

La sécurité des Opérateurs d'Importance Vitale (OIV) continue à se renforcer



La sécurité
des
Opérateurs
d'Importance
Vitale
continue à
se renforcer

Les premiers arrêtés encadrant la sécurité des OIV illustrent la difficulté à mettre en place un dispositif encadrant la cybersécurité des entreprises. L'Anssi vante une démarche pionnière et reconnaît que les organisations concernées devront investir pour se conformer aux nouvelles règles.



Trois arrêtés sectoriels sur 18. L'entrée en vigueur, au 1er juillet, des premières mesures encadrant la sécurité des OIV (Opérateurs d'importance vitale), 249 organisations dont le bon fonctionnement est jugé essentiel au fonctionnement de la Nation, illustre bien la difficulté à poser un cadre réglementaire sur la cybersécurité des grandes entreprises. Découlant de l'article 22 de la Loi de programmation militaire (LPM), votée fin 2013, cet ensemble de règles, qui comprend notamment la notification des incidents de sécurité à l'Anssi (Agence nationale de sécurité des systèmes d'information), avait fait l'objet d'un décret en mars 2015. Restait à adapter ce décret à la réalité des différents secteurs d'activité. Ce qui, de toute évidence, a pris plus de temps que prévu. Rappelons qu'à l'origine, l'Anssi espérait voir les premiers arrêtés sectoriels sortir à l'automne 2015... Mais Guillaume Poupard, le directeur général de l'Anssi, assume tant le choix de la France d'en passer par la loi (plutôt que par un simple référentiel de bonnes pratiques) que le décalage de calendrier, révélateur de la difficulté à traduire sur le terrain l'article 22 de la LPM. Lors d'une conférence de presse organisée à l'occasion de la sortie des premiers arrêtés, dédiés aux secteurs de l'eau, de l'alimentation et de la santé, il explique : « Je préfère avoir dès le départ annoncé un calendrier ambitieux et avoir aujourd'hui un dispositif en place. Avec l'Allemagne, la France fait partie des pays pionniers de ce type de démarche. Et si nous avons pu prendre quelques mois de retard sur le calendrier initial, nous restons très en avance sur nos alliés. » D'autres arrêtés sectoriels devraient sortir en octobre 2016 et janvier 2017. Une fois ces textes publiés, les OIV ont, pour les règles les plus complexes, jusqu'à 18 mois ou 2 ans pour les mettre en œuvre. « On a déjà vérifié que ces règles étaient efficaces et soutenables financièrement », assure Guillaume Poupard.

« Oui, cela coûte de l'argent »

La définition de ces règles, au sein de 12 groupes de travail sectoriels, n'a pourtant pas été simple. Tout simplement parce qu'elles se traduisent par des investissements contraints pour les entreprises concernées sur les systèmes d'information considérés d'importance vitale. Certaines se verront dans l'obligation de revoir leurs architectures réseau par exemple. « On va imposer des règles, des contrôles, des notifications d'incidents, la capacité pour l'Anssi à imposer sa réponse aux incidents en cas de crise. C'est assez violent. Mais, il faut garder à l'esprit que ces règles ont été élaborées au sein de groupes de travail associant les OIV », tranche Guillaume Poupard. Selon ce dernier, la sécurité devrait peser entre 5 et 10 % du budget de la DSI de tout OIV. « Nos mesures ne s'inscrivent pas dans l'épaisseur du trait budgétaire. Mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique », tranche-t-il. Et d'assurer qu'aucun groupe de travail ne connaît une situation de blocage empêchant d'avancer sur la rédaction des arrêtés.

Si le dispositif se met donc en place au forceps, tout n'est pas encore parfaitement défini. Illustration avec les incidents de sécurité que les OIV doivent notifier à l'Anssi. Cette dernière ne peut matériellement pas consolider l'ensemble des incidents des 249 OIV français. Dès lors quels événements devront être communiqués et lesquels devront rester cantonnés entre les murs de l'organisation visée ? « C'est un sujet complexe car les premiers indices d'une attaque sont souvent de la taille d'une tête d'épingle, reconnaît Guillaume Poupard. C'était par exemple le cas pour l'affaire TV5 Monde. » Selon le directeur général de l'Anssi, des expérimentations sont en cours pour placer le curseur au bon endroit.

De l'efficacité de ce dispositif dépendra la réalisation d'un des objectifs de l'Anssi, la capacité à organiser la défense collective. L'Agence se voit en effet comme un tiers anonymisateur permettant d'assurer le partage d'informations sur les menaces à l'intérieur d'un secteur ou à l'échelle de l'ensemble des OIV. Une mise en commun que rechignent à effectuer les entreprises – même si des secteurs comme la banque se sont organisés en ce sens – pour des raisons concurrentielles.

L'Anssi veut les codes sources

En parallèle, pour compléter ce dispositif, l'Anssi s'est lancée dans un travail de qualification des prestataires et fournisseurs à même d'implémenter les règles édictées dans les arrêtés. Un processus plus lourd qu'une simple certification. Aujourd'hui, une vingtaine de prestataires d'audit ont ainsi été qualifiés. L'agence doit également publier des listes de prestataires de détection d'incidents, de réactions aux incidents ainsi que des sondes de détection. Si Guillaume Poupard écarte toute volonté de protectionnisme économique déguisé, il reconnaît que cette démarche de qualification – qui va jusqu'à l'évaluation des experts eux-mêmes ou l'audit du code source pour les logiciels – introduit un biais, favorisant les entreprises hexagonales. « L'accès au code source est par exemple accepté par certains industriels américains, mais refusé par d'autres », reconnaît-il.

Si, malgré les réticences de certains OIV, la France a décidé de presser le pas, c'est que les signaux d'alerte se multiplient. « Nous craignons notamment la diffusion des savoirs aux groupes terroristes, via le mercenariat. Nous avons des informations des services de renseignement nous indiquant que ces groupes ont la volonté de recruter des compétences cyber », assure Louis Gautier, le secrétaire général de la défense et de la sécurité nationale. Un pirate informatique kosovar, arrêté en Malaisie en octobre 2015, a ainsi reconnu avoir vendu ses services à Daesh. Connu sous le pseudonyme Th3Dir3ctorY, il vient de plaider coupable devant la justice américaine et risque 20 ans de prison.

De son côté, Guillaume Poupard s'inquiète du comportement de certains assaillants qui semblent mener des missions d'exploration sur les réseaux des entreprises françaises. « Comme s'ils voulaient préparer l'avenir. Que cherchent-ils à faire exactement ? Nous ne le savons pas, mais ces opérations de préparation sont particulièrement inquiétantes », dit le directeur général de l'Anssi, qui précise que les alliés de la France observent le même phénomène.

Article original de Reynald Fleychaux



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : La sécurité des OIV mise au pas par l'Etat... petit à petit

Cybersécurité : êtes-vous bien protégé?



De nos jours, impossible d'imaginer travailler dans le secteur des valeurs mobilières sans système informatique. Mais avec cet incontournable outil viennent plusieurs risques, qui peuvent faire un tort considérable aux conseillers et à leurs clients.

« Ces dommages peuvent nuire à la réputation d'un cabinet, l'exposer à des pertes financières et perturber gravement ses activités », prévient l'Association canadienne des courtiers de fonds mutuels (ACFM) dans un bulletin sur la cybersécurité publié la semaine dernière.

Selon des sondages réalisés aux États-Unis en 2011 et 2014 par le Financial Industry Regulatory Authority (FINRA), le secteur des valeurs mobilières est exposé à trois menaces de cybersécurité principales :

1. Les pirates informatiques qui infiltrent les systèmes d'une entreprise;
2. Les initiés qui compromettent les données d'un cabinet ou de ses clients;
3. Les risques opérationnels.

QUE FAIRE?

Pour se prémunir contre ces menaces, l'ACFM suggère à ses membres de se doter d'un cadre de cybersécurité, adapté à la taille de leur cabinet, en cinq étapes :

1. Identifier les biens qui doivent être protégés, de même que les menaces et les risques à leur égard;
2. Protéger ces biens à l'aide des mesures appropriées;
3. Détecter les intrusions et les infractions à la sécurité;
4. Intervenir s'il se produit un événement de cybersécurité potentiel;
5. Évaluer l'incident et améliorer les mesures de sécurité à la lueur des événements.

Pour mener à bien ce plan, l'ACFM propose de nombreuses pistes d'action que les cabinets peuvent suivre selon l'envergure de leurs activités.

Parmi elles, assurer la sécurité physique des lieux, notamment contre les menaces humaines, mais aussi environnementales, s'avère un incontournable, tout comme la mise en place de mesures de protection des systèmes (pare-feu récents, chiffrement des réseaux sans fil, processus de sauvegarde et de récupération, protocoles de mots de passe, etc.).

L'Association suggère également de se doter d'une procédure d'enquête sur le personnel, les sous-traitants et les fournisseurs, ainsi que d'instaurer une politique de cybersécurité et une formation continue obligatoire à ce sujet. Former une équipe d'intervention en cas d'incident peut aussi s'avérer une bonne idée.

Il importe de tester régulièrement la vulnérabilité des systèmes pour en détecter les failles et mieux les corriger. En cas d'incident, il est essentiel de le divulguer, rappelle l'ACFM, notamment au commissaire à la protection de la vie privée dans certains cas.

Finalement, il existe des assurances spécifiquement pour les menaces de cybersécurité.

Article original de conseiller.ca



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Cybersécurité : êtes-vous bien protégé? | Conseiller

Incroyable technique pour analyser les agissements des cybercriminels



Depuis 2007, Zeus empoisonne la vie de millions d'internautes. Ce #logiciel malveillant s'installe sournoisement dans les ordinateurs afin de voler des informations bancaires. Zeus et ses variantes ont ainsi réussi à infecter les serveurs de grandes sociétés comme la NASA, Amazon et Facebook. Selon Mourad Debbabi, professeur et titulaire de la Chaire de recherche en sécurité des systèmes d'information à l'Université Concordia, la Toile est un véritable champ de bataille. Les attaques lancées par les pirates informatiques font des victimes chaque jour, mais les chercheurs ont ces cyberfraudeurs à l'œil : ils les observent pour mieux défendre les internautes, prévenir les fraudes et contre-attaquer !

L'équipe de Mourad Debbabi surveille notamment les « botnets » (contraction de *robot* et de *network*), des réseaux de machines infectées appelées « zombies » qui exécutent les directives des cybercriminels. Les gens installent des maliciels comme Zeus en cliquant sur une pièce jointe ou sur un lien compromis par un code nuisible. L'ordinateur contaminé envoie ensuite des courriels indésirables pour attirer d'autres victimes qui feront partie du *botnet*. Cet ensemble de machines infectées communique avec un ou des serveurs de commande et contrôle qui gèrent diverses attaques.

Pour déjouer ces *botnets* et d'autres menaces, le professeur Debbabi et ses collaborateurs des paliers universitaire, gouvernemental et industriel canadiens ont développé une plateforme de cyber-renseignements. Il s'agit d'un réseau d'ordinateurs peu sécurisés qui « attirent » les cyberattaques, permettant aux chercheurs d'analyser en temps quasi réel une multitude de données (pourriels, virus, etc.) nécessaires pour contrecarrer les escrocs du Web. Cette cyberinformation sert à protéger le parc informatique et les renseignements privés des entreprises et des organisations : mise en quarantaine des ordinateurs infectés, pare-feu renforcé, logiciels de détection... Tel est pris qui croyait prendre !



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Cyberguerre : la science contrattaque | Scientifique en chef

Nouvelle forme d'attaque informatique, les crypto-vers



Nouvelle
forme
d'attaque
informatique,
les crypto-
vers

Les cybercriminels ont trouvé une nouvelle manière de se faire de l'argent. Cela faisait longtemps qu'ils tentaient de prendre en otage des disques durs, mais les gens sont devenus plus vigilants et n'ouvrent plus n'importe quelle pièce jointe à un mail. Voilà pourquoi les cybercriminels se sont vu contraints d'inventer une nouvelle façon d'installer leur rançongiciel (#ransomware). Leur solution: le ver.

Le spécialiste de la sécurité Kaspersky lance donc une mise en garde. Le 'crypto-ver' est « une forme mixte dangereuse de maliciel (malware) et de rançongiciel qui se répand d'elle-même ». Elle peut se propager d'ordinateur à ordinateur, sans spam (pourriel) ou autre infection. Le malware se duplique simplement dans les appareils interconnectés.

Le premier ver, baptisé SamSam, s'est manifesté en avril. Et au cours des dernières semaines, des experts en sécurité ont découvert le ver ZCryptor. Ce dernier se présente sous la forme d'une simple mise à jour d'un programme largement utilisé tel Flash. Une fois en place, le ver commence à se propager, puis il crypte des dizaines d'extensions. Les victimes voient ensuite apparaître leur écran habituel, qui les informe que leurs fichiers ont été pris en otage et qu'ils doivent verser une rançon pour pouvoir y accéder de nouveau.

Les spécialistes de la sécurité n'ont pas encore trouvé une parade contre ZCryptor. Voilà pourquoi Kaspersky prodigue le conseil suivant: soyez sur vos gardes, veillez à disposer d'une bonne protection et effectuez régulièrement des sauvegardes (backups).



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.



[Contactez-nous](#)

Réagissez à cet article

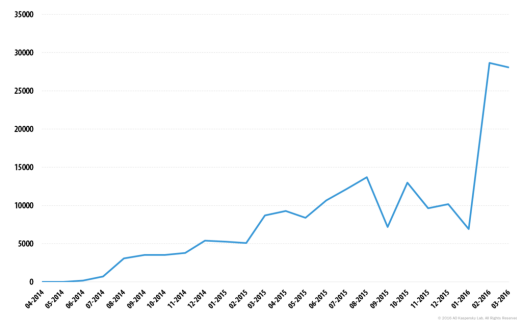
Original de l'article mis en page : Nouveau: le ver ravisseur – ICT actualité – Data News.be

Evolution des Ransomwares pour appareils mobiles en 2014-2016



Evolution
des
Ransomwares
pour
appareils
mobiles en
2014-2016

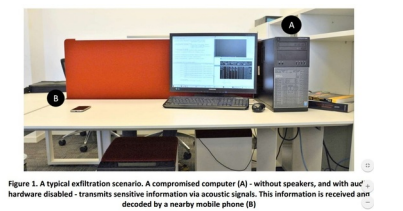
L'activité des ransomwares pour appareils mobiles, qui ne bénéficie pas de la même couverture médiatique que les ransomwares pour PC, a également explosé au cours de la période couverte par le rapport. Et plus particulièrement au cours de la deuxième moitié de celle-ci.



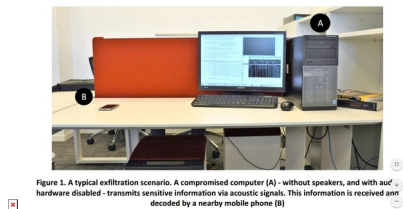
Des chercheurs volent des données en utilisant le bruit des ventilateurs d'un PC



Créé par des chercheurs en sécurité israéliens, le malware Fansmitter exploite les ventilateurs d'un ordinateur pour transmettre des données.



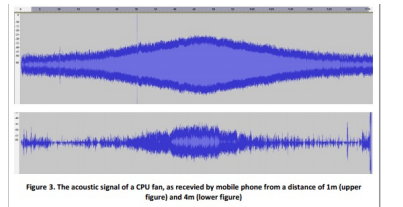
Même le bruit des ventilateurs d'un PC peut être utilisé pour transmettre des données volées sur des machines non connectées à un réseau. Des chercheurs de l'Université Ben Gourion du Néguev en Israël ont en effet trouvé le moyen d'exploiter la vitesse des pales d'un ventilateur équipant un PC classé sensible pour générer des sons particuliers. Les ordinateurs dits sensibles sont isolés et stockent des informations confidentielles. Pour les pirater, les attaquants doivent généralement avoir un accès physique et installer des logiciels malveillants, par le biais éventuellement d'une clef USB.



Pour leurs tests, les chercheurs ont utilisé un simple PC tour Dell et un mobile Samsung. Des recherches antérieures ont montré qu'une fois le PC infecté, les données pouvaient être transmises à partir des haut-parleurs de l'ordinateur sous forme de signaux sonores. Il a alors suffi de désinstaller les haut-parleurs pour améliorer la sécurité de ces machines. Les chercheurs israéliens ont donc exploité une autre méthode pour cibler ces systèmes isolés. Leur malware Fansmitter transmet secrètement des données sur les ondes audio générées par les pales d'un des ventilateurs de l'ordinateur, selon un document publié la semaine dernière.

Des ondes sonores créées par le ventilateur

En contrôlant la vitesse de fonctionnement des ventilateurs, le malware arrive à produire différentes tonalités acoustiques qui peuvent être utilisées pour transmettre des données à un smartphone. Pour récupérer les informations, les cyberpirates ont besoin de placer le micro d'un téléphone mobile près du PC isolé afin de décoder les bruits émis par le ventilateur. Une fois les signaux sonores interprétés, le mobile transmet les données aux cyberpirates. Les chercheurs ont testé leur programme malveillant en utilisant un ordinateur de bureau Dell et un mobile Samsung Galaxy S4.



Les ondes sonores interceptées par le mobile sont décodées puis retransmises. Bien sur, ce malware affiche des limites. Un maximum de 15 bits peut être transmis par minute, ce qui ne paraît pas beaucoup mais suffit pour envoyer des mots de passe et des clefs de chiffrement selon les chercheurs. Pénétrer des PC de cette façon ne semble guère pratique, mais comme la plupart des ordinateurs sont encore équipés de ventilateurs pour refroidir les principaux composants, toutes les machines sont potentiellement vulnérables. Les entreprises et les agences gouvernementales qui exploitent des PC isolés peuvent cependant contrer ces attaques en installant des systèmes de refroidissement à eau ou utiliser des radiateurs passifs, c'est-à-dire sans ventilateur, si les caractéristiques techniques du processeur et des chipsets associés le permettent. Il est également conseillé d'interdire l'utilisation de téléphones mobiles dans les salles équipées de PC isolés et de bloquer, si possible, l'usage des ports USB.

Article de Serge Leblal



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, contenus, 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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Des chercheurs volent des données en utilisant le bruit des ventilateurs d'un PC – Le Monde Informatique

Le nombre de cyberattaques contre des cibles françaises double chaque année

Denis JACOPINI  vous informe	Le nombre de cyberattaques contre des cibles françaises double chaque année
---	--

Le salon international Eurosatory de défense et de sécurité s'ouvre lundi près de Paris alors que les cyberattaques contre des cibles françaises se multiplient.



Le salon international Eurosatory de défense et de sécurité s'installe comme tous les deux ans à partir de lundi à Villepinte, près de Paris. Cette manifestation qui rassemble les stratèges et les industriels du monde entier met de plus en plus l'accent sur deux concepts devenus incontournables : l'utilisation des drones et les outils de la cyberguerre. Une demi-douzaine de conférences se tiendront cette semaine sur la cybermenace et sur les moyens de la contrer ou de la mettre en œuvre. En France, depuis l'adoption du livre blanc 2013 et la loi de programmation militaire 2014-2019, la dimension « cyber » de nos armées « a changé de braquet », comme le confie au JDD l'un des meilleurs experts gouvernementaux de ce dossier.

Selon lui, le nombre de cyberattaques contre des cibles françaises double chaque année et le niveau de sophistication des agressions également. « Un individu aujourd'hui peut nous faire autant de mal qu'un État », précise notre source. Chaque jour en France, les unités informatiques liées aux institutions ou aux entreprises du secteur de la défense sont agressées par des milliers d'attaques. Des raids visant à saturer des adresses liées au ministère de la Défense se multiplient et il peut arriver que le compte personnel du ministre soit visé avec intention de nuire. Au point qu'aujourd'hui pas une seule clé USB ne peut entrer dans une installation de défense française sans être passée par une « station blanche » de décontamination.

Détruire sans avoir à bombarder

Mais le plus grand risque serait évidemment que nos unités militaires engagées sur un théâtre d'opérations soient attaquées en pleine action. Le pacte défense cyber lancé début 2014, et renforcé après les attentats de 2015, a prévu un investissement de plus d'un milliard d'euros et le triplement des effectifs militaires et civils concernés. « Aujourd'hui, plus un seul déploiement d'une unité sur le terrain ne se conçoit sans un accompagnement cyber », indique notre source.

Un officier général « cyber » est affecté en permanence auprès de l'état-major au Centre de planification et de conduite des opérations (CPCO). Il ne s'agit pas seulement de se protéger lors d'une attaque mais aussi de se défendre lorsqu'elle est en cours ou même d'attaquer en cas de besoin. Tout comme le fait depuis longtemps Israël contre ses adversaires au Moyen-Orient, l'État hébreu étant avec les États-Unis, la Chine et la Russie l'un des quatre pays les plus avancés dans ce domaine avec des moyens dix à vingt fois plus importants que ceux de la France. Mais on réfléchit à Paris à l'idée de créer une cyberarmée à l'image de l'US Cyber Command américain. Pour se préparer à ces guerres invisibles où l'on peut détruire une installation ennemie sans avoir à la bombarder ou à brouiller ses radars depuis un ordinateur pour mieux déclencher des raids plus... conventionnels.

Article original de François Clemenceau – Le Journal du Dimanche



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.



[Contactez-nous](#)

Réagissez à cet article

Inquiétantes intrusions dans les réseaux d'entreprises



Les intrusions dans les réseaux informatiques des entreprises se sont multipliées en France ces derniers mois et l'absence de vols de données laisse craindre des tentatives de sabotages ou d'attaques terroristes, a déclaré lundi le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi).



Le Secrétariat général de la défense et la sécurité nationale (SGDSN) et l'Anssi, deux services rattachés à Matignon, ont présenté lundi les trois premiers arrêtés liés à la protection des opérateurs d'importance vitale dans la santé, la gestion de l'eau et l'alimentation, qui entreront en vigueur le 1er juillet.

« Il y a de plus en plus d'attaquants, ce sont des agents dormants qui préparent les choses », a expliqué Guillaume Poupard à des journalistes. « Il y a eu beaucoup de cas à traiter ces derniers mois ».

Ces intrusions, par exemple par le biais d'emails piégés envoyés dans les entreprises, permettent aux attaquants de cartographier un réseau en toute discrétion et, en passant d'un réseau à l'autre, de pénétrer dans des zones inattendues.

« Ils prennent pied progressivement (...) et on les retrouve très profond au sein des réseaux d'entreprises, à des endroits où il n'y a même plus d'informations secrètes à voler, par exemple sur les systèmes de production de contrôle qualité », a ajouté Guillaume Poupard.

Ce nouveau type d'intrusion est d'autant plus inquiétant qu'il est presque plus facile d'entrer dans un réseau pour en modifier le fonctionnement ou en prendre le contrôle que pour voler des données, a-t-il souligné.

Au contraire de la banque, de l'aérospatiale et de l'automobile, habitués à surveiller de près leurs réseaux, l'industrie est encore mal préparée, étant moins sujette aux vols de données, a noté Guillaume Poupard.

« L'idée que des gens qui depuis l'autre bout du monde puissent chercher à détruire leur système de production c'est un nouveau scénario qui n'a pas vraiment d'équivalent dans le monde réel », a-t-il souligné.

Pour mieux défendre les PME, « un des maillons faibles », cible rêvée d'un attaquant, il prône le recours aux solutions de « cloud computing » des spécialistes de la sécurité numérique et à l'intégration de systèmes de protection dans les machines outils et les automates industriels dès leur conception. (Cyril Altmeyer, édité par Jean-Michel Bélot)



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

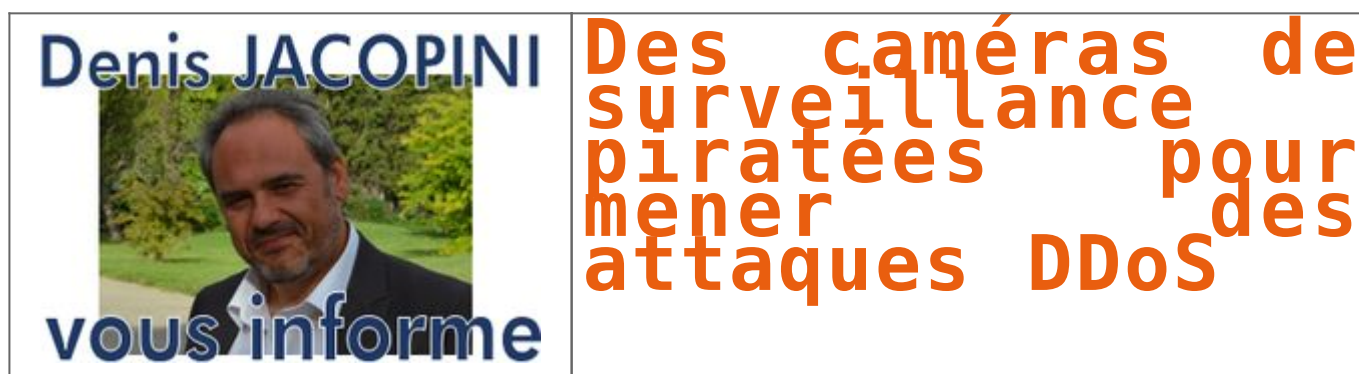
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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



[Contactez-nous](#)

Réagissez à cet article

Des caméras de surveillance piratées pour mener des attaques DDoS



Tous ceux qui refusent d'admettre que l'Internet des Objets pourrait être à l'origine de nombreuses menaces dans la sphère informatique de demain vont probablement avoir du mal à tenir leur position après l'affaire présentée ici. En effet, des hackers ont utilisé un réseau de 25 000 caméras de surveillance piratées pour conduire des attaques DDoS.



Des caméras de surveillance piratées pour former un botnet

Il y a quelques heures, l'entreprise Sucuri, spécialisée dans la sécurité informatique, a découvert que des hackers avaient réussi à prendre le contrôle de quelques 25 000 caméras de surveillance présentes au quatre coins de la planète.

Mais l'objectif des pirates n'était pas que de récupérer des images ou d'espionner des individus puisqu'ils ont utilisé les caméras de surveillance pour créer un botnet, autrement dit un réseau de machines contrôlées à distance par un seul et même individu.

Capables d'agir ensemble, les 25 000 caméras ont ainsi pu être à l'origine d'attaques DDoS contre plusieurs sites Internet. En effet, les hackers se sont servis du réseau de caméras de surveillance pour envoyer des requêtes simultanées sur des sites causant ainsi leur paralysie pendant de longues minutes.

Une preuve supplémentaire de la menace que laissent planer les objets connectés

Si l'utilisation d'objets connectés par les pirates pour mener des attaques DDoS est tout sauf une nouveauté, c'est l'ampleur de l'attaque qui surprend. En effet, même les spécialistes sont restés « coi » devant la capacité d'un réseau de 25 000 caméras de surveillance à générer autant de requêtes simultanément.

L'autre surprise tient au fait que les caméras piratées sont dispatchées aux quatre coins de la planète. 2% seraient d'ailleurs basées en France alors que c'est aux Etats-Unis, en Indonésie et à Taïwan que la majorité d'entre elles se situerait.

Sucuri a d'ailleurs cherché à comprendre ce que pouvait avoir en commun l'ensemble de ces appareils et la piste la plus sérieuse mène à BustyBox, un système qui serait intégré à tous. Or, une importante faille avait été découverte au printemps dans celui-ci ce qui aurait pu permettre à des pirates de l'exploiter pour commettre leurs actions.

Affaire à suivre...

Article original de Jérôme DAJOUX



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Des caméras de surveillance piratées pour mener des attaques DDoS

L'Etat français (ANSSI) va certifier les Cloud de confiance

Denis JACOPINI  vous informe	L'Etat français (ANSSI) va certifier les Cloud de confiance
--	--

L'Agence nationale pour la sécurité des systèmes d'information (Anssi) s'apprête à certifier les Cloud de quelques prestataires. Deux niveaux de labellisation sont attendus.



L'Agence nationale pour la sécurité des systèmes d'information (Anssi), dépendant du Premier ministre, est engagée dans un processus qui aboutira à la qualification des fournisseurs de Cloud. Les prestataires présentant le niveau de sécurité requis recevront donc un label de l'Agence, qui permettra aux entreprises et administrations de recourir à leurs services en se basant sur les garanties fournies par l'Etat français. « Huit prestataires se sont lancés dans ce processus de qualification », assure Guillaume Poupard, le directeur général de l'Anssi, qui a appelé les grands acteurs du Cloud américains à rejoindre le mouvement. « La qualification n'est pas un outil de protectionnisme », reprend Guillaume Poupard. Selon lui, les AWS et autre Microsoft (pour Azure) sont en train d'étudier une éventuelle qualification. Façon de dire aussi qu'il n'est pas acquis qu'ils se soumettent un jour aux exigences de l'Anssi. Notons que, sur ce dossier, l'Anssi travaille en coordination avec ses homologues allemands du BSI (l'Office fédéral de la sécurité des technologies de l'information) : un prestataire homologué outre-Rhin recevra automatiquement son label dans l'Hexagone et vice-versa.

Deux niveaux : Cloud Secure et Cloud Secure +

Ce label étatique fait suite à une démarche entamée dès la mi-2014. A cette époque, l'Anssi avait publié un premier référentiel et appelé les entreprises à le commenter. Un grand nombre de commentaires, parfois critiques, avaient été remontés à l'Agence. Depuis, cette dernière a réuni un comité restreint pour travailler à une seconde version du référentiel, largement inspiré de la norme ISO 27 801.



Guillaume Poupard, directeur général de l'Anssi.

En réalité, la démarche doit accoucher de deux niveaux de qualification : Cloud Secure et Cloud Secure +. Dans la première, selon des déclarations publiques d'un membre de l'Anssi en octobre dernier, on retrouve des bonnes pratiques assez classiques : contrôles d'accès physiques, authentification forte avec mots de passe hachés et salés, chiffrement logiciel et hébergement des données en Europe. Le niveau le plus élevé ira plus loin, imposant une authentification multi-facteurs, un chiffrement matériel (via HSM) ou encore un hébergement en France. Parmi les acteurs figurant dans la liste des premiers prestataires certifiés, on devrait retrouver Thales, Orange ou Oodrive, qui se présentait en octobre dernier comme l'acteur pilote de la qualification Secure Cloud +. Notons qu'à l'époque, l'Anssi indiquait que les OIV – les quelque 250 organisations identifiées comme essentielles au fonctionnement de la nation – pourraient se voir imposer le recours à des prestataires certifiés Secure Cloud +. Les premiers arrêtés encadrant les politiques de sécurité des OIV n'y font toutefois pas référence à ce jour.

Cloud Secure + : Les Américains out ?

« Nous nous sommes engagés à nous conformer à cette norme auprès de certains clients », explique Laurent Seror, le président d'Outscale, le fournisseur de IaaS né sous l'impulsion de Dassault Systèmes. « Etant donné que nous sommes déjà certifiés ISO 27 801, je considère que nous sommes prêts. Ne pas être certifié juste au moment de la sortie du référentiel ne sera pas pénalisant compte tenu de la longueur des cycles de décision », ajoute Laurent Seror. Ce dernier relève toutefois que, par construction, le niveau Cloud Secure + restera difficile à atteindre pour les grands prestataires américains. D'abord parce qu'ils ne possèdent pas, à ce jour, de datacenter en France (à l'exception de Salesforce). Mais, au-delà de ce seul élément, d'autres questions se posent. Selon lui, chez AWS, un administrateur américain, donc soumis au Patriot Act, peut accéder à toutes les machines virtuelles, quelle que soit la zone où ces dernières sont hébergées. « On en est sûr à 99% en raison de la nature d'une fonction qu'ils proposent pour la migration entre deux régions géographiques. Celle-ci suppose l'existence d'un réseau à plat entre toutes les plates-formes. »

La question de la localisation des données reste un élément central de la politique de certains pays européens souhaitant reconquérir leur souveraineté dans le Cloud. Lors du débat au Sénat sur le projet de loi pour une République numérique (porté par Aveline Lemaire), un amendement, déposé par les sénateurs du groupe communiste et prévoyant d'obliger les entreprises à stocker les données personnelles des citoyens français sur le territoire européen, a été voté. « Cet amendement n'était pas téléguilé, assure aujourd'hui Guillaume Poupard. Je l'ai découvert au moment des débats. » Le 29 juin, une commission mixte paritaire doit harmoniser les versions de ce projet de loi sorties respectivement des débats à l'Assemblée et au Sénat. Rien ne permet d'affirmer que ledit amendement, absent de la version votée par le Palais Bourbon, soit présent dans la mouture finale du texte de loi.

Article original de Reynald Fléchaux



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphoniques, risques data, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : L'Etat français va certifier les Cloud de confiance