Quelles tendances en 2017 pour la sécurité du Cloud ?

Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

Les menaces inhérentes à l'IoT obligeront les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux Etats-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cyberespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entraînant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et revoient le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ». Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSI endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'atout concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de privilèges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Sécurité du Cloud : quelles tendances en 2017 ? — Globb Security FR

Les protections de Windows complètement inefficaces à la technique AtomBombing !

Les protections de Windows complètement inefficaces à la technique AtomBombing !

Des chercheurs en sécurité ont découvert un mécanisme qui exploite une propriété propre à Windows pour en contourner tous les mécanismes de protection.

Une véritable bombe atomique pour l'intégrité de Windows. Une équipe de chercheurs de la société de sécurité israélienne Ensilo déclare avoir trouvé un moyen qui permet à un code malveillant de contourner toutes les barrières de sécurité possibles et inimaginables de l'OS de Microsoft. Et quelle que soit sa version. En l'occurrence, les experts ont effectué leurs travaux sur Windows 10.
La technique, qu'ils ont dénommée « AtomBombing » exploite les « Atom Tables ». Inhérentes au système d'exploitation, ces tables permettent aux applications de stocker les données et y accéder. Elles peuvent aussi être utilisées pour organiser le partage des informations entre les applications. *« Nous avons découvert qu'un attaquant pouvait écrire du code malveillant dans une table atom et forcer un programme légitime à récupérer ce code depuis la table*, explique le responsable de l'équipe de recherche Tal Liberman. *Nous avons également constaté que le programme légitime, maintenant infecté du code malveillant, peut être manipulé pour exécuter ce code. »* De plus amples détails sur la technique d'intrusion sont présentés sur cette page.

Pas de correctif possible

Ce n'est évidemment pas le premier cas connu de technique d'injection de code pour pénétrer le système et affaiblir son intégrité. Mais ces techniques s'appuient généralement sur des vulnérabilités de l'OS et la manipulation de son utilisateur amené, sans en avoir conscience, à déclencher l'exécution d'un code malveillant à travers un programme, comme un navigateur par exemple, pour contourner les barrières de sécurité.
Mais rien de tout cela dans le cas présent. *« AtomBombing est exécuté simplement en utilisant les mécanismes sous-jacents à Windows. Il n'est pas nécessaire d'exploiter les bugs ou les vulnérabilités du système d'exploitation*, assure le chercheur. *Comme la question ne peut être résolue, il n'y a pas de notion de correctif. Ainsi, la réponse pour atténuer [le risque] serait de plonger dans les appels des API et de surveiller les activités malveillantes. »* Autrement dit, pas de correctif possible mais du monitoring système en temps réel en quelque sorte (comme en propose au passage Ensilo). L'autre solution serait que Microsoft modifie l'architecture de Windows. Ce qui n'est pas prévu dans l'immédiat.
Ensilo reste discret – et c'est bien normal – sur la méthode pour injecter le code. A notre sens, l'exécution d'un tel script nécessite soit la complicité involontaire de son utilisateur (ce qui n'est pas nécessairement le plus compliqué), soit l'accès direct à une machine non protégée. En cas de succès, l'AtomBombing fait alors tomber toutes les barrières de protection selon les niveaux de restriction, peut accéder à des données spécifiques, y compris les mots de passe chiffrés, ou encore s'installer dans le navigateur pour en suivre toutes les opérations. Explosif !

Réagissez à cet article

Original de l’article mis en page : AtomBombing, le code insensible aux systèmes de protection de Windows

---

Cash investigation ne comprend rien à la cybersécurité

Cash investigation ne comprend rien à la cybersécurité

La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que Cash Investigation a tenté de montrer.

La cybersécurité est un sujet suffisamment sensible pour qu'il mérite d'être traité par les journalistes avec rigueur et sérieux. En la matière, l'approximation et la sous-estimation de sa complexité conduisent inévitablement à des contre-vérités médiatiques et à des biais de représentation.
C'est précisément ce que l'émission de France 2 Cash Investigation Marchés publics : le grand dérapage nous a fourni le mardi 18 octobre à 20h55, tant les approximations et les contre-vérités se succédaient à grande vitesse tout au long du reportage sur le système d'exploitation des ordinateurs du Ministère de la Défense.
Je dois avouer qu'il en faut en général beaucoup pour me choquer mais que ce beaucoup a été très vite atteint par l'équipe de Cash Investigation ! Jamais réalité n'avait été à ce point tordue et déformée dans l'unique but d'entrer par le goulot étroit du format préfabriqué de la désinformation. En clair, on a voulu se payer les balourds du Ministère de la Défense et les militaires qui ont choisi le système d'exploitation Windows (Microsoft) pour équiper leurs machines…

Un piratage en trois clics ?

Pensez donc, Madame, en trois clics et deux failles de sécurité, Élise Lucet nous démontrait qu'elle pouvait prendre le contrôle des ordinateurs du Ministère de la Défense pour déclencher dans la foulée la troisième guerre mondiale…. Il est vrai qu'elle venait de pirater sans pression l'ordinateur de l'un de ses collègues, avec l'aide de deux experts en cybersécurité de l'ESIEA. Et comme chacun le sait, si l'opération fonctionne avec la machine Windows de madame Michu, ça marchera tout pareil avec les machines de la Grande Muette.
Dans le cadre d'un renouvellement de contrat, Microsoft a remporté en 2013 le marché public du Ministère de la Défense concernant l'équipement en systèmes d'exploitations du parc informatique des Armées. Windows est donc installé sur 200 000 ordinateurs de l'armée française.
Partant de cette réalité, Élise Lucet et son équipe en ont déduit que cela constituait un choix risqué en matière de cybersécurité & cyberdéfense tant ce système d'exploitation est truffé de vulnérabilités et de Back Doors (portes dérobées) installées par les méchants espions américains de la NSA.

Le « piège » de Microsoft

En conclusion, toujours selon Élise Lucet, les militaires français sont tombés dans le piège tendu par Microsoft qui dispose désormais de toutes les entrées possibles pour la prise de contrôle à distance des ordinateurs sensibles du Ministère et de leurs secrets Défense. La théorie du complot n'est pas très éloignée dans tout cela, surtout lorsque l'hypothèse d'Élise Lucet se trouve plus ou moins confirmée par les déclarations de l'expert cryptologue Éric Filiol, retraité des services de renseignement et actuellement directeur du centre de recherche en cybersécurité de l'ESIEA.
Ce que dit Éric Filiol durant ses courtes interventions n'est pas contestable : il effectue une démonstration de prise de contrôle à distance d'un ordinateur équipé du système Windows 7 à la suite d'un clic de l'utilisateur (la cible) sur un lien malveillant transmis par mail. La démonstration qu'il donne d'une prise de contrôle n'appelle aucune critique puisqu'elle est un classique du genre, connue de tous les étudiants préparant un Master en cybersécurité.

Quelle preuve des failles de sécurité ?

C'est l'usage qui en est fait qui devient très contestable : puisque la manipulation fonctionne sur l'ordinateur doté de Windows de mon collègue journaliste (qui, au demeurant, a le clic facile et l'antivirus laxiste), c'est qu'elle fonctionne également avec l'ensemble du parc informatique relevant du Ministère de la Défense (cqfd). Preuve est donc faite de l'incompétence des services de l'État, de services chargés de la cybersécurité des infrastructures militaires et de l'ensemble des experts, ingénieurs et chercheurs qui œuvrent chaque jour en France pour sécuriser les systèmes…
Le reportage pousse encore un peu plus loin sa courageuse investigation en allant interroger très brièvement l'Officier Général Cyberdéfense, le vice Amiral Coustillière. Ce dernier est interrogé entre deux portes sur le choix improbable d'installer Windows sur des machines qui font la guerre.

White Hat au grand cœur

N'écoutant que leur sagacité et leur expertise autoproclamée, nos journalistes hackers « White Hat » au grand cœur (donc toujours du bon côté de la Force) donnent pour finir une leçon de cyberstratégie à l'Amiral responsable de la sécurité des infrastructures numériques militaires, tout en le faisant passer pour un amateur déconnecté des réalités informatiques… C'est à ce point que l'on touche au paroxysme de la désinformation du spectateur que l'on considère comme un consommateur compulsif de dysfonctionnements et malversations étatiques…
Et bien non, Madame Lucet, non, le choix de Windows n'est pas plus ou moins défendable que celui d'un système open source. Linux et ses dérivés souffrent également de vulnérabilités, subissent des attaques et des correctifs. C'est le triste destin de tout système complexe que d'avoir été créé imparfait, ouvert aux agressions extérieures exploitées par des individus mal intentionnés ou en quête d'information.

On ne clique pas tous sur les malware

Non, Madame Lucet, ce n'est pas parce qu'un de vos collègues journalistes clique facilement sur un lien malveillant que tout le monde le fait. Ce n'est pas parce que son antivirus ne détecte pas un malware qu'aucun autre antivirus ne le détectera. Ce n'est pas parce que Windows possède des vulnérabilités que les autres systèmes d'exploitation n'en possèdent pas.
Ce n'est pas parce que Microsoft a pu transmettre ou vendre certaines données aux services gouvernementaux américains que cette firme cherche obsessionnellement à piéger l'armée française. Enfin, non chère Élise, l'armée française ne découvre pas les problématiques de sécurité numérique avec votre reportage et ne sous-estime pas les risques de vol de données sensibles. C'est quelque part faire injure aux spécialistes civils et militaires qui œuvrent quotidiennement à la défense des intérêts numériques de la nation.
La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que ce triste reportage a tenté de montrer.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 : Cash investigation ne comprend rien à la cybersécurité | Contrepoints

---

La vente liée d’un OS et d’un PC est elle illégale en Europe ?

La vente liée d’un OS et d’un PC est elle illégale en Europe ?

La Cour de justice de l'Union tranche un conflit opposant un consommateur à Sony dans la vente groupée d'un PC et de Windows. Et valide les pratiques des constructeurs.

La fin d'un long feuilleton ? Cela y ressemble fort. La Cour de justice de l'Union européenne (CJUE) vient en effet d'estimer que la vente d'un ordinateur équipé de logiciels préinstallés « *ne constitue pas, en soi, une pratique commerciale déloyale* ». Cet avis vient trancher une affaire qui a débuté en France en 2008. Au centre des débats : la vente de logiciels – en l'espèce Windows Vista et autres applications – à un PC de marque Sony. Le consommateur qui est à l'origine de l'affaire refuse la pratique imposée par le marché et demande le remboursement des logiciels préinstallés à Sony.
Devant le refus du constructeur, l'affaire est portée en justice par l'utilisateur, qui y voit une pratique commerciale déloyale. Saisie *in fine* de l'affaire, la Cour de cassation demande à la CJUE de statuer sur deux points. Primo, l'absence d'alternative proposée au consommateur (soit le même ordinateur vendu nu) est-elle une pratique commerciale déloyale ? Secundo, une offre groupée – PC + logiciels donc – doit-elle faire obligatoirement apparaître le prix de chacune de ses composantes ?…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : La vente liée d'un OS et d'un PC n'est pas illégale en Europe

La Cnil épingle Windows 10 sur la collecte des données personnelles

La Cnil épingle Windows 10 sur la collecte des données personnelles

Constatant plusieurs manquements dont la collecte de données excessives et non pertinentes par Windows 10, la Cnil a mis en demeure Microsoft de se conformer à la loi dans un délai de 3 mois.

A quelques jours de la fin de la gratuité pour migrer sur Windows 10, la Cnil s'invite dans le débat sur le dernier OS de Microsoft. Et le moins que l'on puisse dire est que le régulateur n'est pas content des méthodes de l'éditeur américain. Elle vient de mettre en demeure Microsoft de se conformer dans un délai de 3 mois à la Loi Informatique et Libertés.

Alertée sur la collecte de données de Windows 10 (dont nous nous étions fait l'écho à plusieurs reprises : « pourquoi Windows 10 est une porte ouverte sur vos données personnelles » ou « Windows 10 même muet il parle encore »), la Cnil a effectué une série de contrôles entre avril et juin 2016 pour vérifier la conformité de Windows 10 à la loi.

De ces contrôles, il ressort plusieurs manquements. Le premier concerne une collecte des données excessives et non pertinentes. Elle reproche par exemple à Microsoft de connaître quelles sont les applications téléchargées et installées par un utilisateur et le temps passé par l'utilisateur sur chacune d'elles. Microsoft s'est toujours défendu de collecter des données personnelles en mettant en avant des relevés de « télémétrie » pour améliorer son produit.

Défaut de sécurité, absence de consentements et référence au Safe Harbor

Autre point soulevé par le régulateur, un défaut de sécurité a été trouvé dans le code PIN à 4 chiffres. Ce dernier est utilisé pour s'authentifier sur l'ensemble des services en ligne. Or le nombre de tentatives de saisie du code PIN n'est pas limité.

De plus, la Cnil constate une absence de consentement des personnes notamment sur le ciblage publicitaire lors de l'installation de Windows 10. Idem pour le dépôt de cookies déposés sur les terminaux des utilisateurs.

Enfin, cerise sur le gâteau, Microsoft est enjoint par la Cnil d'arrêter de se baser sur le Safe Harbor pour transférer les données personnelles aux Etats-Unis. Cet accord a été invalidé par la Cour de Justice de l'Union européenne en octobre 2015. Il a été remplacé par le Privacy Shield qui doit bientôt rentrer en vigueur.

La balle est maintenant dans le camps de Microsoft.

Article original de Jacques Cheminat

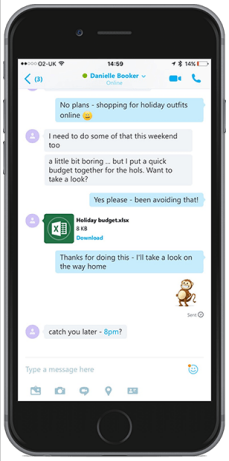
Réagissez à cet article

Original de l'article mis en page : La Cnil épingle Windows 10 sur la collecte des données

Envoyez désormais des fichiers aux contacts hors ligne avec Skype

Envoyez désormais des fichiers aux contacts hors ligne avec Skype

La mise à jour de Skype permet de transmettre des fichiers aux contacts hors ligne. En outre, la limite maximale par fichier a été relevée à 300 Mo.
Si vous avez l'habitude d'envoyer des fichiers par Skype, voilà une nouvelle qui devrait vous satisfaire : en récupérant la version la plus récente du logiciel de téléphonie et de messagerie instantanée, vous pouvez partager des contenus lorsque les destinataires ne sont pas connectés au moment de l'envoi.
Cette fonctionnalité implique manifestement un stockage du fichier sur les serveurs de Microsoft – la maison-mère de Skype – afin que le service puisse être en mesure de le faire suivre quand le destinataire se reconnectera. L'envoi peut concerner un seul contact ou tout un groupe de discussion.



Attention, néanmoins. Une limite à 300 Mo par fichier est appliquée par Microsoft. Si celle-ci suffit amplement dans la plupart des cas, vous ne pourrez pas envoyer une vidéo trop lourde. Il faudra procéder autrement si vous tenez absolument à envoyer ce fichier qui contient « 2016.TRUEFRENCH.EXTENDED.BDRip.XViD.AC3 » dans le titre…
Une autre évolution appréciable de Skype figure dans l'accès à un fichier depuis de multiples appareils. Maintenant, vous pouvez lire le même document depuis votre smartphone, votre tablette ou votre ordinateur, sans avoir besoin de demander à votre interlocuteur de vous le renvoyer.

Article original de Julien Lausson

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 : Skype vous permet d'envoyer des fichiers aux contacts hors ligne – Tech – Numerama

---

Microsoft stocke 200 Mo de données informatiques sous forme d'ADN

Microsoft stocke 200 Mo de données informatiques sous forme d'ADN

L'université de Washington a collaboré avec Microsoft pour écrire 200 Mo de données informatiques sur un bout d'ADN. Le but est d'optimiser au maximum l'espace de stockage et sa durabilité en allant vers un stockage biologique.

Écrire 200 méga-octets de données informatiques sur de l'ADN de synthèse. C'est la prouesse réalisée par des scientifiques de l'université de Washington en collaboration avec Microsoft. Les informations inscrites sur les molécules contiennent la Déclaration universelle des droits de l'homme en plus de 100 langues, les 100 livres électroniques les plus téléchargés sur la bibliothèque Projet Gutenberg, une partie des bases de données de Crop Trust, un groupe consultatif international pour la recherche agricole et un clip musical du groupe américain Ok Go,
« *Nous utilisons l'ADN comme un espace de stockage de données numériques* », explique le professeur Luis Ceze dans une vidéo. « *La raison pour laquelle nous faisons cela est parce que l'ADN est très dense et que l'on peut mettre énormément d'informations dans un très petit volume* », ajoute-t-il.

LA TOTALITÉ DE L'INTERNET POURRAIT TENIR DANS UNE BOÎTE À CHAUSSURES
Il affirme également que la totalité de l'Internet pourrait tenir dans une boîte à chaussures grâce à ce procédé. L'autre motivation des scientifiques est aussi le fait que l'ADN peut être conservé très longtemps. « *Dans les bonnes conditions, il peut durer des milliers d'années tandis que les technologies de stockages ne tiennent que quelques décennies* ».

L'ADN est fait de différentes séquences de quatre molécules : l'adénine (A), la guanine (G), la cytosine (C) et la thymine (T).Les scientifiques ont réussi à encoder les données qu'ils voulaient stocker sur les quatre molécules de base de l'ADN synthétisé.
En analysant l'ADN, ils peuvent lire les informations et les rétablir à leur état original.
Les 200 Mo de documents sont enregistrés sur un bout d'ADN qui fait la taille de quelques grains de sucre. Celui-ci a été encapsulé pour éviter toute dégradation.
Les capacités de stockage de l'ADN sont énormes. Malheureusement, lire les données dessus prend beaucoup de temps – jusqu'à plusieurs heures. Aussi, ce procédé n'est pas prêt d'être démocratisé, d'autant plus qu'il coûte encore très cher. Mais cela serait apparemment en train de changer. « *La technologie pour lire l'ADN est en train de se développer rapidement et pourrait devenir suffisamment rapide et bon marché pour être commercialisée* », explique Luis Ceze à The Register.
Le scientifique pense que les premiers clients seront probablement les centres de données pour qui l'optimisation de l'espace de stockage est un enjeu permanent.

Article original de Omar Belkaab

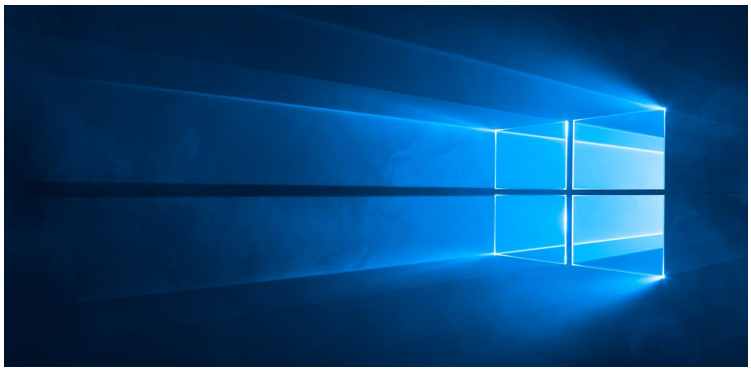
Réagissez à cet article

Original de l'article mis en page : Microsoft stocke 200 Mo de données informatiques sous forme d'ADN – Sciences – Numerama

Microsoft corrige 44 failles de sécurité

	Microsoft corrige 44 failles de sécurité

Microsoft vient de publier une nouvelle mise à jour cumulative pour Windows 10. Elle reprend tous les correctifs de sécurité sortis depuis la dernière, mais ajoute comme d'habitude une série d'optimisations.



Patch Tuesday oblige, toute une série de bulletins de sécurité a été émise par Microsoft. 16 sont disponibles, dont 5 critiques (DNS, Office, JScript/VBScript, Edge et Internet Explorer), pour un total de 44 vulnérabilités colmatées. Toutes les versions de Windows et Office en cours de support sont touchées et il faut donc procéder à la récupération des mises à jour depuis Windows Update.

Correctifs de sécurité et réparations diverses

Dans le cas de Windows 10, cela donne lieu à une nouvelle mise à jour cumulative. Tous les correctifs de sécurité nécessaires y sont bien sûr, mais d'autres réparations sont disponibles, Microsoft restant sur son rythme d'amélioration continue de sa plateforme.

Les apports proposés sont nombreux et concernent aussi bien une meilleure fiabilité pour des composants comme Edge, Cortana, la lecture de sons, Cartes, Miracast et Explorer, que des corrections de bugs divers. Ces derniers concernaient par exemple l'affichage des bulles de notifications qui apparaissaient parfois en haut à gauche de l'écran, des solutions VPN qui ne fonctionnaient plus après certaines bascules entre cartes réseau, une position géographique qui n'était pas aussi rapidement mise à jour que nécessaire, et ainsi de suite.

Les smartphones aussi sont mis à jour

Notez que Windows 10 oblige, cette nouvelle version du système, estampillée 10586.420, se répercute également sur la mouture Mobile. Tous les smartphones l'utilisant peuvent donc se rendre dans la zone des mises à jour pour la récupérer. Il n'y a pas de liste spécifique des nouveautés, mais puisque la plupart des composants et des applications sont les mêmes que pour la mouture PC, les améliorations le sont également. On trouve mention toutefois d'un problème réglé pour lessmartphones : la sonnerie du téléphone qui s'interrompait parfois à la réception d'un SMS.

On rappellera que ces mises à jour cumulatives s'adressent pour l'instant toujours à la version 10586 mise en place initialement avec l'évolution majeure de novembre dernier, surnommée TH2, pour « Threshold 2 ». À la fin du mois prochain arrivera RS1, pour « Redstone 1 », sous la forme d'une Anniversary Update. Elle sera considérée comme le nouveau socle, déclenchant à son tour une nouvelle série de mises à jour cumulatives mensuelles.

Pour l'heure, tous les appareils disposant au minimum de Vista devraient être mis à jour sans attendre.

Article original de Vincent Hermann

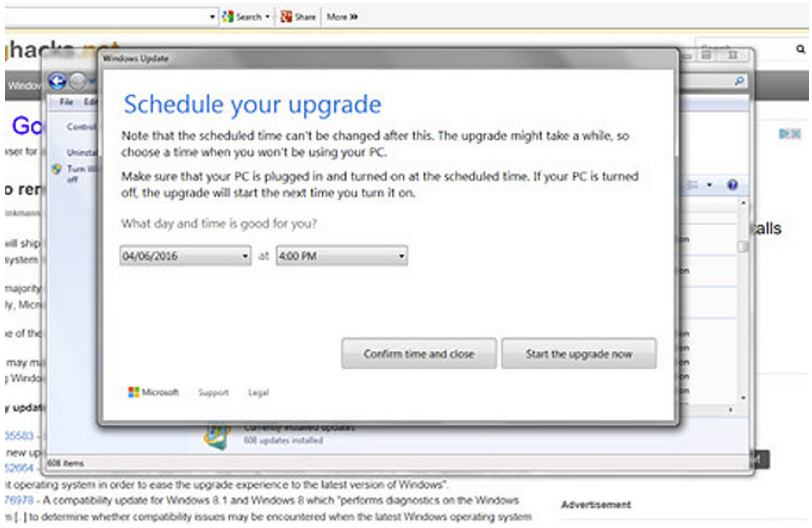
Réagissez à cet article

Original de l'article mis en page : Microsoft : 44 failles colmatées et mise à jour cumulative pour Windows 10 — Next INpact

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

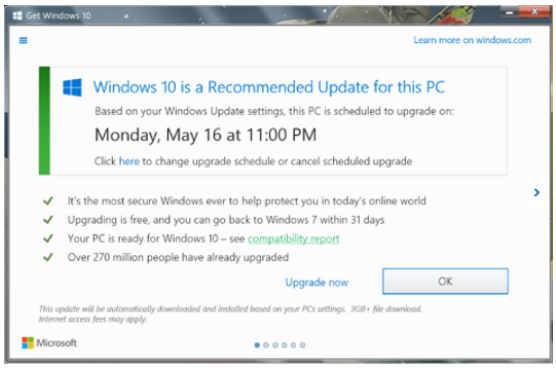
---

Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?

Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?

« Mon ordinateur m'a demandé si je voulais passer à Windows 10. J'ai cliqué sur le bouton X pour fermer la fenêtre car je ne voulais pas, et une heure après, Windows 10 est en train de s'installer. » Ce type de commentaire s'est multiplié sur les réseaux sociaux ces derniers jours. De nombreux internautes se sont plaints de voir leurs ordinateurs installer automatiquement la mise à jour vers Windows 10, alors qu'ils pensaient l'avoir refusée. Tous avaient cliqué sur la croix rouge permettant de fermer la fenêtre proposant ce téléchargement.

En général, ce bouton sert à fermer une pop-up sans avoir à donner de réponse à sa proposition. Mais depuis quelques jours, le fait de cliquer dessus a l'effet inverse : cela installe Windows 10. Une « *tromperie* », selon de nombreux utilisateurs du célèbre système d'exploitation de Microsoft.



Si l'utilisateur ferme cette fenêtre, alors Windows 10 s'installera automatiquement sur son ordinateur. Microsoft

L'entreprise, de son côté, assume et explique sur son site le fonctionnement de cette fenêtre. En fait, celle-ci fait plus que proposer une mise à jour : elle indique que la mise à jour est déjà programmée et précise la date. L'utilisateur est alors invité à cliquer sur le gros bouton « OK ». Il a aussi la possibilité, inscrite en petits caractères, de modifier la date ou d'annuler la programmation de mise à jour. Mais s'il décide simplement de fermer la fenêtre, alors Microsoft part du principe que l'utilisateur accepte la mise à jour, comme s'il avait cliqué sur « OK ».

Les utilisateurs forcés. Normal ?

Cette manœuvre de Microsoft est considérée par beaucoup comme une manière de leur forcer la main, alors que l'entreprise a annoncé sa volonté d'équiper un milliard de machines de Windows 10 en trois ans. D'autant qu'une date clé se rapproche dangereusement : à partir du 30 juillet, la mise à jour, jusqu'ici gratuite pour les utilisateurs de Windows 7 et 8, deviendra payante. Il sera alors bien plus compliqué de convaincre les sceptiques de s'y convertir.

Source : *L'étrange méthode de Microsoft pour imposer le téléchargement de Windows 10*

Réagissez à cet article