Un cousin du malware Furtim cible les énergéticiens européens

Un cousin du malware Furtim cible les énergéticiens européens

SentinelOne a découvert une variante du malware Furtim qui vise les sociétés européennes dans le domaine de l'énergie.

En mai dernier, des chercheurs la société EnSilo ont découvert un malware baptisé Furtim qui devait son nom à une obsession virant à la paranoïa de ne pas être détecté par les outils de sécurité. De la préparation à son installation jusqu'à son implémentation, le malware scrute, analyse et bloque tout ce qui touche de près ou de loin à la sécurité IT.

Il semble que ce malware revienne sous une autre forme pour s'attaquer au système industriel des entreprises énergétiques européennes. Des chercheurs de SentinelOne l'ont détecté au sein du réseau d'un énergéticien européen. Cette menace a un nom, SFG, et a été trouvée à la fois par une remontée d'information des logiciels de SentinelOne, mais aussi sur des forums privés. Les experts ont travaillé sur les échantillons pour comprendre son fonctionnement. Les résultats de cette analyse montrent que le comportement, la sophistication et la furtivité du malware sont l'œuvre d'un Etat ou pour le moins d'une organisation soutenue par un gouvernement. Les experts penchent pour une initiative provenant de l'Europe de l'Est.

Jusqu'au sabotage du réseau énergétique

Dans le détail, le cousin de Furtim s'appuie sur les mêmes exploits pour éviter d'être repéré par les outils de sécurité (antivirus, firewall next gen, solution endpoint, sandboxing). Plusieurs développeurs de haut niveau ont mis la main à la pâte pour perfectionner SFG. L'objectif est multiple, extraire des données ou faire tomber le réseau d'énergie, sans laisser de traces. Le malware affecte toutes les versions de Windows, précise SentinelOne dans un blog. Il situe ses débuts au mois de mai dernier et il est encore actif.

Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque s'appuyant sur le malware Blackenergy. Ce type de menaces est pris très au sérieux par les gouvernements au point de forcer les entreprises à remonter leurs niveaux de sécurité. En France, l'ANSSI peaufine les arrêtés sectoriels sur la sécurité des OIV (opérateurs d'importance vitale) notamment dans le domaine de l'énergie.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Malware : un cousin de

Furtim cible les énergéticiens européens

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

---

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

La rencontre qui devrait être clôturée vendredi dernier vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité.

(CIO Mag) – Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

Le directeur général de l'agence tunisienne de sécurité informatique, lui, indique que Tunis a pris très tôt des initiatives pour lutter contre la cybercriminalité. Mohamed Naoufel Frikha, repris par nos confrères, rappelle qu'un travail important a été réalisé depuis 1999 avec la création du premier centre en Afrique, le troisième dans le monde arabe.

Le rendez-vous de Tunis entend amener les pays arabes à créer des centres de cyber-alerte. Leur nombre est très insuffisant dans l'espace arabophone puisque seuls dix pays en disposent. Des représentants de treize Etats prennent part aux échanges.

Article de Ousmane Gueye

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 : Cybercriminalité: les pays

arabes mutualisent leurs forces pour faire face au phénomène | CIO MAG

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*

Airbus déjoue douze attaques informatiques majeures par an

Airbus déjoue douze attaques informatiques majeures par an

Le chiffre a de quoi inquiéter pour les non-initiés. Airbus Group, la maison mère de l'«aéronner» toulousain, subit chaque année des milliers de cyberattaques en provenance du monde entier.

Parmi ce flot, seule une dazaine sont jugées vraiment «sérieres» par Stéphane Lenco, le directeur de la sécurité informatique du géant de l'aéronactique et de la défense. Airbus Group et ses divisions doivent faire face à deux grands types d'attaques informatiques : contre son propre réseau d'information d'abord (internet, intranet, serveurs…) et contre ses produits, c'est-à-dire contre l'intelligence embarquée à bord de ses avions, ses satellites, ses missiles, etc.

Parmi ces attaques se cachent certains groupes obcrités par des «tats». Ce fut le cas lorsqu'en 2013 un groupe militaire chinois est parvenu à pénétrer les «bseaux du New York Times grâce à une série d'«mails d'hameçonnage et à des logiciels malveillants (malwares) mis au point spécialement pour cette intrusion. «Les motivations de ce type de pirates peuvent être multiples. Ils peuvent rechercher un accès à des brevets, à des propositions commerciales usire à la messagerie des top managers allant jusqu'au MDS» confie une source interne à Airbus Defence and Space spécialiste de la cyberséurité.

Mais pour des industriels comme Airbus le principal danger reste les actions de sabotage qui visersient à ralentir ou perturber la production d'avions par exemple.

Une variante de ce type d'attaque consiste aussi à réclamer une rançon afin par exemple de donner une clef informatique indispensable pour décrypter des fichiers que les pirates ont encryptés. «Airbus s'«ct pas directtement visé par ce type d'attaque mais elles connaissent une énorme explosion actuellement auprès des industriels» a souligné le patron de la sécurité d'Airbus Group au cours d'une récente conférence en Australie.

Les cyberattaques dont doit se protéger Airbus

Les menaces

- Attaques des systèmes industriels
- Vols de données
- Fraude sécurité Airbus
- Usurpation d'identité (F-ion spoofing)
- Cryptomnnaies & Bitcoin
- Cyberattaques de type «Hacktivisme»
- Attaques logicielles (piratage, modification…)

Compromission de drones/satellites (APT Espionnage/sabotage)

- Piratage réseaux
- Attaques ciblée du réseau aircraft
- Détection & analyse cybermenace

Les infrastructures pouvant être visées

Hangars/pylônes — Centrales — Aéroport Toulouse-Blagnac — Tarmac — Satellites — Aéroports — Centrale de surveillance du trafic aérien — Centre d'opérations Continuum

Les équipements pouvant être visés

Aéronef Airbus/drones — Tarmac — Satellites

145 000 employés, autant de portes d'entrée

Et de citer l'exemple de cet employé d'un sous-traitant d'Airbus qui à vu ses fichiers de son ordinateur se crypter alors qu'il se connectait au réseau de l'«entreprise étendue d'Airbus. Il s'agit d'un extranet qui permet aux fournisseurs d'Airbus de dialoguer, d'échanger des documents, de livrer des plans,etc. avec leur donneur d'«rdres.

Grâce à l'action des services de sécurité d'Airbus, cette attaque a pu être déjouée dans les deux heures et les sauvegardes activées. Ainsi, «i les opérations d'Airbus «i les données de ses recherches s'ont été attaquées.

C'«ct bien l'un des problèmes du groupe aéronautique. Il compte 165 sites dans 35 pays et 145 000 employés dans le monde. «Ce sont autant de portes d'entrée qu'il faut sécuriser même si les pirates ne ciblent pas tout le monde mais seulement les plus intéressants ou les plus vulnérables» analyse un expert de la cyber-sécurité.

«Le sonde Keelback Net permet aux cyber experts d'Airbus DS à Élancourt de détecter 24 heures sur 24, 7 jours sur 7, dans le réseau du client toute trace ou comportement suspects, en particulier les signaux faibles confie le responsable d'Airbus Defence and Space». Il faut en effet agir vite pour éviter ou limiter les dégâts de ces intrusions malveillantes. Ainsi Airbus D & S a «is au point Keelback Net qui détecte le plat en amont possible les cyber-menaces persistantes avancées (Advanced Persistent Threats en anglais APT) qui sont les plus dangereuses car les plus difficilement détectables.

Le but d'une attaque APT «ct de s'«mbusiire dans un ordinateur susceptible de contenir des informations de valeur ou, s'il s'«n détient pas, qui peut se transformer en passerelle pour atteindre un ordinateur plus intéressant. Les pirates peuvent ainsi installer un enregistreur de frappes qui lit tout ce que le clavier tape ou bien créer une porte dérobée (backdoor) sur l'ordinateur d'un employé lambda qui «ct connecté sur le même réseau que les ordinateurs qui contiennent, mus, des données importantes.

Aucun hacker n'est embauché chez Airbus

Face à ces attaques qui se multiplient depuis cinq ans, Airbus Group a «kagé en mobilisant des budgets importants. «Quand le patron (Tom Enders) vous donne de l'«rgent, il veut des résultats» a lancé Stéphane Lenco. Mais il concède qu'il y a encore des progrès à faire.

Mais selon des pirates du dernier, pas question d'«mbauche des hackers chez Airbus pour acquérir plus vite cette nouvelle façon de penser. Ce n'est pas la philosophie. De «ours difficiles, du «ment difficiles. Ce «ment ne les intéresse pas.

Sur le terrain, des «mesures régulières rappelent aux salariés d'Airbus les précautions à prendre comme ne pas laisser traîner des clefs USB qui pourraient alors embarquer un logiciel espion si elles tombaient dans des mains mal intentionnées.

Une division spéciale de 600 experts

C'«ct à Élancourt dans les Yvelines qu'Airbus Defence and Space abrite une branche entière dédiée à la cybersécurité. Créée en 2011 elle concentre 600 experts répartis entre la France, l'Allemagne et le Royaume-Uni. Ces compétences particulières sont utilisées tant au «ein même d'Airbus Group que pour des clients externes comme les gouvernements, les infrastructures critiques et les grandes entreprises stratégiques. En décembre dernier, Airbus DS a ainsi «té choisie par TVS Monde pour sécuriser son système l'information suite à la cyber attaque subie par la chaîne le 9 avril 2015 et qui avait paralysé l'«ntenne. Autre client de marque : les forces armées françaises pour lesquelles Airbus DS déploie un système de lutte informatique défensive qui identifie les cyber attaques, récupère les éléments de contexte de chacune d'entre elles (origine, destination, criticité et impact) et les combat dans le cadre d'un plan de «réaction. Airbus DS capitalise sur cette expérience auprès des militaires pour améliorer sa gamme de services qui sont ensuite proposés à des clients civils. «Airbus DS CyberSecurity investit 20 % de son chiffre d'affaires dans la recherche et développement (R & D) pour rester «up to date»… [Lire la suite]

Gil BOUSQUET est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (vols, espionnage, piratage, fraudes, sabotages informatiques) : E. judiciaires (Investigations téléphones, disques durs, e-mails, fichiers informatiques, récupération de fichiers…)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formateur de l'I.S.J. (Intervenants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL et «CNIL Informatique».

Le Net Expert INFORMATIQUE — Spécialiste en Cybercriminalité, Informatique et Libertés

Contactez-nous

Réagissez à cet article

Source : *Piratage informatique : Airbus déjoue douze attaques majeures par an — 06/05/2016 — ladepeche.fr*

article de Gil Bousquet

Une alerte à la bombe dans un avion causée par un réseau Wi-Fi

Une alerte à la bombe dans un avion causée par un réseau Wi-Fi

Les passagers d’un vol interne australien ont eu une petite frayeur à cause d’un réseau WiFi.

Le réseau WiFi en question a été repéré par un des passagers qui, inquiet de ce nom étrange, en a tout de suite informé le personnel de bord. Ce dernier a alors remonté l’information jusqu’au commandant de bord, qui a décidé de garder l’avion au sol tant que l’appareil émetteur de ce réseau n’a pas été repéré. Une annonce retentit dans les hauts parleurs de l’avion afin de prévenir les passagers, mais après une demi-heure de recherche, la source n’est toujours pas localisée.
« Un réseau WiFi peut avoir une bonne portée, donc cela aurait pu venir d’une personne dans le terminal », explique un des passagers. Des recherches sont menées dans et autour de l’avion, sans résultat. Finalement, après trois heures d’attente sur le tarmac, l’avion se met finalement en route pour sa destination, Perth, en Australie, où il atterrit sans encombre 80 minutes plus tard... [Lire la suite]

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

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (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

Suivez-nous sur

Réagissez à cet article

Source : *Une alerte à la bombe dans un avion causée par un réseau Wi-Fi*

Critical Infrastructure Sectors of Nations facing cybercrime

Critical Infrastructure Sectors of Nations facing cybercrime

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.
PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector
The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. A system of prevention, preparedness, response, and recovery elements, the Emergency Services Sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, manmade incidents, and natural disasters.

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century.

Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Réagissez à cet article

Source : *Critical Infrastructure Sectors | Homeland Security*

L’aviation civile n’est pas à l’abri du cyber-terrorisme

L’aviation civile n’est pas à l’abri du cyber-terrorisme

A la demande de l’Agence européenne de sécurité aérienne (Aesa), un hacker pourvu d’une licence de pilote d’avion commercial a démontré qu’il pouvait en quelques minutes entrer dans le système de messagerie des compagnies maritimes.

A l’instar des machines industrielles et des objets domestiques connectés, les véhicules et les avions n’échapperont pas aux attaques des cybercriminels. « L’aviation civile doit se préparer aux cyber-risques », prévient d’ailleurs Patrick Ky, le directeur exécutif de l’Agence européenne de sécurité aérienne (Aesa). En poste depuis 2013, ce dernier s’est exprimé lors d’un petit déjeuner organisé par l’association des journalistes de la presse aéronautique et spatiale (Aspae) en octobre dernier. Ses propos ont été rapportés dans de nombreux journaux tels que Les Echos, Le Parisien ou encore l’Usine Nouvelle. Patrick Ky est formel : le piratage informatique d’un avion est possible et la cybercriminalité représente bien une véritable menace pour le transport aérien.

Pour illustrer ses propos, le directeur exécutif de l’Aesa a confié qu’il avait fait appel à un Hacker. Cet expert en informatique – également titulaire d’une licence de pilote d’avion commercial – est parvenu en quelques minutes à entrer dans le système de messagerie Acars (Aircraft Communication Addressing and Reporting System) en se faisant passer pour un des administrateurs du réseau. Lequel sert aux compagnies aériennes à envoyer des messages automatiques et réguliers de l’avion vers le sol pour s’assurer du bon fonctionnement des systèmes critiques de l’avion.
Risque accru. Demain, le risque de cyberattaque va être accru avec la mise en place du système Sesar (Single European Sky ATM Research ; en français : Ciel unique européen) qui vise à harmoniser en Europe le trafic aérien en déployant un réseau et de nouveaux systèmes de gestion d’ici 2025. Ce nouveau réseau européen de contrôle du trafic aérien aura la possibilité de donner directement des instructions aux systèmes de contrôle de l’avion. Pour limiter les risques de piratage, l’agence européenne pourrait, à long terme, se charger de certifier les équipements contre les risques de cyberattaques sachant qu’elle a déjà la responsabilité de certifier les aéronefs en Europe. A court terme, Patrick Ky veut mettre en place une structure en charge d’alerter les compagnies aériennes sur les cyberattaques. Un risque sur lequel Air France, que nous avons contacté, ne s’est pas encore publiquement prononcé.

Réagissez à cet article

Source : *L’aviation civile n’est pas à l’abri du cyber-terrorisme*

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

	Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Invité à s'exprimer sur France Inter, vendredi 8 janvier, sur les attentats qui ont frappé la France en 2015 et l'attaque, la veille, d'un commissariat du 18e arrondissement de Paris, le procureur de la République à Paris, François Molins, est revenu sur l'une des principales difficultés techniques à laquelle font face les enquêteurs en matière d'antiterrorisme : travailler sur les « téléphones cryptés » retrouvés, dont les codes de verrouillage sont de plus en plus complexes à casser.

« Tous les smartphones qu'on essaie aujourd'hui d'exploiter sont verrouillés et cryptés (…) *toutes les communications passées par les terroristes sont passées à l'aide de logiciel de cryptage »*, a expliqué M. Molins, qui a cependant tu les noms des principaux logiciels utilisés.
« Les évolutions technologiques et les politiques de commercialisation d'un certain nombre d'opérateurs font que si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans les téléphones », a souligné M. Molins. La totalité des données deviennent ainsi inaccessibles à quiconque ne possède pas le code de déblocage.

PLUSIEURS TÉLÉPHONES N'ONT TOUJOURS PAS ÉTÉ « CASSÉS »

Une difficulté qui rend les enquêteurs *« aveugles »* dans certains cas et les prive de moyens d'investigation, a regretté M. Molins, en citant notamment le cas de Sid Ahmed Ghlam.
L'un des téléphones de l'étudiant algérien soupçonné d'un projet d'attentat contre une église de Villejuif au printemps n'a, en effet, toujours pas été « *cassé* » par les policiers. Mais un iPhone 4S saisi dans le cadre de l'enquête sur le 13 novembre garde également, à ce jour, tous ses mystères.
Dans les jours qui ont suivi les attentats du 13 novembre, la direction centrale de la police judiciaire (DCPJ) a ainsi demandé à tous ses services de résumer les problèmes posés par les *« téléphones cryptés »*.*« Les téléphones de dernière génération disposent de codes verrous très compliqués à casser ou contourner »*, expliquait au *Monde* le service central de l'informatique et des traces technologiques de la police judiciaire (SCITT) en réponse à la demande de la DCPJ.

De quoi inquiéter ces experts de la police scientifique : *« Les solutions utilisées ne sont pas pérennes, dans la mesure où elles sont basées sur l'exploitation de failles logicielles, le plus souvent corrigées lors des mises à jour. »* C'est le cas de l'iPhone de l'enquête du 13 novembre.

En 2014, sur 141 téléphones analysés par le SCITT, six n'ont pu être explorés. Quant à 2015, *« huit smartphones n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé »*, a détaillé M. Molins.

Concernant le cryptage, *« il n'existe à ce jour aucune solution permettant aux services techniques de déchiffrer systématiquement les données »*, assure la sous-direction de la lutte contre la cybercriminalité, également sollicitée par *Le Monde*.

UNE ACTION JURIDIQUE POUR REMÉDIER AU PROBLÈME

Deux solutions s'offrent alors aux services d'enquête judiciaire. D'abord faire appel à la direction générale de la sécurité intérieure (DGSI). Mais le centre technique d'assistance du service de renseignement répond dans un délai moyen de trois mois, et sans garantie de succès. De toute façon, reconnaît une source à la DCPJ, *« cette possibilité semble ignorée par de nombreux services »*. Les policiers peuvent aussi, éventuellement, se tourner vers les fabricants, dont certains, comme Apple, acceptent désormais, *« dans le cadre d'une urgence vitale »*, de communiquer les données stockées dans le « cloud ». A supposer qu'une sauvegarde ait été réalisée par le mis en cause.
Autant dire que le pessimisme règne du côté des services d'enquête comme des experts de la police technique et scientifique. *« Il paraît illusoire d'attendre une solution multisupport qui permettrait un accès aux données verrouillées. Seule une action juridique pourrait permettre d'obtenir ces données par le biais d'un instrument légal… Le problème réside cependant dans le poids d'un tel outil juridique face à des opérateurs ou des industriels ayant leur siège à l'étranger »*, conclut le SCITT.

Réagissez à cet article

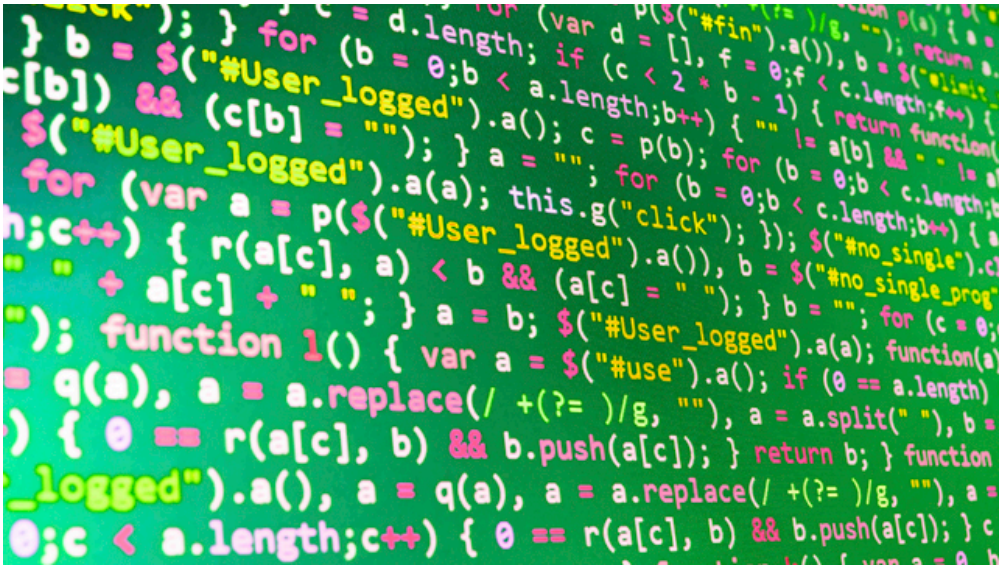
Source : *Les téléphones cryptés, casse-tête des enquêtes antiterroristes*

Par Laurent Borredon

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

Les sites Web censurés sont désormais indiqués par un code « Error : 451 » de l'Internet Engineering Task Force.



L'Internet Engineering Task Force – IETF – vient d'officialiser un nouveau code d'erreur pour indiquer qu'un site est bloqué ou censuré par un organisme gouvernemental. Suite à ce vote, les internautes du monde entier vont désormais savoir quand un gouvernement veut leur interdire d'accéder à un site Internet. Le code en question – Error 451 (en anglais) – devient synonyme de censure sur Internet. Le code HTTP Erreur 404 est bien connu des internautes, tout comme le code Erreur 500 dans une moindre mesure – qui indique un problème de serveur. Ne doutons pas que l'**Erreur 451** va rapidement devenir l'un des codes d'erreur stars de la toile.

L'organisme de standardisation du Web a décidé d'indiquer dans un souci de transparence qu'un site Internet est interdit, bloqué ou censuré dès qu'un utilisateur tente de s'y connecter. L'IETF prévoit notamment que le gouvernement à l'origine de cette censure pourra accompagner le message d'erreur d'une explication sur les causes du blocage d'accès. L'origine du nombre « 451 » est une référence dans la plus pure tradition des geeks, puisque l'erreur 451 renvoie à l'ouvrage de science-fiction de Ray Bradbury « **Fahrenheit 451** » publié en 1953 et dont le thème central est la dénonciation de la censure et de toute forme de propagande. Le message universel de libre accès l'information sur Internet existe encore.

Réagissez à cet article

Source : *Le code Erreur 451 synonyme de censure*