Attention ! Le Cloud est espionné

	Attention ! Le Cloud est espionné

Les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Si vous n'êtes pas propriétaire du hardware, vous n'êtes pas propriétaire des données, selon une étude de Bitdefender.

L'éditeur de solutions de sécurité informatique affirme que les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Les révélations de l'affaire Snowden sur les capacités d'interception des données de la part de la NSA et de ses agences partenaires ont incité les propriétaires d'infrastructures et les fournisseurs de services, ainsi que les utilisateurs, à s'assurer que leurs données sont échangées sans encourir de risque de confidentialité et qu'elles sont stockées sous forme chiffrée. Régulièrement, les chercheurs s'attaquent à des protocoles très utilisés ou à leur mode de mise en œuvre. Des failles sont ainsi découvertes de manière récurrente et corrigées à plus ou moins brèves échéances, comme dans le cas de vulnérabilités bien connues telles que Heartbleed ou Logjam, qui ont entraîné le déploiement massif de correctifs à une échelle jusque-là inédite.
Mais les entreprises, et par conséquent, leurs clients, sont-elles vraiment protégées une fois que ces failles sont corrigées ? Existe-t-il des méthodes dissimulées et plus ou moins légales que les organismes d'État et certaines grandes entreprises bien informées seraient susceptibles d'utiliser pour passer outre les protocoles TLS / SSL, censés protéger les échanges d'informations ? Bref, espionnage dans le Cloud possible ?
Le 26 mai 2016, lors de la Conférence HITB à Amsterdam, Radu Caragea, Chercheur en sécurité des Bitdefender Labs, a démontré lors d'un POC (preuve de concept), que la communication protégée peut être déchiffrée en temps réel, en utilisant une technique qui ne laisse pratiquement aucune empreinte et qui reste invisible pour presque tout le monde, sauf peut-être pour des auditeurs de sécurité particulièrement vigilants.

Espionnage dans le cloud : Quelles conséquences pour votre sécurité ?
Cette attaque permet à un fournisseur de services cloud mal intentionné (ou sur lequel on a fait pression pour qu'il donne des accès à des agences gouvernementales) de récupérer les clés TLS utilisées pour chiffrer chaque session de communication entre votre serveur virtualisé et vos clients (même si vous utilisez Perfect Forward Secrecy !). Si vous êtes un DSI et que votre entreprise externalise son infrastructure de virtualisation auprès d'un prestataire de service, considérez que toutes les informations circulant entre vous et vos utilisateurs ont pu être déchiffrées et lues pendant une durée indéterminée.
Il est impossible de savoir dans quelle mesure vos communications ont pu être compromises et pendant combien de temps, puisque cette technique ne laisse aucune trace anormale derrière elle. Les banques et les entreprises qui gèrent des dossiers de propriété intellectuelle ou des informations personnelles, ainsi que les institutions gouvernementales sont les secteurs susceptibles d'être particulièrement touchés par cette faille.

Espionnage dans le Cloud : Premières découvertes
Cette nouvelle technique, surnommée TeLeScope, a été développée par l'éditeur dans le cadre de ses recherches et permet à un tiers d'écouter les communications chiffrées avec le protocole TLS, entre l'utilisateur final et une instance virtualisée d'un serveur. Cette technique n'est opérationnelle qu'avec les environnements virtualisés fonctionnant au-dessus de l'hyperviseur. Ces infrastructures sont extrêmement répandues et sont proposées par les géants de l'industrie tels qu'Amazon, Google, Microsoft ou DigitalOcean, pour ne citer qu'eux. Si la plupart des experts de l'industrie s'accordent pour dire que la virtualisation est l'avenir, aussi bien en termes de stockage, que de déplacement et de traitement de gros volumes de données, ce type de solutions fait déjà partie du quotidien de nombreuses entreprises.
Plutôt que d'exploiter une faille dans le protocole TLS, cette nouvelle technique d'attaque repose sur l'extraction des clés TLS au niveau de l'hyperviseur par une inspection intelligente de la mémoire. Même si l'accès aux ressources virtuelles de la VM est une pratique déjà connue (accéder au disque dur de la machine, par exemple), le déchiffrement en temps réel du trafic TLS, sans mettre en pause la machine virtuelle de manière flagrante et visible, n'avait jamais été réalisé jusqu'alors.
La découverte de ce vecteur d'attaque a été possible en recherchant un moyen de surveiller des activités malveillantes depuis le réseau de honeypots de l'éditeur, sans altérer la machine et sans que les pirates puissent comprendre qu'ils sont surveillés. Un administrateur réseau ayant accès à l'hyperviseur d'un serveur hôte pourrait surveiller, exfiltrer et monétiser toutes les informations circulant depuis et vers le client : adresses e-mail, transactions bancaires, conversations, documents professionnels confidentiels, photos personnelles et autres données privées.

Espionnage dans le Cloud : Comment cela fonctionne-t-il ?
Normalement, la récupération des clés à partir de la mémoire d'une machine virtuelle nécessiterait de mettre en pause la VM et de décharger le contenu de sa mémoire sur un fichier. Ces deux processus sont intrusifs et visibles par le propriétaire de la VM (de plus ils enfreignent le SLA – Service Level Agreement). L'approche des chercheurs repose sur les mécanismes de Live Migration, disponibles au sein des hyperviseurs modernes, qui nous permettent de réduire le nombre de pages nécessaire pour le vidage de la mémoire de l'ensemble de la RAM, à celles modifiées lors de l'établissement d'une liaison TLS.
« ***Au lieu de mettre la machine en pause (ce qui entraînerait une latence notable) et de réaliser un vidage complet de la mémoire, nous avons développé une technique de différentiel de la mémoire qui utilise des fonctions de base déjà présentes dans les technologies de l'hyperviseur,*** » explique Radu Caragea. « ***Ensuite, bien que cela permette de réduire le volume de vidage mémoire de giga-octets à méga-octets, le temps nécessaire pour écrire une telle quantité de données sur un espace de stockage reste non négligeable (de l'ordre de quelques millisecondes) et c'est pourquoi nous montrons comment 'déguiser ' le processus pour le faire passer pour une latence du réseau, sans qu'il soit nécessaire de stopper la machine.*** »

Atténuation des risques
L'attaque TeLeScope n'exploite pas de faille lors de l'implémentation du protocole TLS et ne tente pas de contourner le niveau de chiffrement de l'implémentation TLS via des attaques par repli (downgrade attacks). Au lieu de cela, elle exploite une caractéristique de l'hyperviseur pour exfiltrer les clés utilisées par le protocole pour chiffrer la session. Notre POC révèle un écart fondamental qui ne peut être corrigé ou atténué sans réécrire les bibliothèques de cryptographie qui sont déjà en cours d'utilisation. La seule solution à ce jour est, en premier lieu, de bloquer l'accès à l'hyperviseur – en exécutant votre propre hardware à l'intérieur de votre propre infrastructure.
Article original de Damien BANCAL

Réagissez à cet article

Original de l’article mis en page : ZATAZ Espionnage dans le Cloud – ZATAZ

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

Daech prend le contrôle d'une centrale nucléaire – Futuriste ?

Daech prend le contrôle d'une centrale nucléaire. Futuriste ?

Le coordinateur de l'UE pour la lutte contre le terrorisme estime que les djihadistes seront bientôt capables de cyberattaques contre des sites sensibles.

La prise de contrôle d'une centrale nucléaire par des mouvements djihadistes pourrait devenir une réalité « avant cinq ans », a admis samedi le coordinateur de l'Union européenne pour la lutte contre le terrorisme alors que la sécurité des sites nucléaires belges est pointée du doigt.
« Je ne serais pas étonné qu'avant cinq ans il y ait des tentatives d'utiliser l'Internet pour commettre des attentats », notamment en prenant le contrôle du « centre de gestion d'une centrale nucléaire, d'un centre de contrôle aérien ou l'aiguillage des chemins de fer », estime Gilles de Kerchove dans une interview au quotidien La Libre Belgique.
« À un moment donné, il y aura bien un gars » au sein de l'organisation djihadiste État islamique « avec un doctorat en technologie de l'information qui sera capable d'entrer dans un système », a-t-il estimé.

La miniaturisation des explosifs mais également la connaissance accrue des combattants de l'État islamique dans les biotechnologies constituent de réelles menaces pour l'avenir, selon lui. « Que se passera-t-il quand on en sera à comment élaborer un virus dans la cuisine de sa mère ? » s'est-il demandé.
En revanche, M. de Kerchove a estimé que le département belge de la Défense était « assez bon » en matière de cybersécurité. « Ils n'ont, bien sûr, pas les capacités de représailles des Français, des Anglais ou des Américains, mais en cas d'attaque, je pense que notre département de la Défense est assez bon », a-t-il dit, précisant cependant qu'il ne savait pas « si le gouvernement » belge était « capable d'anticiper et de résoudre de grosses attaques ».

Sécurité renforcée
Des médias belges et internationaux ont rapporté vendredi que la cellule terroriste bruxelloise responsable des attentats de mardi avait prévu une attaque à l'arme de guerre dans les rues de Bruxelles, type 13 novembre à Paris, et la fabrication d'une « bombe sale » radioactive après une surveillance vidéo par deux des kamikazes, les frères El Bakraoui, d'un « expert nucléaire » belge.
À la suite des attaques survenues mardi à Bruxelles qui ont fait 31 morts, la sécurité avait été renforcée autour des deux centrales nucléaires de Belgique.
C'est dans ce contexte de suspicion sur la sécurité des sites nucléaires qu'un agent de sécurité dans le nucléaire a été abattu et son badge volé jeudi soir dans la région de Charleroi, dans le sud de la Belgique, selon le journal La Dernière Heure. Samedi, la piste terroriste a été écartée, par la justice belge. La piste terroriste est formellement démentie, rapporte l'agence de presse Belga, citant le parquet de Charleroi, dans le sud du pays. Le juge d'instruction spécialisé dans les matières terroristes n'a pas été saisi. Les raisons de la mort de la victime, abattue, tout comme son chien, de plusieurs balles à son domicile, ne sont pas encore connues mais les enquêteurs pensent à un cambriolage qui aurait mal tourné ou à un crime pour des raisons privées.
Le parquet de Charleroi a démenti le vol de son badge d'accès de centrale nucléaire… [Lire la suite]

-

Réagissez à cet article

Source : *Quand Daech prendra le contrôle d'une centrale nucléaire – Le Point*

Nos empreintes digitales en danger à cause d’Android ? | Le Net Expert Informatique

	Nos empreintes digitales en danger à cause d’Android ?

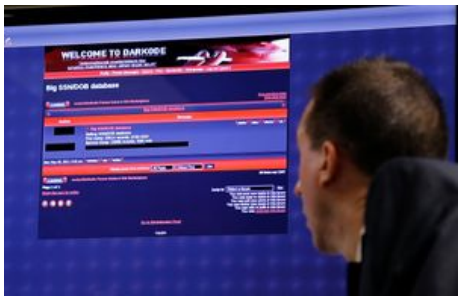
Alors que les failles de sécurités concernant Android n'ont jamais été aussi nombreuses à être révélées, une nouvelle attaque permettrait de voler les empreintes digitales à cause d'une nouvelle lacune du système Android ! Une affaire qui mérite certainement d'être prise au sérieux non ?

S'il est vrai qu'Android n'est pas le meilleur exemple en termes de sécurité, succès oblige comme Windows il y a quelques années, on ne peut cependant pas l'accuser de tout et n'importe quoi. Cette soi-disant faille permettrait à un pirate de récupérer les empreintes d'un utilisateur qui utilise ce type de fonctionnalité sur son smartphone afin d'en assurer la sécurité d'accès. Quelle horreur nous sommes donc tous en danger !
Plus sérieusement le risque évoqué est assez limité et avec n'importe quel objet qu'on touche nous laissons tous des empreintes digitales un peu partout. Ne pas être totalement parano est certainement la meilleure chose à faire et être prudent dans la manière de protéger ses données personnelles est la seconde chose à penser. Avec l'informatique nous sommes tous vulnérable et des victimes potentielles de piratage et c'est en faisant attention à ce qu'on fait qu'on se protégera le mieux. Pour rappel une empreinte digitale même si elle est unique est sans aucun doute un des moyens les moins sûrs pour protéger un système informatique. Utiliser une empreinte c'est comme laisser un Post-It avec son mot de passe sur chaque objet qu'on touche !

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

Source : http://android.smartphonefrance.info/actu.asp?ID=3966

Le forum de pirates Darkode est tombé après une opération menée par le FBI | Le Net Expert Informatique

	Le forum de pirates Darkode est tombé après une opération menée par le FBI

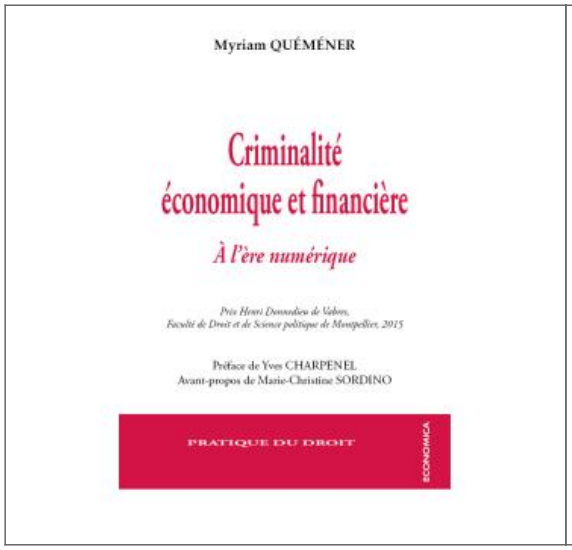
Sous la supervision du FBI , le forum Darkode, qui constituait un point de rendez-vous majeur des pirates pour mener des cyber-attaques, est tombé.

C'est la fin du forum dédié au piratage par lequel il était possible d'acheter, de vendre, de monnayer et de partager des informations ou des outils favorisant des cyber-attaques.
Il a fallu que le FBI s'infiltre dans ce monde underground pour en connaître les coulisses d'administration.
Un accès était uniquement possible par cooptation sous le contrôle des gestionnaires de Darkode : on recensait plusieurs centaines de membres (entre 250 et 300 selon LeMonde.fr).
Mais tout postulant devait démontrer au préalable ses « talents » c'est-à-dire ses capacités à alimenter les ressources malware diffusées via Darkode.
Selon les autorités américaines, des mandats d'arrêt concernant une douzaine de personnes présumées en charge de l'administration de Darkode ont été émis dans trois districts, mais en tout, on évoque 70 membres de Darkode interpellés ou recherchés dans le monde.
Une vingtaine de pays ont été associés à la coupure de ce forum qui entre dans une opération plus large contre la cyber-criminalité baptisée « Shrouded Horizon » : outre les Etats-Unis, on trouve des pays comme l'Australie, le Royaume-Uni, le Brésil, le Canada, la Colombie, la Croatie, le Nigéria, l'Allemagne ou Israël.
« Sur les 800 forums dédié à la criminalité sur Internet, Darkode représentait l'une des plus graves menaces à l'intégrité des données informatiques aux Etats-Unis et dans le monde », déclare David Hickton, procureur fédéral pour le district Ouest de Pennsylvanie, cité dans le communiqué du ministère de la Justice.

A travers le centre anti-cyberciminalité EC3, l'Europe était dans la boucle.
Europol a précisé de son côté que l'opération menée sous la supervision du FBI a abouti à 28 arrestations, 37 perquisitions et un nombre important de saisies de matériel informatique susceptibles d'abriter des preuves et des données pour pousser l'enquête encore plus loin.

Source : http://www.itespresso.fr/darkode-fbi-fait-tomber-forum-ombre-102787.html
Par Philippe Guerrier

La criminalité économique et financière à l’ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l’ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

La Marine Française infectée par Thales ? | Le Net Expert Informatique

La Marine Française infectée par Thales ?

L'affaire du piratage dont a été victime Thales en début d'année rebondit. Selon le Canard Enchaîné, son programme classé-défense SIC21 livré à la Direction Générale de l'Armement et équipant des navires et des installations terrestres, pourrait avoir été infecté.

L'attaque informatique dont a été victime Thales en avril dernier continue de faire couler beaucoup d'encre. Dans un document confidentiel daté du 18 mai évoqué par le Canard Enchaîné, l'entreprise de défense confirme en effet que l'ensemble des postes, serveurs et équipements du groupe aux Etats-Unis ont été infectés en décembre par un virus à partir des serveurs des sites de Thales Avionics à Piscataway, dans le New Jersey, et à Irvine, en Californie, avant de se répandre au Canada et de toucher la messagerie France de Thales en mars dernier. Mais l'histoire ne s'arrête pas là : dans un mail envoyéle 13 mai à Olivier Daloy (directeur du système informatique de Thales), Ivan Maximoff (le spécialiste sécurité informatique maison) aurait fait aussi état de ses inquiétudes concernant la découverte du virus Courch Yeti spécialisé dans l'espionnage industriel, dans le programme classé-défense SIC21 datant de 2004.
Problème : le programme SIC21 équipe aussi des navires et des installations terrestres. « Six livraisons de Thales au centre d'expertise de la Direction Générale de l'Armement dans le domaine de la guerre électronique installé près de Rennes, et à la DGA Techniques navales à Toulon, pourraient avoir été infectées », indique le Canard Enchaîné. Dans un extrait du mail du 13 mai d'Ivan Maximoff repris par le journal satirique, ce dernier fait également mention que des programmes potentiellement indésirables ont été livrés dans le cadre du programme SIC21. Afin de faire le point sur la situation, une réunion aurait eu lieu le 18 mai entre Thales, la DGA mais aussi l'Agence nationale de la Sécurité des Systèmes d'Information pour évoquer la sécurisation du groupe.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-piratage-de-thales-la-dga-pourrait-avoir-ete-infectee-par-le-virus-courch-yeti-61453.html
Par Dominique Filippone

La NSA écoute nos disques durs ?

La NSA écoute nos disques durs ?

Kaspersky Lab a découvert une plate-forme de cyber-espionnage dont l'une des composantes, très certainement exploitée par la NSA, permet de surveiller des disques durs.

Iran, Russie, Pakistan, Afghanistan, Chine, Mali, Syrie, Yémen, Algérie… Les gouvernements, organes militaires, sociétés télécoms, banques, médias, chercheurs et activistes d'une trentaine de pays auraient été exposés à des logiciels espions cachés dans des disques durs.
Les équipes de Kaspersky Lab en sont arrivées à cette conclusion après plusieurs années d'enquête sur ce qu'elles considèrent aujourd'hui comme le dispositif de surveillance électronique « le plus complexe et le plus sophistiqué » découvert à date*.
Encore activement exploitée, cette plate-forme serait opérationnelle depuis au moins 2001, voire 1996, si on se fie à la date d'enregistrement de certains serveurs utilisés pour contrôler les malware.
Elle hébergerait notamment un ver très proche de Stuxnet. Ce virus complexe et polymorphe dont la conception est attribuée à l'Agence américaine de sécurité nationale (NSA) avec la collaboration de l'unité 8200 de l'armée israélienne (cyberdéfense) avait mis à mal un site d'enrichissement d'uranium implanté en Iran, endommageant un millier de centrifugeuses.
Mais c'est bien le module de piratage des disques durs qui retient l'attention de Kaspersky. Dans son rapport publié lundi (document PDF sur http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf, 44 pages), l'éditeur russe note que la quasi-totalité des produits du marché sont affectés : Seagate, Western Digital, Toshiba, IBM, Micron, Samsung…
Il est d'autant plus difficile de détecter l'infection qu'elle se loge dans le firmware des disques durs. Ce qui lui permet aussi de s'activer presque instantanément au démarrage (la seule étape qui précède dans la séquence d'amorçage est l'initialisation du BIOS) et d'ouvrir discrètement des portes dérobées permettant de récupérer des données à foison.
Pour Kaspersky Lab, réussir à implanter un logiciel malveillant dans le firmware d'un disque dur est une prouesse. A moins que les pirates aient eu accès au code dudit firmware. Du côté de Western Digital, on assure ne pas avoir communiqué ce genre de données. Chez Seagate, on estime avoir intégré des couches de sécurité pour éviter les modifications non sollicitées du micrologiciel, ainsi que son étude par reverse engineering.

A qui la faute ?
Le problème remonte peut-être à 2009. Dans le cadre d'une vague de cyber-attaques contre des sociétés high-tech américaines, les pirates avaient eu accès à du code source qualifié de « très précieux » car hébergé sur les serveurs de multinationales et d'organes gouvernementaux.

Dans ce butin figuraient probablement des copies du firmware des différentes marques de disques durs. Et pour cause : lorsqu'elles acquièrent un équipement informatique, les agences classées « sensibles » peuvent demander, pour le compte du gouvernement américain, un audit de sécurité des produits pour s'assurer de l'intégrité du code source… lequel est certainement sauvegardé au passage.

Kaspersky Lab n'affirme pas que la NSA est à l'origine de ce « mouchard à disques durs ». Ses chercheurs disposent toutefois de nombreux indices, comme ce mot-clé GROK trouvé dans le code d'un enregistreur de frappe et déjà présent dans un outil d'espionnage dévoilé en 2013 par Edward Snowden.

Les multiples révélations du lanceur d'alertes pèsent sur l'activité des sociétés high-tech américaines : les ventes de solutions – aussi bien matérielles que logicielles – chutent. A tel point que Peter Swire, membre du groupe de réflexion «Renseignement et Nouvelles technologies» monté par Barack Obama, reconnaît qu'il est «plus que jamais indispensable, pour les Etats-Unis, de mesurer l'impact que chaque décision d'exploiter une faille de sécurité pourrait avoir sur les relations commerciales […] et diplomatiques».

* Malgré sa puissance, il semble que la plate-forme ne soit exploitée que contre un nombre restreint de «cibles d'intérêt» localisées hors des Etats-Unis.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.itespresso.fr/cyber-espionnage-nsa-ecoute-disques-durs-88684.html
Par Clément Bohic

Les opérateurs télécoms nous espionnent-ils ? | Le Net Expert Informatique

Les opérateurs télécoms nous espionnent-ils ?

Votre téléphone est-il sur écoute ? Depuis plusieurs semaines, une affaire secoue le milieu des télécoms suite à la révélation du journal arabophone Al Massae quant à l'utilisation d'un logiciel «d'espionnage des données personnelles» par un opérateur télécoms de la place. Il s'agit du LCS, un logiciel en principe prohibé en Europe et aux États-Unis, qui permet de surveiller l'activité des utilisateurs en dehors de tout cadre légal.

La question qui se pose aujourd'hui : les opérateurs télécoms ont-il le droit d'utiliser les outils qu'ils ont pour contrôler et accéder aux informations et aux données des utilisateurs ? «Il s'agit d'un système permettant de retracer toutes les actions d'un utilisateur sur sa ligne téléphonique et d'effectuer les perquisitions numériques, explique Carlo Lando, un expert italien en sécurité des télécoms.

«En principe, les opérateurs téléphoniques doivent avoir des autorisations du tribunal pour utiliser cette technologie de système sur les réseaux, notamment pour les enquêtes», précise l'expert. Interpellé, le DG de l'Agence nationale de régulation des télécoms (ANRT), Azeddine Mountassir Billah, dit tout ignorer de cette affaire et refuse de la commenter.

En revanche, à la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), on apprend qu'une réunion aura lieu cette semaine, avec à l'ordre du jour, entre autres, cette affaire de «logiciel LCS». Le président du CNDP, Saïd Ihrai, a déclaré que la commission n'a pas encore été saisie sur ce type de «procédé prohibé» permettant de surveiller et de contrôler les données personnelles des utilisateurs.

Source : http://www.leseco.ma/maroc/30623-donnees-personnelles-les-operateurs-telecoms-nous-espionnent-ils.html
Par NAIMA CHERII

Les 5 dangers du projet de loi sur le renseignement | Denis JACOPINI

	Les 5 dangers du projet de loi sur le renseignement

Dernière ligne droite pour le projet de loi sur le renseignement. Le vote solennel du texte est prévu ce mardi 5 mai à l'Assemblée, malgré une mobilisation des opposants, lundi soir au Trocadéro, à Paris.
Que dit le texte ? Au fil des débats, les députés ont fait évoluer le projet de loi. « Il a été considérablement enrichi », estime son rapporteur, Jean-Jacques Urvoas (PS), dans une note envoyée aux députés dont « l'Obs » a eu connaissance. Au total, 260 amendements ont été adoptés. Cela répond en partie aux demandes des adversaires du texte, mais ne lève pas toutes les inquiétudes, loin de là.

Ce que l'Assemblée a modifié :
Une commission de contrôle renforcée
Est surtout renforcé « la composition, l'indépendance et les pouvoirs de la [nouvelle] Commission nationale de contrôle des techniques de renseignements » (CNCTR). Celle-ci remplacera l'actuelle Commission nationale des interceptions de sécurité (CNCIS) et, comme réclamé dans « l'Obs » par son actuel président, cette nouvelle instance disposera d'un « accès aux locaux des services, aux dispositifs de traçabilité, aux opérations de transcription, d'une saisine élargie du Conseil d'Etat ». De plus, les renseignements collectés seront bien centralisés par le Groupement interministériel de contrôle (GIC), que « l'Obs » a pu visiter en exclusivité.

Des professions moins exposées
Le texte exclut désormais certaines professions de la procédure d'urgence. Pour les magistrats, les avocats, les journalistes et les parlementaires, les écoutes ne peuvent être mises en œuvre que sur autorisation du Premier ministre, après avis de la commission. (Art. L. 821-7)

Un statut de lanceur d'alerte
De même, un « statut de lanceur d'alerte a été créé afin d'apporter une protection juridique à tout agent souhaitant révéler des illégalités commises ». N'est en revanche pas précisé si ce statut pourra être étendu à tous ceux qui révèlent des illégalités, à la manière d'Edward Snowden sur la NSA.

Les hackers plus fortement sanctionnés
Les députés ont également profité du texte pour renforcer l'arsenal de sanctions contre les hackers. Dans le sillon de la cyberattaque contre TV5 Monde, ils ont décidé de doubler les sanctions pécuniaires pour tout piratage (actuellement puni au maximum de 75.000 euros), voire de les tripler s'il s'agit d'un service de l'Etat.

Un fichier des personnes mises en cause pour terrorisme
Le gouvernement a également profité de cette loi pour créer un nouveau fichier (FIJAIT) qui recensera les noms et adresses de toutes les personnes condamnées ou mises en examen pour terrorisme.

Malgré des améliorations notables du texte, certains points continuent de poser problème.

1 – Le Premier ministre, seul maître à bord
La loi dote les six services de renseignement français de nombreux moyens supplémentaires pour enquêter, et la plupart n'auront plus besoin de l'aval d'un juge. En effet, le Premier ministre se positionne comme seul décisionnaire.
Les autorisations sont délivrées, après avis de la CNCTR, par le Premier ministre », pointe le texte.
Surtout que le Premier ministre pourra passer outre l'avis de la CNCTR, mais devra alors motiver sa décision (et risquer une saisine du Conseil d'Etat). Et tout ceci s'applique, sauf « en cas d'urgence absolue »…

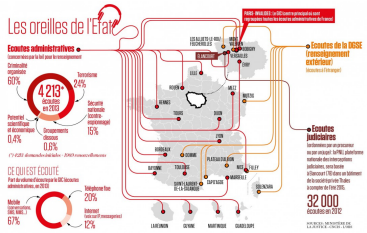
2 – Des données conservées longtemps
Afin de surveiller une personne, le projet de loi prévoit de nombreuses interceptions à distance (e-mails, conversations téléphoniques, SMS…) mais aussi la pose de micros et caméras dans des lieux ou des véhicules. Le texte prévoit que l'ensemble des renseignements ainsi collectés seront détruits au terme de certaines durées :
• 30 jours pour les correspondances,
• 90 jours pour les sonorisations, les géolocalisations et les images vidéo,
• 5 ans pour les données de connexion, aussi appelées métadonnées (qui donnent le détail de qui écrit un e-mail à qui, à quelle heure, etc.).
Et, en cas de cryptage des données, ces délais ne s'appliquent qu' »à compter de leur déchiffrement ».

3 – Eviter de croiser la route d'un suspect
Le projet de loi prévoit que les mesures de surveillance seront utilisées à la fois pour les suspects, mais aussi pour les « personnes appartenant à [son] entourage » s'il « existe des raisons sérieuses de croire [qu'elles ont] joué un rôle d'intermédiaire, volontaire ou non ». En somme, n'importe qui se trouvant au mauvais endroit, au mauvais moment, et ayant croisé une mauvaise route, pourra être mis sous surveillance.

Lors de la manifestation contre le projet de loi sur le renseignement, le 13 avril (CITIZENSIDE/ANTHONY DEPERRAZ/AFP)

4 – Tous suspects sur internet
Le projet de loi entend mettre à profit les opérateurs internet. Fournisseurs d'accès, moteurs de recherche, réseaux sociaux… Tous pourront fournir « en temps réel » les données techniques de connexion des internautes suspectés de terrorisme. Concrètement, il s'agit de pister une connexion (exprimée par une adresse IP) pour savoir quel site elle a visité, à quelle heure, si elle a envoyé un message Facebook à telle personne, si elle a tapé tel mot clef sur Google…
Le texte souhaite aussi contraindre les opérateurs internet à « mettre en œuvre sur leurs réseaux un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés ». Concrètement, les services de renseignement installeront une « boîte noire » dotée d'un algorithme qui passera au crible l'ensemble du trafic internet pour détecter automatiquement des internautes soupçonnés d'être des terroristes. A terme, cette boîte noire pourra être mise en place chez les fournisseurs d'accès à internet, mais aussi les Américains Google, Facebook, Apple ou Twitter.
L'ensemble du système surveille l'ensemble des internautes de manière anonyme pour détecter des « signaux faibles ». Et, en cas de suspicion, les opérateurs devront dénoncer la personne correspondant aux enquêteurs.
La CNCTR aura accès « au code source » de cette boîte noire afin de limiter la collecte des données aux seuls terroristes. Du moins, tant qu'un décret n'a pas étendu le champ d'action de ce dispositif qui s'apparente à « une surveillance de masse » inspirée par l'agence de renseignement américaine NSA.

5 – Surveiller les terroristes, mais pas seulement
Finalement, il convient de rappeler que, malgré les présentations du texte par François Hollande ou Manuel Valls, il ne s'agit pas d'une loi anti-terroriste, mais bien d'un texte sur le renseignement. Le projet prévoit sept finalités pour recourir aux diverses techniques de renseignement :
• l'indépendance nationale, l'intégrité du territoire et la défense nationale,
• les intérêts majeurs de la politique étrangère et la prévention de toute forme d'ingérence étrangère,
• les intérêts économiques, industriels et scientifiques majeurs de la France,
• la prévention du terrorisme,
• la prévention des atteintes à la forme républicaine des institutions, des violences collectives de nature à porter atteinte à la sécurité nationale ou de la reconstitution de groupements dissous,
• la prévention de la criminalité et de la délinquance organisées,
• la prévention de la prolifération des armes de destructions massives.
Pour rappel, en 2014, 60% des écoutes administratives visaient la criminalité organisée, 24% le terrorisme, 15% la sécurité nationale (contre-espionnage), 0,6% les groupements dissous, et 0,4% la protection du potentiel scientifique et économique. Depuis l'attaque meurtrière contre « Charlie Hebdo », la part dédiée au terrorisme est montée à 48%.



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

Note de Jean-Jacques Urvoas publié par NouvelObs.com

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://tempsreel.nouvelobs.com/loi-renseignement/20150504.OBS8368/les-5-dangers-du-projet-de-loi-renseignement.html?cm_mmc=EMV-_-NO-_-20150505_NLNOACTU08H-_-les-5-dangers-du-projet-de-loi-renseignement##xtor=EPR-1-Actu8h-20150505
Par Boris Manenti