Vol de données : cinq conseils pour se protéger contre les intrusions | Denis JACOPINI



Ransomware, chevaux de Troie et logiciels malveillants : les entreprises ne sont guère à l'abri des attaques de pirates qui représentent un grand risque pour leur sécurité. Mais contrairement aux idées préconçues, les menaces ne proviennent pas uniquement de l'extérieur. Les employés de l'entreprise peuvent ainsi mettre à profit les nombreuses possibilités qu'ils ont d'accéder aux systèmes de l'entreprise pour une utilisation frauduleuse des données, et cela sans beaucoup d'effort. Les organisations sont d'ailleurs rarement aussi bien protégées des attaques venant de l'interne que de celles extérieures.

Les cinq recommandations suivantes peuvent aider les entreprises à se protéger efficacement contre le vol de données par des employés.

1. Octroyer des droits d'accès différents
Pour protéger les données sensibles, il est nécessaire de donner aux employés travaillant dans différents départements des droits d'accès appropriés. Ainsi, le niveau de securité est determiné par le besoin de connaissances d'un projet : un employé n'a accès à certains documents et dossiers que si ceux-ci sont nécessaires pour effectuer une tâche qui tombe sous sa responsabilité. Ces divers cloisonnements mis en place au sein de l'entreprise sous la forme de « murailles de Chine » empêchent l'échange d'informations non nécessaire entre les différents départements, permettant de limiter la perte de données.

2. Utiliser une double authentification forte

Afin de limiter tout risque, l'étape supplémentaire recommandée est une authentification à deux facteurs. Pour accéder au système, l'utilisateur doit, par exemple, non seulement entrer son mot de passe, mais aussi recevoir un SMS contenant un mot de passe unique, valable pour une seule session. Ainsi, il n'est pas possible d'accéder à l'information et aux données sensibles, même si le mot de passe a été volé.

3. Durcir la protection des informations

Les fonctionnalités en terme de sécurité doivent inclure la protection des données. Le fournisseur ne devrait en aucun cas avoir accès aux fichiers et documents, par exemple. En outre, les droits des administrateurs doivent être limités aux informations pertinentes à leurs activités.

4. Mettre en œuvre une gestion des droits d'information

Les technologies de gestion des droits d'information des documents sensibles peuvent contrôler et protéger contre le téléchargement non autorisé. Celles-ci assurent un contrôle efficace des documents même si les utilisateurs sont autorisés à accéder à l'information. Le filigrane empêche, en outre, une capture d'écran des informations. Il n'y a aucun risque de perte de données dans cet environnement protégé et elles ne tombent pas entre de mauvaises mains.

5. Enregistrer toute modification

Pour éviter le vol de données par un employé de l'entreprise et de s'en rendre compte après coup, il est conseillé d'enregistrer tous les changements effectués afin que ceux-ci soient répertoriés dans un historique. Cela permet un flux d'informations toujours clair et transparent.

Sofia Rufin, Vice Présidente Régionale de Brainloop, commente la menace croissante que représentent les employés de l'entreprise dans le cadre de vols de données : « Nous avons observé au cours des dernières années, une augmentation du nombre des pertes de données dues à des failles en interne, les entreprises faisant encore trop souvent confiance à des standards de sécurité déficients. L'impact peut pourtant s'avérer désastreux sur l'image de l'entreprise, et les conséquences financières et légales peuvent menacer son développement économique… [Lire la suite]

[block id="24761" title="Pied de page HAUT"]

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"]

Source : Vol de données : cinq conseils pour se protéger contre les intrusions — Global Security Mag Online

5 bons conseils pour sécuriser tous vos achats sur Internet



Cadeaux de Noël, billets de trains, les achats en ligne n'ont plus de secret pour vous ? Restez vigilants ! Voici 5 conseils pour réduire significativement le risque de vous faire pirater à votre insu.

Ne jamais acheter en ligne depuis un Wi-Fi public



Il est fortement déconseillé de se connecter sur son site bancaire ou sur un site de paiement connecté via un wifi public ou le wifi d'un hôtel. Parmi les risques ; un éventuel pirate peut saisir l'occasion d'un WiFi mal chiffré pour installer un logiciel malveillant sur votre terminal ou intercepter certaines de vos données.

Méfiez-vous des (sites) inconnus !

-	1000 000 (01100)	
		O V*
	PayPaul	
	Entrez vos coordonnées bancair	es
	Cryptogramme	

Attention aux faux-sites! Avant d'acheter, renseignez-vous systématiquement sur la réputation du site et privilégiez les achats sur les sites reconnus (lisez les notes/avis de consommateurs, méfiez-vous des sites qui proposent un prix nettement plus bas que ses homologues ...).

... Canal de paiement non chiffré, fuyez ...



Au moment du paiement, **entrez uniquement vos coordonnées bancaires sur un formulaire qui comprend une sécurisation HTTPS** (un petit cadenas est visible dans la barre d'adresse de votre navigateur). D'une manière générale, ne communiquez jamais votre numéro de carte bancaire ainsi que le cryptogramme visuel (trigramme) par téléphone, par mail ou via un canal non-sécurisé spécialement pour cet usage.

Dans tous les cas, un commerçant en ligne ne peut vous demander la transmission d'une copie de la carte de paiement même si le cryptogramme visuel et une partie des numéros sont masqués.

Privilégiez la sécurité au gain de temps …



Il est préférable de ne pas enregistrer votre carte sur une application smartphone. La CNIL recommandela non-conservation des données relatives à la carte de paiement sur l'application ou dans le navigateur des clients dans la mesure où ces terminaux ne sont pas nécessairement conçus pour garantir une sécurité optimale des données bancaires.

Activez le double verrou !



Mettez en place une double sécurité de paiement proposée par votre banque. Elle peut se matérialiser par un code secret demandé juste après un paiement. Celui-ci peut vous être envoyé par SMS, par mail, par téléphone, le code SMS étant le plus souvent utilisé.

A savoir : le dispositif 3D Secure pour les cartes Visa et Mastercard n'est pas mis en œuvre sur tous les sites marchands.

ET QUAND C'EST TROP TARD ?

Vous avez la possibilité de contacter votre banquier pour demander le remboursement des opérations frauduleuses ou demander l'attribution d'une nouvelle carte bancaire. En cas de contestation par le titulaire de la carte dans un délai de 15 mois après la transaction, le commerçant se verra retirer par sa banque le montant qu'il avait percu.

Vous pouvez contacter le centre national d'opposition au 0825 39 39 30 (0,34 € par minute). Ce numéro permet de faire immédiatement opposition à sa carte bancaire, notamment en cas de vol ou de perte.

Depuis l'étranger, composez le +33 442 605 303. Ouvert 7 jours/7 et 24h/24.

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

Original de l'article mis en page : Ces 5 réflexes qui sécurisent votre paiement en ligne ... | CNIL

Spam et Arnaques Internet -

Denis JACOPINI vous en parle sur LCI | Denis JACOPINI



Denis JACOPINI, formateur consultant en cybercriminalité, formateur en protection des données personnelles et expert informatique assermenté nous parle des spams et des arnaques Internet en direct sur La Chaine d'Info LCI le 13 novembre 2015 dans l'émission de Valérie Expert « Choisissez votre camp ».

LES CHIFFRES OU ETAT DES LIEUX

- + de 3,2 milliards d'internautes dans le monde (4 nouveaux internautes par seconde)
- + de 2,4 milliards d'emails sont envoyés par seconde dans le monde dont près de la moitié est du spam.

Chaque jour en France :

un peu + de 2 milliards d'emails sont reçus, soit 39 mails par personne. 1 milliards sont du spam (e-mails non désirés)

LES MAILS FRAUDULEUX

— 3,4% (1,3 par personne) sont des e-mails avec des pièces jointes malveillantes (que j'appelle « méchangiciels » ce sont des virus, vers, trojan… dont le but du pirate est de s'introduire dans votre ordinateur) — 10% (4 mails par personne) de ces e-mails sont des e-mails de phishing avec POUR SEUL BUT, récupérer vos identifiants pour usurper votre identité, accéder à vos e-mails, vos comptes bancaires ou de réseaux sociaux…

UNE FORME PARTICULIERE : Le spear Phishing (le phishing ciblé)

Au lieu d'envoyer le même mail d'arnaque à tout le monde, c'est un e-mail ciblé car il est le résultat de recherches sur vous ou directement à la suite d'un contact direct sur les réseaux sociaux, forums, blogs...).

Sur une campagne de mails frauduleux

- 11% ouvriront des pièces jointes malveillantes
- 23% ouvriront des e-mails de fishing
- Les premiers mails seront ouverts dans les 82 secondes qui suivent l'envoi…

D'après le Ministère de l'intérieur, + de 2 millions d'internautes français se sont déclarées victimes de phishing en 2015

LES EMAILS PEUVENT RENFERMER :

Des pièces jointes infectées ou des scripts piégés (Virus, RANÇONGICIELS, ESPIONGICIELS). Denis JACOPINI appelle ça des « **MÉCHANGICIELS**» .

Des mails d'arnaques ou d'escroquerie (SCAM)

Des mails de phishing

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.

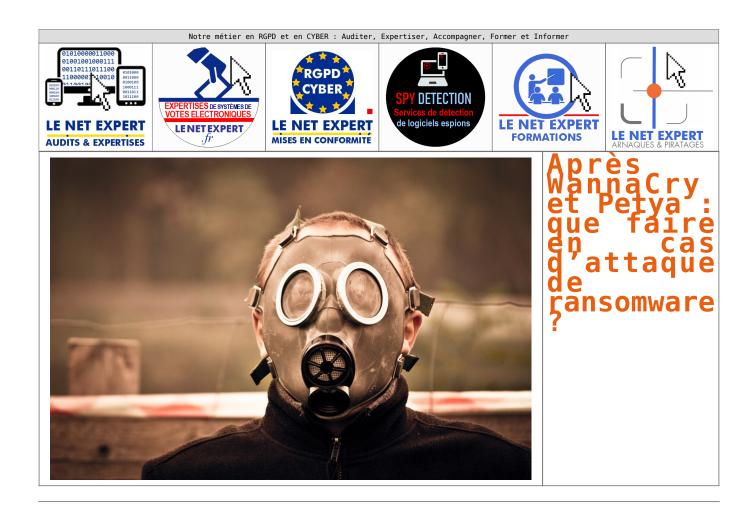
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : Denis JACOPINI

Après WannaCry et Petya : que

faire en cas d'attaque de ransomware ?



Bruxelles, le 17 juillet 2017 — C'est le plus grand cauchemar des équipes de sécurité : une attaque de ransomware comme WannaCry ou Petya. Balabit, fournisseur leader de solutions de gestion des accès privilégiés (PAM) et des logs, a reçu pendant ces attaques des informations en temps réel de ses clients et d'autres professionnels de la sécurité. L'organisation a aidé d'autres entreprises à minimiser leurs risques, tandis que sa propre équipe de sécurité a analysé les risques encourus en interne. Grâce à cette expérience, Balabit a reconstitué le déroulement des attaques afin d'en tirer des leçons. Que doivent donc faire les organisations pour contrer les programmes malveillants ? Elles doivent prendre les cinq mesures suivantes. Publié dans informaticien.be par zion

Isolez

Débranchez aussi vite que possible les appareils tels que les téléphones et les ordinateurs portables. Si vous êtes contaminé par un programme malveillant, retirez aussitôt le câble d'alimentation.

2. Collectez des informations

Qu'est-ce que c'est ? Quel est son mode opératoire ? Comment s'en prémunir ? Des équipes de désastre informatique nationales sont-elles disponibles ? Utilisez les plates-formes les plus pratiques pour diffuser ces informations : Twitter et les blogs de sécurité. Et bien sûr aussi la communication informelle entre entreprises.

3. Segmentez le réseau

Isolez le protocole infecté dans le trafic réseau. C'est une décision difficile : allez-vous contrer la diffusion du programme malveillant ou bien maintenir vos processus métier ?

4. Déployez des contre-mesures

Utilisez des Indicateur de compromission (IOC) et mettez à jour votre Système de détection des intrusions (IDS) et les paramètres du firewall, des systèmes AV et d'autant de serveurs et clients Windows que possible. Dans l'intervalle, les fournisseurs d'anti-virus travaillent évidemment sur une réponse adaptée à l'attaque.

5. Croisez les doigts et espérez

Anticipez l'avenir. Qu'est-ce qui se prépare ? Peut-être une nouvelle variante ? Tous les systèmes ont-ils eu leur patch ? L'organisation doit-elle craindre de figurer dans les journaux demain ? Une chose a-t-elle été perdue de vue dans l'urgence ? Étudiez tous les scénarios et essayez ainsi d'éviter un nouveau problème.

[block id="24761" title="Pied de page HAUT"]

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"]

Source : Après WannaCry et Petya : que faire en cas d'attaque de ransomware ? — Press Releases — Informaticien.be

Denis JACOPINI sur C8 explique comment se protéger des arnaques Internet à l'occasion de la sortie de son livre « CYBERARNAQUES S'informer pour mieux se protéger » dans l'émission « C'est que de la télé! » avec Valérie BENAÏM



DENIS JACOPINI - MARIE NOCENTI

GYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

PLON

Denis
JACOPINI sur
C8 explique
comment se
protéger des
arnaques
Internet
toccasion de
son livre «
CYBERARNAOUES
informer
pour mieux se
protéger de
son livre «
CYBERARNAOUES
informer
pour mieux se
protéger de
arnaques
L'émission «
cest que de
avec yalérie

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 2010 (Symantec)
13,8 Milions de victimes de la Cybercriminalité en 2017 (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 invitésVous remarquerez que Julien COURBET, l'animateur de cette émission, exceptionnellement absent était remplacé par Valérie BENAÏM.https://youtu.be/lDw3kI7ra2s

Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire… Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent.

« Puisse cet ouvrage avoir de nombreux lecteurs ! Il ne devrait pas plaire aux arnaqueurs, car il est un réquisitoire contre leur perfidie et, sans aucun doute, une entrave à leur chiffre d'affaire. » Général d'armée (2S) Watin- Augouard

DENIS JACOPINI - MARIE NOCENTI

CYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

PLON

Plutôt qu'un inventaire. Denis Jacopini, avec la collaboration de Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviterez les conséquences parfois dramatiques... et coûteuses. Un livre indispensable pour « surfer » en toute tranquillité ! Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier. Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques. Commandez CYBERARNAQUES sur le site de la FNAC

[block id="24761" title="Pied de page HAUT"]

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 : Cyberarnaques S'informer pour mieux se protéger — broché — Denis Jacopini, MARIE NOCENTI — Achat Livre — Achat & prix | fnac

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

Denis JACOPINI et Julien

COURBET vont parler du livre « CYBERARNAQUES S'informer pour mieux se protéger » ce jeudi sur C8 dans l'émission « C'est que de la télé! »



DENIS JACOPINI - MARIE NOCENTI

GYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

PLON

Denis JACOPINI et JULIEN vont COURBET vont parler du CYBERARNAQUES Informer Pour mieux se protéger » ce leudi sur C8 Jeudi sur C8 Jeudi sur C8 L'émission « C'est que de La télé! » Internet et les réseaux sociaux ont envahi notre quotidien, pour le meilleur mais aussi pour le pire… Qui n'a jamais reçu de propositions commerciales pour de célèbres marques de luxe à prix cassés, un email d'appel au secours d'un ami en vacances à l'autre bout du monde ayant besoin d'argent ou un mot des impôts informant qu'une somme substantielle reste à rembourser contre la communication de coordonnées bancaires ? La Toile est devenue en quelques années le champ d'action privilégié d'escrocs en tout genre à l'affût de notre manque de vigilance. Leur force ? Notre ignorance des dangers du Net et notre « naïveté » face aux offres trop alléchantes qui nous assaillent.

« Puisse cet ouvrage avoir de nombreux lecteurs ! Il ne devrait pas plaire aux arnaqueurs, car il est un réquisitoire contre leur perfidie et, sans aucun doute, une entrave à leur chiffre d'affaire. »

Général d'armée (2S) Watin- Augouard

Denis JACOPIN et Julien COURBET en parlent en parle ce jeudi sur C8 dans l'émission « C'est que

DENIS JACOPINI - MARIE NOCENTI

CYBER ARNAQUES S'INFORMER POUR MIEUX SE PROTÉGER

PLON

de la télé! ». https://www.mycanal.fr/chaines/c8

Marie Nocenti, a choisi de vous faire partager le quotidien de victimes d'Internet en se fondant sur des faits vécus, présentés sous forme de saynètes qui vous feront vivre ces arnaques en temps réel. Il donne ensuite de précieux conseils permettant de s'en prémunir. Si vous êtes confronté un jour à des circonstances similaires, vous aurez le réflexe de vous en protéger et en éviterez les conséquences parfois dramatiques… et coûteuses. Un livre indispensable pour « surfer » en toute tranquillité! Denis Jacopini est expert judiciaire en informatique, diplômé en cybercriminalité et en droit, sécurité de l'information et informatique légale à l'université de droit et science politique de Montpellier. Témoin depuis plus de vingt ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus soigneusement élaborées, il apprend aux professionnels à se protéger des pirates informatiques. Marie Nocenti est romancière.

Plutôt qu'un inventaire, Denis Jacopini, avec la collaboration de

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 : Cyberarnaques S'informer pour mieux se protéger — broché — Denis Jacopini, MARIE NOCENTI — Achat Livre — Achat & prix | fnac

TCP Stealth : Un nouveau logiciel pour se protéger des cybercriminels | Denis JACOPINI



Les balayeurs de ports sont des programmes qui parcourent le web en recherchant les ports ouverts, donc vulnérables, sur un serveur de réseau. Dans le cadre des récentes révélations de cyber-espionnage massif, un tel logiciel aurait été utilisé. Une équipe de l'Université technique de Munich (TUM, Bavière) a développé un logiciel de défense contre ce type d'attaques.

Baptisé « TCP Stealth », ce programme peut empêcher la détection des systèmes sur le net lors d'attaques par balayage de ports, ainsi que la prise de contrôle massive de ces systèmes. Ce logiciel, gratuit, nécessite tout de même certaines connaissances en informatique et systèmes pour être utilisé. Un usage plus large nécessitera encore une phase de développement. Cet outil peut venir en complément des pare-feux, antivirus et réseaux privés virtuels qui ne protègent que partiellement face à de telles attaques.

La connexion d'un utilisateur à un serveur se fait à travers un protocole de transport fiable (TCP). Afin d'accéder au service souhaité par l'utilisateur, sa machine envoie une demande au serveur. La réponse du serveur contient parfois des données susceptibles d'être utilisées pour mener des attaques. Le logiciel développé se fonde sur le principe suivant : un nombre est partagé uniquement entre la machine d'un utilisateur et le serveur. Sur la base de ce numéro, un code secret est généré puis transmis de manière invisible au serveur lors de la mise en connexion. Si le code reçu par le serveur n'est pas correct, le système ne répond pas et ne transmet donc pas d'informations au possible pirate. De tels moyens de défense sont déjà connus, mais le logiciel développé est présenté par les chercheurs comme un outil de protection plus fiable, car il gère également une variante de cette attaque. Il est ici question d'attaques générées lors de l'échange de données entre l'utilisateur et le serveur, mais cette fois-ci dans le cas où la connexion est déjà établie. Les données envoyées par l'utilisateur au serveur peuvent être, à ce stade, encore interceptées et modifiées. Afin d'empêcher cette attaque et suivant le même principe que précédemment, un code secret intégré au flux de données est également envoyé au serveur. Le serveur reconnaîtra alors si le contenu est conforme à l'original.

Le logiciel est disponible au téléchargement à l'adresse suivante : https://gnunet.org/knock.

Les personnes intéressées peuvent également participer à son développement.

Christian Grothoff, chercheur à la TUM, faculté d'architecture des réseaux et services

email : knock@gnunet.org

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"]

Sources : « TUM-Forscher entwickeln Abwehrsystem gegen Cyberangriffe », dépêche idw, communiqué de presse de la TUM — 15/08/2014- http://idw-online.de/pages/en/news599759 Rédacteurs :

Aurélien Filiali, aurelien.filiali@diplomatie.gouv.fr — http://www.science-allemagne.fr

Références

: http://www.bulletins-electroniques.com/actualites/76579.htm

Wifi gratuit: Attention à vos données personnelles!





Wifi gratuit: Attention à vos données personnelles

Les utilisateurs de réseaux de wifi du monde entier ne sont pas à l'abri du danger. D'après une enquête réalisée par Norton by Symantec, la grande majorité des internautes de l'Hexagone adoptent des comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les Français parmi les mauvais élèves

Un sondage a été réalisé par Norton by Symantec sur un échantillon de 1 000 personnes environ dans chacun des 15 pays supervisés, dont la France et les Etats-Unis. L'enquête a tenté de mettre en avant les dangers d'une connexion à des réseaux de wifi gratuit. Il a été révélé que les internautes prennent de très gros risques pour leur sécurité et leur confidentialité par le biais du troc connexion-information. Ce dernier se manifeste sous plusieurs formes : adresse email à fournir, coordonnées, géolocalisation à accepter ou encore publicité à voir. Selon l'étude, la quasi-totalité des internautes de l'Hexagone (87%) ne cesse de multiplier les comportements dangereux pour leur sécurité comme pour leur confidentialité.

Les comportements dangereux des mobinautes

L'étude a mis en avant le comportement des internautes du monde entier. Ainsi, 43% des sondés sont impatients de se connecter à peine installés au restaurant, au café, à l'hôtel, dans un magasin ou même chez un ami. Plus encore, l'envie est si pressante que 25% avouent avoir déjà tenté de se connecter sans la permission du propriétaire du réseau. Les 7% ont déjà tenté de pirater ou deviner le mot de passe (7%), rapporte *LCI*. Pour avoir une bonne **connexion**, 55% des personnes enquêtées accepteraient de fournir n'importe quelle information...[lire la suite]

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.linfo.re/magazine/high-tech/722259-wifi-gratuit-hal te-a-vos-donnees-personnelles »>Wifi gratuit: attention à vos données personnelles! — LINFO.re — Magazine, High-Tech