

Un ado attaque sa mère en justice parce qu'elle lui avait confisqué son smartphone



Un ado
attaque sa
mère en
justice
parce
qu'elle
lui avait
confisqué
son
smartphone

Parfois les adolescents ont des réactions bien surprenantes face à certaines situations. En Espagne, un ado de 15 ans a attaqué sa mère en justice pour lui avoir confisqué son smartphone. Une réaction disproportionnée que le juge n'a pas manqué de souligner. Non seulement le jeune homme a perdu son procès, mais il a en plus eu droit à un joli sermon.

Ah l'adolescence ! Cette période difficile de passage à l'âge adulte laisse place parfois à des réactions bien étonnantes. Néanmoins, certains ados vont tout de même plus loin que d'autres. Et dans le genre relation conflictuelle avec les parents, celui-ci est plutôt bien classée.

En Espagne, à Almeria, un adolescent de 15 ans a porté plainte contre sa mère parce que cette dernière lui avait confisqué son smartphone. Oui, c'est assez hallucinant, mais c'est bien vrai. Toute la presse locale en Andalousie en a parlé.

Un ado porte plainte contre sa mère qui l'avait privé de son smartphone

Il s'agit pourtant d'une histoire on ne peut plus banale. L'adolescent à l'origine de la plainte avait des mauvais résultats scolaires depuis quelques temps. Afin de le recadrer, sa mère lui a confisqué son smartphone. Une mesure que de nombreux parents peuvent prendre, rien de plus normal.

Mais plutôt que de pester contre sa mère et d'aller bouder à l'arrêt de bus avec ses copains, le jeune garçon de 15 ans a décidé d'aller porter plainte contre sa mère. Face à une demande si surprenante, les policiers ont tenté de raisonner le jeune homme, mais ce dernier a bien validé la plainte pour mauvais traitements.

Le juge félicite la mère

La plainte validée, la mère et l'adolescent sont passés devant le juge Luis Columna. L'histoire ne nous dit pas s'ils y sont partis ensemble en voiture. Toujours est-il qu'après avoir écouté les deux partis, le juge a non seulement donné raison à la mère, mais il l'a en plus félicitée...[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.



[Contactez-nous](#)

Réagissez à cet article

Source : Insolite : un ado attaque sa mère en justice parce qu'elle lui avait confisqué son smartphone

**Mettez à jour de toute
urgence votre Windows**

	Mettez à jour de toute urgence votre Windows
---	---

Une vulnérabilité critique découverte par Google et touchant Windows a vite été corrigée par Microsoft. Au bénéfice de ceux qui laissent Windows Update activé.

La semaine dernière, le 24 mai, Microsoft a discrètement corrigé une vulnérabilité critique du composant MsMpEng de Windows. Plus précisément, MsMpEng est un processus de base de Windows Defender, le logiciel anti-malware livré en standard sur Windows 10 et 8.1, et installable sur Windows 7. Découverte le 12 mai dernier par Tavis Ormandy, chercheur en sécurité du Google Zero Project, cette faille autorise l'exécution de programmes non certifiés et donc potentiellement malveillants.

« *MsMpEng comprend un émulateur système x86 complet qui est utilisé pour exécuter des fichiers non fiables qui ressemblent à des programmes exécutables. L'émulateur s'exécute sous la forme NT AUTHORITY\SYSTEM et ne réside pas dans un bac à sable* », explique l'expert sur la page signalant le bug. Et sur laquelle il revient avec moult détails techniques sur le mode d'exploitation de la vulnérabilité.

Cette nouvelle brèche qui touche l'anti-malware de Microsoft est la deuxième que Tavis Ormandy dénicher à quelques jours d'intervalle. Le 9 mai dernier, une faille de MsMpEng risquait d'infecter les utilisateurs... qui lançaient une inspection de leur machine à l'aide de l'outil de sécurité. Paradoxalement, les utilisateurs qui avaient désactivé le scan automatique en étaient donc protégés...[lire la suite]

Denis JACOPINI :

Vous avez aussi la possibilité (et nous vous recommandons fortement) d'installer un logiciel de sécurité géré par ceux pour qui la cybersécurité est le métier. Nous vous recommandons depuis 1996 les produits ESET et en particulier celui-ci (cliquez).

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.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Microsoft corrige encore Windows Defender en toute discrétion*

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]

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.



[Contactez-nous](#)

Réagissez à cet article

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

Microsoft corrige encore Windows Defender en toute discrétion



Mettez
à jour
de
toute
urgence
votre
Windows

Une vulnérabilité critique découverte par Google et touchant Windows a vite été corrigée par Microsoft. Au bénéfice de ceux qui laissent Windows Update activé.

La semaine dernière, le 24 mai, Microsoft a discrètement corrigé une vulnérabilité critique du composant MsMpEng de Windows. Plus précisément, MsMpEng est un processus de base de Windows Defender, le logiciel anti-malware livré en standard sur Windows 10 et 8.1, et installable sur Windows 7. Découverte le 12 mai dernier par Tavis Ormandy, chercheur en sécurité du Google Zero Project, cette faille autorise l'exécution de programmes non certifiés et donc potentiellement malveillants.

« MsMpEng comprend un émulateur système x86 complet qui est utilisé pour exécuter des fichiers non fiables qui ressemblent à des programmes exécutables. L'émulateur s'exécute sous la forme NT AUTHORITY\SYSTEM et ne réside pas dans un bac à sable », explique l'expert sur la page signalant le bug. Et sur laquelle il revient avec moult détails techniques sur le mode d'exploitation de la vulnérabilité.

Cette nouvelle brèche qui touche l'anti-malware de Microsoft est la deuxième que Tavis Ormandy dénicher à quelques jours d'intervalle. Le 9 mai dernier, une faille de MsMpEng risquait d'infecter les utilisateurs... qui lançaient une inspection de leur machine à l'aide de l'outil de sécurité. Paradoxalement, les utilisateurs qui avaient désactivé le scan automatique en étaient donc protégés...[lire la suite]

Denis JACOPINI :

Vous avez aussi la possibilité (et nous vous recommandons fortement) d'installer un logiciel de sécurité géré par ceux pour qui la cybersécurité est le métier. Nous vous recommandons depuis 1996 les produits ESET et en particulier celui-ci (cliquez).

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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Microsoft corrige encore Windows Defender en toute discrétion*

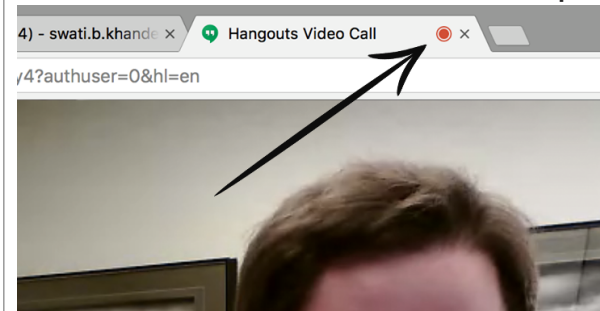
Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication



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.

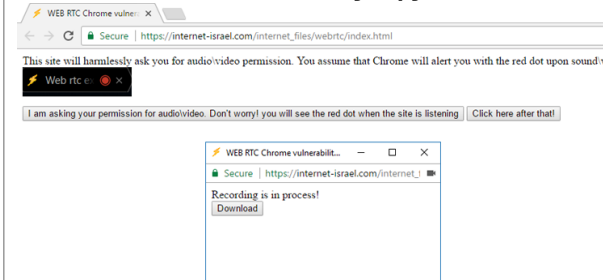
Once granted, the website will have access to your camera and microphone forever until you manually revoke WebRTC permissions.

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.



[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]

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.



[Contactez-nous](#)



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]

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.



[Contactez-nous](#)

Réagissez à cet article

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

RGPD : moins d'un an pour se mettre en conformité



RGPD : moins d'un an
pour se mettre en
conformité

Depuis le 25 mai dernier, les entreprises ont un peu plus de 11 mois pour se mettre en conformité avant l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD). Alors que le délai est relativement court, une récente étude du cabinet Vanson Bourne pour Compuware révèle que seules 43 % des organisations françaises disposent d'un plan complet pour s'adapter à ce règlement européen.

Pour Gerard Allison, Vice-Président EMEA chez Gigamon, il est essentiel que toutes les organisations s'y préparent dès à présent, aussi bien pour échapper aux sanctions que pour se protéger des hackers :

« Tout non-respect du RGPD exposera les entreprises à des amendes pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial. En outre, alors que ce nouveau règlement est une avancée positive dans la protection des données, les organisations doivent avoir conscience que les cybercriminels peuvent profiter de la situation en utilisant de nouvelles méthodes. Comme l'ont démontré les récents événements liés à l'attaque WannaCry, le ransomware est une technique largement utilisée par les hackers, qui évolue et peut devenir encore plus dangereuse, notamment si un pirate réussit à accéder à un réseau et que l'organisation ciblée n'a pas les outils nécessaires en place pour détecter la faille, ou simplement pour la signaler. Il pourrait alors, par exemple, menacer de la dénoncer auprès de la CNIL pour non-conformité, si elle ne paie pas la rançon. Est-il possible qu'une entreprise puisse préférer acheter le silence d'un hacker plutôt que de payer une amende pour ne pas avoir respecté le règlement ?

Ainsi, pour éviter de se retrouver en mauvaise posture et être en phase avec le RGPD, les organisations devront être capables de détecter, se protéger, prédire et contenir les menaces au cœur de leur réseau. Cela leur permettra notamment de répondre à l'obligation de signaler toute vulnérabilité dans les 72 heures au plus tard après en avoir pris connaissance, et de sauvegarder les données de leurs clients dans un endroit sûr. Et pour y parvenir, elles auront besoin d'une visibilité complète sur toutes les données qui transitent sur leurs réseaux, puisqu'on ne peut pas sécuriser ce qu'on ne voit pas...[lire la suite]

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner 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.

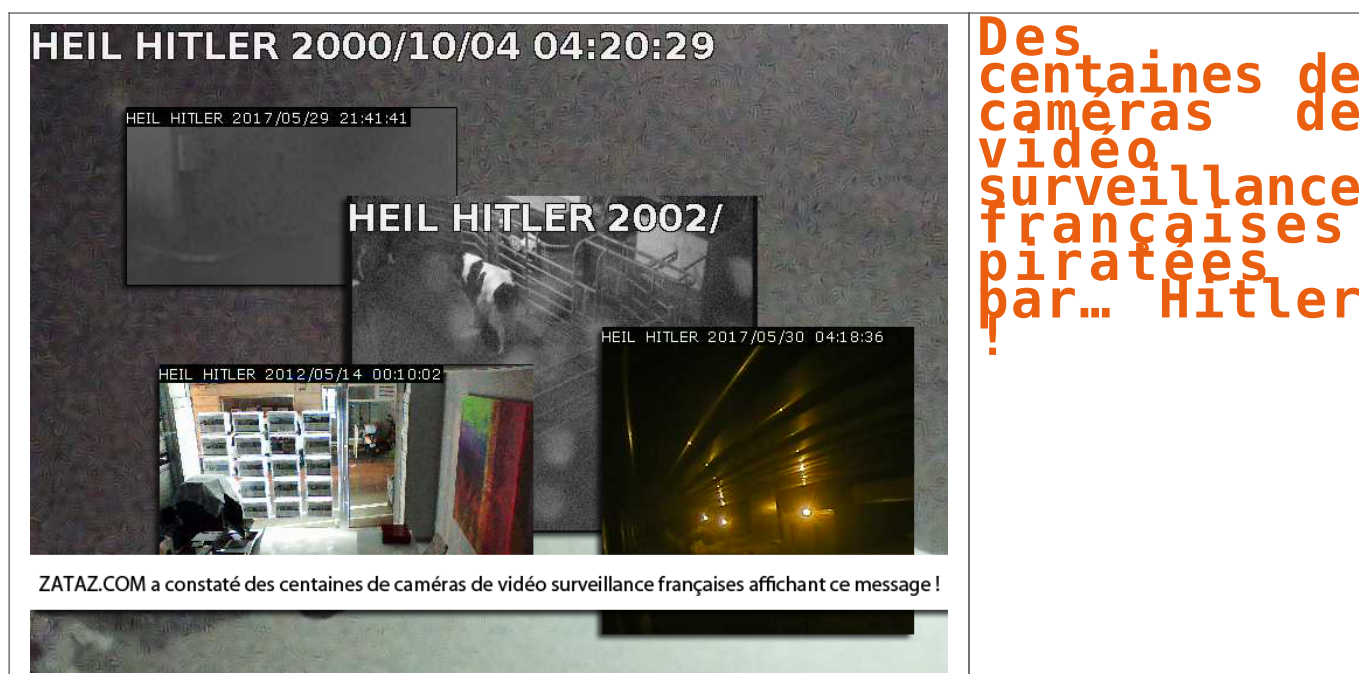


Contactez-nous



Réagissez à cet article

Des centaines de caméras de vidéo surveillance françaises piratées par... Hitler !



Piratage : Plus de 1500 caméras de vidéo surveillance d'entreprises Françaises infiltrées par un pirate informatique. Il a signé son forfait « Heil Hitler » sur les écrans de contrôle.

Je vous contais, il y a peu, de la vente d'accès à des caméras de vidéo surveillance. Un grand classique, malheureusement ! Les pirates profitent de la feignantise de certains utilisateurs à lire le mode d'emploi de leur appareil. Des utilisateurs qui ne changent pas le mot de passe usine, ou ne pensent même pas à l'activer. Bilan, l'accès aux images et à la webcam se font en deux clics de souris...[lire la suite sur ZATAZ]

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.

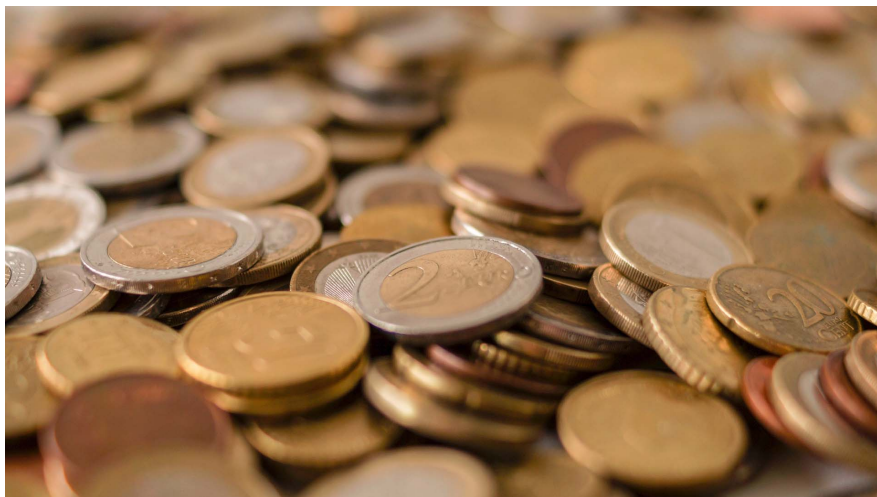


[Contactez-nous](#)

Réagissez à cet article

Source : *ZATAZ Vidéo surveillance : des centaines de caméras françaises piratées par... Hitler ! – ZATAZ*

Des banques autorisées par la Cnil à tester la reconnaissance vocale



Des banques
autorisées par
la Cnil à
tester la
reconnaissance
vocale

La Cnil indique avoir autorisé neuf établissements bancaires à expérimenter la reconnaissance vocale pour s'authentifier lors d'une connexion à un compte ou pour effectuer certaines transactions.

Lorsque vous vous connectez à votre compte bancaire, vous entrez certainement le numéro de votre compte, un mot de passe et éventuellement d'autres informations, comme votre code postal, pour être redirigé sur votre caisse régionale. Quand vous effectuez un virement bancaire ou un paiement quelconque, peut-être validez-vous la transaction en tapant un code. Ces méthodes d'authentification mises en place pour s'assurer que c'est bien vous qui cherchez à accéder au compte ou qui donnez certains ordres ne sont pas la panacée en matière de sécurité informatique mais elles ont le mérite d'être familières pour le grand public et facilement renouvelables en cas de besoin. Or aujourd'hui, elles sont concurrencées par la biométrie...[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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Neuf banques autorisées par la Cnil à tester la reconnaissance vocale – Business – Numerama*