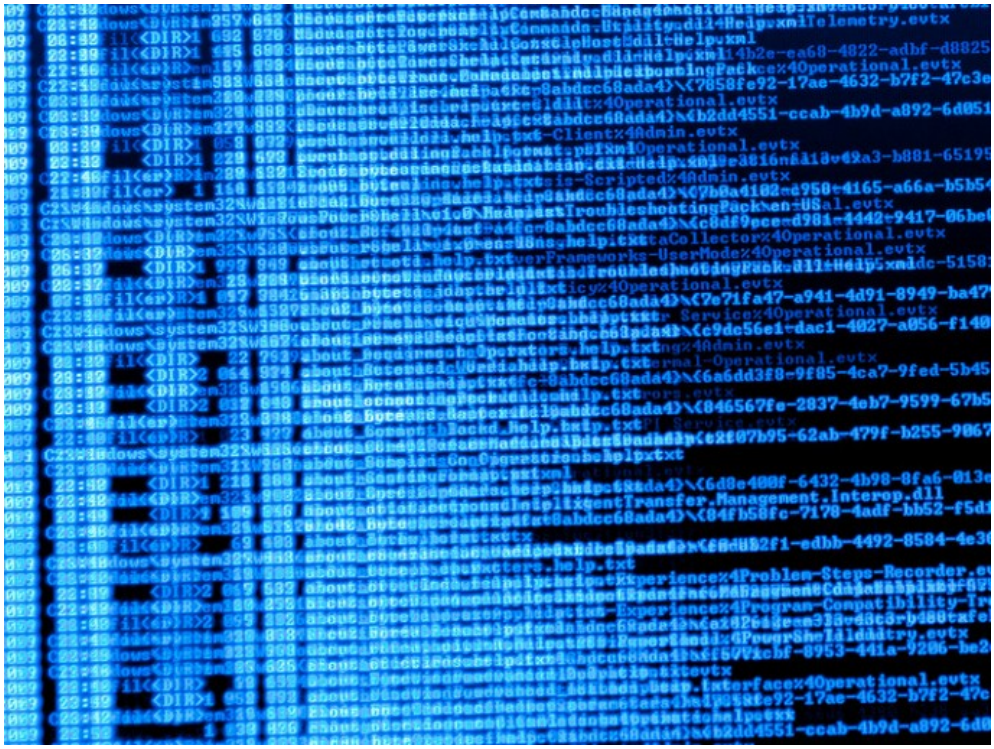
Un DSI laisse des backdoors pour pirater son ancien employeur



Un DSI laisse des backdoors pour pirater son ancien employeur

Un ancien responsable IT de Columbia Sportswear a laissé 2 backdoors pour récupérer des documents commerciaux utiles à son nouvel employeur.

En matière de sécurité informatique, la menace n'est pas uniquement à l'extérieur de l'entreprise, mais aussi à l'intérieur. Columbia Sportswear, fabricant de vêtements de sports, vient d'en faire l'amère expérience.
En effet, la Cour de l'Oregon va être amené à se prononcer sur une affaire concernant Michael Leeper, ancien DSI de Columbia Sportswear. Il est accusé de vol de données confidentielles au bénéfice d'un partenaire commercial.
Petit rappel historique, Michael Leeper a démarré sa carrière chez Columbia en 2000, comme responsable de l'équipe en charge des PC. Il obtient des promotions pour atteindre le poste de directeur des infrastructures technologiques où il est en charge de la maintenance du système d'information de Columbia et de signer les contrats avec les fournisseurs technologiques. Il était en contact notamment avec Denali, un fournisseur qu'il a rejoint en 2014.

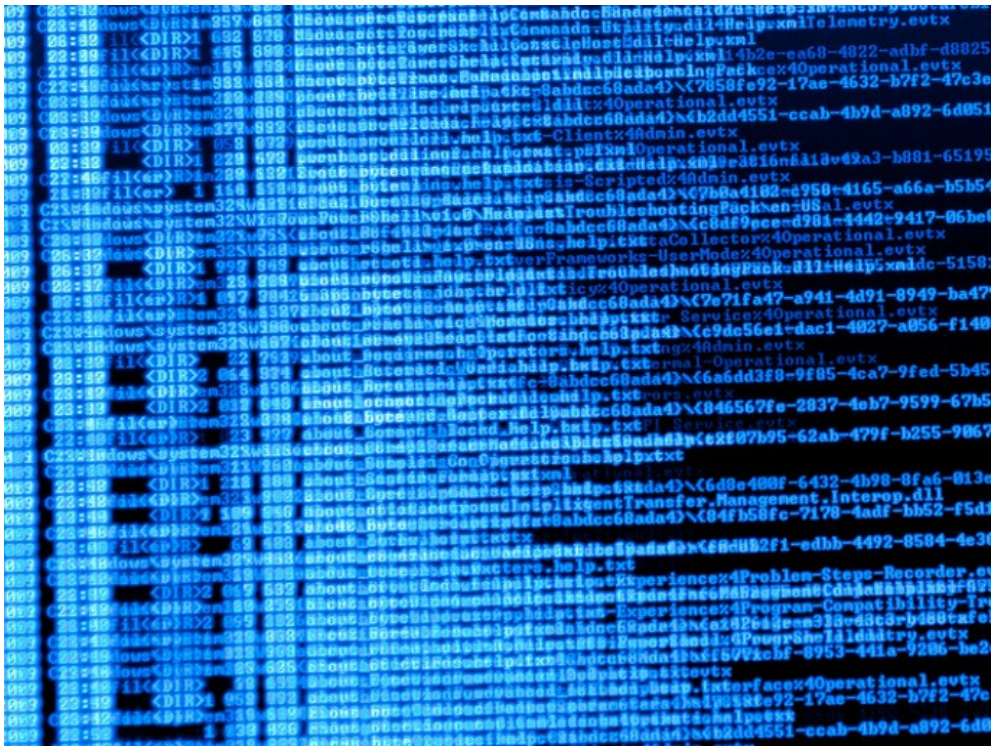
Rester dans le réseau de manière masquée

Mais, juste avant de partir, le responsable IT se serait créé un compte réseau sous le nom « Jeff Maning », aussi appelé « jmanning ». Ce qui lui aurait permis d'accéder au réseau de Columbia, y compris via le VPN et le VDI de la société. Un accès utilisé plus de 700 fois par Michael Leeper pendant 2 ans, afin de voler des documents sensibles de Columbia (plan d'affaires, budget IT, etc) au profit de Denali selon l'accusation. Il aurait mis en place une seconde backdoor (« svcmon ») liée à un compte utilisé par les administrateurs systèmes pour surveiller l'activité réseau. Avant de partir, Michael Leeper s'y serait octroyé le privilège maximal.
Dans sa plainte, Columbia estime que Michael Leeper a eu accès à des e-mails sur des accords commerciaux dans lesquels Denali avait des intérêts financiers. Le prestataire s'est défendu dans un communiqué en indiquant qu'une telle affaire « *ne reflète nullement la politique de Denali et ses valeurs* ». La société précise coopérer à l'enquête et a donné congé à son CTO, Michael Leeper, afin, officiellement, qu'il puisse organiser sereinement sa défense…[lire la suite]

Réagissez à cet article

Source : *Quand un DSI laisse des backdoors pour pirater son ancien employeur*

Un DSI laisse des backdoors pour pirater son ancien employeur



Un DSI laisse des backdoors pour pirater son ancien employeur

---

Un ancien responsable IT de Columbia Sportswear a laissé 2 backdoors pour récupérer des documents commerciaux utiles à son nouvel employeur.

En matière de sécurité informatique, la menace n'est pas uniquement à l'extérieur de l'entreprise, mais aussi à l'intérieur. Columbia Sportswear, fabricant de vêtements de sports, vient d'en faire l'amère expérience.
En effet, la Cour de l'Oregon va être amené à se prononcer sur une affaire concernant Michael Leeper, ancien DSI de Columbia Sportswear. Il est accusé de vol de données confidentielles au bénéfice d'un partenaire commercial.
Petit rappel historique, Michael Leeper a démarré sa carrière chez Columbia en 2000, comme responsable de l'équipe en charge des PC. Il obtient des promotions pour atteindre le poste de directeur des infrastructures technologiques où il est en charge de la maintenance du système d'information de Columbia et de signer les contrats avec les fournisseurs technologiques. Il était en contact notamment avec Denali, un fournisseur qu'il a rejoint en 2014.

Rester dans le réseau de manière masquée

Mais, juste avant de partir, le responsable IT se serait créé un compte réseau sous le nom « Jeff Maning », aussi appelé « jmanning ». Ce qui lui aurait permis d'accéder au réseau de Columbia, y compris via le VPN et le VDI de la société. Un accès utilisé plus de 700 fois par Michael Leeper pendant 2 ans, afin de voler des documents sensibles de Columbia (plan d'affaires, budget IT, etc) au profit de Denali selon l'accusation. Il aurait mis en place une seconde backdoor (« svcmon ») liée à un compte utilisé par les administrateurs systèmes pour surveiller l'activité réseau. Avant de partir, Michael Leeper s'y serait octroyé le privilège maximal.
Dans sa plainte, Columbia estime que Michael Leeper a eu accès à des e-mails sur des accords commerciaux dans lesquels Denali avait des intérêts financiers. Le prestataire s'est défendu dans un communiqué en indiquant qu'une telle affaire « *ne reflète nullement la politique de Denali et ses valeurs* ». La société précise coopérer à l'enquête et a donné congé à son CTO, Michael Leeper, afin, officiellement, qu'il puisse organiser sereinement sa défense…[lire la suite]

Réagissez à cet article

Source : *Quand un DSI laisse des backdoors pour pirater son ancien employeur*

Bordeaux : des drones pour mettre des amendes sur les routes

Bordeaux : des drones pour mettre des amendes sur les routes

Comment les drones vont changer nos vies Progressivement, les avions sans pilote se déploient dans de multiples secteurs d'activité, mais le marché, prometteur, peine encore à décoller, freiné par la législation.…[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 sur cette page.

Réagissez à cet article

---

3 auteurs d'arnaques aux faux

sentiments arrêtés : 235 ans de prison pour les trois prévenus

	3 auteurs d'arnaques aux faux sentiments arrêtés : 235 ans de prison pour les trois prévenus

Trois individus de nationalité nigériane ont été condamnés aux États-Unis à une peine totale de 235 ans de prison. Des adeptes de l'arnaque sentimentale.

Âgés de 30 à 45 ans, trois ressortissants nigérians ont été condamnés la semaine dernière aux États-Unis à des peines de 25 ans, 95 ans et 115 ans de prison. Membres d'un groupe de cybercriminels d'une vingtaine de personnes actif depuis au moins 2001, ils avaient été extradés depuis l'Afrique du Sud en 2015.

Ce groupe était basé au Nigeria et aux États-Unis. Les individus sont accusés d'avoir mené et participé à diverses escroqueries en ligne ayant causé des pertes de plusieurs dizaines de millions de dollars. Parmi celles-ci, l'arnaque sentimentale.

En l'occurrence, un arnaqueur utilisait par exemple une fausse identité sur un site de rencontres afin d'établir une relation amoureuse avec une victime. Une fois la confiance de la victime gagnée, elle était incitée à envoyer de l'argent.

Les arnaqueurs pouvaient aussi faire effectuer des transferts d'argent. Du blanchiment d'argent via Western Union et MoneyGram qui sont des noms régulièrement évoqués par des adeptes de l'arnaque sentimentale.

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 d'expertises, d'audits, de formations et de sensibilisation 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

---

Réagissez à cet article

Source : *Arnaque à la nigériane : 235 ans de prison pour trois prévenus*

---

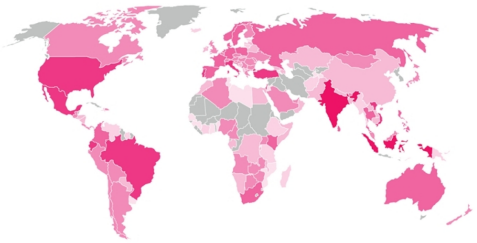
250 millions de PC infectés par un nouveau malware

250 millions de PC infectés par un nouveau malware

Après Wannacry, c'est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines pour exiger de l'argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.

Les internautes n'ont pas fini de s'arracher les cheveux à cause des virus informatiques. Après Wannacry qui bloquait les ordinateurs pour demander des rançons, voici le malware Fireball. Ce logiciel asiatique qui infecte les ordinateurs a été détecté par les experts de **Check Point**.
Il prend discrètement le contrôle d'un PC pour détourner les recherches et récupérer les données. Il aurait déjà infecté plus de 250 millions de machines dans le monde. Les zones géographiques les plus touchées sont l'Inde, le Brésil et l'Amérique, mais l'Europe et la France ne sont pas épargnées.

Ce logiciel n'est pourtant pas le fruit d'un gang de hackers. C'est officiellement un adware -nom donné aux logiciels publicitaires- qui a été développé en toute légalité par **Rafotech**, une agence de marketing digitale chinoise qui a pignon sur rue. Et pour le répandre, l'entreprise l'a inséré discrètement dans des suites logicielles téléchargeables gratuitement, tels que « FVP Imageviewer », « Deal Wifi » ou « SoSo Desktop ». Mais il ne se contente pas de diffuser de la pub.



Check Point – Diffusion mondiale de Fireball
Une fois installé, Fireball change la page d'accueil du navigateur pour afficher un faux moteur de recherche (« Trotux ») qui redirige les recherches vers des moteurs que l'utilisateur n'aura pas forcément choisis. Il va également installer un système de traçage pour collecter des données de navigation, mais aussi, selon Check Point, les mots de passe ou les numéros de cartes bancaires.
Fireball pourrait également prendre le contrôle d'une machine pour installer et d'exécuter à distance des logiciels espions. Il crée aussi une porte dérobée pour espionner ses victimes. Les experts en sécurité conseillent aux victimes de le supprimer au plus vite. Si la page d'accueil de votre PC a été modifiée sans votre intervention, il y a de grande chance qu'il ait été contaminé.
[Source : BFM Business]

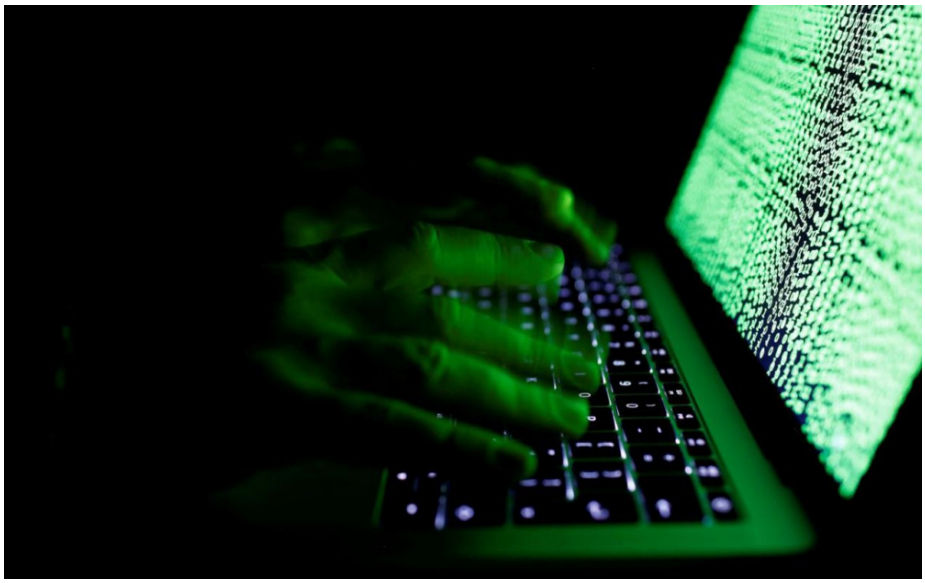
Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

---

Réagissez à cet article

Source : *Après Wannacry, c'est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines pour exiger de l'argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.*

Victime de cyberattaque ? Une plateforme d’aide aux victimes existe : ACYMA



Victime de cyberattaque ? Une plateforme d’aide aux victimes existe : ACYMA

Le gouvernement a lancé une plateforme Internet d'aide aux victimes de piratage et autres cyberattaques.
L'ordinateur familial ne répond plus, victime d'un virus. Pis, ses données ont été cryptées par un rançongiciel comme le désormais célèbre Wannacry. Pas de panique. Hier, le gouvernement a lancé le site www.cybermalveillance.gouv.fr afin de répondre en urgence aux victimes d'attaques informatiques de plus en plus dangereuses.
Cette plate-forme met en relation des victimes – particuliers comme entreprises – avec des prestataires dans leur zone de vie. De plus, le site regorge de vidéos et de fiches pratiques afin d'adopter les bons réflexes d'hygiène numérique. La région Hauts-de-France sera à partir d'aujourd'hui zone de test. L'initiative sera généralisée à toute la France en octobre…[lire la suite]

Denis JACOPINI : Nous sommes prestataire inscrit sur la plateforme ACYMA (www.cybermalveillance.gouv.fr) depuis les premiers jours et en relation avec l'ANSSI depuis fin 2016 pour apporter nos compétences et notre expérience à ce projet .
Notre grande connaissance du monde de la cybercriminalité et les nombreuses expertises judiciaires sur lesquelles nous intervenons vous garantissent non seulement l'usage des meilleurs outils en matière d'investigation numérique (forensic) et un respect minutieux des procédures de respect de l'intégrité de la preuve pour un usage judiciaire des données collectées.
Nous pouvons intervenir indépendamment ou en assistance d'un huissier et nos dossiers peuvent être utilisés en justice.
Contactez-nous

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 d'expertises, d'audits, de formations et de sensibilisation 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 RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Une plateforme d'aide en cas de cyberattaque – Le Parisien*

Des clés de déchiffrement pour le ransomware Crysis mises en ligne

Des clés de déchiffrement pour le ransomware Crysis mises en ligne

---

Au total, 200 clés principales ont été publiées sur Internet. Elles permettent à des victimes du ransomware de déchiffrer leurs fichiers et de récupérer ainsi le contrôle de leurs données.

Le monde a été secoué par WannaCry, un ransomware qui a causé des perturbations et des bouleversements dans d'importants services et des entreprises au cours de la dernière semaine. Mais il y a de bonnes nouvelles pour les victimes d'un autre rançongiciel baptisé Crysis, avec la diffusion auprès du public de 200 clés principales.
Publiées sur le forum BleepingComputer, les clés peuvent être utilisées par les victimes du ransomware, ainsi que par les entreprises de sécurité spécialisée dans la création d'outils de déchiffrement.
Les clés, téléchargées sur Pastebin, sont valides, ont confirmé des chercheurs en sécurité. Les utilisateurs des clés ont également confirmé qu'ils avaient pu recouvrer l'accès à leurs fichiers.

Si vous avez été affecté par cette souche de ransomware, vous pouvez télécharger un outil de déchiffrement fourni par l'éditeur de sécurité ESET…[lire la suite]

Réagissez à cet article

Source : *Ransomware Crysis : des clés principales mises en ligne – ZDNet*

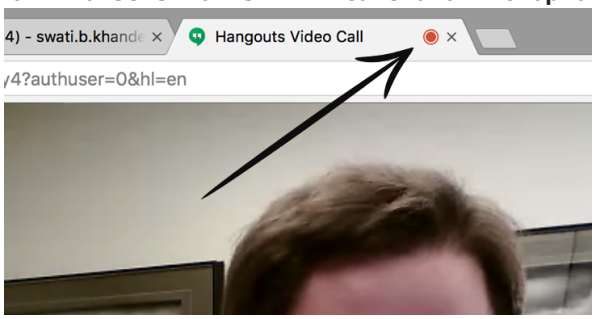
Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication

Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication

Sounds really scary! Isn't it? But this scenario is not only possible but is hell easy to accomplish.A UX design flaw in the Google's Chrome browser could allow malicious websites to record audio or video without alerting the user or giving any visual indication that the user is being spied on.

AOL developer Ran Bar-Zik reported the vulnerability to Google on April 10, 2017, but the tech giant declined to consider this vulnerability a valid security issue, which means that there is no official patch on the way.

How Browsers Works With Camera & Microphone



Before jumping onto vulnerability details, you first need to know that web browser based audio-video communication relies on WebRTC (Web Real-Time Communications) protocol – a collection of communications protocols that is being supported by most modern web browsers to enable real-time communication over peer-to-peer connections without the use of plugins.

However, to protect unauthorised streaming of audio and video without user's permission, the web browser first request users to explicitly allow websites to use WebRTC and access device camera/microphone.

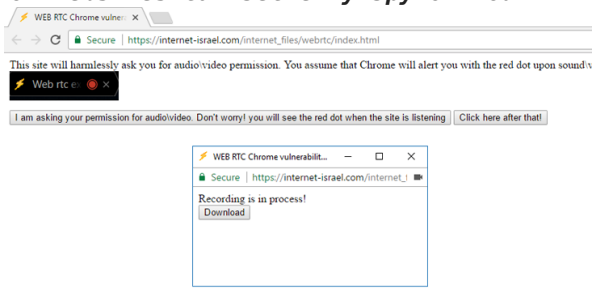
Once granted, the website will have access to your camera and microphone forever until you manually revoke WebRTC permissions.

In order to prevent 'authorised' websites from secretly recording your audio or video stream, web browsers indicate their users when any audio or video is being recorded.

« Activating this API will alert the user that the audio or video from one of the devices is being captured, » Bar-Zik wrote on a Medium blog post. « This record indication is the last and the most important line of defense. »

In the case of Google Chrome, a red dot icon appears on the tab, alerting users that the audio or video streaming is live.

How Websites Can Secretly Spy On You



The researcher discovered that if any authorised website pop-ups a headless window using a JavaScript code, it can start recording audio and video secretly, without the red dot icon, giving no indications in the browser that the streaming is happening…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication*

Judy Android Malware Infects Over 36.5 Million Google Play Store Users

Judy Android Malware Infects Over 36.5 Million Google Play Store Users

Security researchers have claimed to have discovered possibly the largest malware campaign on Google Play Store that has already infected around 36.5 million Android devices with malicious ad-click software.

The security firm Checkpoint on Thursday published a blog post revealing more than 41 Android applications from a Korean company on Google Play Store that make money for its creators by creating fake advertisement clicks from the infected devices.

All the malicious apps, developed by Korea-based Kiniwini and published under the moniker ENISTUDIO Corp, contained an adware program, dubbed Judy, that is being used to generate fraudulent clicks to generate revenue from advertisements.

Moreover, the researchers also uncovered a few more apps, published by other developers on Play Store, inexplicably containing the same the malware in them…[lire la suite]

Réagissez à cet article

Source : *Judy Android Malware Infects Over 36.5 Million Google Play Store Users*

Un simple lien permet de faire planter les PC Windows 7 et 8.1

Un simple lien permet de faire planter les PC Windows 7 et 8.1

Un bug du NTFS exploitable depuis le web met à genoux les PC Windows. Windows 10 est épargné, mais Windows 7 et 8.1 devront être corrigés.

À l'époque de Windows 95 et Windows 98, un bug permettait de faire planter un PC via un simple document au nom non supporté par le système de fichiers. Il suffisait pour cela d'accéder à certains périphériques, représentés par un nom de fichier virtuel.

Aussi incroyable que cela paraisse, un bug similaire existe dans **Windows 7 et Windows 8.1**, dévoile *Ars Technica*. Tenter d'accéder au fichier « **c:\$MFT\123** » bloque complètement le système de fichiers NTFS. La MFT n'est pas en principe accessible directement, mais en la traitant comme un dossier, son accès est totalement bloqué. Tout le système se trouve alors figé, ne pouvant plus accéder aux données de la partition NTFS concernée. Seule solution : redémarrer la machine…[lire la suite]

Réagissez à cet article

Source : *Un simple lien permet de faire planter les PC Windows 7 et 8.1*