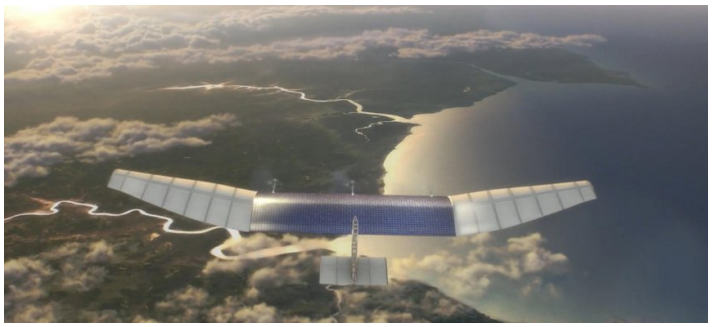
Boeing planche sur des drones capables de déployer des logiciels espions | Le Net Expert Informatique



Boeing planche sur des drones capables de déployer des logiciels espions

Le spécialiste de l'aéronautique Boeing travaille sur la production de drones capables d'infecter les ordinateurs et smartphones aux alentours.

En début de mois, nous apprenions que la société milanaise Hacking Team, qui propose des outils d'interception des communications entre internautes aux gouvernements ou aux pouvoirs publics, avait elle-même été hackée. Quelque 400 gigaoctets de données confidentielles ont été récupérés révélant la nature des relations entre Hacking Team et ses partenaires. Ces documents sont mis à disposition sur le site Wikileaks.
Parmi les informations révélées, la filiale Insitu de Boeing, spécialisée dans la production de drones, avait signé un partenariat avec Hacking Team afin de procéder à des hacks à distance. L'appareil serait ainsi en mesure de cibler un smartphone ou un ordinateur portable en particulier puis de l'infiltrer via un réseau Wi-Fi.
Selon le magazine The Intercept, qui rapporte l'information, le drone en question est prévu pour pouvoir accéder aux fichiers à distance, récupérer le journal des appels, l'historique des messageries instantanées ou encore les emails.
Au sein des emails aspirés sur les serveurs de Hacking team, nous trouvons notamment une feuille de route datant du mois de juin. Celle-ci fait mention d'un petit appareil pouvant être transporté par un drone et capable de récupérer les données transitant via les réseaux.
Le document explique que l'attaque devra prendre en charge Windows 10 ainsi que le navigateur Microsoft Edge et Skype Web. Sur OS X, Hacking Team a finalisé un dispositif scannant les sauvegardes locales d'iTunes et planchait sur la capture des certificats d'iCloud et des images de l'application Photos.
Retrouvez tous les détails de ce projet en italien sur cette page.

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.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spyware-logiciel-espion/actualite-774222-boeing-planche-drones-capables-deployer-spyware.html

---

Alerte partagez – Nouvelle faille Android…| Le Net

Expert Informatique

	**Alerte partagez – Nouvelle faille Android…**

En début de semaine l'affaire Stagefright révélait une faille majeure sur Android. Trend Micro en remet aujourd'hui une couche dévoilant une nouvelle faille critique. Non patchée par Google assure l'expert en sécurité.

Dure semaine pour Android. Trend Micro annonce la découvre d'une nouvelle faille qui cette fois permet de rendre le téléphone non fonctionnel. En début de semaine, l'affaire Stagefright avait déjà ébranlé l'aura de Google. Aucun correctif n'est encore disponible.
Quand cette faille est exploitée avec succès, le téléphone équipé d'Android devient silencieux. Plus d'alertes sur les messages, plus de sonnerie d'appel. Rien. Puis le téléphone se grippe, peu à peu, et s'arrête. La faille « est causée par un débordement d'entier lorsque le service de mediaserver analyse un fichier MKV. Il lit la mémoire de tampon ou écrit des données à l'adresse NULL lors de l'analyse des données audio » analyse Trend Micro.

Jelly Bean et Lollipop touchés
« La vulnérabilité réside dans le service mediaserver, qui est utilisé par Android pour les index de fichiers multimédias qui sont situés sur le périphérique Android. Ce service ne peut pas traiter correctement un fichier vidéo malformé utilisant le conteneur Matroska (généralement avec l'extension. mkv). Lorsque le processus ouvre un fichier MKV malformé, le service peut se bloquer (et avec lui, le reste du système d'exploitation) » explique Trend Micro.
Cette faille de sécurité peut être exploitée en incitant un internaute à visiter un site infecté, ou en lui faisant télécharger une application vérolée. Les versions d'Android impactées par cette faille courent d'Android 4.3 (Jelly Bean) à Android 5.1.1 (Lollipop).
Trend Micro a informé discrètement Google en mai dernier, mais l'entreprise n'aurait pas classé cette faille autrement qu'une «vulnérabilité de faible priorité », selon Trend Micro. Conséquence : aucun patch n'a été publié. Trend Micro prend donc aujourd'hui les devants et rend public cette faille, espérant que Google ait la même réactivité qu'avec Stagefright. Et Trend Micro en profite bien sûr pour faire la publicité de ses solutions, qui évidemment, protègent des complications de Google.

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

Source : http://www.zdnet.fr/actualites/android-a-nouveau-victime-d-une-faille-39823130.htm

---

Des chercheurs développent une étonnante attaque web sur

la DRAM | Le Net Expert Informatique

Des chercheurs développent une étonnante attaque web sur la DRAM

Des chercheurs ont réussi à exploiter un défaut nommé « Rowhammer » qui inquiéte depuis longtemps les experts de la sécurité informatique. Leur attaque, menée depuis le web, s'appuie sur JavaScript et cible la DRAM des ordinateurs, exposant des millions d'internautes.

On sait depuis plusieurs années que les cellules mémoire des ordinateurs sont vulnérables à une interférence intentionnelle. Mais un récent document de recherche explique comment mener une attaque depuis le web qui augmente considérablement le danger pour les utilisateurs. Ce document, publié par des institutions autrichiennes et françaises – il a été coécrit par Daniel Gruss et Stefan Mangard de l'Université de Technologie de Graz en Autriche, et par Clémentine Maurice de Technicolor et Eurecom en France – pourrait obliger les fondeurs à trouver en urgence une solution qui résout le défaut connu sous le nom de « Rowhammer ».
Pour augmenter la densité de la DRAM, les concepteurs n'ont cessé de rapprocher les cellules, les rendant vulnérables aux interférences électriques. Une technique décrite sous le nom de « rowhammering » permet de changer la valeur binaire des cellules adjacentes en activant de manière répétée une rangée donnée de cellules de mémoire. Pendant longtemps, les concepteurs se sont préoccupés de la fiabilité posée par cette fuite électrique, sans considérer la question de la sécurité. Mais cette approche est en train de changer rapidement.

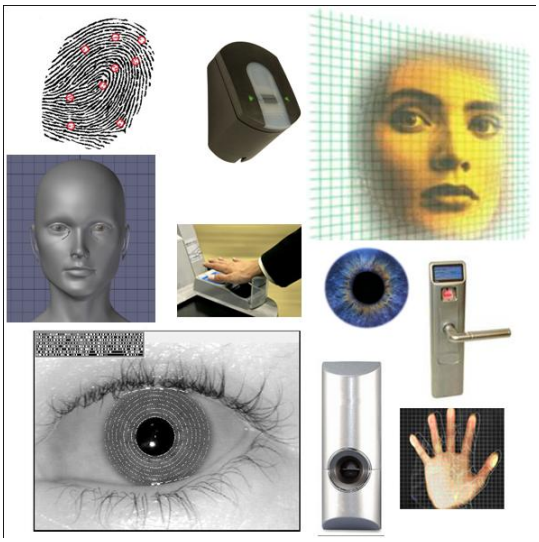
Une attaque à distance en JavaScript
Plus tôt cette année, des chercheurs de Google ont annoncé qu'ils avaient réussi à développer deux exploits opérationnels : le premier leur a permis de mener une attaque par escalade de privilège et l'autre utilise le changement de polarité induit par le défaut « Rowhammer » pour obtenir des privilèges au niveau du noyau. Mais, pour que l'attaque réussisse, ils avaient été obligés d'installer leurs exploits sur la machine de l'utilisateur. Ce qui est remarquable dans ce nouveau document, c'est qu'une telle attaque pourrait être menée depuis le web en s'appuyant sur JavaScript. Le code proof-of-concept Rowhammer.js a été testé dans Firefox 39, « mais notre technique d'attaque est générique et peut être appliquée avec tout type d'architecture, de langage de programmation et d'environnement runtime », ont-ils écrit. Elle ne nécessite pas un accès physique à un ordinateur, ce qui la rend beaucoup plus dangereuse.
Cela signifie également qu'un grand nombre de personnes pourraient être ciblées depuis le web, ce qui augmente le pool de victimes potentielles. « Étant donné que l'attaque peut être lancée simultanément et furtivement contre un nombre arbitraire de machines, elle représente une énorme menace pour la sécurité », ont-ils ajouté. De plus, un grand nombre d'ordinateurs sont vulnérables, puisque l'attaque est indépendante du système d'exploitation, et que le bug « Rowhammer » affecte de nombreux types d'architectures de puces. Les chercheurs essayent encore de savoir combien de systèmes seraient vulnérables à leur attaque. Jusqu'à présent, ils n'ont pas développé d'exploit qui permettrait d'obtenir un accès root à un ordinateur en exploitant le « rowhammering », mais ils pensent que des pirates pourraient éventuellement étendre les capacités de l'exploit qu'ils ont découvert.

Bloquer JavaScript avec NoScript
Tant que les fondeurs ne trouvent pas de solution à long terme pour résoudre le problème Rowhammer.js, les chercheurs proposent d'inclure dans les navigateurs web un test permettant de vérifier si l'ordinateur est vulnérable. Si le test est positif, « JavaScript doit être mis sous contrôle pour éliminer la possibilité d'un exploit. Même si le système est très probablement résistant, il faut laisser à l'utilisateur la possibilité d'activer explicitement JavaScript quand il visite une page web », écrivent-ils. Une autre alternative serait de désactiver complètement JavaScript en utilisant une extension comme NoScript. Mais de nombreux sites web reposent sur JavaScript et sans lui, la consultation de ces sites devient problématique.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-des-chercheurs-developpent-une-etonnante-attaque-web-sur-la-dram-61920.html
Par Jean Elyan et IDG NS

Les risques d’avoir votre mot de passe écrit dans votre corps | Le Net Expert Informatique



Les risques d’avoir votre mot de passe écrit dans votre corps

Reconnaissance faciale, empreinte digitale, reconnaissance vocale… Les marques du secteur du numérique rivalisent d'ingéniosité pour trouver des clés de sécurité en utilisant les données biométriques. Le corps humain est-il devenu « le nouveau mot de passe », l'ultime rempart le plus à même de se protéger contre le piratage de ses données personnelles ?

Jean-Paul Pinte : Comme je le précisais encore il y a deux mois dans différents articles « Rien n'est inattaquable ». Le corps humain non plus.
Penser que protéger des données au sein du corps humain en faisant de notre corps l'ultime carapace de protection de notre identité et de nos données personnelles n'est pas nouveau.
Elle ne constitue pas non plus à non sens l'unique solution face aux piratages. Le sujet est certes d'actualité et d'autant plus pertinent que l'on est entré dans l'époque de la traque du renseignement.
En 2002 on évoquait déjà l'avenir de la biométrie dans le Journal du Net. Voici ce que l'on en disait « avec la reconnaissance d'iris et d'empreintes digitales, « scan » de la main et analyse de la voix, autant de technologies qui se banalisent – et qui ne méritent plus leur place dans les films d'anticipation ». Mais patience, nous avons volontairement écarté de notre dossier les technologies qui ne sont pas tout à fait mûres, ainsi que celles qui sont en cours de développement.
Dans quelques années, on devrait ainsi entendre parler de biométrie comportementale, de thermographie et d'ADN. Pour l'instant, ces techniques sont encore dans les laboratoires, mais elles vont progressivement venir renforcer l'arsenal de l'authentification.
Les futurs modes d'identification seront basés et fondés, c'est sûr, en grande partie sur l'analyse de notre corps : rétines, activité cérébrale ou encore la forme de nos veines. Donc des solutions basées sur l'homme. Intel annonçait d'ailleurs, dans ce sens, le lancement de True Key, un système d'identification sécurisé par le biais de la reconnaissance faciale.
Dans un article de l'Atelier du Net on peut également lire que des chercheurs de l'université de Rutgers aux États-Unis, en collaboration avec l'Institut Max Planck et l'université d'Helsinki se sont, quant à eux, penchés sur le dessin ou les formes libres en tant que mot de passe. Ils présenteraient notamment des atouts significatifs en matière de sécurité.

Par

François Dominic Laramée dans un article de « Branches vous » évoque des chercheurs de l'université de Binghamptom, dans l'État de New York, tentant de développer une méthode potentiellement infaillible pour identifier un individu : lire la «signature» de son cerveau.

Aujourd'hui la NSA s'intéresse également à la reconnaissance d'écriture. Après la reconnaissance vocale, la biométrie et son cortège (empreinte digitale, ADN, iris), Facebook cherche à nous reconnaître visage caché. Une technique qui devrait servir encore plus la surveillance.

Paypal investirra une pilule pour que notre corps devienne le meilleur des mots de passe. J'en parlais encore il y a peu de temps.

Toutes ces avancées technologiques, ont pour certaines, fait leurs preuves mais ne sont pas forcément source de fiabilité !

Cette nouvelle technologie, qui utilise les données biométriques, est-elle pour autant (plus) « fiable », moins facile à pirater ?
Jean-Paul Pinte : Il y a encore du travail avant de confirmer définitivement la fiabilité de la technologie biométrique. En effet, comme pour tout domaine d'activité, elle n'échappe pas aux cyber-délinquants qui semblent toujours avoir ce pas d'avance et des parades pour arriver à leurs fins.

Pour la CNIL la biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Les données biométriques sont des données à caractère personnel car elles permettent de trouver ou de vérifier l'identité d'une personne. Ces données ont, pour la plupart, la particularité d'être uniques et stables dans le temps (ADN, empreintes digitales…).

En dix ans, la biométrie a su trouver sa place dans de nombreux domaines, excepté celui de l'authentification. L'empreinte digitale reste encore facilement falsifiable. La technologie par la voix a certes beaucoup évoluée, mais elle n'est utilisée que pour de la dictée ou des commandes vocales. La reconnaissance faciale a trouvé sa place dans la vidéosurveillance, où elle excelle dans l'identification biométrique.

L'iris demeure encore trop mobile pour les capteurs du marché et bute sur des questions de coût. Il bouge beaucoup trop pour réussir une capture fiable, et rares sont les appareils (téléphones ou webcam) équipés d'un capteur suffisamment précis pour réaliser cette empreinte.

S'il s'avère qu'elle n'est pas invulnérable au piratage, quel recours est alors possible ? Que peut-on utiliser d'autre que le corps humain comme moyen de protéger ses données personnelles ?
Quelques projets de recherche ont été menés pour développer des technologies biométriques plus protectrices de la vie privée. Biométrie révocable, anonyme ou cryptage biométrique pourraient être la solution pour concilier confort et vie privée.

Le site Biométrie Online aborde les travaux de thèse professionnelle de Marion Briquet sur le thème « Usages non régaliens de la biométrie : quel équilibre entre confort et vie privée ? ». Cette dernière reprend les avancées des technologies suivantes :

Biométrie « non traçable »
L'objectif de ces technologies de biométrie « untraceable » est de transformer de manière irréversible les données biométriques de la personne afin de ne pas pouvoir remonter jusqu'à elle en les utilisant (« data connectivity »). La notion de « traçabilité » ne se rapporte pas ici à la notion de trace physique laissée par la personne, via ses empreintes digitales par exemple, mais concerne plutôt la façon dont on peut retrouver son identité en utilisant un gabarit de ses données biométriques, laissé dans tel ou tel système.

Cryptage biométrique
Le cryptage biométrique permet de transformer de manière irréversible les données biométriques en données qui ne contiennent aucune information – sur les données biométriques- sources fournies par la personne. Ainsi, aucune donnée biométrique n'est conservée, ni aucun gabarit biométrique.

Biométrie révocable
La biométrie révocable fait également partie des technologies de biométrie non traçable. Il s'agit dans ce cas de créer, à partir de la donnée biométrique, un gabarit « transformé » et non biométrique qui sera le seul conservé. La donnée biométrique n'est pas conservée, comme pour le cryptage biométrique. La comparaison se fait entre les deux gabarits « transformés ». Il est ici aussi possible d'annuler et de renouveler un gabarit.

Biométrie anonyme
Enfin, la biométrie anonyme ou « désidentifiée » (terme préféré par la CNIL) est un dispositif dans lequel les données biométriques ne sont reliées à aucune donnée personnelle permettant d'identifier la personne. Il n'y a pas d'interconnexion avec un autre système où elle pourrait être identifiée. Elle peut être utilisée pour les dispositifs d'authentification seulement, en utilisant par exemple, un tiers de confiance qui authentifierait la donnée biométrique à la demande de la personne ou du fournisseur de service. La seule donnée communiquée serait un numéro de transaction. Cela demanderait de la part du tiers de confiance qu'il mette en place des procédures sécurisées et adéquates d'enrôlement, de conservation, de comparaison…

En dehors de ces recherches approfondies et pour protéger vos données biométriques personnelles le capteur biométrique de la montre Biowatch se met à l'heure du progrès et des objets connectés. C'est ainsi qu'il apparaît plus sûr qu'un autre système d'identification corporel.

Avec la biométrie des veines, les vaisseaux sanguins sont illuminés par une lumière infrarouge qui pénètre de quelques millimètres sous la peau en vue d'analyser précisément les veines. Faire un fake du schéma veineux d'un individu est donc quasi impossible. On imagine vite les avantages de cette technologie car cette identification absolue permet de pallier la perte des mots de passe ou l'égarement de clés voire de cartes d'accès.

Quel type de nouvelle délinquance cela peut-il entraîner ? Assistera-t-on – ou assiste-t-on déjà – par exemple à l'amputation d'un doigt pour récupérer les empreintes digitales ?
Jean-Paul Pinte : Parmi toutes les données biométriques utilisées aujourd'hui l'empreinte digitale présente la caractéristique d'être une « biométrie à trace ». En effet, chaque personne laisse des traces de ses empreintes digitales, plus ou moins exploitables dans beaucoup de circonstance de la vie courante signale la CNIL dans ce dossier.

Par exemple, sur un verre ou une poignée de porte.
A noter que c'est aussi le cas des empreintes génétiques. D'autres biométries ne présentent pas cette spécificité comme le contour de la main ou le réseau veineux en l'état actuel de la technologie nous signale encore la CNIL.

Je vous laisse simplement imaginer le détournement d'une empreinte pour l'identification d'un smartphone et ses dérives possibles aux données contenues dans l'appareil et la projection de cet acte au simple fait d'utiliser cette empreinte dans un paiement ou une identification biométrique. Les gens doivent savoir que l'on collecte des données à leur insu et le risque possible pourrait venir justement de l'utilisation secrète de ces données biométriques, du seul fait que les données sont accessibles au public (photographie des gens, système de balayage des yeux perceptibles à deux mètres, captation des réseaux veineux de la paume de la main et des doigts).

Dans le cas de plusieurs types d'échange avec L'État, les personnes n'ont souvent d'autres choix que de se résoudre à communiquer des renseignements personnels qui sont souvent de nature délicate, et ce, parfois en grande quantité. En effet, les données personnelles sont souvent la monnaie d'échange permettant de bénéficier des programmes, des services ou des prestations du gouvernement.

Dans quels domaines cet enjeu est-il le plus prégnant ? On pense par exemple au piratage des données d'entraînement de Chris Froome, le coureur cycliste, ou à la possibilité qui existe par exemple désormais de pirater à distance un pacemaker.
Jean-Paul Pinte : La biométrie est la mesure d'éléments biologiques, comportementaux ou physiologiques uniques et propres à chaque individu. Ses domaines d'action ne manquent donc pas dans notre société mais c'est surtout dans les domaines du Big Data et de l'Open Data, qui touchent entre autres à nos données de santé, qu'il y a de quoi s'inquiéter dès maintenant.

Le risque réside principalement dans la captation des données, leur prise en main et leur exploitation par des personnes mal intentionnées.

La Falco Wheel , dernier vélo fabriqué par une entreprise américaine peut fonctionner comme un outil d'entraînement sportif, mais aussi comme un système de contrôle du rythme cardiaque. Il suffit d'enregistrer, via une application smartphone dédiée, le nombre de pulsations à atteindre ou à ne pas dépasser pendant l'effort. Le dispositif s'occupe du reste. Il en va de même pour le T-Shirt biométrique. Toutes les données sont aujourd'hui facilement traçables voire captables à distance.

Jusqu'ici rien de trop grave dirons-nous ? Allons plus loin et revenons en 2012 avec l'expérience faite uniquement à des fins de preuve de concept. Jack Barnaby a effectué un peu de reverse engineering sur le transmetteur d'un pacemaker. Il a ainsi pu, non seulement, réécrire le firmware de ces appareils mais aussi (et surtout) déclencher des chocs électriques mortels de 830 volts, le tout à une distance d'un peu plus de neuf mètres depuis un simple ordinateur portable.

Le pire résiderait enfin dans le vol de données biométriques effectué sous la menace en vue de diffusion, voire encore de chantage à la donnée comme cela se pratique déjà sur la toile !

Source : http://www.atlantico.fr/decryptage/votre-corps-comme-mot-passe-rempart-contre-piratage-donnees-qui-est-pas-sans-risque-jean-paul-pinte-2242870.html
Par Atlantico et Jean-Paul Pinte

Un drone mis au point contre les incendies de forêt | La foire du drone | Le Net Expert Informatique

Un drone mis au point contre les incendies de forêt

Le drone est moins cher, plus souple d'utilisation qu'un hélicoptère et, souvent, moins dangereux. Ces arguments font déja mouche dans l'audiovisuel, la supervision agricole, la surveillance des ouvrages d'art mais aussi sur le terrain du maintien de l'ordre puisque la gendarmerie va se doter, dans ce but, d'une flotte d'une vingtaine de petits appareils sans pilote, selon Le Parisien.

Les drones pourraient, demain, également changer la donne dans le domaine de la sécurité civile, plus particulièrement en matière de prévention et de lutte contre les incendies de forêt.

Conçu par la société catalane Singular Aircraft, installée à Barcelone et à Malte, le Flyox 1 est un gros hydravion sans pilote. Apparemment, il s'agit du plus imposant drone civil qui existe à l'heure actuelle. Cet engin volant mesure 11,50 mètres de longueur pour 14 mètres d'envergure et pèse 1 750 kilos. Il peut emporter un chargement de deux tonnes, décoller (sur 313 mètres) ou atterrir (209 mètres lui suffisent) sur une piste classique, l'eau ou des marécages. Il peut rester 6 heures et 45 minutes en vol. Flyox 1 – dommage qu'il ait hérité d'un nom qui fleure bon le produit antimoustiques – a réalisé un premier test grandeur nature mi-mai en Islande où il a effectué un vol de 457 kilomètres sans perturber le trafic aérien autour de l'aéroport de Reykjavik.

Singular Aircraft

« Chaque année, environ une centaine de pompiers meurent (…). Flyox 1 souhaite mettre fin à ces statistiques en surveillant les forêts, en détectant de façon précoce les incendies et en les éteignant », affirme l'entreprise. Singular Aircraft assure que son gros hydravion peut larguer un peu plus de deux mille litres d'eau ou de produit retardant. Ses caractéristiques d'aéronef dépourvu de pilote lui permettent de multiplier les passages (ravitaillements compris, il peut fonctionner plus de cinquante heures d'affilée) et les vols nocturnes ne lui posent aucun problème. Cet appareil peut aussi, assurent ses inventeurs, surveiller les frontières et porter assistance ou encore transporter du fret vers des zones inhospitalières et les parachuter.

Eléments du tableau de commande du Flyox (Singular Aircraft)

Apparemment opérationnel au plan technique, le plus dur commence pour Flyox 1. Même si son promoteur fait valoir que son coût d'utilisation est très largement avantageux – mais ne fournit pas vraiment de données chiffrées –, ce drone-hydravion à très large rayon d'action risque fort de représenter un coût d'acquisition très élevé pour les collectivités. Il devra donc faire la démonstration de son efficacité, ce qui passe sans doute par la capacité de ne pas cantonner chaque appareil à un seul type d'usage. Sur ce terrain des gros drones civils, la concurrence ne manque pas. A commencer par celle des grands groupes déjà présents sur le secteur du drone militaire.

Source : http://drones.blog.lemonde.fr/2015/07/19/un-drone-mis-au-point-contre-les-incendies-de-foret/

Alerte à partager : Une faille sur Android à corriger d’urgence | Le Net Expert Informatique

	Alerte à partager : Une faille sur Android à corriger d’urgence

Si votre fournisseur de smartphone ou de tablette ne patche pas Stagefright de lui même, ce malware basé sur l'envoi de MMS peut être vraiment effrayant. Mais vous pouvez vous en protéger en respectant quelques étapes.

Franchement, la plupart des gens qui reçoivent les logiciels malveillants recherchent les ennuis. Ils ouvrent un fichier suspect envoyé par une personne qu'ils ne connaissent pas, vont sur un site Internet mal famé, voire téléchargent le dernier film ou jeu à la mode sur BitTorrent. Mais Stagefright, c'est différent. Ce logiciel malveillant basée sur une faille de sécurité se déclenche en recevant un MMS sur un appareil Android non patchées. Et bang, vous êtes piraté.
Stagefright peut attaquer tout smartphone Android, tablette, ou un autre dispositif fonctionnant sous Android 2.2 ou supérieur. Des approximativement quelque 1 milliard de gadgets Android présents sur le marché, Stagefright pourrait, en théorie, toucher 95% d'entre eux. Joshua J. Drake, le vice-président de Zimperium zLabs qui a découvert Stagefright prétend qu'il est parmi les « pires vulnérabilités Android découvertes à ce jour ».
Car la partie vraiment sournoise est qu'il n'est pas nécessaire de consulter le MMS pour être infecté. Si vous utilisez l'application Hangouts de Google , vous êtes infectés sans même consulter cette application de messagerie si l'on vous fait parvenir ce message.

Un malware pas comme les autres
Tout ce que l'attaquant a besoin de faire est d'envoyer ce paquet empoisonné à votre numéro de téléphone. Il allume alors votre appareil, et l'attaque commence. Cela peut arriver si vite que le temps que votre téléphone vous avertisse qu'un message est arrivé, vous avez déjà été piraté. Si par ailleurs vous utilisez l'application native de messagerie proposée avec Android, vous devez ouvrir le MMS, mais pas nécessairement déclencher la vidéo, pour être infecté.
Ce détournement de la sécurité d'Android fonctionne en profitant de la bibliothèque Stagefright incluse dans Android. Ce moteur de lecture multimedia est fourni avec des codecs basés sur des logiciels pour lire plusieurs formats de médias populaires. La faille de sécurité semble provenir du fait que pour réduire la latence de l'affichage vidéo Stagefright traite automatiquement la vidéo avant même que vous ne vouliez la regarder. Joshua J. Drake va révéler les détails de du fonctionnement de Stagefright au Black Hat début Août.

Google a été réactif…
Zimperium à informé Google du problème en Avril. Selon Drake, « Google a agi promptement et appliqué les correctifs à des branches de code interne sous 48 heures ». Une porte-parole de Google mentionne dans une réponse par e-mail : « Nous avons déjà répondu rapidement (…) en envoyant le correctif pour tous les appareils Android à nos partenaires ».

Elle ajoute :
La sécurité est renforcée dans Android : les applications Android sont exécutées dans ce que nous appelons une « sandbox d'application ». De la même manière qu'un bac à sable empêche le sable de sortir, chaque application est installée dans une « sandbox » virtuelle pour l'empêcher d'accéder à autre chose qu'à ses propres composants, ce qui signifie que même si un utilisateur devait installer accidentellement un morceau de malware, il lui est interdit d'accéder à d'autres parties du dispositif.
L'ouverture de l'écosystème améliore la sécurité et rend Android plus puissant. Comme Android est open source, tout le monde peut l'examiner pour comprendre comment il fonctionne et d'identifier les risques potentiels de sécurité. Toute personne peut mener des recherches et faire des contributions pour améliorer la sécurité d'Android.
Google encourage la recherche en matière de sécurité : le programme de récompenses de sécurité Android, lancé en 2015, et le programme Google Patch Rewards, lancé en 2014, récompensent les contributions de chercheurs en sécurité qui investissent leur temps et leurs efforts à aider à rendre les applications plus sûres.
Alors, avec toutes ces précautions, pourquoi une telle agitation? Oui, il s'agit d'une faille de sécurité particulièrement vicieuse, mais le correctif est là… n'est ce pas ?

…mais pas les fabricants
Euh, et bien en fait Android a un autre problème de sécurité bien plus important. À l'exception des appareils Nexus, Google fournit les correctifs de code source, mais ce sont les fabricants de smartphones et les opérateurs qui doivent les faire parvenir aux utilisateurs qui mettent à jour le firmware. Et au 27 Juillet aucun des principaux acteurs de l'écosystème Android n'a annoncé de plan pour fournir le patch. Pour des appareils anciens, les patches pourraient ne jamais être livrés.

Zimperium affirme que le Blackphone de SilentCircle est protégé contre cette attaque depuis la version 1.1.7 de PrivatOS. Firefox de Mozilla a également inclus un correctif pour ce problème depuis la version 38. Et bien sûr Zimperium propose sa propre protection contre les attaques Stagefright avec sa plate-forme de défense de la menace mobile, zIPS.

Voici comment se débrouiller sans patch
Mais ce que Zimperium ne mentionne pas, c'est qu'Android a déjà une excellente façon de bloquer la plupart des attaques de Stagefrights : bloquer tous les messages texte provenant d'expéditeurs inconnus.

Pour paramétrer cela avec Android Kitkat, la version la plus populaire d'Android, ouvrez l'application 'Messenger' et appuyez sur le menu dans le coin supérieur droit de l'écran (les trois points verticaux), puis appuyez sur 'Paramètres'. Une fois là, sélectionnez Bloquer les expéditeurs inconnus, et c'est tout.

Sur Lollipop, où Hangouts est l'application de messagerie par défaut, il n'y a aucun moyen par défaut de bloquer les expéditeurs inconnus. Vous pouvez toutefois sous 'Paramètres' aller aux 'messages multimédia' et désactivez 'Récupérer automatiquement les messages multimédias'.

Avec Lollipop et d'autres versions d'Android, je recommande de vous tourner vers des applications de blocage de SMS tierces. Pour Android 2.3 à 4.3, j'apprécie 'Blocage des Appels et SMS'. Si vous utilisez KitKat ou les versions au dessus, où une seule application de SMS peut être active au même moment, j'apprécie Postman, alias TEXT BLOCKER. Ce programme fonctionne en conjonction avec votre application préférée de textos pour bloquer les expéditeurs inconnus.

Rien de tout cela n'est parfait. Un ami peut toujours être infecté et propager des programmes malveillants. Mais c'est un bon début. La solution de court terme adviendra quand les fabricants et les opérateurs se magneront enfin le train et pousseront le correctif vers leurs clients. Mais compte tenu de leur historique, je ne vais pas attendre et je vais bloquer les MMS. La solution à long terme arrivera quand les entreprises qui utilisent Android commenceront à travailler avec Google pour fournir des correctifs de sécurité le plus rapidement possible, et tout le temps.

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

Source : http://www.zdnet.fr/actualites/stagefright-a-quel-point-les-utilisateurs-d-android-doivent-ils-etre-inquiets-39823010.htm
Par Steven J. Vaughan-Nichols

A quelles attaques informatiques doit-on s’attendre dans les mois qui viennent ? | Le Net Expert Informatique

A quelles attaques informatiques doit-on s’attendre dans les mois qui viennent ?

Brèches de sécurité et atteintes à la vie privée font régulièrement la une des journaux. Comment la course à l'armement entre les auteurs de cyberattaques et les spécialistes de la défense se développe t-elle ? Nous analysons dans cet article les prévisions des experts.

La sécurité des informations et le respect de la vie privée ont toujours été des sujets brûlants, mais cette année la température semble encore monter d'un cran. Ces derniers mois ont été marqués par des cyberattaques très médiatisées qui ont concentré l'attention du monde entier sur la protection des données, le cryptage, le respect de la vie privée et la surveillance, comme jamais auparavant. Ces événements ô combien médiatiques se déroulent sur fond de multiplication des fuites de données au niveau des gouvernements, des entreprises et autres organisations, familles et individus.
Nous avons examiné les articles prospectifs de 17 entreprises et attribué les 130 prévisions résultantes à un certain nombre de catégories émergentes pour produire le graphique ci-dessous.

Prévisions de sécurité de Blue Coat, Damballa, FireEye, Fortinet, Forrester, Gartner, IDC, ImmuniWeb, Kaspersky Lab, Lancope, McAfee, Neohapsis, Sophos, Symantec, Trend Micro, Varonis Systems et Websense.
Image : Charles McLellan/ZDNet
En tête de liste, figurent les « nouveaux vecteurs et plates-formes d'attaque » et « l'évolution des solutions de cybersécurité existantes », deux catégories qui illustrent la réalité de la course à l'armement en matière de cybersécurité.
Dans la première catégorie, plusieurs commentateurs ont souligné les « nouveaux bugs dans du code ancien largement utilisé » (Kaspersky Lab), tels que Heartbleed/OpenSSL et Shellshock/Bash. Sophos a noté des failles exploitables dans le protocole IPv6, ainsi que des capacités de robot et de rootkit dans l'environnement d'amorçage enrichi UEFI qui peuvent générer de nouveaux vecteurs d'attaque. Apple était la principale nouvelle plate-forme signalée, par exemple par FireEye, qui note que « étant donné qu'Apple est de plus en plus présent dans les entreprises, les concepteurs de programmes malveillants vont ajuster leur jeu d'outils ». Les récents chiffres de ventes record ne feront que creuser davantage l'appétit des pirates informatiques pour les produits d'Apple.

Source : http://www.zdnet.fr/actualites/cybersecurite-a-quoi-s-attendre-dans-les-mois-qui-viennent-39822112.htm
Par Charles McLellan

Boulanger, épinglé par la Cnil pour des commentaires sur un fichier client | Le Net Expert Informatique

Boulanger épinglé par la Cnil pour des commentaires sur un fichier client

La Cnil a mis en demeure la société Boulanger, dont les employés ont quelque peu abusé de l'espace libre laissé au sein d'un fichier client. Plusieurs commentaires insultants ont été constatés par la Commission, qui laisse 3 mois à la société pour se mettre en règle.

Peut-on inscrire n'importe quoi dans le champ commentaire d'un fichier client ? Pas vraiment : la Cnil a ainsi annoncé aujourd'hui avoir épinglé l'enseigne Boulanger suite à une plainte lui ayant signalé des commentaires injurieux dans ses fichiers clients.
Sur son site, la Cnil explique avoir effectué un contrôle sur place doublé d'un contrôle en ligne suite à un dépôt de plainte, qui lui a permis de constater des pratiques contrevenant à la loi Informatique et Libertés. « Les fichiers de la société comportaient de nombreux commentaires excessifs sur ses clients, comme par exemple « n'a pas de cerveau », « cliente avec problème cardiaque », « client alcoolique » ou encore des propos insultants » rapporte ainsi la Cnil, qui explique avoir mis en demeure Boulanger, sommé de se mettre en conformité avec la loi sous trois mois.

La Cnil veut faire un exemple
La Cnil explique avoir relevé pas moins de 5828 commentaires désobligeants parmi les fichiers clients de Boulanger. La société est également épinglée pour non-respect des règles encadrant l'usage des cookies : la société manquait à son obligation de prévenir l'utilisateur de l'utilisation de cookies pour le tracking et la Cnil relève également la mise en place « de certains cookies à finalité publicitaire [ayant] une durée de vie pouvant aller jusqu'à 15 ans. »
Pas de chance pour Boulanger, la Cnil explique avoir choisi de mettre en avant cette procédure « afin d'appeler notamment l'attention des entreprises sur la nécessité de ne pas enregistrer de commentaires excessifs dans leurs fichiers clients. » Il fallait faire un exemple et la Cnil précise que cette mise en demeure n'est pas une sanction, mais rappelle que si Boulanger ne se met pas en règle, une nouvelle procédure pourrait être initiée à l'encontre de Boulanger.Via son compte Twitter, la marque s'est excusé et promet de remédier à la situation.

Source : http://www.zdnet.fr/actualites/boulanger-epingle-par-la-cnil-pour-des-commentaires-sur-un-fichier-client-39822914.htm

---

Attention aux arnaqueurs qui

sévissent sur le site Immoweb ! | Le Net Expert Informatique

Attention aux arnaqueurs qui sévissent sur le site Immoweb !

Avec l'été, les fausses petites annonces pour des lieux de villégiature fleurissent sur les sites internet. Et dans quelques semaines, ce sera au tour des faux kots pour étudiants.

Le modus operandi des arnaqueurs est simple : on vous appâte avec un bien à louer à prix cassé. Puis, on vous demande une caution, à verser via un mandat postal ou Western Union. Et vous êtes quitte de votre argent… Immoweb tire la sonnette d'alarme. L'arnaque en question n'est pas nouvelle, mais elle a repris de plus belle avec l'arrivée des vacances scolaires. Pour l'instant, ce sont principalement des annonces pour des lieux de villégiature qui se révèlent fausses. « On peut ainsi voir une maison dans le sud de la France ou dans un lieu exotique, à un prix dérisoire », explique Olivier Bogaert, commissaire à la Computer Crime Unit, l'unité spécialisée dans la cybercriminalité de la police fédérale.
Le candidat locataire tombe sous le charme des photos alléchantes, et du prix cassé. Et il contacte via le site internet le propriétaire. Les discussions quittent alors l'espace du site internet où était placée l'annonce.
« Le propriétaire peut expliquer qu'il avait un locataire qui s'est désisté au dernier moment et qu'il baisse donc le prix, ou qu'il recherche surtout à ce que sa maison ou son appartement ne reste pas vide. Il est souvent à l'étranger, de sorte qu'il demande à ce que vous versiez un acompte ou le loyer via Western Union, ou via une banque étrangère. Il peut aussi demander à ce que vous lui envoyiez une carte de crédit prépayée, que vous aurez crédité d'un certain montant ».

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.sudinfo.be/1334805/article/2015-07-17/immoweb-previent-ses-utilisateurs-attention-aux-arnaqueurs-qui-sevissent-sur-le

---

Microsoft trop lent à corriger quatre failles zero-day dans Internet Explorer |

Le Net Expert Informatique

Microsoft trop lent à corriger quatre failles zero-day dans Internet Explorer

Alerté en janvier par TippingPoint (HP) de l'existence de 4 vulnérabilités d'Internet Explorer, Microsoft avait plus de 6 mois pour les corriger. Le délai écoulé et faute de correctifs, des détails sur ces vulnérabilités ont été divulgués.

Microsoft se montre une nouvelle fois trop lent à corriger des vulnérabilités dans ses logiciels. C'est Internet Explorer, son navigateur, qui est à présent pointé du doigt par la Zero Day Initiative de TippingPoint, une filiale d'HP.
Les spécialistes des failles logicielles accordent six mois aux éditeurs pour corriger des vulnérabilités signalées avant de dévoiler publiquement leur existence. Et c'est ce qui vient de se produire pour quatre failles d'Internet Explorer.

Interaction avec la cible requise
Faute de correctifs une fois le délai écoulé, la ZDI a donc communiqué sur ces vulnérabilités zero-day du navigateur. Ces failles avaient été signalées en janvier 2015 à Microsoft qui n'a pas fourni de correctifs et avait demandé, et obtenu, une extension jusqu'au 19 juillet.
Les chercheurs en sécurité de TippingPoint précise que ces vulnérabilités permettent à un attaquant d'exécuter du code à distance sur les installations vulnérables d'Internet Explorer.
Pour s'exécuter, l'attaque nécessite cependant une interaction avec l'utilisateur au travers d'une visite sur une page (lien transmis dans un email ou par messagerie instantanée) ou l'ouverture d'un fichier malveillant.
Microsoft se trouve à présent confronté à l'obligation de corriger quatre failles critiques dans Internet Explorer. ZDI ne précise pas quelles sont les versions du navigateur affectées.

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

Source : http://www.zdnet.fr/actualites/zdi-microsoft-trop-lent-a-corriger-quatre-failles-zero-day-dans-internet-explorer-39822812.htm