L’Europe prend un mauvais virage en matière numérique | Le Net Expert Informatique

	L’Europe prend un mauvais virage en matière numérique

Dans l'exercice consistant à élaborer de bonnes politiques en matière numérique, l'Europe a raté son premier test majeur. Au mois de mai, la Commission européenne annonçait la création d'un marché unique du numérique réunissant 500 millions de consommateurs, censé apporter 415 milliards € au PIB de l'Union européenne et créer quelque 3,8 millions d'emplois. Seulement voilà, une récente décision autour d'une problématique numérique majeure – la confidentialité des données – menace de faire dérailler la locomotive.

Au mois de juin, les ministres de l'Intérieur et de la Justice de l'UE ont voté en faveur de la conservation de pouvoirs nationaux significatifs en matière de protection de la confidentialité numérique, plutôt que d'élaborer un ensemble de règles s'appliquant aux 28 Etats de l'UE. Si le Parlement européen venait à approuver cette proposition, la divergence des règles nationales serait alors de retour. Plus inquiétant encore, ceci ouvrirait la voie à la mise en place de dispositions rendant illégales les activités bénignes et peu risquées d'exploration des données, qui sous-tendent la publicité en ligne.

La publicité sur Internet permet aux citoyens de l'UE d'accéder à de l'information, à des contenus éducatifs, à des canaux de commerce et autres sites de divertissement, sans avoir à en payer directement l'accès. En Europe, les montants dépensés dans ce domaine sont en pleine augmentation. Les revenus du secteur ont plus que quadruplé depuis 2006, malgré la stagnation de l'économie européenne dans son ensemble. Le nouveau combat de la confidentialité en UE vient menacer toute cette évolution. Non seulement faut-il s'attendre à une importante charge administrative liée aux coûts supplémentaires et aux difficultés bureaucratiques, mais un risque réel existe également de voir ces nouvelles règles mettre à mal le modèle d'entreprise d'un grand nombre des principales sociétés européennes en ligne.

Il s'agirait d'un véritable gâchis – qui plus est facilement préventible. En 2012, la Commission européenne a formulé une proposition de remplacement de la législation de l'UE existante en matière de protection des données, dont la plus récente version avait été élaborée en 1995, époque à laquelle Internet ne jouait qu'un rôle minime dans l'économie. Le texte initial était prometteur. Il entendait harmoniser les cadres juridiques fragmentés de l'Europe, fournir aux entreprises un guichet unique fort utile, et rassurer les consommateurs en leur garantissant une utilisation appropriée de leurs données.

Malheureusement, beaucoup des propositions les plus judicieuses ont été depuis abandonnées. Lors du rassemblement ministériel du mois de juin, le principe majeur de guichet unique a été véritablement éviscéré. Plutôt que de permettre aux entreprises d'avoir affaire à l'autorité de protection des données compétente au sein du pays dans lequel ces entreprises possèdent leur siège ou leur principale implantation européenne, les Etats membres insistent aujourd'hui pour que les régulateurs nationaux conservent le contrôle. Conformément aux nouvelles règles proposées, toute autorité « concernée » pourrait s'opposer à une décision prise par un autre régulateur national, donnant lieu à une procédure d'arbitrage complexe faisant intervenir l'ensemble des 28 agences.

Les ministres ont également adopté une large définition de ce que l'on entend par données personnelles. Y figureraient ainsi à la fois les cookies (petits ensembles de données stockés sur l'ordinateur d'un internaute) et les adresses IP (code utilisé pour identifier un ordinateur lorsqu'il se connecte à Internet) – bien que ces éléments ne fournissent aucun lien en direction d'un individu donné. Au mieux, cette définition étendue et peu pointue des données personnelles menace de créer des obstacles inutiles pour les annonceurs numériques basés dans l'UE. Au pire, elle risque de plonger leur modèle d'entreprise dans l'illégalité.

Ces règles inutilement strictes en matière de données sont vouées à affecter les entreprises européennes dans une mesure disproportionnée. On peut comprendre qu'il soit demandé à Google, Facebook et autres géants américains d'Internet de solliciter le consentement explicite de leurs utilisateurs. Pour autant, le secteur européen de l'Internet est dominé par des entreprises de B to B, dont les marques peu connues traitent effectivement les données des consommateurs, mais manquent d'un contact direct avec les utilisateurs. Ainsi, la seule véritable alternative consistera pour ces sociétés Internet européennes à travailler auprès des grandes plateformes américaines, et à devenir encore plus dépendantes de celles-ci.

Bien que le Royaume-Uni, la Suède, la Norvège et les Pays-Bas comptent parmi les pays leaders de l'Internet à travers le monde, de nombreux autres Etats européens évoluent considérablement à la traîne. Ainsi, l'économie numérique contribue au PIB de l'UE à hauteur d'environ 4 %, contre 5 % aux États-Unis et 7,3 % en Corée du Sud. Les nouvelles réglementations proposées ne feront qu'accentuer cet important retard des entreprises européennes par rapport à leurs concurrentes internationales.

L'Europe est confrontée à un choix important. Bien entendu, l'UE doit pouvoir rassurer ses citoyens quant à l'utilisation appropriée de leurs données ; les mesures en ce sens peuvent contribuer à la croissance de l'économie numérique. En revanche, les dirigeants du continent ne doivent pas oublier qu'un marché unique du numérique ne pourra exister aussi longtemps que les règles accentueront la divergence des approches nationales autour de la confidentialité, et qu'elles feront obstacle à l'utilisation par Internet des données anonymes à des fins de publicité numérique. Le sort d'une génération toute entière d'entrepreneurs numériques européens est aujourd'hui en jeu.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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.libe.ma/L-Europe-prend-un-mauvais-virage-en-matiere-numerique_a66663.html

Par Christopher Engman PDG de la société suédoise de commercialisation en ligne, «Vendemore» (Traduit de l'anglais par Martin Morel)

Ce malware avale des cartes bancaires pour les restituer… aux pirates | Le Net Expert Informatique

Ce malware avale des cartes bancaires pour les restituer… aux pirates

Un nouveau code malveillant a été découvert par des chercheurs en sécurité, ciblant les distributeurs de marque NCR et Diebold.

Un nouveau type de malware pourrait bientôt frapper les distributeurs de banque dans le monde. Les chercheurs en sécurité de FireEye viennent de mettre la main sur un code particulièrement vicieux et, semble-t-il, unique en son genre. Baptisé « Backdoor.ATM.Suceful », il est capable d'infecter des distributeurs de marque NCR ou Diebold -sous Windows- qui sont également présents en France. Son originalité est qu'il s'attaque directement à la carte bancaire de l'utilisateur. Il l'avale tout cru en faisant croire qu'il s'agit d'une erreur de manipulation ou de logiciel.

Le pirate pourra ensuite la récupérer auprès du distributeur. Il lui suffira, pour cela, de tapoter un code particulier sur le clavier de la machine. Le malware peut également lire la bande magnétique ou la puce de la carte. Il peut aussi désactiver certaines fonctionnalités de l'appareil, comme l'alarme, la lumière ou le capteur audio. « Suceful est le premier malware ciblant des distributeurs dans le but de voler les données des cartes ainsi que les cartes elles-mêmes. Le degré de sophistication atteint donc un nouveau record », estime FireEye, dans une note de blog.

Toutefois, il n'existe pas encore de preuve que ce malware soit réellement utilisé à l'heure actuelle. Le code a été trouvé dans la base partagée de VirusTotal, avec une date de création du 25 août 2015. Il pourrait s'agir d'une version de développement, estiment les experts. Par ailleurs, le code n'indique pas comment les pirates pourraient l'installer sur un distributeur.

Quoi qu'il en soit, si votre carte est avalée, il est recommandé d'aller immédiatement prendre contact avec l'agence. Tout en gardant un œil sur le distributeur… sait-on jamais !

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.01net.com/actualites/ce-malware-avale-des-cartes-bancaires-pour-les-restituer-aux-pirates-915042.html
et FireEye

La Police se dote d'un laboratoire cybercriminalistique

informatique | Le Net Expert Informatique

La Police se dote d'un laboratoire cybercriminalistique informatique

La Police nationale s'est dotée d'un laboratoire cybercriminalistique informatique qui est un dispositif qui consiste à mettre des méthodes et protocoles d'investigation permettant de récolter une preuve numérique en vue de mieux lutter contre la cybercriminalité et la cybersécurité, selon Papa Gueye, élève-commissaire à l'Ecole nationale de police.

''Il s'agit d'un laboratoire cybercriminalistique informatique logé au sein de la Division des investigations criminelles (DIC). Il est équipé avec des matériels de dernière génération et sert à analyser les données et supports informatiques'', a expliqué M. Gueye.

Il intervenait à une table ronde à l'initiative de la Direction générale de la police nationale sur le thème : ''La cybercriminalité et la cybersécurité : enjeux et défis pour les forces de sécurité''.
Cette rencontre qui entre dans le cadre des cycles de conférences intitulées ''Les mercredi de la police'', a réuni des experts informatiques, des juristes, des spécialistes en cybercriminalité, plusieurs policiers entre autres participants.

''De plus en plus les forces de la police sont appelées à faire face à des crimes nouveaux avec une cybercriminalité pointue et trés bien structurée, d'où la nécessité de se doter de ce genre de laboratoire'', a poursuivi Papa Gueye qui a introduit un exposé intitulé ''Cybercriminalité au Sénégal : manifestations et réponses des forces de sécurité''.

Dans sa communication, M. Gueye, ancien officier à la Police, est revenu sur les différents types de cybercriminalité au Sénégal, les réponses apportées par les forces de la police et les obstacles liés à la répression du phénomène. Pour lui, il est ''obligatoire pour les forces de défense de s'adapter face à des infractions de type nouveau''.

Il a invité les populations à se rendre auprès de la DIC qui héberge ce laboratoire pour exposer leurs mésaventures si elles sont victimes d'infractions liées à la cybercriminalité. Papa Gueye a aussi insisté sur la nécessité de capaciter les acteurs de la police et de sensibiliser les populations sur ces ''crimes nouveaux''.

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.aps.sn/actualites/societe/article/la-police-se-dote-d-un-laboratoire-cybercriminalistique-informatique-commissaire

---

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

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

Source : http://www.globalsecuritymag.fr/Trend-Micro-identifie-de-nouvelles,20150917,55924.html

---

Un Russe plaide coupable aux

États-Unis pour plusieurs cyberattaques | Le Net Expert Informatique

Un Russe plaide coupable aux États-Unis pour plusieurs cyberattaques

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 ».

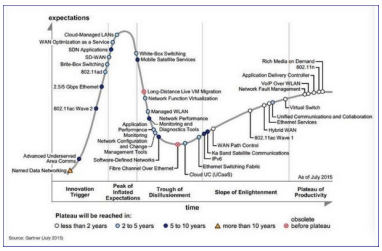
Arrêté en juin 2012 à Amsterdam puis extradé vers les États-Unis, Drinkman était depuis incarcéré dans l'attente de son procès. Si le jeune homme a plaidé non coupable dans un premier temps, il s'est ravisé depuis. Bien que 9 autres chefs d'accusation ont été rejetés, il encoure 30 ans de prison pour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

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

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.

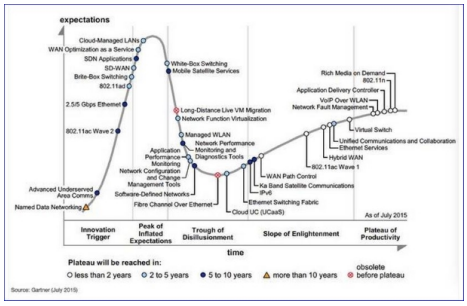
« Ce type d'attaques particulièrement virulent impose d'instituer de nouvelles priorités, de la part des 'CISO' (Chief information security officers – ou RSSI, responsables sécurité du système d'information) mais également de la part des responsables BCM (Business continuity management) », observe le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

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.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

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

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

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.

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.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.

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