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*

Vers une nouvelle plainte européenne contre Google

Vers une nouvelle plainte européenne contre Google

Google n'en a pas encore fini avec sa série de déboires judiciaires. Alors que le géant américain fait l'objet d'investigations à propos de son moteur de recherche et de sa plate-forme Androïd pour abus de position dominante, on apprend que le groupe américain pourrait être visé par une nouvelle enquête toujours de la part de la Commission européenne. Cette fois, cela concerne le cœur de l'entreprise, à savoir les services publicitaires.

Le site generation-nt.com qui reprend Bloomberg indique que la nouvelle procédure serait indépendante de deux précédentes et suivre son propre cours. Elle découle d'une procédure lancée depuis 2010 et qui concernerait des contrats avec des clients de Google dont le but était d'écarter l'utilisation de services concurrents.

Seulement, l'action annoncée pourrait être très coûteuse pour le géant américain parce qu'elle touche un domaine qui représente la majeure partie des solides revenus de Google, soit plus de soixante-quatorze milliards de dollars, seulement pour l'année 2015. Une perspective à laquelle il serait très difficile d'échapper puisque generation-nt.com nous apprend que Google a déjà épuisé ses possibilités de négociations avec la Commission européenne…. [Lire la suite]

Réagissez à cet article

Source : *Vers une nouvelle plainte européenne contre Google | CIO-MAG*

Conficker : un virus de 8 ans toujours vivace !

Conficker : un virus de 8 ans toujours vivace !

D'après des chercheurs de Check Point, le ver Conficker est toujours bien présent et à l'origine de nombreuses infections. Pourtant, la faille exploitée par ce malware a été corrigée en 2008.

Le mois dernier, il a été à l'origine de plus d'une attaque sur six d'après les mesures réalisées par l'éditeur de sécurité Check Point. Et pour cela, nul besoin d'être le programme malveillant le plus récent.

En effet, ce malware n'est autre que Conficker, apparu pour la première fois en 2008 – même si de nombreuses variantes ont été signalées ensuite. Comment après tant d'années, un virus peut-il rester toujours aussi actif ?

C'est avec les vieux virus qu'on fait les meilleures infections

Certes, à l'époque, Confiker était présenté comme « le plus complexe et sophistiqué » virus jamais réalisé. Mais si de telles menaces persistent, c'est car les failles logicielles exploitées par celles-ci persistent également.

Or, la vulnérabilité liée à Conficker a été corrigée par Microsoft fin 2008. Mais sur de nombreux postes Windows et réseaux, des brèches de sécurité demeurent permettant ainsi à ce malware de provoquer des attaques.

Mais Conficker n'est pas un cas isolé. Toujours selon Check Point, le virus Sailty et le ver Zeroaccess, apparus respectivement en 2003 et 2011, continuent eux aussi de cibler des machines Windows. Avec Conficker, ce sont les trois familles de malware les plus impliquées dans des attaques reconnues.

En 2015, selon le patron du CERT britannique, Chris Gibson, Conficker a été à l'origine de plus de 500.000 incidents de sécurité. Un bilan « excessivement déprimant » déplorait ce spécialiste… [Lire la suite]

Réagissez à cet article

Source : *Conficker : un virus de 8 ans toujours vivace ! –*

ZDNet

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*

Les métadonnées téléphoniques très bavardes sur notre vie privée

Les métadonnées téléphoniques très bavardes sur notre vie privée

---

Les métadonnées téléphoniques révèlent des informations très privées

Une équipe de chercheurs de l'université de Stanford a publié une vaste étude montrant l'étendue des informations personnelles qui peuvent être déduites des seules métadonnées de ses appels et SMS sur la vie privée d'une personne. A savoir toutes les informations qui « entourent » un message : durée d'un appel, numéro appelé, heure de l'envoi d'un SMS… En bref, tout ce qui concerne un message, à l'exception de son contenu.
En 2013, le lanceur d'alerte Edward Snowden avait révélé que la NSA, les services secrets américains, et leurs partenaires procédaient à une surveillance de masse de ces métadonnées, enregistrant quotidiennement les informations autour de millions de messages. La NSA affirme depuis 2013 que ces informations ne revêtent pas un caractère privé, mais qu'elles sont indispensables à l'efficacité de ses actions, notamment en matière de lutte contre le terrorisme.
Les conclusions de l'étude menée par les chercheurs de Stanford montrent tout le contraire. Pendant plusieurs mois, ils ont enregistré, avec l'accord des 823 participants à l'étude, les métadonnées de 251 788 appels et de 1 234 231 SMS. Ils ont ensuite analysé de manière automatique les tendances récurrentes dans les métadonnées. Des appels réguliers à des commerces dans une zone géographique précise peuvent par exemple indiquer que la personne habite dans ce quartier. Les chercheurs ont ensuite procédé à des analyses « manuelles » pour identifier des numéros appelés et tenter d'en déduire des informations sur la vie privée des participants.

GROSSESSE, PROBLÈME CARDIAQUE, ARMES À FEU…

Ils sont ainsi parvenus à déterminer que l'un des participants venait de se voir diagnostiquer un problème cardiaque : après un long appel à un centre de cardiologie, l'homme avait appelé un laboratoire médical, puis reçu plusieurs coups de fil d'une pharmacie, avant d'appeler le service consommateur d'une entreprise qui commercialise des outils permettant de surveiller son rythme cardiaque. Dans d'autres cas, la seule analyse des métadonnées a permis de montrer l'existence de grossesses, ou le fait qu'une personne avait acheté une arme à feu.
Les analyses automatiques des données se sont révélées moins précises : la technique n'a permis d'identifier la ville où résident les participants à l'expérience que dans 57 % des cas – mais dans 90 % des cas, l'analyse a permis de déterminer la localisation des personnes à moins de 80 km de leur domicile réel.
Interrogé par le Guardian, l'un des coauteurs de l'étude, Patrick Mutchler, affirme que ces résultats sont bien en deçà de ce dont sont capables les agences de renseignement, qui disposent de moyens considérables. « Gardez à l'esprit que [ces résultats] ne sont que le reflet de ce que peuvent faire deux doctorants disposant de ressources limitées. »… [Lire la suite]

Réagissez à cet article

Source : *Les métadonnées téléphoniques révèlent des informations très privées*

Et si la reconnaissance faciale de Facebook était excessive ?

Et si la reconnaissance faciale de Facebook était excessive ?

Depuis 2010, Facebook propose à ses utilisateurs un système de reconnaissance faciale qui permet de gagner du temps dans le « taguage » des personnes qui sont sur les photos. Sous couvert d'une nouvelle fonctionnalité, c'est un véritable dispositif biométrique qui a été mis en œuvre car il permet d'identification d'un individu à partir d'une simple photographie de son visage.

En Californie, trois utilisateurs ont reproché au réseau social n°1 d'avoir « secrètement et sans leur consentement » collecté des « données biométriques dérivées de leur visage ». Ces plaintes ont été jugées recevables par le juge James Donato qui « accepte comme vraies les allégations des plaignants » et juge « plausible » leur demande.

Au sein de l'Union européenne, le danger a rapidement été perçu s'agissant du système de reconnaissance faciale de Facebook qui l'a suspendu en 2012. Mais aux Etats-Unis, bien moins vigilants, cette fonctionnalité a perduré et il apparait bienvenu que la Justice y réagisse enfin. Facebook a constitué des profils qui répertorient les caractéristiques du visage de ses utilisateurs, leur cercle d'amis, leurs goûts, leurs sorties, etc. Avec plus de 3 milliards d'internautes dans le monde, cela revient à ce qu'environ 28% de la population ait un double virtuel rien que sur Facebook.

Facebook is watching you : Reconnaissance faciale, intelligence artificielle et atteinte aux libertés

Eu égard à leur grand potentiel discriminatoire, les données biométriques sont strictement encadrées par la loi du 6 janvier 1978 puisque d'après son article 25, une autorisation préalable de la Commission nationale de l'informatique et des libertés est indispensable pour mettre en œuvre des « traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes ». Cela regroupe l'ensemble des techniques informatiques qui permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Les conditions générales d'utilisation de Facebook ne sont pas donc pas conformes à la législation française sur les données personnelles, notamment s'agissant de la condition de consentement préalable, spécifique et informé au traitement des multiples données à caractère personnel collectées. Mais le géant de l'internet ne répond qu'à l'autorégulation. Par opposition à la règlementation étatique, la régulation n'entend prendre en compte que la norme sociale, c'est-à-dire l'état des comportements à un moment donné. Si la norme sociale évolue, alors les pratiques de Facebook s'adapteront.

Vers une remise en cause mondialisée des abus de Facebook ?

L'affaire pendante devant les Tribunaux met en lumière le manque de réactivité des américains face aux agissements de Facebook. C'est seulement au bout de 5 années que la Justice s'empare de la question des données biométriques à l'initiative de simples utilisateurs, alors même qu'une action de groupe à l'américaine d'envergure aurait pu être engagée pour mettre sur le devant de la scène les abus de Facebook.

Néanmoins, « mieux vaut tard que jamais » et l'avenir d'une décision répressive ouvre la porte vers de nouveaux horizons pour l'ensemble des utilisateurs. En effet, Facebook prend comme modèle pour toutes ses conditions générales d'utilisation à travers le monde la version américaine de « licencing ». Plus Facebook se verra obligé dans son pays natal à évoluer pour respecter les libertés individuelles des personnes inscrites, plus on s'éloignera du système tentaculaire imaginé par Mark Zuckerberg qui n'est pas sans rappeler celui imaginé par Georges Orwell dans son roman 1984.

Par Antoine CHERON, avocat associé, est docteur en droit de la propriété intellectuelle, avocat au barreau de PARIS et au barreau de BRUXELLES et chargé d'enseignement en Master de droit à l'Université de Assas (Paris II). Il est le fondateur du cabinet d'avocats ACBM… [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

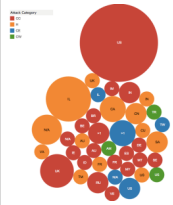
Réagissez à cet article

Source : *Facebook is watching you : système biométrique efficace – Data Security BreachData Security Breach*

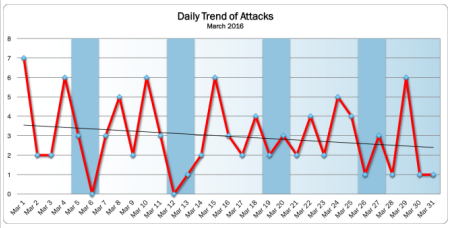
April 2015 Cyber Attacks Statistics – HACKMAGEDDON

Météo des cyberattaques de mars 2016

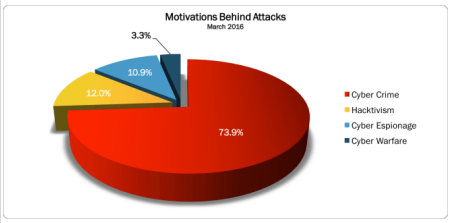
Afin de vous tenir informé de la météo des cyberattaques, nous avons souhaité partager avec vous l'étude récemment parue sur l'état des lieux des cyberattaques pour le mois de mars 2016 .



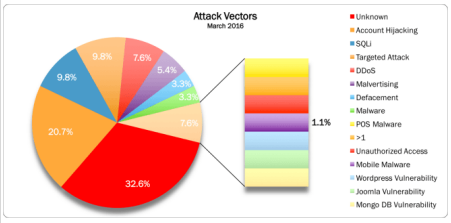
I finally found the time to aggregate the data of the timelines of March (part I and part II) into statistics.
As usual let's start from the **Daily Trend of Attacks**, which shows quite a sustained level of activity throughout the entire month, most of all during the first half.



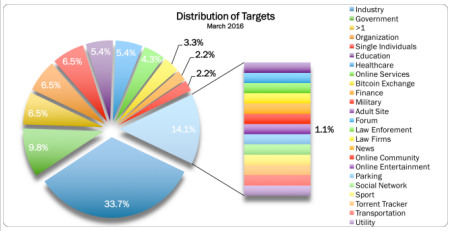
Cyber Crime ranks on top of the **Motivations Behind Attacks** chart with a noticeable 73.9%, a sharp increase compared with 62.7% of February. On the other hand hacktivists seem to have taken a temporary period of vacation in March (maybe due to the beginning of Spring), since Hacktivism reduces its quota to a modest 12%, less than one half of the percentage reported in February (28%). Cyber Espionage ranks at number three and also reports a noticeable growth (10.9% vs 5.3% in February). Last but not least, the attacks motivated by Cyber Warfare drop to 3.3% from 4% reported in February.



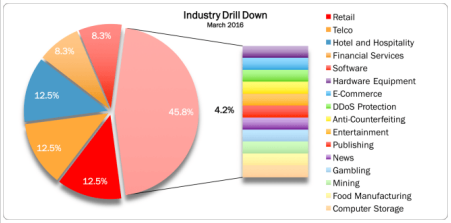
In the 32.6% of the cases the **Attack Vectors** are unknown. Account Hijackings rank at number one among the known attack vectors with 20.7% (was 12%, this growth is the effect of the numerous BEC and tax return scams reported in March). SQLi, an evergreen, confirms its momentum with 9.8% (was 10.7% in March), the same percentage of Targeted attacks (was 9.3% in March).



Industries lead the **Distribution of Targets** chart with 33.7% (was 29.3% in February). Governments rank at number two (9.8%, was 14.7% in February), whereas all the other targets are behind. Effectively this month the Distribution of Targets appear particularly fragmented.



The **Industry Drill Down** Chart is also particularly fragmented this month (tax scams do not privilege any particular sector) and is led by Retail, Telco and Hospitality (12.5% each). Software and Financial Services are behind (8.3%) and above all the other sectors.



As usual, the sample must be taken very carefully since it refers only to discovered attacks included in mytimelines, aiming to provide an high level overview of the "cyber landscape".
If you want to have an idea of how fragile our data are inside the cyberspace, have a look at the timelines of the main Cyber Attacks in 2011, 2012, 2013, 2014 and now 2015 (regularly updated). You may also want to have a look at the Cyber Attack Statistics.
Of course follow @paulsparrows on Twitter for the latest updates, and feel free to submit remarkable incidents that in your opinion deserve to be included in the timelines (and charts)… [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 : *April 2015 Cyber Attacks Statistics – HACKMAGEDDON*

Mais à quoi sert Spaces, le nouveau service de Google ?

Mais à quoi sert Spaces, le nouveau service de Google ?

Google a sorti aujourd'hui son nouveau service nommé Spaces. Disponible sur le web, sur iOS et sur Android, cet outil est difficile à cerner : voici quelques pistes d'utilisation après un premier test à la rédaction.

Le monde découvre en ce moment un nouveau service Google : Spaces. Non, il ne s'agit pas du petit nom du programme spatial de Mountain View, mais d'une application qui vous permet de créer des groupes avec des amis / collègues / inconnus pour partager… des choses. Des liens, des images, des commentaires et des vidéos YouTube pour l'instant.
Mais à quoi cela sert ? Eh bien c'est assez difficile à dire pour l'instant. Nous nous sommes empressé de créer un groupe pour Humanoid et d'inviter nos collègues préférés à tester l'application qui se paie le luxe d'être multiplateformes, disponible sur le web, iOS et Android. Nous avons partagé quelques liens, modifié ce qui était modifiable. Nous sommes aussi passés à côté des premiers bugs : une phrase qui sort de l'écran (dommage, c'est celle qui présente le service) ou l'impossibilité d'utiliser un compte Gmail d'entreprise… alors qu'il est proposé au lancement de l'application… [Lire la suite]

Réagissez à cet article

Source : *Mais à quoi sert Spaces, le nouveau service de Google ? — Tech — Numerama*

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

Lorsque Microsoft a abandonné Windows XP en 2014, on pouvait alors découvrir que 95% des distributeurs de billets de banque tournaient encore sous cette version obsolète de l'OS, devenant ainsi vulnérables au piratage. En 2016, rien n'a changé et les banque comme les constructeurs ne semblent pas décidés à faire le nécessaire.

Lorsque Microsoft a abandonné Windows XP en 2014, la menace de piratage est devenue de plus en plus grande pour les distributeurs de billets. Pourtant, fin 2015, **95% d'entre eux** tournaient encore sous cette version obsolète du système d'exploitation. On dénombre d'ailleurs pas moins de 9000 risques de sécurité sur ces machines. Pourtant les banques semblent s'en laver les mains, pourquoi ?
Comme l'explique Alexey Osipov, ingénieur chez Kaspersky, les constructeurs de distributeurs automatiques ont très peu de concurrents et les banques sont sous contrat avec eux, ils ne font donc pas l'effort de prendre les mesures suffisantes pour sécuriser leurs machines.
Pour Olga Kochetova, également ingénieur chez Kaspersky après avoir travaillé plusieurs années sur le marché des distributeurs bancaires, la réponse est encore plus simple. Ces machines étant désormais trop vieilles pour faire tourner des versions plus récentes et sécurisées de Windows, elles nécessitent donc d'être remplacées, or « **l'investissement serait trop coûteux** ». En outre, ça impliquerait aussi d'embaucher un nouveau personnel mieux formé vis à vis des nouveaux risques de piratage.

Il faut dire que pour un hacker, pirater un distributeur de billet est d'une simplicité enfantine puisqu'il suffit d'acheter une clé sur internet pour se connecter physiquement aux machines. Ils prennent ainsi tout simplement le contrôle du DAB pour lui réclamer la somme qu'ils souhaitent. L'an dernier, une attaque massive baptisée « Carbanak » avait fait perdre plus de **10 millions de dollars** à différentes banques situées un peu partout dans le monde… [Lire la suite]

Réagissez à cet article

Source : *Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage*

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

La version mobile de Windows 10 gagnera bientôt la compatibilité avec les lecteurs d'empreinte digitale déjà exploités par Android et iOS.

Selon *Engadget*, Microsoft en a fait l'annonce aujourd'hui dans le cadre de la conférence WinHEC. Alors qu'il était déjà possible de déverrouiller son téléphone Windows grâce à la reconnaissance faciale du système, la lecture d'empreinte digitale pourra également être employée.

Pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question.

Ainsi, Windows Hello gagnera cette fonctionnalité dans la mise à jour anniversaire de Windows 10 Mobile dont le déploiement est prévu pour juillet prochain.

Bien entendu, pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question. Pour le moment, seul l'Elite X3 de HP – un téléphone Windows toujours en développement destiné pour le marché des affaires et promettant d'agir comme un ordinateur portable – intègre un lecteur d'empreinte digitale… [Lire la suite]

Réagissez à cet article

Source : *Windows 10 Mobile acceptera l'empreinte digitale comme moyen d'authentification cet été | Branchez-vous*

Laurent LASALLE