Le Canada adhère à la Convention de Budapest – Conseil de l’Europe | Le Net Expert Informatique

Le Canada adhère à la Convention de Budapest – Conseil de l’Europe

L’Observateur permanent du Canada au Conseil de l’Europe, Alan Bowman, a déposé ce matin l’instrument de ratification de la Convention de Budapest sur la cybercriminalité.
Ainsi, le nombre de Parties atteint 47. Sept autres États ont signé la Convention et douze autres pays ont été invités à y adhérer. Actuellement, 66 États sont des Parties ou se sont officiellement engagés à devenir Parties à ce traité.

Liste des signatures, ratifications et adhésions à la Convention de Budapest

---

Source : http://www.coe.int/fr/web/cybercrime/-/canada-joins-budapest-convention

Cybercriminalité : 80 interpellations enregistrées au premier trimestre 2015 en Côte d'Ivoire – Abidjan.net | Le Net Expert Informatique

	Cybercriminalité : 80 interpellations enregistrées au premier trimestre 2015 en Côte d'Ivoire

Quatre-vingts personnes soupçonnées de cybercriminalité ont été interpellés au premier trimestre 2015 en Côte d'Ivoire, avec 480 affaires traitées contre 450 affaires traitées et 70 interpellations 2014 dans le pays, a appris l'AIP auprès du directeur de la direction de l'informatique et des traces technologiques (DITT), le commandant Ouattara Guelpetchin.

Le directeur de la DITT, qui a fait cette annonce vendredi à Yamoussoukro, lors d'un colloque international sur la cybercriminalité, a indiqué par ailleurs que 90 % des infractions recensées au monde sont des infractions classiques avec usage des technologies de l'information et de la communication (TIC).

» En 2013, 85% de ces infractions sont commis depuis l'Afrique « , a précisé le commandant Ouattara Guelpetchin.
Initié par l'institut de lutte contre la criminalité économique (ILCE) de la haute école de gestion Arc (HEG Arc) et l'Ecole supérieure de commerce et d'administration des entreprises (ESCAE) de l'institut national polytechnique Houphouët-Boigny de Yamoussoukro, le colloque international a pour thème » l'impact de la cybercriminalité sur la société Ouest-africaine : exemple de la Côte d'Ivoire « .
Les infractions qualifiées « délinquance astucieuse » sur internet ont un impact au plan culturel, social et sur les investissements étrangers. « On évalue le préjudice subi à 1,5 milliards F CFA », a confié lors de sa communication l'étudiant Koné Aboubacar Sidiki de l'INP-HB dans le cadre de ses travaux de recherche .
Le colloque international sur la cybercriminalité, deuxième du genre, rassemble des experts du domaine en provenance de Suisse et de la Côte d'Ivoire, ainsi que les représentants des institutions publiques, des entreprises privées et des établissements d'enseignement supérieur, la presse et société civile.

Source : http://news.abidjan.net/h/559340.html

La Marine Française infectée par Thales ? | Le Net Expert Informatique

La Marine Française infectée par Thales ?

L'affaire du piratage dont a été victime Thales en début d'année rebondit. Selon le Canard Enchaîné, son programme classé-défense SIC21 livré à la Direction Générale de l'Armement et équipant des navires et des installations terrestres, pourrait avoir été infecté.

L'attaque informatique dont a été victime Thales en avril dernier continue de faire couler beaucoup d'encre. Dans un document confidentiel daté du 18 mai évoqué par le Canard Enchaîné, l'entreprise de défense confirme en effet que l'ensemble des postes, serveurs et équipements du groupe aux Etats-Unis ont été infectés en décembre par un virus à partir des serveurs des sites de Thales Avionics à Piscataway, dans le New Jersey, et à Irvine, en Californie, avant de se répandre au Canada et de toucher la messagerie France de Thales en mars dernier. Mais l'histoire ne s'arrête pas là : dans un mail envoyéle 13 mai à Olivier Daloy (directeur du système informatique de Thales), Ivan Maximoff (le spécialiste sécurité informatique maison) aurait fait aussi état de ses inquiétudes concernant la découverte du virus Courch Yeti spécialisé dans l'espionnage industriel, dans le programme classé-défense SIC21 datant de 2004.
Problème : le programme SIC21 équipe aussi des navires et des installations terrestres. « Six livraisons de Thales au centre d'expertise de la Direction Générale de l'Armement dans le domaine de la guerre électronique installé près de Rennes, et à la DGA Techniques navales à Toulon, pourraient avoir été infectées », indique le Canard Enchaîné. Dans un extrait du mail du 13 mai d'Ivan Maximoff repris par le journal satirique, ce dernier fait également mention que des programmes potentiellement indésirables ont été livrés dans le cadre du programme SIC21. Afin de faire le point sur la situation, une réunion aurait eu lieu le 18 mai entre Thales, la DGA mais aussi l'Agence nationale de la Sécurité des Systèmes d'Information pour évoquer la sécurisation du groupe.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.lemondeinformatique.fr/actualites/lire-piratage-de-thales-la-dga-pourrait-avoir-ete-infectee-par-le-virus-courch-yeti-61453.html
Par Dominique Filippone

Les dessous de la société d'espionnage Hacking Team… | Le Net Expert Informatique

Les dessous de la société d'espionnage Hacking Team…

La firme, qui s'est fait voler plus de 400 gigaoctets de données confidentielles, avait présenté ses technologies aux services de renseignements français. La société Hacking Team, soupçonnée d'avoir livré des logiciels d'espionnage à des régimes autoritaires, assure n'avoir rien commis d'illégal.

On soupçonnait Hacking Team de rouler sa bosse pour des dictatures. Et voilà que le journal Le Monde nous apprend que la sulfureuse entreprise d'espionnage a également eu des contacts avec les services d'espionnage français… Lundi 6 juillet, la société italienne a été victime d'un piratage de grande ampleur de ses données confidentielles et des comptes Twitter de plusieurs de ses responsables. Des centaines de gigaoctets de données se sont déversées sur le Web et ont été immédiatement téléchargées et consultées par ceux qui l'accusaient de faire bénéficier de ses technologies des régimes autoritaires.
L'entreprise est en effet spécialisée dans le développement et la commercialisation de logiciels de surveillance ou de piratage très performants, principalement destinés à des États. Logiciels de blocage de pages internet, systèmes de mise sous surveillance de boîtes mails jugées suspectes… Hacking Team a développé une impressionnante gamme de services. Leur produit phare, dénommé RCS (pour Remote Control Systems), est un packaging incluant des logiciels tels que DaVinci et Galileo, qui permettent de visualiser les frappes effectuées sur le clavier de l'ordinateur visé, d'en collecter les informations sensibles telles que les adresses mails, les documents enregistrés ou les mots de passe, ou encore de récupérer les historiques de navigation.

Ennemie d'Internet
La facilité avec laquelle ces outils peuvent être utilisés à des fins d'espionnage de masse avait conduit certaines ONG à dénoncer les pratiques de cette société. Cette dernière avait même fini par être classée parmi les ennemis d'Internet par Reporters sans frontières en 2013, en raison des rapports commerciaux qu'elle entretenait alors avec le Maroc et les Émirats arabes unis. Des traces de ses logiciels avaient ainsi été retrouvées sur les ordinateurs du site d'information marocain Mamfakinch, quelques jours après que ce média a reçu le Breaking Borders Award 2012 remis par Global Voices et Google.
Autre soupçon : « Un expert en sécurité, Morgan Marquis-Boire, a examiné des pièces jointes attachées à un e-mail envoyé à Ahmed Mansoor, un blogueur émirati. Elles étaient contaminées. Il y a trouvé de fortes indications suggérant que la source du cheval de Troie provenait de Hacking Team », écrit également RSF.
L'entreprise jouit dans le milieu d'une réputation douteuse, et est soupçonnée de collaborer avec des pays peu recommandables. Jusqu'à présent, la société clamait son innocence et aucune preuve de son implication dans la mise en place des systèmes de surveillance électronique de ces pays n'avait été découverte. « Nous faisons extrêmement attention à qui nous vendons nos produits. Nos investisseurs ont mis en place un comité légal qui nous conseille continuellement sur le statut de chaque pays avec lequel nous entrons en contact », assurait le PDG de Hacking Team, David Vincenzetti, dans une interview accordée en 2011 au journaliste Ryan Gallagher.

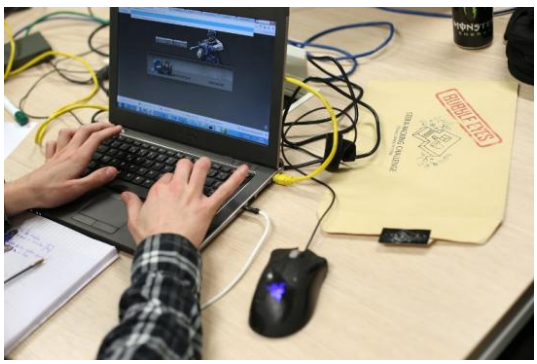
Des régimes autoritaires en clients
Kazakhstan, Arabie saoudite, Azerbaïdjan… De nombreux États – dont les dirigeants ne font pas toujours des libertés individuelles une priorité de leur règne… – font partie de la liste des clients. Parmi ces pays, certains sont connus pour une répression dure de leur population et leurs violations répétées des droits de l'homme. On peut ainsi noter l'exemple du Soudan, avec lequel Hacking Team a toujours nié avoir collaboré. Cependant, les documents publiés révèlent l'existence d'un contrat de 480 000 euros avec le gouvernement actuellement en place. La Russie fait également partie des heureux bénéficiaires des services de Hacking Team. La firme prend même la peine d'indiquer sur ses documents internes que ces deux pays ne sont « officiellement pas clients » (« oficially not supported ») de l'entreprise.
Interrogé au sujet de la série de contrats signés avec le Soudan, le porte-parole de l'entreprise, Éric Rabe, a quant à lui maintenu que le document cité remontait à avant les sanctions décidées par les Nations unies contre le pays.

La France, elle aussi intéressée par les services de l'entreprise
D'après certains documents, la France et Hacking Team seraient entrés en contact plusieurs fois ces dernières années. La prise de contact entre le ministère de la Défense et l'entreprise a eu lieu en 2013, alors qu'une réunion de présentation s'est tenue fin 2014 dans un hôtel près de l'aéroport Charles-de-Gaulle à Paris. Étaient représentés à cette réunion la DGSI et le Groupement interministériel de contrôle (GIC) chargé quant à lui des écoutes administratives (c'est-à-dire menées sans mandat judiciaire), et dirigé par le Premier ministre.
Si la DGSI affirme n'avoir donné aucune suite à cette réunion, ce n'est pas le cas du GIC qui a poursuivi ses échanges avec Hacking Team. Comme le révèle un échange de courriels entre le GIC et Hacking Team, Philippe Vinci, l'un des responsables de l'entreprise, s'est rendu au siège du GIC le vendredi 3 avril 2015. Cette information est confirmée par un échange de courriels entre la société et le groupement interministériel datant du mardi 7 avril. On y apprend également que le GIC serait intéressé par une démonstration de la part d'Hacking Team. L'entreprise aurait alors proposé aux représentants du GIC de venir assister à une telle démonstration en Italie courant mai. Aucune information concernant la suite à donner à ces rendez-vous n'a pour le moment fuité.

« Nous n'avons rien à cacher »
Après deux jours sans réaction, l'entreprise a finalement commenté ce vol de données dans une interview accordée au site IBTimes : « Nous n'avons rien à cacher sur nos activités et nous pensons qu'il n'y a aucune preuve dans ces 400 gigabits de données que nous avons violé une quelconque loi », a ainsi affirmé le porte-parole de l'entreprise, Éric Rabe.
Pour le moment, et en attendant de connaître exactement le contenu des données qui ont été piratées, la société italienne a demandé à ses clients de cesser d'utiliser ses logiciels. Les auteurs du piratage ne se sont pas encore manifestés.

Source : http://www.lepoint.fr/high-tech-internet/les-curieux-clients-de-la-societe-d-espionnage-hacking-team-08-07-2015-1943190_47.php
Par Ian BEAURAIN

Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team | Le Net Expert Informatique



Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team

Les cybercriminels s'en frottent déjà les mains entre deux piratages. Deux jours après la mise en ligne de données piratées de l'éditeur de logiciels espions Hacking Team, les experts, qui ont épluché les 400 Go de documents, ont fait la découverte d'une faille de sécurité importante de Flash Player, un lecteur multimédia autonome utilisé par des sites commes Youtube, Dailymotion ou encore Facebook.

C'est l'éditeur d'antivirus Micro Trend qui a révélé sur son blog cette faille «zero-day», c'est à dire inconnue jusqu'à présent et sans correctif pour l'instant. Elle permet à un attaquant de prendre le contrôle à distance d'un ordinateur en exécutant un code arbitraire à distance ou dans le cas plus précis d'une entreprise de surveillance comme Hacking Team d'installer ses logiciels espions sans se faire remarquer.
Symantec a confirmé cette porte d'entrée dans votre ordinateur et conseille sur son blog (en anglais) de désactiver temporairement Flash Player sur les sites Internet douteux surtout sur Internet Explorer, le navigateur le plus exposé.
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) a lui aussi confirmé la faille et ses potentielles conséquences. Le CERT-FR précise que des «plusieurs kits d'exploitation (de pirates informatiques, NDLR) ont intégré cette vulnérabilité qui est activement exploitée».
Prise à défaut, l'entreprise américaine Adobe, à l'origine de Flash Player, a promis d'apporter un patch correcteur dans la journée de mercredi. D'autres failles de sécurité pourraient être révélées sur la masse de documents qui ont fuité. Mais les plus dangereuses restent celles dont seul un groupe d'initiés est au courant.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.leparisien.fr/high-tech/flash-player-une-faille-de-vulnerabilite-revelee-par-le-piratage-de-hacking-team-08-07-2015-4928849.php
Par Damien Licata Caruso

Comment prémunir les visiteurs de votre site internet de cyberattaques ? | Le Net Expert Informatique

Comment prémunir les visiteurs de votre site internet de cyberattaques?

Switch propose un site web visant à aider les propriétaires de noms de domaines internet en Suisse à protéger leur site web contre des cyber-attaques.

Afin d'aider les propriétaires de sites internet à lutter contre les malwares qui pourraient y être installés, Switch met en ligne Safer Internet, un site internet d'information sur les menaces que représentent les criminels sur internet et les mesures préventives à adopter. Michael Hausding, expert en sécurité de Switch, explique les raisons de la mise en place d'un tel site: «Par la plateforme de sécurité Safer Internet, nous nous adressons à tous les détenteurs d'un site web .ch. Nous y donnons des conseils sur la prévention de l'abus de noms de domaine et informons sur les dangers relatifs à des contenus online.»
Les propriétaires de noms de domaines y trouveront notamment cinq conseils pour prévenir des attaques par Drive-by (qui infectent les usagers d'un site contenant un malware) et par Phishing (qui consistent à obtenir des informations personnelles via notamment des sites contrefaits). Parmi ses conseils se trouvent par exemple le fait d'utiliser une système de gestion du contenu (CMS) toujours à jour.
Ce site est disponible en quatre langues: allemand, français, italien et anglais. Il s'adresse en premier lieu aux gestionnaires de sites web qui sont tenus de nettoyer leur site s'il est infecté au risque de les voir bloqué.
La fondation Switch a pour objectif de rendre internet sûr en Suisse.

Le lien vers le site Internet « Safer Internet » de la société « Switch » : http://www.switch.ch/saferinternet

---

Source : http://www.ictjournal.ch/fr-CH/News/2015/07/07/Comment-premunir-les-visiteurs-de-votre-site-internet-de-cyberattaques.aspx

---

Le responsable des attaques DDoS du Playstation Network et du Xbox Live échappe à 15

ans de prison ! | Le Net Expert Informatique

Le responsable des attaques DDoS du Playstation Network et du Xbox Live échappe à 15 ans de prison !

Vous souvenez-vous de Julius « zeekill » Kivimak ? Le jeune homme de 17 ans est le responsable des attaques DDoS du Playstation Network et du Xbox Live survenues en fin d'année dernière. Il avait témoigné à visage découvert quelques temps après avoir oeuvré puis avait été interpellé par les autorités. Son jugement a eu lieu, et figurez-vous que le bougre a réussi à échapper à 15 ans de prison !

Le jeune Julius « zeekill » Kivimak est le hacker à l'ego surdimensionné qui a pris le risque de se faire repérer par les autorités en accordant une interview plutôt qu'en restant discret. Se revendiquant comme étant membre de Lizard Squad, il avait affirmé être l'auteur des attaques DDoS du Playstation Network et du Xbox Live l'année dernière.
Appréhendé par les autorités finlandaises, il a dû répondre (enfin son avocat) à 50 700 charges qui pesaient contre lui parmi lesquelles on compte la fraude bancaire, l'intrusion dans un système informatique, le harcèlement, la fraude etc.
Mais visiblement la quantité de charges retenues contre lui n'ont pas suffi à le faire condamner. Le jeune homme risquait 15 à 16 ans de prison et s'en est finalement sorti quasiment indemne puisqu'il n'a écopé que de 2 ans de prison avec sursis. En outre le tribunal lui a demander de combattre le cybercrime.
Ce jugement, Blair Strater l'a en travers de la gorge. Car, outre les attaques DDoS, le jeune Julius « zeekill » Kivimaki avait également harcelé pendant trois ans cet américain. Il est allé extrêmement loin puisqu'il a fait intervenir le SWAT (forces d'intervention américaines) chez lui, a usurpé son identité et a plus ou moins détruit sa vie ainsi que celle de sa famille. Le jeune américain de vingt ans a déclaré qu'il était « absolument dégoutté par le jugement ».

L'interview du pirate en question : https://youtu.be/fPX8yCBdIZ8

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.phonandroid.com/responsable-attaques-ddos-playstation-network-xbox-live-echappe-15-ans-prison.html

Menacé de chantage sur Skype, un lycéen se suicide| Le Net Expert Informatique

	Menacé de chantage sur Skype, un lycéen se suicide

Après avoir été menacé par son interlocutrice virtuelle de voir une « vidéo intime » diffusée sur Internet s'il refusait de la payer, un jeune homme s'est donné la mort dans sa chambre.

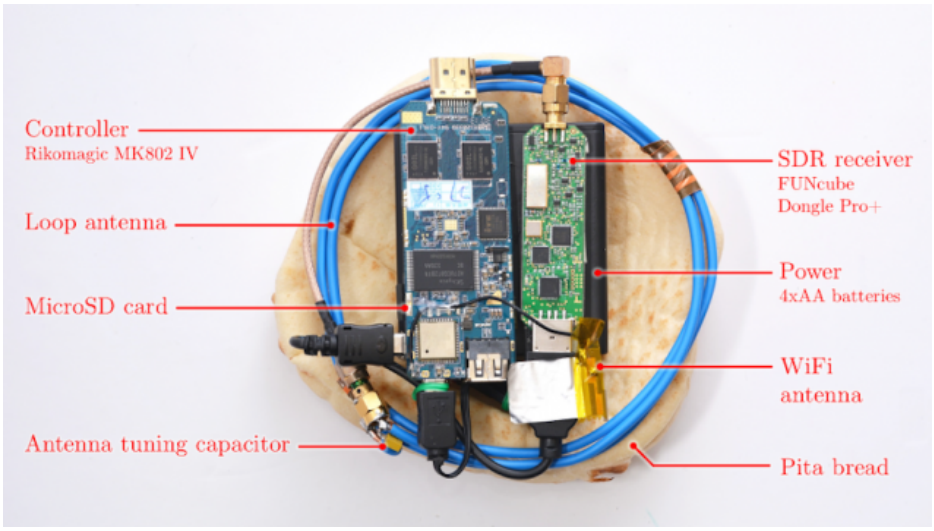
Mercredi 4 juin, un peu avant 20 heures, à Castelsarrasin (Tarn-et-Garonne), un lycéen de 18 ans – qui s'appellerait Quentin – est attendu à la table familiale pour dîner. En l'absence de réponse à leurs appels, ses parents se rendent dans sa chambre. Et le découvrent dans une mare de sang, un couteau planté en plein coeur.
Quentin est déclaré mort peu après l'arrivée des secours. Les policiers qui leur font suite se concentrent sur son ordinateur portable, resté allumé. Ils y découvrent les causes probables de son suicide grâce à la fenêtre de conversation restée ouverte sur sa messagerie vidéo Skype : un chantage à la webcam.

Une jeune femme le menace de diffuser une vidéo intime
Les enquêteurs remontent le fil de la discussion et constatent que Quentin s'était filmé nu pour son interlocutrice. Celle-ci l'avait ensuite menacé de diffuser cet enregistrement sur internet s'il refusait de payer une certaine somme d'argent sur le champ. Pris de panique, Quentin se serait donné la mort pour éviter un scandale.
Le parquet de Montauban a ouvert une enquête préliminaire.
« La Dépêche du midi », qui avait d'abord évoqué l'hypothèse d'un chagrin d'amour avant de retenir celle du chantage, précise que la mère du lycéen l'aurait découvert avec une « corde au cou ». Mais évoque également, comme RTL, une « mare de sang ».
Le jeune homme, décrit comme un « très bon élève » de terminale au lycée professionnel de Beaumont-de-Lomagne, n'avait jamais parlé de suicide à ses proches. Les centres d'intérêt de son probable profil Facebook tournaient essentiellement autour des mangas.

Un scénario similaire à Brest, en 2012
Ce suicide rappelle un drame similaire survenu à Brest en octobre 2012. Un jeune homme de 18 ans s'était dénudé par webcam, sur Facebook, à la demande d'une jeune femme rencontrée en ligne qui faisait de même. Avant d'interrompre le « jeu » au bout de 10 minutes en le menaçant : « J'ai une vidéo porno de toi, si tu ne me donnes pas 200 euros, je vais détruire ta vie. »
Paniqué à l'idée de voir la vidéo diffusée à ses amis Facebook, le lycéen s'était pendu après avoir laissé un SMS d'adieu à ses parents. L'adresse IP de la femme provenait de Côte d'Ivoire, où des maîtres chanteurs connus sous le nom de « brouteurs » sont devenus des professionnels de ce genre de pratique.

Source : http://tempsreel.nouvelobs.com/faits-divers/20150605.OBS0251/menace-de-chantage-sur-skype-un-lyceen-se-suicide.html
Par Alexis Orsini

Pour pirater un ordinateur, une pita suffit | Le Net Expert Informatique

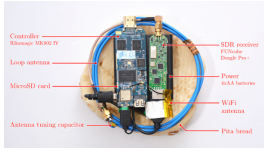


Pour pirater un ordinateur, une pita suffit

Selon une étude de l'université de Tel-Aviv, travailler dans un café pourrait s'avérer risqué pour la sécurité de votre ordinateur

Cette pita, qui donne l'apparence innocente que quelqu'un mange ostensiblement en face de vous dans le café de votre quartier, pourrait contenir un système d'espionnage informatique pouvant infiltrer les protocoles d'encodage les plus sécurisés de votre ordinateur.

Pire encore, ont déclaré les chercheurs de l'Université de Tel-Aviv, les utilisateurs de cet ordinateur ne peuvent pas faire grand chose pour se protéger.
« Des techniques d'atténuation… pourraient inclure des cages Faraday », des écrans en métal spécialement posés au sol qui bloquent les radiations… « Pourtant, la protection peu chère de PC de niveau commercial semble difficile », explique l'équipe.
Dans un article publié mardi, les chercheurs décrivent le très faible coût de l'équipement de type Radio Shack, que l'on peut facilement cacher dans un pain pita standard et qui peut être utilisé pour « lire » des impulsions électromagnétiques provenant du clavier d'un ordinateur standard, y compris les frappes sur le clavier afin de décrypter les documents sécurisés.
De manière amusante, l'Université de Tel-Aviv a appelé l'attaque PITA, Instrument portable pour l'acquisition de signaux.



L'étude, menée par les chercheurs Daniel Genkin, Itamar Pipman, Lev Pachmanov et Eran Tromer a été publiée pour coïncider avec une conférence majeure de sécurité informatique qui va avoir lieu à l'Université de Tel-Aviv (UTA) cette semaine.
« Nous avons pris avec succès des codes d'ordinateurs de divers modèles fonctionnant avec GnuPG (une source populaire d'encodage, en utilisant le standard d'encodage OpenPGP) en quelques secondes », a écrit l'équipe de l'UTA dans l'article, intitulé « Voler des codes de PC en utilisant une radio : des attaques électromagnétiques à moindre coût sur une exponentiation de fenêtres ».
En plus d'OpenPGP, l'équipe a été capable de dupliquer avec réussite les attaques sur d'autres systèmes d'encodages, très sécurisés, y compris RSA et ElGamal.
« L'attaque envoie quelques textes informatiques bien conçus et lorsque ces textes sont décryptés par la cible, ils entraînent l'occurrence de valeurs spécialement structurées dans le logiciel d'encodage », ont déclaré les chercheurs.
En utilisant un appareil qui peut recevoir des signaux radio, une simple radio ou une clé USB pouvant recevoir des émissions et les lire sur l'ordinateur, les chercheurs ont été capables d'observer les fluctuations dans le champ électromagnétique entourant l'ordinateur et de traduire ces fluctuations en frappes de clavier en utilisant un programme d'analyse.
L'article fournit des détails complets sur l'équipement nécessaire (tout est disponible et peu cher dans un magasin local d'électronique ou sur Internet), et sur la façon d'assembler et de connecter les parties, et même de les plier dans un pain pita.

L'équipement détecte les fluctuations dans le champ électromagnétique émis par le matériel informatique (clavier et processeur) lorsque l'ordinateur essaie de décrypter les signaux (les modules d'encodage contiennent des composants qui peuvent être exploités pour fonctionner automatiquement lorsque le texte encodé est rencontré).

En envoyant ces textes pièges, les pirates peuvent voler les codes d'authentification sur l'ordinateur de l'utilisateur, leur autorisant un accès libre aux documents et aux données encodés.

Une attaque PITA pourrait probablement être utilisée par des pirates en cas d'une attaque qui « balaie » des données et les documents d'un ordinateur.

Si ces données sont encodées, il est peu probable que les pirates pourront les lire (en fonction de niveau de complexité du codage), mais avec des clés d'encodage, les pirates pourraient trouver des informations encodées comme des numéros de cartes de crédit ou des mots de passe.

La seule mise en garde est que la pita « espion » a besoin de se trouver à 50 centimètres de la cible.

Mais d'après l'équipe, la totalité de l'opération peut être réalisée en quelques secondes, rendant l'attaque parfaite pour les pirates dans les cafés où de nombreux utilisateurs d'ordinateurs profitent des installations électroniques, du wifi et de boissons pour travailler.

Un pirate pourrait obtenir les codes dans une attaque « en marchant », attaque menée en transportant une « pita empoisonnée » sur un plateau avec de la vraie nourriture. L'étude notait pourtant que la « qualité du signal variait fortement en fonction du modèle de l'ordinateur cible et de la position de logiciel espion ».

L'équipe de UTA n'est pas la première à penser à utiliser des impulsions électromagnétiques pour pirater des systèmes.

En 2014, des chercheurs de l'Université Ben Gourion (UBG) ont pu utiliser un programme pirate sur un téléphone portable pour collecter des radiations électromagnétiques provenant de claviers, de moniteurs et d'autres équipements pour lire des informations importantes.

L'équipe de l'UBG a démontré comment les données collectées par le programme espion, auparavant placé sur un ordinateur (à travers une attaque de phising ou une autre méthode), pouvaient être captées par un téléphone portable qui créait un réseau local en utilisant des impulsions émanant de matériel informatique.

Les informations du système cible pouvaient être captées, même s'il n'est pas connecté à internet ou à un réseau local (Ethernet).

Le pire, a déclaré l'équipe, est qu'il n'y a pas grand chose que les utilisateurs d'ordinateur puissent faire pour éviter ces attaques, si ce n'est éviter les cafés et garder leur ordinateurs loin des pitot.

Malheureusement, l'équipe a déclaré « qu'empêcher la fuite à un bas niveau de prévention est presque impossible » parce que mettre en place des mesures efficaces (comme des cages Faraday) serait très gênant à cause du matériel informatique excessif ou ralentirait la capacité au point que les utilisateurs seraient incapables d'accomplir le moindre travail.

« Même lorsqu'un programme cryptographique est sûr mathématiquement, ses mises en place peuvent être vulnérables à des attaques de réseaux secondaires qui exploitent des émanations physiques », a déclaré l'équipe. Le pirate « peut facilement viser les ordinateurs ».

« Nous avons testé de nombreux ordinateurs de modèles variés », et lorsqu'il s'agit d'une attaque PITA, chaque utilisateur d'ordinateur devrait se sentir concerné.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://fr.timesofisrael.com/pour-pirater-un-ordinateur-une-pita-suffit/
Par David Shamah

L'Afrique a besoin de cybersécurité| Le Net Expert Informatique

L'Afrique a besoin de cybersécurité

Avec un taux de croissance au niveau des TIC de l'ordre de 30% sur un marché de plus d'un milliard de personnes, l'Afrique représente le nouvel Eldorado du monde numérique.

Or, la surface d'attaque augmentant, les cybercriminels élargissent leur champ d'action. La cybercriminalité en Afrique est organisée et bien enracinée, en particulier au Nigéria, au Ghana et en Côte d'Ivoire. Désormais, l'Afrique n'est plus le théâtre des seuls cybercriminels mais aussi de cyberhacktivistes voire de hackers. Le Sénégal a été la victime de cyberattaques en janvier dernier revendiquées par le collectif anonymous du Sénégal. Par rebond des attaques massives menées en janvier en France suite aux attentats de Charlie Hebdo, les serveurs de l'agence de l'informatique de l'Etat du Sénégal sont tombés.
Devant ce désert cybernétique, les Etats d'Afrique tentent de réagir en relevant le défi de sécuriser leurs infrastructures réseau, leurs données et en formant leurs personnels. La France participe activement à la formation cyber des officiers et des techniciens par le biais de la coopération opérationnelle (ministère de la défense). Depuis 2013, une centaine d'officiers et sous-officiers ont été formés au Sénégal, au Niger et au Burkina Faso par les Eléments français au Sénégal.
Le Security Day, qui se tiendra les 15 et 16 mars 2016 à Dakar, sera l'occasion d'aborder l'ensemble de ces sujets.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Newsletter n°3 FIC
https://www.forum-fic.com/site/FR/Newsletter/S_inscrire_a_la_newsletter,C58881,I58949.htm