Conséquences innatendues des cyberattaques

Conséquences innatendues des cyberattaques

Les dégâts informatiques de premier jour ne constituent pas la seule conséquence d'une cyberattaque pour une entreprise. Il y a aussi la réduction en nombre des clients, déçus notamment du vol ou de la perte de leurs données. Certains peuvent même penser à poursuivre l'entreprise en justice. L'après est ainsi encore plus dure à gérer pour les dirigeants et les responsables informatiques.

Impact sur la confiance des consommateurs

La préparation d'une cyberattaque peut prendre plusieurs semaines, voire des mois. Par conséquent, leurs effets vont bien au-delà des « simples » dégâts informatiques. Une étude internationale réalisée par VansonBourne et publiée le 12 mai dernier le confirme, en insistant sur des atteintes sur la performance commerciale de la société victime. Elle révèle en effet que la confiance des consommateurs vis-à-vis de cette dernière s'amenuise après les attaques. Logique quand on sait que bon nombre de clients de TV5 Monde et Orange ont encore du mal à oublier les attaques respectives d'avril 2015 et de 2014 ayant entraîné une fuite de données. Cette étude avance même que 34% des Français voient leur loyauté envers une marque ayant laissé fuiter leurs données, diminuée. Les efforts de cybersécurité devront ainsi se trouver dans le plan de toute entreprise qui se veut être compétitive.
Les consommateurs sont également nombreux à perdre le désir d'acheter auprès d'une entreprise victime d'une attaque informatique. Plus de trois sur quatre ont même affirmé qu'ils iraient jusqu'à arrêter l'achat de produits ou services chez cette dernière, notamment si la vulnérabilité exploitée provient de l'erreur de l'équipe dirigeante. Pour une erreur humaine d'un subordonné, les clients sont plus compréhensifs. La publication de cette étude confirme par ailleurs que la sécurité des données figure depuis quelques années parmi les critères les plus considérés par les Français avant une décision d'acheter. Ce paramètre a été pris en compte par 61% des Français en 2015, contre 53% en 2014.

Risques de poursuite en justice

La perte de chiffre d'affaires est donc quasiment incontournable pour toute entreprise qui vient de faire l'objet d'une attaque informatique d'ampleur. Elle est toutefois moins grave par rapport à un autre risque, celui de la poursuite en justice. Cette étude a en effet permis de connaître que 50% des Français sont prêts à poursuivre en justice les entreprises attaquées pour négligence ou inattention apportée à la protection de leurs données personnelles. Target et Sony Picture en ont déjà payé le prix, trouvant même, parmi les auteurs de ces poursuites, leurs propres salariés. Face à ce risque, certaines entreprises envisagent de garder secrètes toutes les attaques atteignant leur système d'information. Serait-ce une bonne initiative de leur part ? La réponse est non. A l'heure d'Internet, la moindre information peut se trouver à la portée de tout le monde. Une éventuelle fuite pourrait ainsi écorner définitivement l'image d'une société choisissant une telle démarche. Au contraire, cette société devrait plutôt informer le plus rapidement ses clients, pour faire preuve de transparence. Cette démarche sera par ailleurs rendue obligatoire par le règlement européen sur la protection des données, un texte dont la mise en vigueur est prévue en mai 2018.

Article original de sekurigi.com complété par Denis JACOPINI

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.

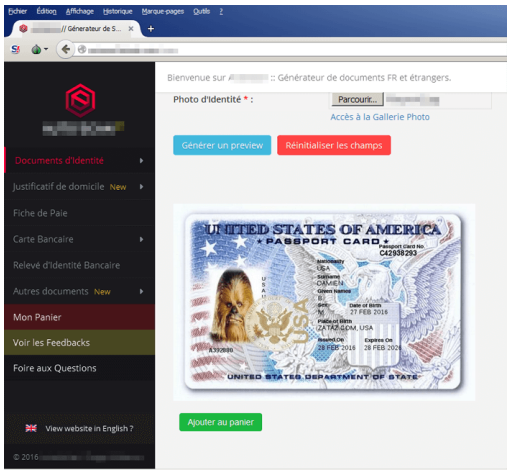
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

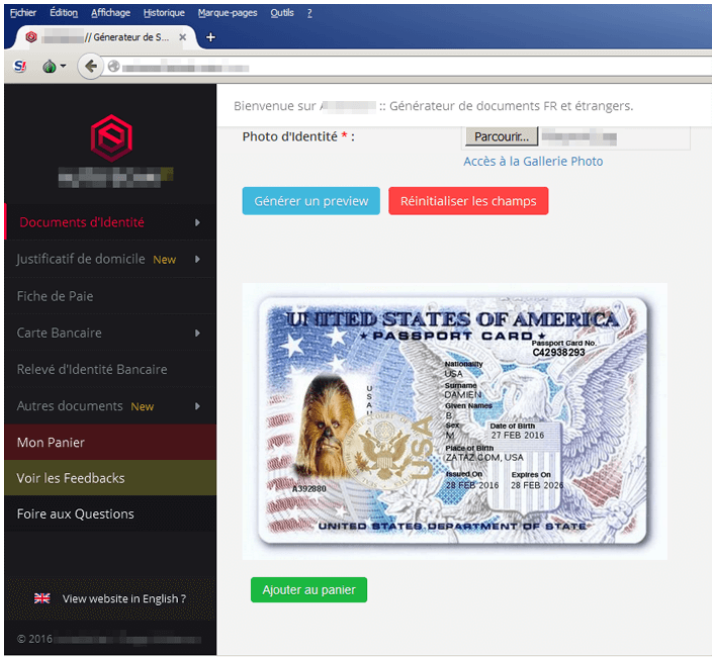
Original de l'article mis en page : Les traces laissées par les cyberattaques – @Sekurigi

Le Darknet cache un générateur de faux documents



Le Darknet cache un générateur de faux documents

Vous cherchez de faux documents comme un diplôme du baccalauréat, de BTS ? Une fausse facture FREE, EDF, Direct Énergie ? Un faux permis de conduire ? Une fausse fiche de paie ou une fausse carte bancaire ? Un site Internet vous propose d'automatiser l'usurpation.



Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. Leur site, pas la peine de me réclamer l'adresse, est caché sous une adresse .onion. A.S. profite de l'anonymat proposé par le service TOR pour éviter d'afficher ouvertement son serveur, son ip d'origine. Et même si vous mettiez la main sur ce dernier, l'hébergement est hors de l'hexagone.

« ***Bienvenue sur A'S. :: Générateur de documents FR et étrangers*** » souligne l'introduction affichée par le site. Mission de ce dernier, pour quelques euros, facturés en Bitcoins, générer de fausses factures, fausses fiches de paie, faux relevé d'identité bancaire (RIB). Il est possible de générer un faux diplôme du Baccalauréat, de BTS, d'IUT. Une fausse carte vitale ? Pas de problème. Une facture d'un achat effectuée chez Darty, ok. Passeport Français, Américain et autres copies d'une carte nationale d'identité boucles ce service… qui n'a rien d'illégal, du moins si vous rentrez vos propres coordonnées. Il en va tout autrement si les informations que vous fournissez permettent d'usurper une identité, une fonction, un titre via ses faux documents. La loi punit de trois ans d'emprisonnement et de 45000 euros d'amende le faux et l'usage de faux documents.

Les prix varient de 4,99€ pour une copie de passeport, une facture. 9,99€ pour le scan d'un bulletin de fiche de paie. 6,99€ pour la copie d'un diplôme du baccalauréat général. Les auteurs de ce business proposent même un abonnement à vie. Pour ~~79 800~~ euros, les commerciaux indiquent permettre « ***un accès illimité et à vie à tous les articles de cet Autoshop pour 200€ ~~BTC~~***« . La boutique annonce un anonymat garanti. [Correction : selon les auteurs, il s'agit de 200€ et non 200 BT comme il était écrit sur leur site, NDR]… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Générateurs de faux documents – ZATAZ*

Des complices de cyberescrocs arrêtés en Côte d’Ivoire

	**Des complices de cyberescrocs arrêtés en Côte d’Ivoire**

Utilisation frauduleuse d'éléments d'identification de personne physique, tentative d'escroquerie et complicité d'escroquerie sur internet. Accusés de tous ces crimes, Traoré Issouf, 28 ans, et Kouadio Konan Daniel, 27 ans, tous deux caissiers dans une agence de transfert d'argent nouvellement ouverte, séjournent à la Maison d'arrêt et de correction d'Abidjan (Maca), dans l'attente d'un procès.

Comme l'explique la Plateforme de lutte contre la cybercriminalité (PLCC), ces deux individus ont été arrêtés le 20 juin 2016 par ses agents. Ils sont suspectés d'avoir effectué des transferts frauduleux au profit de quelques cyberescrocs, qui recourent bien souvent à des employés de maisons de transfert d'argent pour encaisser leur butin.
Pour chaque transfert effectué, Kouadio Konan Daniel a avoué avoir perçu une commission de 10%. Mais pouvaient-ils vraiment nier les faits? Après analyse des éléments en leur possession, le Laboratoire de criminalistique numérique (LCN) de la Direction de l'informatique et des traces technologiques (DITT) a pu extraire de nombreux codes de transfert d'argent envoyés par téléphone portable.
Article original de Anselme Akéko – CIO-Mag Abidjan

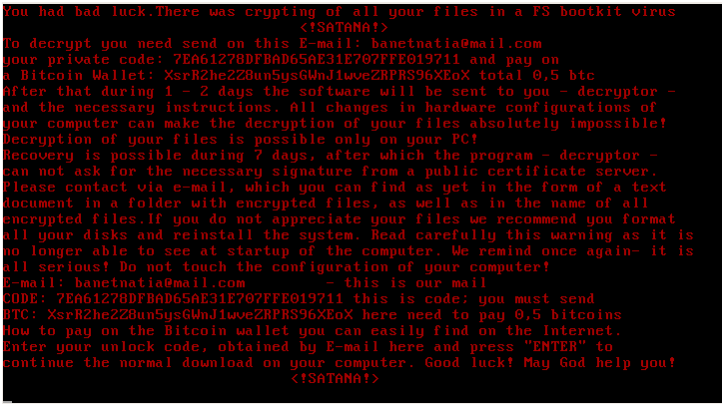
Réagissez à cet article

Original de l'article mis en page : Transfert d'argent : des complices de cyberescrocs arrêtés en Côte d'Ivoire | CIO MAG

Satana, un ransomware pire que Petya

Satana, un ransomware pire que Petya

Le nouveau rançomware Satana cumule chiffrement des fichiers et remplacement du secteur d'amorçage du disque.



Une nouvelle génération de ransomware est en train d'émerger. Satana, nom du nouveau malware, combine chiffrement des fichiers et écriture de code sur le secteur d'amorçage du disque, le MBR. Deux techniques inspirées de Petya et Mischa, note Malewarebytes qui constate la croissance du nouvel agent satanique ces dernières semaines.

« *Satana fonctionne en deux modes*, note la société de sécurité sur son blog. *Le premier se comporte comme Petya, un fichier exécutable (sous Windows, NDLR) [et] écrit au début du disque infecté un module de bas niveau, un bootloader avec un noyau personnalisé. Le deuxième mode se comporte comme un ransomware typique et chiffre les fichiers un par un (tout comme Mischa).* » Mais à la différence que les deux modes ne sont pas exploités alternativement mais bien appliqués ensemble, l'un après l'autre, pour s'attaquer à leurs victimes.

Payer ne garantit rien chez Satana

Malwarebytes ne le précise pas mais le mode de propagation de Satana reste probablement classique. A savoir par e-mail (et éventuellement d'un expéditeur en recherche de travail avec des liens vers les fichiers infectieux comme dans le cas de la première version de Petya). Une fois le MBR remplacé, le malware s'attaque au chiffrement des fichiers du disque (et des éventuels volumes reliés à l'ordinateur) et attend patiemment que le système soit redémarré. Quand c'est le cas, un message s'affiche sur l'écran expliquant la démarche à suivre pour récupérer l'accès à son PC, à savoir le paiement d'une rançon de 0,5 bitcoin (plus de 300 euros au cours du jour).

Si l'utilisateur parvient néanmoins à remplacer le MBR par un fichier d'amorçage sain (une manipulation manuelle qui est loin d'être à la portée de tout le monde), il se heurtera aux fichiers chiffrés sur le disque. Lesquels ont été renommés avec, en en-tête du nom, un e-mail aléatoirement choisi parmi ceux de l'équipe des développeurs de Satana, selon l'expert en sécurité (Gricakova@techmail.com, dans l'exemple présenté). Et les méthodes de chiffrement semblent suffisamment avancées pour rendre les fichiers piégés définitivement irrécupérables. D'autant que Malewarebytes pointe un bug pour le moins problématique pour la victime. De par le mécanisme de chiffrement/déchiffrement des fichiers, en cas de déconnexion au serveur de commandes et contrôle (C&C), la clé de décryptage (qui est la même que pour le cryptage) est perdue. Brisant tout espoir de la victime à pouvoir récupérer ses données (sauf à avoir fait préalablement des sauvegardes). « *Même les victimes qui paient peuvent ne pas récupérer leurs fichiers si elles (ou le C&C) sont hors ligne lorsque le chiffrement arrive* », prévient la société de sécurité.

Du code en cours de perfectionnement

Ce n'est pas la seule bizarrerie que remarque le chercheur Hasherezade, auteur du billet. Il constate également que, le ransomware affiche toute la procédure de son déploiement, y compris la progression du chiffrement des fichiers. « *Habituellement les auteurs de logiciels malveillants ne veulent pas laisser le code de débogage dans leur produit final* », écrit le chercheur. Lequel conclut que Satana est probablement encore en cours de développement et contient des failles. « *Le code d'attaque de bas niveau semble inachevée – mais les auteurs montrent un intérêt dans le développement du produit dans ce sens et nous pouvons nous attendre que la prochaine version sera améliorée.* » Une nouvelle génération de rançongiciel est bien en marche.

Article original de Christophe Lagane

Réagissez à cet article

Original de l’article mis en page : Satana, un ransomware pire que Petya

---

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.

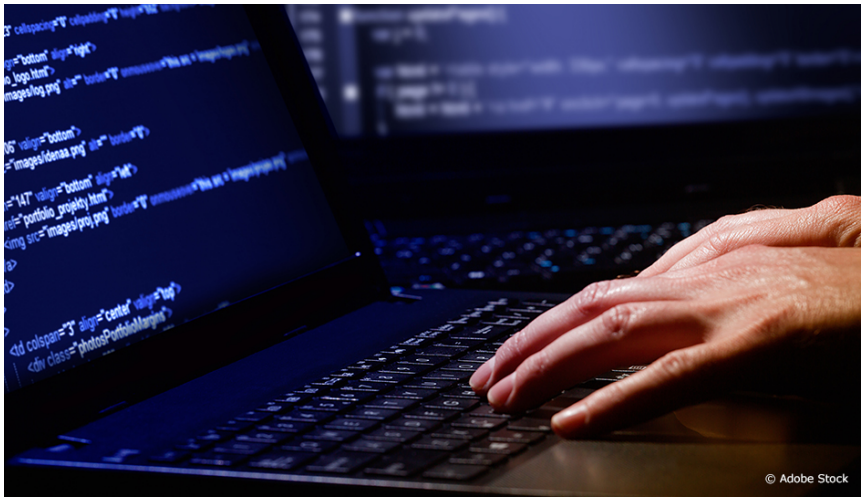
QUE FAIRE?
Pour se prémunir contre ces menaces, l'ACFM suggère à ses membres de se doter d'un cadre de cybersécurité, adapté à la taille de leur cabinet, en cinq étapes :
1. Identifier les biens qui doivent être protégés, de même que les menaces et les risques à leur égard;
2. Protéger ces biens à l'aide 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

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.

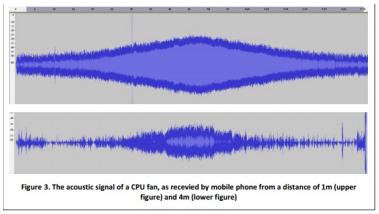


Figure 3. The acoustic signal of a CPU fan, as recevied by mobile phone from a distance of 1m (upper figure) and 4m (lower figure)

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

Des caméras de surveillance piratées pour mener des attaques DDoS

Des caméras de surveillance piratées pour mener des attaques DDoS

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

Des caméras de surveillance piratées pour former un botnet

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

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

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

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

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

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

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

Affaire à suivre…

Article original de Jérôme DAJOUX

Réagissez à cet article

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