Piratage du capteur d’empreinte d’un téléphone avec une simple imprimante à jet d’encre

	Piratage du capteur d’empreinte d’un téléphone avec une simple imprimante à jet d’encre

Les capteurs de biométrie sont sur le grill après une nouvelle tentative fructueuse de piratage sur des téléphones Samsung Galaxy S6 et Huawei Honor 7. L'iPhone 5s a pour sa part résisté.

La biométrie serait pour beaucoup l'avenir de la sécurité, surtout en situation de mobilité. Et bien ce sont les chercheurs de l'université du Michigan qui viennent de prouver qu'une imprimante à jet d'encre pouvait à elle seule permettre de pirater les systèmes de capture d'empreinte de téléphones Samsung et Huawei. Objectif : rentrer dans le téléphone. Une imprimante à jet d'encre basique certes, mais pour réaliser ce hack, ils ont toutefois du s'équiper d'encre et de papier spécifique.
Démonstration en vidéo du hack de capteur biométrique réalisé par l'université du Michigan. (Source : Université du Michigan)

En moins de 15 minutes, selon les chercheurs qui publient une vidéo à ce sujet, il est donc possible d'entrer par effraction dans un smartphone, à condition bien sûr de récupérer l'empreinte digitale du possesseur du téléphone. Ensuite, une impression en haute résolution sur un papier brillant et une encre spécifique permet de duper le module d'analyse d'empreinte des téléphones Samsung Galaxy S6 et Huawei Honor 7. Les chercheurs précisent par ailleurs que la tentative de hack sur un iPhone 5s s'est soldée par un échec.

Pas une première, mais très peu cher et facile a réaliser

Ce n'est pas la première fois que les capteurs d'empreinte digitale sont floués par des tentatives de piratage. Mais jusqu'alors les techniques utilisées reposaient sur de l'impression 3D et des moules spécifiques. Cette nouvelle méthode s'avère de fait bien moins onéreuse, et bien plus rapide. De quoi poser quelques questions quand on sait que Samsung (et d'autres) prévoient de proposer de l'authentification de paiement avec de la biométrie.
Il convient de noter toutefois que l'utilisation de la biométrie à tord et à travers fait l'objet de critiques depuis fort longtemps. Il s'agit de ne pas confondre authentification et identification d'une part, et surtout de ne pas l'utiliser pour de l'authentification forte… [Lire la suite]

Réagissez à cet article

Source : *Capteur d'empreinte : un piratage avec une simple imprimante à jet d'encre – ZDNet*

Comment une cyberattaque a mis des centrales ukrainiennes hors service

Comment une cyberattaque a mis des centrales ukrainiennes hors service ?

S'il reste encore des zones d'ombres, le doute n'est désormais plus permis : la panne électrique qui a touché l'Ukraine à Noël a bien été causée par une cyberattaque. C'est la première fois qu'un réseau électrique est mis hors service par une attaque informatique. Mais que les opérateurs d'importance critique soient prévenus : ce n'est sûrement pas la dernière.

Le rapport publié jeudi 3 mars par l'équipe de réponse d'urgence pour la sécurité informatique des systèmes de contrôle industriels (ICS-CERT) du département de la Sécurité intérieure des Etats-Unis (DHS) est sans appel : le blackout électrique qu'a connu une partie de l'Ukraine fin 2015 a bien été causé par des hackers. Il confirme ce faisant les conclusions avancées par le SANS ICS (un autre groupe d'experts en cybersécurité industrielle) début janvier, et entérine l'évènement comme étant la première attaque réussie sur un réseau électrique.

UNE SÉRIE D'ATTAQUES SOIGNEUSEMENT PLANIFIÉES

Les intrusions dans le réseau de trois opérateurs énergétiques ont impacté environ 225 000 clients. Bien que le service ait repris quelques jours plus tard, il reste encore limité, même à l'heure actuelle. D'après les témoins interrogés par l'ICS-CERT, les attaques auraient été coordonnées de telle manière qu'elles se sont produites à 30 minutes d'intervalle sur chaque réseau, touchant des installations centrales et régionales. L'opération a très probablement nécessité une longue reconnaissance et étude des victimes.

Lors de l'attaque, plusieurs individus ont pris l'accès des systèmes grâce à des outils de contrôle à distance, soit au niveau de l'OS, soit au niveau des systèmes ICS, le tout via des accès VPN (réseau privé virtuel) dont ils avaient précédemment obtenu les codes d'accès. Une fois l'attaque effectuée, le malware KillDisk a été utilisé pour effacer les fichiers compromis et corrompre les secteurs de démarrage des machines ou les firmwares des équipements pour les rendre inopérants. Les attaquants auraient également surchargé les centres d'appels des énergéticiens pour les empêcher de réagir immédiatement à l'évènement. De plus, trois autres organisations en charge d'infrastructures critiques ont aussi été pénétrées, mais sans impact direct sur leurs opérations.

DES ZONES D'OMBRES PERSISTENT

Malgré ces nouvelles informations, le rôle exact qu'a joué le malware BlackEnergy dans l'attaque n'est toujours pas connu. Ce malware, connu du milieu de la cybersécurité depuis 2007, a été retrouvé sur trois des systèmes impactés. Originellement présenté comme la potentielle arme du crime, il est possible qu'il n'ait en fait été utilisé que pour obtenir des codes d'accès. Il est aussi bon de noter que le rapport de l'ICS-CERT se base uniquement sur les témoignages du personnel IT de six organisations ukrainiennes qui ont été directement témoins des évènements, et pas sur une analyse technique du code ou du matériel impliqué dans l'incident.

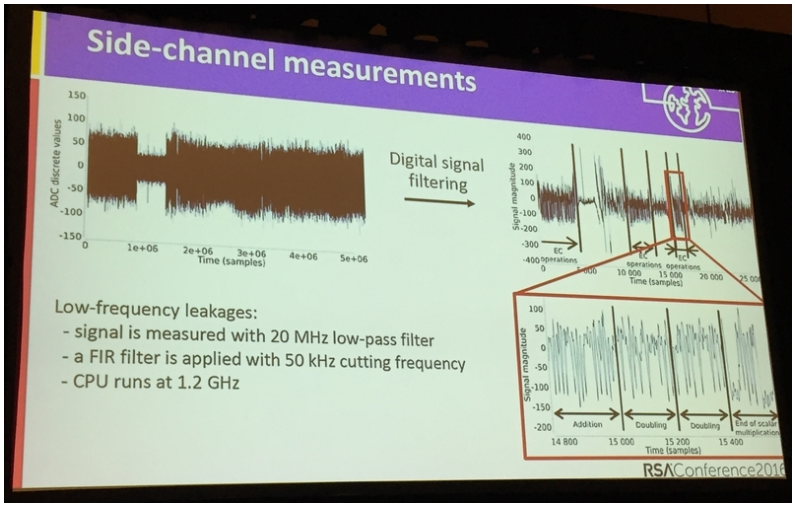
Ces considérations mises à part, le fait que différents groupes d'experts soient d'accord sur l'origine cybercriminelle de la panne constitue une ultime (et sinistre) mise en garde à l'égard des opérateurs d'importance vitale (OIV). Car ces incidents ne font malheureusement que commencer. … [Lire la suite]

Réagissez à cet article

Source : *Les détails de la cyberattaque qui a mis des centrales ukrainiennes hors service*

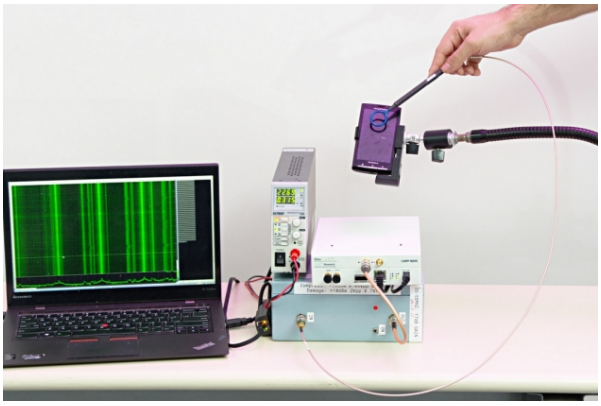
Piratages des smartphones iOS ou Android possibles à cause de leurs fuites

électromagnétiques

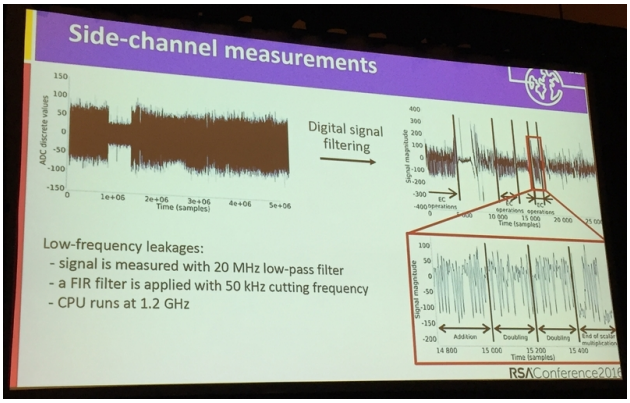


Piratages des smartphones iOS ou Android possibles à cause de leurs fuites électromagnétiques

Des chercheurs arrivent à extraire des clés de chiffrement privées en captant les signaux involontaires des circuits imprimés. Parmi les applications vulnérables figurent OpenSSL et les porte-monnaie Bitcoin.



Les smartphones d'aujourd'hui embarquent de plus en plus procédés cryptographiques pour sécuriser tout un tas d'échanges et de transactions. L'équipement matériel, toutefois, n'est pas forcément à la hauteur des enjeux. Deux équipes de chercheurs viennent de présenter concomitamment des attaques non invasives qui s'appuient sur les émanations électromagnétiques des terminaux mobiles pour récupérer des clés privées de signatures électroniques. Elles permettraient, par exemple, de pirater des porte-monnaie Bitcoin, des transactions Apple Pay ou des connexions sécurisées par OpenSSL.
La première équipe est française et regroupe quatre chercheurs issus d'Orange Labs, HP Labs, NTT et l'université de Rennes. Le 3 mars, à l'occasion de la conférence RSA 2016, ils ont montré comment extraire d'un téléphone Android des clés privées basées sur les algorithmes de courbes elliptiques (Elliptic Curve Digital Signature Algorithm, ECDSA). Leur étude se limite à une librairie cryptographique spécifique, à savoir Bouncy Castle 1.5. Quand celle-ci réalise les calculs mathématiques liés à la signature d'un message, les circuits intégrés du téléphone émettent des ondes électromagnétiques à basse fréquence (50 kHz).



Le traitement du signal révèle les opérations mathématiques (« addition », « doubling »)

Les chercheurs captent ce signal au moyen d'une antenne appliquée sur le téléphone et arrivent, par traitement de signal, à reconnaitre les différentes opérations de ce calcul. Cette information est suffisante pour récupérer in fine la clé secrète. La librairie vulnérable a, depuis, été modifiée de telle manière que l'on ne puisse plus reconnaitre les opérations (version 1.51). Néanmoins, une attaque concrète aurait pu être, selon les chercheurs, de cibler les porte-monnaie Bitcoin car ils s'appuient sur Bouncing Castel.
Ainsi, un attaquant aurait pu piéger le lecteur NFC d'un commerce qui accepte les Bitcoins et, ainsi, récupérer les adresses Bitcoin des clients. Ce qui lui permettait alors d'en disposer comme bon lui semble. « On pourrait également imaginer des attaques à plus longue distance, à condition de disposer d'un équipement de captation suffisamment puissant, comme peuvent en avoir les agences gouvernementales », nous explique Mehdi Tibouchi, l'un des quatre chercheurs français, à l'issue de leur présentation.

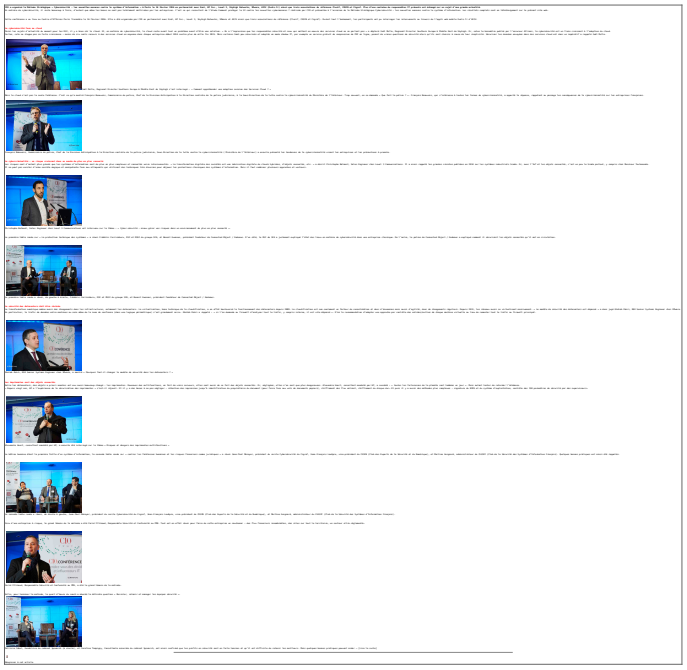
Des attaques low-cost
La seconde équipe qui a planché sur ce type d'attaques est israélienne et regroupe cinq chercheurs issus de l'université de Tel Aviv et de l'université d'Adelaide (Australie). Leur attaque cible également les signatures basées sur les courbes elliptiques ECDSA, mais son domaine d'application est nettement plus large.
Ainsi, ces chercheurs ont réussi à extraire des clés privées sur les librairies OpenSSL et CoreBitcoin sur iOS, qui sont toujours vulnérables à l'heure actuelle. Ils ont également réussi des extractions partielles de clés privées avec la librairie CommonCrypto d'iOS et la version Android d'OpenSSL. Toutefois, CommonCrypto – qui est notamment utilisé par Apple Pay – n'est pas vulnérable au-delà de la version iOS 9 car Apple a intégré des « mécanismes de défense » contre ce type d'attaques.
Selon les chercheurs israéliens, les fuites de signaux peuvent être captées de façon électromagnétique par une petite antenne, ou de manière électrique par une petite résistance intégrée au niveau du câble de chargement USB (prix : quelques dollars). Dans les deux cas, le signal est envoyé dans l'entrée d'une carte son Creative Track Pre Sound, ce qui permet de le numériser et de l'amplifier (prix : 50 dollars). Au final, la mise en œuvre de l'attaque est donc de faible coût. Les chercheurs ont réalisé leurs tests avec un iPhone 3GS et un Sony-Ericsson Xperia x10 … [Lire la suite]

Réagissez à cet article

Source : *On peut pirater les smartphones iOS ou Android à cause de leurs fuites électromagnétiques*

Comment contrer les nouvelles menaces en Cybersecurité contre le système d'information ?

Comment contrer les nouvelles menaces en Cybersecurité contre le système d'information ?



Source : *Cybersécurité : contrer les nouvelles menaces contre le système d'information*

Apple contre le FBI : Un cadeau aux pirates informatiques ?

Apple contre le FBI : Un cadeau aux pirates informatiques ?

Le Haut-Commissariat aux droits de l'homme de l'ONU a décidé de soutenir officiellement Apple dans l'affaire qui l'oppose au FBI. Le chiffrement doit rester un droit fondamental, même dans les affaires de terrorisme.

C'est excessivement rare, si ce n'est pas une première, que des représentants des Nations Unies s'invitent très directement dans une affaire judiciaire. Pourtant, c'est bien aux côtés de très nombreux industriels et organisations de la société civile (dont Apple dresse la liste) que le Haut-Commissariat aux droits de l'homme de l'ONU a décidé de venir apporter à la firme de Cupertino son soutien très officiel, contre le FBI.

Totalement indépendant des états membres de l'ONU, le Rapporteur Spécial des Nations Unies pour la protection et la promotion de la liberté d'expression et d'expression, David Kaye, a ainsi écrit (.pdf) à la juge californienne Sheri Pym, avec le soutien du Haut-Commissariat chargé de veiller au respect des traités en matière de droits de l'homme. Il demande à la magistrate de ne pas ordonner à Apple de supprimer la protection qui permettrait au FBI de découvrir le code de déblocage de l'iPhone 5C de l'auteur de la tuerie de San Bernardino, pour accéder en clair aux données chiffrées qui y sont stockées.
Pour David Kaye, la législation américaine ne permet pas à un tribunal de prendre une telle décision qui obligerait Apple, non pas à fournir des données qui sont en sa possession, mais à fournir son aide technique pour accéder à des données qui, normalement, ne doivent être accédées par personne d'autre que le propriétaire du téléphone.

LA VIE PRIVÉE GARANTIT LA LIBERTÉ DE PENSER ET DE S'EXPRIMER

Il rappelle que l'article 19 du pacte international relatif aux droits civils et politiques(PIDCP) n'autorise des restrictions à la liberté d'opinion – qui comprend celle de les dissimuler – et d'expression que si elles sont « *expressément fixées par la loi* ». C'est le même raisonnement, appuyé sur la Constitution américaine, qu'a eu le juge de New York qui a donné tort au FBI dans une affaire similaire.
Il peut paraître surprenant que l'auteur du courrier soit l'expert de l'ONU chargé de la liberté d'expression, et non celui en charge de la vie privée, Joe Cannataci, qui ait pris la plume pour soutenir Apple. Mais c'est parce que les droits de l'homme sont liés et interdépendants.

Atteindre à la vie privée des individus pour aller sonder ce qu'ils pensent ou ce qu'ils se disent en privé, c'est inciter les individus à ne plus penser librement, ou à ne plus se parler librement.
LES DÉBATS SUR LE CHIFFREMENT ET L'ANONYMAT SE SONT BIEN TROP SOUVENT CONCENTRÉS UNIQUEMENT SUR LEUR UTILISATION POTENTIELLE POUR DES DESSEINS CRIMINELS

David Kaye, Rapporteur spécial des Nations unies sur la promotion et la protection de la liberté d'opinion et d'expression.

C'est pourquoi David Kayes avait déjà à plusieurs reprises exigé le respect du droit au chiffrement. L'expert, qui a été mandaté en 2014, est aussi un opposant farouche aux backdoors, auxquels peut s'assimiler la méthode demandée à Apple au FBI (non pas fournir la clé, mais faire en sorte que la serrure ne fonctionne plus). « Les gouvernements qui proposent des accès par backdoor n'ont pas démontré que l'utilisation criminelle ou terroriste du chiffrement serve de barrière insurmontable pour les objectifs d'application de la loi », avait-il critiqué dans un rapport contre les backdoors.
« Les débats sur le chiffrement et l'anonymat se sont bien trop souvent concentrés uniquement sur leur utilisation potentielle pour des desseins criminels dans des périodes de terrorisme. Mais des situations urgentes ne dispensent pas les États de leur obligation de s'assurer du respect du droit international des droits de l'homme »,
UN CADEAU FAIT AUX RÉGIMES AUTORITAIRES ET AUX PIRATES INFORMATIQUES

L'initiative de David Kayes en faveur d'Apple est publiquement soutenue par la Haut-Commissaire de l'ONU aux droits de l'Homme, Zeid Ra'ad Al Hussein, qui ***explique*** *que « dans le but de régler un problème de sécurité relatif au chiffrement des données dans un cas bien précis, les autorités risquent d'ouvrir la boîte de Pandore, avec des implications qui pourraient être extrêmement dommageables pour les droits de l'Homme de millions de personnes, y compris pour leur sécurité physique et financière ».*
« Un succès dans l'affaire contre Apple aux États-Unis établirait un précédent qui pourrait rendre impossible pour Apple ou toute autre société informatique internationale majeure de protéger la vie privée de ses clients partout dans le monde. Cela pourrait être un cadeau fait aux régimes autoritaires et aux pirates informatiques ». ***[Lire la suite]***

Réagissez à cet article

Source : *Apple contre le FBI : l'ONU intervient au nom des droits de l'homme – Politique – Numerama*

Le piratage de TV5 Monde en avril dernier a poussé la chaîne à durcir sa sécurité

Le piratage de TV5 Monde en avril dernier a poussé la chaîne à durcir sa sécurité

À la suite de son piratage, la direction de TV5 Monde a pris une série de mesure en coopération avec l'ANSSI et Airbus Defense & Space pour renforcer drastiquement sa sécurité informatique. Des choix qui pèsent de fait sur ses finances.

L'attaque informatique qui a frappé TV5 Monde au cours du printemps 2015 a eu des effets substantiels sur l'organisation interne de la chaîne de télévision, mais aussi sur ses finances. Pratiquement un an après les faits, le groupe est encore en phase de rémission et ses salariés doivent maintenant composer avec de nouvelles consignes de sécurité afin de réduire les risques qu'un autre incident, révèlent Les Échos.

EMPÊCHER UNE NOUVELLE INTRUSION

Ainsi, plus question de laisser les employés de TV5 Monde brancher n'importe quoi sur les ordinateurs de la chaîne. Les clés USB, les smartphones et les tablettes – bref, les principaux périphériques – ne peuvent plus être connectés, afin d'éviter l'intrusion d'un logiciel malveillant dans le réseau interne. Et ce régime vaut bien sûr pour d'autres produits, comme les disques durs externes.
Du côté d'Internet, de nouvelles règles de filtrage concernant les pièces jointes ont aussi été mises en place pour empêcher le téléchargement par inadvertance d'un fichier douteux ou d'un contenu vérolé. Les connexions elles-mêmes ne tournent plus à plein régime. Enfin, les salariés doivent apprendre tous les trois mois de nouveaux mots de passe pour se connecter à l'infrastructure.

DES DÉPENSES ÉLEVÉES DEPUIS 2015

Toutes ces mesures ne pèsent pas directement sur les finances de TV5 Monde, à la différence de certaines autres. Toutes les machines affectées par l'attaque informatique ont dû être remplacées, des postes de travail aux serveurs. Il a également fallu repenser l'architecture informatique de la chaîne, mobiliser les équipes, recruter du personnel et établir des contrats avec des sociétés spécialisées.
Ainsi, TV5 Monde a fait le choix de souscrire une police d'assurance dédiée auprès d'Axa et s'est rapproché d'Airbus Defense & Space pour observer en permanence le flux entrant et sortant du réseau de la chaîne. Au total, ces orientations ont été évaluées par la chaîne à 4,6 millions d'euros l'an dernier, 3,1 millions d'euros pour 2016 et 2,5 millions d'euros pour chaque année à partir de 2017.

SOUTIEN DE L'ANSSI

TV5 Monde a aussi pu compter sur l'aide de l'agence nationale de sécurité des systèmes d'information (ANSSI), qui avait d'ailleurs repéré une anomalie dans les serveurs de la chaîne avant le déclenchement de la cyberattaque. L'agence a ainsi dépêché une aide technique « pour analyser l'attaque et permettre à la chaîne de rétablir le service dans de bonnes conditions de sécurité ».
L'attaque subie par TV5 Monde est considérée comme la plus grave de l'histoire de la télévision. Les assaillants n'ont pas seulement diffusé leur propagande sur la page Facebook, dont des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'EI, ils ont aussi réussi à interrompre la diffusion des chaînes du groupe … [Lire la suite]

Réagissez à cet article

Source : *Le piratage de TV5 Monde a poussé la chaîne à durcir sa sécurité – Politique – Numerama*

Cybercriminalité, comment l'entreprise peut se protéger ?

Cybercriminalité, comment l'entreprise peut se protéger ?

Denis Jacopini, spécialiste en cybercriminaltié et dans la protection des données personnelles interviewé par l'Entreprise connectée.

 **Il acte des formations auprès des dirigeants d'entreprises et des salariés, pour leur donner des conseils et détecter les attaques. Il nous donne son avis d'expert pour aider les entreprises dans la prévention des cyberattaques.**

EC: Quels sont les risques de la cybercriminalité ?
Denis Jacopini : La cybercriminalité prend plusieurs formes : des pirates qui ont message à faire passer et dont le but est la défiguration de sites internet, et d'autres qui recherchent l'aspect pécuniaire de la cybercriminalité. Une attaque entraine une mauvaise image et une perte de confiance autant auprès des clients que des salariés. Ces derniers risquent de moins s'engager dans l'entreprise et de perdre confiance dans la sécurité informatique avec la peur de voir leurs données personnelles volées.
EC: Que conseillerez-vous aux entreprises pour améliorer leur sécurité ?
DJ : Les entreprises ont conscience de la cybercriminalité mais se font toujours avoir. Il faut absolument éduquer. Toutes les entreprises risquent de se faire pirater. L'élément souvent négligé est la charte informatique qui va lier le salarié aux usages des outils informatiques.
EC: Et concrètement ?
DJ : Concrètement, pour anticiper, l'entreprise doit, faire un audit de la sécurité de son système d'information (analyses des mesures de sécurité existantes, test d'intrusion, analyse des usages illicites internes ou externes à l'entreprise) et prévoir une sensibilisation des salariés par un organisme extérieur. Les actions qui en ressortent souvent sont : l'amélioration d'outils et de mesures de sécurité, la mise en place d'une charte informatique, d'outils de cryptage des e-mails ou de cryptage des données. Enfin, la mise à niveau tous les 12 mois des employés car ils doivent connaître les nouvelles techniques couramment utilisées par les cybercriminels.
EC: Quel est le plus grand danger pour les entreprises ?
DJ : La plus grande menace reste le mail piégé. Dans la précipitation, l'employé va l'ouvrir et cliquer sur une page web usurpée. A partir de là, le pirate peut s'infiltrer, c'est ce qu'il s'est passé avec TV5 Monde. Contre ce genre d'attaque, appelée « spear-phising », la technologie arrive à ses limites. La question désormais, est celle du comportement. La sensibilisation des salariés est très difficile mais il est possible de leur apprendre toutes les formes d'attaques, grâce à des formations. … [Lire la suite]

Réagissez à cet article

Source : *Cybercriminalité, comment se protéger ? – L'entreprise connectée*

Gare aux « tarifs délirants » des numéros en 118

Gare aux « tarifs délirants » des numéros en 118

Les numéros de renseignements téléphoniques comme le « 118 218 » existent encore, et ils sévissent auprès d'usagers fragiles, mal informés ou pressés… qui en paient le prix fort.

Des numéros de renseignements téléphoniques, la plupart d'entre vous n'en connaissent que le duo moustachu qui amusait la galerie dans les spots TV voilà quelques années. À force de le répéter sur un air de générique des années 80, le numéro « 118 218 » s'est peut-être inscrit durablement chez certains. Ce que l'on sait moins, c'est que cette société – leader du marché – ainsi que ses pairs, génèrent une « vague de plaintes » des utilisateurs.

L'association 60 Millions de consommateurs dit avoir reçu un certain nombre de réclamations de personnes ayant vu leur facture téléphonique exploser suite à un appel en « 118 ». Après la libéralisation complète du « 12 » en 2007, ces services se sont mis à pulluler. Depuis, la plupart a disparu et le nombre d'appels a fondu, mais une dizaine survit. Le 118 218, de la société Le Numéro (filiale de l'américain KGB), a même lancé son application.

Une arnaque en 3 leçons

« Pour à peine 2 minutes et 40 secondes au bout du fil, un de nos lecteurs s'étonne d'avoir payé 10,80 euros au 118 218 », rapporte l'association. Elle voit trois explications. La première : « Face à la baisse des appels, les services de renseignements téléphoniques ont augmenté leurs tarifs jusqu'à des sommets inédits. La plupart facturent désormais 5 à 6 euros la première minute d'appel, puis 2,50 à 3 euros les minutes suivantes. »

En effet, les services de renseignements téléphoniques « sont les seuls numéros surtaxés pour lesquels la réglementation ne fixe aucun plafond tarifaire », rappelle 60 Millions de consommateurs, alors que les autres numéros à tarification majorée (08) ont plafonnés à 0,80 euro la minute depuis la réforme d'octobre 2015.

Réagissez à cet article

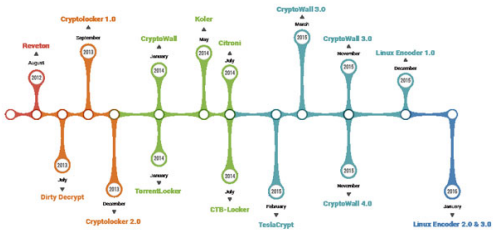
Source : *Gare aux « tarifs délirants » des numéros en 118*

Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données

Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données

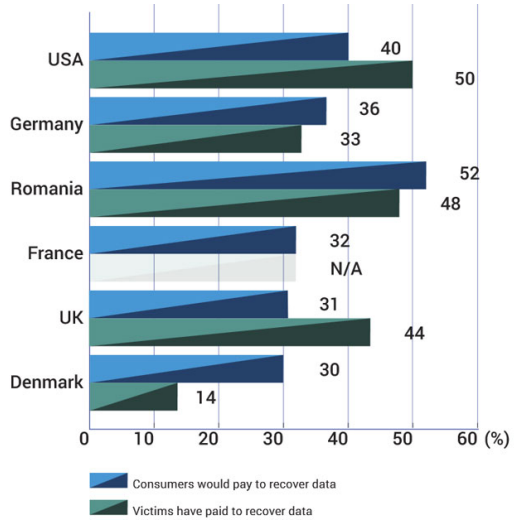
Le ransomware est une catégorie de programme malveillant qui une fois installé chiffre les données du PC et exige de son propriétaire qu'il paie une rançon pour les récupérer. Et les victimes seraient, pour une bonne partie d'entre eux, disposées à payer cette rançon.
Si vous étiez victime d'un ransomware (ou rançongiciel), paieriez-vous la rançon exigée pour récupérer vos fichiers ou enverriez-vous les cybercriminels promener ? Le fait que vous soyez au travail ou à votre domicile ferait-il une différence ?

Selon une étude, le comportement des victimes de ransomware pourrait bien dépendre du lieu où celles-ci se trouvent lorsque la demande de rançon leur parvient. Ce qui varierait également, c'est le montant de cette rançon.



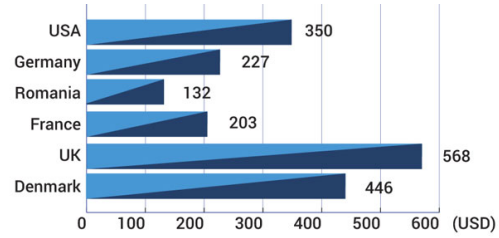
32% des sondés français paieraient pour leurs fichiers.
Comme son nom le suggère, le ransomware va chiffrer les fichiers enregistrés sur l'ordinateur compromis. Menaçant les utilisateurs de l'impossibilité de récupérer ces documents, les cybercriminels exigent le versement d'une rançon. Une fois celle-ci versée, promesse serait faite de déchiffrer les données des victimes.

Et d'après une étude de l'éditeur de sécurité Bitdefender, tous les internautes, en fonction de leur nationalité, ne sont pas égaux face à ces logiciels malveillants. Ainsi aux Etats-Unis, 50% des victimes de ransomware ont accepté de payer.
En France ? Cette donnée n'est pas disponible. En revanche, 32% des internautes français interrogés déclarent qu'ils paieraient en cas d'infection. Cette part dépend aussi, très logiquement, de l'importance accordée aux fichiers devenus inaccessibles en raison du chiffrement.



Par exemple, 18% des répondants du Royaume-Uni paieraient pour les documents personnels, 17% pour les photos personnelles et seulement 10% pour les documents liés au travail » détaille BitDefender.

Accepter de payer est une chose, mais quel montant ? Sur ce point aussi, les sommes varient très significativement d'un pays à un autre. Au Royaume-Uni, une victime accepterait de verser jusqu'à 568 dollars, contre 203 dollars en France.



Payer la rançon aide juste les cybercriminels
Un tel comportement consistant à céder aux cybercriminels est-il cependant recommandé ? Catalin Cosoi, responsable de la stratégie sécurité de BitDefender, déconseille de payer. « Alors que les victimes sont généralement enclines à payer la rançon, nous les encourageons à ne pas à se livrer à de telles actions, car cela contribue uniquement à soutenir financièrement les développeurs du malware. »
En janvier, à l'occasion du FIC 2016, le directeur de l'Anssi a évoqué l'infection du ministère des Transports par un ransomware. Et Guillaume Poupard était formel : « On ne paie pas, ce n'est pas une solution raisonnable. »
Pourquoi ? Notamment, car le cybercriminel peut tout à fait choisir de ne pas livrer les clefs nécessaires au déchiffrement des fichiers, et rien ne garantit non plus qu'il ne relancera pas une nouvelle attaque ultérieurement. Les sauvegardes restent donc la meilleure parade face à ces malwares, préconise l'Anssi … ***[Lire la suite]***

Réagissez à cet article

Source : *Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données*

Un ransomware paralyse un hôpital américain

Un #ransomware paralyse un hôpital américain

La France n’est pas la seule à voir ses infrastructures infectées par les ransomwares. Aux États Unis, le Hollywood Medical Presbyterian Center a été victime d’une attaque similaire à celle relayée dans la presse au ministère des Transports en début d’année.

La France n’est pas la seule à voir ses infrastructures infectées par les ransomwares. Aux États Unis, le Hollywood Medical Presbyterian Center a été victime d’une attaque similaire à celle relayée dans la presse au ministère des Transports en début d’année.

Le système informatique de l’hôpital a été infecté par des cyberattaquants ayant recours à un malware de type ransomware (ou rançongiciel) : celui-ci chiffre les données contenues sur la machine et les rend inaccessibles à l’utilisateur, qui se voit contraint de verser une rançon afin d’espérer récupérer l’accès à ses fichiers. Sans système de sauvegarde fonctionnel, la situation peut rapidement devenir critique et cela semble être le cas de cet hôpital, dont les services administratifs se retrouvent paralysés depuis une semaine comme le relatent les médias locaux.

Si l’attaque n’a pas entièrement bloqué le traitement des patients, mais environ 900 nouveaux entrants ont été redirigés vers d’autres hôpitaux en attendant que le problème soit résolu.

L’attaque n’est, selon les déclarations du directeur de l’établissement, pas directement ciblée contre l’hôpital. Il s’agirait plutôt d’une attaque classique, issue d’un utilisateur peu précautionneux ou d’une politique de sécurité informatique défaillante.

Néanmoins, plusieurs sources expliquent que les cybercriminels exigent le versement de 9000 bitcoins afin de déchiffrer les données retenues par le malware.

Un plan sans accroc?

Et on avoue être un peu surpris : effectivement, les ransomwares sont une menace en pleine expansion et le ministère des Transports a récemment été victime d’une attaque de ce type. En revanche, le succès de ce nouveau type de menace tient à un modèle économique bien rodé. Les auteurs d’attaques par ransomware visent généralement un large panel de cibles et demandent des rançons relativement modérées, afin de s’assurer que les victimes pourront les payer.

9000 bitcoins, même pour un hôpital de grande taille, paraissent être une somme inhabituelle pour une demande de rançon. Cela ne représente pas moins de 3,6 millions de dollars. L’information n’a pas été confirmée par les sources officielles en charge du dossier ou par la communication de l’hôpital, prudence donc avant de tirer des conclusions hâtives. Gageons que si cette information venait à se vérifier, le FBI ne conseillera pas de simplement payer la rançon pour résoudre le problème.

Rançon extravagante ou non, les dégâts sont réels pour l’hôpital : le directeur explique ainsi que les formalités administratives et le renseignement des dossiers médicaux se fait maintenant à la main en attendant que le système informatique soit rétabli… [Lire la suite]

Réagissez à cet article

Source : *Quand un ransomware paralyse un hôpital américain*