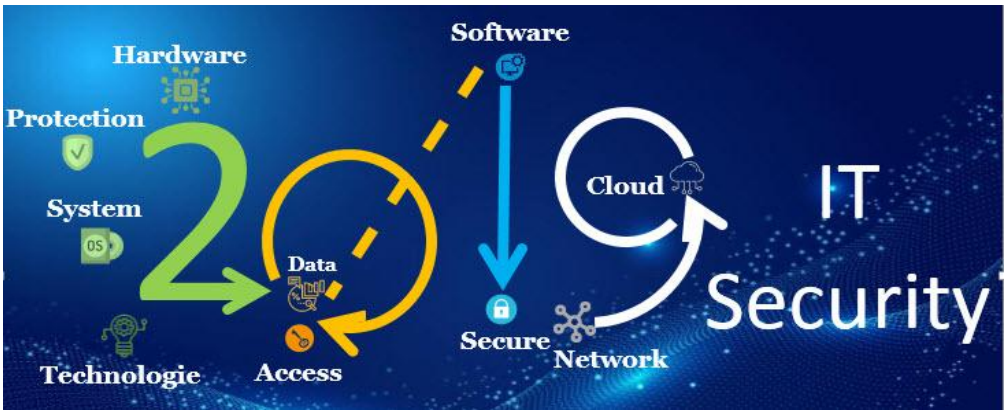

BULLETIN DE VEILLE N°8

ANPT-2019-BV-08

«Alors que le monde est de plus en plus interconnecté, tout le monde partage la responsabilité de sécuriser le cyberespace.» - Newton lee-

Decembre 2019

Alertes de sécurité

Réseaux sociaux

Mettez à jour votre application Twitter dès maintenant si vous êtes sur Android

20 décembre 2019

Twitter a corrigé une vulnérabilité dans son application Android qui aurait pu permettre à des individus malveillants de voir les informations de compte non public ou de contrôler votre compte (par exemple, envoyer des tweets ou des messages directs). Avant le correctif, grâce à un processus compliqué impliquant l'insertion de code malveillant dans des zones de stockage restreintes de l'application Twitter, un attaquant pouvait avoir accès à des informations (par exemple, messages directs, tweets protégés, informations de localisation) à partir de l'application, aucune preuve qu'un code malveillant a été inséré dans l'application ou que cette vulnérabilité a été exploitée.

Twitter lance une mise à jour de son application sous Android. Il est recommandé de la mettre à jour immédiatement à partir du Play Store.

Source : *http://bit.ly/34RALpf*

WhatsApp corrige une autre faille de sécurité dans la conversation de groupe

17 Décembre 2019

Un bug dans la conversation de groupe de l'application WhatsApp aurait pu laisser un pirate informatique bloquer complètement l'application.

La vulnérabilité spécifique, révélée par la société de sécurité Check Point en août et corrigée en septembre, aurait permis à un pirate de provoquer un chaos de discussion de groupe avec un message spécialement conçu. Pour empêcher leur application d'échouer chaque fois qu'ils ouvraient le thread infecté, les destinataires devaient désinstaller complètement WhatsApp, le réinstaller et supprimer le chat de groupe compromis de leurs comptes. Les victimes qui n'ont pas sauvegardé leurs données WhatsApp perdraient tout dans le processus de désinstallation, et même celles avec des sauvegardes abandonneraient le contenu du chat affecté, car il doit être supprimé sans le rouvrir pour arrêter le cycle de plantage.

Source : *http://bit.ly/2ZiN0df*

Firefox

Firefox corrige de multiples vulnérabilités dans ses produits.

03 décembre 2019

De multiples vulnérabilités ont été découvertes dans Mozilla Firefox et Firefox Extended Support Release (ESR), dont les plus graves permettraient à un attaquant distant d'exécuter du code arbitraire ou de provoquer un déni de service.

Il est recommandé de mettre à jour Firefox à la version 71 ou à une version supérieure. Il est aussi recommandé d'exécuter les logiciels en tant qu'utilisateur non privilégié (sans privilèges d'administration) pour diminuer les effets d'une attaque réussie.

Produits affectés :

- Versions Firefox antérieures à 71.
- Versions Firefox ESR antérieures à 68.3.

Source : *http://bit.ly/2tFUmeT*

Android

Vulnérabilité Android non corrigée et exploitée par StrandHogg

04 décembre 2019

Mauvaise nouvelle pour les utilisateurs d'Android qui installent de nombreuses applications sur leurs appareils. Il existe une vulnérabilité Android non corrigée appelée *StrandHogg* qui a été découverte par des chercheurs en sécurité de *promon*. Cette

vulnérabilité est déjà exploitée par des applications malveillantes. Un attaquant peut piéger l'appareil de sorte que lorsque l'utilisateur clique sur l'icône d'une application légitime, une version malveillante s'affiche à sa place. La victime saisit ses identifiants de connexion dans cette interface, les détails sensibles sont immédiatement envoyés à l'attaquant, qui peut ensuite se connecter et contrôler les applications.

Toutes les versions d'Android, y compris Android 10, sont concernées, il n'y a pas de correctif.

Il est à noter que l'utilisateur doit installer l'application avec le code malveillant lui-même afin que StrandHogg puisse l'exploiter. Donc, il est recommandé de bien lire la description et les commentaires des applications sur le play store avant de les installer.

Source : http://bit.ly/2scEP5N

Google confirme la menace critique DoS dans Android 8, 9 et 10

07 décembre 2019

Le bulletin de sécurité Android de décembre 2019 a été publié par Google et contient des détails sur plusieurs vulnérabilités du système d'exploitation Android. Au total, trois vulnérabilités ont reçu une note critique. Cependant, Google a souligné que la vulnérabilité référencée CVE-2019-2232 est « la plus critique » et pour une très bonne raison : un seul message conçu de manière malveillante pourrait « provoquer un déni de service permanent ».

La description officielle de la vulnérabilité par la NIST National Vulnerability Database indique qu'un message conçu de manière malveillante pourrait entraîner un DoS permanent à votre Appareil Android. « L'interaction des utilisateurs n'est pas nécessaire pour l'exploitation », poursuit la description, et l'attaque par DoS à distance n'a besoin « d'aucun privilège d'exécution supplémentaire ».

La bonne nouvelle est que les correctifs pour CVE-2019-2232 et les autres vulnérabilités de sécurité révélées dans le bulletin de sécurité Android de décembre 2019 ont déjà été publiés dans le référentiel AOSP (Android Open Source Project).

La mauvaise nouvelle est que la durée de l'obtention de la mise à jour dépend du fabricant de votre appareil.

Les systèmes affectés : Android 8, 9, et 10.

Source : http://bit.ly/2SkekNB5

Microsoft

Le correctif de décembre 2019 de Microsoft corrige la vulnérabilité zero-day de Win32k

11 décembre 2019

Microsoft a publié une mise à jour pour corriger 36 vulnérabilités. Le correctif a résolu la vulnérabilité Zero-day nommée CVE-2019-1458 d'élévation des privilèges dans Win32k.

Vous trouverez dans la source la liste complète des vulnérabilités résolues et des avis publiés dans les mises à jour du Patch de décembre 2019. Pour accéder à la description complète de chaque vulnérabilité et les systèmes affectés, vous pouvez consulter le rapport complet ici .

Source : http://bit.ly/2YDbVQY

VPN

Une nouvelle vulnérabilité permet aux attaquants de détourner les connexions VPN

05 Décembre 2019

Une faille de sécurité affectant Linux, Android, macOS et d'autres systèmes d'exploitation basés sur Unix permet à un attaquant de détecter, détourner et de falsifier les connexions via des tunnels VPN.

La vulnérabilité CVE-2019-14899 réside dans la pile réseau de plusieurs systèmes d'exploitation basés sur Unix, et plus précisément, dans la façon dont les systèmes d'exploitation répondent aux sondes de paquets réseau inattendues. L'intelligence de l'attaque réside dans la façon dont l'équipe de recherche a conçu ces paquets et dans la façon dont ils ont utilisé les réponses pour déduire ce que l'utilisateur faisait à l'intérieur de son tunnel VPN.

Selon l'équipe de chercheurs, les attaquants peuvent utiliser cette vulnérabilité pour sonder les appareils et découvrir divers détails sur l'état de la connexion VPN de l'utilisateur […].

L'équipe de recherche a déclaré que leur attaque avait fonctionné contre des technologies VPN comme OpenVPN, WireGuard et IKEv2 / IPSec, et peut-être d'autres, car "la technologie VPN utilisée ne semble pas avoir d'importance" […].

Une attaque effectuée via cette vulnérabilité n'est pas triviale à exécuter, ce qui exclurait les scénarios d'exploitation de masse jusqu'à ce que des correctifs soient disponibles.

Les systèmes affectés : Ubuntu 19.10 (systemd), Fedora (systemd), Debian 10.2 (systemd),Arch 2019.05 (systemd), Manjaro 18.1.1 (systemd), Devuan (sysV init), MX Linux 19 (Mepis+antiX), Void Linux (runit), Slackware 14.2 (rc.d), Deepin (rc.d), FreeBSD (rc.d), OpenBSD (rc.d) ; D'autres systèmes d'exploitation basés sur Unix comme Android et macOS sont également affectés.

Source : https://zd.net/2s6OHbP

Détails : http://bit.ly/2EQm22Z

Intel

La faille de Plundervolt permet aux attaquants de manipuler la tension délivrée au CPU ciblé et de voler des données.

11 décembre 2019

La méthode **overclocking** de modification des tensions et de la fréquence du processeur d'Intel directement dans le système d'exploitation […], n'est peut-être pas aussi sécurisée que prévu.

Récemment, une équipe d'experts en cybersécurité a prouvé que cette fonctionnalité particulière peut être exploitée par des acteurs de la menace qui peuvent causer des dommages importants en visant à détourner Intel SGX. […] La technique d'attaque est surnommée Plundervolt et classée CVE-2019-

11157 . Selon les conclusions de l'équipe, l'attaque exploite la fonction de réglage de la fréquence et de la tension du processeur moderne, en la contrôlant de manière à générer des erreurs dans la mémoire du système via des bits de retournement. Cette attaque affecte presque tous les processeurs Intel Core compatibles SGX, y compris la génération Skylake […]. L'attaque fonctionne sur les processeurs Intel 6e, 7e, 8e, 9e et 10e génération ainsi que sur les Xeon E3, v5, v6, E-2100 et E-2200, et n'a pas besoin d'un accès hôte avec des privilèges administratifs ou root pour être lancée.

Pourtant, exploiter la vulnérabilité aurait été difficile, voire impossible, mais il aurait fallu une combinaison d'attaques en spécifiant des cibles particulières, affirment les chercheurs. Il est également à noter que l'attaque ne peut pas être lancée dans des environnements virtuels.

Source : http://bit.ly/2PRxBx9
Correctifs : https://intel.ly/2EPTAOU

Wordpress

Vulnérabilité critique corrigée dans les redirections 301 - Easy Redirect Manager

19 Décembre 2019

L'équipe Threat Intelligence a découvert des vulnérabilités présentes dans 301 Redirects - Easy Redirect Manager, un plugin WordPress installé sur plus de 70 000 sites Web. Ces failles ont permis à tout utilisateur authentifié, même les abonnés, de modifier, supprimer et injecter des règles de redirection qui pourraient potentiellement entraîner une perte de disponibilité du site.

L'équipe a signalé le problème en privé au développeur du plugin, qui a été incroyablement rapide à répondre et à publier un correctif.

Bien que cette vulnérabilité nécessite que l'attaquant soit authentifié, de nombreux sites WordPress permettent l'enregistrement en tant qu'abonné. Pour ces sites, l'exploitation de cette vulnérabilité serait assez simple […].

Les failles ont été corrigées dans la version 2.45 et nous recommandons fortement la mise à jour à la dernière version disponible dès que possible.

Source : http://bit.ly/2sXshQ5

Apache

Deux vulnérabilités dans Apache Tomcat.

17 décembre 2019

Deux vulnérabilités ont été découvertes dans Apache Tomcat. La vulnérabilité CVE-2019-17563 réside dans la fonction d'authentification FORM qui permet de perpétrer une attaque de type Session Fixation. La deuxième vulnérabilité nommée CVE-2019-12418 permet à un attaquant local de capturer les noms d'utilisateur et les mots de passe utilisés pour accéder à l'interface JMX. L'attaquant peut ensuite exploiter ces informations d'identification pour accéder à l'interface JMX et obtenir un contrôle complet sur l'instance de Tomcat.

Il est recommandé de télécharger la version 7.0.99 qui inclut le correctif à ce problème.

Systèmes affectés : Apache Tomcat 7 versions antérieures à 7.0.99

Source : http://bit.ly/2SjnW4h

Actualité

Les extensions de ces deux antivirus vous espionnent depuis Google et Firefox

06 Décembre 2019

Wladimir Palant, fondateur d'AdBlock, a découvert que quatre extensions d'Avast et d'AVG (Avast Online Security, AVG Online Security, Avast SafePrice et AVG SafePrice) collectaient massivement des données de navigation sans en informer au préalable l'utilisateur, rapporte le site PhonAndroid.

Les informations récoltées sont les URL visitées, les titres des pages visitées, les liens sur les moteurs de recherche, l'utilisation des favoris et les saisies directes d'adresses.

En outre, M.Palant a réussi à relever un identifiant unique pour l'installation de chaque extension, la provenance géographique des utilisateurs, les mots saisis dans les champs de recherche des pages visitées, ainsi que la version exacte du navigateur Web et du système d'exploitation utilisés. Selon lui, ces informations permettent à ces deux marques connues pour l'élaboration depuis de nombreuses années d'antivirus pour Windows de créer un profil comportemental de navigation pour chaque utilisateur.

Google et Mozilla en ont été informés par le créateur d'AdBlock. Seul Mozilla a décidé de supprimer ces extensions de sa boutique en attendant qu'Avast et AVG y apportent les modifications nécessaires, sans pour autant les ajouter à la liste noire, ce qui veut dire qu'elles ne sont pas désinstallées automatiquement de Firefox. Quant à Google, il a choisi de les laisser sur son Chrome Web Store.

Source : http://bit.ly/2P1IbkS

Une nouvelle campagne de phishing utilise une page Web autonome pour voler des informations d'identification

09 Décembre 2019

Les chercheurs ont repéré une nouvelle campagne de phishing qui dérobe des informations d'identification. Cependant, cette campagne est différente des campagnes couramment observées. Elle ne redirige pas les victimes vers un autre site pour la connexion, comme le font généralement de nombreuses campagnes de phishing […]. Lorsque la victime ouvre la pièce

jointe dans l'e-mail, un formulaire de connexion Microsoft Docs est rendu directement dans le navigateur.

Le formulaire fournit un certain nombre d'options pour se connecter, notamment Gmail, Yahoo et Office 365.

Lorsque la victime entre ses identifiants, le script malveillant recueille les informations puis les redirige vers un site distant avec une fausse facture de paiement. Même si la victime se rend compte qu'il s'agit d'une page de phishing, cela ne fait aucune différence car les informations d'identification ont déjà été récoltées.

Bien que ce ne soit pas la première campagne de phishing à utiliser cette technique, les experts en sécurité disent qu'elle est l'une des rares à contenir une pièce jointe HTML aussi complexe.

Source : *http://bit.ly/38sbncz*

Bilan de l'année 2019 : mêmes menaces, plus de cibles

10 Décembre 2019

Les cyberattaques contre les infrastructures critiques ne sont pas un phénomène nouveau […]. La menace a augmenté en raison de deux tendances. Premièrement, les pirates développent en permanence des outils plus avancés, tels que Triton, un nouveau malware conçu pour arrêter les contrôleurs de sécurité et causer des dommages physiques à l'infrastructure critique. Deuxièmement, la numérisation et l'introduction d'Internet dans les systèmes antérieurs ont introduit de nouvelles vulnérabilités. Auparavant, la technologie opérationnelle était contrôlée par des systèmes analogiques, qui sont séparés des réseaux informatiques, l'isolant ainsi dans une certaine mesure des logiciels malveillants […]. Dans certains pays, comme l'Allemagne, les exploitants de certains types d'infrastructures critiques, comme les hôpitaux et les réseaux de transports publics, ne sont pas tenus de signaler les cyberattaques aux autorités. Compte tenu des conséquences potentielles de cette opération, il n'est pas difficile d'imaginer que les attaques dans ces secteurs ne sont souvent pas signalées. Malheureusement pour les gouvernements et les entreprises, ces problèmes ne disparaîtront pas aussitôt. Avec l'avènement de la technologie des villes intelligentes, le niveau d'interconnectivité et le nombre de cibles parmi lesquelles les attaquants peuvent choisir vont augmenter considérablement au cours des prochaines années. […]. Enfin, alors que la technologie des villes intelligentes a le potentiel d'améliorer la sécurité et d'optimiser les systèmes urbains, les gouvernements doivent veiller à ne pas simplement créer plus de cibles pour les adversaires en fixant et en respectant des normes de sécurité élevées pour la vague entrante d'appareils connectés.

Source : *https://on.cfr.org/2E8zFdz*

La nouvelle variante de Snatch Ransomware évite la détection en utilisant le mode sans échec

10 Décembre 2019

En enquêtant sur une série d'attaques de ransomware, les chercheurs de Sophos Labs ont repéré cette nouvelle variante du ransomware Snatch. Cette technique consistant à forcer les machines Windows à redémarrer en mode sans échec est peut-être un moyen d'ignorer la protection des terminaux.

En mode sans échec, la plupart des logiciels, y compris les logiciels de sécurité, ne s'exécutent pas, et le malware tente de chiffrer les disques durs du système infecté.

« Les SophosLabs estiment que la gravité du risque posé par les ransomwares qui s'exécutent en mode sans échec ne peut pas être surestimée, et que nous devions publier ces informations comme un avertissement pour le reste de l'industrie de la sécurité, ainsi que pour les utilisateurs finaux », ont déclaré les chercheurs de Sophos. […]

Pour éviter que ce malware n'affecte votre réseau, voici quelques actions à envisager :

- Les organisations doivent implémenter l'authentification multifacteur, en particulier pour les comptes disposant de plus de privilèges.
- Les vulnérabilités doivent être régulièrement analysées et corrigées dès que possible.
- Les organisations doivent éviter d'exposer au maximum leur Remote Desktop interface à Internet.

Source : *http://bit.ly/36ol4qt*

Plus de 750 000 demandes de copies de certificats de naissance aux États-Unis exposées en ligne

9 Décembre 2019

Une entreprise en ligne qui permet aux utilisateurs d'obtenir une copie de leurs certificats de naissance et de décès auprès des gouvernements des États américains a dévoilé un énorme cache d'applications - y compris leurs informations personnelles.

Plus de 752 000 demandes de copies de certificats de naissance ont été trouvées sur un compartiment de stockage Amazon Web Services (AWS). Le seau contenait également 90 400 demandes de certificat de décès, mais celles-ci n'étaient pas accessibles ni téléchargeables.

Le compartiment n'était pas protégé par un mot de passe, permettant à toute personne connaissant l'adresse Web, facile à deviner, d'accéder aux données […].

Source : *https://tcrn.ch/2RENTL8*

2020 pourrait apporter une toute nouvelle génération de menaces de cybersécurité

13 Décembre 2019

Un sondage de la communauté Infosec Europe - principalement des professionnels de niveau C dans l'espace de la cybersécurité, a révélé que nous pourrions très bien voir une toute nouvelle race de menaces de cybersécurité dans l'année à venir.

L'année prochaine, davantage d'outils d'automatisation de la sécurité seront déployés, selon Peter Gooch, partenaire de Deloitte en matière de cyber-risque. S'il est bien fait, il garantira aux organisations de faire face aux menaces avec agilité. Cependant, une implémentation mal faite compliquera considérablement les choses. Gooch pense également que les pirates ciblent de plus en plus les données non structurées pour masquer et lancer des attaques, ce qui signifie que les entreprises doivent mettre en œuvre une gouvernance robuste.

De plus, avec la 5G à l'horizon, il s'attend à une surface d'attaque beaucoup plus grande et à des flux de données plus difficiles à suivre.

D'un autre côté, pour Mark D. Nicholls, responsable de la sécurité de l'information et de la gouvernance à l'association du logement, Peabody, la véritable IA est à la fois une bénédiction et une malédiction. «Imaginez une attaque DDOS propulsée par une véritable IA», dit-il. […]

De nombreux autres sujets ont été abordés à Infosec Europe, y compris le RGPD, la pénurie de compétences, les violations de données et les nouvelles approches de sécurité, mais une chose sur laquelle tout le monde est d'accord - l'industrie doit travailler plus étroitement ensemble pour s'attaquer à ce qui va arriver.

Source *: http://bit.ly/2POv0D0*

Comment fonctionnent les techniques de phishing ? Des chercheurs mettent en lumière certaines techniques de phishing intelligentes

12 Décembre 2019

Selon Microsoft, les tentatives de phishing sont passées de moins de 0,2% de tous les e-mails analysés dans le monde en janvier 2018 à environ 0,6% en octobre 2019.

Pendant ce temps, le géant de la technologie basé à Redmond a également noté que le nombre de ransomwares, de crypto-mining et d'autres infections de logiciels malveillants a diminué par rapport aux enregistrements précédents. La société a publié un blog où elle a passé en revue trois des attaques de phishing les plus intelligentes qu'elle a observé et tracé cette année.

En utilisant des générateurs de trafic, les hameçonneurs s'assurent que la page de redirection est le premier résultat de recherche pour certains mots clés ou pour des termes très spécifiques afin de guider les utilisateurs vers la page d'hameçonnage réelle.

Tous les internautes connaissent bien la page 404 Not Found ; il vous indique que vous êtes sur un lien cassé ou mort. Mais, cela peut ne pas être le cas à chaque fois, car les hameçonneurs abusent de *404 pages* pour desservir des sites de phishing.

Au lieu d'inclure un lien vers l'URL de phishing, les attaquants incluent des liens qui pointent vers des pages inexistantes, c'est-à-dire pages d'erreur 404.

Désormais, lorsque les systèmes de sécurité de Microsoft analysent le lien, ils reçoivent une erreur 404 car le lien n'existait pas à l'origine et Microsoft considérait le lien comme sûr.

Cependant, pour un utilisateur réel, le site de phishing les détecterait et les redirigerait vers une page de phishing réelle au lieu de la page d'erreur 404 standard du serveur.

Le phishing continue d'être un vecteur d'attaque de premier plan pour les cybercriminels. Les individus et les organisations doivent être conscients des techniques de phishing intelligentes pour éviter d'être victimes de vol d'identité, d'escroqueries et de fraudes.

Source *: http://bit.ly/2YX70Sw*

Une faille de sécurité de verrouillage intelligent pourrait laisser votre porte grande ouverte

19 décembre 2019

[…] F-Secure Consulting a découvert la faille de la serrure intelligente KeyWe qui permet aux utilisateurs d'ouvrir et de fermer les portes de leur maison en utilisant une application sur leur smartphone. L'entreprise a découvert qu'ils étaient capables d'exploiter des protocoles de communication mal conçus pour intercepter la phrase secrète envoyée entre le verrou et l'application KeyWe.

Krzysztof Marciniak de F-Secure Consulting a aidé à développer le hack utilisé pour déverrouiller le verrou intelligent et il a fourni un aperçu supplémentaire de la découverte, en disant : « La serrure a plusieurs mécanismes de protection. Malheureusement, la conception du verrou permet de contourner ces mécanismes pour intercepter les messages échangés par le verrou et l'application assez facilement pour les attaquants - le laissant ouvert à une attaque relativement simple. Il n'y a aucun moyen d'atténuer cela, donc accéder aux maisons protégées par la serrure est une valeur sûre pour les cambrioleurs capables de reproduire le piratage. Tous les attaquants ont besoin d'un peu de savoir-faire, d'un appareil pour les aider à capturer le trafic - qui peut être acheté dans de nombreux magasins d'électronique grand public pour aussi peu que 10 dollars - et un peu de temps pour trouver les propriétaires des serrures. »

Les problèmes de sécurité rencontrés par F-Secure dans le verrou intelligent KeyWe sont un autre exemple des défis de sécurité auxquels les fabricants et les consommateurs ont commencé à faire face alors que les appareils IoT ont inondé le marché.

Malheureusement, l'appareil ne peut pas recevoir de mises à jour du micrologiciel. Les propriétaires du KeyWe Smart Lock devront donc remplacer le verrou ou vivre avec le risque qu'un attaquant le pirate pour accéder à leur domicile.

Pour éviter d'être victime de cette attaque ou d'autres attaques similaires, Marciniak recommande aux consommateurs de prendre en compte les implications de sécurité des appareils connectés à Internet avant de remplacer leurs appareils hors ligne par des versions en ligne.

Source : *http://bit.ly/2QjeUBP*

Microsoft n'encourage en aucun cas les victimes de ransomware à payer

16 Décembre 2019

Depuis que les ransomwares sont devenus une menace majeure au milieu des années 2010, les gens se sont disputés sur la bonne façon de faire face à une attaque de ransomware et sur les avantages de payer ou de ne pas payer une demande de rançon.

« Nous n'encourageons jamais une victime de ransomware à payer une forme quelconque de demande de rançon », a déclaré Ola Peters , consultante principale en cyber-sécurité pour Microsoft Detection and Response Team (DART) […].

Cependant, Microsoft comprend que dans de nombreux cas, les organisations n'ont parfois qu'une seule option sur la table - payer la rançon - car elles n'ont pas accès aux sauvegardes récentes, ou le ransomware a également chiffré les sauvegardes.

Mais même si les victimes choisissent de payer la rançon, Microsoft prévient que « payer des cybercriminels pour obtenir une clé de décryptage de ransomware ne garantit pas que vos données cryptées seront restaurées ».

Plus précisément, le fabricant du système d'exploitation recommande aux entreprises de suivre six étapes simples pour se préparer à répondre à une attaque de ransomware, chaque fois que cela se produira :

1. Utilisez une solution de filtrage des e-mails efficace.
2. Correctif régulier des systèmes matériels et logiciels et gestion efficace des vulnérabilités.
3. Utilisez un antivirus à jour et une solution de détection et de réponse des postes (EDR).
4. Séparez les informations d'identification administratives et privilégiées des informations d'identification standard.
5. Mettre en œuvre un programme efficace de mise en liste blanche des applications.
6. Sauvegarder régulièrement les systèmes et fichiers critiques.

Source : *https://zd.net/2QgVNIw*

Evènements

Evènements du mois

CSE Local Hack Day Build 2019

14 décembre 2019, Alger, Algérie

http://bit.ly/2Mo2LKH

CSE Local Hack Day Build 2019 est une journée de renforcement de capacités qui a été animée de la part du Club Scientifique de l'ESI (CSE) et qui a eu lieu le 14 Décembre 2019 à Alger. Cette journée s'est définit par une journée locale de piratage de MLH (Major League Haking). Build Day est un hackathon mondial d'une journée dont il est possible de partager avec sa communauté. Les participants ont pu donner de la vie à leurs idées afin de construire de nouveaux projets. Des ateliers et des discussions avec une communauté mondiale ont eu lieu dans cet événement. Pendant une durée de 12 Heures, les participants ont utilisés du matériel et des logiciels afin de créer des sites web, des applications mobiles, des robots etc. C'est un événement qui a concerné l'ensemble des niveaux de compétences, en partant des débutants jusqu'aux développeurs les plus expérimentés. Les participants de l'atelier ont appris des compétences dont ils seront capables d'appliquer dans leurs projets, leur travail ou encore leurs travaux scolaires etc.

Hack-it-N 2019

10 décembre 2019, Bordeaux, France

https://www.hack-it-n.com/

Une conférence de cybersécurité a été organisée par la société TEHTRIS, experte en cybersécurité. Le programme a inclut des tables rondes sur les enjeux de la cybersécurité dans les technologies et les entreprises, des retours d'expérience à travers des présentations.

Nous citons : AIS GSM Tracking, Entraînement à la cybersécurité, OWASP Mobile Security Testing Guide, Active Directory : Hack-it & Harden-it, Security Operating Center en entreprise

Reference	ANPT-2019-BV-08
Titre	Bulletin de veille N°8
Date de version	31 Décembre 2019
Contact	ssi@anpt.dz