Cryptovirus Petya : La police ukrainienne saisit les PC de l’éditeur M.E.Doc

Cryptovirus Petya : La police ukrainienne saisit les PC de l’éditeur M.E.Doc

Les malwares Petya ont utilisé le mécanisme de mise à jour du logiciel de comptabilité et de fiscalité M.E.Doc, très répandu en Ukraine, pour se propager et bloquer les ordinateurs du pays et du monde entier.

La cyberpolice ukrainienne est intervenue pour prévenir de nouvelles attaques à l’image de celle perpétrée en fin juin 2017. L’attaque NotPetya – également appelée Diskcoder.c, ExPetr, PetrWrap et Petya – avait été d’abord considérée par les chercheurs comme une attaque de ransomware. Si NotPetya a ciblé des entreprises partout dans le monde, l’Ukraine a été particulièrement touchée parce que, comme l’ont constaté les chercheurs en sécurité, pour diffuser le malware, les premières attaques ont détourné le système de mise à jour automatique du logiciel de comptabilité et de fiscalité M.E.Doc très utilisé dans le pays.

Selon la police qui a analysé l’un des ordinateurs du développeur du logiciel, une porte dérobée a probablement été introduite dans M.E.Doc dès le 15 mai. Mercredi, les autorités ont annoncé qu’elles avaient saisi des ordinateurs et des logiciels du développeur de M.E.Doc après avoir repéré de nouveaux signes d’activités malveillantes pour analyse. Les enquêteurs espèrent que la mise hors circuit de ces machines empêchera une nouvelle diffusion incontrôlée du malware NotPetya utilisé dans la précédente attaque…[lire la suite]

Notre métier : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec le RGPD (réglement Européen relatif 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 : *Petya : La police ukrainienne saisit les PC de l’éditeur M.E.Doc – Le Monde Informatique*

ESET attribue la cyberattaque Petya au groupe TeleBots

	ESET attribue la cyberattaque Petya au groupe TeleBots

Selon les experts ESET®, la cyberattaque dite « Petya » pourrait être attribuée au groupe TeleBots. Il existe des similitudes entre les nombreuses campagnes menées contre l'Ukraine, l'amélioration des outils utilisés par le cyber-groupe entre décembre 2016 et mars 2017 et la menace Diskoder.C (Petya).

« La cyberattaque de 2016 menée contre les institutions financières ainsi que le développement d'une version Linux du malware KillDisk par TeleBots, ont attiré l'attention des chercheurs ESET. En parallèle, le nombre croissant d'attaques contre les systèmes informatiques que connaît l'Ukraine **nous ont fait pointer du doigt le groupe TeleBots,** » déclare Anton Cherepanov, Senior malware researcher chez ESET.

Le mode opératoire du groupe TeleBots est l'utilisation systématique du malware KillDisk qui réécrit les extensions de fichiers des victimes. L'obtention d'une rançon n'est donc pas leur objectif principal, car les fichiers cibles ne sont pas chiffrés, mais réécrit. Si l'évolution du malware contient de nouvelles fonctions, comme le chiffrement ou l'ajout de leurs coordonnées, l'objectif de KillDisk n'est toujours pas de récolter de l'argent.

Entre janvier et mars 2017, TeleBots a compromis une société d'édition de logiciels en Ukraine, utilisant alors des tunnels VPN pour accéder aux réseaux internes de plusieurs institutions financières. Au cours de cette campagne, l**es cybercriminels ont utilisé tout un arsenal d'outils en Python, SysInternals PsExec et des logins de session Windows volés pour déployer un nouveau ransomware.** Il fut détecté par ESET comme Win32/Filecoder.NKH et fut suivi par une version pour Linux, détecté comme Python/Filecoder.R.

TeleBots a ensuite lancé un nouveau malware le 18 mai 2017 : Win32/Filecoder.AESNI.C (également appelée XData). C**e ransomware s'est principalement diffusé en Ukraine via une mise à jour du logiciel financier M.E.Doc, largement utilisé en Ukraine.** Selon le LiveGrid® d'ESET, le malware se déploie juste après l'exécution du logiciel, **ce qui lui permet de se répandre automatiquement à l'intérieur d'un réseau compromis.** Bien qu'ESET ait mis à la disposition un outil de déchiffrement pour la plateforme Windows®, cette attaque ne fut pas très médiatisée.

Le 27 juin 2017, l'épidémie de ransomwares de type Petya (Diskoder.C) ayant compromis de nombreux systèmes notamment en Ukraine, a permis de montrer **la capacité du malware à remplacer le MBR par son propre code malveillant, code qui a été emprunté au ransomware Win32/Diskoder.Petya :** c'est pourquoi certains chercheurs ont nommé cette menace ExPetr, PetrWrap, Petya ou NotPetya.

Cependant, contrairement au ransomware original Petya, **les auteurs de Diskcoder.C ont modifié le code MBR de telle sorte que la récupération de fichiers ne soit pas possible, malgré l'affichage des instructions de paiement.** Une fois le malware exécuté, **il tente de se propager à l'aide de l'exploit Eternablue, en s'aidant de la backdoor DoublePulsar.** Il s'agit de la même méthode utilisée par le ransomware WannaCry.

Le malware est également capable de se diffuser de la même manière que le ransomware Win32/Filecoder.AESNI.C (XData), en utilisant Mimikatz, pour obtenir des mots de passe, puis en exécutant SysInternals PsExec. En outre, les attaquants ont mis en place une troisième méthode de diffusion à l'aide d'un mécanisme WMI.

Ces trois méthodes ont été utilisées pour diffuser les ransomwares, cependant et contrairement à WannaCry, l'exploit EternalBlue utilisé par le malware Diskoder.C cible uniquement des ordinateurs ayant un adressage interne.

Lier TeleBots à cette activité permet de comprendre pourquoi les infections se sont étendues à d'autres pays que l'Ukraine. ESET a analysé les connexions VPN entre les employés, les clients et les partenaires mondiaux de l'éditeur ainsi que le système interne de messagerie et d'échange de documents. Tout cela a permis aux cybercriminels d'envoyer des messages aux victimes (spearphishing). Les pirates ayant eu accès au serveur légitime de mise à jour ont diffusé des mises à jour malveillantes automatiquement (aucune interaction avec l'utilisateur ne fut nécessaire).

« Avec une infiltration si poussée dans l'infrastructure de l'éditeur du logiciel M.E.Doc et de sa clientèle, les pirates disposaient des ressources nécessaires pour diffuser Diskoder.C. Bien qu'il y eut des dommages collatéraux, cette attaque a permis de démontrer la connaissance approfondie de leur cible par les pirates. D'autre part, **l'amélioration du kit d'exploit EternalBlue le rend encore plus sophistiqué, ce à quoi devront faire face les acteurs de la cybersécurité dans les prochaines années,** » conclut Anton Cherepanov.

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 : *ESET*

Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage

Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage

---

Le déchiffrement des machines impactées est impossible. La demande de rançon n'était donc qu'un leurre pour camoufler un cybersabotage. La piste d'un acte politique, probablement réalisé par une agence gouvernementale, émerge.

Mauvaise nouvelle pour toutes les victimes de NotPetya. Les dernières analyses des chercheurs en sécurité montrent que ce malware est en réalité un logiciel de sabotage déguisé en ransomware. Les victimes ne pourront donc retrouver leurs données, à moins qu'un expert arrive à détecter une faille dans le processus de chiffrement.

Plusieurs indices prouvent que les auteurs de NotPetya n'ont jamais eu l'intention d'envoyer une quelconque clé de déchiffrement. Le premier concerne l'identifiant unique affiché dans le message de rançonnage et que la victime doit envoyer aux pirates après avoir effectué le paiement en bitcoins. En théorie, cet identifiant doit permettre aux auteurs de NotPetya d'identifier la victime. Il doit, par conséquent, contenir des informations sur les clés de chiffrement utilisées sur la machine en question. Mais selon les chercheurs de Kaspersky, il s'avère que cet identifiant est totalement aléatoire. *« Les attaquants ne peuvent extraire une quelconque information de déchiffrement d'une telle suite de caractères aléatoire »*, soulignent-t-ils dans une note de blog.

Kaspersky – L'identifiant unique affiché est totalement aléatoire

De son côté, le chercheur en sécurité Matt Suiche a découvert que les données de la zone d'amorçage ne sont sauvegardées nulle part, mais simplement remplacées par autre chose. Le système de fichier du disque serait donc de toute façon irrécupérable. *« La version actuelle de Petya a été réécrite pour être un wiper, et non un ransomware »*, souligne l'expert….[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 : *Non, NotPetya n'est pas un ransomware… mais un logiciel de sabotage*

Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?

	Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?

Il s’est répandu à très grande vitesse, et est plus évolué que son prédécesseur, WannaCry.

Après WannaCry, Petya. Pour la deuxième fois en quelques semaines, un « rançongiciel » (*ransomware*, en anglais) s’est largement propagé sur Internet, rendant inutilisable de nombreux ordinateurs et perturbant lourdement le fonctionnement de plusieurs grandes entreprises.
Le code de ce rançongiciel a été disséqué par de nombreux experts et entreprises de sécurité informatique ces dernières heures, permettant de mieux comprendre la manière dont il fonctionne.

Que fait-il exactement ?

Petya est un rançongiciel visant les systèmes Windows : il rend indisponibles les données d’un ordinateur, qui ne peuvent être déverrouillées qu’en versant une rançon. Il s’agit d’une variation très modifiée d’une souche apparue au printemps 2016.
A la différence de WannaCry, Petya commence par s’attaquer à la toute petite partie du disque dur – qui recense tous les fichiers présents dans la mémoire d’un ordinateur – et la chiffre, les rendant inutilisables. Ensuite, il s’en prend à la partie du disque dur qui permet de lancer le système d’exploitation, le logiciel qui fait fonctionner l’ordinateur. Cette partie est modifiée de manière à ce que l’ordinateur ne puisse plus démarrer en utilisant le système d’exploitation prévu. Lorsqu’on allume l’ordinateur, c’est Petya qui se lance, et le rançongiciel fait son travail. Un message s’affiche alors, réclamant que soient envoyés 300 dollars en bitcoin, la monnaie électronique, pour obtenir la clé de déchiffrement.
Il est extrêmement déconseillé de verser la rançon : outre le fait que payer entretient les réseaux mafieux qui se cachent souvent derrière les rançongiciels, l’adresse e-mail qui servait aux auteurs de Petya à rentrer en contact avec les victimes a été désactivée par le fournisseur de messagerie, rendant tout versement parfaitement inutile.

Comment se propage-t-il ?

Les développeurs de ce logiciel ont mis beaucoup de soin aux fonctionnalités d’infection de Petya, qui utilise plusieurs méthodes de propagation dites *« latérales »*, vers les ordinateurs appartenant au même réseau que la machine infectée.
Une fois installé sur un ordinateur, Petya va chercher à y obtenir les plein pouvoirs et repérer les autres appareils branchés sur le même réseau. Le rançongiciel va ensuite fouiller dans l’ordinateur qu’il a infecté pour récupérer des identifiants et des mots de passe qu’il va pouvoir ensuite réutiliser dans le réseau pour prendre le contrôle de davantage d’appareils et démultiplier sa propagation. Ensuite, à l’aide de fonctionnalités classiques de Windows utilisées pour gérer les réseaux, il va se transférer vers d’autres machines.
Outre cette fonctionnalité, il utilise aussi deux outils – EternalBlue et EternalRomance – volés à la NSA, la puissante agence de renseignement américaine, qui, en exploitant une faille dans un protocole permettant aux ordinateurs de se « parler » au sein d’un même réseau, permettent sa propagation de machine en machine. EternalBlue était d’ailleurs déjà utilisé par WannaCry.
L’utilisation de plusieurs méthodes d’infection expliquerait pourquoi certaines machines pourtant immunisées contre EternalBlue et EternalRomance, car ayant installé les mises à jour de sécurité correspondantes de Microsoft, soient quand même infectées par Petya.
Son mécanisme de propagation à l’intérieur d’un réseau d’une entreprise fait que les postes de travail classiques ne sont pas les seuls à succomber à Petya. Des ordinateurs plus centraux, plus sensibles, sont aussi atteints, comme les serveurs sur lesquels fonctionnent les sites Web. C’est pour cette raison que plusieurs sites du groupe Saint-Gobain étaient inaccessibles mercredi 28 juin au matin, selon une source interne…[lire la suite]

Réagissez à cet article

Source : *Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?*

« Erebus », un ransomware qui vise des systèmes fonctionnant sous Linux

« Erebus », un ransomware qui vise des systèmes fonctionnant sous Linux

---

L'hébergeur coréen Nayana a été victime du ransomware « Erebus », un ransomware spécialement modifié par les attaquants pour viser des systèmes fonctionnant sous Linux.

Contrairement à toutes les recommandations, la société a accepté de payer 550 bitcoins, soit environ un million de dollars, afin de récupérer ses données. Dans un communiqué, Nayana explique que plus de 150 de ses 300 serveurs ont été compromis et infectés par le malware, soit plus de 3400 sites web hébergés par Nayana mis hors ligne par l'attaque. Il s'agit de l'une des plus importantes rançons jamais évoquées publiquement par une entreprise victime de ransomware à ce jour.
N'oublions pas que **des premiers malwares de la famille Trojan.Encoder sont apparus en 2006-2007**. Depuis, leur nombre ne cesse de croître et les ransomware à chiffrement représentent l'une des menaces les plus dangereuses avec plusieurs milliers de modifications et des douzaines d'algorithmes de chiffrement différents pour crypter les fichiers de l'utilisateur.
Ainsi, **Boris Sharov, PDG de Doctor Web**, affirme: « **Nous recevons une centaine de demandes par jour pour déchiffrer des fichiers et dans 90 % des cas**, les utilisateurs lancent eux-mêmes les Trojan.Encoder sur leur ordinateur »…[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 : *« Erebus », un ransomware qui vise des systèmes fonctionnant sous Linux – Globb Security FR*

« La plupart des crypto virus

viennent de Russie et d’Ukraine»

	« La plupart des crypto virus viennent de Russie et d’Ukraine»

Lors du salon Viva Technology, qui se déroulait à Paris du 15 au 17 juin, Ondrej Vlcek, directeur technique de la société Avast, l'un des antivirus les plus populaires du monde, animait une conférence sur «le commerce des malwares». Alors qu'une nouvelle attaque d'un logiciel malveillant appelé WannaCry a touché la planète en mai dernier, comment se prémunir d'une telle menace à l'avenir? Quelles sont les bonnes pratiques à adopter pour minimiser les risques?

Ondrej Vlcek : C'est le nom d'une catégorie de malwares («logiciels malveillants») qui réclament une rançon. Généralement, une fois qu'un rançongiciel est installé, le hacker s'empare du disque dur des victimes avec tous leurs fichiers personnels et demande de l'argent pour rendre les fichiers – sans quoi il les supprime. Une fois que l'ordinateur est infecté, le rançongiciel commence à chiffrer les fichiers, c'est-à-dire à les transformer afin qu'ils ne soient plus lisibles et que l'on ait besoin d'un mot de passe ou d'une clé de chiffrement pour y avoir accès. Il existe aujourd'hui de nouvelles variantes : en plus de crypter le disque dur, le rançongiciel peut aussi menacer l'utilisateur de faire fuiter les fichiers volés sur tout l'Internet.

Les vieux virus étaient beaucoup moins agressifs : ils détournaient votre ordinateur et l'utilisaient simplement pour envoyer des spams ou vous obliger à cliquer sur des pubs afin de générer de l'argent. Ils pouvaient aussi détourner votre ordinateur pour vous espionner et connaître vos mots de passe et identifiants. Là, une fois que la machine est infectée, vos fichiers personnels sont immédiatement modifiés et l'on vous réclame tout de suite de l'argent pour y accéder.

WannaCry est particulièrement inquiétant, car c'est un rançongiciel « auto-répliquant ». Qu'est-ce que cela signifie ?

Normalement, la plupart des logiciels malveillants aujourd'hui nécessitent l'action de l'homme : vous devez cliquer sur un lien, ouvrir une pièce jointe associée à un message électronique ou faire quelque autre exécution manuelle. Ici, tout est entièrement automatisé, c'est-à-dire que si vous avez un ordinateur vulnérable ou pas à jour, WannaCry peut l'infecter sans avoir besoin d'aucune interaction humaine, sans même que vous soyez devant votre ordinateur.

Quelles conséquences cela peut-il avoir sur l'ampleur de WannaCry ?

Cela rend sa propagation beaucoup plus rapide, car le fait de devoir cliquer sur un lien peut prendre des jours ou des semaines. Concernant WannaCry, le monde entier a été infecté en deux heures, le logiciel passant d'un ordinateur à l'autre.

Savons-nous aujourd'hui d'où viennent tous ces logiciels malveillants ? Et quelles sommes d'argent sont impliquées dans ces attaques ?

Pour ce qui concerne les rançongiciels, la plupart viennent de Russie et d'Ukraine (concernant WannaCry, la piste nord-coréenne semble la plus probable, ndlr). Nous avons des indications qui nous laissent penser que la majorité des rançongiciels aujourd'hui sont déployés de façon à ce qu'ils n'affectent pas les personnes vivant en Russie. La raison est qu'il existe en Russie une loi qui rend la création de rançongiciels illégale lorsqu'ils peuvent avoir un impact sur des citoyens russes, mais techniquement légale, d'une certaine manière, lorsqu'ils infectent des gens hors de Russie. L'année dernière, une estimation publiée par le FBI chiffrait le coût de ces cyberattaques à plus d'un milliard de dollars. Cette année, ce montant va probablement doubler et monter à plus de deux milliards de dollars.

Peut-on neutraliser ce type de logiciels malveillants ?

Il y a deux enjeux. Le premier, c'est la prévention. Très important : utiliser un système d'exploitation à jour afin de ne pas être trop vulnérable. Il faut aussi installer un logiciel antivirus de qualité. Enfin, il vaut mieux faire des sauvegardes régulièrement, car vous pouvez ainsi récupérer vos fichiers en cas d'attaque. Je fais des sauvegardes tous les jours et je recommande à tout le monde de faire de même.

La majorité des sauvegardes se font automatiquement, mais il faut être prudent sur ce point parce que, si le rançongiciel est installé sur l'ordinateur depuis un certain temps – un jour ou deux – la sauvegarde peut aussi enregistrer les fichiers infectés qui écraseront les anciennes versions saines.

Le second enjeu apparaît lorsque l'infection s'est produite : que peut-on faire ? En fait, quasiment la moitié des rançongiciels peuvent être supprimés et décryptés sans payer la rançon, car le chiffrement n'est pas bien installé, et possède des failles. Nous ou d'autres entreprises spécialisées dans la cybersécurité sommes capables d'accéder à l'algorithme de chiffrement et de décrypter les fichiers. Mais s'il est installé correctement, il n'y a aucune chance. Avec les ordinateurs d'aujourd'hui, décrypter les fichiers prendrait des centaines d'années.

Mon conseil : si vous êtes attaqué et qu'il n'y a pas de moyen de décrypter le disque dur aujourd'hui, ne supprimez pas vos fichiers infectés pour autant si vous en avez vraiment besoin. Bien que l'outil de décryptage pour ce rançongiciel en particulier ne soit pas disponible pour le moment, il peut l'être dans six mois, un mois ou même une semaine…[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 : *Cybercriminalité: «La plupart des rançongiciels viennent de Russie et d'Ukraine» – Technologies – RFI*

L'humain, maillon faible de la cybersécurité

L'humain, maillon faible de la cybersécurité

« Le Facteur Humain 2017 » indique que les cybercriminels se reposent de plus en plus sur l'humain plutôt que sur les failles logicielles pour installer des programmes malveillants, dérober des informations confidentielles et transférer des fonds.
Pas vraiment une nouveauté, le **piratage informatique** s'est toujours d'abord reposé sur le facteur humain. Le **social engineering** en est une preuve. Dans son rapport, Proofpoint spécialiste en sécurité et conformité, a interrogé plus de 5000 entreprises en 2016. Bilan, les indicateurs sur les attaques par le biais des emails, mobiles et réseaux sociaux, donne une tendance des clients de cette société.

« C***ette tendance d'exploitation du facteur humain, qui a vu le jour en 2015, s'accélère, et les cybercriminels multiplient désormais les attaques générées par les clics des utilisateurs plutôt que par des logiciels d'exploitation vulnérables, conduisant ainsi les victimes à exécuter elles-mêmes les attaques*** », a déclaré Kevin Epstein, Vice-Président du centre d'opération des menaces de Proofpoint. « ***Il est essentiel que les entreprises mettent en place une protection avancée pour arrêter les cybercriminels avant qu'ils puissent atteindre leurs potentielles victimes. La détection anticipée des contenus malveillants dans la chaîne d'attaques permettra de les bloquer, de les canaliser et de les supprimer plus facilement.*** »…[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 : *L'humain, maillon faible de la cybersécurité – Data Security BreachData Security Breach*

Des clés de déchiffrement pour le ransomware Crysis mises en ligne

Des clés de déchiffrement pour le ransomware Crysis mises en ligne

Au total, 200 clés principales ont été publiées sur Internet. Elles permettent à des victimes du ransomware de déchiffrer leurs fichiers et de récupérer ainsi le contrôle de leurs données.

Le monde a été secoué par WannaCry, un ransomware qui a causé des perturbations et des bouleversements dans d'importants services et des entreprises au cours de la dernière semaine. Mais il y a de bonnes nouvelles pour les victimes d'un autre rançongiciel baptisé Crysis, avec la diffusion auprès du public de 200 clés principales.
Publiées sur le forum BleepingComputer, les clés peuvent être utilisées par les victimes du ransomware, ainsi que par les entreprises de sécurité spécialisée dans la création d'outils de déchiffrement.
Les clés, téléchargées sur Pastebin, sont valides, ont confirmé des chercheurs en sécurité. Les utilisateurs des clés ont également confirmé qu'ils avaient pu recouvrer l'accès à leurs fichiers.

Si vous avez été affecté par cette souche de ransomware, vous pouvez télécharger un outil de déchiffrement fourni par l'éditeur de sécurité ESET…[lire la suite]

Réagissez à cet article

Source : *Ransomware Crysis : des clés principales mises en ligne – ZDNet*

EternalRocks, le successeur de WannaCry encore plus inquiétant ?

	EternalRocks, le successeur de WannaCry encore plus inquiétant ?

Après l’attaque du ransomware WannaCry, les chercheurs ont identifié le ver de réseau EternalRocks. Celui-ci utilise jusqu’à 7 outils de hacking ayant été volés à la NSA puis exposés par le groupe Shadow Brokers.

Selon Malwarebytes, WannaCry a recherché les ports SMB vulnérables avant d’utiliser EternalBlue pour rentrer sur le réseau et le backdoor DoublePulsar pour installer le ransomware. EternalRocks utilise aussi ces deux outils. (crédit : D.R.)

Une semaine après l’attaque perpétrée par le ransomware WannaCry au niveau mondial, un autre logiciel d’exploitation de failles fait parler de lui. Selon des chercheurs en sécurité, il y a au moins une personne qui utilise 7 des outils d’attaque volés à la NSA dans un ver de réseau dénommé EternalRocks par ceux qui l’ont identifié. Les chercheurs ont constaté que ce ver ciblait la même vulnérabilité du protocole SMB de Windows, en s’avérant plus menaçant et plus difficile à contrer. Comme WannaCry, EternalRocks utilise EternalBlue, l’un des outils de la NSA.

Malwarebytes pense que WannaCry n’a pas été diffusé par une campagne de spams malveillant mais par une opération de scanning qui a d’abord recherché les ports SMB accessibles publiquement et vulnérables avant d’utiliser EternalBlue pour rentrer sur le réseau et d’utiliser la porte dérobée DoublePulsar pour installer le ransomware…[lire la suite]

Réagissez à cet article

La cyberattaque ‘‘WannaCry’’

aurait déjà coûté… 1 Milliard de dollars

	La ‘‘WannaCry’’ cyberattaque aurait déjà coûté… 1 Milliard de dollars

La cyberattaque globale WannaCry a causé des dégâts s'élevant à 1 milliard de dollars, relate le cabinet spécialisé ''McClatchyDC''. Ces dommages ont été causés par l'immobilisation de la production de grandes entreprises dans le monde entier.

Une situation liée à la perte de donnés, à la réduction de la productivité, à des perturbations du travail, au préjudice porté à la réputation, ainsi qu'à plusieurs autres facteurs.

La cyberattaque utilisant le virus WannaCry est considérée comme le plus grand piratage à rançon de l'histoire.

L'attaque a fait, selon Europol, 300 000 victimes dans au moins 150 pays depuis le 12 mai.

Et parmi les organisations touchées par cette attaque, on retrouve notamment Vodafone, FedEx, Renault, le National Health Service britannique ou encore la Deutsche Bahn.

Rédaction Infomédiaire

Remarques de Denis JACOPINI

L'évolution de ce virus et les dégâts qu'il produit sont à la mesure du nombre d'ordinateurs interconnectés dans le monde.

Pour ma part, ce virus n'a à ce stade, rien d'exceptionnel en terme d'ampleur. Il suffit de se renseigner un peu et découvrir que le virus Conficker, un ver informatique exploitant une faille de Windows, apparu en 2008 a touché, d'après les estimations 15 millions de victimes alors qu'il y avait 2 milliards d'internautes en moins (57% en moins car aux alentours de 3.5 milliard aujourd'hui et seulement aux alentours de 1,5 milliard en 2018 http://www.journaldunet.com/ebusiness/le-net/1071539-nombre-d-internautes-dans-le-monde)

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 : *Economie mondiale : La cyberattaque ''WannaCry'' a coûté… 1 MM$ | Infomédiaire*

http://www.liberation.fr/futurs/2017/05/15/guillaume-poupard-la-cybercriminalite-devient-une-question-de-securite-nationale_1569743