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.

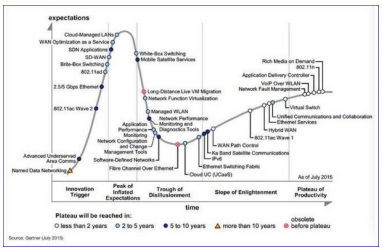
Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

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

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.

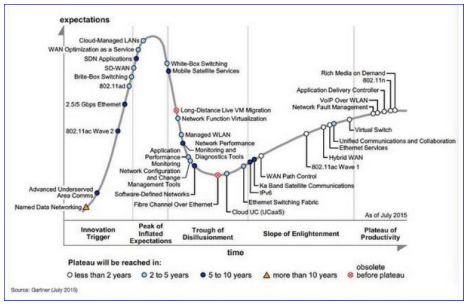
« Ce type d'attaques particulièrement virulent impose d'instituer de nouvelles priorités, de la part des 'CISO' (Chief information security officers – ou RSSI, responsables sécurité du système d'information) mais également de la part des responsables BCM (Business continuity management) », observe le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

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)

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

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.

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

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

Le certificat électronique est une arme efficace contre la Cybercriminalité | Le Net Expert Informatique

	Le certificat électronique est une arme efficace contre la Cybercriminalité

Lutter contre la cybercriminalité est un axe stratégique pour les entreprises et les institutions. En effet, nous assistons quotidiennement à des attaques toujours plus sophistiquées qui viennent durablement compromettre l'intégrité et la confidentialité des échanges réalisés sur le net. Bien entendu, nombre d'entreprises et d'institutions mettent en place des dispositifs pour se protéger, mais en laissant «certains trous dans la raquette» qui sont immédiatement utilisés par les pirates pour mener à bien leurs actions.

Très répandues, ces pratiques créent des désastres financiers et montrent bien que les flux sortants sont tout aussi exposés que les flux entrants. Il est donc nécessaire de les prendre en compte dans la mise en œuvre de dispositifs de protection efficace.

L'usage du certificat électronique ID (pour personne physique) est la piste à privilégier. Il est d'ailleurs largement plébiscité par l'Etat et les collectivités avec la norme RGS. Véritable rempart contre l'usurpation d'identité, il permet au destinataire d'un mail d'en vérifier l'émetteur, il permet également de garantir la confidentialité des données échangées. L'autre avantage tient à sa simplicité d'utilisation sur les mobiles et tablettes. Avec un certificat, les envois de mails à partir d'un smartphone ne représentent plus une faille de sécurité mais sont protégés efficacement.

Au regard de ces éléments, institutions et entreprises doivent accélérer le déploiement de certificats pour sécuriser leurs échanges de données. Une prise de conscience dans ce domaine permet de colmater des brèches importantes et complète des dispositifs traditionnels de type Firewall qui jouent pour leur part un rôle de filtrage pour les données entrantes. Avec les certificats électroniques, les flux sortants sont parfaitement sécurisés, leur apport dans la lutte contre la cybercriminalité est donc stratégique, d'autant que leur coût d'acquisition n'est pas onéreux.

Source : http://www.edubourse.com/finance/actualites.php?actu=89518

Les entreprises doivent se préparer à une nouvelle génération de cyber-risques |

Le Net Expert Informatique

ALes entreprises doivent se préparer à une nouvelle génération de cyber-risques

Les entreprises doivent se préparer à une nouvelle génération de cyber-risques qui progressent rapidement, passant de menaces avérées de violations de données, problèmes de confidentialité et atteintes à la réputation, à l'interruption d'activité et même à des pertes potentielles catastrophiques, en passant par des dommages opérationnels.

Dans un nouveau rapport — A Guide to Cyber Risk : Managing The Impact of Increasing Interconnectivity —, l'assureur spécialisé Allianz Global Corporate & Specialty (AGCS) observe les dernières tendances en matière de cyber-risques et les dangers émergents au niveau mondial. Le cyber-risque est l'une des principales menaces auxquelles font face les entreprises et connaît une croissance rapide. La cybercriminalité à elle seule coûte approximativement 445 milliards de $ par an à l'économie mondiale et les 10 plus grandes économies représentent plus de la moitié de ce montant (3 milliards de $ pour la France).
« Il y a à peine 15 ans, les cyber-attaques étaient assez rudimentaires et généralement l'œuvre de hacktivistes, mais avec l'accroissement de l'interconnectivité, de la mondialisation et de la commercialisation de la cybercriminalité, la fréquence et la gravité des cyber-attaques ont pris une ampleur considérable », déclare Chris Fischer Hirs, PDG d'AGCS. « La cyber-assurance ne remplace pas une sécurité informatique solide, mais elle crée une seconde ligne de défense qui limite les incidents. AGCS observe une augmentation de la demande pour ces services, et nous nous engageons à collaborer avec nos clients afin de mieux comprendre l'exposition croissante aux cyber-risques et d'y faire face. »

Des réglementations plus strictes et de nouveaux cyber-dangers

Une prise de conscience croissante des expositions aux cyber-risques ainsi qu'une adaptation de la réglementation vont propulser la croissance future de la cyber-assurance. Avec moins de 10 % des entreprises qui achètent actuellement des cyber-polices spécifiques, AGCS prévoit une augmentation des primes de cyber-assurance à l'échelle mondiale de 2 milliards de $ par an aujourd'hui à plus de 20 milliards de $ au cours de la prochaine décennie, soit un taux de croissance annuel de plus de 20 %.
« Aux États-Unis, la croissance a déjà commencé, portée par des règles relatives à la protection des données qui attirent l'attention sur le problème. Dans le reste du monde, de nouvelles dispositions législatives et des niveaux de responsabilité plus élevés seront des moteurs de croissance », affirme Nigel Pearson, responsable mondial de la cyber-assurance chez AGCS. « La tendance générale tend à opter pour une protection des données plus strictes et elle est soutenue par la menace d'amendes importantes en cas d'infraction. » Hong Kong, Singapour et l'Australie, par exemple, travaillent sur de nouvelles lois ou en appliquent déjà. Même si l'Union européenne ne parvient pas à se mettre d'accord sur ses règles paneuropéennes de protection des données, on peut s'attendre à des directives plus strictes à l'échelle de chaque pays.
Auparavant, l'attention se focalisait largement sur la menace de violation de données d'entreprise et d'atteinte à la vie privée, mais la nouvelle génération de cyber-risques est plus complexe : les menaces futures porteront sur le vol de propriété intellectuelle, la cyber-extorsion et l'impact de l'interruption d'activité après une cyber-attaque, ou sur une défaillance opérationnelle ou technique — un risque qui est souvent sous-estimé. « La prise de conscience des risques d'interruption d'activité et de l'assurance relative aux cyber-risques et à la technologie ne cesse de croître. Dans les cinq à dix prochaines années, l'interruption d'activité sera perçue comme un risque majeur et un élément principal du paysage des cyber-assurances », déclare Georgi Pachov, expert cyber dans l'équipe de souscription mondiale Dommages aux Biens d'AGCS. Dans le contexte des cyber-risques et des risques informatiques, la couverture interruption d'activité peut être très étendue, incluant les systèmes informatiques d'entreprise, mais aussi les systèmes de contrôle industriel (SCI) utilisés par des entreprises du secteur de l'énergie, ou encore les robots utilisés dans la production.

La connectivité engendre le risque

L'interconnectivité accrue des appareils que nous utilisons au quotidien et la dépendance croissante à la technologie et aux données en temps réel au niveau personnel comme à l'échelle de l'entreprise, connue sous le nom d'« Internet des objets », créent d'autres vulnérabilités. Certaines estimations suggèrent qu'un billion d'appareils pourraient être connectés d'ici 2020 et 50 milliards de machines pourraient échanger des données quotidiennement. Les SCI sont un autre sujet de préoccupation étant donné que nombre de ces systèmes qui sont toujours utilisés aujourd'hui ont été conçus avant que la cyber-sécurité devienne un problème prioritaire. Une attaque contre un SCI pourrait donner lieu à des dommages matériels comme un incendie ou une explosion, ainsi qu'à une interruption d'activité.

Evénements catastrophiques

Alors que des violations de données très importantes ont déjà eu lieu, la perspective d'une perte catastrophique est devenue plus probable, mais il est difficile de prédire ce qu'elle impliquera exactement. Les scénarios comprennent une attaque réussie contre l'infrastructure de base d'Internet, une violation grave des données ou une panne de réseau chez un fournisseur de cloud, alors qu'une cyber-attaque importante impliquant une entreprise d'énergie ou de services publics pourrait se traduire par une interruption significative des services, des dommages matériels ou même des pertes humaines à l'avenir.

Couverture autonome

D'après Allianz, la portée de la cyber-assurance doit également évoluer en vue de fournir une couverture plus étendue et plus approfondie, prenant en charge l'interruption d'activité et comblant les lacunes entre la couverture traditionnelle et les cyber-polices. Alors que les exclusions des cyber-risques dans les polices IARD vont vraisemblablement devenir monnaie courante, la cyber-assurance autonome va continuer d'évoluer pour devenir la source principale de couverture complète. On observe un intérêt croissant dans les secteurs des télécommunications, de la distribution, de l'énergie, des services publics et du transport, ainsi que de la part des institutions financières.

La formation — en termes de compréhension de l'exposition de l'entreprise comme de connaissances en souscription — doit s'améliorer pour permettre aux assureurs de répondre à une demande croissante. De plus, comme pour tout autre risque émergent, les assureurs doivent en outre faire face à des défis concernant la tarification, les libellés des polices non testés, la modélisation et l'accumulation des risques.

Réponse aux cyber-risques

Le rapport d'AGCS expose les démarches que les entreprises peuvent entreprendre pour couvrir les cyber-risques. L'assurance ne peut être qu'une partie de la solution, avec une approche globale de la gestion des risques en guise de fondement de la cyberdéfense. « Le fait de contracter une cyber-assurance ne signifie pas que vous pouvez ignorer la sécurité informatique. Les aspects technologiques, opérationnels et assurantiels de la gestion des risques vont de pair », explique Jens Krickhahn, expert Cyber & Fidelity chez AGCS Central & Eastern Europe. La gestion des cyber-risques est trop complexe pour être l'apanage d'un seul individu ou département, de sorte qu'AGCS recommande la constitution d'un groupe de réflexion pour combattre les risques, au sein duquel différentes parties prenantes dans toute l'entreprise collaboreraient pour partager leurs connaissances.

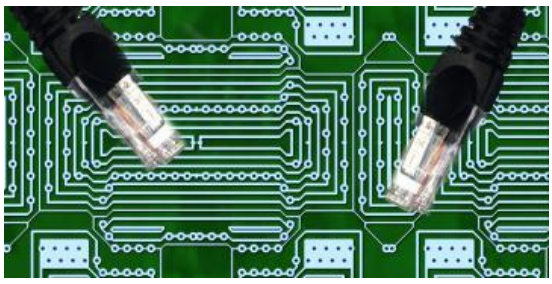
De cette manière, différentes perspectives sont remises en question et d'autres scénarios sont pris en considération : ceux-ci peuvent par exemple inclure le risque découlant des développements de l'entreprise comme les fusions et acquisitions, ou de l'utilisation de services externalisés ou d'un cloud. De plus, la contribution intersociétés est essentielle pour identifier les actifs clés en matière de risque et, surtout, pour développer et tester des plans d'action solides en cas de crise.

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/Allianz-Global-Corporate-Specialty,20150909,55621.html

---

Quand le frigo vole vos données personnelles | Le Net Expert Informatique



Quand le frigo vole vos données personnelles

Des experts en sécurité viennent de démontrer que des pirates, en passant par un réfrigérateur connecté, seraient capables de s'introduire sur les comptes de la messagerie Gmail de Google. Un type d'attaque informatique qui relance le débat sur les failles de sécurité des objets innombrables que nous connectons au web.

Désormais, les lave-linge commandent leur stock de lessive en ligne, les voitures tweetent à leur garagiste et toutes sortes de gadgets communicants nous aident à mieux contrôler notre environnement. L'internet des objets n'en fini plus de nous étonner en permettant d'associer des puces électroniques aux choses qui nous entourent. D'ici à 2020, quelque 200 milliards d'objets reliés à un réseau seront utilisés par les internautes sans intervention spécifique de leur part. Un nouvel eldorado économique pour les industriels de la high tech, mais aussi le paradis des pirates qui s'empresseront de piller cette nouvelle informatique qui ne possède pas un véritable système de sécurité.

Les experts tirent la sonnette d'alarme depuis des années, dénonçant le manque de protection des objets reliés en permanence à la Toile. Récemment, des hackers ont réalisé un coup d'éclat en prenant le contrôle de plus de 100 000 gadgets électroniques en les détournant de leur fonction première comme des téléviseurs, des consoles de jeux, des box internet et même un réfrigérateur connecté. Jusqu'à présent, il était inutile de s'inquiéter de ces attaques spectaculaires sur nos grille-pain, lave-linge ou autres joujoux électroniques en ligne, les cybercriminels se contentaient seulement de les dérégler.

Le problème prend aujourd'hui, une toute autre dimension, une équipe de chercheurs vient d'identifier une faille de sécurité plus inquiétante. Elle offre la possibilité à des pirates de s'introduire sur les comptes de la messagerie de Google Gmail, en passant par les cuisines de particuliers où trône le dernier modèle des réfrigérateurs intelligents de la marque Samsung. L'appareil qui gère la fraicheur de nos denrées alimentaires a été conçu pour télécharger l'agenda de notre boite électronique et de l'afficher automatiquement sur son écran intégré.

Une porte d'entrée idéale, estiment les chercheurs, qui permet aux pirates d'accéder facilement à nos courriels et à nos données confidentielles. Qu'on se rassure, jusqu'à présent, aucune intrusion de ce type n'est à déplorer, s'empressent-ils d'ajouter. La firme Samsung promet de corriger cette anomalie, mais le développement exponentiel de l'internet des objets, sans un système de sécurité pensé à l'avance, a de quoi inquiéter et risque de se métamorphoser bien vite en cyber cauchemar pour consommateurs techno-branchés.

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.rfi.fr/emission/20150906-quand-le-frigo-vole-vos-donnees-objets-connectes-internet-cyber-attaque-securite
Par Dominique Desaunay

Le Summer Camp de la NSA, école de cybersécurité | Le

Net Expert Informatique

	**Le Summer Camp de la NSA, école de cybersécurité**

29 universités ont accueilli cet été des jeunes pour les initier aux rudiments de la sécurité informatique. Le tout financé par l'agence américaine de renseignement.

Comprendre les écoutes des présidents français par la NSA

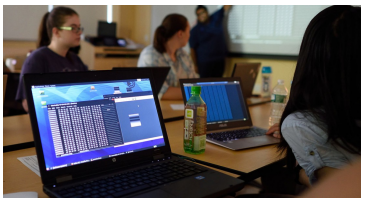
Un été entre ados dans de grands espaces bucoliques, avec canoë et camping au coin du feu ? Pas cette fois. Cet été, 1.400 collégiens et lycéens américains ont été accueillis dans 29 universités pour des « summers camps » qui ne ressemblent pas au traditionnel camp de vacances.

Au fond d'universités aux allures d'hôpitaux, ils ont passé l'essentiel de leur temps dans des salles de classes jaunies, éclairées aux néons, le nez rivé sur un écran d'ordinateur. Normal : ils ont participé au programme GenCyber, pour « Inspirer la nouvelle GENération de professionnels du CYBERespace ». Plus simplement, les « stagiaires » sont venus apprendre à bidouiller dans le code d'ordinateurs. Et devinez qui est le mécène de ces cours d'été pour apprentis-hackers ? La NSA.

Oui, la « No Such Agency », longtemps considérée comme l'agence de renseignement la plus secrète du monde, mais dont les pratiques d'espionnage massif des Américains (et du reste du monde) ont été mises en lumière par les révélations de son ancien consultant Edward Snowden, puis de WikiLeaks.

Pourquoi donc la NSA, avec son budget annuel de plus de 10 milliards de dollars, ses 850.000 employés et ses « clients » comme la CIA ou le FBI, s'enquiquine-t-elle à organiser des camps d'été ?

« Notre ambition est d'intéresser les jeunes à la cybersécurité », nous explique le créateur et directeur du programme, Steve LaFountain. « Il y a entre 600.000 et 1 million d'emplois dans la cybersécurité qui ne sont pas pourvus aux Etats-Unis, parce que nous n'avons pas assez de gens entraînés à cette discipline. GenCyber vise à combler ce gap. »



Une enveloppe de 4 millions de dollars

D'une fac à l'autre, l'enseignement varie : le camp de San Bernardio (Californie) s'attarde sur les drones, tandis qu'au camp de Norwich (Vermont) les élèves fabriquent leurs propres ordinateurs, depuis l'assemblage des puces jusqu'au logiciel de sécurité interne, et peuvent le rapporter chez eux.

Lors des 47 camps organisés cet été, une vingtaine d'ados sont accueillis pendant une ou deux semaines, totalement gratuitement. Chaque camp représente un budget moyen 85.000 dollars, pour une enveloppe totale de 4 millions de dollars. L'ensemble est financé par la NSA et la National Science Foundation (NSF), équivalent américain de notre CNCRS (Centre national de la recherche scientifique). Les universités y sont aussi de leur poche, mais seulement pour la rémunération des professeurs, soit « une dizaine de milliers de dollars », selon Nasir Memon, responsable du programme à l'université de New York.

Derrière ces summer camps pointe l'objectif inavoué par la NSA, pas connue pour sa philanthropie, de repérer une nouvelle génération de petits génies de la sécurité informatique, et de les attirer dans les rangs de l'agence. Depuis les révélations de Snowden, la NSA peine à séduire les talents dont elle a besoin. Difficile pour l'espionne controversée de rivaliser avec l'esprit libertaire de la Silicon Valley et ses salaires mirobolants. Rien que pour cette année, l'agence serait à la recherche de 1.600 recrues, dont plusieurs dizaines dans la cybersécurité.

Steve LaFountain a été chargé de mettre en place plusieurs programmes pour attirer les talents universitaires, et il en a profité pour lancer les camps d'été pour collégiens et lycéens. L'intéressé se défend d'une quelconque ambition de repérer de (très) jeunes recrues :

« Il s'agit uniquement de les intéresser à la sécurité informatique », nous rétorque-t-il avec vigueur. « En offrant ce programme gratuitement, nous espérons bousculer les barrières économiques et géographiques qui empêchent les jeunes — en particulier ceux avec un faible accès à l'informatique dans leurs classes — d'apprendre les fondamentaux de la cybersécurité. »

« Un impact dans la formation des talents »

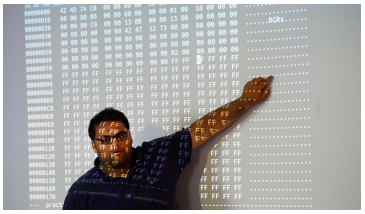
Les universités s'affichent sur la même ligne. Le programme GenCyber viserait uniquement à faire connaître les études de sciences informatiques aux lycéens du coin.

Ils font quelque chose de constructif et s'ouvrent à une nouvelle discipline », estime Nasir Memon, de l'université de New York. « En répétant l'opération partout dans le pays, le gouvernement a un vrai impact dans la formation des talents. »

Les facs insistent au passage sur le fait que la NSA laisse toute latitude aux instructeurs pour définir l'organisation et le programme du camp d'été. A l'université de New York, les professeurs entendent inciter des lycéennes à poursuivre un cursus dans leur département, en formant des apprenties-hackers sur deux semaines.

Le terme « hacker » s'avère d'ailleurs quelque peu galvaudé, puisqu'il ne s'agit pas d'apprendre des techniques pour pirater des sites gouvernementaux ou des bases de données bancaires, mais plutôt de savoir mettre les mains dans le cambouis informatique.

Nous ne leur montrons pas d'outils de piratage mais plutôt ceux permettant de trouver ce qui ne va pas, dans l'optique de résoudre des crimes, d'aider les autres », précise Linda Sellie.



« On leur montre jamais rien d'illégal »

De 8h à 15h, dans une salle blafarde du deuxième étage de l'école polytechnique de l'université de New York, cette professeure spécialiste des algorithmes enseigne à une vingtaine de jeunes filles, bit par bit, le fonctionnement de la machine, de la programmation, des réseaux et d'internet, des bases de données, du cryptage… L'ambiance est studieuse. Sous des dizaines de lignes de code incompréhensibles projetées au tableau, les adolescentes s'affairent à changer des chiffres et des lettres blancs sur leurs écrans.

« C'est de la programmation informatique, ces lignes vont créer les pixels de la photo », nous explique Ashley, 17 ans, dans un sourire qui dévoile un appareil dentaire. « A la ligne 48, allez modifier les données pour dissimuler votre message dans l'image », lance sibylline Linda Sellie.

On leur montre comment l'informatique fonctionne, comment détecter des vulnérabilités et comment les réparer, mais jamais rien d'illégal », nous assure la seconde professeure, Phyllis Frankl.

A New York, trois sessions successives ont été organisées cet été, pour un total de 75 étudiantes, l'université ayant décidé de réserver ses camps aux filles, particulièrement peu présentes dans ce type de filières. Elles ont pour seul point commun d'être de bonnes élèves dans les écoles publiques environnantes. Iman, qui porte fièrement le voile islamique du haut de ses 17 ans, vient de Brooklyn et raconte être venue « pour faire quelque chose de [son] été ». Radhaka, 17 ans et d'origine pakistanaise, vit elle dans le Queens et a été encouragée ses profs « parce qu'[elle] veut devenir développeur ». Cachée derrière ses lunettes à monture large, Winxy, 18 ans, du Bronx, a vu dans ce camp « l'opportunité d'apprendre comment fonctionnent les ordinateurs », parce que « c'est toujours utile ».

Le professeure Linda Sellie note :

« Ces filles viennent avec une connaissance minimale en informatique. Elles repartiront avec une ouverture d'esprit vis-à-vis de la cybersécurité et surtout un usage plus prudent d'internet et des technologies. »

« C'est quoi déjà la NSA ? »

Si les lycéennes sont studieuses et appliquées dans leur apprentissage, elles semblent totalement indifférentes à la question de l'espionnage mené par la NSA. « C'est quoi déjà la NSA ? », interroge Iman, les sourcils froncés. Radhaka tente :

C'est l'agence de la sécurité, ils s'occupent de sécuriser des choses. »

Mira, 17 ans et originaire du New Jersey, renchérit : « Comme dans le livre 'La Forteresse digitale' », en référence au livre de Dan Brown dont l'intrigue se déroule au cœur de la NSA. Lorsque l'on évoque une surveillance généralisée des communications aux Etats-Unis, en s'appuyant notamment sur les opérateurs internet et télécom, le silence se fait. Ce sont aussi eux qui financent ce camp d'été, glisse-t-on enfin. « S'ils nous aident à étudier une discipline compliquée gratuitement, alors ils sont biens », rétorque Ashley.

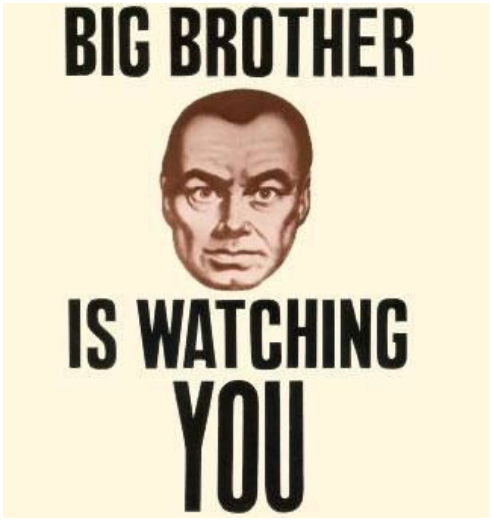
L'agence, qui espère proposer 200 camps d'ici 2020, dont au moins un par Etat, semble avoir cette année rempli son objectif. Dès la fin du premier jour de camp à New York, plusieurs élèves disent déjà envisager de travailler dans la cybersécurité, et pourquoi pas pour la NSA. C'est le cas de la discrète Ashley, qui se dit « très excitée par ce qu'elle fait ». Son nouveau défi : décoder un message dissimulé dans des photos de la Skyline de New York, pour résoudre une enquête sur un meurtre fictif.

Former des apprentis-hackers oui, mais à condition qu'ils restent du bon côté des autorités.

Source : http://tempsreel.nouvelobs.com/tech/20150828.OBS4906/a-l-ecole-de-la-cybersecurite-bienvenue-au-summer-camp-de-la-nsa.html

Par Boris Manenti

Alerte Faille Android ! Big Brother pourrait bien vous surveiller | Le Net Expert Informatique

	Alerte Faille Android ! Big Brother pourrait bien vous surveiller

Des chercheurs en sécurité ont récemment découvert une faille de sécurité considérée comme la pire jamais découverte dans le système Android. Détecté dans la bibliothèque multimédia de l'OS, ce bug nommé « Stagefright » expose près d'1 milliard de terminaux Android aux malwares.

En exploitant la faille « Stagefright », les hackers peuvent accéder aux contacts et aux autres données stockées dans un appareil mobile telles que les photos et les vidéos. Ils peuvent également accéder au microphone et à la caméra de cet appareil, ce qui leur permet d'espionner l'utilisateur via l'enregistrement de son et la prise d'images.

Tous les appareils exécutant des versions Android 2.2 Froyo jusqu'aux versions 5.1.1 Lollipop sont concernés. Cela représente environ 95% de l'ensemble des terminaux Android.

Le plus effrayant, c'est que les pirates ont uniquement besoin du numéro de téléphone de l'utilisateur pour infecter son appareil. Le malware est transmis lors de l'envoi d'un message multimédia à n'importe quelle application de messagerie pouvant traiter les formats vidéo MPEG4, telle que l'application de messagerie par défaut de l'appareil Android, Google Hangouts ou Whatsapp. Comme ces applications de messagerie Android récupèrent automatiquement des vidéos ou du contenu audio, le code malveillant est exécuté sans que l'utilisateur n'ait besoin de faire quoi que ce soit. En effet, la faille n'exige pas que la victime ouvre le message ou clique sur un lien. Il s'agit d'un malware unique en son genre car ce type de menace nécessite généralement une action de la part de l'utilisateur pour que l'appareil soit infecté. Il pourrait par exemple être relayé via un lien envoyé par courrier électronique ou partagé sur les réseaux sociaux. Toutefois, cela nécessiterait encore et toujours une action de la part de l'utilisateur, puisque le chargement d'une vidéo se fait uniquement via l'ouverture d'un lien. Cela est extrêmement dangereux, car si les utilisateurs sont infectés via MMS, aucune action ne leur sera demandée et les effets indésirables seront imperceptibles. Avant même que les victimes s'en aperçoivent, le hacker est en mesure d'exécuter le code et de retirer toute trace attestant que l'appareil a été infecté.

Le rêve du cybercriminel et du dictateur

Les cybercriminels profitent de cette faille de sécurité pour espionner des millions de personnes et exécuter d'autres codes malveillants. Les gouvernements répressifs pourraient abuser de ce bug en vue d'espionner leurs citoyens ou leurs ennemis. Toutefois, ce bug pourrait également être utilisé à des fins d'espionnage apolitique. Les pirates peuvent facilement surveiller les personnes de leur entourage comme leur conjoint ou leurs voisins. Ils n'ont besoin pour ce faire que du numéro de téléphone de la personne visée. Les hackers ont aussi la possibilité de dérober des informations personnelles qu'ils utiliseront pour faire chanter des millions de personnes ou usurper leur identité. Les conséquences possibles de ce type de faille sont donc à prendre au sérieux.

Une nécessité urgente de patchs

Des patchs complets doivent désormais être fournis par les fabricants de téléphones à l'aide d'une mise à jour à distance ou « over-the-air » (OTA) d'un firmware pour les versions Android 2.2 et plus. Malheureusement, les mises à jour pour appareils Android ont toujours mis beaucoup de temps pour arriver jusqu'à l'utilisateur final. Espérons que les constructeurs réagiront plus rapidement dans ce cas précis.

Google y a pour sa part déjà répondu d'après un témoignage d'HTC publié dans le magazine d'information hebdomadaire américain Time : « Google a informé HTC de cette problématique et fourni les patchs nécessaires qu'HTC a commencé à prendre en compte dans les projets mis en œuvre au début du mois de juillet. Tous les projets en cours contiennent le patch requis. » Pour le moment et par mesure de précaution, il est recommandé aux utilisateurs de désactiver la fonction récupération automatique des MMS dans les paramètres par défaut de l'application de messagerie.

Source : http://www.journaldun
et.com/solutions/expert/61932/big-brother-po
urrait-bien-vous-surveiller-grace-a-la-faille-stagefright.shtml
Par Filip Chytrý

Les cyber-attaques provenant

du Dark Web empruntent de plus en plus le réseau Tor | Le Net Expert Informatique

	Les cyber-attaques provenant du Dark Web empruntent de plus en plus le réseau Tor

I**BM Sécurité vient de dévoiler les résultats de son rapport Q3 2015 IBM X-Force Threat Intelligence. Celui-ci pointe les dangers grandissants provoqués par les cyber-attaques provenant du Dark Web à travers l'utilisation du réseau Tor (The Onion Router), ainsi que les nouvelles techniques mises en place par les criminels pour les attaques avec rançon. Rien que depuis le début de l'année, plus de 150 000 événements malveillants provenant de Tor ont eu lieu aux Etats-Unis.**

Même si on entend davantage parler des fuites de données que des demandes de rançon, les « ransomware » représentent une menace grandissante. Comme la sophistication des menaces et des attaquants croît, leur cible fait de même, et ainsi certains attaquants se sont par exemple spécialisés dans la demande de rançon concernant les fichiers de joueurs de jeux en lignes populaires. Le rapport dévoile que les agresseurs peuvent maintenant également bénéficier de « Ransomware as a Service » en achetant des outils conçus pour déployer de telles attaques.
Comme les hauts fonds des océans, le Dark Web demeure largement inconnu et inexploré, et il héberge des prédateurs. L'expérience récente de l'équipe IBM Managed Security Services (IBM MSS) montre que les criminels et d'autres organisations spécialisées dans les menaces utilisent Tor, qui permet d'anonymiser les communications aussi bien en tant que vecteur d'attaques que d'infrastructure, pour commander et contrôler les botnets. La façon dont Tor masque le cheminement offre des protections supplémentaires aux attaquants en les rendant anonymes. Ils peuvent aussi masquer la location physique de l'origine de l'attaque, et même la remplacer par une autre de leur choix.
Le rapport étudie également Tor lui-même, et fournit des détails techniques permettant de protéger les réseaux contre les menaces, intentionnelles ou non, véhiculées par Tor.
Le rapport est accessible ici.

Source : http://www.infodsi.com/art
icles/157784/cyber-attaques-provenant-dark-web-emprunt
ent-plus-plus-reseau-tor.html