Comment un cybercriminel peut infiltrer votre réseau ?

Comment un cybercriminel peut infiltrer votre réseau ?

La sécurité est plus que jamais une priorité pour les entreprises, contribuant activement à sa réussite. Les RSSI doivent désormais s'assurer que leurs projets en matière de sécurité IT sont en phase avec les objectifs de l'entreprise.

Nous sommes tous connectés à Internet, ce qui est très positif. Mais ce lien permanent implique que nous sommes tous au cœur d'un écosystème de grande envergure. Il est essentiel de comprendre que tout ce qui touche une organisation impactera également de nombreuses autres entreprises, et notamment ses partenaires.
Ainsi, en cas de piratage d'une entreprise, ce sont des données personnelles identifiables qui sont détournées. Ces données peuvent être revendues à des spécialistes de l'usurpation d'identité ou constituer un terreau favorable aux attaques de phishing. Plus l'assaillant disposera d'informations sur vous, plus l'email qu'il vous enverra apparaîtra comme légitime et vous incitera à cliquer sur un lien malveillant.
Notons que les tactiques d'attaques actuelles sont similaires à celles d'il y a quelques années : récupération de mots de passe faibles, attaques de type phishing et téléchargement de logiciels malveillants à partir de sites web infectés ou de publicités malveillantes. Sauf qu'aujourd'hui, l'assaillant a gagné en furtivité et en efficacité lorsqu'il mène son attaque.

Penchons-nous, par exemple, sur les réseaux sociaux et les services en ligne. Nous sommes très nombreux à les utiliser, qu'il s'agisse de Facebook, de LinkedIn, ou encore des sites de rencontres en ligne. Les assaillants l'ont parfaitement compris et capitalisent sur la fibre émotionnelle de chacun. Ils établissent ainsi leur passerelle d'entrée vers les dispositifs des utilisateurs en s'aidant de ces sites et de techniques d'ingénierie sociale. Ainsi, si les méthodes d'ingénierie sociale restent les mêmes, les vecteurs et la surface d'attaque ont, en revanche, progressé. Parallèlement, ce sont les techniques de furtivité qui ont gagné en précision, avec des assaillants toujours plus aptes à se dissimuler. Se contenter d'utiliser les antivirus traditionnels n'est donc tout simplement plus suffisant.
Parmi les techniques utilisées, l'attaque de type phishing est la méthode principale pour s'immiscer au sein des réseaux d'entreprise.
Un email de phishing, conçu pour paraître le plus légitime possible, est envoyé avec un fichier joint ou une URL malveillante, et incitant l'utilisateur à ouvrir le fichier ou à cliquer sur l'URL. L'attaque par téléchargement furtif (ou drive–by attack) est une autre technique utilisée par les assaillants. Ces derniers piratent un site Web et y installent un script java malveillant qui redirigera l'utilisateur vers un autre site hébergeant un logiciel malveillant téléchargé en arrière-plan vers l'équipement de l'utilisateur. Dans le cas d'une attaque ciblée, les assaillants peuvent passer des mois à identifier les sites Web les plus consultées par les organisations ciblées, pour ensuite les infecter.
Le malvertising (publicité malveillante) compte également parmi les techniques utilisées. Cette attaque emprunte les codes des attaques drive-by, mais l'assaillant se focalisera sur l'infection des sites de publicités. Il devient possible d'infecter un seul de ces sites qui, à son tour, pourra infecter jusqu'à 1 000 autres sites Web. Ou l'art d'industrialiser son attaque.
Enfin, n'oublions pas l'attaque mobile. Nombre de ces attaques sont similaires à celles mentionnées plus haut, mais elles ciblent les dispositifs mobiles. Notons qu'il est possible d'infecter un dispositif mobile via un message SMS, ou à l'aide d'un logiciel malveillant qui se présente en tant qu'application ludique ou de contenu pour adultes.
Lorsque l'assaillant est rentré dans un réseau et qu'il réside sur le dispositif d'un utilisateur (ordinateur de bureau ou portable, équipement mobile), il doit désormais injecter de nouveaux logiciels malveillants et outils pour mener à bien sa mission. Généralement, les informations de valeur ne sont pas stockées sur les postes de travail, mais plutôt sur les serveurs et des bases de données.

Voici donc un aperçu des étapes supplémentaires pouvant être mises en œuvre par un cybercriminel déjà présent dans le réseau:
• Téléchargement d'autres outils et logiciels malveillants pour compromettre davantage le réseau.
• Exploration du réseau pour identifier les serveurs hébergeant les données ciblées.
• Recherche du serveur Active Directory contenant tous les identifiants d'authentification, dans l'objectif de pirater ces données, véritable sésame pour le cybercriminel.
• Une fois les données ciblées identifiées, recherche d'un serveur provisoire pour y copier ces données. Le serveur idéal est un serveur stable, à savoir toujours disponible, et disposant d'un accès sortant vers Internet.
• Exfiltration furtive et lente de ces données vers les serveurs des assaillants, généralement déployés dans le cloud, ce qui rend la neutralisation des communications plus complexe.

Les cybercriminels présents au sein du réseau sur une longue durée pourront obtenir tous types d'informations disponibles puisque les données d'entreprise, dans leur grande majorité, sont archivées sous format électronique. Plus le cybercriminel est présent sur le réseau, plus il en apprend sur les processus et les flux de données de votre entreprise. L'attaque Carbanak qui a ciblé de nombreuses banques dans le monde en est la parfaite illustration. Lors de cette exaction, les cybercriminels sont remontés jusqu'aux ordinateurs des administrateurs ayant accès aux caméras de vidéosurveillance. Ils ont ainsi pu surveiller de près le fonctionnement du personnel bancaire et enregistrer tous les processus dans le détail. Ces processus ont été reproduits par les cybercriminels pour transférer des fonds vers leurs propres systèmes.
Comme déjà souligné, une brèche dans le réseau s'initie généralement par un simple clic d'un utilisateur sur un lien malveillant. Après avoir investi le poste de l'utilisateur piraté, l'assaillant commence à explorer le réseau et à identifier les données qu'il souhaite détourner. C'est dans ce contexte que la notion de segmentation de réseau devient essentielle. Cette segmentation permet de maîtriser l'impact d'un piratage puisque l'entreprise victime peut isoler la faille et éviter tout impact sur le reste du réseau. D'autre part, elle permet de cloisonner les données sensibles au sein d'une zone hyper-sécurisée qui rendra la tâche bien plus complexe pour ceux qui souhaitent les exfiltrer. Pour conclure, gardons à l'esprit qu'il est impossible de protéger et de surveiller le réseau dans sa totalité, compte tenu de son périmètre étendu et de sa complexité. Il s'agit donc d'identifier les données les plus sensibles, de les isoler et de porter son attention sur les chemins d'accès vers ces données.

Réagissez à cet article

Source : *Comment un cybercriminel peut infiltrer votre réseau | Data Security Breach*

Que trouve-t-on dans le darknet ?

Que trouve-t-on dans le darknet ?

Sur le darknet, les pages Internet ne sont pas indexées. Vous ne pouvez donc pas les trouver via les moteurs de recherche classiques, comme Google ou Yahoo par exemple. Vous ne pouvez pas non plus y accéder par votre navigateur habituel, comme Internet Explorer ou Mozilla. Ces pages ne répondent pas au codage classique du genre « .fr » ou « .net ». Elles se terminent par « .oignon » : pour que les échanges soient anonymes sur cet Internet caché, il faut passer par une multitude de relais, comme plusieurs couches d'un oignon.

Tous ces relais expliquent pourquoi sur le darknet la connexion est plus longue. Au départ, cet Internet fantôme qui garantit l'anonymat a été créé pour aider à la liberté d'information dans des pays où tout est verrouillé, comme en Chine. Les dissidents pouvaient, via le darknet, communiquer de manière protégée. Un anonymat et une clandestinité largement détournés à des fins malhonnêtes : ventes d'armes, pédophilie ou drogues pullulent sur ce Web caché. L'un des logiciels les plus utilisés pour surfer sur le darknet s'appelle Tor (pour The Onion Router). On estime que les sites Internet sur le Web crypté sont 500 fois plus nombreux que sur le Web traditionnel.

Réagissez à cet article

Source : *Internet : que trouve-t-on dans le darknet ?*

Quels sont les gadgets de la NSA utilisés par la police ?

Quels sont les gadgets de la NSA utilisés par la police ?

The Intercept a pu mettre la main sur un catalogue de périphériques utilisés par les agences américaines de renseignement pour espionner et collecter des données. Un inventaire digne de James Bond. Des questions se posent quant à la légalité de ces appareils et la nécessité d'encadrer leur utilisation par la justice.

A vos portefeuilles ! En effet, les équipements présentés par *The Intercept* et que l'on peut découvrir à cette adresse ne sont accessibles ni à toutes les bourses ni à tous les quidams. Il s'agit en effet d'appareils particulièrement sophistiqués qui permettent aux agences américaines, et tout particulièrement la NSA, de se livrer à leurs activités d'écoute et de surveillance. Certains de ces appareils sont fixes alors que d'autres peuvent être installés dans des automobiles, avions ou drones. Ces différents appareils portent des noms évocateurs comme Cyberhawk, Yellowstone, Blackfin, Maximus, Cyclone ou encore Spartacus. Selon notre confrère, un tiers de ces équipements n'auraient jamais été décrits publiquement jusqu'à présent.

Les possibilités sont différentes selon les appareils. Certains sont destinés à cibler 10000 identifiants téléphoniques différents. La plupart sont capables de géolocaliser les personnes ciblées et, selon les modèles, des fonctions plus avancées comme l'écoute des appels ou la capture des SMS sont proposées. Deux modèles permettent de récupérer les fichiers contenus sur les smartphones ainsi que les carnets d'adresses, notes ou encore récupérer les messages préalablement supprimés.

Spoofing d'adresses

L'un des appareils les plus répandus est le StingRay qui est utilisé pour récupérer les conversations en se faisant passer pour les relais officiels des opérateurs mobiles comme Verizon, AT&T et autres. Cette technique d'interception, baptisée Spoofing, est aujourd'hui largement répandue non seulement par les agences de renseignement mais également par la police fédérale ou municipale. Et c'est là que les défenseurs des libertés individuelles commencent à se faire entendre, arguant que l'utilisation de ces appareils n'est pas suffisamment encadrée et que des dizaines de milliers de personnes voient leurs conversations espionnées au seul motif qu'elles se trouvent dans une même zone géographique qu'une personne suspectée et écoutée.

Stingray I/II

Ground Based Geo-Location (Vehicular)

"Ensnares bystanders, drains batteries, blocks calls"

Review by Nathan Wessler

$134,952.00

Le 4ème amendement mis à mal

Les défenseurs de la vie privée expliquent que l'utilisation de ces appareils, dans des conditions pas ou trop peu encadrées, viole le 4ème amendement de la constitution américaine. En effet, dans un premier temps, ces différents appareils, et tout particulièrement le StingRay commercialisé par la société Harris, était essentiellement utilisé à des fins militaires ou par des agences fédérales. Cependant à partir de 2007, l'usage croissant fait par les polices municipales a commencé à poser problème car cette utilisation semble s'effectuer hors de tout cadre juridique. *The Intercept* prend l'exemple de la police de Baltimore qui a utilisé le StingRay plus de 4300 fois depuis 2007. Comme à l'habitude, la lutte contre le terrorisme sert de viatique à l'emploi de ces appareils et techniques de surveillance. Toutefois, cet argument laisse trop souvent à désirer. En effet, nos confrères citent le cas de la police de l'Etat du Michigan qui a employé 128 fois le StingRay l'année dernière dans le but d'identifier la localisation physique d'une personne suspectée de terrorisme mais l'Association de défense des libertés civiles a précisé que sur les 128 utilisations aucune n'avait un quelconque rapport avec un acte terroriste.

Des fonds douteux utilisés pour les acquérir

Plus ennuyeuses encore sont les modalités d'acquisition de ces appareils. En effet, puisqu'ils sont achetés « hors la loi », les fonds utilisés sont également hors la loi et proviendraient de saisies financières lors des découvertes de trafics en tous genres, de drogue notamment. *The Intercept* écrit que les forces de police de l'Illinois, du Michigan et du Maryland ont utilisé des fonds d'origine crapuleuse pour procéder à leurs achats. L'accusation est particulièrement grave puisque cela revient à accuser les services de police de blanchiment d'argent sale pour mener des opérations notoirement illégales.

Dans ces conditions, un certain nombre de juges américains s'alarment des dérives et souhaitent une évolution de la loi encadrant l'utilisation de ces appareils. Au mois de novembre dernier, le juge fédéral de l'Illinois, Iain Johnston a publié un mémorandum sur la manière dont avaient été utilisées ces techniques de spoofing dans une enquête autour d'un trafic de drogue. « *Un simulateur de ce type est simplement trop puissant et les informations capturées sont trop vastes pour que l'autorisation d'emploi ne soit pas délivrée par une cour dûment habilitée* ».

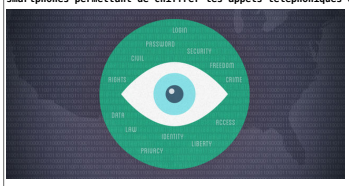
Réagissez à cet article

Source : *Les gadgets de la NSA utilisés par toute la police*

Des communications téléphoniques sécurisées avec Signal

Des communications téléphoniques sécurisées avec Signal

A 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.



À 23 ans, Frederic Jacobs est déjà une célébrité dans le milieu de la cryptologie. Ce jeune Belge, étudiant-chercheur à l'Ecole polytechnique de Lausanne (Suisse), est l'un des trois créateurs de Signal, une application gratuite pour smartphones permettant de chiffrer les appels téléphoniques et les SMS.

Les communications entre deux appareils équipés de Signal passent par l'Internet ouvert, mais restent indéchiffrables pour tout observateur extérieur. N'importe quel possesseur de smartphone peut ainsi disposer, sans formalités ni inscription, d'un service naguère réservé aux chefs d'Etat, aux PDG de multinationales et aux agents secrets.

La nouveauté de Signal est que l'on n'a pas besoin d'être un « geek » pour s'en servir : une fois l'application chargée, tout se fait automatiquement. « Les systèmes précédents en demandaient trop aux utilisateurs, relève Frédéric Jacobs. C'est pour ça que jusqu'à présent, le grand public a très peu utilisé le chiffrement. » Il fait allusion à PGP (Pretty Good Privacy), inventé il y a 25 ans par l'Américain Philip Zimmermann, pionner mondial du chiffrement sur Internet.

PALLIER LA DIFFICULTÉ DU CHIFFREMENT

Outre la facilité d'utilisation, l'autre objectif prioritaire de Signal était de proposer un chiffrement intégral, de bout en bout. « Le cryptage et le décryptage se font à l'intérieur de votre téléphone, explique Frederic Jacobs. Quand vous chargez l'application, elle crée automatiquement une centaine de clés de chiffrement, qui restent stockées dans l'appareil. »

Le système permet une rotation systématique : « Chaque clé servira une seule fois. Quand vous recevez un message, vous utilisez une clé qui se détruira aussitôt, et quand vous envoyez un message, l'application crée une nouvelle clé. De cette façon, si un attaquant voulait casser le chiffrement de vos communications, il serait obligé de recommencer le travail pour chaque message. Et s'il s'emparait d'une clé, il ne pourrait pas lire vos vieux messages. »

Frédéric Jacobs travaille avec deux développeurs américains installés à San Francisco : Moxie Marlinspike, un vétéran du chiffrement sur mobile qui a vendu sa première startup à Twitter, et Lilia Kai, ex-militante de l'Electronic Frontier Foundation, association de défense des libertés numériques. Au total, l'équipe permanente de Signal se compose de cinq personnes. Elle est financée par des fondations américaines engagées dans la défense des libertés sur Internet, notamment la Freedom of the Press Foundation et l'Open Technology Fund.

Le budget reste serré, et les salaires modestes. Pour gagner correctement sa vie, Frederic Jacobs travaille comme consultant informatique pour des entreprises. A court terme, cet arrangement le satisfait : « A aucun moment je n'ai pensé à m'enrichir grâce à Signal. Auparavant, j'ai travaillé dans des startups, mais j'ai vite été dégoûté par l'ambiance. Aujourd'hui, je fais partie d'une organisation libérée de l'influence perverse de l'argent. Et rassurez-vous, nous n'allons pas nous vendre à Google. »

UN LARGE PUBLIC EN ALLEMAGNE ET AUX ÉTATS-UNIS

En ces temps d'état d'urgence et de guerre contre le terrorisme, les créateurs de logiciels de chiffrement se sont fait des ennemis puissants, depuis le directeur du FBI jusqu'au premier ministre britannique. De plus en plus, les responsables politiques et policiers exigent que les développeurs créent des backdoors (portes de derrière), par exemple des systèmes permettant de récupérer les clés de chiffrement d'utilisateurs visés par des enquêtes.

Frederic Jacobs assure que Signal ne possède aucune backdoor, et qu'il peut le prouver : « Notre code est en open source, disponible librement sur Internet. Tous les experts peuvent l'analyser et le décortiquer à loisir. » Il affirme aussi qu'à ce jour, Signal n'a subi aucune pression, officielle ou autre : « Personne n'est venu nous voir, peut-être parce que nous sommes encore peu connus. »

Signal ne donne pas de chiffre précis sur son nombre d'utilisateurs, mais l'application a été chargée plusieurs millions de fois. Les plus gros contingents sont aux Etats-Unis et en Allemagne : « Signal a été adopté par des hauts fonctionnaires, y compris à Washington, mais aussi par des familles ordinaires qui veulent protéger les communications de leurs enfants, ou des jeunes couples qui s'échangent des photos intimes… »

Signal dispose de dizaines de relais sur tous les continents. Fin décembre, les principaux se trouvaient aux Etats-Unis (côte est et côte ouest), en Allemagne, en Irlande, au Brésil, en Australie et à Singapour : « Leur nombre exact varie en fonction des besoins, explique Frederic Jacobs, ce sont des serveurs ordinaires, qui se louent à la minute. Si par exemple, le trafic est important en Allemagne vers 17 heures, nous ajoutons des relais locaux, et s'il baisse à 18 heures, nous en retirons. »

Signal possède aussi un serveur central, installé aux Etats-Unis, qui envoie les notifications aux appareils avant un appel. De ce fait, le système n'est pas complètement invulnérable. Si un attaquant réussit à avoir accès à un serveur, par effraction ou lors d'une perquisition, il ne pourra pas déchiffrer le contenu des messages, mais pourra s'emparer des informations techniques dont le réseau a besoin – origine et destination des messages, date et durée des appels… En ce sens, Signal n'a pas été pensé pour les lanceurs d'alerte qui doivent rester totalement inconnus des autorités.

Pour le reste, les cryptologues célèbres qui ont audité le code de Signal se sont dit impressionnés par sa qualité. La consécration la plus éclatante vient de Philip Zimmermann qui travaille aujourd'hui pour Silent Circle, société américaine offrant un service payant de chiffrement des communications, dont le siège social est en Suisse depuis 2014. Créée par des anciens membres des commandos d'élite de l'US Navy et visant une clientèle haut de gamme, ainsi que les militaires et les humanitaires en mission, Silent Circle, pour les messages-texte, a abandonné son ancien protocole de chiffrement, et a adopté celui de Signal.

Réagissez à cet article

Source : *Signal, une application pour téléphoner de manière sécurisée*

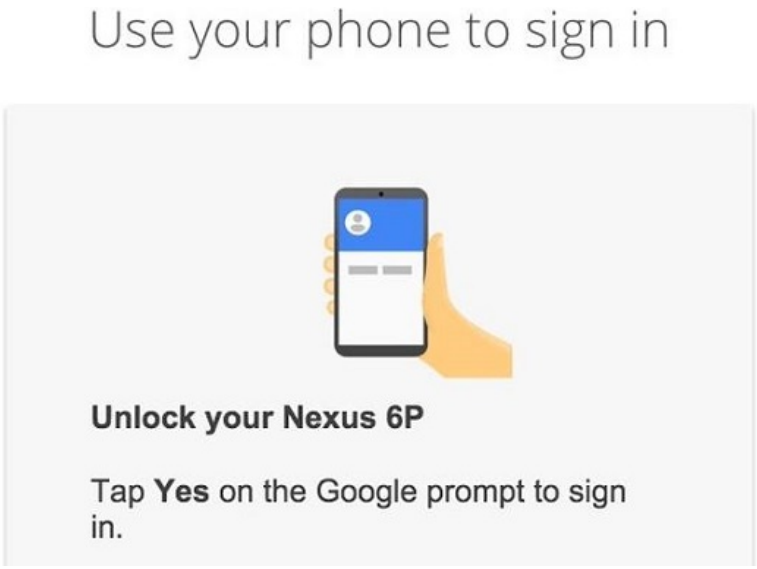
Google propose d'utiliser son téléphone en guise de mot de passe

Google propose d'utiliser son téléphone en guise de mot de passe

Saisir sur votre ordinateur un long mot de passe pour accéder à votre compte Google pourrait devenir une chose du passé pour peu que vous ayez en poche votre téléphone mobile.

Google s'efforce depuis longtemps de retirer les différentes barrières s'opposant à un accès rapide aux données. Et il pourrait bien avoir un nouveau tour dans son sac : au lieu de saisir comme d'habitude un mot de passe depuis son PC, sa tablette ou un autre terminal, vous pourriez simplement utiliser votre téléphone pour vous authentifier.
L'utilisateur de Reddit, Rohit Paul, a été invité à tester la fonctionnalité, qui nécessite encore un peu de saisie de la part de l'internaute.

Adresse Gmail saisie sur un mobile pour se connecter sur PC



Comme relevé par Android Police, une fois le téléphone de Rohit Paul enrôlé comme terminal d'authentification, ce dernier n'a plus eu qu'à entrer son adresse Gmail sur son smartphone pour se connecter à Google depuis son ordinateur.
Si le processus ne s'avère pas aussi rapide pour tous, ceux dont le mot de passe Google compte de nombreux caractères pourraient en profiter en réduisant le temps de saisie nécessaire à l'authentification.
Naturellement, si vous perdez votre téléphone ou si vous ne souhaitez plus utiliser ce mode d'authentification, vous pouvez toujours vous connecter à votre compte Google de manière classique.
Google n'ayant pas annoncé officiellement cette nouvelle fonctionnalité, les détails techniques de la procédure d'accès restent inconnus. La firme de Mountain View n'est cependant pas la seule à vouloir s'affranchir des mots de passe et à développer des méthodes alternatives d'authentification. C'est par exemple le cas de Microsoft dans Windows 10 au travers d'une fonction comme Next Generation Credentials.

Réagissez à cet article

Source : *Google souhaite remplacer le mot de passe par votre téléphone*

Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender publie ses prévisions en matière de sécurité. Dans son rapport, Bitdefender énonce les cinq évolutions notables qui impacteront notre façon de travailler, de jouer et de se sociabiliser sur Internet, au cours de l'année prochaine.

L'année 2016 verra un changement majeur dans la façon dont opèrent les cybercriminels. Le domaine probablement le plus impacté par cette refonte sera celui des PUA, dont l'activité s'est déjà accrue sur des plates-formes telles que Mac OS X et Android.
Suite aux nombreuses fermetures de réseaux de machines zombies et arrestations en 2015, les nouveaux cybercriminels transiteront probablement vers des systèmes de monétisation publicitaire spécifiques aux adwares agressifs, plutôt que de développer de nouvelles souches de malwares. Si pour le moment les botnets constituent toujours une partie importante de l'écosystème de la cybercriminalité, nous assisterons à une augmentation de la sophistication des PUA et des programmes incluant plus de greywares à l'installation.

La publicité sur le Web va également évoluer : étant donné le taux d'adoption ainsi que la popularité des bloqueurs de publicités, les régies publicitaires chercheront à utiliser des mécanismes plus agressifs afin de contourner ces blocages.

Les APT abandonneront le facteur de longévité
Les entreprises et les institutions gouvernementales feront toujours face à des attaques de ce type tout au long de 2016. Cependant, les APT (Advanced Persistent Threats, menaces persistantes avancées) mettront l'accent sur l'obfuscation et la récolte d'informations plutôt que sur la longévité. Les pirates ne s'infiltreront sur le réseau de l'entreprise que quelques jours, voire quelques heures.
Le monde de l'entreprise connaîtra une augmentation des attaques ciblées et des bots fortement obfusqués, avec une courte durée de vie et des mises à jour fréquentes, estime Dragoş Gavriluţ, Chef d'équipe au sein des Laboratoires antimalwares de Bitdefender. La plupart de ces attaques se spécialiseront dans le vol d'informations.
Également, l'évolution latérale de l'infrastructure des fournisseurs de services Cloud ira de pair avec l'avènement d'outils permettant aux pirates de compromettre l'hyperviseur à partir d'une instance virtuelle et de passer d'une machine virtuelle à l'autre. Ce scénario est particulièrement dangereux dans des environnements de « mauvais voisinage », où un tiers mal intentionné serait amené à partager des ressources sur un système physique avec un fournisseur de services ou une entreprise légitimes.

Des malwares mobiles de plus en plus sophistiqués
Du côté des particuliers, les types de malware sous Android sont désormais globalement les mêmes que sous Windows. Alors que les rootkits sont en perte de vitesse sur Windows, ils vont probablement devenir monnaie courante sur Android et iOS, car les deux plates-formes sont de plus en plus complexes et offrent une large surface d'attaque, affirme Sorin Dudea, Chef de l'équipe de recherche antimalwares. De nouveaux malwares mobiles, aux comportements similaires à ceux des vers, ou un réseau botnet mobile géant, sont deux autres possibilités envisagées pour l'année prochaine, selon Viorel Canja, Responsable des Laboratoires antimalwares et antispam chez Bitdefender. Ces attaques pourraient être la conséquence de techniques d'ingénierie sociale ou de l'exploitation de vulnérabilités majeures (telles que Stagefright) sur des plates-formes non patchées.

L'Internet des Objets (IOT) et la vie privée
La façon dont nous gérons notre vie privée va aussi changer durant l'année 2016. En effet, les récents vols de données ont contribué à mettre une quantité importante d'informations personnelles en libre accès sur Internet, rendant ainsi le « doxing » (processus de compilation et d'agrégation des informations numériques sur les individus et leurs identités physiques) beaucoup plus facile pour des tiers.
Les objets connectés vont devenir de plus en plus répandus, donc plus attrayants pour les cybercriminels. Compte tenu de leur cycle de développement très court et des limites matérielles et logicielles inhérentes à ce type d'objet, de nombreuses failles de sécurité seront présentes et exploitables par les cybercriminels ; c'est pourquoi la plupart des objets connectés seront compromis en 2016, ajoute Bogdan Dumitru, Directeur des Technologies chez Bitdefender. Également, les réglementations de surveillance de type « Big Brother », que de plus en plus de pays essaient de mettre en place pour contrecarrer le terrorisme, déclencheront des conflits quant à la souveraineté des données et le contrôle de leur mode de chiffrement.

Les ransomwares deviennent multiplateformes
Les ransomwares sont probablement la menace la plus importante pour les internautes depuis 2014 et resteront l'un des plus importants vecteurs de cybercriminalité en 2016. Alors que certains pirates préfèrent l'approche du chiffrement de fichiers, certaines versions plus novatrices se concentreront sur le développement de « l'extortionware » (malware qui bloque les comptes de services en ligne ou expose les données personnelles aux yeux de tous sur Internet).
Les ransomwares visant Linux vont se complexifier et pourraient tirer parti des vulnérabilités connues dans le noyau du système d'exploitation pour pénétrer plus profondément dans le système de fichiers. Les botnets qui forcent les identifiants de connexion pour les systèmes de gestion de contenu pourraient aussi se développer. Ces identifiants pourraient être ensuite utilisés par les opérateurs de ransomwares visant Linux pour automatiser le chiffrement d'une partie importante d'Internet.
Enfin, les ransomwares chiffrant les fichiers s'étendront probablement aux systèmes sous Mac OS X, corrélant ainsi avec les travaux de Rafael Salema Marques et sa mise en garde illustrée autour de son 'proof of concept' malware nommé Mabouia. En effet, si le principe de conception de Mabouia reste pour le moment privé, il pourrait être créé par des cybercriminels enrichissant alors leurs offres orientées MaaS (Malware-As-A-Service).

Réagissez à cet article

Source : *Bitdefender : Les 5 tendances en cybercriminalité pour 2016 – Global Security Mag Online*

Hello Kitty : les données de

millions de fans compromises

Hello Kitty : les données de millions de fans compromises

Les données personnelles de millions fans d'Hello Kitty étaient facilement accessibles. C'est un chercheur en sécurité Chris Vickery qui a donné l'alerte. Il a découvert une base contenant les informations de plus de trois millions d'utilisateurs, tels que nom, prénom, pays d'origine, emails, mots de passe. La société japonaise Sanrio qui gère la licence Hello Kitty assure avoir comblé la faille de vulnérabilité.

Et pour l'heure, l'entreprise assure aussi n'avoir détecté aucun vol de données. Une mauvaise configuration serait à l'origine du problème.
A quelques jours de Noël, la nouvelle passe mal. Le mois dernier déjà, c'est le fabricant de jouets hongkongais VTech qui était sur la sellette après le piratage de centaines de milliers de comptes et de profils d'enfants.

Réagissez à cet article

Source : *Hello Kitty : les données de millions de fans compromises | euronews, monde*

Les entreprises doivent prendre au sérieux la protection des données

Les entreprises doivent prendre au sérieux la protection des données

---

L'intelligence économique est devenue un mode de gestion (Le management est la mise en ?uvre des moyens humains et matériels d'une entreprise pour (…)) et de gouvernance de l'entreprise. Cet ouvrage réfléchit sur la démarche que le chef d'entreprise peut entreprendre pour éclairer ses décisions, garder sa marge de manoeuvre de compétitivité et toutes ses possibilités de développement afin de sécuriser sa pérennité.

Traitement de l'information et renseignements

Un renseignement utile peut être obtenu de façon proactive, active, ou réactive.

Le cycle de renseignement pour l'entreprise doit s'intégrer au processus de veille stratégique sur les différents volets de l'intelligence économique : veille technologique, veille d'image, veille concurrentielle, etc.

L'intelligence économique distingue trois niveaux d'information utile au renseignement :

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_2_0.jpg

L'intelligence économique ne cherche pas à obtenir l'information noire. Elle se limite à l'information que l'on peut obtenir par des moyens légaux (ex : pour se protéger des problèmes de réputation, d'escroquerie, de fraude, de cybercriminalité, de propriété intellectuelle, de savoir-faire, de brevets, etc.).

Il s'agit surtout de formaliser de façon pragmatique, ou de rendre systématique, une démarche proactive de veille dans ce domaine, notamment pour l'obtention de l'information « grise ».

Les PME sont souvent très en retrait sur la construction du savoir (ex : suivi des avancées des concurrents, organisation de la veille juridique, réglementaire, lobbying, etc.).

Sécurité et protection de l'information

Trop peu d'entreprises prennent au sérieux la protection des données. Il devient impératif de disposer d'un solide processus de sauvegarde, de prévention, d'action, et de réaction aux pannes et aux attaques informatiques. Notons ici que certaines entreprises sensibles aux problématiques de reprise après incident commencent à considérer les prestations d'externalisation applicatives (Cloud computing ou autres solutions) pour optimiser le niveau de sécurité des données.

Quantité et gouvernance des données

Les données sont la base de l'information, et comme le disent souvent les anglo-saxons: « data is the oil of the 21st century ». Savoir chercher et collecter l'information, la traiter et la diffuser (tout en protégeant la part de données sensibles qui doivent être protégées), constitue une tâche prioritaire de tous les acteurs économiques, et la définition même de l'intelligence économique.

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_3_0.jpg

Le pouvoir c'est l'information, mais à condition qu'elle soit de qualité …

La direction et les organes sociaux doivent s'appuyer sur des informations de qualité (fiables, précises, actualisées)

Read more at http://www.atlantico.fr/decryptage/entreprises-doivent-prendre-au-serieux-protection-donnees-gouvernance-et-intelligence-economique-en-pme-georges-nurdin-daniel-2494228.html##Vrl3qqLdiB14upbK.99

Réagissez à cet article

Source : *Marketing/ Les entreprises doivent prendre au sérieux la protection des données*

Vaincre les attaques DoS/DDoS en temps réel

Vaincre les attaques DoS/DDoS en temps réel

La vulnérabilité des serveurs DNS des fournisseurs de services vis-à-vis des attaques DoS/DDoS est bien réelle et s'intensifie à un rythme effréné, mettant ainsi en péril l'expérience utilisateur des clients ainsi que la réputation des fournisseurs de services.

Les techniques actuelles visent à arrêter les attaques en dotant le site du fournisseur de matériel supplémentaire ou en identifiant le coupable caché dans le logiciel malveillant sur le site du client. Cependant, ces deux méthodes sont onéreuses et ne permettent de résoudre le problème que partiellement. La nouvelle approche consiste à intégrer la protection contre les attaques DoS/DDoS directement dans un serveur cache DNS à haute fiabilité et à contrecarrer l'attaque en temps réel au moment où elle pénètre dans l'infrastructure, la désamorçant avant même qu'elle n'affecte les performances ou le service.
Lire la suite…

Réagissez à cet article

Source : *InfoBlox*

Juniper : une faille de sécurité permettait de surveiller le trafic VPN

	**Une faille de sécurité permettait de surveiller le trafic VPN**

La firme indique avoir découvert des portes dérobées dans ScreenOS, présent dans ses pare feux et services VPN. Par mesure de sécurité, Juniper a mis à jour son système d'exploitation.

Juniper indique qu'un morceau de code informatique non-autorisé était présent dans son système d'exploitation maison. Ce dernier est utilisé pour une partie de ses solutions de sécurité tels que les firewall et les services de VPN. La société a donc émis un bulletin de sécurité au sujet de ce code-espion.
Ce dernier aurait été initialement publié en 2008, de quoi laisser le temps aux éventuels attaquants d'utiliser cette porte dérobée pour utiliser des informations transitant par le biais de ces équipements. Un correctif est donc actuellement déployé par Juniper, en particulier pour les équipements de la gamme NetScreen.
Malgré ces mises à jour de sécurité, Juniper n'a pas identifié la provenance de ce code aux effets malfaisants. Si la thèse des services de renseignement n'est pas à exclure, il pourrait également s'agir de hackers ou même de développeurs présents en interne (voire des sous-traitants).

La porte dérobée doit en principe permettre à un attaquant d'accéder à distance en mode administration à un équipement sous ScreenOS. Quant à la seconde vulnérabilité mise au jour par Juniper, elle autorise un pirate à surveiller un trafic au sein d'un VPN.
Malgré l'ampleur du problème, la direction se veut rassurante. Elle précise : « pour le moment, aucun rapport n'indique que ces vulnérabilités ont été exploitées. Nous recommandons vivement aux clients de mettre à jour leurs systèmes et d'appliquer les versions corrigées sans délai ».

Réagissez à cet article

Source : *Juniper : une faille de sécurité permettait de surveiller le trafic VPN*