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

	La cyberattaque ‘‘WannaCry’’ 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

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

---

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

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*

Des hackers à l'origine de la cyber attaque mondiale

menacent de divulguer d’autres failles

Des hackers à l’origine de la cyber attaque mondiale menacent de divulguer d’autres failles

Le groupe de pirates Shadow Brokers, qui avaient révélé la faille du système Windows à l’origine de la vaste opération de cyberattaque, affirme dans un message qu’il pourrait récidiver.

Le mystérieux groupe de pirates informatiques Shadow Brokers, qui a révélé en avril la faille exploitée pour mener une attaque informatique massive la semaine dernière dans le monde, a menacé d’en révéler d’autres le mois prochain.

Dans un message posté tard mardi soir sur internet, le groupe indique dans un très mauvais anglais qu’il acceptera à partir de début juin des paiements en échange desquels les souscripteurs recevront chaque mois des informations sur des techniques de piratage et des vulnérabilités informatiques…[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: des hackers menacent de divulguer d’autres failles*

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

Google tente d’arrêter une attaque de phishing sur Gmail

Google tente d’arrêter une attaque de phishing sur Gmail

Cette tentative de hameçonnage a tenté de faire croire aux utilisateurs ciblés qu’ils étaient en liaison avec Google Docs. Moins de 0,1% des utilisateurs de Gmail ont été touchés, assure Google.
Le courrier électronique provenait de l’adresse réelle d’un contact connu et demandait de cliquer sur un lien censé conduire à un fichier partagé avec le service en ligne de Google Docs. En cliquant sur le lien, on arrivait sur une véritable adresse web de Google et une autorisation pour exécuter une application que le(s) hackers(s) avait(ent) habilement appelée « Google Docs » était demandée…[lire la suite]

Réagissez à cet article

Source : *Cybersécurité : Google essuie une attaque de phishing sur Gmail – Les Echos*

Toutes les sirènes d’urgence de Dallas piratées et déclenchées

	Toutes les sirènes d’urgence de Dallas piratées et déclenchées

Tornade imminente ? Menace non identifiée mais liée aux récents bombardements américains en Syrie ? Dans la nuit du vendredi 7 au samedi 8 avril, les habitants de Dallas, au Texas, ont eu tout le temps de se demander pourquoi les 156 sirènes habituellement utilisées pour avertir d'un danger météorologique ont retenti pendant plus d'une heure et demie, entre 23h40 et 1h20.

Si la municipalité a parlé dans un premier temps de « *dysfonctionnement* », elle a fini par reconnaître qu'il s'agissait d'un piratage, dont le ou les auteur(s) reste(nt) à ce jour non identifié(s).
En pleine nuit, Dallas a donc pris des airs de ville submergée par une catastrophe de grande ampleur, comme le montrent les vidéos postées par différents habitants sur les réseaux sociaux, qu'ils soient ouvertement inquiets ou s'interrogent plus ou moins ironiquement : « *Vous vous êtes déjà demandé à quoi ressemblait la fin du monde ?* » D'autant qu'il était impossible d'échapper aux sirènes, celles-ci retentissant du nord au sud de la ville, selon la disposition voulue par la municipalité.

L'IDENTITÉ DU OU DES HACKER(S) RESTE INCONNUE

Les sirènes ont retenti une quinzaine de fois pendant 1 minute 30 à chaque nouveau déclenchement, alors que les équipes techniques de la ville les éteignaient en vain, comme l'explique Sana Syed, porte-parole de la municipalité : « *À chaque fois que nous pensions les avoir éteintes, les sirènes sonnaient de nouveau car le hacker nous piratait en continu* ». Résignée, la ville a finalement désactivé entièrement le système d'alarme, y compris pendant le week-end : il doit être relancé à temps pour les tornades attendues cette semaine.
Quant à l'identité du ou des pirate(s), le mystère reste entier. « *Nous sommes convaincus que le piratage provient de la région de Dallas car vous devez nécessairement être à proximité du signal pour le déclencher* » souligne Sana Syed. Rocky Vaz, directeur du Bureau de gestion des urgences de Dallas, se montre assez pessimiste sur les chances de retrouver le coupable, une recherche qu'il assimile à trouver « *une aiguille dans une botte de foin* » contrairement au maire de la ville, Mike Rawlings, qui affirme que les autorités « *retrouveront et poursuivront le responsable, quel qu'il soit* ». La municipalité a notamment demandé l'aide de l'Agence de régulation des télécoms pour mener l'enquête…[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 : *Un hacker déclenche toutes les sirènes d'urgence de Dallas, les habitants paniquent — Tech — Numerama*

Les services Cloud au centre d’attaques d’entreprises par APT10

	Les services Cloud au centre d’attaques d’entreprises par APT10

Le groupe de pirates chinois APT10 a infiltré des services Cloud managés pour remonter aux serveurs des entreprises qui les utilisent.

La maturité des attaques ciblées contre les entreprises est montée d'un cran. *« Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience »*, a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme *« l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées »*. Pas moins.

De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. *« PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles »*, indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne…[lire la suite]

Réagissez à cet article

Source : *Les services Cloud au centre d'attaques d'entreprises par APT10*

Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

Chers revendeurs informatiques, attention à la nouvelle arnaque. Les intentions des pirates ne sont pas encore connues, mais les intentions sont forcément malveillantes.

En tant que revendeur informatique, il est fort probable que vous commandiez votre matériel destiné à la revente ou non chez les principaux et parmis les plus anciens grossistes et importateurs Français : Ingram ou Techdata.
Une récente communication de Techdata, qui nous a été remontée par un précieux partenaire Parisien, nous informe que Techdata vient de lancer l'alerte suivante auprès de ses clients :

Cher client,
Il a été porté à notre connaissance que certains Clients de TECH DATA ont reçu des emails comportant un lien internet vers un site web frauduleux leur demandant :
– de s'inscrire à une conférence dans laquelle TECH DATA et d'autres distributeurs participeraient,
– de fournir des informations type login et mot de passe de TECH DATA ainsi que d'autres informations sensibles.
Le site Web apparaît comme indiqué ci-dessous :

Veuillez noter que ce site web n'est d'aucune façon associé à TECH DATA. La sécurité de nos partenaires est une priorité pour TECH DATA et nous n'autorisons aucun tiers à collecter les identifiants de connexion de nos clients.
Aussi, actuellement nous œuvrons avec les autorités compétentes pour la fermeture de ce site frauduleux.
A ce jour, à notre connaissance les clients européens ne semblent pas affectés, ce site frauduleux visant les clients américains principalement.
Cependant, nous comptons sur votre vigilance et vous remercions de nous informer dans le cas où vous recevriez des emails contenant des liens vers ce site internet ou similaires en vous adressant à l'adresse suivante : itsecurity@techdata.com
Nous attirons votre attention sur la sophistication et l'augmentation de la cybercriminalité (phishing), dès lors restez vigilants.
Nous vous remercions de votre attention et collaboration.
Tech Data Europe

Comme vous pouvez le remarquer, à l'instar de KPMG pourtant spécialisé en audit et conseil dans de nombreux domaines dont la sécurité informatique, pourtant victime d'une arnaque au Président leur ayant coûté plusieurs millions d'Euros (7,6) en 2014, les professionnels de l'informatique sont aussi la cible des pirates.
Nous espérons que, même si la plupart n'ont pas assisté à nos conférences de sensibilisation à la Cybercriminalité, ils sauront à quoi ressemble le loup pour ne pas le laisser rentrer dans la bergerie.

Denis JACOPINI

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 : *E-mailing Tech Data France*