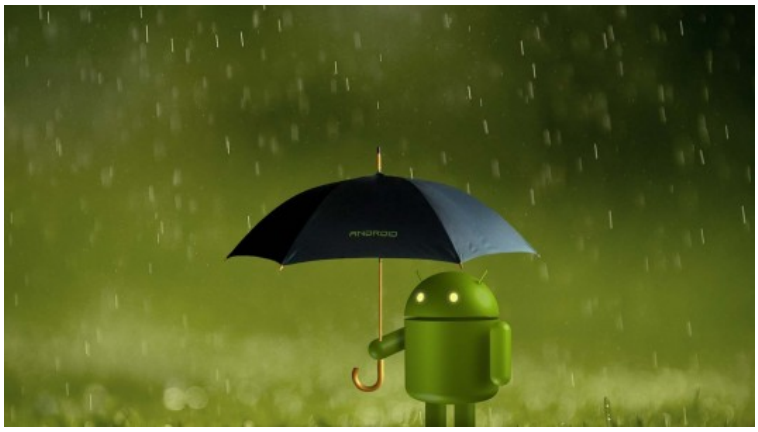
8 failles critiques dans Android corrigées

	8 failles critiques dans Android corrigées

Alors que Google s'était déjà illustré au mois de juin en apportant 28 corrections au système d'exploitation mobile Android, la firme de Mountain View a livré il y a quelques heures une nouvelle salve de correctifs. 8 failles critiques ont d'ailleurs été patchées !

Encore des corrections en masse pour Android

Souvent décrié en raison du nombre de failles qui affectent son célèbre système d'exploitation mobile, Google a une nouvelle fois livré un nombre (trop) important de patchs correctifs et le problème, c'est que plusieurs vulnérabilités corrigées sont estimées comme « critiques ».

Eh oui, aussi surprenant que cela puisse paraître, la société implantée à Mountain View vient bel et bien d'apporter 57 correctifs dont 8 ont servi à patcher des failles pouvant s'avérer être une vraie menace pour les terminaux.

Trois sets de correctifs disponibles

Le premier set, disponible depuis le 1er septembre 2016, permet de combler 25 failles Android. Deux d'entre elles étaient critiques. L'une permettait d'exécuter du code distant via une attaque de type « dépassement de mémoire » au niveau du package libutils d'Android. L'autre donnait la possibilité d'exécuter du code distant dans les composants Mediaserver d'Android.

Le deuxième set, mis en ligne le 5 septembre 2016, propose quant à lui de corriger 30 failles exposant largement l'utilisateur. Les plus critiques permettent d'obtenir des privilèges système, d'accéder à un noyau de sous-système réseau, de netfilter ou encore de driver USB…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Encore 8 failles critiques patchées dans Android

L’Agence mondiale anti-dopage victime de piratage

L’Agence mondiale anti-dopage victime de piratage

L'Agence mondiale anti-dopage (AMA ou WADA en anglais) a été victime d'un piratage. Un groupe de hackers a pu subtiliser les dossiers médicaux de quatre athlètes américaines et dévoiler des informations confidentielles. Surprise : les pirates sont russes !

Les Russes l'auraient-ils mauvaise suite à la disqualification de la quasi-totalité de leurs athlètes lors des Jeux Olympiques de Rio ? Ce vaste « nettoyage » opéré par les fédérations sportives internationales faisait suite au scandale sur le dopage d'Etat généralisé en Russie. Toujours est-il que le groupe russe Tsar Team (APT28), Fancy Bear pour les intimes, a piraté une base de données de l'AMA.
La date exacte de l'attaque n'est pas connue. Les hackers ont vraisemblablement obtenu l'accès aux serveurs de l'Agence en obtenant par phishing des mots de passe ADAMS (pour Anti-Doping Administration and Management System, le SI de l'AMA), via un compte du Comité International Olympique créé à l'occasion des JO de Rio. Ils ont ainsi pu dérober les données relatives à quatre athlètes américaines, notamment leurs dossiers médicaux détaillés.

Simone Biles, quadruple championne olympique en athlétisme

Sur les réseaux sociaux, Fancy Bear a divulgué une partie de ces informations, pointant du doigt des « *analyses anormales* » dans les dossiers des joueuses de tennis Venus et Serena Williams, de la basketteuse Elena Delle Donne et de la gymnaste Simone Biles. L'AMA a pris la défense des athlètes mises en cause, expliquant qu'elles bénéficient d'exemptions thérapeutiques. Dans le cas de Simone Biles, par exemple, il s'agit d'un traitement pour trouble du déficit de l'attention, dont il avait déjà été question lors des JO. Mais les hackers promettent bien d'autres révélations.

« Miner le système anti-dopage mondial ».

Le CIO a condamné cette attaque, « *destinée à salir la réputation d'athlètes propres* ». L'AMA elle aussi condamne, et y voit une tentative de « *miner le système anti-dopage mondial* »…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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

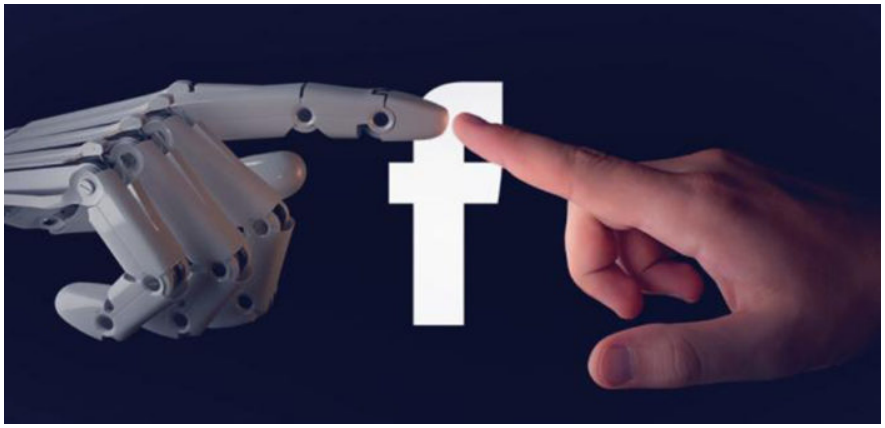
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Des hackers russes derrière le piratage de l’Agence mondiale anti-dopage

---

L’intelligence artificielle (IA) de Facebook sur le point d’être dévoilée

	L’intelligence artificielle (IA) de Facebook sur le point d’être dévoilée

---

Nous le répétons souvent au sein de nos articles, Facebook Inc. n'est plus seulement la première plateforme sociale au monde, c'est avant tout une société créant des technologies. Des technologies dont Facebook est l'édifice principale qui rend le groupe si rentable. Mais Mark Zuckerberg voit beaucoup plus loin et il a pour habitude de dévoiler ses futurs défis. Celui de cette année concerne l'élaboration d'une intelligence artificielle, rien que ça…

En janvier, Mark Zuckerberg présentait, dans une de ses publications Facebook, son nouveau challenge : « construire une intelligence artificielle comme Jarvis pour Iron Man ». Dans ces paroles, qui sont les siennes et au-delà de la référence au Comics, c'est la vision de Facebook qui s'éclaire.

Depuis le début de l'année, l'intelligence artificielle semble présentable pour Facebook. Dans un de ses récents Facebook Live à Rome, Zuckerberg a évoqué le sujet en annonçant une présentation dès septembre soit demain…

Mais à quoi consisterait cette intelligence artificielle ?
Celle-ci servirait comme un assistant pour une maison : paramétrer le réveil selon son agenda, préparer les toasts au petit-déjeuner selon une présence humaine ou non, ouvrir la porte d'entrée à des individus pré-sélectionnés par la reconnaissance faciale, augmenter la température intérieure selon la météo et une présence et on imagine bien d'autres choses. Vous me direz qu'au niveau de la domotique, il y a déjà eu de belles avancées et que programmer une cafetière ou un toast n'est pas compliqué… Mais là où Facebook veut progresser, c'est l'élaboration d'une perception artificielle capable d'entendre, de voir et d'interpréter un langage. Nous avons hâte d'avoir plus d'informations officielles de la part de la firme dès la rentrée !…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : L’intelligence artificielle de Facebook prête à être dévoilée

L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

Cour de justice de l'Union européenne a jugé aujourd'hui qu'un fournisseur de hotspot n'était pas responsable des contrefaçons réalisées par ses utilisateurs. Cependant, cet acteur pouvait se voir enjoindre d'exiger un mot de passe par une juridiction ou une autorité administrative nationale.

Le litige est né en 2010 : Sony Music avait adressé une mise en demeure à Thomas Mc Fadden. Cet exploitant d'une entreprise de sonorisation outre-Rhin avait laissé son réseau Wi-Fi ouvert sans mot de passe. Or, un tiers a pu mettre à disposition une œuvre du catalogue de la major. L'affaire était remontée jusqu'à la CJUE où les juridictions allemandes ont déversé une série de questions préjudicielles.

FAI ou exploitant de hotspot Wi-Fi, même combat

Dans son arrêt (PDF) du jour, la Cour va d'abord considérer que la fourniture d'un tel accès Wi-Fi relève de la fourniture d'un service de la société de l'information, à l'instar donc des prestations d'un FAI (article 12 de la directive de 2000). Cela implique cependant que l'exploitant du hotspot ait un rôle « *purement technique, automatique et passif* » et qu'il n'a ni la connaissance ni le contrôle des informations transmises.

Ceci vérifié, la Cour rappelle qu'un tel prestataire n'est alors pas responsable des contenus qui passent dans ses tuyaux à la triple condition :

1. de ne pas être à l'origine d'une telle transmission,
2. de ne pas sélectionner le destinataire de cette transmission et
3. de ne ni sélectionner ni modifier les informations faisant l'objet de ladite transmission.

Si ces conditions sont remplies, alors un titulaire de droit ne peut demander la moindre indemnisation à cet intermédiaire ou le remboursement de ses frais…[lire la suite]

Qu'en est-il des professionnels de l'hôtellerie qui mettent à disposition de leurs clients du Wifi ? Réagissez

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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 : CJUE : l’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

---

Comment préparer les enfants aux Réseaux Sociaux ?

Comment préparer les enfants aux Réseaux Sociaux ?

Dangers de l'Internet au-delà de logiciels malveillants, ou l'enlèvement des données par des ransomware. Sur le Net, le respect de la vie privée est mis à mal par les réseaux sociaux, les moteurs de recherche et la publicité. Dans le cas des mineurs, il y a des risques plus inquiétants, dont ils ne sont pas pleinement conscients, mais leurs parents, les enseignants et la société doivent assurer leur sécurité. Une étude récente, appelé Kids Connected, et menée par la firme de sécurité Kaspersky Lab avec iconKids et jeunesse, révèle des faits troublants sur la façon dont les enfants se comportent en ligne. Comportements qui peuvent conduire à provoquer plus de crainte.

Ce rapport montre que **les enfants âgés de 8 à 16 ans sont accros aux réseaux sociaux**. En outre, l'activité peut les mettre en danger, eux et leurs **familles**. 35% des enfants disent qu'ils ne veulent pas être sans réseaux sociaux, et sont désireux de rejoindre des groupes en leur sein, ils sont en mesure de partager beaucoup d'informations personnelles. **Le problème** est qu'ils le font sans avoir conscience que les données qu'ils partagent sont vues par de nombreux utilisateurs et peuvent être utilisées par des personnes potentiellement dangereuses.

Trop d'informations personnelles

Mais **qu'est-ce que les mineurs partagent le plus** ? La plupart des enfants, 66%, **montrent l'école** où ils étudient, 54% **des lieux qu'ils visitent**, et 22% partagent même **la gestion de leurs maisons**. Mais, 33% des enfants donnent également des **informations sur les effets de leur famille et de leurs parents**, sur leur travail (36%) ou sur **ce que leurs parents facturent** (23% des enfants).
Mais, outre le partage des données réelles, **les mineurs sont également prêts à mentir sur le réseau**, et ils le font surtout **si ça peut leur ouvrir des portes**. Un tiers des enfants est prêt à mentir au sujet de l'âge. 17% des enfants font semblant d'être plus âgés, et de modifient leur âge en fonction du web ou le service qu'ils veulent utiliser, étant donné que beaucoup d'entre eux ont des restrictions (très facile à sauter) d'âge.
Avec ces données, **les cybercriminels disposent d'informations suffisantes pour être utilisés à des fins malveillantes**. Parmi les activités criminelles qu'ils pourraient commettre, ils trouvent l'emplacement physique des mineurs. **Tous les enfants doivent apprendre à un âge précoce ce qu'ils devraient partager en ligne**, ou non. Et connaître les paramètres des réseaux sociaux de la vie privée, de sorte que seuls leurs amis peuvent voir leurs publications et leurs données.

Comprendre quelles sont vos données et la façon de les protéger

Tous les enfants et leurs parents doivent comprendre ce que sont les données personnelles, et **la façon dont on peut les protéger**. "Ceci est comparable aujourd'hui à lire et à écrire», dit Janice Richardson, consultant senior chez European Schoolnet, qui explique que **«les enfants ont besoin d'apprendre à un âge précoce que la vie privée est votre bien le plus précieux, et un droit fondamental ».**
Comme des **conseils de base** qui sont donnés par Kaspersky Lab afin d'éviter autant que possible les risques:
• Une bonne **communication est essentielle**. Il faut parler aux enfants au sujet de leurs expériences et préoccupations.
• **Réalisez les premières étapes dans les réseaux sociaux avec eux** pour créer le profil, activez les options de confidentialité, publiez votre premier poste …
• Les réseaux sociaux ont des **restrictions d'âge**. La plupart sont fixée à 13 ans. À cet âge, il est commode d'en profiter pour leur parler et leur expliquer leurs droits, les responsabilités et les préparer à l'entrée dans le monde numérique.
• Cela peut **devenir un jeu**, quelque chose que vous faites en famille: par exemple, l'impression de leur profil, accroché au mur, leurs postes … Ils pourront visualiser le public à qui est destiné chaque contenu.
• **Établir des règles** pour leur utilisation.
• **Encourager les enfants à communiquer avec vous**, ils vous apprendront de nouvelles applications récemment installées, les services qu'ils utilisent … Si cela devient une habitude depuis le début, il sera plus facile de partager des informations et de leur **parler de la vie privée et de sécurité**.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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 : La situation préoccupante des enfants dans le réseau: mentir pour accéder aux réseaux sociaux et y donner trop d’informations

---

Trend Micro ausculte la cybercriminalité underground en France

	A quoi ressemble de DarkNet ?

L'éditeur de sécurité a dressé un état des lieux de l'underground de la cybercriminalité en France. Méfiance, bitcoins et forte orientation vers les falsifications des documents sont les maîtres mots.
Un chercheur de Trend Micro s'est livré à un exercice délicat : plonger dans l'univers de la cybercriminalité souterraine en France. Connu sous le vocable « underground », cette partie du web accueille des places de marchés, des forums où s'achètent contre monnaie virtuelle des armes, de la drogue, des faux documents, mais aussi des malwares.
Dans son étude, l'éditeur japonais précise que le tréfonds du web français reste relativement modeste par rapport à d'autres pays comme la Chine ou la Russie. Néanmoins, il recense 40 000 cybercriminels sur l'underground hexagonal ayant des compétences hétérogènes (expert à novice). Ce foyer génère entre 5 à 10 millions d'euros par mois.

Une prudence de sioux
Un des leitmotiv des cybercriminels français est la prudence. Pour approcher ce monde souterrain, il faut montrer patte blanche. L'objectif est d'éviter de se faire coincer par les forces de l'ordre. Le climat de méfiance règne donc allant jusqu'à la délation (signalement des actes malhonnêtes et frauduleux) et jusqu'à l'affrontement (les places de marché se piratent mutuellement pour se piquer des clients).
L'acceptation sur les forums fait par cooptation, par évaluation de la réputation. Mais ce qui distingue le Dark Net Français, c'est le recours à des tiers de confiance (escrow en anglais). Ils jouent un rôle d'intermédiaire dans la transaction entre les deux parties pour s'assurer que chacun récupère son dû. Ces intermédiaires prennent une commission (entre 5 et 7%) sur la transaction. Certaines places de marché ont même créé leurs propres plateformes de tiers de confiance (mais faut-il encore avoir confiance ?).
La disparition des forums est aussi un grand classique, comme le précise le chercheur de Trend Micro. « Un des forums les plus en vue du French Dark Net qui recensait 40 000 utilisateurs avec la possibilité de gérer leurs transactions a fermé du jour au lendemain et les administrateurs se sont enfuis avec la caisse. Le préjudice est estimé à 180 000 euros. » Et d'ajouter que les mêmes administrateurs ont créé une nouvelle structure dans les jours suivant. Rien ne se perd, tout se crée.

Chiffrement et bitcoin de rigueur
Parmi les autres enseignements, l'underground français n'échappe pas à la vague du chiffrement des communications. Logique, avec un degré de méfiance qui frise la paranoïa, les conversations sont chiffrées et plutôt fortement, assure Trend Micro. « On est principalement sur du PGP. » De même, l'usage de Tor s'est banalisé. Pour trouver les forums ou les places de marché, il est quasiment impossible de les repérer sur le web normal. Les sites se terminent par .onion indiquant son appartenance au réseau anonymisé Tor.
Le Bitcoin et les cartes prépayées sont les moyens de paiement préférés sur l'underground français. La crypto-monnaie est traditionnellement utilisée dans ce genre de secteur. Mais la carte prépayée PCS est une spécificité française. « Elles sont devenues si populaires que certains cybercriminels vendent ce type de cartes avec de faux papiers d'identité et des fausses informations personnelles comme adresse physique, e-mail et carte SIM. L'objectif est de déverrouiller le plafond de paiement pour atteindre jusqu'à 3000 euros. L'opération coûte à peu près 60 euros », souligne Trend Micro.

Le royaume des faux documents officiels et Pass PTT
Héritage du système jacobin et du régime napoléonien, la France est la partie des papiers administratifs. On ne s'étonnera donc pas que les propositions commerciales sur le Dark Net hexagonal concernent la fraude aux documents administratifs. Fausse carte d'identité, carte grise (500 euros), carte PMR (mobilité réduite pour 40 euros), justificatif de domicile (utile pour certaines démarches), vente de points pour le permis de conduire, ouverture d'un compte bancaire (700 euros).
Autre élément typiquement français, le pass PTT. Il s'agit d'une clé dont dispose les livreurs pour ouvrir l'ensemble des boîtes aux lettres d'un immeuble. Les personnes peuvent ainsi chercher des plis contenant de l'argent, des chéquiers ou des clés de maison. Ces pass PTT sont disponibles sur les forums underground à des tarifs abordables. Un vendeur proposait 25 clés pour 220 euros, un autre vendait à l'unité au tarif de 15 euros et un troisième livrait un fichier d'impression 3D de la dite clé, rapporte l'éditeur de sécurité…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Trend Micro ausculte la cybercriminalité underground en France

---

Alerte : Une faille permet aux hackers de contrôler les connexions internet des particuliers

Alerte : Une faille permet aux hackers de contrôler les connexions internet des particuliers

---

Les chercheurs F-Secure viennent de mettre à jour une faille critique présente sur certains des routeurs Inteno. Cette vulnérabilité est assez importante pour permettre à un pirate de prendre le contrôle total de l'appareil de la victime et des communications internet. Cette découverte met en lumière les problématiques de sécurité propres aux routeurs.

La vulnérabilité récemment détectée permet au pirate d'installer son propre firmware sur l'appareil, qui continuera, en apparence, à fonctionner comme avant…mais en coulisses, des backdoors et autres fonctionnalités pirates feront leur apparition. Le hacker sera capable de lire tout le trafic non-chiffré passant par le routeur : non seulement les communications appareil-internet, mais aussi celles établies entre deux appareils. Il pourra également manipuler le navigateur de la victime afin de la rediriger vers des sites malveillants.

« En remplaçant le firmware, le pirate peut changer n'importe quelle règle du routeur », explique Janne Kauhanen, Cyber Security Expert chez F-Secure. « Vous regardez du contenu vidéo stocké sur un autre ordinateur ? Alors, le pirate y a lui aussi accès. Vous mettez un jour un autre appareil à partir du routeur ? Pourvu que l'appareil en question ne renferme pas d'importantes vulnérabilités, sinon le pirate pourra également s'en saisir. Bien entendu, le trafic https est chiffré. Les pirates n'y auront pas accès facilement. Ils peuvent néanmoins vous rediriger systématiquement vers des sites malveillants afin d'installer des malware sur votre machine. »

« Le type de routeur en question reçoit des mises à jour firmware depuis un serveur associé au fournisseur d'accès de l'utilisateur. Problème : les routeurs vulnérables ne vérifient pas si la mise à jour est valide, ni si elle vient de la bonne source. Un pirate qui a déjà eu accès au trafic circulant entre le routeur et le serveur de mise à jour du FAI (par exemple, en accédant à la distribution réseau de l'immeuble où se trouve l'appartement) peut installer son propre serveur de mises à jour. Il peut ensuite installer son firmware malveillant.

Les chercheurs expliquent qu'il ne s'agit que de la partie émergée de l'iceberg en matière de sécurité routeurs. Les ordinateurs sont de mieux en mieux protégés mais les utilisateurs ignorent souvent que le routeur peut être lui aussi vulnérable.

« C'en est ridicule de constater à quel point les routeurs vendus sont peu sécurisés », explique Janne Kauhanen. « Nous trouvons des vulnérabilités routeurs en permanence. Les firmware utilisés par les routeurs et les objets connectés sont mal conçus. L'aspect sécurité est négligé tant par les fabricants que par les clients. Personne n'y porte attention, si ce n'est le pirate, qui utilise les vulnérabilités pour détourner le trafic internet, voler des informations, répandre des malware. »

La vulnérabilité détectée, bien que sévère, n'est pas immédiatement exploitable. Un pirate doit avoir déjà acquis une certaine position sur le réseau, en réalisant une incursion entre le routeur et le point d'entrée internet. Les routeurs concernés sur les Inteno EG500, FG101, DG201. D'autres modèles sont probablement concernés….[lire la suite]

Réagissez à cet article

Original de l’article mis en page : F-Secure : Une nouvelle faille, permettant aux hackers de contrôler les connexions internet des particuliers, révélée sur plusieurs routeurs – Global Security Mag Online

---

Les données d’une banque en partie détruites à la suite d’un test…

Les données d’une banque en partie détruites à la suite d’un test…

Le fonctionnement d'un datacenter à Bucarest en Roumanie a été complètement stoppé pendant plus de 10 heures suite à un phénomène rarissime.

Une banque roumaine a fait face à un arrêt complet de ses systèmes de paiement ainsi que de ses distributeurs automatiques pendant environ 10 heures suite à un dysfonctionnement de son système d'alarme anti-incendie. L'événement est particulièrement rare et inhabituel : le son a été produit par la diffusion d'un gaz inerte au cours d'un test routinier du système d'alarme incendie.

Non seulement celui-ci a forcé le datacenter à passer hors ligne, mais il a également causé la destruction d'une douzaine de disques durs, ce qui a provoqué de sérieux dommages.
La semaine dernière, Daniel Llano, directeur de la banque ING a expliqué à ses clients que les dysfonctionnements avaient été causés par une propagation de gaz Inergen.
L'Inergen est utilisé pour éteindre des incendies sans avoir besoin de passer par un liquide ou de la mousse, les méthodes plus traditionnelles. Utile dans les espaces clos, le gaz Inergen est conservé sous forme compressé dans des cylindres et celui-ci est dispersé via le système de canalisation pour empêcher la propagation d'incendies.
En temps normal, cette technique est idéale pour les datacenters. Les liquides ou la mousse pourraient en effet facilement endommager les équipements les plus sensibles. Mais dans ce cas précis, quelque chose est allé de travers.
Lorsque le gaz a été propulsé dans le système de ventilation, la pression de celui-ci était bien trop forte, ce qui a produit un son incroyablement fort lors de la libération du gaz Inergen.
Un porte-parole d'ING a expliqué à nos confrères de Motherboard que « l'exercice s'est déroulé comme prévu, mais nous devons faire face à des dommages collatéraux. »
Une autre source citée par la publication précise que le son produit par le système s'est révélé bien plus fort qu'escompté. Évalué à plus de 130Db, celui-ci a largement dépassé l'échelle des outils de mesure du son mis en place par la banque. Malheureusement, le son provoque des vibrations, qui se sont propagées aux boîtiers des disques durs et ont endommagé les composants internes.
Motherboard relate que la situation pouvait être comparée au fait « de placer une baie de stockage à côté d'un moteur d'avion à réaction. »…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Comment un simple son a mis un datacenter à genoux — ZDNet

Le site de la Gironde infiltré par des pirates informatiques

	Le site de la Gironde infiltré par des pirates informatiques

Des pirates informatiques s'infiltrent et installent des pages malveillantes sur le site du Département de la Gironde. Un espace dédié aux personnes handicapées.

Un piratage classique, malheureusement, mais qui démontre que même face à des internautes à la culture et au savoir informatiques faibles, les dégâts peuvent être importants. Le site du Département de la Gironde en est un parfait exemple. Il est pris pour une grande cours de récréation par des « pirates ». Pour preuve, la page « Troll » John Cena n'est pas l'unique passage malveillant que j'ai pu constater. D'autres pages ont été cachées, en ce mois de septembre, par des pirates informatiques différents [SirXL3 aka Kartz], avec plus ou moins de réussite. Les archives Zone H rappellent aussi que ce même site web avait été maltraité en avril 2016 par un barbouilleur baptisé Sneaky. En avril 2015, je vous expliquais comment d'autres malveillants du numérique s'étaient invités dans le site de l'association des maires de la Gironde…[lire l'article complet]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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 : ZATAZ Le site Culture Accessible de la Gironde infiltré par des pirates informatiques – ZATAZ

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

En proposant de nouvelles règles télécom cette semaine, la Commission européenne introduirait des obligations de sécurité aux services de messagerie. Des obligations déjà en vigueur pour les opérateurs, qui réclament une parité réglementaire avec les acteurs en ligne.

Équilibrer les obligations entre opérateurs et messageries en ligne ressemble souvent à un travail de funambule, dans lequel se lancerait la Commission européenne. Dans quelques jours, l'institution doit dévoiler une révision des règles télécoms en Europe. Selon un brouillon obtenu par Reuters, elle y introduirait des obligations de sécurité pour les services de messagerie en ligne, déjà appliquées par les opérateurs.

Des obligations de signalement des brèches

À la mi-août, plusieurs médias affirmaient que la Commission européenne comptait proposer cette parité entre acteurs. Le brouillon obtenu par Reuters viendrait donc confirmer cette piste. Dans celui-ci, les services « over the top » devront ainsi signaler les brèches « *qui ont un impact important sur leur activité* » aux autorités et disposer d'un plan de continuité de l'activité. Les services qui proposent des numéros de téléphone ou d'en appeler, comme Skype, devront aussi permettre les appels d'urgence.

Pourtant, ces règles pourront être plus légères pour ces services que pour les opérateurs classiques, dans la mesure où les services ne maîtrisent pas complètement la transmission des contenus via les tuyaux. Dans l'absolu, ces règles doivent réduire l'écart d'obligations entre les acteurs télécoms et ceux d'Internet, avec en toile de fond le combat entre des acteurs européens et des sociétés principalement américaines.

Rappelons que le règlement sur les données personnelles, voté en avril par le Parlement européen, doit lui aussi obliger les services à divulguer aux autorités les fuites de données, dans un délai court. En France, cette obligation ne concerne que les opérateurs.

Le moment est d'ailleurs pour celle-ci, le secteur télécom étant notamment le théâtre de lobbyings intenses. Elle a d'ailleursretiré une proposition de « fair use » pour la fin des frais d'itinérance il y a quelques jours, suite à des levées de bouclier du côté des associations de consommateurs, des opérateurs et des eurodéputés. Comme le rappelle Reuters, ce texte passera entre les mains du Parlement et du Conseil de l'Europe, avec des changements possibles à la clé…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : L’UE préparerait l’extension de règles de sécurité des opérateurs aux acteurs du Net