Comment se protéger du virus Dridex contenu dans les e-mails piégés | Denis JACOPINI

	Comment se protéger du virus Dridex contenu dans les e-mails piégés

Après un mois d'interruption seulement, l'un des logiciels malveillants les plus virulents de 2015 fait son retour en France : plusieurs vagues d'envois massifs de courriels contenant le virus Dridex ont été constatées ces derniers jours. Ce malware de type « cheval de Troie » s'installe sur les ordinateurs Windows par le biais de pièces jointes piégées, dans le but de voler des coordonnées bancaires.

D'où vient ce virus ?

Identifié dès juillet 2014 et repéré dans au moins 26 pays, Dridex n'a jamais vraiment disparu. Pourtant, fin août, une opération internationale coordonnée par le FBI et Europol (E3C), les agences de sécurité américaine et européenne, aboutissait à l'arrestation du Moldave Andreï Ghinkul, dit « Smilex », principal administrateur du virus. Les envois des courriels non-sollicités avaient été stoppés presque totalement le 2 septembre.

Mais le soulagement a été de courte durée : le 1er octobre, Palo Alto Networks détecte une nouvelle activité de Dridex au Royaume-Uni, puis le 14 octobre, c'est au tour de l'éditeur d'antivirus Avira d'émettre des doutes sur l'arrêt réel du botnet (réseau de serveurs et programmes destinés à propager le virus). Ce dernier paraît en effet toujours actif, selon Ayoub Faouzi, l'un des experts d'Avira.

Et effectivement, en France, le CERT-FR avertit le 23 octobre qu'une soixantaine de vagues d'envois massifs d'e-mails piégés visant la France ont eu lieu en moins de quinze jours.

Une nouvelle technique d'assemblage du code dite « just-in-time » (ou à la volée) permet aux pirates d'éviter les détections, mais aussi d'adapter plus rapidement le malware – une technique utilisée par d'autres logiciels malveillants comme GameOver Zeus.

Comment fonctionne t-il ?

Le mail reçu se présente de façon anodine : la plupart du temps, une relance de facture, incluant une pièce jointe au format. doc de Microsoft Office. À l'heure actuelle, peu d'antivirus détectent la nouvelle variante de ce logiciel (qui est signé avec un certificat officiel paraissant émaner de l'entreprise de sécurité Comodo), et la plupart ne suppriment donc pas la pièce jointe.

Si le destinataire tente d'ouvrir le document Word joint, une page vierge va s'afficher, mais le logiciel de Microsoft va tout de même demander à l'utilisateur s'il veut activer les macros (permettant d'interpréter les codes éventuellement contenus dans les documents Office). Une réponse positive active le virus et va lancer le téléchargement discret d'un premier code malicieux.

D'autres fichiers sont ensuite téléchargés afin d'installer divers programmes-espions. Il ne reste plus au pirate qu'à décider quand et quel programme utiliser et installer pour récupérer les données personnelles et bancaires puis effectuer des opérations frauduleuses.

A quoi ressemblent ces e-mails piégés ?

Les premières vagues de mails, le plus souvent intitulés « Relance Facture urgent » ou de « AR CDE + Facture Proforma », ont touché des messageries personnelles ou d'entreprises dès le mois de juin. Ecrits dans un français très correct et sans fautes d'orthographe, ces textes courts, et suffisamment sibyllins pour inquiéter ceux qui les reçoivent, ont déjà fait l'objet d'une première alerte officielle émanant du CERT-FR, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. La nouvelle vague de mails reçus ces deux dernières semaines sont du même tonneau.

Exemples :

« Objet : PIXOLUTIONS – FACTURE N°03480830-260615
Bonsoir,
Veuillez trouver en pièce jointe la facture n°03480830-260615 correspondant à la réalisation et pose du logo végétalisé à Perpignan. Vous en souhaitant bonne réception, bien cordialement, ».
« Objet : DUPLICATA FAC N°87878241
Salut,
Il parait que tu recherches la facture avec les Rimauresq Rosé et Blanc ? La voici en pièce jointe. Veux-tu que je te la remette au courrier également ? »
« Objet : Comptabilité de PACAR : facture n° 94352132 du 26/10 de 439,99 euros
Bonjour,
Pouvez-vous nous envoyer un chèque de 439,99 euros en paiement de la facture n° 94352132 dont vous trouverez la copie ci-jointe. En vous remerciant,
Bien cordialement, »

Comment s'en protéger ?

En plus d'un antivirus à jour, il est recommandé d'observer une grande vigilance à la réception de tout message contenant une pièce jointe, et ce quel que soit son format (.doc, .odt, .xls, .pdf, etc.).

Si le courriel semble émaner d'un organisme officiel (administrations, banques, boutiques en ligne, etc.), il est préférable de tenter de les contacter soit par téléphone, soit par mail pour vérifier l'objet de la correspondance et la légitimité de l'envoi.

Enfin, l'étape de sécurité optimale consiste à désactiver l'exécution automatique des macros dans les suites bureautiques de type Microsoft Office (aller dans Fichiers/Options/Centre de gestion de la confidentialité/Paramètre du Centre de gestion de la confidentialité/Paramètres des macros/Désactiver toutes les macros avec notifications).

Comment vérifier sa présence et s'en débarrasser ?

La société française de sécurité Lexsi propose un simple outil de détection permettant tout à la fois de vérifier sa présence sur un ordinateur puis de l'éradiquer complètement. Il est également possible, comme l'explique Lexsi, de nettoyer manuellement son ordinateur.

Téléchargez l'outil sur :
https://www.lexsi.com/securityhub/campagne-dridex-outils-de-detection-et-desinfection/

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemonde.fr/pixels/article/2015/10/29/e-mails-pieges-nouvelle-alerte-au-virus-dridex-en-france_4799355_4408996.html

Les petites entreprises aussi victimes de cybercriminalité | Denis JACOPINI

	Les petites entreprises aussi victimes de cybercriminalité

Vols de données clients, piratage de propriété intellectuelle… les cyberattaques sont légion, mais les petites entreprises se croient souvent peu concernées. A tort. Pour se protéger de ces actes malveillants, une bonne « hygiène numérique » simple à mettre en place s'avère nécessaire.

« Dirigeant d'une petite entreprise, vous pensez n'avoir jamais été victime d'une cyberattaque ? Soit vous ne l'avez pas détectée, soit vous n'intéressez plus personne et il faudrait penser à changer de métier ! « .
Cette boutade, destinée à faire prendre conscience aux patrons de PME des risques qu'ils encourent face aux hackers en tout genre, émane du contre-amiral Dominique Riban, directeur général adjoint de l'Anssi, l'Agence nationale de la sécurité des systèmes d'information.
Il faut dire que pour une PME, détecter ne serait-ce que les incidents de sécurité, autrement dit le fait qu'un pirate essaie de s'introduire dans le système sans y parvenir, s'avère bien compliqué. Idem pour les attaques. Certes, des comportements bizarres de l'ordinateur peuvent attirer l'attention, comme son ralentissement, des connexions qui s'effectuent toutes seules, la flèche de la souris qui se ballade… Mais les » méchants » savent surtout se faire discrets. Et il s'agit d'un sujet très – trop – technique, lorsqu'on ne possède pas un collaborateur spécialisé à plein temps pour s'en préoccuper…

Peu de PME portent plainte
Difficile d'avoir des chiffres fiables sur la réalité de la cybercriminalité subie par les PME. Pour une raison simple: peu portent plainte, lorsqu'elles en sont victimes. Pourquoi risquer la mauvaise publicité ? Retrouver l'auteur de l'infraction s'avère de toute façon souvent mission impossible, admet Jean-Louis Di Giovanni, associé PwC du département Litiges et Investigations auteur d'une enquête sur les fraudes en entreprises* : » On peut remonter sa trace, mais quand l'adresse IP provient d'un cybercafé aux alentours de la gare de l'Est, comment voulez-vous mettre la main dessus ? « . Devenir cybercriminel est en tout cas à la portée de tous. » Aujourd'hui, pour une centaine d'euros, vous disposez d'une solution pour attaquer le système d'information de votre concurrent, ou, pour trois fois moins cher, son smartphone « , indique Dominique Riban.

Une menace à plusieurs visages
Fomentée par de malveillants collaborateurs, actuels ou anciens, ou bien perpétrée par des hackers externes, la cybercriminalité s'avère multi-formes. Les attaques ciblées, qui visent à voler un savoir-faire particulier ou des données sensibles (secrets de fabrication, brevets, plans industriels, fichiers clients…), côtoient des attaques que Philippe Humeau, directeur général de NBS System, spécialisée dans l'hébergement de haute sécurité et les tests d'intrusion, nomme d' » opportunistes » : » Il suffit que l'entreprise ait un bout de son système connecté sur le net, qu'elle laisse traîner un mot de passe par défaut, et ça y est, elle est vulnérable. Il faut savoir qu'une adresse IP est scannée vingt fois par jour, explique-t-il. Une vraie industrie, que ces scanners qui recherchent des données relatives à des cartes bleues ou à des » identités « , autrement dit à des informations sur les personnes (celles que l'entreprise doit signaler détenir à la Cnil, ndlr). Aux commandes, des pirates qui effectuent de la récupération massive de données de ce type, puis les revendent au détail à d'autres pirates. » Car elles ont de la valeur. Des données bancaires se revendent dix dollars. Une « identité », entre 5 et 15 dollars. » Une filière aussi organisée que le recel de bijoux « , confirme Dominique Riban.

Des piégeurs pros
Parfois, les cybercriminels entrent carrément en contact avec l'entreprise. Leur inventivité sans faille leur permet de s'engouffrer dans toute nouvelle brèche. Dernier coup à la mode, la » fraude Sepa « . Les entreprises ont, rappelons-le, jusqu'au 31 juillet 2014 maximum, pour opérer leur migration afin d'être conforme à ces nouvelles normes de paiement européennes. Une aubaine, pour les fraudeurs.

Jean-Louis Di Giovanni détaille le processus : » Quelques jours auparavant, ils envoient un mail à la société, pour l'avertir qu'ils vont la contacter par téléphone afin de procéder à des essais. Le mail semble officiel évidemment. On y trouve le numéro du fraudeur, et, comble du raffinement, si l'on appelle, on tombera sur la petite musique d'attente officielle de la banque. Le jour J, ils téléphonent donc à l'entreprise, et demandent à leur interlocuteur de télécharger un programme… qui sert en réalité à prendre la main sur son ordinateur. Le fraudeur voit sur l'écran toutes les informations qu'aurait normalement la banque, et cela le rend ainsi crédible pour passer un ordre, du type : allez sur le compte x sur lequel vous disposez de 2,5 millions d'euros et faites un virement vers ce numéro de compte étranger. » Nombreuses ont été les entreprises à s'exécuter. 48 h plus tard – le délai maximum pour faire bloquer in extremis le virement – c'est trop tard !

80 % de risques évités avec des mesures simples
Des mesures de protection sont aujourd'hui nécessaires. Contrairement aux idées reçues, le recours à des solutions » technologiques » ne constituerait pas forcément la meilleure arme de défense contre les hackers. » Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques « , assure Philippe Trouchaud, associé PwC, spécialiste de la cybersécurité.

L'Anssi publie sur son site un mode d'emploi pour éviter les incidents. Il s'agit d'une quarantaine de » règles d'hygiène « , concernant la sécurité des messageries, du poste de travail, des imprimantes etc. Une quinzaine sont applicables par les petites entreprises. » 80 % des attaques n'auraient pas lieu si ces recommandations étaient respectées « , assure Dominique Riban. Parmi elles, des gestes simples… mais trop souvent négligés. Une évidence, par exemple, de toujours utiliser des mots de passe solides? » 70 % d'entre eux sont faibles, se désole Philippe Humeau. Cette négligence généralisée cause énormément de désastres. Sans compter que les gens utilisent les mêmes partout. »

En plus du choix de mot de passe costauds, les experts font trois recommandations essentielles :

1. Des mises à jour régulières
Se doter d'au moins deux anti-virus et les remettre à jour. » Même si un antivirus n'a jamais été la panacée « , concède le contre-amiral Riban. Même nécessité de remise à jour pour tous ses logiciels. » Si les éditeurs font évoluer leurs versions, c'est parce qu'ils ont constaté des failles de sécurité, pointe Philippe Humeau. Mieux vaut éviter de reporter sans cesse le » rebootage » de sa machine quand elle le demande. »

2. Attention au cloud
Toute nouvelle pratique engendre de nouvelles menaces. C'est le cas du cloud. « N'y stockez pas de données cruciales, exhorte Dominique Riban. Privilégiez des opérateurs français dont vous trouverez la liste sur le site de l'Anssi. Je ne dis pas qu'il n'y aura pas d'accident, mais au moins, notre structure a analysé leur façon de travailler, les a audité, leur a fait corriger leurs failles. Ce n'est pas le cas, par exemple, avec Google ou Microsoft. »

3.Haro sur le BYOD
Philippe Humeau n'hésite pas également à pointer du doigt ce qu'il appelle le » problème des jeunes générations » : » Elles débarquent dans l'entreprise avec des notions de sécurité et de vie privée assez light. Elles ont encore moins de réflexes que leurs aînées. Lorsqu'un jeune n'hésite pas à dévoiler sa cuite du week-end sur Facebook, il ne faut pas s'attendre à ce qu'il sache mettre des barrières là où il devrait les mettre. » Souvent associé à la génération Y – mais pas que – , le phénomène BYOD (» bring your own device «) tient du fléau en matière de cybersécurité. La pratique nécessite d'être encadrée.

» Il devient difficile de l'interdire, mieux vaut donc accompagner l'usage « , préconise Philippe Humeau. Mettre en place par exemple un réseau internet privé et un autre public, pour que les collaborateurs s'y connectent avec leur machine. Dominique Riban se montre, lui, beaucoup plus radical : » Même si l'appareil appartient à l'employé, seul l'employeur doit pouvoir administrer la machine, afin que l'utilisateur, ou ses enfants, ne puisse pas télécharger tout et n'importe quoi le week-end ou désactiver l'anti-virus. » Pas sûr que les collaborateurs acceptent…

Procéder ou pas à un test d'intrusion
Pour évaluer la capacité de résistance de son système informatique, on peut évidemment faire effectuer un test d'intrusion. A une petite entreprise, il en coûtera aux alentours de 7000 euros. Une facture qui peut paraître prohibitive. » Evidemment cela ne s'adresse pas à tout petit entrepreneur , se défend Philippe Humeau, dont la société propose de tels tests. Mais si l'on a des secrets de fabrication, la dépense est justifiée. Nos interventions se déroulent encore malheureusement trop souvent en post-mortem, nous faisons peu de prévention. »

* Selon cette récente étude, la cybercriminalité est la 2ème fraude la plus signalée en France. Son évolution inquiète particulièrement les dirigeants qui la classent comme la fraude la plus redoutée dans les 24 mois à venir.

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 !

Source : http://lentreprise.lexpress.fr/high-tech-innovation/cybercriminalite-les-petites-entreprises-ne-sont-pas-a-l-abri_1518760.html

Comment déjouer les arnaques aux distributeurs automatiques de billets (DAB)

	Comment déjouer les arnaques aux distributeurs automatiques de billets (DAB) ?

Déjouer les escroqueries au DAB et adopter les bons gestes pour s’en prémunir, par la brigade des fraudes aux moyens de paiement

Denis JACOPINI :
Parce que nous considérons que notre connaissance des risques et le premier rempart contre les pirates, nos avons souhaité partager avec vous cette vidéo.
N’hésitez pas à nous contacter pour l’organisation de sessions de formations ou de conférences de sensibilisation aux risques informatiques, pour apprendre à vous protéger des pirates, des arnaques et limiter ainsi votre exposition à ces pièges.
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Les TPE et les PME, cibles privilégiées des cybercriminels | Denis JACOPINI

Les TPE et les PME, cibles privilégiées des cybercriminels

Selon le spécialiste de la sécurité Symantec, 71 % des TPE et les PME qui font l'objet d'une cyber-attaque ne s'en remettent pas. Pourtant, la sécurité du système informatique ne fait pas partie des priorités des petites et moyennes entreprises, même si c'est un enjeu majeur pour leur survie.

Face à des systèmes d'information de plus en plus ouverts, un usage généralisé d'internet et des terminaux mobiles connectés, les entreprises doivent mettre en œuvre des politiques de sécurité informatique de plus en plus exigeantes. Pourquoi les cybercriminels s'en prennent d'avantage aux TPE et aux PME ? Explication.

La cybercriminalité n'est pas un fait nouveau. Pourtant depuis quelques années, nous sommes tous devenus ultra-connectés et multi-équipés. Ce constat n'épargne pas les entreprises qui ont vu apparaître de nouveaux outils qui permettent aux salariés de rester connecter en étant plus mobile et plus productif. Ces nouveaux modes de travail, sont aujourd'hui autant de failles de sécurité possibles et donc d'attaques possibles. Cette forme de criminalité ne concerne plus les grandes entreprises qui ont majoritairement mis en place des moyens coûteux pour lutter contre le piratage. La nouvelle cible privilégiée des hackers serait les TPE et les PME qui seraient plus simple à attaquer.

Des cibles plus accessibles
Les enquêtes le confirment : les gérants de TPE et PME ont une vision assez exacte du piratage informatique, mais ils se sentent peu concernés. Selon eux, cette forme moderne de criminalité menace surtout les grandes entreprises. Pourtant, les délits constatés contredisent cette perception. Plus encore, le pourcentage des attaques vers les entreprises de moins de 250 salariés progressent. Selon le rapport Symantec Security Threat, elles seraient passées de 18% à 31% en 4 ans. Or ce sont justement les entreprises de moins de 250 salariés qui doivent protéger leurs données. Le constat est le suivant : 40% de la valeur des entreprises est issue des informations qu'elles détiennent. Ce qui intéresse les cybercriminels : dossiers clients, listes de contacts, renseignements sur le personnel et informations bancaires de l'entreprise, cartes de crédit comprises et propriétés intellectuelles. Elles représentent aussi des passerelles d'accès à leurs partenaires.

Un frein pour travailler avec les grandes entreprises
Loin des considérations financières et ne se sentant pas concernées, les TPE et PME s'estiment à l'abri de ces attaques. En conséquence, leurs infrastructures ne sont pas adaptées. Elles sont alors des cibles idéales permettant d'attaquer leurs différents partenaires qui sont parfois des grandes entreprises ou des administrations. Elles deviennent alors un moyen d'accéder à leurs systèmes d'information. Et cela peut constituer un frein à la compétitivité. Les Grandes Entreprises, ne pouvant contrôler le système d'information de leurs partenaires, exigent alors de leurs sous traitants un matériel informatique similaire afin de contrôler les flux.

Des attaques virales invisibles
Les attaques les plus fréquentes sont de natures virales. A l'insu des utilisateurs, elles visent à installer de petits programmes capables d'identifier les mots de passe (via des enregistreurs de frappe), d'accéder aux services bancaires en ligne de l'entreprise (Chevaux de Troie bancaires), de contrôler à distance les ordinateurs de l'entreprise pour lancer des attaques commandées (réseaux de zombies ou botnet) ou d'espionner les employés pour connaître leurs habitudes, leurs mots de passe ou leurs préférences (Spyware)…

De nouvelles attaques plus structurées
Les techniques de piratages évoluent et le matériel n'est plus l'unique faille. On voit apparaître de nouveaux types d'attaques basées sur les failles humaines et sociales. Les environnements de travail des salariés sont ciblés à travers les postes de travail des salariés. A titre d'exemple, les hackers identifient le lien entre les entreprises et leurs partenaires. Des mails sont envoyés depuis les réseaux sociaux type Linkedin ou Viadéo au nom du partenaire. L'email sera donc ouvert sans réel méfiance de la part du salarié. Cette technique, appelée « social engineering », permet alors au pirate d'accéder au poste de travail de l'utilisateur en premier lieu pour ensuite évoluer dans le système d'information de l'entreprise.

Des règles simples de cyber-stratégie
Il n'est pas rare qu'en entreprise les salariés utilisent des outils réservés aux particuliers. Ce type de pratique multiplie les dangers d'intrusion car les systèmes peuvent être piratés. Ils pointeraient vers l'installation de « maliciels » (logiciels malveillants conçus pour infiltrer un ordinateur et y réaliser des activités non autorisées). Il en est de même pour tous les outils connectés. Malheureusement, ce n'est souvent qu'une question de temps avant qu'un hacker arrive à ses fins. Il est donc primordial de faire preuve de plus de rigueur pour gagner du temps afin de décourager l'intrusion. Une entreprise qui connait les risques et montre qu'elle a pris des mesures de sécurité simples, décourage les pirates. Il existe aujourd'hui des services de sécurité informatiques adaptés aux TPE/PME. A titre d'exemple, des prestataires proposent des offres sous forme de machine virtuelle, un proxy complet et simple. Le service permet de filtrer les pages internet en se basant sur des listes préétablies.

Mais bien avant de se consacrer à la sécurisation du matériel de travail, la première mesure à prendre concernera celle des bonnes pratiques des salariés. Des mesures de protection humaines sont nécessaires. « Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques », assure Philippe Trouchaud, associé PricewaterhouseCoopers, spécialiste de la cyber sécurité. Le gouvernement met à disposition un Guide d'Hygiène et de Sécurité de l'ANSSI, il fournit les bases de la sécurité pour les utilisateurs au sein des entreprises.

Aussi une politique de sécurité consistera tout d'abord à mener de front trois actions :
• Identifier les points de vulnérabilité généralement utilisés par les criminels informatiques pour s'introduire dans les systèmes d'information,
• Définir les règles de prudence à appliquer au quotidien par l'entreprise et son personnel,
• Mettre en œuvre systèmes de protection électroniques adéquats. Le tout devant être organisé et planifié dans la durée.

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 !

Source : http://www.axione-limousin.fr/actualites/tpe-et-pme—cibles-privilegiees-des-cybercriminels—57.xhtml

Comment vérifier si votre site Internet a été victime d’un Hackeur | Denis JACOPINI

	Que ça soit à cause d’une simple erreur de frappe ou du fait que votre site Internet a été Hacké, l’auteur, l’éditeur ou le rédacteur en chef d’un site Internet peut être pénalement responsable des conséquences causées par son contenu non désiré.

Afin de vérifier si votre site Internet a été Hacké, voici quelques conseils pour vérifier si votre site Internet a été victime d’un Hackeur :

Que votre site Internet ait été victime d’un hackeur ou que votre site Internet ait été victime d’un pirate sont deux choses différentes.

Le pirate va pomper une partir ou la totalité du contenu de votre site Internet. Le hackeur va modifier le contenu de votre site Internet dans un but de malveillance.

Les conseils que je vais vous donner concernent le cas où un site Internet a été Hacké.

DU CONTENU ETRANGE APPARAIT ?

En premier lieu, consultez votre site Internet sur plusieurs ordinateurs ayant des systèmes d'exploitation et des navigateurs différents afin de vérifier si un affichage anormal apparaît.

UN ANTIVIRUS DECLENCHE UNE ALERTE A L'OUVERTURE DE VOTRE SITE INTERNET ?

Un message d'alerte de votre antivirus est aussi un bon indicateur de la présence éventuelle d'un code suspicieux sur votre site Internet.

Première solution : Depuis votre dernière sauvegarde vous n'avez plus fait de modifications :

Restaurez les pages Web ou la base de donnée contaminée.

Seconde solution : Vous n'avez pas de Sauvegarde de votre site Internet ou la sauvegarde est trop vieille :

Dans ce cas, vous allez devoir résoudre le problème à la main.

COMMENT TESTER VOTRE SITE INTERNET

Enfin, si vous ne savez pas si votre site Internet a été hacké, vous pouvez le vérifier en utilisant les outils suivants :

https://www.virustotal.com/url

VirusTotal est un service gratuit qui *analyse les fichiers et URL suspects*, et facilite la détection rapide des virus, vers,

trojans et tous types de malwares.

http://www.urlvoid.com
URLVoid.com is a free service developed by NoVirusThanks Company Srl that allows users to scan a website address with multiple website reputation engines and domain blacklists to facilitate the detection of possible dangerous websites, used to distribute malware and spyware or related to fraudulent activities.

http://urlquery.net
Query.net is a service for detecting and analyzing web-based malware. It provides detailed information about the activities a browser does while visiting a site and presents the information for further analysis.

http://wepawet.iseclab.org/
Dans ce cas, vous allez devoir résoudre le problème à la main.

COMMENT SE PROTEGER D'UN HACKEUR ?

Voici quelques astuces simples vous aideront a protéger votre site efficacement contre les pirates et hackers de l'internet :

Ces techniques sont efficace contre les hackers débutants.

- Avoir un hébergeur de qualité et lui même utilisant des surveillances automatiques et permanentes.
- Mettez à jour systématiquement le système d'exploitation de votre serveur ainsi que toutes les applications liées à l'hébergement des sites internet, du FTP, des messageries et des bases de données.
- Supprimer l'utilisateur « admin » des logiciels et créez le votre
- Mot de passe sécurisé (minuscules, majuscules, chiffres et symboles)

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)

Quelques conseils pour surfer un peu plus tranquille sur Internet

	Quelques conseils pour surfer un peu plus tranquille sur Internet

---

Quelques conseils de bon sens pour se protéger au mieux des attaques liées à l'utilisation d'Internet.

Des mises à jour régulières et automatiques

L'un des meilleurs moyens de se prémunir des risques de piratage, est de **maintenir son matériel informatique et ses logiciels à jour** avec les derniers correctifs de sécurité et les dernières mises à jour.

Par ce biais, le risque d'intrusion est minimisé. Il est donc très important de **configurer son ordinateur** pour que le système d'exploitation se mette **régulièrement et automatiquement à jour.**

Une bonne configuration matérielle et des logiciels adaptés

Les **niveaux de sécurité** de l'ordinateur doivent être **réglés au plus haut** pour minimiser les risques d'intrusions. Les **paramètres des navigateurs** et des **logiciels de messageries** électroniques peuvent aussi être configurés avec des niveaux de sécurité élevés.

L'utilisation d'un **anti-virus à jour** et d'un **pare-feu** (*firewall*) assureront un niveau de protection minimum pour surfer sur la toile. Le*firewall* permet de filtrer les données échangées entre votre ordinateur et le réseau. Il peut être réglé de manière à bloquer ou autoriser certaines connexions.

Utiliser un bon mot de passe

Les mots de passe sont une **protection incontournable** pour sécuriser l'ordinateur et ses données ainsi que tous les accès au service sur Internet.

Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.

Lire nos conseils pour choisir un bon mot de passe .

Se méfier des courriers électroniques non-sollicités et leurs pièces jointes

A la réception d'un mail dont l'**expéditeur est inconnu**, un seul mot d'ordre : **prudence** !

Les courriers électroniques peuvent être accompagnés de **liens menant vers des sites frauduleux** (voir l'article sur le *phishing*) ou de **pièces jointes piégées**. **Un simple clic sur une image suffit pour installer à votre insu un logiciel ou code malveillant**(cheval de Troie) sur votre ordinateur. La pièce jointe piégée peut être : une page html, une image JPG, GIF, un document word, open office, un PDF ou autre.

Pour se protéger de ce type d'attaque, la règle est simple : **ne jamais ouvrir une pièce jointe dont l'expéditeur est soit inconnu, soit d'une confiance relative.**

En cas de doute, une recherche sur internet permet de trouver les arnaques répertoriées.

Que faire si j'ai déjà cliqué sur la pièce jointe?

Déconnectez-vous d'internet et **passez votre ordinateur à l'analyse anti-virus** (à jour) pour détecter l'installation éventuelle d'un logiciel malveillant.

Pour tout renseignement ou pour signaler une tentative d'escroquerie :

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

---

Réagissez à cet article

Original de l'article mis en page : Conseils de prévention sur

Comment bien se protéger contre les Cyberattaques ?

Comment bien se protéger contre les Cyberattaques ?

On l’a encore vu récemment, aucun système informatique n’est à l’abri d’une faille…
Et en matière de cybercriminalité, les exemples nous montrent que l’attaque semble toujours avoir un coup d’avance sur la défense. L’enjeu, pour les institutions et les entreprises, est d’anticiper et de se préparer à ces situations de crise en développant, en amont, une stratégie à-même de minorer au maximum leurs conséquences.

Demande de rançons, fraudes externes, défiguration de sites web, vols ou fuites d’informations, cyber-espionnage économique ou industriel…, en 2016 huit entreprises françaises sur dix ont été victimes de cybercriminels, contre six en 2015. La tendance n’est malheureusement pas à l’amélioration et l’actualité récente regorge d’exemples frappants : le logiciel malveillant WannaCry qui vient de frapper plus de 300 000 ordinateurs dans 150 pays avec les conséquences désastreuses que l’on connait, l’attaque du virus Adylkuzz qui ralentit les systèmes informatiques, le vol de la copie numérique du dernier opus de la saga « Pirates des Caraïbes » quelques jours avant sa sortie mondiale…, les exemples de cyberattaques ne cessent de défrayer la chronique.

Pour bien se protéger contre les Cyberattaque, nous vous conseillons de suivre les étapes suivantes :

1. Faire ou faire faire un état des lieux des menaces et vulnérabilités risquant de mettre en danger votre système informatique ;
2. Faire ou faire faire un état des lieux des failles aussi bien techniques qu’humaines ;
3. Mettre en place les mesures de sécurité adaptées à vos priorités et aux moyens que vous souhaitez consacrer ;
4. Assurer une surveillance des mesures de sécurité et s’assurer de leur bon fonctionnement et de leur adaptation au fil de vos évolutions aussi bien techniques que stratégiques.

• Vous souhaitez faire un point sur l’exposition de votre entreprise aux risques cyber ?
• Vous souhaitez sensibiliser votre personnel aux différentes arnaques avant qu’il ne soit trop tard ?
• Vous rechercher une structure en mesure de mettre en place une surveillance de votre réseau, de votre installation, de vos ordinateurs ?

Contactez-vous

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

Par des actions d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cyberattaque, comment faire pour limiter les risques ?*

Conseils pour bien se protéger des demandes de rançon informatiques / rançongiciels / ransomwares / cryptovirus ?

	Conseils pour bien se protéger des demandes de rançon informatiques / rançongiciels / ransomwares / cryptovirus ?

Les rançongiciels (ransomware en anglais) sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des internautes et réclament le paiement d'une rançon pour en obtenir à nouveau l'accès.
Depuis 2013, une variante est apparue avec des virus chiffrants ou crypto-virus (cryptolocker, cryptoDefense, cryptorBit et plus récemment locky, petya ou WannaCry). Cette forme de rançongiciels chiffre les documents se trouvant sur l'ordinateur cible, voire sur des serveurs qui hébergent les données. Les cybercriminels communiquent parfois la clé de déchiffrement une fois le paiement de la rançon effectué, mais ce n'est jamais une garantie. Cliquez ci-dessous pour en savoir plus:

Victime d'un rançongiciels / ransomwares / cryptovirus ou d'une demandes de rançon informatiques ? Contactez-nous

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Les rançongiciels ou ransomware – ANSSI – Plateforme Cyber Malveillance*

Alerte Virus ! Rombertik détruit le PC lorsqu'il est

détecté | Denis JACOPINI

	Alerte Virus ! Rombertik détruit le PC lorsqu'il est détecté

La menace a de quoi faire froid dans le dos. Les équipes de chercheurs de Talos (Cisco) viennent de repérer un nouveau type de malware capable de mettre à genoux un PC et les données qu'il contient. Rien de neuf, me direz-vous…

Mais Rombertik, c'est son petit nom, a été pensé pour contourner les protections mises en place, qu'elles soient système ou liées à un anti-virus. Pire, il devient particulièrement agressif lorsqu'il est chatouillé ou en phase d'être repéré.
Comme d'habitude, Rombertik se loge dans votre PC via un mail (spam ou phishing) contenant un lien piégé, souvent un faux PDF. Une fois exécuté, le malware fait le tour du propriétaire et s'assure de ne pas être enfermé dans une sandbox. Après s'être déployé, il est ensuite capable de s'insérer dans le navigateur utilisé pour collecter des données personnelles, même sur un site en https, et les expédier vers un serveur distant. Classique.
Dans le même temps, et c'est à ce moment qu'il est le plus dangereux, le malware vérifie qu'il n'est pas en cours d'analyse mémoire. Si c'est le cas, il va alors tenter de détruire le Master Boot Record (MBR), endommageant gravement le PC. Ce composant est essentiel pour démarrer une machine Windows.
S'il ne parvient pas à ses fins, il s'attaquera alors aux fichiers présents dans le dossier utilisateurs, fichiers qui seront alors cryptés avec une clé RC4 aléatoire. La machine est alors rebootée mais entre dans une boucle infinie. Bref, les dégâts sont majeurs. Et une analyse anti-virus aura les mêmes effets. la réinstallation du système est alors le seul moyen d'accéder à sa machine.
« Ce qui est intéressant avec ce malware, c'est qu'il n'a pas une fonction malveillante, mais plusieurs », souligne les experts de Talos. « Le résultat est un cauchemar », ajoutent-ils.
Comment alors se protéger ? « Etant donné que Rombertik est très sensible à la traditionnelle sandboxing réactive, il est crucial d'utiliser des systèmes de défense modernes – prédictifs. Des systèmes qui n'attendent pas qu'un utilisateur clique pour déclencher un téléchargement potentiel de Rombertik. », explique Charles Rami, responsable technique Proofpoint..
« De plus, comme le malware peut être expédié via de multiples vecteurs – comme Dyre, via des URL ou des fichiers .doc ou .zip/exe etc. – il est crucial d'utiliser des systèmes qui examinent l'ensemble chaîne destructrice, et bloquent l'accès des utilisateurs aux URL et pièces jointes envoyées par emails avant ceux-ci ne cliquent dessus. Enfin, les aspects « autodestruction » de Rombertik état susceptibles d'être déclenchés par les technologies telles que les antivirus, il est crucial que les entreprises utilisent des systèmes automatisés de réponse aux menaces – des systèmes qui peuvent localiser et bloquer l'exfiltration de données par Rombertik – sans – déclencher d'action sur le PC, et alerter les équipes de sécurité pour répondre rapidement aux dommages pouvant être causés », poursuit-il.

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 !

Source : http://www.zdnet.fr/actualites/rombertik-un-virus-qui-detruit-le-pc-lorsqu-il-est-detecte-39818978.htm

Detekt un logiciel pour supprimer des programmes espions | Denis JACOPINI

DETEKT	#Detekt, un logiciel pour supprimer des programmes espions

Voila un logiciel qui va vous aider à supprimer les RAT que vous pouvez trouver éventuellement sur vos PC.

Les RAT sont des programmes espions (Remote Administration Tool, ou Outil d'Administration Distante), ce sont des programmes qui peuvent effectuer une prise de contrôle à distance de votre ordinateur, sans que vous sachiez même que ce programme est sur votre machine.

Le logiciel proposé est le logiciel Detekt, il est également disponible avec son code source et vous aidera grandement à scanner votre PC et à éradiquer les RAT facilement de votre machine.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

Réagissez à cet article