Révélations sur de petits piratages informatiques entre alliés…

Révélations sur de petits piratages informatiques entre alliés…

C’est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l’ancien directeur technique de la DGSE, le service de renseignement extérieur français, s’est livré en juin dernier à une longue confession devant les élèves de l’école d’ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l’explique Le Monde.

Cet ex-cadre de l’espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l’attaque informatique de l’Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l’Elysée. Jusqu’à présent, les soupçons se portaient bien vers la NSA mais ils n’avaient jamais été confirmés. « Le responsable de la sécurité informatique de l’Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l’aide. On a vu qu’il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J’en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s’entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c’était eux. A la fin de la réunion, Keith Alexander (l’ex-directeur de la NSA), n’était pas content. Alors que nous étions dans le bus, il me dit qu’il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : ‘Vous êtes quand même bons.’ Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. »

Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l’implication de la France dans une vaste opération d’espionnage informatique commencée en 2009 qui avait touché notamment l’Espagne, la Grèce ou l’Algérie. Le Canada, lui aussi visé, avait à l’époque soupçonné Paris, mais rien n’avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu’ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu’il était français. Et effectivement, c’était un Français. »

Article original de Thomas Liabot

Réagissez à cet article

Original de l’article mis en page : Les Etats-Unis étaient bien à l’origine du piratage informatique de l’Elysée en 2012 – leJDD.fr

---

Pokémon Go inquiète l’armée française !

Pokémon Go inquiète l’armée française !

Une note de la Direction de la protection des installations militaires explique en quoi le jeu Pokémon Go représente une menace pour les sites protégés du ministère de la Défense, et délivre des consignes pour interdire le jeu à proximité des zones concernées.

L'accès aux sites militaires est interdit – ou très restreint – au grand public. Et cela vaut également pour les Pokémon. Du moins c'est l'intention affichée par le ministère de la Défense dans une note dévoilée par Le Canard Enchaîné dans son numéro du 31 août (page 4).

Le document révélé date du 25 juillet et est en effet signé par le contre-amiral Frédéric Renaudeau, patron de la Direction de la protection des installations, moyens et activités de la Défense (DPID). On y apprend que plusieurs zones sensibles du ministère de la défense « *abriteraient ces objets et créatures virtuelles. Les risques d'intrusion ou d'attroupement à proximité immédiate sont réels* ».

TOUTE PRÉSENCE DE CRÉATURES ET D'OBJETS VIRTUELS À L'INTÉRIEUR DES ENCEINTES DEVRA ÊTRE SIGNALÉE

Le ton est grave et les risques de Pokémon Go sont fortement soulignés par le contre-amiral. Celui mentionne en effet plusieurs points qu'il juge très dangereux :

- *« sous couvert du jeu, il ne peut être exclu que des individus mal intentionnés cherchent à s'introduire subrepticement ou à recueillir des informations sur nos installations […] ;*
- *les données de géolocalisation des joueurs, non protégées, pourraient donner lieu à exploitation ;*
- *ce jeu peut générer des phénomènes addictifs préjudiciables à la sécurité individuelle et collective du personnel de la défense. »*

Pour contrer la menace, le contre-amiral a délivré des consignes strictes. Le Canard Enchaîné affirme ainsi que dans une annexe de la note, ce dernier interdit l'utilisation de l'application à l'intérieur et à proximité des sites militaires et demande à ce que les forces de sécurité intérieure soient alertées en cas d'attroupement sur la voie publique.

La conclusion de la note est sûrement l'élément le plus incongru. Il y est en effet précisé que « toute présence de créatures et d'objets virtuels à l'intérieur des enceintes » devra être signalée à la DPID. Grâce à cela, le document officiel estime que « cette cartographie permettra de consolider notre évaluation de la menace ».

Il est intéressant de voir à quel point le jeu Pokémon Go peut susciter les pires craintes des hautes sphères décisionnelles. Ici, on ne peut s'empêcher d'esquisser un sourire en lisant les termes un tantinet exagérés pour parler des dangers de l'application. On peut également dénoncer quelques paradoxes. En effet, comment signaler la présence d'une créature sur les sites concernés si l'utilisation de Pokémon Go est formellement interdite ?

On peut tout de même nuancer en estimant que le ton un brin catastrophique de la note est de rigueur pour tout ce qui touche à la sécurité intérieure, surtout dans le contexte actuel. À noter que, récemment, la ministre Najat Vallaud-Belkacem, a demandé rendez-vous avec Niantic pour retirer tous les Pokémon rares dans les établissements scolaires.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Quand Pokémon Go inquiète l'armée française – Pop culture – Numerama

---

Filtre anti espion sur les

prochains ordinateurs portables Hewlett-Packard

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Le géant de l'informatique Hewlett-Packard s'associe avec 3M pour préinstaller sur ses prochains ordinateurs portables professionnels un filtre anti espion.

Quoi de plus courant que de croiser à la terrasse d'un café, dans le train ou dans un aéroport ces fiers commerciaux pressés de travailler, même dans un lieu non sécurisé. Autant dire que collecter des données privées, sensibles, en regardant juste l'écran de ces professionnels du « c'est quoi la sécurité informatique ? » est un jeu d'enfant.

Hewlett-Packard (HP), en partenariat avec 3M, se prépare à commercialiser des ordinateurs portables (Elitebook 1040 et Elitebook 840) dont les écrans seront équipés d'un filtre anti voyeur. Un filtre intégré directement dans la machine. Plus besoin d'utiliser une protection extérieure.

Une sécurité supplémentaire pour les utilisateurs, et un argument de vente loin d'être négligeable pour le constructeur. Selon Mike Nash, ancien chef de la division de sécurité de Microsoft et actuellement vice-président de Hewlett-Packard, il est possible de croiser, partout, des utilisateurs d'ordinateurs portables sans aucune protection écran. Bilan, les informations affichés à l'écran peuvent être lues, filmées, photographiées.

Le filtre pourra être activé et désactivé à loisir.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : Filtre anti espion sur les

prochains Hewlett-Packard – Data Security BreachData Security Breach

---

Shadow Brokers, une affaire de Cyberespionnage

Shadow Brokers, une affaire de Cyberespionnage

Tour d'horizon des conséquences d'une affaire de cyber-espionnage au retentissement international alors que les fichiers mis en ligne par les mystérieux Shadow Brokers, et probablement dérobés à la NSA, commencent à livrer leurs secrets.

1) Pourquoi un tel intérêt pour les Shadow Brokers ?

Lundi 15 août, un groupe de hackers appelé Shadow Brokers a annoncé avoir piraté des systèmes informatiques utilisés par Equation, une organisation réputée proche de la NSA. A l'appui de ses affirmations, ce groupe jusqu'alors inconnu a posté deux archives sur des sites de partage. La première, en libre accès, renferme 300 Mo de données, où se mêlent des outils et des techniques pour infiltrer des systèmes…. [lire la suite]

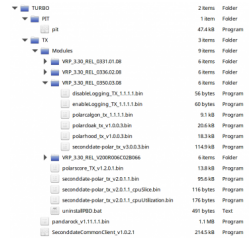
2) Le hacking de la NSA est-il établi ?

Bien entendu, ni la célèbre agence américaine ni le groupe de hackers Equation, réputé proche de celle-ci, n'a confirmé que les outils mis en ligne par les Shadow Brokers provenaient bien de leurs serveurs. Mais plusieurs éléments concordants établissent un lien direct entre les fichiers mis en ligne par les Shadow Brokers et le couple NSA/Equation. D'abord, c'est l'éditeur russe Kaspersky qui remarque que plus de 300 fichiers présents dans la première archive utilisent une implémentation des algorithmes de chiffrement RC5 et RC6 identique à celle utilisée par le groupe Equation. « *La probabilité que tout ceci (l'archive mise en ligne, NDLR) soit un faux ou ait été conçu par rétro-ingénierie est extrêmement faible* », écrivent les chercheurs de Kaspersky dans un billet de blog. [lire la suite]

3) Que dit cette affaire du groupe Equation ?

Le nom de ce groupe, choisi en raison de sa prédilection pour les techniques de chiffrement de haut vol, a été donné début 2015 par Kaspersky à un groupe de hackers, que l'éditeur russe décrivait alors comme le plus techniquement doué qu'il ait jamais identifié. La société parlait alors « *d'une menace qui dépasse tout ce qui est connu en termes de complexité et de sophistication des techniques employées, une menace active depuis au moins deux décennies* ». Equation exploitait depuis 2008 des failles zero day qui ne seront mises à jour que plus tard, à l'occasion du piratage du nucléaire iranien par Stuxnet. [lire la suite]

4) Que renferme l'archive des Shadow Brokers ?



Plusieurs chercheurs en sécurité se sont déjà penchés sur le cyber-arsenal mis à disposition par les Shadow Brokers (lire notamment l'analyse de Mustafa Al-Bassam ou la synthèse réalisée par *Softpedia*). On y trouve des *exploits*, autrement dit des codes d'exploitation permettant de prendre le contrôle ou d'espionner des pare-feu ou passerelles VPN fournis par de grands constructeurs comme Cisco, Juniper ou Fortinet. Des constructeurs qui ont déjà reconnu que les outils mis en ligne menaçaient bien certains de leurs matériels. Mais, dans tous les cas, il s'agit de générations anciennes de machines. Les appliances Cisco Pix, ciblées par plusieurs outils, ne sont par exemple plus supportées par le constructeur depuis 2009. [lire la suite]

5) L'archive a-t-elle livrée tous ses secrets ?

Et il y a aussi les outils dont la vocation ne se limite pas à cibler une gamme de machines en particulier. *The Intercept* explique ainsi que des éléments d'une architecture exploitée par la NSA pour mettre en place des attaques de type Man-in-the-Middle, autorisant l'interception de requêtes Web, figurent dans l'archive des Shadow Brokers.Sans risque de se tromper, la réponse est non. « *Comme il y a 300 Mo de code, de documentations, de binaires, personne n'a publié d'analyse complète* », remarquent Hervé Schauer et Christophe Renard.[lire la suite]

6) Quels sont les risques pour les entreprises ?

Voir de tels outils mis à la disposition de cybercriminels est évidemment inquiétant. « *On est ici face à des outils d'attaque de haut niveau, mis librement à disposition sur le Web*, explique Gérôme Billois. *Les entreprises doivent donc être très attentives, effectuer l'inventaire des matériels exposés sur leur parc et apporter les modifications nécessaires pour protéger leurs infrastructures. Heureusement, les exploits mis au jour sont assez anciens et ciblent donc du matériel âgé. Mais certaines machines peuvent toujours être en exploitation.* » Au fur et à mesure que les codes de l'archive des Shadow Brokers seront décortiqués, des correctifs et des indicateurs de compromission vont être publiés. Ce qui permettra aux RSSI de contrer la menace. C'est donc plutôt une course de fond qui s'engage. [lire la suite]

7) Qui a fait le coup ?

La liste des suspects s'est très vite limitée à quelques noms. Très rapidement, Nicolas Weaver, de l'université de Berkeley, pointe la Chine, soupçonnée de nombreux actes de cyber-espionnage contre les intérêts américains, et la Russie. Une seconde hypothèse que défend lui aussi Edward Snowden, précisément réfugié en Russie après avoir été à l'origine de la plus importante fuite de données de l'histoire de la NSA. [lire la suite]

8) Un second lanceur d'alertes à la NSA ?

Car une autre hypothèse a également de nombreux partisans : celle de l'implication d'un 'insider', un nouveau lanceur d'alerte à la NSA. Plusieurs éléments viennent étayer cette hypothèse. Primo, l'archive en question renferme différentes versions d'un même outil, des manuels d'utilisation ou des fichiers à vocation interne. Ce qui cadre mal avec l'hypothèse d'un serveur d'attaque, ou d'un serveur de pré-production, qui aurait été compromis par un assaillant externe. [lire la suite]

9) Quelles sont les conséquences possibles ?

D'ores et déjà, la fuite a dû déclencher un branle-bas de combat au sein de la NSA, qui doit chercher l'origine de cette encombrante archive et, surtout, comment mettre fin aux révélations successives sur ses activités offensives. L'agence devra également s'assurer qu'elle n'exploite plus les codes révélés au public pour ses opérations actuelles. Car, très rapidement, les outils de sécurité seront en mesure de détecter les signatures des outils révélés par les Shadow Brokers.[lire la suite]

10) Qu'en pense Bernard Cazeneuve ?

Passée la boutade, le ministre de l'Intérieur français, qui entend prendre la tête d'une initiative internationale permettant d'encadrer le chiffrement, a devant les yeux une autre illustration des limites que pointent de nombreux spécialistes, y compris le Conseil national du numérique (CNNum).Après l'affaire Juniper (le constructeur avait employé un algorithme de chiffrement affaibli par la NSA, qui avait été détourné par un acteur inconnu), les révélations des Shadow Brokers illustrent une fois encore le caractère spécifique des armes cyber.[lire la suite]

Article original de Reynald Fléchaux

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 : Cyberespionnage : 10 questions pour comprendre l’affaire Shadow Brokers

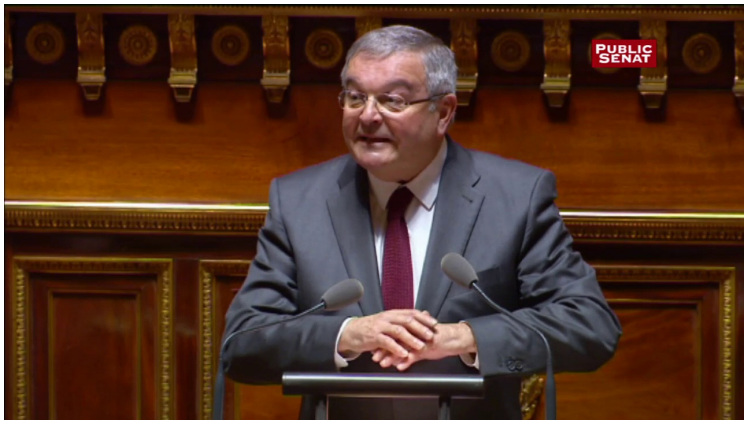
Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Mercredi, le Sénat examinera le projet de loi de prorogation de l'état d'urgence, et discutera à cette occasion d'un amendement qui vise à donner à la police le pouvoir d'obtenir en temps réel les données de connexion de tout suspect de terrorisme, sans aucun contrôle même administratif.

Au nom du comité de suivi de l'état d'urgence dont il est le rapporteur spécial, le sénateur Michel Mercier (UDI-UC) a présenté mardi la substance des amendements qu'il entend présenter devant la commission des lois ce mercredi, pour compléter le projet de loi de prorogation de l'état d'urgence déposé par le gouvernement. Ces amendements ont de fortes chances d'être adoptés par la majorité de droite du Sénat.

Parmi eux, M. Mercier explique qu'un « *amendement aura pour objet de remédier aux rigidités et lourdeurs dans la mise en œuvre de la technique de recueil de renseignements, créée par la loi du 24 juillet 2015, permettant de recueillir en temps réel, sur les réseaux des opérateurs de communications électroniques, les données de connexion relatives à une personne préalablement identifiée comme présentant une menace terroriste* ».



Il s'agit de la procédure créée par la loi Renseignement et codifiée à l'article L851-2 du code de la sécurité intérieure, qui permet « *pour les seuls besoins de la prévention du terrorisme* » d'autoriser « *le recueil en temps réel* » des « *informations ou documents* » détenus par les opérateurs télécoms et les hébergeurs « *relatifs à une personne préalablement identifiée comme présentant une menace* ».

C'EST CE CADRE POURTANT DÉJÀ CRITIQUÉ PAR LES DÉFENSEURS DES DROITS FONDAMENTAUX QUE MICHEL MERCIER ESTIME CONSTITUER DES « RIGIDITÉS ET LOURDEURS »

Même s'il y a débat juridique pour savoir jusqu'où vont ces « informations ou documents », et s'ils vont jusqu'au contenu-même des communications (en principe non), il s'agit au minimum de l'ensemble des données de connexion : adresses IP, numéros de téléphones composés, durées et heures des appels, géolocalisation du téléphone mobile, nombre de SMS échangés, avec qui, de quelle longueur, etc. Potentiellement ce sont donc des données très intrusives dans la vie privée des individus, qui permettent de renseigner sur les habitudes, les déplacements et les contacts.

Actuellement, pour avoir accès en temps réel à ces données, les services de renseignement doivent obligatoirement ***obtenir au préalable une autorisation du Premier ministre****, elle-même délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'avis de la CNCTR doit intervenir dans les 24 heures ou pour les cas les plus complexes, dans les 72 heures. Mais en cas « d'urgence absolue », il est même* ***possible de se passer de l'avis de la CNCTR****.*

Or c'est ce cadre pourtant déjà critiqué par les défenseurs des droits fondamentaux (en raison de l'absence de contrôle d'un juge indépendant) que Michel Mercier estime constituer des « rigidités et lourdeurs » qu'il faudrait supprimer en cas d'état d'urgence.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : open bar pour la police sur les données de connexion ? – Politique – Numerama

---

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.

Combien y a-t-il d'attaques par rançongiciel en France ?
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
Avez-vous quand même une idée de l'évolution du phénomène ?
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
Les victimes ont-elles le réflexe de porter plainte ?
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
Qu'est-ce qui pousse à porter plainte ?
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
Qui sont les victimes ?
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
Quel est votre rôle dans la lutte contre les rançongiciels ?
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
Quel rapport entretenez-vous avec les entreprises ?
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
Parvenez-vous, dans vos enquêtes, à identifier les responsables ?
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
Parvenez-vous à collaborer avec vos homologues à l'étranger ?
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

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.

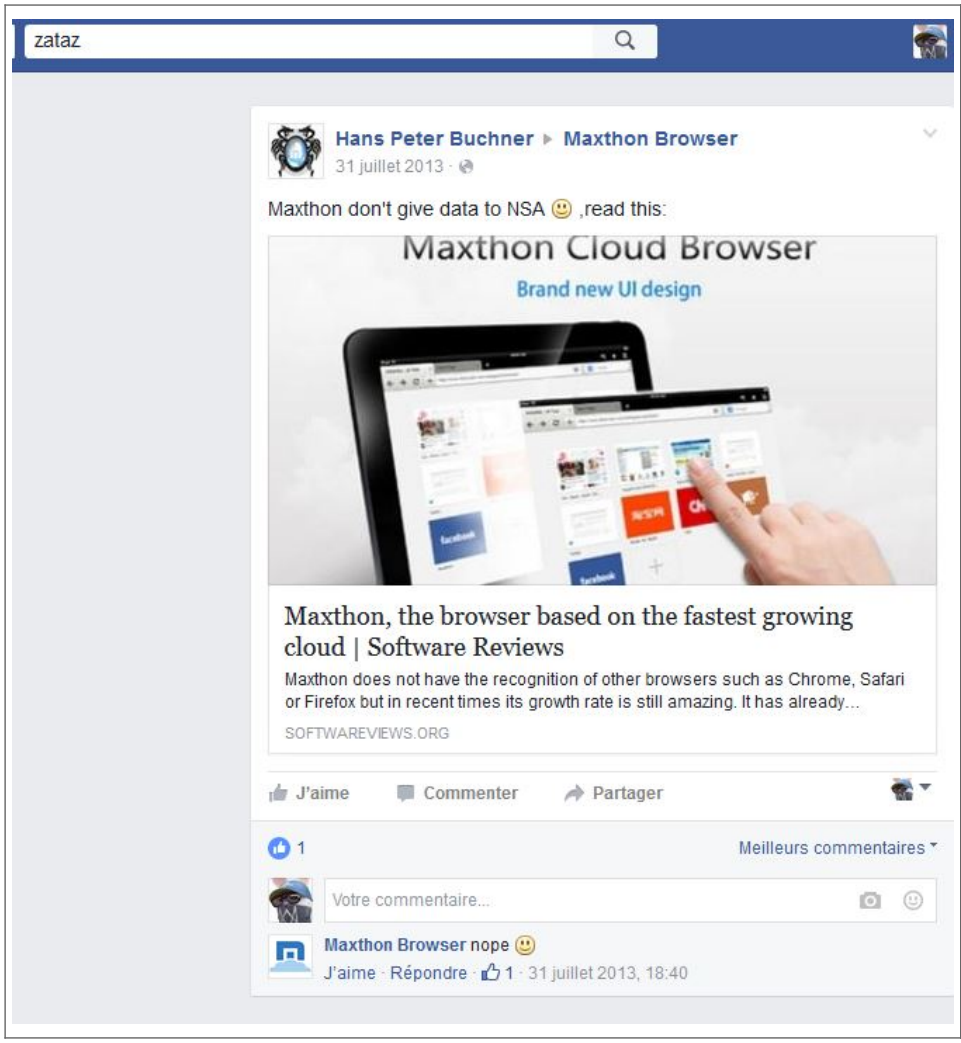
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Attention, le navigateur Maxhton espionne ses utilisateurs !



Attention, le navigateur Maxhton espionne ses utilisateurs !

Le navigateur Maxhton ne serait rien d'autre qu'un outil d'espionnage à la solde de la Chine ?

Des experts en sécurité informatiques de l'entreprise polonaise Exatel viennent de révéler la découverte de faits troublant visant le navigateur *Maxhton*. Ce butineur web recueille des informations sensibles appartenant à ses utilisateurs. Des informations qui sont ensuite envoyées à un serveur basé en Chine. Les chercheurs avertissent que les données récoltées pourraient être très précieuses pour des malveillants.

Les données des utilisateurs de Maxhton envoyées en Chine !
Et pour cause ! Les ingénieurs de *Fidelis Cybersecurity* et *Exatel* ont découvert que Maxthon communiquait régulièrement un fichier nommé ueipdata.zip. Le dossier compressé est envoyé en Chine, sur un serveur basé à Beijing, via HTTP. Une analyse plus poussée a révélé que ueipdata.zip contient un fichier crypté nommé dat.txt. Dat.txt stocke des données sur le système d'exploitation, le CPU, le statut ad blocker, l'URL utilisé dans la page d'accueil, les sites web visités par l'utilisateur (y compris les recherches en ligne), et les applications installées et leur numéro de version.
En 2013, après la révélation du cyber espionnage de masse de la NSA, Maxhton se vantait de mettre l'accent sur la vie privée, la sécurité, et l'utilisation d'un cryptage fort pour protéger ses utilisateurs. (Merci à I.Poireau)
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Le navigateur Maxhton espionne ses utilisateurs – ZATAZ

Panorama des menaces sur la cybersécurité industrielle

Panorama des menaces sur la cybersécurité industrielle

Le nombre de vulnérabilités dans les composants de supervision industrielle ne cesse d'augmenter.
Vu l'augmentation de l'attention portée à la sécurité de la supervision industrielle au fil des dernières années, de plus en plus d'informations sur les vulnérabilités qui touchent ces systèmes sont publiées. Toutefois, ces vulnérabilités peuvent très bien avoir été présentes dans ces produits pendant des années avant d'être dévoilées. C'est un total de 189 vulnérabilités dans des composants de supervision industrielle qui a été publié en 2015 et la majorité d'entre elles était critique (49 %) ou de gravité moyenne (42 %).

Vulnérabilités de supervision industrielle par année.

Les vulnérabilités peuvent être exploitées.
Il existait des codes d'exploitation pour 26 des vulnérabilités publiées en 2015. De plus, pour bon nombre de vulnérabilités (comme les identifiants codés en dur), un code d'exploitation n'est absolument pas requis pour obtenir un accès non autorisé au système vulnérable. Qui plus est, nos projets d'évaluation de la sécurité de la supervision industrielle montrent que les propriétaires de solutions de supervision industrielle considèrent souvent celles-ci comme une « boîte noire », ce qui signifie que les identifiants par défaut des composants de supervision industrielle restent souvent inchangés et peuvent être utilisés pour obtenir un contrôle à distance du système. Le projet SCADAPASS de l'équipe SCADA Strangelove fournit une représentation des identifiants par défaut de supervision industrielle connus. Le projet dispose actuellement d'informations sur 134 composants de supervision industrielle de 50 éditeurs.

Vulnérabilités dans la supervision industrielle en 2015 par niveau de risque (CVSS v.2 et CVSS v.3)

Les vulnérabilités dans les composants de supervision industrielle sont très diverses.
De nouvelles vulnérabilités ont été détectées en 2015 dans les composants de supervision industrielle de différents éditeurs (55 fabricants différents) et types (interface homme-machine, dispositifs électriques, SCADA, périphériques de réseau industriel, automates programmables industriels, et bien d'autres). Le plus grand nombre de vulnérabilités a été détecté chez Siemens, Schneider Electric et Hospira Devices. Les vulnérabilités dans les composants de supervision industrielle sont de nature différente. Les types les plus répandus sont les débordements de tampon (9 % de l'ensemble des vulnérabilités détectées), utilisation des identifiants codés en dur (7 %) et le cross-site scripting (7 %).

Toutes les vulnérabilités découvertes en 2015 n'ont pas été éliminées.
Il existe des correctifs et de nouveaux micrologiciels pour 85 % des vulnérabilités publiées. Les 15 % restants n'ont pas été réparés ou n'ont été que partiellement réparés pour différentes raisons. La majorité des vulnérabilités qui n'ont pas été éliminées (14 sur 19) présente un risque élevé. Ces vulnérabilités sans correctif représentent un risque significatif pour les propriétaires des systèmes concernés, surtout pour ceux chez qui les systèmes de supervision industrielle vulnérables sont exposés à Internet en raison d'une gestion inadéquate de la configuration réseau. A titre d'exemple, citons 11 904 interfaces SMA Solar Sunny WebBox accessibles à distance qui pourraient être compromises via les mots de passe codés en dur. Bien que ce nombre a considérablement diminué pour Sunny WebBox depuis 2014 (à l'époque, plus de 80 000 composants disponibles avaient été identifiés), il est toujours élevé et le problème des identifiants codés en dur (publié en 2015) qui n'a pas été résolu expose ces systèmes à un risque bien plus élevé qu'on ne le pensait jusqu'à présent.

Application de correctif dans les systèmes de supervision industrielle

De nombreux composants de supervision industrielle sont disponibles via Internet.
220 668 composants de supervision industrielle ont été découverts via le moteur de recherche Shodan. Ils sont installés sur 188 019 hôtes dans 170 pays. La majorité des hôtes accessibles à distance et dotés de composants de supervision industrielle est située aux Etats-Unis (30,5 %) et en Europe. Parmi les pays européens, l'Allemagne arrive en première position (13,9 %), suivie de l'Espagne (5,9 %). Les systèmes disponibles proviennent de 133 éditeurs différents. Les plus répandus sont Tridium (11,1 %), Sierra Wireless (8,1 %) et Beck IPC (6,7 %).

Top 20 des pays par disponibilité de composants de supervision industrielle

Les composants de supervision industrielle accessibles à distance utilisent souvent des protocoles qui ne sont pas sécurisés.
Il existe un certain nombre de protocoles, ouverts et non sécurisés par nature, comme HTTP, Niagara Fox, Telnet, EtherNet/IP, Modbus, BACnet, FTP, Omron FINS, Siemens S7 et de nombreux autres. Ils sont utilisés sur 172 338 hôtes différents, soit 91,6 % de l'ensemble des périphériques de supervision industrielle accessibles depuis l'extérieur trouvés. Les attaquants disposent ainsi de méthodes complémentaires pour compromettre les dispositifs via des attaques de type « homme au milieu ».

Top 15 des protocoles des composants de supervision industrielle accessibles depuis l'extérieur

De nombreux composants de supervision industrielle vulnérables sont accessibles depuis l'extérieur.
Nous avons répertorié 13 033 vulnérabilités sur 11 882 hôtes (soit 6,3 % de l'ensemble des hôtes dotés de composants accessibles depuis l'extérieur). Les vulnérabilités les plus répandues sont Sunny WebBox Hard-Coded Credentials (CVE-2015-3964) et les vulnérabilités critiques CVE-2015-1015 et CVE-2015-0987 dans Omron CJ2M PLC. Si nous combinons ces résultats aux statistiques d'utilisation de protocoles non sécurisés, nous pouvons estimer le nombre total d'hôtes de supervision industrielle vulnérables à 172 982 (92 %).

Top 5 des vulnérabilités dans les composants de supervision industrielle

Plusieurs secteurs sont touchés.
Nous avons découvert au moins 17 042 composants de supervision industrielle sur 13 698 hôtes différents dans 104 pays et probablement présents dans de grandes entreprises. La disponibilité de ces composants sur Internet est probablement associée à des risques élevés. Parmi les propriétaires, nous avons pu identifier 1 433 grandes entreprises, dont certaines appartenant aux secteurs d'activité suivants : électricité, aérospatial, transport (y compris les aéroports), pétrole et gaz, métallurgie, chimie, agriculture, automobile, distribution d'eau, de gaz et d'électricité, agroalimentaire, construction, réservoirs de stockage de liquide, villes intelligentes et éditeurs de solution de supervision industrielle. Des institutions académiques et de recherche, des institutions gouvernementales (y compris la police), des centres médicaux, des organisations financières, des complexes hôteliers, des musées, des bibliothèques, des églises et de nombreuses petites entreprises figurent également parmi les propriétaires de systèmes de supervision industrielle accessibles à distance identifiés. Le nombre d'hôtes de supervision industrielle vulnérables accessibles depuis l'extérieur qui appartiennent probablement à de grandes organisations s'élève à 12 483 (91,1 %) où 453 hôtes (3,3 %), dont des hôtes actifs dans le secteur de l'énergie, des transports, du gaz, de l'ingénierie et de l'industrie et de l'agroalimentaire, contenaient des vulnérabilités critiques.

Disponibilité des systèmes de supervision industrielle par éditeur

Les résultats ci-dessus ne sont que la limite inférieure des estimations. Le nombre réel de composants de supervision industrielle accessibles associés à de gros risques pourrait être bien plus élevé.

Conclusion

En matière de protection, l'isolement des environnements critiques ne peut plus être considéré comme une mesure de contrôle de la sécurité suffisante pour la supervision industrielle. Les exigences des activités économiques au 21e siècle imposent souvent la nécessité d'intégrer la supervision industrielle à des systèmes et des réseaux externes. De plus, les capacités, les motivations et le nombre des auteurs de menaces qui se concentrent sur les systèmes de supervision industrielle augmentent. Depuis les disques durs ou les clés USB infectés jusqu'aux connexions non autorisées depuis des réseaux de supervision industrielle à Internet via des smartphones ou des modems en passant par les kits d'installation infectés obtenus auprès d'un éditeur ou le recrutement d'un initié, toutes ces méthodes sont à la disposition d'individus malintentionnés très qualifiés qui préparent des attaques contre des réseaux de supervision industrielle isolés physiquement et logiquement.
Les propriétaires de systèmes de supervision industrielle doivent être au courant des vulnérabilités et des menaces modernes et exploiter ces informations pour améliorer la sécurité de leur environnement de supervision industrielle. Ici, le soutien actif de l'éditeur joue un rôle crucial dans l'identification et l'élimination rapides des vulnérabilités du système de supervision industrielle ainsi que dans le partage de solutions temporaires qui permettent de protéger les systèmes jusqu'à la publication des correctifs.
Les caractéristiques des systèmes de supervision industrielle, à savoir que leur sécurité sur le plan informatique est étroitement liée à la sécurité physique, reçoivent souvent un traitement contraire au traitement exigé dans de telles conditions. Les petites et moyennes entreprises, ainsi que les particuliers, s'en remettent complètement aux éditeurs lorsqu'il s'agit de la sécurité de l'Internet des objets. Les consommateurs ne s'aventurent pas au-delà des étapes simples décrites dans les manuels. Ils disposent donc de dispositifs prêts à l'emploi et facilement accessibles, mais également vulnérables. Les grandes entreprises, de leur côté, mesurent bien les risques élevés associés à une configuration incorrecte de l'environnement de supervision industrielle. Toutefois, c'est pour cette même raison que les propriétaires des systèmes considèrent souvent les dispositifs de supervision industrielle comme des « boîtes noires » et ont peur de modifier l'environnement, y compris sous la forme d'améliorations de la cybersécurité.
Les résultats de cette recherche nous rappellent une fois de plus que le principe de la « Sécurité par l'obscurité » ne peut être invoqué pour atteindre une protection efficace contre les attaques modernes et que la sûreté des systèmes de supervision industrielle ne doit pas être négligée au profit de la sécurité car dans ce domaine, la sûreté et la sécurité sont étroitement liées.
Article original de Kaspersky

Réagissez à cet article

Original de l’article mis en page : Panorama des menaces sur la cybersécurité industrielle – Securelist

---

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Lors de son déplacement en Israël, une délégation de Matignon a laissé ses portables sans surveillance pendant une réception officielle. Et a relevé des anomalies de fonctionnement sur certains terminaux ensuite, assure l'Express.

Manuel Valls s'est-il fait pirater son smartphone lors de son déplacement en Israël, fin mai dernier ? C'est la question que posent nos confrères de l'Express. Lors de son déplacement qui avait pour ambition de relancer le processus de paix avec la Palestine, le Premier ministre, qui se présente volontiers comme « l'ami d'Israël » et la délégation l'accompagnant ont été priés de laisser leurs téléphones portables à l'accueil avant d'être reçu en haut lieu. Demande à laquelle ils auraient accédé, laissant leurs terminaux sans surveillance pendant l'entretien.
Problème : quand ils ont récupéré leurs terminaux pourtant sécurisés, certains présentaient des « anomalies », selon l'Express. Des dysfonctionnements qui peuvent laisser suspecter une tentative d'intrusion de la part des services secrets israéliens. L'Express ne précise pas le ou les modèles des terminaux concernés par ces tentatives d'espionnage supposées.

Pas d'espionnage entre alliés. Sans blague ?
Depuis, les téléphones en question ont été remis à l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui mène l'enquête. Interrogée par nos confrères, celle-ci s'est toutefois refusée à tout commentaire. De son côté, Matignon reconnaît qu'un terminal est bien tombé en panne durant la visite du Premier ministre en Israël. Et indique à nos confrères qu'un allié n'espionne jamais ses amis. Défense de rire.
Rappelons que, pour les échanges les plus sensibles, les officiels français disposent de terminaux Teorem, fournis par Thales et habilités confidentiel-défense. Ceux-ci se révèlent toutefois peu pratiques d'usage, si bien que les ministres utilisent souvent des smartphones du commerce, durcis avec des technologies de sécurité complémentaires. Récemment, l'Elysée s'est ainsi équipé de smartphones Hoox, conçus par Bull. Ces machines, des smartphones Android bénéficiant d'une surcouche logicielle de sécurisation, sont vouées aux échanges de type « diffusion restreinte », un niveau de classification de l'information moins exigeant que le confidentiel-défense.
Article original de Reynald Fleychaux

Réagissez à cet article

Original de l’article mis en page : Le portable de Manuel Valls a-t-il été piraté par Israël ?

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