Les recommandations de Microsoft pour se protéger de Wannacry

	Les recommandations de Microsoft pour se protéger de Wannacry

Il fait le buzz à travers les systèmes d'exploitation de Microsoft, Windows, son nom c'est Wannacry.

VOICI LES ÉTAPES POUR SE PROTÉGER DE CETTE MENACE :

En mars dernier, nous avons publié une mise à jour de sécurité (MS17-010) qui corrige la vulnérabilité exploitée par ces attaques. Tous les clients ayant Windows Update activé sur les versions de Windows supportées, sont donc protégés contre cette attaque.

1.D éployer le bulletin de sécurité MS17-010 :

Nous conseillons d'ailleurs à toutes les organisations qui n'ont pas encore appliqué cette mise à jour de sécurité, de déployer immédiatement le Bulletin de sécurité Microsoft MS17-010.

Nous savons aussi que certains de nos clients entreprises et utilisateurs grand public exploitent encore des versions de Windows qui ne sont plus supportées. Ils n'ont donc pas reçu cette mise à jour de sécurité en mars. Compte-tenu de l'impact potentiel de cette attaque et afin d'en limiter la propagation, Microsoft a pris la décision de publier pour tous nos clients, même s'ils ne disposent pas d'un Custom Support Agreement, **les mises à jour de sécurité permettant de corriger cette vulnérabilité pour** Windows XP SP3, Windows 8 et Windows Server 2003 SP2.

2. Mettre à jour votre antivirus

Windows Defender, System Center Endpoint Protection, et Forefront Endpoint Protection detectent cette famille de virus sous le nom de Ransom:Win32/WannaCrypt.

En complément, l'outil Microsoft Safety Scanner http://www.microsoft.com/security/scanner/ disponible gratuitement, a été mis à jour pour détecter aussi cette famille de virus.

En cas de menace avérée :

Si vous êtes victimes par cette attaque contacter le support Microsoft

3. Procédez à la restauration de votre machine

https://blogs.technet.microsoft.com/mmpc/2016/05/18/the-5ws-and-1h-of-ransomware/
https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

Liens utiles :

Microsoft Guidance for WannaCrypt
2. Microsoft Malware Prevention Center Technical Details about the ransomware worm
3. MS17-010 Update Catalogue

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 recommandations de Microsoft pour se protéger de Wannacry – Socialnetlink-La référence technologique en Afrique*

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*

Voici deux outils permettant de lutter contre les épidémies récentes de ransomwares dont WannaCry

	Voici deux outils permettant de lutter contre les épidémies récentes de ransomwares dont WannaCry

ESET® annonce la publication d'un outil de contrôle de la vulnérabilité EternalBlue et une clé de déchiffrement pour les variantes de Crysis. Ces deux outils, mis au point par les chercheurs ESET, permettent aux entreprises une mise à jour efficace suite aux récentes cyberattaques.

Le premier outil vérifie si Windows® est protégé contre l'exploit EternalBlue, responsable en partie de l'attaque WannaCry. Ce dernier est d'ailleurs toujours utilisé pour diffuser entre autres des logiciels de cryptomonnaie. L'exploit EternalBlue (CVE-2017-0144) détecté par ESET a été ajouté le 25 avril 2017 avant son exploitation par la menace WannaCry.
Le deuxième outil publié par ESET permet le déchiffrement et s'adresse aux victimes de l'une des variantes du ransomware Crysis, qui utilise comme extension pour les fichiers chiffrés .wallet et .onion. Les clés ont été publiées le 18 mai sur les forums de BleepingComputer.com.
Les deux outils sont disponibles en téléchargement à partir de la page Internet d'ESET :
– Vérificateur de la vulnérabilité EternalBlue : https://help.eset.com/eset_-tools/ESETEternalBlueChecker.exe
– Clé de déchiffrement du ransomware Crysis .wallet / .on : https://download.eset.com/com/-eset/tools/decryptors/crysis/latest/esetcrysisdecryptor.exe

---

Réagissez à cet article

Source : ESET

WannaCry : seulement trois antivirus protègent de

l’exploit EternalBlue

WannaCry : seulement trois antivirus protègent de l’exploit EternalBlue

Prompts à clamer qu’ils bloquent WannaCry, les éditeurs d’antivirus oublient de mentionner qu’ils ne détectent pas, à trois exceptions près, l’exploit EternalBlue. Or, c’est celui-ci qui risque d’être réutilisé par de nouvelles menaces.

Depuis la crise WannaCry, qui s’est déclenchée le 12 mai 2017 et s’est traduite par l’infection de centaines de milliers de systèmes, les éditeurs d’antivirus n’hésitent pas à clamer que leurs outils arrêtent tous la menace. Un test monté par MRG Effitas, une entreprise anglaise spécialisée dans la recherche en sécurité informatique (MRG signifiant Malware Research Group), montre que la réalité est un peu plus contrastée.

En testant la capacité des logiciels de protection grand public (avec leurs paramétrages par défaut) à détecter l’exploit EternalBlue, mis à profit par WannaCry pour se diffuser, MRG Effitas établit que seuls trois produits stoppent le code de la NSA récupéré par les auteurs du ransomware : Eset Smart Security, F-Secure Safe et Kaspersky Internet Security. « *Deux de ces produits utilisent le filtrage réseau pour détecter cet exploit et le bloquer avant son exécution au niveau du noyau* », écrit MRG Effitas, qui précise que ce mode de détection pourrait être contourné en masquant la signature de l’exploit.
..[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 : *WannaCry : seulement trois antivirus protègent de l’exploit EternalBlue*

Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?

	Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?

Pour exiger une rançon, des hackers pourraient pirater vos cafetières, télévisions, GPS connectés. Mais est-ce vraiment crédible ?

Les récentes attaques massives de « ransomwares », ces logiciels malveillants exigeant une rançon pour débloquer les ordinateurs qu'ils ont infectés, font craindre pour l'avenir des objets connectés, **des jouets aux téléviseurs en passant par le réfrigérateur ou la cafetière**, qui se multiplient dans nos foyers.
« Concernant l'attaque du week-end passé, il n'y a pas de risque pour les objets connectés. Elle touchait en particulier des systèmes avec Windows (…), et il n'y a pas d'objets connectés grand public aujourd'hui qui embarquent Windows pour fonctionner », assure Gérôme Billois, consultant chez Wavestone. « En revanche, il y a **déjà eu des attaques massives sur des objets connectés**« , rappelle-t-il.
Le malware (logiciel malveillant) Mirai a ainsi récemment infecté par centaines de milliers des objets connectés mal sécurisés, non pas pour les bloquer, mais **pour les transformer en zombies et créer des relais pour de futures cyberattaques**.

Transformer vos objets en mouchards

Mardi à La Haye, le jeune prodige Reuben Paul, 11 ans, a épaté une galerie d'experts en cybersécurité en piratant le bluetooth de leurs appareils électroniques pour prendre le contrôle d'un ours en peluche.
Les objets connectés sont donc des cibles tout à fait crédibles, qui peuvent aussi bien **siphonner des données** que se **transformer en mouchards**. Selon des documents révélés en mars par Wikileaks, les services de renseignement américains sont capables de « hacker » des smartphones, des ordinateurs et des télévisions intelligentes, notamment pour prendre **le contrôle de leurs micros et écouter ce qu'il se passe**.

« Tous les autres objets connectés sont piratables, ça a été démontré, que ce soit la cafetière, le réfrigérateur, le thermostat, la serrure électronique, le système d'éclairage… »Loïc Guézo stratégiste cybersécurité
…[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 : *Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ? – Sud Ouest.fr*

Cyberattaque mondiale : trois Français ont créé un logiciel anti WannaCry

	Cyberattaque mondiale : trois Français ont créé un logiciel anti WannaCry

Il s’appelle WannaKiwi, et peut éviter le verrouillage de fichiers, mais il faut l’utiliser de tout urgence, selon ses inventeurs français

Cocorico ! Un groupe de trois Français, experts en sécurité informatique, a annoncé ce vendredi avoir mis au point un logiciel qu’ils ont nommé WannaKiwi permettant de récupérer les documents Windows cryptés par le virus informatique WannaCry, lors d’une cyberattaque massive.

« Rançongiciel », WannaCry a infecté quelque 300 000 ordinateurs dans plus de 150 pays la semaine dernière. En France, c’est principalement le groupe automobile Renault qui a été affecté, avec le blocage de chaînes de production. Une fois implanté, ce logiciel malveillant, qui utilise une faille de Windows, paralyse le système informatique en cryptant les données. Pour récupérer ces fichiers, il faut un code que les pirates fournissent (ou pas) en échange d’une rançon.

…/…

Pour télécharger WannaKiwi : https://github.com/gentilkiwi/wanakiwi/releases
Pour voir le blog d’informations (en anglais) : https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d

---

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 : trois Français ont créé un logiciel anti WannaCry – Le Parisien*

Adylkuzz, la nouvelle menace plus performante que WannaCry

Adylkuzz, la nouvelle menace plus performante que WannaCry

Cette nouvelle cyberattaque, plus discrète que WannaCry serait en action depuis début mai 2017. Elle se servirait de la même faille dans le système informatique Windows pour s'infiltrer dans les données des ordinateurs.

Adylkuzz opère de façon plus invisible en créant une monnaie virtuelle dans l'ordinateur infecté avant d'envoyer cet argent à des adresses cryptées, volant les utilisateurs sans laisser de traces et sans qu'ils ne s'en aperçoivent.

« Bien que plus silencieuse et sans interface utilisateur, l'attaque d'Adylkuzz est plus rentable pour les cybercriminels. Elle transforme les utilisateurs infectés en participants involontaires au financement de leurs assaillants », explique Nicolas Godier, un expert en cyber sécurité de Proofpoint à l'AFP.

Le seul effet secondaire de ce virus est un ralentissement des performances de l'ordinateur infecté. Il est donc très difficile à diagnostiquer. Adylkuzz ferait aujourd'hui des centaines de milliers de victimes, et les sommes volées sont beaucoup plus importantes que celles de WannaCry.

***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 : *WannaCry: malgré un ralentissement de l'infection, la cyberattaque reste inquiétante*

WannaCrypt : une énorme épidémie de ransomwares perturbe les systèmes informatiques du monde entier

	WannaCrypt : une énorme épidémie de ransomwares perturbe les systèmes informatiques du monde entier

Une nouvelle vague de ransomwares connus sous le nom de « WannaCrypt » (détectée par ESET sous Win32 / Filecoder.WannaCryptor.D) s'est répandue dans le monde entier. Ce ransomware a infecté des dizaines de milliers d'ordinateurs. Il se propage en exploitant une vulnérabilité Microsoft® Windows dans des ordinateurs non patchés.

Touchant des centaines de milliers d'ordinateurs à travers le monde, la cyberattaque de vendredi est, de l'avis même d'Europol, « d'un niveau sans précédent ». A l'heure actuelle c'est plus de 75 000 victimes qui auraient été recensées dans le monde, parmi lesquelles le service public de santé britannique, le service de livraison FedEx, le ministère russe de l'Intérieur, des universités chinoises, l'opérateur télécom espagnol Telefonica, la compagnie ferroviaire allemande Deutsche Bahn ou encore Renault en France.

ESET® détecte et bloque la menace WannaCryptor.D et ses variantes. Le module de protection du réseau ESET bloque l'exploit au niveau du réseau. **ESET a alerté ses utilisateurs sur son site Internet. Toutes les instructions, étape par étape, sont renseignées pour qu'ils s'assurent d'être correctement protégés contre cette menace.**

Pour ESET, la sécurité du client a toujours été sa priorité. L'éditeur recommande aux utilisateurs de mettre à jour de manière proactive leurs systèmes d'exploitation, et de faire preuve de prudence lors de l'ouverture des pièces jointes. Dans ses solutions, ESET recommande d'activer LiveGrid.

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

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

Pour AV-Test, 29 suites de sécurité sur 32 ne sont pas correctement protégées

	Pour AV-Test, 29 suites de sécurité sur 32 ne sont pas correctement protégées

AV-Test publie l'analyse de 32 suites de sécurité visant à mesurer leur capacité à s'autoprotéger. Seuls trois éditeurs, dont ESET, ont réussi le test.

De la même façon que les utilisateurs protègent leurs appareils, les logiciels doivent disposer de mesures de sécurité pour s'autoprotéger en cas d'attaque. Plusieurs techniques existent comme l'ASLR et la DEP.

« Pour offrir une protection exceptionnelle en matière de cybersécurité, les éditeurs doivent fournir une protection reposant sur un noyau parfaitement protégé », déclare Andreas Marx, PDG d'AV-TEST GmbH. Lors de la publication du premier test d'autoprotection **en 2014, 2 produits seulement (dont ESET) utilisaient en continu la technique de l'ASLR et de la DEP**. Une prise de conscience s'est alors emparée des autres éditeurs, mais cela ne suffit pas.

Autre mesure de sécurité, l'utilisation de signatures et de certificats de fichiers. Ceci est important, car elle permet de vérifier l'authenticité et l'intégrité des fichiers. AV-Test analyse donc dans son test un certificat et sa validité concernant les fichiers PE en mode utilisateur pour 32 et 64 bits. Là encore, **certains éditeurs de sécurité ont jusqu'à 40 fichiers non sécurisés sur leur produit**, soit 16% de la totalité des fichiers.

« Certains fabricants n'ont toujours pas compris qu'une suite de sécurité doit être cohérente dans son ensemble : elle doit offrir la meilleure protection à l'utilisateur tout en étant parfaitement sûre elle-même, à commencer par le téléchargement de la version d'essai sur un serveur protégé », ajoute Andreas Marx.

AV-Test étudie également le protocole de transfert utilisé. En théorie, les logiciels de sécurité doivent passer par le protocole HTTPS. Il garantit la sécurité de leur site Internet. Sans cette protection, des attaques peuvent avoir lieu à l'insu de l'utilisateur. Bien qu'il n'y ait pas de téléchargements directs pour les solutions réservées aux entreprises, de nombreux éditeurs proposent une version d'essai gratuite aux particuliers. AV-Test dresse alors un constat effrayant : **sur les 19 fabricants, 13 d'entre eux ne disposent pas d'un protocole HTTP sécurisé.** Seuls 6 éditeurs, dont ESET, ont recours au protocole HTTPS.

Si vous souhaitez accéder à l'analyse complète du rapport AV-Test, cliquez ici. Pour toutes questions relatives aux règles de sécurisation, nous nous tenons à votre disposition.

[Article original]

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 : *Boîte de réception (302) – denis.jacopini@gmail.com – Gmail*