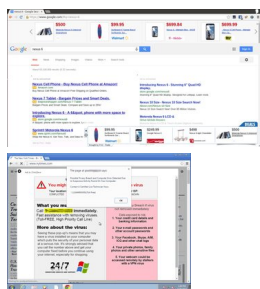


5% des utilisateurs de Google seraient victimes d'un adware sur leur machine | Le Net Expert Informatique



5% des utilisateurs de Google seraient victimes d'un adware sur leur machine

Google a publié les résultats d'une étude sur la publicité intrusive et plus particulièrement les adware installés sur les machines des internautes à leur insu.



Google explique que depuis le début de l'année, la société a reçu 100 000 plaintes émanant des utilisateurs du navigateur Chrome, victimes d'adware. Ces logiciels malveillants injectent littéralement de la publicité au sein des pages Web affectant leur lisibilité, mais générant également des erreurs réseau ou malmenant les performances du navigateur. En partenariat avec l'université de Berkeley en Californie, Google annonce avoir lancé une étude dont les résultats finaux seront dévoilés au 1er mai prochain. Celle-ci a été menée sur 100 millions de pages vues sur les sites de Google au travers des navigateurs Chrome, Firefox et Internet Explorer. Google explique que les adware ciblent aussi bien les systèmes Windows et OS X ainsi que les trois navigateurs. En outre, plus de 5% des internautes visitant les sites de Google auraient au moins un injecteur publicitaire installé sur leur machine. La moitié d'entre eux en disposeraient d'au moins deux et un tiers en auraient au moins quatre. En outre, 34% des extensions pour Chrome injectant des publicités seraient directement classées en tant que malwares. Les chercheurs ont trouvé 192 extensions malveillantes. Avant d'être bloquées celles-ci affectaient 14 millions d'utilisateurs. Google indique avoir implémenté les technologies de ces chercheurs pour scanner automatiquement le Chrome Web Store à la recherche de nouvelles menaces potentielles.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : http://www.clubic.com/antivirus-securite-informatique/actualite-761347-google-5-internautes-disposeraient-adware-machine.html?estat_svc=s%3D223023201608%26crmID%3D639453874_922037053

Géolocalisation : tous traqués ? Emission du 12 février 2015 à voir ou à revoir | Le Net Expert Informatique

Géolocalisation : tous traqués ? Emission du 12 février 2015 à voir ou à revoir

Les Français utilisent leur portable près de 170 fois par jour. Mais ils font bien plus que téléphoner. Ils prennent des photos, vont sur les réseaux sociaux, se déplacent... tout en se géolocalisant. Pour Envoyé spécial, une équipe a rencontré plusieurs adeptes de ce procédé.

Grâce à la puce GPS de leur smartphone, ils peuvent trouver la boulangerie ou le cinéma le plus proche, calculer leur trajet en voiture ou en bus, repérer les embouteillages... Plus surprenant : ils peuvent aussi suivre leurs amis à la trace, draguer des passant(e)s, payer leur prime d'assurance de voiture moins cher et même... gagner de l'argent en faisant leurs courses ! Tout ça grâce à des applications de géolocalisation qui se téléchargent en un clic sur leur téléphone.

Mais à force de dire en permanence où nous sommes, notre portable est devenu un véritable mouchard, capable de nous traquer à notre insu... Une aubaine pour les publicitaires, les géants du net, et même les enseignes - qui peuvent cibler le contenu qu'ils vous envoient.

La géolocalisation est désormais une arme commerciale redoutable. Envoyé spécial a enquêté sur ce phénomène mondial qui menace notre vie privée.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source

:
http://www.francetvinfo.fr/replay-magazine/france-2/envoye-special/envoye-special-du-jeudi-12-fevrier-2015_822079.html

Gmail et Inbox : Google va-t-il trop loin ?

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Gmail et Inbox : Google va-t-il trop loin ?</p>
---	--

Google vient de lancer Inbox, une version nouvelle et plus structurée de Gmail. La solution soulève de nombreuses questions autour de l'utilisation et de la protection des données personnelles et notamment : quel est l'objectif de Google avec Inbox ?

Inbox présente un grand nombre de fonctionnalités intéressantes : une bonne classification des e-mails, un algorithme intelligent, une interface plus ergonomique et facile à utiliser, en particulier à partir d'un téléphone mobile. Cependant, il subsiste quelques zones d'ombre, que ce soit avec Gmail ou Inbox.

Google se positionne parmi les acteurs qui protègent la vie privée de ses utilisateurs, alors qu'il met tout en œuvre dans ses outils pour analyser leur comportement. Nous savons tous que les données qui transitent dans nos e-mails sont analysées et utilisées, soit pour classer nos e-mails, soit pour nous envoyer/identifier une publicité ciblée. Google analyse les données et doit donc les stocker pour y avoir accès à tout moment.

Peut-on continuer à parler de vie privée lorsqu'il n'y a ni option ni moyen d'interdire l'accès à mes données ?

Inbox propose à l'utilisateur de faire le tri et de filtrer les e-mails commerciaux et les newsletters, que celui-ci peut désormais recevoir dans des catégories (« promotions », « réseaux sociaux », etc.). Pourtant, Google pousse des publicités vers les utilisateurs grâce à ce même outil. Alors Google est-il vraiment impartial lorsque Inbox filtre et classifie les e-mails ? La publicité est tout de même l'un des principaux revenus de Google... AdWords a d'ailleurs évolué pour devenir la principale source de revenus de Google et les recettes publicitaires totales de Google ont dépassées les 50 milliards de dollars en 2013, faisant de lui le leader, bien loin devant ses concurrents.

La principale différence entre Google Inbox et Gmail résulte dans l'affichage des publicités : apparemment, il n'y a pas de pub dans Inbox alors qu'il y en a toujours dans Gmail. Cela signifie-t-il que les publicités sont cachées... peut-être dans ce que Google appelle les « Bundle » (groupement de plusieurs emails) ? Car, il est difficile de croire que Google va supprimer l'affichage des publicités dans l'un de ses principaux services. Par contre, il est fort probable qu'ils continuent à utiliser l'une de leurs tactiques bien rodées qui consiste à promouvoir de nouvelles offres sans publicité au départ...

Avec Inbox, Google offre un algorithme, une classification et de nombreuses autres fonctionnalités d'un très bon niveau. Toutefois, sur le marché du filtrage des e-mails (de l'anti-spam à la solution de graymail management), seul Google a besoin de lire le contenu des e-mails alors que les autres acteurs se basent sur sa structure et d'autres paramètres pour définir sa nature. Par ailleurs, les pure-players qui offrent des solutions identiques de filtrage des e-mails, ne tirent aucun bénéfice de la publicité. Ils sont donc impartiaux dans la classification, aucun émetteur ne sera mis en avant au détriment d'un autre. Ainsi, le contenu des e-mails n'influence pas les contenus et les publicités lors des connexions du navigateur. On peut facilement comparer cette situation avec une affaire du passé concernant le paiement de Google vers AdBlock.

Les débats autour de la protection de la vie privée et des données personnelles n'ont jamais été aussi présents. Les solutions du type Gmail et Inbox sont largement utilisées par le grand public parce qu'elles sont gratuites et performantes. Toutefois, les utilisateurs n'ont pas forcément pris conscience de l'utilisation de leurs données. Quand une solution est gratuite, cela signifie que l'utilisateur est le produit... Si cela peut être acceptable pour le grand public (à voir sur le long terme), dans le monde de l'entreprise, la confidentialité des données doit être prise au sérieux. Le choix d'une solution de graymail management doit se faire en connaissance de cause.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.journaldunet.com/ebusiness/expert/59293/gmail-et-inbox-google-va-t-il-trop-loin.shtml>

Google monte une équipe de supers hackers pour traquer les failles informatiques



Une équipe de
supers hackers
pour traquer les
failles
informatiques

Google veut éradiquer les bugs qui peuvent être exploités par les pirates, mais aussi le gouvernement.

On croirait lire le scénario d'un film d'espionnage. Google a annoncé la création d'une équipe spéciale chargée de traquer les failles informatiques. Dénommée Project Zero, cette nouvelle équipe de sécurité sera composée des meilleurs hackers. Parmi eux, George Hertz, un Américain de 24 ans, surtout connu pour avoir piraté l'écran verrouillé de l'iPhone à l'âge de 17 ans et la Playstation 3, raconte le magazine spécialisé Wired. Quand il a découvert, au début de l'année, des failles dans le système d'exploitation de Google, Chrome OS, l'entreprise l'a payé 150.000 dollars pour les corriger. Outre Hertz, Project Zero accueille d'autres hackers célèbres, et Chris Evans, le recruteur du projet, continue de chercher des talents.

Project Zero sera chargée de trouver les failles dites «zero-day», c'est à dire des vulnérabilités qui n'ont pour l'instant jamais été découvertes et peuvent être dangereuses si elles sont exploitées par des pirates. L'équipe travaillera sur n'importe quel produit, et donc pas uniquement sur ceux de Google. «Nous ne posons pas de limite particulière à ce projet et travaillerons à l'amélioration de la sécurité de n'importe quel programme informatique utilisé par de nombreuses personnes. Nous porteront une grande attention aux techniques, aux cibles et aux motivations des attaquants», explique Chris Evans dans son communiqué.

Une réponse de Google à Heartbleed

Ce projet de Google arrive après Heartbleed, la faille de sécurité qui a secoué Internet il y a quelques mois. Fin avril déjà, l'entreprise s'associait à Facebook, Microsoft et d'autres pour lancer la Core Infrastructure Initiative. Un regroupement qui finance les projets Open Source en difficulté financière, et donc ceux qui seraient le plus exposés à une faille de sécurité passée inaperçue. Project Zero c'est aussi la réponse de Google à la NSA. La firme a mal encaissé les failles utilisées par l'agence américaine pour espionner ses utilisateurs. Google a déjà mis en place de nouveaux mécanismes de sécurité pour mieux protéger ses données.

Le mythe des hackers embauchés par les entreprises dont ils révèlent les failles n'est pas nouveau. En 2011, Apple embauchait Nicholas Allegra. À 19 ans, il était un membre éminent de la communauté du jailbreaking, c'est à dire du débridage d'iOS (le système d'exploitation des iPads et iPhones). Un an plus tard, la firme embauchait Kristin Paget dans son équipe de sécurité. Cette informaticienne avait longtemps fait partie d'un groupe de hackers éminents qui avait révélé des failles chez Microsoft.

Cet article vous a plu ? Laissez-nous un commentaire (Source de progrès)

Références :

<http://www.lefigaro.fr/secteur/high-tech/2014/07/16/01007-20140716ARTFIG00221-google-monte-une-equipe-de-supers-hackers-pour-traquer-les-failles-informatiques.php>

Google espionne et dénonce des pédophiles aux Etats Unis. Qu'en est t-il en France ?

Google espionne et dénonce des pédophiles aux Etats Unis. Qu'en est t-il en France ?

Google a fait arrêter un Américain qui échangeait des photos pédopornographiques. Une pratique dont la légalité reste à prouver.

Il a alerté les autorités après avoir découvert des photos pédopornographiques dans les e-mails d'un habitant de Houston (Texas, Etats-Unis), rapporte la chaîne locale KHOU. Ce Texan, déjà coupable d'agression sexuelle sur un garçon de 8 ans en 1994, a été inculpé pour possession de pornographie infantile et promotion de pédopornographie.