# Un technique d'attaque informatique très répandue : Le « Watering Hole » | Denis JACOPINI



Les motivations des attaquants sont diverses. Les plus répandues sont le gain financier, la gloire personnelle, la malveillance ou encore l'espionnage. Quelle que soit la finalité de l'attaque, cette dernière passe le plus souvent par la compromission d'un système. Pour parvenir à leur fin, les attaquants disposent d'un large arsenal comprenant le contournement des mécanismes de sécurité, l'accès physique à la machine ou encore l'exploitation de vulnérabilités. Au sein de cet arsenal, l'exploitation de vulnérabilités constitue sans aucun doute le principal vecteur d'intrusion. Les méthodes d'infection employées peuvent alors prendre différentes formes : Infection par média amovible (CD, USB, cartes SD, ...)

- Infection par e-mail (pièce jointe ou un lien malicieux notamment)
- Infection via le réseau interne (fichiers partagés)
- Infection par visite d'un site Web

Le « Watering Hole » fait partie de la dernière catégorie : «Infection par site Web », autrement appelé «Drive-By Download». Cette dernière repose sur le principe suivant :

- 1. Création ou compromission d'un site Web par l'attaquant (accès à l'interface d'administration, compromission des régies publicitaires pour injecter du code au sein des publicités affichées, découverte d'une vulnérabilité de type XSS...)
- 2. Dépôt du malware sur le site (Ex : code JavaScript offusqué s'exécutant au chargement de la page, iframe contenant un ActiveX ou un applet Java malicieux hébergé sur un autre site, ...)
- 3. Compromission de la machine cliente. La victime est incitée à se rendre ou redirigée de manière automatique sur le site Web hébergeant le malware. Son navigateur exécute le code malicieux et un malware est installé à son insu sur son poste de travail ou son Smartphone, très souvent de manière transparente. L'attaquant dispose alors d'un accès partiel ou complet sur l'appareil infecté.

### Simple attaque de type « Drive-by Download » ?

La subtilité de cette attaque réside dans le choix des sites Web initialement compromis (cf étape 1). En effet, en fonction de la cible, le choix est principalement réalisé en fonction de la localité de l'entité ciblée ou en lien avec son métier.

Plusieurs cas concrets récents peuvent être cités en exemple :

- Professionnel : (politique/religieux/syndical…) Dans le cas d'Apple, de Microsoft ou de Facebook en février dernier, le site Web compromis était un site Web consacré au développement sur iPhone (iphoneDevSDK), site susceptible d'être visité par les développeurs des trois sociétés. La population cible peut également être plus restreinte comme l'illustre la compromission du site « http://www.rferl.org (Radio Free Europe Radio Liberty) ».
- Géographique : En Septembre 2012 lors de l'attaque VOHO[1], les cybercriminels avaient compromis un site gouvernemental local au Maryland, celui d'une banque régionale dans le Massachusetts afin de compromettre les machines de populations spécifiques résidant ou travaillant dans les localités ciblées.
- Et pourquoi pas Personnel : Il est tout à fait possible de voir le site du club de sport ou de musique où les enfants de la victime sont inscrits, être compromis...

### Pourquoi utiliser cette méthode plutôt qu'une autre ?

En comparaison de l'envoi de phishing par exemple, cette méthode présente de nombreux avantages pour les attaquants :watering hole — scalable

### Scalable :

Elle permet de couvrir un grand nombre de victimes « facilement ». Le «Drive-By Download» est largement utilisé dans le domaine de la #cybercriminalité permettant de compromettre un très grand nombre de machine rapidement ;

L'exploitation de vulnérabilités Java ou Adobe Flash récentes, peuvent permette de contourner les mécanismes de cloisonnement au sein des navigateurs Web et ainsi de couvrir de nombreux systèmes d'exploitation et navigateurs Web vulnérables différents

### Efficace

Couplée avec l'exploitation d'une vulnérabilité de type « 0-day », le taux d'infection peut être très élevé. Le rapport sur la campagne « VOHO »[2] publié par RSA et portant sur des attaques par « Watering Hole » recensait 32 160 machines infectées appartenant à 731 organisations pour un taux d'infection de 12%.

### Discret :

Aucune action de l'utilisateur n'est nécessaire si ce n'est d'aller visiter ses sites Web habituels. L'absence de signaux rend également l'identification de la source de l'infection difficile. Enfin, la possibilité de filtrer les postes infectés (classe IP, langue du navigateur, localité …) permet de restreindre les dommages collatéraux et donc de limiter la visibilité de l'attaque.

Cette méthode présente cependant un certain nombre d'inconvénients :

- · Potentiellement, une phase de reconnaissance, consistant à identifier sur quels sites se rendent les futures victimes
- Une phase de compromission de sites légitimes est nécessaire : les attaquants peuvent cependant identifier les sites vulnérables via des scans automatisés.
- Les attaquants doivent réaliser une analyse post-infection afin de déterminer, pour chaque poste compromis, quel type de profil a été infecté et si le profil correspond à la cible (société, fonction, ...)



A noter que le filtrage effectué afin de réduire le périmètre des postes compromis émergent également au sein des attaques par phishing.

### Quels sont les mécanismes de défense ?

Face à ce type de menace, il n'existe pas de solution « miracle ». Il convient donc d'appliquer des bonnes pratiques afin de limiter les risques d'infection et d'être réactif en cas de compromission :

- 1. [Mise à jour du parc] On constate que les vulnérabilités exploitées sont le plus souvent liées aux technologies Java ou à Adobe Flash. A minima, il convient de maintenir à jour le parc applicatif. Cependant, cette mesure peut ne pas être suffisante (cas des 0-day). Nous recommandons donc de les désinstaller lorsqu'ils ne sont pas nécessaires.
- 2. [Filtrage Web] Mettre à jour régulièrement en ajoutant automatiquement et au besoin manuellement les sites connus comme hébergeant des malwares au sien des listes noire des équipements de filtrage Web (nécessite de disposer d'un service de veille). De manière plus radicale, il est envisageable d'imposer la navigation Web pour des populations sensibles depuis des postes séparés du reste du réseau de l'entreprise.
- 3. [Durcissement des postes] Des mécanismes de contournement peuvent également être mis en place. Pour Java par exemple, il est possible de configurer le niveau de sécurité sur « high » de manière à n'exécuter les applets non signés qu'après validation manuelle de l'utilisateur. Des mesures similaires peuvent être appliquées sur le plug-in Flash. Il est aussi possible de pousser des plugins comme « NoScript » afin d'interdire l'exécution de code JavaScript, Flash, Java …

### Conclusio

La compromission par « Watering Hole » partage les mêmes objectifs que par « spear-phishing » et la même méthode d'infection que les attaques par « Driveby download ».

Cette combinaison est ainsi surtout utilisée pour des attaques cherchant à s'introduire au sein d'une organisation, quel que soient les postes compromis. Avec le temps et grâce aux campagnes de sensibilisations, les utilisateurs et en particulier les populations VIP sont de plus en plus précautionneuses quant à l'ouverture des pièces jointes aux courriels. Les attaques par « Spear-phishing » sont ainsi complétées par des attaques de type « Watering-Hole » qui ne nécessitent aucune action de la part de la victime si ce n'est de visiter ses sites Web habituels…

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre) Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances

similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître ! Commandez sur Fnac.fr https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : http://www.lexsi-leblog.fr/cert/watering-hole-et-cybe rcriminalite.html

### Pourquoi ne pas partager

# l'avertissement mettant en garde contre le pirate Jayden K. Smith ?



Depuis le début du mois de juillet, un hoax (canular) circule sur Facebook. Il a été traduit de l'anglais et te met en garde contre un hacker nommé Jayden K. Smith. Pas de panique, c'est une mise en garde totalement fausse. Alors ignore le message, n'accepte rien et surtout, ne le repartage pas! C'est un peu soûlant.

« S'il te plaît dis à tous tes contacts de ta liste messenger de ne pas accepter la demande d'amitié de Jayden K. Smith. C'est un hacker et a un système connecté à votre compte facebook. Si un de tes contacts l'accepte, tu seras aussi piraté, aussi assures toi que tous tes contacts le sachent. Merci. Retransmis tel que reçu. Gardes ton doigt appuyé sur le message. En bas, au milieu il sera dit transmettre. Appuyer dessus et cliquer sur les noms qui sont sur ta liste et cela leur sera envoyé. »

Voilà le message que vous avez peut-être reçu ce matin via Messenger. Il s'agit d'une nouvelle chaîne totalement infondée, comme l'ont fait remarquer certains médias outre-Atlantique. Le message est juste une traduction d'un texte en anglais qui est devenu viral un peu partout dans le monde la semaine dernière…[lire la suite]

### L'avis de notre Expert Denis JACOPINI

Même s'il nous paraît difficile de pirater un compte Facebook par une simple lecture ou une demande d'ami, nous recommandons de ne pas partager ce message et de simplement le supprimer ou l'ignorer.

Ces canulars peuvent aussi bien prendre la forme d'un faux virus, d'une chaine de solidarité (comme ici), d'un gain hypothétique, d'une pétition ou d'une fausse information destinée à influencer l'opinion publique.

Vous pouvez aisément comprendre que les intérêts ne sont pas tous dans un but de vous arnaquer ou vous soutirer de l'argent. Certains auteurs de ces chaines recherchent la fierté d'avoir leur message qui fait le tour de la planète, d'autres de saturer les réseaux avec des messages inutiles mais les plus dangereux sont ceux qui vous demandent de cliquer ou de partage.

Même si je suis certains que vous êtes vigilants lorsqu'on vous demande de télécharger ou d'exécuter un programme, vous l'êtes certainement bien moins lorsque vous partagez un message à vos amis. L'expéditeur peut du coup disposer et utiliser de manière malveillante des informations sur eux.

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre) Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances

similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître ! Commandez sur Fnac.fr https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj\_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : Ne partage pas cet avertissement qui te met en garde contre le pirate Jayden K. Smith, c'est un hoax

## Pourquoi le vol de données

# personnelles devient-il de plus en plus commun ? | Denis JACOPINI



Des pirates informatiques Russes viennent de réaliser « le casse du siècle » en récoltant 1,2 milliard de comptes utilisateurs (identifiants et mots de passe associés) et plus de 500 millions d'adresses e-mail, provenant de 4200 000 site Internet d'entreprises de toute taille. NetIQ, fournisseur de solutions de #sécurité informatique, ne s'étonne pas de la multiplication de ce type de hack. Geoff Webb, Senior Director, Solution Strategy chez NetIQ, explique pourquoi le vol de données personnelles devient de plus en plus commun :

« Dans ce type de cas, la faute ne repose pas uniquement sur les hackers. Il faut aussi prendre en compte le comportement des entreprises et celui des utilisateurs finaux face à la sécurisation des accès.

Commençons par les hackers. De nos jours, il n'est pas nécessaire d'avoir un groupe sophistiqué et étendu de pirates informatiques expérimentés pour perpétrer les plus gros cyber-crimes. Aujourd'hui une simple recherche Internet permet à quiconque de rapidement trouver toutes les informations nécessaires pour pénétrer les systèmes informatiques vulnérables. Les pirates informatiques ont même cartographié toutes les vulnérabilités de la toile, et le tout est disponible en ligne. De plus, avec l'avènement du cloud, les hackers ont une porte d'entrée supplémentaire pour accéder aux données des entreprises. On entend régulièrement parler dans nos médias de la sécurité, ou plutôt du manque de sécurité lié au cloud.

Continuons avec les entreprises. Le cloud n'est pas le cœur du problème. Le problème de fond est que les entreprises ne mettent pas assez l'accent sur la sécurité des accès, que ça soit au niveau des accès cloud, aux applications d'entreprise, ou aux applications Web. Tant que les entreprises n'auront pas assimilé le caractère critique de la protection des mots de passe, ce type de hack continuera de se multiplier.

Enfin, il faut s'intéresser au comportement des utilisateurs finaux, qui ne facilitent pas la tâche des entreprises en matière de sécurité des mots de passe. En effet, de nombreuses études l'ont révélé récemment, par souci de facilité, les mots de passe utilisés sont souvent très (trop) simples. Les utilisateurs utilisent les mêmes mots de passe pour accéder à leurs comptes bancaires, messagerie électronique qu'elle soit personnelle ou professionnelle, et compte Facebook, par exemple. Ce comportement est une aubaine pour les cybercriminels. En laissant aux utilisateurs finaux le choix de leurs mots de passe, nous confions tout simplement une étape cruciale dans le processus de sécurisation des données à ceux qui sont les moins qualifiés et surtout les moins préoccupés par la sécurité informatique. Vous comme moi, nous n'avons pas envie d'avoir à nous souvenir de mots de passe compliqués et différents pour chaque compte que nous devons utiliser au quotidien. C'est donc bien notre propre comportement en tant qu'utilisateur qui constitue le plus gros risque.

On ne peut empêcher un hacker d'agir, mais on peut le stopper aux portes de l'entreprise en ayant des solutions de sécurité globale prenant en compte toutes les potentielles portes d'entrée. C'est pourquoi il est impératif que des solutions de gestion des identités et des accès soient intégrées dans les projets de sécurité des entreprises, au même titre que peut l'être la sécurisation des réseaux, ou des terminaux. »

## Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ? Victime d'usurpation d'identité sur facebook, tweeter ? Portez

plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

### Références

: http://www.globalsecuritymag.fr/1-2-milliard-de-mots-de-pass e,20140806,46775.html

# Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?



Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel?

Un Employeur peut-il examiner les messages échangés par ses employés sur leur téléphone professionnel ?

Dès lors que le téléphone du salarié est professionnel, l'employeur a ce droit, à moins d'avoir mentionné avant le message «personnel». Dans ce cas, l'employeur n'a plus le droit. Mais souvent, on n'oublie de l'écrire… »

**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



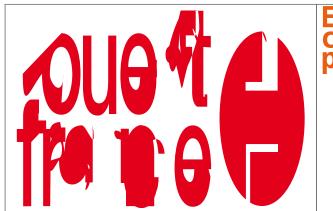
Contactez-nous

×

Réagissez à cet article

Source : Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? — La Voix du Nord

# Est-il risqué de se connecter au wifi public ? | Denis JACOPINI



Est-il risqué de se connecter au wifi public ? Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants... Mais y a-t-il un risque à partager ces accès sans fil à internet avec

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français). Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en

sécurité informatique, nous explique pourquoi.

ADUS (4)

Die 69

Benis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

### À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ?

Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

### Ouel est le danger ? Se faire espionner ?

rout à fait À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.



OLO (Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : FlickR/Richard Summers)

La confidentialité de la navigation n'est donc pas garantie ?
En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » — par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. — ont désormais des adresses commençant par « https » au lieu de « http ». Le souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

### Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?

Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel… sur lequel étaient aussi connectés des pirates!

### QUe 4

Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

### Peut-on se faire abuser par une fausse borne wifi ?

Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé… Aujourd'hui, c'est très facile de devenir pirate !

### Comment se protéger ?

En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais c'est beaucoup plus sûr.

Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

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

Cet article vous plait ? Partagez !

Source : http://www.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/7 Par Corinne Bourbeillon



## Place de ciné pas chère : une

# faille pour Gaumont Pathé ? | Denis JACOPINI



Place de ciné pas chère ? Bluff, escroquerie ou piratage informatique ? Une boutique du black market francophone propose de payer ses places de cinéma 5 fois moins chères que le prix initial. Une possibilité pirate qui ne viserait que les cinémas Pathé Gaumont !

Les amateurs de cinémas ne me contrediront pas, le cinéma est devenu un petit luxe loin d'être négligeable dans un budget. Même si des cartes de réductions existent, cela fait rarement la sortie cinéma (deux adultes, deux enfants) à moins de 50€ (si on rajoute quelques friandises), et à la condition ou la séance n'est pas en 3D, ce qui fait gonfler la note. Bref, tout le monde n'a pas la chance d'aller au cinéma deux fois par semaine. Bilan, ce qui est mon cas, les cartes de réduction sont un bon moyen d'assouvir son plaisir de salle obscure. D'autres internautes, beaucoup plus malhonnêtes, n'hésitent pas à revendre des entrées à un prix défiant toutes concurrences.

### Place de ciné pas chère ?



Dans une boutique du black market francophone, je suis tombé sur une publicité annonçant proposer des places de cinéma à 1,5€/2€. Des places ne pouvant être utilisées que dans les cinémas Gaumont Pathé! Le président des cinémas Pathé, Jérôme Seydoux et Nicolas Seydoux, président de Gaumont (Grand Père et Oncle respectifs de la dernière James Bond Girl, Léa Seydoux) auraient-ils décidé de faire des réductions aussi inattendues qu'impossibles ? Malheureusement pour les cinéphiles, ce n'est pas le cas.Il semble que le vendeur derrière cette proposition alléchante de Place de ciné pas chère a trouvé une méthode pour escroquer l'entreprise. « J'ai des places de cinéma gratuites et illimitées valables dans tous les Pathé de France, indique ce commerçant. Ces places ne sont pas cardées [comprenez acquises avec des données bancaires piratées, NDR], juste ma tête« . Le vendeur indique ne pas vouloir donner plus d'informations sur sa méthode. Une technique qu'il utiliserait depuis deux ans « pour moi et mes amis et qu'il n'est jamais rien arrivé« . D'après ce que j'ai pu constater, le pirate semble être capable de générer des codes « invitation ». Le pirate a même créé un shop (boutique automatisée) qui permet d'acquérir autant de place que le black marketeur est capable de générer contre la somme demandée. Paiement en bitcoins… [Lire la suite]





Contactez-nous

Réagissez à cet article

Source : ZATAZ Place de ciné pas chère : une faille pour Gaumont Pathé ? — ZATAZ

Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur?



Ne pas effacer ses données personnelles sur son ordinateur de fonction est-il dommageable (risque d'accès à nos données personnelles, vol d'identité ou accès frauduleux etc...)? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :

- Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix;
- Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox...;
- Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité. Même si l'article 226-4 du code pénal complété par la loi LOPPSI du 14 mars 2011 d'un article 226-4-1, l'usurpation d'identité numérique est un délit puni de deux ans d'emprisonnement et de 20 000 euros d'amende, il sera fastidieux d'une part pour vous, de prouver que vous n'êtes pas le véritable auteur des faits reprochés, et difficile pour les enquêteurs de retrouver le véritable auteur des faits.

Ne pas effacer ses données personnelles sur l'ordinateur que l'on rend, donne, vend, c'est laisser l'opportunité à un inconnu de fouiller dans vos papier, violer votre intimité et cambrioler votre vie.

Pire ! vous connaissez bien le donataire de votre matériel et vous savez qu'il n'y a aucun risque qu'il ait des intentions répréhensibles. Mais êtes vous certain qu'il sera aussi prudent que vous avec son matériel ?

Êtes-vous prêt à prendre des risques s'il perdait ce matériel ?

Dormiriez-vous tranquille si vous imaginiez que votre ancien ordinateur est actuellement sous l'emprise d'un pirate informatique prêt à tout pour tricher, voler et violer en utilisant votre identité ?

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.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée — ZDNet

Pourquoi, malgré le danger connu, cliquons nous sur des e-mails d'expéditeurs inconnus ?



Pourquoi, malgré le danger connu, cliquons nous sur des emails d'expéditeurs inconnus ? Contact and experimental contact of the Contact of

Original de l'article mis en page : One in two users click on links from unknown senders > FAU.EU

# Un oeil sur vous, citoyens sous surveillance — Documentaire 2015 | Denis JACOPINI



Des milliards de citoyens connectés livrent en permanence — et sans toujours s'en rendre compte — des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la #cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez ! Un avis ? Laissez-nous un commentaire ! Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?



Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé (effacer l'historique de ses comptes mails et personnelles, formatage complet, logiciel d'aide à la suppression etc.) ? La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage. Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons : • Des programmes ajoutés ; • Nos e-mails : Nos traces de navigation ; Nos fichiers téléchargés ; Divers identifiants et mots de passe ; Les fichiers temporaires Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse Concernant les programmes ajoutés
Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillentions de procéder :
\* soit par le raccourcis de désinstallation que le programme a créé ;
\* soit par le raccourcis de désinstallation que le programme a créé ;
\* s'il n'y a pas de raccourci préva à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
\* Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que Revoluinstaller (gratuit). Concernant les e-mails
Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les Concernant nos traces de navigation
En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ». Concernant les fichiers téléchargés
En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker. Concernant divers identifiants et mots de passe

Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».

Du fait que les mots de passe que vous avez mémorisé au fil de vos consultations de sites Internet sont également stockés dans vote ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs. Pour finir
Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »... 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 030401 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les armaques 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 puevent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpourt.fr/formations-cybercrisminalise protection-des-données-personnelles Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles. conternieux, détournements de cérnièle—):

Expartisas de systèmes de vote électronique ;

Formations et conférences en cybercriminalité ;

Formation de C.I.I. (Correspondants Informatique et Ubertés) ; Accompagnement à la mise en conformité CNII, de votre établissement. Le Net Expert
INFORMATIQUE
Consultant en Optionnellal et en
Fronkcio de Zoonnele Procenties

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée — ZDNet