WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

Si les messageries mobiles se renforcent grâce à un dispositif de chiffrement, un hackeur a trouvé le moyen de récupérer l'intégralité des messages en clair.

Avec un chiffrement de bout-en-bout, les messages sont normalement sécurisés. Cela permet d'éviter les attaques de type man-in-the-middle, et par ailleurs, même le prestataire de service n'est pas en mesure de prendre connaissance du contenu de ces échanges. Pourtant, il existe un moyen de contourner ces dispositifs. La société Ability a partagé ses exploits en vidéo avec le magazine Forbes.
Concrètement, la faille se trouve au sein du système de signalisation n° 7 (SS7), un ensemble de protocoles de signalisation téléphonique. C'est le réseau principal permettant de connecter les réseaux téléphoniques entre eux. C'est également lui qui établit des relations entre le téléphone d'un utilisateur et le réseau, par exemple les tonalités d'appel après une numérotation ou de mise en attente ou encore le renvoi vers la messagerie.

Téléchargez WhatsApp Le hackeur fait ainsi croire au SS7 qu'il dispose du même numéro de téléphone que celui de la victime. Il est ensuite en mesure d'installer l'application WhatsApp ou Telegram puis de recevoir le code secret permettant d'authentifier son smartphone.
sécurité security banner gb
Dès lors, le hackeur peut récupérer l'historique des conversations synchronisées et se faire passer pour la victime. De son côté, cette dernière recevra un message l'avertissant que son compte est utilisé autre part. L'application sera donc déconnectée et l'identité de la victime… usurpée.
Puisque le SS7 est un réseau global utilisé par les opérateurs téléphoniques à travers le monde, celui-ci n'appartient vraiment à personne. Cela signifie que la vulnérabilité n'a pas été corrigée et le processus semble pour l'heure compliqué. Autant dire qu'il s'agit d'une porte ouverte pour les agences de renseignement.

Voici la procédure en vidéo :

Article original de Guillaume Belfiore

Réagissez à cet article

Original de l’article mis en page : WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

---

Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

Adepte du malware Lurk, un réseau de cybercrimels vient dêtre démantelé en Russie. Il est responsable du vol de plus de 22 millions deuros à des banques.

Une cinquantaine d'interpellations en Russie ont abouti au démantèlement d'un réseau de cybercriminels surnommé Lurk. Un nom qui découle de l'emploi d'un cheval de Troie identifié en 2012.
À l'époque, Kaspersky Lab avait évoqué le cas de Lurk dans des attaques drive-by. Conçu pour voler des données sensibles d'utilisateurs afin d'obtenir un accès à des services de banques en ligne russes, le malware n'était pas téléchargé sur le disque dur et opérait uniquement dans la mémoire RAM.
Threatpost (Kaspersky Lab) écrit que Lurk a commencé à attaquer des banques il y a un an et demi, et a rapatrié divers malwares de serveurs de commande et contrôle. Les attaquants ont utilisé un VPN compromis afin de rendre leur campagne plus difficile à détecter.
Grâce à Lurk, les cybercriminels ont dérobé plus de 1,7 milliard de roubles (près de 22 millions d'euros) à des comptes d'institutions financiers russes, a indiqué le FSB (l'ancien KGB) à l'agence de presse russe TASS.
Article original de Jérôme GARAY

Réagissez à cet article

Original de l’article mis en page : Piratage de banques : un gang russe démantelé

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

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

Un caïd du ransomware gagne 90 000 dollars par an

Un caïd du ransomware gagne 90 000 dollars par an

Spécialiste du Dark web, Flashpoint a étudié les dessous d'une campagne russe de « ransomware-as-a-service » (RaaS). Son pilote aurait gagné 7 500 dollars par mois en moyenne.

Fournisseur d'analyses des Deep et Dark web, Flashpoint a étudié les dessous d'une campagne de « ransomware-as-a-service » (RaaS) pilotée, selon lui, par des escrocs russes. Le RaaS consiste pour l'auteur du rançongiciel à proposer à d'autres de diffuser des versions personnalisées de son programme pour chiffrer les données et verrouiller les terminaux d'utilisateurs. Les cibles sont appelées à payer en cryptomonnaie pour reprendre le contrôle de leurs données. La rançon est perçue par l'auteur du ransomware qui la partagera ensuite avec les diffuseurs.
C'est ainsi qu'une pointure des ransomwares en Russie aurait mené la campagne RaaS étudiée ces cinq derniers mois par Flashpoint. L'auteur de la campagne, qui ciblait des entreprises occidentales et des particuliers depuis au moins 2012, selon Flashpoint, aurait recruté des diffuseurs du programme ayant pour mission de trouver et infecter des cibles en échange d'un pourcentage sur les profits générés. Les novices étaient également invités à se lancer, sans frais d'entrée, le programme malveillant à diffuser étant accompagné d'instructions détaillées qu'un « écolier » pourrait suivre.

L'appât du gain

Le « patron » russe aurait ainsi recruté 10 à 15 « affiliés » chargés de diffuser le code de son ransomware. Soit en achetant un accès à des ordinateurs infectés, soit en passant par des serveurs insécurisés, ou du spam, ou encore en leurrant des utilisateurs de sites de rencontre et réseaux sociaux. Une fois que le code est installé et s'exécute, son auteur se charge des communications avec les victimes pour obtenir une rançon d'un montant moyen de 300 dollars par clé de déchiffrement et par victime, mais une somme additionnelle peut être exigée avant l'envoi de la clé.
Pour le paiement, la cryptomonnaie Bitcoin a été utilisée. 40 % des fonds ainsi détournés auraient été partagés entre les affiliés et 60 % seraient revenus au pilote de la campagne. Le « boss du ransomware » aurait ainsi empoché 7 500 dollars par mois en moyenne (90 000 dollars par an) et ses affiliés près de 600 dollars par mois chacun. Cela représente près de 30 paiements de rançon par mois.
« Nos résultats contestent la perception commune de cybercriminels hors du commun, éclairés, aisés, inaccessibles, inexposables et inarrêtables », soulignent les auteurs de l'étude. Et « Les montants des revenus du ransomware ne sont pas aussi séduisants et juteux » que l'on pourrait le croire. Il n'empêche, ces montants sont bien supérieurs au salaire moyen russe passé, selon une analyse de la Sberbank citée par RFI, de 1058 dollars par mois en 2012 à 433 dollars par mois en 2016.

crédit photo © frank_peters / Shutterstock.com
Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : Un caïd du ransomware gagne 90 000 dollars par an

---

Les géants du web s'accordent

pour bloquer les contenus illégaux

Les géants du web ensemble pour bloquer les contenus illégaux

Alors que les propos haineux sont malheureusement légion sur les réseaux sociaux, plusieurs géants du web ont trouvé un accord avec la Commission Européenne pour respecter un code de conduite. Toutefois, cette solution ne semble pas à ce jour convenir à plusieurs associations de défense des droits.

Les contenus illégaux bientôt bannis d'Internet ?

Depuis de longs mois maintenant, la Commission Européenne s'était fixée comme objectif d'éradiquer une majorité des propos haineux circulant sur la Toile.

Dans ce cadre, elle est parvenue à un accord avec YouTube, Microsoft, Twitter et Facebook pour l'établissement et le respect d'un code de conduite. Ainsi, les différents acteurs se sont engagés à bloquer les contenus gênants dans les 24 heures suivant leur signalement officiel.

En acceptant ce code de conduite pour bloquer les contenus illégaux, les acteurs du web montrent qu'ils ont bien conscience que leurs outils sont utilisés pour diffuser la violence et la haine mais aussi pour recruter des individus susceptibles de rejoindre leurs groupes.

Point positif, ce code de conduite ne vient pas entraver la liberté d'expression sur la Toile, celle-ci étant très importante en particulier pour les géants du web qui l'ont toujours prônée.

Un code de conduite pas suffisant selon les associations de défense des droits

Si la Commission Européenne s'est d'ores et déjà réjouie de l'accord trouvé avec les grandes entreprises du web, celui-ci ne fait assurément pas que des heureux.

En effet, Access Now et European Digital Rights (EDRi), deux associations de défense des droits, ont vivement critiqué cet accord estimant qu'il se contente de rappeler des règles déjà existantes à savoir celles qui consistent à supprimer des contenus illégaux.

Selon ces associations, il aurait donc fallu que le texte aille beaucoup plus loin et qu'il prévoit des poursuites contre ceux qui profèrent des propos haineux sur la Toile. En effet, Joe McNamee, Directeur Exécutif de l'EDRi, juge qu'« il est ironique que la Commission menace les Etats membres de les traduire en justice pour ne pas respecter les lois contre le racisme et la xénophobie alors qu'ils persuadent des entreprises comme Google et Facebook de glisser les infractions sous le tapis ».

Tout est dit…

Article original

Réagissez à cet article

Original de l'article mis en page : Les géants du web ensemble

pour bloquer les contenus illégaux

Sensibilisation aux Arnaques à la Loterie

Sensibilisation aux Arnaques à la Loterie

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

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

Euro 2016 et sécurité informatique, quelques conseils face à quelques risques…

Euro 2016 et sécurité informatique, quelques conseils face à quelques risques…

Euro 2016 – Les événements sportifs mondiaux ont toujours constitué un terrain de chasse idéal pour les cybercriminels. L'Euro 2016, qui débute le 10 juin prochain, ne devrait pas déroger à la règle.

Euro 2016 – Voici quelques éléments clés à retenir, amateur de football, de l'Euros 2016 ou non. Se méfier du spam et autre fausses « bonnes affaires » (places pour assister aux matchs à des prix défiant toute concurrence, par exemple). Ces mails peuvent contenir une pièce jointe infectée contenant un malware accédant au PC et interceptant les données bancaires des internautes lorsqu'ils font des achats en ligne. Ils peuvent également contenir un ransomware, qui verrouille et chiffre les données contenues dans le PC et invite les victimes à verser une rançon pour les récupérer.
Détecter les tentatives de phishing (vente de tickets à prix cassés voire gratuits, offres attractives de goodies en lien avec l'évènement,…) en vérifiant l'URL des pages auxquelles le mail propose de se connecter et en ne communiquant aucune information confidentielle (logins/mots de passe, identifiants bancaires, etc.) sans avoir préalablement vérifié l'identité de l'expéditeur.
Être prudent vis à vis du Wi-Fi public pour éviter tout risque de fuite de données, par exemple en désactivant l'option de connexion automatique aux réseaux Wi-Fi. Les données stockées sur les smartphones circulent en effet librement sur le routeur ou le point d'accès sans fil (et vice-versa), et sont ainsi facilement accessibles.
Redoubler de vigilance vis-à-vis des mails invitant à télécharger un fichier permettant d'accéder à la retransmission des matchs en temps réel. Il s'agit en réalité de logiciels malveillants qui, une fois exécutés, permettent d'accéder aux données personnelles stockées dans le PC (mots de passe, numéro de CB, etc.) ou utilisent ce dernier pour lancer des procédures automatiques comme l'envoi de mails massifs. (TrendMicro).
Auteur : Damien Bancal

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

Original de l'article mis en page : Football : Euro 2016 et sécurité informatique – Data Security BreachData Security Breach

---

L'État crée encore un nouveau fichier secret de données personnelles

L'État crée encore un nouveau fichier secret de données personnelles

Le gouvernement a fait connaître vendredi la création d'un fichier de données personnelles utilisé pour les services de renseignement intitulé « #BCR-DNRED », dont le contenu et la portée sont confidentiels. Il s'agit d'un fichier permettant les enquêtes contre la fraude douanière, orienté vers les crimes graves.

Le gouvernement a fait publier vendredi au Journal Officiel un décret n° 2016-725 du 1er juin 2016 qui ajoute un 13e fichier à la liste des fichiers confidentiels de données personnelles mis en œuvre par l'État, « *intéressant la sûreté de l'Etat, la défense ou la sécurité publique* ».
Comme le veut la règle, on ne sait strictement rien de ce fichier si ce n'est qu'il est baptisé « BCR-DNRED » et sera utilisé par les « *services du ministère des finances et des comptes publics (administration des douanes et droits indirects) traitant de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la prolifération des armes de destruction massive* ».
L'acronyme BCR-DNRED est sans aucun doute une référence à la Direction nationale du renseignement et des enquêtes douanières (DNRED), rattachée à Bercy. Considérée comme un service de renseignement, elle est chargée notamment de collecter des informations sur les les grands trafics de contrebande, et de lutter contre les flux financiers clandestins.

UN FICHIER CONTRE LE TRAFIC

JORF n°0128 du 3 juin 2016
texte n° 87

Délibération n° 2016-010 du 21 janvier 2016 portant avis sur un projet de décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé « BCR-DNRED »

NOR: CNIX1614799X
ELI: Non disponible

Avis favorable avec réserve.

L'avis « favorable avec réserve » de la Cnil.

On imagine donc que le fichier BCR-DNRED s'inscrit dans une politique de croisement d'informations concernant de possibles trafics internationaux illicites de biens ou d'argent qui transitent par la France, avec une orientation plus spécifique vers la recherche de financements de crimes graves.
La Cnil, qui n'a pas le droit de publier son avis, a émis un avis « favorable avec réserve », ce qui veut dire qu'elle a estimé qu'au moins sur certains points, le fichier projeté n'était pas conforme à la loi de 1978 sur la protection des données personnelles. Elle avait déjà émis des réserves non publiées concernant les deux derniers fichiers créés par l'État, le fichier CAR relatif au suivi des prisonniers créé en novembre 2015, et le Fichier de traitement des Signalés pour la Prévention et la Radicalisation à caractère Terroriste (FSPRT) modifié quelques jours plus tôt.

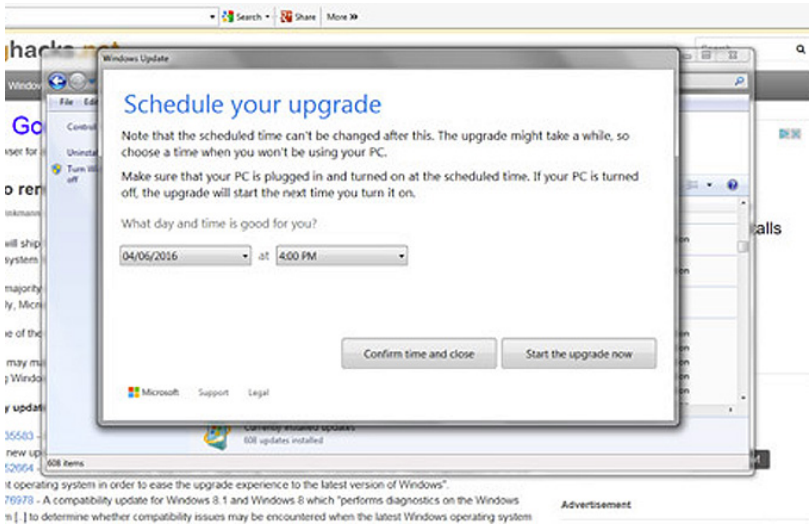
Article original de Guillaume Champeau

Original de l'article mis en page : L'État crée encore un nouveau fichier secret de données personnelles — Politique — Numerama

Microsoft supprimerait carrément la possibilité de refuser Windows 10

Microsoft supprimerait carrément la possibilité de refuser Windows 10

Selon une capture d'écran diffusée par The Register, Microsoft changerait à nouveau de méthode pour imposer la mise à jour vers Windows 10. Cette fois littéralement.



Le site britannique The Register publie ainsi la capture d'écran réalisée par un lecteur, qui montre qu'en lieu et place de la popup, Windows 7 lui a affiché une fenêtre qui impose de programmer une mise à jour vers Windows 10, avec un réglage de la date et de l'heure de l'opération. Il y a deux boutons sur la fenêtre ; le premier qui permet de confirmer la date et l'heure saisis ; le deuxième qui permet de demander une mise à jour immédiate.
Il n'y a aucun autre bouton pour refuser la mise à jour, ni de bouton « X » pour fermer la fenêtre (ce que Microsoft prenait de toute façon pour un accord).

COMMENT FAIRE ?

Les utilisateurs qui souhaitent refuser la mise à jour pourront toujours mettre une date de programmation très lointaine. Notez qu'au pire, en cas de mise à jour involontaire, il est possible de revenir vers Windows 7 ou Windows 8 en refusant d'accepter les conditions d'utilisation de Windows 10, présentées lors du premier lancement du système d'exploitation.
Le refus entraîne en effet une annulation de l'installation de Windows 10 puisque, même s'il peut forcer l'installation des fichiers du système, Microsoft ne peut pas encore obliger l'utilisateur à accepter son contrat.
La mise à jour vers Windows 10 reste gratuite jusqu'au 29 juillet 2016. Il faudra ensuite payer une licence. Notez que si vous avez déjà effectué la mise à jour et que vous devez réinstaller votre système, la gratuité de Windows 10 ne vaudra que si vous réinstallez l'OS sur le même ordinateur, reconnu par ses principaux composants. En cas de changement de carte mère ou de processeur par exemple, il devrait être imposé d'acheter la licence de Windows 10, auquel vous vous serez habitué…
Auteur : Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Microsoft supprimerait carrément la possibilité de refuser Windows 10 – Tech – Numerama

---

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

La rencontre qui devrait être clôturée vendredi dernier vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité.

(CIO Mag) – Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

Le directeur général de l'agence tunisienne de sécurité informatique, lui, indique que Tunis a pris très tôt des initiatives pour lutter contre la cybercriminalité. Mohamed Naoufel Frikha, repris par nos confrères, rappelle qu'un travail important a été réalisé depuis 1999 avec la création du premier centre en Afrique, le troisième dans le monde arabe.

Le rendez-vous de Tunis entend amener les pays arabes à créer des centres de cyber-alerte. Leur nombre est très insuffisant dans l'espace arabophone puisque seuls dix pays en disposent. Des représentants de treize Etats prennent part aux échanges.

Article de Ousmane Gueye

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité: les pays

arabes mutualisent leurs forces pour faire face au phénomène | CIO MAG