Savoir profiter des erreurs des Cybercriminels | Le Net Expert Informatique

Savoir profiter des erreurs des Cybercriminels

L'affaire Ashley Madison semble le prouver une fois de plus, les cybercriminels commettent des erreurs qui peuvent leur nuire. Détecter ces fautes et savoir les utiliser sont des éléments essentiels dans la gestion des crises cyber.

DES ATTAQUES DONT LES OBJECTIFS SONT SOUVENT DIFFICILES À CERNER

L'actualité le montre trop régulièrement, les actes cybercriminels se multiplient et visent tous types d'organisation. Certains sont revendiqués et leurs objectifs sont rapidement connus. C'est le cas pas exemple de l'attaque visant le site Ashley Madison où les motivations sont explicites.

Mais dans la plupart des cas, les objectifs de l'attaquant sont beaucoup plus difficiles à identifier ! Il est pourtant crucial de le faire pour pouvoir réagir au mieux et protéger rapidement ce qui n'a pas encore été touché par l'attaque.

Une des clés pour mieux comprendre une attaque consiste à exploiter les erreurs des attaquants. En effet, malgré leur niveau de compétences potentiellement élevé, les pirates restent des humains et commettent souvent des erreurs. Des fautes qu'il est possible d'exploiter pour mieux comprendre l'attaque et la contrer, mais aussi pour identifier ceux à son origine.

UTILISER LES ERREURS DES ATTAQUANTS POUR MIEUX LES COMPRENDRE

Le cas récent d'Ashley Madison semble être un bon exemple, même s'il faudra attendre les investigations complètes pour confirmer tous les éléments. Les attaquants auraient diffusé les données volées via BitTorrent en utilisant un serveur loué chez un hébergeur aux Pays Bas. Ils auraient cependant oublié de sécuriser ce serveur, en particulier ils n'ont pas mis de mot de passe sur les interfaces d'administration web. Même si cela ne permet pas de les identifier directement, il s'agit d'une piste de premier choix pour les forces de l'ordre en charge des investigations. Il faut cependant rester prudent car cela peut aussi être une forme de diversion réalisée par les attaquants. Affaire à suivre !

Autre exemple, le cas « Red October ». C'est l'affaire d'une vaste opération de cyber espionnage qui a commencé en mai 2007 et qui a été découverte par le cabinet Kaspersky quelques années plus tard. Le cabinet a réussi à identifier, bloquer et neutraliser le logiciel malveillant en utilisant une faille de l'attaque. En effet, les noms de domaines pour les serveurs d'exfiltration qui étaient utilisés dans le code malveillant n'avaient pas été réservés par les attaquants. Cela a permis à Kaspersky de simuler un de ces serveurs et de voir qui était infecté et quelles données étaient capturées.

Parfois, ces erreurs permettent même d'identifier les auteurs de l'attaque, comme ce fut le cas avec la traque de la personne derrière le malware PlugX.

Nos consultants ont d'ailleurs eux aussi rencontré ce genre de situation dans le cadre d'une attaque ciblée chez un de nos clients. Les pirates avaient en effet « oublié » la présence d'un keylogger sur les serveurs internes utilisés pour l'exfiltration des données, ce qui a permis à nos experts d'identifier quelles données étaient ciblées et où elles étaient envoyées. Nous avons même pu récupérer le login et le mot de passe utilisés par les attaquants. Le concept de « l'arroseur arrosé » remis au goût du jour.

SAVOIR TIRER PARTI DE CES INFORMATIONS POUR MIEUX GÉRER LA CRISE

Les informations obtenues grâce à ces erreurs sont très précieuses, elles permettent ensuite d'adapter la réponse à l'incident. D'autant plus que les attaquants utilisent parfois des mécanismes de diversion « bruyants » (redémarrage de machines, effacement de fichiers, forte activité CPU, voir déni de service…) afin de détourner l'attention des vrais données qu'ils visent. Une compréhension « métier » des objectifs de l'attaque permet d'éviter de se focaliser sur ces pièges.

Il est même souvent intéressant de laisser l'attaque se dérouler pour mieux la comprendre.

Les réflexes face aux incidents de sécurité « classiques » (déployer des signatures antivirales, réinstaller des serveurs…) sont donc aujourd'hui largement révolus. Il faut adopter une approche dynamique de la crise, s'intéresser à son objectif métier et utiliser les erreurs des attaquants pour être plus pertinent, en pouvant même envisager des réponses « actives » à l'attaque. Un challenge pour les équipes de réponses à incidents, qui doivent adapter leurs méthodologies et leurs réflexes, mais un objectif crucial pour lutter contre ces attaques

---

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Source :

http://www.solucominsight.fr/2015/08/attaques-ciblees-profiter-des-erreurs-des-attaquants-pour-mieux-les-comprendre-et-les-contrer/

Le secteur public ciblé par la cybercriminalité | Le Net Expert Informatique

Le secteur public ciblé par la cybercriminalité

« Au cours du second trimestre, nous avons assisté à une mutation dans l'univers des menaces. Les pirates informatiques font désormais preuve de davantage de sophistication et de créativité afin de renforcer et de réinventer leurs méthodes d'attaques existantes », observe Raimund Genes, CTO de Trend Micro. « La vision éthérée de la cybercriminalité n'est plus d'actualité. Ce trimestre a démontré que les dommages potentiels des cyberattaques vont bien au-delà de simples bugs logiciels. Le piratage d'avions, de voitures intelligentes et des chaines de TV est en effet devenu une réalité. »

Les hackers identifient et affinent leurs approches de façon plus stratégique, ciblant ainsi leurs victimes de manière plus sélective afin d'améliorer le taux d'infection de leurs attaques. Une tendance qui reflète une réelle progression de plusieurs méthodes d'attaques traditionnelles, avec notamment un bond de 50% de l'utilisation du kit d'exploitation Angler et de +67% pour les menaces utilisant des kits d'exploitation en général. Les attaques ciblant les banques en ligne sont par ailleurs en forte augmentation dans l'hexagone, avec plus de 60% du nombre de PC infectés entre le premier et le second trimestre 2015. D'autre part, l'adware Opencandy et le malware Upatre ont été particulièrement actifs en France ce trimestre, avec respectivement 12 773 et 3 854 PC infectés. Le malware Dyre arrive quant à lui en 4ème position avec 1 469 infections.

De même, les administrations ont été les cibles privilégiées de cyberattaques au cours du second trimestre, avec les piratages massifs des données de l'Internal Revenue Service (le fisc américain) en mai et du système de l'U.S. Office of Personnel Management (une agence gouvernementale américaine responsable de la fonction publique) en juin. Le piratage des données de l'OPM constitue un modèle du genre avec, à la clé, la divulgation de données personnelles identifiables portant sur près de 21 millions d'individus. D'autres agences gouvernementales ont été impactées par des campagnes ciblées utilisant des macros malveillantes, de nouveaux serveurs C&C (Command & Control), de nouvelles vulnérabilités, ainsi que la faille zero-day Pawn Storm.

En se penchant sur le panorama global des menaces au cours du second trimestre, on remarque que les États-Unis jouent un rôle majeur, que ce soit en tant que pays d'origine mais également en tant que cible de nombreuses attaques. Les liens malveillants, le spam, les serveurs C&C et les ransomware y sont tous très présents.

Parmi les points essentiels du rapport :

Des attaques perturbant les services publics : réseaux de diffusion, avions, véhicules automatisés et routeurs résidentiels présentent non seulement un risque d'infection élevé par malware, mais sont également susceptibles d'avoir des répercussions sur l'intégrité physique de leurs utilisateurs.

Le succès d'attaques ransomware ou ciblant les terminaux de points de vente (PoS), aubaine pour les cybercriminels solitaires en quête de notoriété : en déployant les attaques FighterPoS et MalumPoS, ainsi que keylogger Hawkeye, les hackers solos "Lordfenix" et "Frapstar" ont démontré que la force de frappe d'individus isolés est aujourd'hui indéniable.

La lutte des gouvernements contre la cybercriminalité : Interpol, Europol, le département américain de la sécurité nationale et le FBI ont contribué à démanteler des réseaux botnets majeurs et déjà bien établis. D'autre part, l'inculpation de Ross Ulbricht, fondateur de Silk Road, a mis en lumière la nature obscure et redoutable du Dark Web.

Les impacts nationaux et politiques d'attaques ciblant des organisations gouvernementales : la redoutable attaque sur l'OPM a prouvé que la confidentialité de nos données personnelles n'est pas avérée. Les macros malveillantes, les tactiques d'island-hopping (piratage d'une entité tierce avant de remonter vers la cible finale) et les serveurs C&C comptent parmi les tactiques les plus utilisées pour cibler les informations gouvernementales lors d'attaques.

De nouvelles formes de menaces visant les sites web publics et les dispositifs mobiles : alors que les menaces ciblant les logiciels sont toujours d'actualité, les vulnérabilités des applications web se montrent tout aussi dangereuses. Les assaillants savent tirer parti de toute vulnérabilité existante, tandis que les applications personnalisées nécessitent une prise en charge toute aussi personnalisée afin de neutraliser ces passerelles potentielles d'intrusion.

Le rapport

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.globalsecuritymag.fr/Trend-Micro-identifie-de-nouvelles,20150917,55924.html

---

L'écran de verrouillage

d'Android cède une nouvelle fois | Le Net Expert Informatique

L'écran de verrouillage d'Android cède une nouvelle fois

La méthode, assez simple, ne nécessite pas l'injection d'un malware. Elle concerne tous les terminaux sous Android 5.x et supérieurs.

Contourner l'écran de verrouillage des smartphones Android n'est décidément pas très compliqué. Un spécialiste en fait une nouvelle fois la démonstration, utilisant une méthode assez simple qui n'exige pas de connaissances particulières ni l'injection d'un malware. Elle concerne tous les terminaux sous Android 5.x et supérieurs dont l'accès est protégé par un code (et pas un schéma).
La marche à suivre consiste d'abord à accéder aux appels d'urgence puis d'entrer une chaîne de caractères, les surligner (double-clic) et les copier. Il s'agit ensuite de copier et de coller autant de fois que c'est possible cette chaîne dans le champ mot de passe. Puis de se rendre dans l'appli photo, de faire apparaître la zone de notifications et de copier la chaîne de caractère lorsque l'appli demande à nouveau le mot de passe.
A ce moment, (après un moulinage plus ou moins long), l'appli Photo plante et le terminal se débloque comme par magie, permettant d'accéder à tout son contenu.
Prévenu de cette faille, Google n'a pas encore communiqué sur la question.

Source :
http://www.zdnet.fr/actualites/android-l-ecran-de-verrouillage-cede-une-nouvelle-fois-39824986.htm

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.

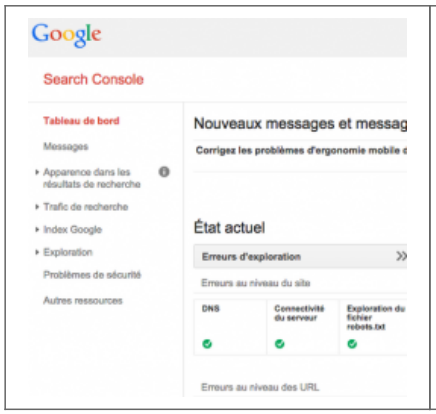
Afin de monétiser leur attaque, ils ont stocké l'ensemble des données volées dans des serveurs à l'étranger pour pouvoir les vendre ensuite au marché noir sur différents forums. Un souci d'anonymat rencontré jusque dans leur moyen de communication, chiffré, au cours de leurs opérations afin de brouiller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

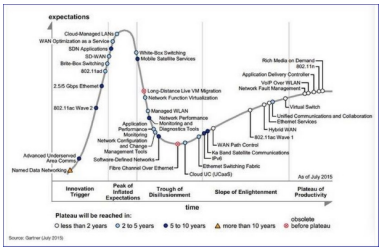
Utiliser les méthodes alternatives de Google pour s'identifier

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.

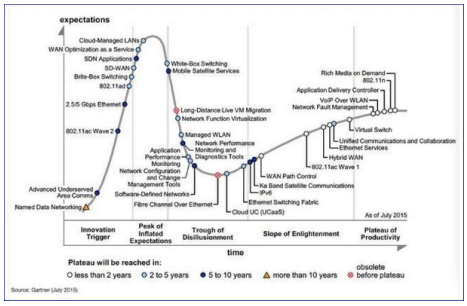
« Ce type d'attaques particulièrement virulent impose d'instituer de nouvelles priorités, de la part des 'CISO' (Chief information security officers – ou RSSI, responsables sécurité du système d'information) mais également de la part des responsables BCM (Business continuity management) », observe le 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

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