Skimer, la nouvelle menace pour distributeurs de billets

Skimer, la nouvelle menace pour distributeurs de billets

Skimer, un groupe russophone, force les distributeurs automatiques de billets (DAB) à l'aider à dérober de l'argent. Découvert en 2009, Skimer a été le premier programme malicieux à prendre pour cible les DAB. Sept ans plus tard, les cybercriminels ré-utilisent ce malware. Mais le programme, ainsi que les escrocs, ont évolué ; ils représentent une menace encore plus importante pour les banques et leurs clients partout dans le monde.

Imaginons qu'une banque découvre avoir été victime d'une attaque. Étrangement, aucune somme d'argent n'a été dérobée et rien n'a été modifié dans son système. Les criminels sont partis comme ils sont venus. Serait-ce possible ? Je vous parlais de ce type d'attaque l'année dernière. L'éditeur Gdata m'avait invité en Allemagne pour découvrir l'outil malveillant qui permettait de pirater un distributeur de billets. Aujourd'hui, l'équipe d'experts de Kaspersky Lab a mis au jour le scenario imaginé par les cybercriminels et découvert des traces d'une version améliorée du malware Skimer sur l'un des DAB d'une banque. Il avait été posé là et n'avait pas été activé jusqu'à ce que les criminels lui envoient un contrôle : une façon ingénieuse de couvrir leurs traces.
Le groupe Skimer commence ses opérations en accédant au système du DAB, soit physiquement, soit via le réseau interne de la banque visée. Ensuite, après été installé avec succès dans le système, l'outil Backdoor.Win32.Skimer, infecte le cœur de l'ATM, c'est-à-dire le fichier exécutable en charge des interactions entre la machine et l'infrastructure de la banque, de la gestion des espèces et des cartes bancaires.
Ainsi, les criminels contrôlent complètement les DAB infectés. Mais ils restent prudents et leurs actions témoignent d'une grande habileté. Au lieu d'installer un skimmer (un lecteur de carte frauduleux qui se superpose à celui du DAB) pour siphonner les données des cartes, les criminels transforment le DAB lui-même en skimmer. En infectant les DAB avec Backdoor.Win32.Skimer, ils peuvent retirer tout l'argent disponible dans le distributeur ou récupérer les données des cartes des utilisateurs qui viennent retirer de l'argent, y compris le numéro de compte et le code de carte bancaire des clients de la banque.
Il est impossible pour un individu lambda d'identifier un DAB infecté car aucun signe de le distingue d'un système sain, contrairement à un DAB sur lequel a été posé un skimmer traditionnel qui peut être repéré par un utilisateur averti.

Un zombie dormant
Les retraits directs depuis un DAB ne peuvent pas passer inaperçu alors qu'un malware peut tranquillement siphonner des données pendant une longue période. C'est pourquoi le groupe Skimer n'agit pas immédiatement et couvre ses traces avec beaucoup de prudence. Leur malware peut opérer pendant plusieurs mois sans entreprendre la moindre action.
Pour le réveiller, les criminels doivent insérer une carte spécifique, qui contient certaines entrées sur sa bande magnétique. Après lecture de ces entrées, Skimer peut exécuter la commande codée en dur ou requérir des commandes via le menu spécial activé par la carte. L'interface graphique de Skimer n'apparaît sur l'écran qu'une fois la carte éjectée et si les criminels ont composé la bonne clé de session, de la bonne façon, sur le pavé numérique en moins de 60 secondes.
À l'aide du menu, les criminels peuvent activer 21 commandes différentes, comme distribuer de l'argent (40 billets d'une cassette spécifique), collecter les données des cartes insérées, activer l'auto-suppression, effectuer une mise à jour (depuis le code du malware mis à jour embarqué sur la puce de la carte), etc. D'autre part, lors de la collecte des données de cartes bancaires, Skimer peut sauvegarder les fichiers dumps et les codes PIN sur la puce de la même carte, ou il peut imprimer les données de cartes collectées sur des tickets générés par le DAB.
Dans la plupart des cas, les criminels choisissent d'attendre pour collecter les données volées afin de créer des copies de ces cartes ultérieurement. Ils utilisent ces copies dans des DAB non infectés pour retirer de l'argent sur les comptes clients sans être inquiétés. De cette manière, ils s'assurent que les DAB infectés ne seront pas découverts. Et ils récupèrent de l'argent simplement.

Des voleurs expérimentés
Skimer a été largement répandu entre 2010 et 2013. À son arrivée correspond une augmentation drastique du nombre d'attaques sur des distributeurs automatiques de billets, avec jusqu'à neuf différentes familles de malwares identifiées par Kaspersky Lab. Cela inclut la famille Tyupkin, découverte en mars 2014, qui est devenue la plus populaire et la plus répandue. Cependant, il semblerait maintenant que Backdoor.Win32.Skimer soit de retour. Kaspersky Lab identifie 49 modifications de ce malware, dont 37 ciblent les DAB émanant de l'un des plus importants fabricants. La version la plus récente a été découverte en mai 2016.
En observant les échantillons partagés avec VirusTotal, on note que les DAB infectés sont répartis sur une large zone géographique. Les 20 derniers échantillons de la famille Skimer ont été téléchargés depuis plus de 10 régions à travers le monde : Émirats Arabes Unis, France, États-Unis, Russie, Macao, Chine, Philippines, Espagne, Allemagne, Géorgie, Pologne, Brésil, République Tchèque… [Lire la suite]
Remarquable article de Damien Bancal

Réagissez à cet article

Source : *Skimer, la nouvelle menace pour distributeurs de billets – Data Security BreachData Security Breach*

L’Écosse veut désactiver les téléphones utilisés en prison

L’Écosse veut désactiver les téléphones utilisés en prison

L'Écosse a trouvé possiblement une solution radicale pour lutter contre la présence des téléphones portables dans les prisons : elle veut tout simplement pouvoir faire désactiver la carte SIM en cause dans les mains des opérateurs.

Les tribunaux de shérif d'Écosse (ou «Sheriff courts») auront bientôt la compétence de contraindre les opérateurs télécoms à déconnecter les téléphones portables non autorisés dont on détecterait une utilisation en prison. Concrètement, le tribunal ordonnera à l'opérateur de réseaux de désactiver ou déconnecter un téléphone mobile et/ou une carte SIM. C'est le sens d'un texte qui vient d'être notifié à Bruxelles, cette disposition imposant une restriction normative dans un État membre.

Accéder aux réseaux sociaux, intimider les témoins

« *Des détenus ont utilisé des téléphones portables non autorisés pour accéder aux réseaux sociaux, intimider des témoins et poursuivre et contrôler leurs activités criminelles depuis les institutions pénitentiaires,* expliquent les autorités écossaises en appui de leur texte. *Ils représentent par conséquent une menace notable pour la sécurité et le bon fonctionnement des établissements pénitentiaires.* »

Le hic est qu'actuellement, « *il est extrêmement difficile de trouver à l'intérieur d'institutions pénitentiaires des cartes SIM en raison de leur taille. Si c'est moins le cas pour les téléphones portables, ces détenus qui ont pris possession de téléphones portables seront prêts à faire l'impossible pour empêcher la détection desdits téléphones, notamment par des menaces et l'intimidation d'autres personnes.* »

En France, le projet de loi sur la réforme pénale

Le texte pourra entrer en vigueur dans trois mois, une fois achevé le round de la notification bruxelloise. En France, si les pouvoirs du juge profitent théoriquement d'une large latitude pour ordonner ce type de mesure, dans le projet de loi sur la réforme pénale, la réaction du législateur gagne plusieurs crans au-dessus par rapport aux textes antérieurs.

D'un, le pénitentiaire va devenir un service du renseignement. De deux, les autorités, qu'elles soient judiciaires ou administratives et sans qu'on sache très bien où se placera la frontière de leurs compétences, pourront installer une ribambelle de dispositifs techniques pour détecter des communications, et notamment des IMSI catchers. De là, elles seront en capacité d'effectuer des interceptions de sécurité pour prendre connaissance des correspondances échangées avec l'extérieur, etc… [Lire la suite]

Marc Rees auteur de cet article

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

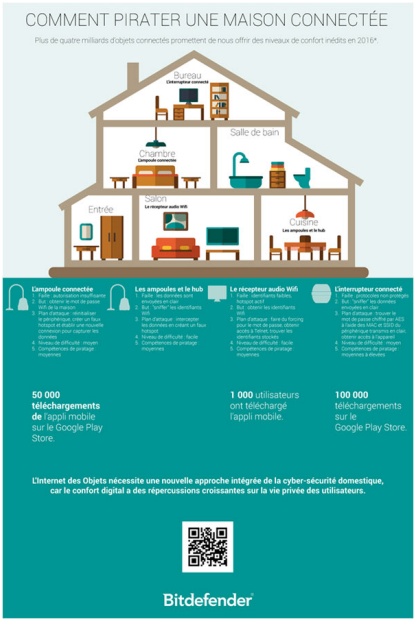
Source : *L'Écosse veut désactiver les téléphones utilisés en prison – Next INpact*

Est-ce facile de pirater une

maison connectée ?

	**Est-ce facile de pirater une maison connectée ?**

L'analyse révèle que les mécanismes d'authentification de ces objets connectés peuvent être contournés et donc exposer potentiellement les foyers et leurs occupants à une violation de leur vie privée. L'Internet des Objets pose des problèmes de sécurité spécifiques, et par conséquent, nécessite une nouvelle approche intégrée de la cyber-sécurité domestique, qui passe de la sécurité centrée sur le périphérique à une solution capable de protéger un nombre illimité d'appareils et d'intercepter les attaques là où elles se produisent : sur le réseau.



Les chercheurs des Bitdefender Labs ont réalisé une étude sur quatre périphériques de l'Internet des Objets (IdO) destinés au grand public, afin d'en savoir plus sur la sécurisation des données de l'utilisateur et les risques dans un foyer connecté :
1. **L'interrupteur connecté WeMo Switch** qui utilise le réseau WiFi existant pour contrôler les appareils électroniques (télévisions, lampes, chauffages, ventilateurs, etc.), quel que soit l'endroit où vous vous trouvez ;
2. **L'ampoule LED Lifx Bulb** connectée via WiFi, compatible avec Nest ;
3. Le kit **LinkHub**, incluant des**ampoules GE Link et un hub** pour gérer à distance les lampes, individuellement ou par groupes, les synchroniser avec d'autres périphériques connectés et automatiser l'éclairage selon l'emploi du temps ;
4. **Le récepteur audio Wifi Cobblestone de Muzo** pour diffuser de la musique depuis son smartphone ou sa tablette, via le réseau WiFi.
L'analyse révèle que les mécanismes d'authentification de ces objets connectés peuvent être contournés et donc exposer potentiellement les foyers et leurs occupants à **une violation de leur vie privée**. Les chercheurs de Bitdefender sont parvenus à découvrir le mot de passe pour accéder à l'objet connecté et à intercepter les identifiant et mot de passe WiFi de l'utilisateur.
Les **failles identifiées** par l'équipe de recherche Bitdefender concernent des protocoles non protégés et donc vulnérables, des autorisations et authentifications insuffisantes, un manque de chiffrement lors de la configuration via le hotspot (données envoyées en clair) ou encore des identifiants faibles.
L'IdO pose des problèmes de sécurité spécifiques, et par conséquent, nécessite **une nouvelle approche intégrée de la cyber-sécurité domestique**, qui passe de la sécurité centrée sur le périphérique à une solution capable de protéger un nombre illimité d'appareils et d'intercepter les attaques là où elles se produisent : **sur le réseau**.
Si des marques comme Philips et Apple ont créé un écosystème verrouillé, **l'interopérabilité reste essentielle** à ce stade du développement des nouveaux objets connectés. Il est donc plus que temps que les constructeurs prennent en compte nativement la sécurité dans le développement de leurs différents appareils… [Lire la suite]

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Source : *Comment pirater une maison connectée ?*

Hoverboards, solowheels et

autres gadgets roulants se préparent à conquérir Noël

Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël m

Noël 2016 sera encore placé sous le signe des gadgets roulants électriques. Au MedPi, les constructeurs alignent leurs gammes .

On ne découvre pas vraiment des produits que l'on ne connaissait pas au MedPi, mais comme il s'agit avant tout du supermarché des professionnels de la distribution, il est possible de sentir les tendances qui se dessineront pour les événements commerciaux français à venir – et en particulier la rentrée et Noël. Quand on découvre un gadget incroyable et qu'il n'est pas disponible en France, on sait que son adoption sera lente, réservée aux passionnés. Ici, nous sommes dans le réel, dans les rayons des grands magasins. Et le réel, en 2016, c'est beaucoup de choses qui roulent.
Si vous aviez des enfants en âge de commander un hoverboard à Noël dernier, vous pouvez être sûr qu'ils ne passeront pas à côté de la deuxième génération de ces produits qui ont envahi les rayons et se classent en premier rang des vidéos de chutes ridicules sur YouTube. En tout cas, au MedPi, on ne peut pas parcourir une allée sans voir au moins une marque ou un importateur qui cherche à placer dans les rayons ses engins à roues uniques, double roues parallèles, double roues sur un axe, double roues sur un axe avec selle… la liste est longue.

L'idée derrière ces engins ne différencie pas vraiment entre les modèles : il s'agit d'exploiter les performances actuelles des moteurs électriques et des batteries pour proposer des engins qui répondent aux problématiques de la mobilité urbaine. Il faut pouvoir se déplacer rapidement, sans risque majeur de chute… et sans effort. Ce dernier point pourrait paraître regrettable, mais nous nous sommes aperçus dans notre premier test d'une trottinette électrique qu'elle ne remplaçait pas, naturellement, les trajets que l'on aurait fait à pied ou en vélo, mais bien plus volontiers les trajets en transports en commun. En somme, les plus pénibles.
Bien entendu, sur ce secteur, le bon grain côtoie l'ivraie. Les marques les plus réputées comme Ninebot, qui possède Segway, ont des brevets et de nombreuses innovations dans leur portefeuille en plus d'avoir des appareils de grande qualité, autostabilisés. Les autres rattrapent leur retard ou proposent des ersatz de technologies pas vraiment convaincantes (ni légales), laissant sur le carreau tout le côté stable des engins qu'ils proposent, les faisant entrer dans la catégorie « jouets pour ados » plus que dans celle de la mobilité urbaine. Et pour un Ninebot ou équivalent, il y a au moins 3 constructeurs aux noms étranges dans les allées du MedPi.
Plusieurs problématiques restent d'ailleurs à résoudre pour que ce marché explose véritablement. La première, c'est bien entendu la question de la sécurité des utilisateurs : les hoverboards qui ont assailli l'Europe et les États-Unis l'an passé étaient loin d'être tous conformes aux régulations en vigueur en matière d'électronique et plusieurs affaires de batteries défectueuses ou anormalement inflammables avaient conduit au bannissement de certains modèles, notamment vendus par Amazon.
Ensuite vient la route – ou les trottoirs. Où doivent rouler ces engins ? Sur les trottoirs, ils peuvent être dangereux pour les piétons et pour eux-mêmes, dans la mesure où les voies piétonnes sont pavées d'obstacles contre lesquels les personnes en chaise roulante doivent lutter depuis longtemps, malheureusement. Sur la route, c'est l'utilisateur qui devient vulnérable, debout en équilibre, lancé à plusieurs dizaines de kilomètres par heure. On l'imagine mal à l'aise dans les croisements. Si les voies pour les vélos étaient massivement installées, comme chez nos voisins hollandais, la question ne se poserait pas.
En France, elle est encore ouverte : peut-être est-il temps que les municipalités s'en emparent avant que nous ayons à écrire des articles sur les premiers accidents graves. Même si les hoverboards ne volent (presque) toujours pas… [Lire la suite]

Réagissez à cet article

Source : *Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël – Tech – Numerama*

BMW lance un défi aux startups françaises pour améliorer la voiture de demain

	**BMW lance un défi aux startups françaises pour améliorer la voiture de demain**

Le BMW Tech_Date, prévu pour le 9 juin prochain, est un concours ouvert aux startups françaises. Ces dernières doivent y présenter des innovations intégrables dans les voitures intelligentes conçues par le constructeur.

BMW sollicite les startups françaises. Le constructeur automobile organise le 9 juin prochain la première édition du BMW Tech_Date dans son magasin des Champs Élysées à Paris. L'objectif : accélérer la construction de la mobilité des cent prochaines années.
Ce concours permettra aux startups de présenter des innovations qu'elles pensent pouvoir intégrer aux futures voitures intelligentes de BMW. C'est en tout cas ce que souhaite le constructeur.
« Nous avons les technologies pour rendre la voiture intelligente mais nous sommes en recherche constante de solutions qui peuvent rendre l'usage de la voiture plus intelligent », explique Pierre Jalady, responsable marketing de BMW en France, dans une interview au Journal du Net. L'entreprise souhaite en effet adapter ses services pour qu'ils soient plus centrés sur l'utilisateur.
Les startups ont jusqu'au 30 mai pour candidater. Une vingtaine d'entre elles seront sélectionnées pour le Tech_Date afin de présenter leurs technologies devant un jury qualifié.

Trois vainqueurs seront désignés en fonction de plusieurs critères dont :
• niveau d'innovation de la solution proposée
• le délai d'intégration potentiel pour BMW
• D'autres éléments seront pris en compte tels que le niveau préexistant de relations commerciales avec l'industrie automobile, la solidité de la société et la communauté fédérée par les startups sur les réseaux sociaux.
Les trois gagnants « seront reçus pendant une semaine au siège de Munich, où ils rencontreront toutes les équipes qui auront un intérêt à travailler avec eux, des achats au marketing. Ils seront aussi mis en avant au Mondial de l'automobile de Paris en octobre prochain », affirme Pierre Jalady.
Ce concours a également pour but de célébrer le siècle d'existence de BMW qui fêtait son anniversaire en mars dernier. Le constructeur estime que le Tech_Date est une occasion de mettre en lumière les innovations françaises et déclare vouloir travailler en partenariat avec les entreprises les plus créatives.
Crédit photo de la une : BMW… [Lire la suite]

Réagissez à cet article

Source : *BMW lance un défi aux startups françaises pour améliorer la voiture de demain – Tech – Numerama*

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

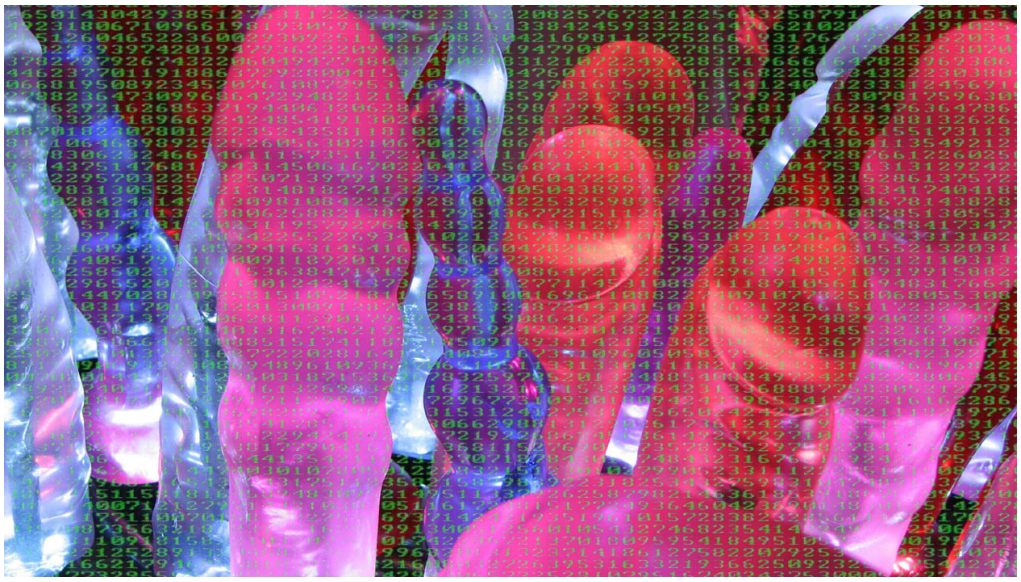
EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*

Piratage de sextoys ! Que faut il craindre ?



Piratage de sextoys ! Que faut il craindre ?

Un éditeur de logiciels de sécurité a mis en lumière le danger que représentent les objets connectés en piratant un vibromasseur. De quoi limiter le potentiel ludique de l'engin!

Les hackers pourront peut-être pourrir nos vies jusque dans notre plus stricte intimité… c'est en tous les cas ce qu'ont essayé de démontrer des ingénieurs de l'éditeur de logiciels de sécurité Trend Micro au salon informatique allemand CeBit qui vient de s'achever à Hanovre.

Les attaques récentes contre les données informatiques d'un… hôpital nous ont mis en garde sur l'impact que peut avoir le piratage sur les systèmes professionnels connectés, mais la menace concerne tous les objets connectés. Y compris les sextoys !

Face à un panel de journalistes, un ingénieur de Trend Micro a en effet piraté un vibromasseur en l'allumant à distance, une action qui a s'abord provoqué l'hilarité, selon l'agence Reuters qui rapporte les faits. Cité par l'agence, le responsable de la technologie de l'éditeur a affirmé que si un « hacker un vibromasseur est amusant […] mais si j'accède au back end (le logiciel de contrôle, ndr) je peux faire chanter le constructeur ».

Un individu mal intentionné et assez qualifié pourrait tout à fait contrôler la vitesse du moteur de l'appareil, accélération qui pourrait potentiellement mener à sa destruction… limitant ainsi son potentiel ludique !

Si nous commençons à nous habituer aux piratages d'infrastructures, le fait que de plus en plus d'objets soient connectés – à nos smartphones voire directement à internet – ne va faire qu'augmenter le périmètre des menaces potentielles.

Espérons que les constructeurs n'attendent pas d'incidents graves pour prendre les mesures de sécurité qui s'imposent…. [Lire la suite]

Réagissez à cet article

Source : *Tout ce qui est connecté peut être piraté, y compris… les sextoys!*

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

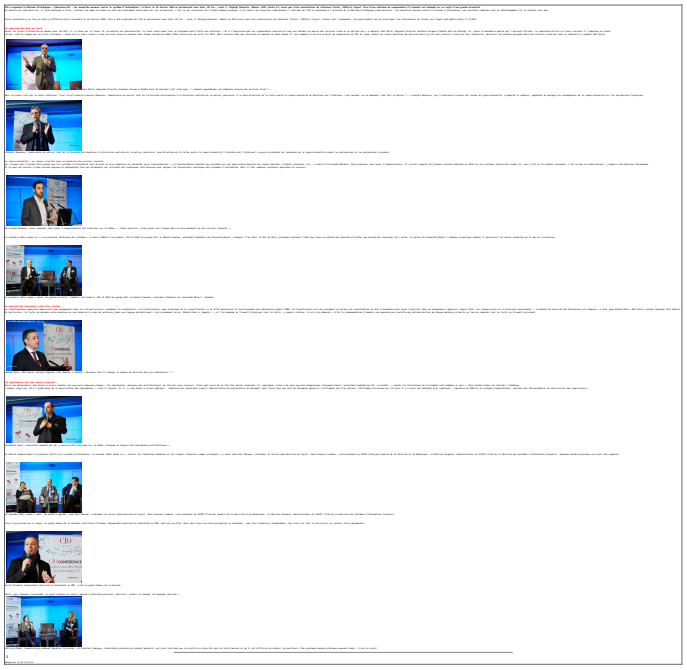
Ce n'est pas la première fois que les capteurs d'empreinte digitale sont floués par des tentatives de piratage. Mais jusqu'alors les techniques utilisées reposaient sur de l'impression 3D et des moules spécifiques. Cette nouvelle méthode s'avère de fait bien moins onéreuse, et bien plus rapide. De quoi 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 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*

Des données personnelles de développeurs trouvés dans des caméras de surveillance

Des données personnelles de développeurs trouvés dans des caméras de surveillance

Gmail, Dropbox et comptes FTP, voici ce qu'ont laissé des développeurs dans les entrailles des caméras sur lesquelles ils travaillaient. Des informations personnelles qui montrent le manque de vigilance de ces techniciens, ayant utilisés leurs comptes privés lors du développement de ces caméras… Une affaire qui pourrait faire tâche sur les CV de ces indélicats !

Selon un article de Forbes, des développeurs ayant travaillé sur la création du software pour les caméras Motorola Focus 73 ont fait preuve d'un manque de vigilance flagrant au moment de finaliser leur travail, juste avant la commercialisation de ce modèle. Des experts de « Context Information Security » sont parvenus à accéder aux entrailles des caméras, et on pu en extraire plusieurs informations suprenantes. Les développeurs y avaient laissé trainer leurs identifiants Gmail, Dropbox et FTP d'entreprise.
Les caméra, facilement piratées et contrôlables à distance pour quiconque ayant un minimum de connaissance dans le domaine, ont apporté la preuve de la négligence de ces développeurs, comma l'a expliqué le responsable de Context Information Security :
Les comptes laissés dans le firmware sont apparus comme étant des comptes de développeurs partagés, utilisés pour recevoir les alertes de mouvement et les extraits de vidéo pour leurs tests. Nous n'avons pas accédé à ces comptes pour des raisons légales, mais nous avions tout ce qu'il nous fallait pour le faire. (…) On ne s'attend pas à ce qu'une entreprise de développement utilise ce type de comptes pour ce genre d'activité et ils n'auraient certainement pas du être laissés dans le firmware final.
Un constat d'autant plus affligeant que les mots de passe utilisés pour la sécurité des caméras et ces comptes Gmail sont plus que décevants : « 000000 » ou « 123456 ».

Réagissez à cet article

Source : *Gmail : des données personnelles de développeurs trouvés dans des caméras de surveillance – 1001Web*