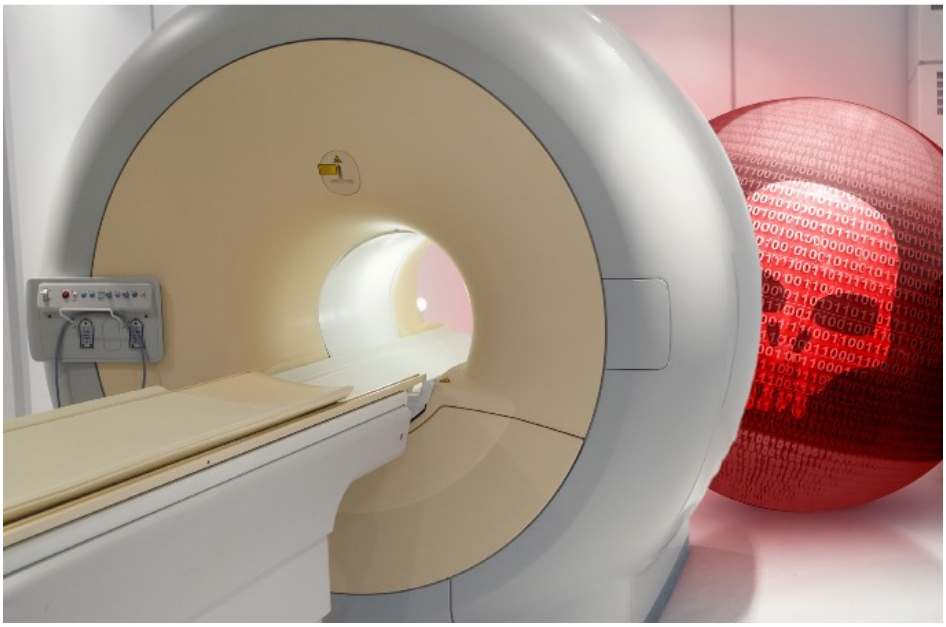
Risques d’infection dans le médical des Objets Connectés



Risques d’infection dans le médical des Objets Connectés

La faible sécurité des équipements de santé connectés entraîne la résurgence des vieux virus comme Conficker.

Un des problèmes de la montée en puissance de l'Internet des objets ? La sécurité.
Spécialistes, constructeurs, éditeurs répètent à longueur de conférences qu'il faut absolument que l'IoT soit « secure by design ». Entendez par là que les capteurs, le protocole de communication, la plateforme de traitement de l'information, l'architecture soient sécurisés dès leur conception.
Oui mais voilà, c'est sans compter sur le fameux héritage technique. Le monde de la santé rentre typiquement dans ce cadre et tout particulièrement les outils médicaux connectés. On pense ici aux IRM, scanners, radios, ou pompes à insuline. Ces équipements sont de plus en plus ciblés par les cyberattaquants, car ils sont moins bien protégés que des PC ou des serveurs.
Conséquence de cette faible sécurité, les vieux virus se rappellent aux bons souvenirs des administrateurs et des RSSI. Un rapport de la société de sécurité TrapX Labs, disséquant une attaque baptisée MEDJACK.2, montre que les attaques utilisent des malwares comme networm32.kido.ib ou le ver Conficker en complément de menaces plus sophistiquées. Moshe Ben Simon, co-fondateur de TrapX, résume bien ce paradoxe : « *un loup intelligent déguisé avec des vieux habits de mouton* ».

Mise en place de backdoors

Premier constat, les équipements médicaux connectés à Internet fonctionnent avec des versions de Windows non corrigées allant de XP (qui n'est plus supporté par Microsoft) aux versions 7 et 8. Des cibles de choix pour les anciens virus. « *Ces vieux virus sont utilisés avec des malwares (en l'occurrence MEDJACK.2) plus élaborés pour installer des backdoors dans l'établissement de santé et ensuite mener une campagne par exfiltration de données, voire se transformer en #ransomware* », souligne le rapport.
Les échantillons de Conficker que les experts de la société de sécurité ont analysé, montrent que le ver a été modifié pour avoir une meilleure capacité à se déplacer dans un réseau. Pire, son évolution fait qu'il est devenu indétectable pour les équipements médicaux. Dans son enquête auprès de 3 hôpitaux, TrapX relève qu'aucune alerte n'a été remontée par les établissements sur la présence de Conficker. A son apogée en 2009, Conficker avait infecté entre 9 et 15 millions d'ordinateurs. Il avait, comme capacité, de casser les mots de passe, d'enrôler les PC dans des botnets, etc. La version actuelle est diffusée par phishing envoyé aux personnels de l'hôpital.

Les données patients : la ruée vers l'or

L'objectif de ces attaques : obtenir les dossiers patients. Des informations très demandées sur le Dark Web et affichant une forte valeur marchande au marché noir. « *Les cybercriminels peuvent voler l'identité d'un patient pour se faire rembourser par les assurances des traitements coûteux et, en plus, revendre ces traitements au marché noir* ». TrapX estime qu'un dossier médical se monnaye entre 10 et 20 dollars sur le marché, contre 5 dollars pour une information financière. En début de semaine, on apprenait le vol de 9,3 millions de données de santé de citoyens américains. Le calcul est vite fait…
Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Sécurité : Conficker revient infecter l’IoT médical

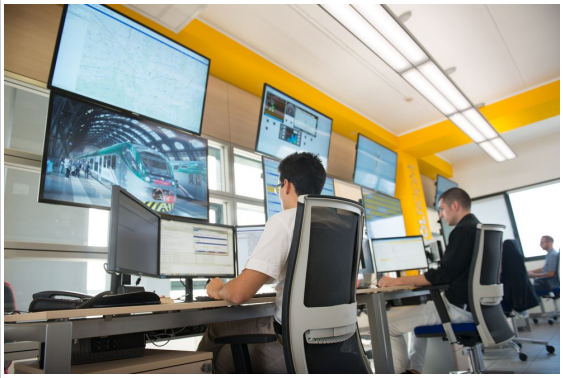
---

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 élaborés 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

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?

	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.

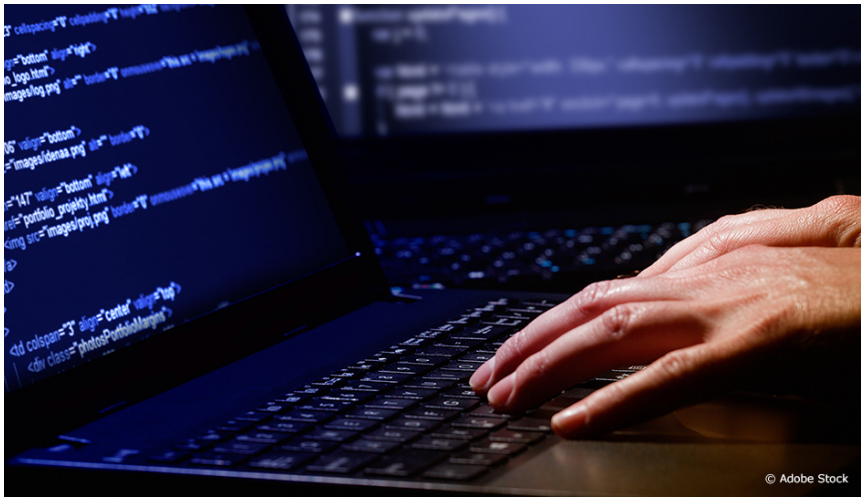
QUE FAIRE?
Pour se prémunir contre ces menaces, l'ACFM suggère à ses membres de se doter d'un cadre de cybersécurité, adapté à la taille de leur cabinet, en cinq étapes :
1. Identifier les biens qui doivent être protégés, de même que les menaces et les risques à leur égard;
2. Protéger ces biens à l'aide des mesures appropriées;
3. Détecter les intrusions et les infractions à la sécurité;
4. Intervenir s'il se produit un évènement de cybersécurité potentiel;
5. Évaluer l'incident et améliorer les mesures de sécurité à la lueur des évènements.
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

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



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 !

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

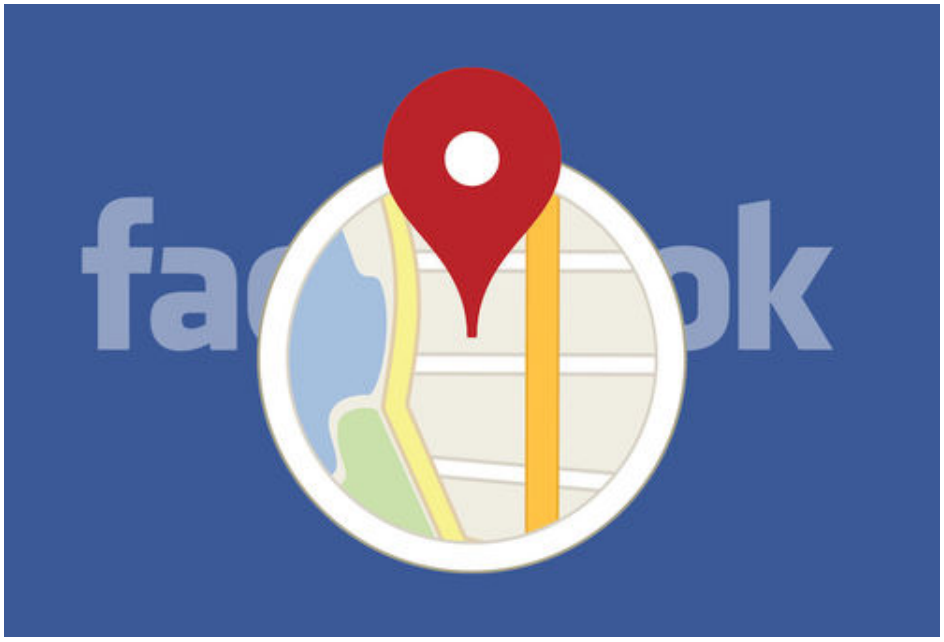
Les cybercriminels ont trouvé une nouvelle manière de se faire de l'argent. Cela faisait longtemps qu'ils tentaient de prendre en otage des disques durs, mais les gens sont devenus plus vigilants et n'ouvrent plus n'importe quelle pièce jointe à un mail. Voilà pourquoi les cybercriminels se sont vu contraints 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 des 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).

Réagissez à cet article

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

Facebook vous suit à la trace pour vous suggérer des amis



Facebook vous suit à la trace pour vous suggérer des amis

La géolocalisation de Facebook, utilisée notamment sur l'application mobile du réseau social, faisait déjà l'objet de nombreuses suspicions de la part des utilisateurs. Cette semaine, un porte-parole de Facebook a confirmé que la position géographique avait effectivement été utilisée par l'application pour suggérer de contacts que vous auriez pu croiser.

La fonction « Vous connaissez peut-être » de Facebook est souvent surprenante par sa précision, suggérant généralement des contacts pertinents. Si le site n'a jamais révélé vraiment les méthodes utilisées pour faire mouche aussi souvent, un de ses secrets vient en revanche d'être découvert : la géolocalisation permettrait de déterminer les personnes que vous fréquentez et qui disposent d'un compte. Concrètement, si deux personnes disposant d'un compte Facebook se trouvent au même endroit et ont activé la géolocalisation, le site proposera alors de les mettre en relation sur le réseau social. « La localisation elle-même ne suffit pas à déterminer que deux personnes peuvent être amies », indique un porte-parole de Facebook au journal anglais The Telegraph. Et c'est justement un des arguments avancés par les détracteurs de cette fonction, qui y voient une atteinte à la vie privée. Le site n'étant pas capable de déterminer si deux personnes se trouvant au même endroit sont amies, ou même si elles se connaissent réellement, l'usage d'une telle fonction peut sembler abusif sur certains aspects, et poser quelques problèmes concernant l'anonymat que certains voudraient conserver en public. Facebook a cependant indiqué que cette fonction n'était aujourd'hui plus active sur son application mobile, et que celle-ci avait simplement fait l'objet d'un test limité. Les plus inquiets peuvent néanmoins désactiver la géolocalisation pour l'application.

Article original de Nicolas AGUILA

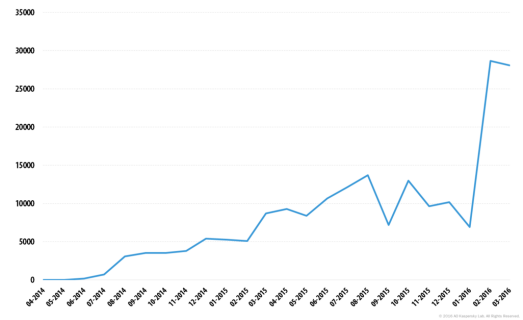
Réagissez à cet article

Original de l'article mis en page : Facebook vous suit à la trace pour vous suggérer des amis

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.



Nombre d'utilisateurs confrontés à des ransomwares pour appareils mobiles au moins une fois au cours de la période comprise entre avril 2014 et mars 2016

D'avril 2014 à mars 2015, les solutions de Kaspersky Lab pour Android ont protégé 35 413 utilisateurs contre des ransomwares pour appareils mobiles. Un an plus tard, ce nombre avait presque quadruplé et atteignait 136 532 utilisateurs. La part des utilisateurs attaqués par des ransomware par rapport aux utilisateurs attaqués par n'importe quel autre type de malware a également augmenté : de 2,04 % pour la période 2014-2015, elle est passée à 4,63 % pour la période 2015-2016. La courbe de croissance est peut-être plus modeste que celle observée pour les ransomwares pour PC, mais son ampleur suffit à confirmer une tendance inquiétante.

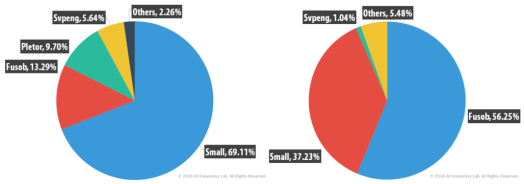
Principaux acteurs dans le milieu des ransomwares pour appareils mobiles

Sur l'ensemble de la période couverte par le rapport, les chercheurs de Kaspersky Lab ont été en mesure d'identifier les quelques familles de ransomwares pour appareils mobiles auxquelles les utilisateurs de nos produits étaient les plus souvent confrontés. En 2014-2015, il s'agissait de : Pletor, Fusob, Svpeng et Small. En 2015-2016, l'activité de Svpeng a enregistré une dégringolade et n'a concerné qu'une part modeste des utilisateurs attaqués.

A un moment donné en 2014-2015, Svpeng, connu à l'origine comme un malware bancaire, a été modifié par ses créateurs afin de pouvoir verrouiller un appareil infecté. Depuis lors, nous avons suivi les deux versions de Svpeng : le malware bancaire et le ransomware. La version ransomware est devenue populaire en 2014-2015 lorsqu'elle a touché 5,64 % des utilisateurs attaqués par un malware quelconque.

La situation a toutefois changé au cours de la deuxième période lorsque le ransomware a chuté vers le bas du Top 30 des menaces. Toutefois, la version malware bancaire de Svpeng a repris du service, ce qui signifie probablement que les créateurs du malware ont simplement perdu leur intérêt dans le développement d'un ransomware et ont décidé de se concentrer sur le malware bancaire.

Pletor, le malware considéré comme le premier exemple de ransomware et prétendument créé par les auteurs du tristement célèbre trojan bancaire Acecard, a connu une situation similaire. Au cours de la période 2014-2015, il a touché une part considérable des utilisateurs mobiles attaqués par des ransomwares mais en 2015-2016, il ne figurait plus dans le haut du classement et laissait le « marché » à seulement trois grandes familles de ransomwares.



Répartition de la part d'utilisateurs attaqués entre les familles de ransomwares pour appareils mobiles les plus actives en 2014-2015 (gauche) comparée à celle de 2015-2016 (droite).

Parmi les autres phénomènes importants observés au cours des 24 mois couverts par le rapport, on ne peut ignorer la concurrence entre deux grandes familles de ransomwares : Small et Fusob. En 2014-2015, c'est la famille Small qui dominait, du moins en termes de parts d'utilisateurs attaqués. Elle était signalée par 69,11 % de l'ensemble des utilisateurs qui avaient été confrontés au moins une fois à des ransomwares pour appareils mobiles. Mais un an plus tard, c'est la famille Fusob qui prenait la tête avec 56,25 % des utilisateurs. Toutefois, la famille Small se maintenait en 2e position avec 37,23 % des utilisateurs attaqués. Il est probable que les malwares Svpeng, Pletor, Small et Fusob seront vendus par leurs auteurs à d'autres cybercriminels ou qu'ils seront propagés via des réseaux d'affiliés. Les quatre familles ont subi de nombreuses modifications. Cependant, Small et Fusob semblent avoir été les plus modifiés, comme on peut le voir clairement dans les statistiques.

A la différence du phénomène des ransomwares pour PC qui est déjà largement couvert par les chercheurs de différentes sociétés, dont Kaspersky Lab, les ransomwares pour appareils mobiles n'ont pas encore fait l'objet d'une analyse en profondeur. Afin de remédier à cette situation, nous proposons une brève description des ransomwares les plus répandus et les plus dangereux à compter d'avril 2016

Pour en savoir plus sur l'évolution de la menace des ransomwares, lisez le rapport complet accessible via.

Article original de Kaspersky Lab

Réagissez à cet article

Original de l’article mis en page : Rapport KSN : ransomwares pour appareils mobiles en 2014-2016 – Securelist

---

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

	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.

Figure 1. A typical exfiltration scenario. A compromised computer (A) - without speakers, and with aud hardware disabled - transmits sensitive information via acoustic signals. This information is received and decoded by a nearby mobile phone (B)

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.

Figure 1. A typical exfiltration scenario. A compromised computer (A) - without speakers, and with aud hardware disabled - transmits sensitive information via acoustic signals. This information is received and decoded by a nearby mobile phone (B)

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.

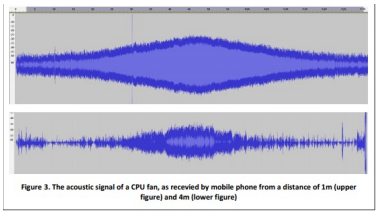


Figure 3. The acoustic signal of a CPU fan, as recevied by mobile phone from a distance of 1m (upper figure) and 4m (lower figure)

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, 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

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

	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

---

Réagissez à cet article

Original de l’article mis en page : Faut-il investir dans la guerre invisible? – leJDD.fr

---

Inquiétantes intrusions dans les réseaux d’entreprises

Inquiétantes intrusions dans les réseaux d’entreprises

Les intrusions dans les réseaux informatiques des entreprises se sont multipliées en France ces derniers mois et labsence de vols de données laisse craindre des tentatives de sabotages ou dattaques terroristes, a déclaré lundi le directeur général de lAgence nationale de la sécurité des systèmes dinformation (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)

Réagissez à cet article

Original de l’article mis en page : SAFRAN : France : Inquiétantes intrusions dans les réseaux dentreprises