclaré Jason Schmitt, Directeur Général Fortify de l'entité HP Security. « Avec l'accélération de l'adoption des smartwatches, cette plate-forme va devenir bien plus attrayante pour tous ceux qui voudraient en faire une utilisation frauduleuse. Il devient nécessaire de prendre des précautions lors de la transmission des données personnelles ou du raccordement de ces équipements aux réseaux d'entreprise. »
L'étude HP s'interroge ainsi sur la capacité des smartwatches à stocker et à sécuriser les données sensibles pour lesquelles elles ont été conçues. HP s'est appuyé sur HP Fortify on Demand pour évaluer 10 montres connectées à des applications mobiles et un cloud Android ou iOS.

Cette étude révèle de nombreuses failles de sécurité parmi lesquelles les plus fréquentes et les plus faciles à corriger sont :

L'insuffisance des fonctions d'autorisation et d'authentification des utilisateurs :
Chaque montre connectée testée était couplée à une interface sur téléphone mobile qui ne gérait pas l'authentification à deux facteurs, et qui ne verrouillait pas les comptes après 3 ou 5 saisies de mots de passe infructueux. Trois montres sur dix, c'est à dire 30%, étaient vulnérables aux tentatives de moisson de comptes utilisateurs, ce qui veut dire qu'un pirate informatique pourrait obtenir le contrôle de la montre et de ses données en profitant d'une politique de mots de passe faible, du non blocage des comptes, ou en énumérant des listes de comptes utilisateur potentiels.

Le manque de chiffrement lors du transfert de données :
Le chiffrement lors du transport d'information est essentiel, dans la mesure où des informations personnelles sont envoyées vers de multiples destinations dans le cloud. Même si 100 pourcents des montres testées intégraient le chiffrement lors transport avec le protocole SSL/TLS, environ 40% des connexions vers le cloud restaient vulnérables à l'attaque POODLE, permettant l'utilisation d'outils de déchiffrement peu puissants, ou encore le protocole SSL v2.

Interfaces peu sécurisées :
30% des montres testées utilisaient des interfaces web accessibles en mode cloud, et toutes présentaient des risques d'énumération de comptes utilisateur. Dans un test spécifique, 30% ont également révélé des risques d'énumération de comptes utilisateur depuis leurs applications sur mobile. Cette défaillance permet aux hackers d'identifier des comptes utilisateurs valides en s'appuyant sur les informations reçues via les mécanismes de réinitialisation de mots de passe.

Logiciels et microcode peu sécurisés :
70% des montres ont révélé des failles dans la protection des mises à jour de microcode, comme par exemple la transmission en clair des mises à jour, sans chiffrer les fichiers. Cependant, plusieurs mises à jour étaient protégées par une signature, évitant ainsi l'installation d'un microcode contaminé. Même si des updates malicieuses ne peuvent être installées, le manque de chiffrement permet aux fichiers d'être téléchargés puis analysés.

Soucis sur la protection des données personnelles :
Toutes les montres collectent des données personnelles – comme le nom, l'adresse, la date de naissance, le poids, le sexe, la fréquence cardiaque, et bien d'autres informations relatives à la santé de l'utilisateur. Si l'on rapproche ceci des problèmes relevés sur l'énumération des comptes utilisateur ou l'utilisation de mots de passe faiblement sécurisés sur certaines montres, le risque de diffusion des données personnelles depuis une montre connectée devient un problème réel.

En attendant que les fabricants incorporent les dispositifs nécessaires permettant de mieux sécuriser leurs smartwatches, les utilisateurs sont priés d'examiner scrupuleusement les fonctions de sécurisation existantes avant de choisir un modèle de montre connectée. HP recommande aux utilisateurs de ne pas activer les fonctions de contrôle des accès sensibles, comme par exemple l'accès à leur domicile ou leur véhicule, sauf si un mécanisme d'autorisation performant est proposé par la montre. De plus, en activant la fonctionnalité passcode, en imposant des mots de passe sophistiqués et en introduisant une authentification à deux facteurs, il est possible d'éviter des accès frauduleux aux données. Au delà de la protection des données personnelles, ces mesures sont essentielles dès lors que la smartwatch va être utilisée dans un environnement de travail et connectée au réseau de l'entreprise.

Méthodologie
Réalisée par HP Fortify, l'étude HP Smartwatch Security Study a utilisé la méthodologie HP Fortify on Demand IoT testing methodology, combinée avec des tests manuels et d'autres outils de test automatisés. Les équipements et les composants testés ont été évalués sur la base de l'outil OWASP Internet of Things Top 10 et des vulnérabilités spécifiques associées à chacune des 10 premières catégories.
Toutes les données et les tous les pourcentages inclus dans l'étude ont été extraits des tests menés sur les 10 montres évaluées. Malgré l'existence d'un nombre croissant de fabricants et de modèles de smartwatches, HP pense que les résultats obtenus sur cet échantillon de 10 modèles donne un bon indicateur du niveau de sécurité des smartwatches actuelles du marché.

Des conseils complémentaires sur la sécurisation des smartwatches sont disponibles dans le rapport complet (http://go.saas.hp.com/fod/internet-of-things)

Pour toute information complémentaire, il est possible de consulter le premier rapport de la série sur l'Internet des Objets, 2014 HP Internet of Things Research Study, qui passe en revue le niveau de sécurité des 10 objets connectés les plus courants du marché. De plus, l'étude 2015 HP Home Security Systems Report (http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-7342ENW&cc=us&lc=en) examine les 10 systèmes les plus répandus en matière de protection connectée du domicile.
(1) "HP Internet of Things Security Report: Smartwatches," HP, Juillet 2015.

Source : http://www.itrnews.com/articles/157450/100-montres-connectees-presentent-failles-securite.html et ITRmobiles.com