Découvrez comment supprimer le ransomware WannaCry, sans payer la rançon

	Découvrez comment supprimer le ransomware WannaCry, sans payer la rançon

La ransomware WannaCry est toujours d'actualité, bien que Microsoft ait déployé les correctifs il y a quelques jours maintenant. Certains utilisateurs ne les ont pas encore appliqués et d'autres ont été infectés avant la diffusion. Bonne nouvelle cependant, il est possible de retirer WannaCry et donc d'avoir de nouveau accès aux fichiers de son ordinateur sans payer la rançon demandée (300 dollars).

Avant de commencer, il est bon de préciser qu'il est nécessaire de ne pas avoir redémarré ou éteint son ordinateur depuis qu'il a été infecté. Si c'est le cas, la solution tombe à l'eau malheureusement. Mais pour les autres, la solution s'appelle **Wanakiwi** et a été développée par des Français, à savoir Benjamin Delpy, Adrien Guinet et Matthieu Suiche.
Comment fonctionne Wanakiwi ? Il se charge d'analyser la mémoire du PC parce que la clé de déchiffrement s'est inscrite brièvement dans celle-ci. L'outil va alors tenter de la retrouver pour déchiffrer tous les documents qui sont verrouillés sur l'ordinateur par WannaCry. L'opération prend quelques minutes. Elle fonctionne aussi bien sur Windows XP que sur Windows 7. Cela devrait aussi fonctionner sur Windows Vista, mais un test n'a pas été réalisé.
Pour utiliser Wanakiwi, il faut télécharger la version la plus récente (wanakiwi_0.2.zip pour l'instant) sur GitHub, dézipper l'archive, lancer l'invité de commande sur Windows en mode administrateur et ouvrir le fichier wanakiwi.exe depuis l'invité de commande. Le travail va alors s'effectuer automatiquement. Il est possible de s'aider de cette vidéo si besoin.

Réagissez à cet article

Source : *Il est possible de supprimer le ransomware WannaCry, sans payer la rançon demandée | KultureGeek*

Cyberattaque mondiale par le cryptovirus Wannacrypt. Pourquoi changer une équipe qui gagne ?

	Cyberattaque mondiale. Pourquoi changer une équipe qui gagne ?

Des dizaines de milliers d'ordinateurs dans une centaine de pays ont été infectés depuis vendredi par un rançongiciel ou ransomware appelé Wannacry.
Denis JACOPINI Interviewé par RFI et propos personnels

De quoi s'agit-il ? comment ça marche ?
Depuis vendredi 12 mai 2017, une cyberattaque d'envergue mondiale a touché des dizaines de milliers d'ordinateurs. En fait, peut-être beaucoup plus d'ordinateurs on été infectés car il ne s'agit qu'un nombre estimatif…
Les ordinateur en question ont été infectés par un virus qui s'est introduit dans les systèmes informatiques au travers de la messagerie électronique et d'e-mails.
Ce type de virus, une fois introduit et activé bloque l'usage de votre ordinateur ou de votre système informatique en cryptant vos données. une fois vos données cryptées, un message vous invite à payer une somme d'argent en échange du code qui vous permettre de décrypter vos fichier et de les rendre à nouveau utilisables.
Le virus crypteur de données auquel nous avons à faire face s'appelle **WannaCry** (probablement un nom de ransomware qui est la contraction de Want a cryt).

Quelles suites peut-on donner à ce type d'attaques d'un point de vue judiciaire ?
Dans un monde idéal, il vous suffirait d'aller porter plainte à la Police ou à la Gendarmerie avec les preuves techniques à votre disposition pour qu'une enquête soit ouverte, que l'auteur du pirate soit recherché, retrouvé, arrêté, puis que son matériel saisi.
Des cas précédents ont montré que grâce à ça, des enquêteurs ont réussi à retrouver des clés de décryptage pour les mettre à disposition des victimes sur des sites internet spécialisés comme nomoreransom.org.
Malheureusement, la réalité bien différente. Il est essentiel de recueillir les preuves de cette attaque (ne serait-ce que pour votre assurance et porter plainte), mais une fois la plainte déposée il peut se passer plusieurs plusieurs mois ou plusieurs années avant de retrouver un pirate.

Dans ce grand désarrois certains décident de payer la rançon aux pirates pour récupérer l'accès à leurs données mais malheureusement peux nombreux seront qui auront satisfaction.
Dans le cas de cette cyber attaque mondiale, vu que le parquet de Paris se saisit de cette affaire, les choses devraient bouger plus vite.
Les chefs d'accusation qui peuvent être retenus contre les auteurs de cette d'attaque sont ;
• « accès et maintien frauduleux dans des systèmes de traitement automatisé de données », (deux ans d'emprisonnement et 30 000 euros d'amende et trois ans d'emprisonnement et 45 000 euros d'amende lorsque l'accès ou le maintien a entraîné une altération du système),
• « entraves au fonctionnement » d'un système de traitement automatisé de données (cinq ans d'emprisonnement et de 75 000 € d'amende);
• et « extorsions et tentatives d'extorsions ».

N'est-on pas protégé contre cette forme d'attaque ?
Depuis des dizaines d'années, pirates informatiques et forces de l'ordre jouent au chat et à la souris. La quasi totalité les victimes ayant fait les frais de telles attaques numériques se sont bien rendu compte qu'elle ne recevraient d'aide ni de la Police, ni de la Gendarmerie pour avoir réparation. Particuliers, entreprises, TPE, libéraux PME et même grandes entreprises ayant été piégées par de telles attaques informatiques devraient se poser des questions sur les compétences de leurs informaticiens.
Spécialisés pour être au service de leurs client pour gérer des parcs informatiques, ils assurent l'assistance, la maintenance, l'infogérance, mais pas la sécurité !
Assurer la sécurité informatique et plus particulièrement la sécurité de vos données est un métier à part entière et doit couvrir aussi bien des domaines techniques que pédagogiques pour amener les utilisateurs à faire évoluer leurs réflexes face aux usages du numériques.

Pourquoi changer une équipe qui gagne ?
Le premier virus qui a demandé une rançon date de 1989 et s'appelle PC Cyborg. Certes, il n'y avait pas encore l'Internet qu'on connaît aujourd'hui, mais déjà un mode opératoire habile destiné à tromper la vigilance de l'utilisateur était utilisé.
Depuis que l'internet s'est répandu, les techniques de propagation sont désormais différentes et peuvent s'adapter au support infecté (smartphone, tablette, PC, Mac et aussi objet connecté) mais la techniques pour s'introduire dans les réseau est depuis toujours la même dans la très grande majorité des cas. Même les virus, ransomwares (rançongiciels) les plus perfectionnés utilisent le bon vieil e-mail piégé ou le site Internet piégé pour s'introduire dans un réseau informatique. Les technique de camouflage, de dissimulation et de propagation vers les autres équipements du réseau peuvent par contre, elles, être extrêmement perfectionnées, mais les techniques pour pénétrer un système sont quant à elles quasiment systématiquement les mêmes.
Pourquoi faire autrement quand cette technique fonctionne encore !

Comment alors contrer de telles attaques ?

La solution n'est pas seulement technique. Certes il faut utiliser des logiciels de sécurité adaptés, mettre en place (et suivre !) des procédures de gestion de sécurité de parc rigoureuses mais ce qui nous paraît essentiel est le changement de comportement des utilisateurs.
C'est pour cela que nous proposons des formations dans le but de changer les réflexes des utilisateurs face à un e-mail, un site internet ou un appel téléphonique suspect. Nous apprenons à nos stagiaires à quoi ressemble le loup afin qu'ils évitent à l'avenir de le faire rentrer dans la bergerie.

Qui se trouve derrière ces attaques ?
Enquêteurs et experts informatiques internationaux sont lancés sur les traces des pirates informatiques à l'origine de cette cyberattaque. L'attaque est « d'un niveau sans précédent » et « exigera une enquête internationale complexe pour identifier les coupables », a indiqué l'Office européen des polices Europol, en précisant qu'une équipe dédiée au sein de son Centre européen sur la cybercriminalité avait été « spécialement montée pour aider dans cette enquête, et qu'elle jouera un rôle important ».
On évoque désormais « 200.000 victimes dans au moins 150 pays » (d'après Rob Wainwright, le directeur d'Europol) visés par les pirates informatiques et de nombreuses entreprises ou services publics reconnaissaient avoir été touchés ou avoir fait l'objet d'attaques. Mais il faudra attendre lundi et la réouverture des entreprises pour dresser un bilan plus complet de cette attaque, a-t-il prévenu.

Selon nous, si la vague de cyberattaques lancée vendredi semble marquer le pas, de nouvelles offensives sont à craindre. Une version encore plus redoutable de **WannaCry** risque bien d'arriver. En espérant que les OIV ne soient pas cette fois touchés.

Réagissez à cet article

Un nouveau ransomware basé sur l'index Big Mac

Un nouveau ransomware basé sur l'index Big Mac

Comment un cybercriminel arrive-t-il à savoir combien il doit demander? Un nouveau malware (maliciel) calcule pour lui le prix correct des données dévoilées sur base du bien connu 'Big Mac Index' de l'Economist.
Des cybercriminels ont conçu une sorte de ransomware (rançongiciel) qui adapte son prix à l'emplacement de la victime. Fatboy, comme ce ransomware s'appelle, utilise à cette fin le Big Mac Index de la revue économique The Economist. Il s'agit là d'une liste assez frivole reposant sur le prix du Big Mac de McDonald's pour savoir si un pays ou une région s'en tire bien ou non sur le plan économique. Les victimes de Fatboy dans les pays caractérisés par un standard de vie plus élevé paieront donc davantage que celles vivant dans des pays plus pauvres…[lire la suite]

Réagissez à cet article

Source : *Un nouveau ransomware basé sur l'index Big Mac – ICT actualité – Data News.be*

La nouvelle version du virus Locky vise les entreprises françaises

	La nouvelle version du virus Locky vise les entreprises françaises

La nouvelle charge de propagation du ransomware Locky s'est particulièrement concentré sur la France ces derniers jours, selon Vade Secure.

La nouvelle campagne de propagation de Locky qui se répand ces derniers jours a particulièrement frappé la France lundi 24 avril. Vade Secure annonce avoir bloqué, à lui seul, 369 000 exemplaires de l'email contenant le ransomware. *« Dont 200 000 chez nos partenaires clients et opérateurs et 169 000 sur notre Cloud »*, précise Sébastien Gest, Tech évangéliste chez l'éditeur français de sécurisation des boîtes emails. Qui ajoute avoir constaté un nouveau pic de 25 000 envois, ce mardi 25 avril, lors d'une courte attaque autour de 12h. Signalons, à titre personnel, que les équipes de NetMediaEurope, éditeur de *Silicon.fr*, ont elles-mêmes reçu un avertissement de son prestataire technique sur l'existence de cette nouvelle campagne. Une alerte relativement rare dans nos services.

Certes, le volume constaté depuis hier peut sembler insignifiant en regard des 1,4 million d'emails infectieux Locky que Vade Secure bloquait chaque jour en juillet 2016. Un taux qui s'était affaibli au fil des mois pour tomber à 600 000 fin décembre. Mais la nouvelle campagne de tentative d'infection semble se distinguer par des attaques ciblant des zones géographiques précises. *« Plus de 95% des e-mails bloqués hier se destinaient à des entreprises françaises »*, confirme l'expert qui rappelle que sa société protège quelques 400 millions de boîtes électroniques de 76 pays dans le monde dont les Etats-Unis et le Japon. En revanche, Vade Secure n'a pas constaté de profil particulier des entreprises ciblées. *« Tous les types d'entreprises sont concernés, du grand compte à la petite PME »*, assure le technicien. Rappelons que Locky est un crypto-ransomware qui, s'il est exécuté, va chiffrer tous les fichiers rencontrés sur son passage et réclamer une rançon, généralement en bitcoin, pour que la victime retrouve l'usage de ses documents…[lire la suite]

Réagissez à cet article

Source : *Le nouveau Locky vise les entreprises françaises*

Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs

	Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs

Script kiddies and online criminals around the world have reportedly started exploiting NSA hacking tools leaked last weekend to compromise hundreds of thousands of vulnerable Windows computers exposed on the Internet.

Last week, the mysterious hacking group known as Shadow Brokers leaked a set of Windows hacking tools targeting Windows XP, Windows Server 2003, Windows 7 and 8, and Windows 2012, allegedly belonged to the NSA's Equation Group.

What's Worse?

Microsoft quickly downplayed the security risks by releasing patches for all exploited vulnerabilities, but there are still risks in the wild with unsupported systems as well as with those who haven't yet installed the patches.

Multiple security researchers have performed mass Internet scans over the past few days and found tens of thousands of Windows computers worldwide infected with **DoublePulsar**, a suspected NSA spying implant, as a result of a free tool released on GitHub for anyone to use.

Security researchers from Switzerland-based security firm Binary Edge performed an Internet scan and detected more than 107,000 Windows computers infected with DoublePulsar.

A separate scan done by Errata Security CEO Rob Graham detected roughly 41,000 infected machines, while another by researchers from Below0day detected more than 30,000 infected machines, a majority of which were located in the United States.

The impact ?

DoublePulsar is a backdoor used to inject and run malicious code on already infected systems, and is installed using the **EternalBlue** exploit that targets SMB file-sharing services on Microsoft's Windows XP to Server 2008 R2.

Therefore, to compromise a machine, it must be running a vulnerable version of Windows OS with an SMB service expose to the attacker.

Both DoublePulsar and EternalBlue are suspected as Equation Group tools and are now available for any script kiddie to download and use against vulnerable computers.

Once installed, DoublePulsar used hijacked computers to sling malware, spam online users, and launch further cyber attacks on other victims. To remain stealthy, the backdoor doesn't write any files to the PCs it infects, preventing it from persisting after an infected PC is rebooted….[lire la suite]

Réagissez à cet article

Source : *Leaked NSA Hacking Tools Being Used to Hack Thousands of Vulnerable Windows PCs*

Alerte : un ransomware sur Android trompeur arrive à échapper aux antivirus

	Alerte : un ransomware sur Android trompeur arrive à échapper aux antivirus

Des chercheurs en sécurité ont trouvé un ransomware pour Android, capable d'éviter la détection par les antivirus. Il n'est dans l'absolu pas considéré comme très dangereux mais, comme certains malwares actuels, pourrait représenter une tendance.
L'histoire des malwares n'est pas nouvelle. Si l'on en croit un rapport publié en février par Eset (éditeur notamment de NOD32), le nombre d'attaques par ce vecteur a augmenté de 50 % en 2016 sur la plateforme de Google. Une conjonction de facteurs en est responsable, mais l'utilisation des boutiques tierces et les méthodes visant à tromper l'utilisateur sont clairement les plus présentes.

Des évolutions que l'on retrouve dans un nouveau ransomware découvert par la société ZScaler.
Rappelons – s'il est encore besoin de le faire – qu'il s'agit d'un logiciel malveillant dont l'objectif est de chiffrer les données de l'utilisateur puis de lui réclamer une rançon. Il peut payer et avoir une chance de les retrouver, ou refuser et faire avec les conséquences. Les sauvegardes régulières et une bonne hygiène informatique sont les deux seules armes vraiment efficaces contre ce type de menace.

Un compte à rebours de quatre heures

…[lire la suite]

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

---

Réagissez à cet article

Source : *Android : un ransomware trompeur arrive à échapper aux antivirus*

Alerte : Une publicité sur

Skype propage un rançongiciel

Alerte : Une publicité sur Skype propage un rançongiciel

Selon plusieurs utilisateurs, un logiciel malfaisant serait répandu via une publicité sur Skype par Roman De Schrijver

© Reddit

La publicité en question se présente comme une fausse page web d'Adobe. Ensuite, une fenêtre émergente surgit demandant de mettre à jour Adobe Flash Player. Si les utilisateurs se laissent tenter, c'est en réalité un maliciel qui s'installe sur leur ordinateur. Selon toute vraisemblance, ce maliciel est plutôt un rançongiciel (ransomware), à savoir un programme qui verrouille votre ordinateur et crypte vos données, de telle sorte que vous ne puissiez vous-même plus y accéder.

On ne sait pas encore à ce jour combien de victimes la fausse publicité a faites. Ce n'est du reste pas la première fois que les utilisateurs de Skype sont confrontés à ce genre d'annonce factice. Quoi qu'il en soit, il vous est toujours conseillé de rester vigilant vis-à-vis de ce que vous téléchargez et des liens sur lesquels vous cliquez.

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

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

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

---

Réagissez à cet article

Source : *Une publicité sur Skype propage un rançongiciel – ICT actualité – Data News.be*

Alerte : Faux mods de Minecraft dans le Google Play

Les chercheurs ESET® découvrent plus de 80 applications malveillantes sur Google Play® déguisées en mods[1] de Minecraft® et ayant généré pas loin d'un million de téléchargements.

Au total, les 87 faux mods ont donné lieu à 990 000 téléchargements avant d'être signalés par ESET les 16 et 21 mars 2017. Les applications répertoriées se divisent en deux catégories : le téléchargement de publicités (Android/TrojanDownloader.Agent.JL) et les fausses applications redirigeant les utilisateurs vers des sites Internet frauduleux (Android/FakeApp.FG).
Pour Android/TrojanDownloader.Agent.JL, ESET signale **14 fausses applications ayant causé 80 000 téléchargements, contre 910 000 installations pour les 73 applications malveillantes** agissant sous Android/FakeApp.FG. Comme elles ne disposent pas de fonctionnalités réelles et qu'elles affichent de nombreuses publicités agressives, les avis négatifs apparaissent clairement sur Google Play.

Si un utilisateur a téléchargé des mods de Minecraft, il se peut qu'il ait rencontré l'une des 87 applications malveillantes. **Il est facile de reconnaître ce type d'escroqueries :** l'application ne fonctionne pas et un message apparaît avoir cliqué sur le bouton de téléchargement. Pour les fausses applications qui téléchargent des publicités, il n'y a pas non plus de fonctionnalités permettant de jouer et l'appareil continue d'afficher des publicités injustifiées. **Toutefois, comme l'application malveillante est capable de télécharger des applications supplémentaires sur des périphériques infectés, la charge utile responsable des annonces peut, par la suite, être remplacée par des malwares plus dangereux.**
Bien que ce qui suit ne soit pas encore entré dans les habitudes des Français, **les chercheurs ESET [NDLR : et Denis JACOPINI] rappellent qu'il est important d'équiper son téléphone portable avec une solution de sécurité efficace** et adaptée aux mobiles. Il n'y a pas que les ordinateurs qui peuvent être infectés par un logiciel malveillant. En 2016, ces derniers ont augmenté de 20% sur Android™. Une solution de sécurité pour mobile permet, au même titre que celle dédiée aux ordinateurs, de détecter et supprimer les menaces.
Si un utilisateur souhaite supprimer les menaces manuellement, il doit désactiver les droits d'administrateur du périphérique pour l'application et le module téléchargés en allant dans Paramètres -> Sécurité -> Administrateur de périphériques. Il suffit ensuite de désinstaller les applications en allant dans Paramètres -> Gestionnaire d'applications.
Si vous souhaitez plus d'informations notamment sur le fonctionnement de ces logiciels malveillants, nous vous invitons à cliquer ici ou à nous contacter pour une demande d'interview. Nous vous proposons également de visualiser cette courte vidéo qui montre **l'installation de l'une de ces fausses applications.**

---

[1] « Jeu vidéo créé à partir d'un autre, ou modification du jeu original, sous la forme d'un greffon qui s'ajoute à l'original, le transformant parfois complètement. » Source : https://fr.wikipedia.org/wiki/Mod_(jeu_vid%C3%A9o)

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

Arnaques entre cybercriminels !

	Arnaques entre cybercriminels !

Les chercheurs de Kaspersky Lab ont découvert PetrWrap, une nouvelle famille de malware exploitant le module d'origine du ransomware Petya et distribuée via une plate-forme RaaS (Ransomware as a Service) pour mener des attaques ciblées contre des entreprises. Les créateurs de PetrWrap ont produit un module spécial qui modifie le ransomware Petya existant « à la volée », laissant les auteurs de ce dernier impuissants face à l'utilisation non autorisée de leur propre malware. Ce pourrait être le signe d'une intensification de la concurrence sur le marché souterrain du ransomware.

En mai 2016, Kaspersky Lab avait découvert le ransomware Petya, qui non seulement chiffre les données stockées sur un ordinateur mais écrase aussi le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées. Ce malware est un modèle de RaaS (Ransomware as a Service), c'est-à-dire que ses créateurs proposent leur produit malveillant « à la demande », afin de le propager via de multiples distributeurs en s'octroyant un pourcentage des profits au passage. Pour s'assurer de recevoir leur part du butin, les auteurs de Petya ont inséré certains « mécanismes de protection » dans leur malware de façon à prévenir un usage non autorisé de ses échantillons. Les auteurs du cheval de Troie PetrWrap, dont les activités ont été détectées pour la première fois au début de 2017, sont parvenus à contourner ces mécanismes et ont trouvé un moyen d'exploiter Petya sans verser de redevance à ses auteurs.

Le mode de diffusion de PetrWrap reste à éclaircir. Après infection, PetrWrap lance Petya afin de chiffrer les données de sa victime, puis exige une rançon. Ses auteurs emploient leurs propres clés de chiffrement privées et publiques en lieu et place de celles fournies avec les versions « standard » de Petya. Cela leur permet d'exploiter le ransomware sans avoir besoin de la clé privée d'origine pour décrypter la machine de la victime, dans le cas où cette dernière paie la rançon…[lire la suite]

Réagissez à cet article

Source : *PetrWrap : des cybercriminels volent le code de ransomware d'autres criminels Le nouveau ransomware mène des attaques ciblées contre des entreprises – Global Security Mag Online*

Autopsie d’un virus qui se cache dans les pixels d’une publicité

	Autopsie d’un virus qui se cache dans les pixels d’une publicité

Soyez prudents ! Les pirates informatiques sont très inventifs, et là, ils nous font, une fois de plus, la démonstration qu'ils sont de plus en plus malins. En effet, un laboratoire de sécurité a découvert un logiciel malveillant qui se cache dans les pixels composant l'image d'une publicité. Ce virus profite en fait d'une faille du navigateur Internet Explorer et de Flash Player, ce petit complément vous permettant notamment d'afficher des vidéos sur les pages que vous visitez.

Et parce qu'il s'intègre dans une photo, ce virus a été baptisé Stegano, en référence à la technique de la sténographie qui permet de dissimuler des informations secrètes dans des supports anodins. Très concrètement, vous ouvrez votre navigateur, quelques clics au cours d'une recherche et vous arrivez sur une page sur laquelle va aussi s'afficher une bannière publicitaire. Et du coup, le processus d'exécution du logiciel malveillant va se mettre en route. Il va d'abord vérifier si votre navigateur lui permet de s'installer et il va aussi récolter quelques informations au sujet de votre ordinateur.
Si ces informations sont favorables à la poursuite du processus, l'image de la publicité va être remplacée par une image similaire mais légèrement modifiée. Même en zoomant, la différence n'est pas facile à percevoir. Et c'est via cette image que l'installation va se poursuivre.
Durant cette seconde phase, le niveau de sécurité de votre ordinateur va être testé. Si la voie est libre, la dernière phase consistant à installer le logiciel malveillant va se déclencher. Ce dernier permettra, par exemple, aux pirates de collecter des données personnelles ou encore d'ouvrir une porte dérobée sur votre ordinateur pour en permettre l'accès et ceci, sans attirer votre attention.
Il est aussi possible que certains des internautes touchés voient leur ordinateur infecté par un logiciel qui va crypter les données, ce qui permet ensuite aux pirates de réclamer une rançon pour obtenir la clef permettant de les récupérer…[lire la suite]

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

---

Réagissez à cet article

Source : *Virus informatique: attention Stegano se cache dans les pixels d'une publicité*