BULLETIN DE VEILLE N°4

ANPT-2020-BV-04

« La confidentialité n'est pas une option, et ce ne devrait pas être le prix que nous acceptons pour simplement accéder à Internet. » -Gary Kovacs-

Avril 2020

Alertes de sécurité

Appel

Safari : une faille sur iPhone et Mac permet de pirater votre webcam

07 avril 2020

Une vulnérabilité critique dans Safari a récemment été découverte par un chercheur en sécurité nommé Ryan Pickren. Quand un utilisateur donne l'accord à un site web d'accéder à la CAM et au micro de son Mac ou de son iPhone, Safari conserve les paramètres pour ne pas demander à chaque fois une autre autorisation. C'est là que la vulnérabilité a été identifiée. Le pirate, en s'aidant d'un code malveillant, arrive à tromper Safari. D'après Ryan Pickren, il est possible d'exploiter la faille dans la création d'une confusion, rendant le site malveillant semblable à une autre plateforme de vidéoconférence connue, telle que Skype par exemple. Cette vulnérabilité dans Safari permet un lancement discret d'un logiciel d'infiltration de CAM dans le but d'enregistrer des conversations ou encore prendre des photos et des partages d'écrans.

Apple a publié un patch en Janvier et en Mars 2020 sur macOS et iOS. Pour les utilisateurs qui disposent de la dernière mise à jour de Safari sur leur Mac ou leur iPhone, ils n'ont rien à craindre. Il faudrait alors s'assurer que Safari est à jour sur votre appareil Apple.

Source *: https://bit.ly/3cZXKm7*

Deux vulnérabilités zero-day dans Apple Mail

22 avril 2020

Des chercheurs en sécurité ont découvert deux vulnérabilités zero-day dans l'application Mail pour iPhone et iPad. Après une enquête approfondie, ils ont trouvé des preuves d'attaques ciblées, qu'ils ont décrites dans un rapport publié. Les vulnérabilités permettent à un attaquant d'exécuter du code à distance en exploitant les processus MobileMail et Mailid d'Apple dans iOS 12 et iOS 13, respectivement, grâce à l'utilisation d'un courrier électronique spécialement conçu. Et, s'il était déclenché correctement, un utilisateur ne saurait pas qu'il était piraté.

ZecOps a déclaré avoir alerté Apple des vulnérabilités en février. Les deux failles ont depuis été corrigées dans les dernières versions bêta d'iOS 13, et un correctif devrait arriver dans la prochaine mise à jour iOS (iOS et iPadOS 13.4.5).

Source *: https://bit.ly/2KEQe45*

Microsoft

Une vulnérabilité permet le détournement de compte Microsoft Teams avec un GIF

27 avril 2020

Les chercheurs de CyberArk auraient identifié une vulnérabilité de type ver dans Microsoft Teams, que les pirates pourraient exploiter pour hacker des comptes MS Teams en envoyant des URL malveillantes ou des images GIF aux utilisateurs de Teams. La vulnérabilité est liée à la façon dont MS Teams traite les jetons d'accès d'authentification et les transmet aux ressources contenant des images. Si un attaquant parvient à créer un fichier GIF ou une URL, Teams enverra le jeton d'authentification au serveur de l'attaquant lors de son traitement. Pour réussir l'attaque via l'envoi de liens, la victime doit cliquer sur le lien ; mais dans le cas d'une image GIF, l'attaque peut réussir si l'utilisateur affiche l'image dans le chat Teams. Une fois l'image affichée ou l'URL cliquée, l'attaquant reçoit le jeton. À l'aide de ce jeton, un attaquant peut pirater le compte Teams de la victime en exploitant ses interfaces API et peut accéder aux données de la victime sur Teams, envoyer des messages, créer et supprimer des groupes au nom de la victime ou modifier les autorisations d'un groupe.

CyberArk a publié un article de blog détaillé sur la vulnérabilité, accessible ici . Selon Microsoft la faille a été corrigée.

Source *: https://bit.ly/2KFx1Q0*

Microsoft Advisory met en garde contre les vulnérabilités affectant Office

27 avril 2020

Microsoft a publié un avertissement de plusieurs vulnérabilités dans la bibliothèque Autodesk FBX (FilmBox), qui est intégrée dans certains logiciels, y compris les nouvelles versions de Microsoft Office.

Les failles existent dans le Kit de développement logiciel FBX d'Autodesk, qui est pris en charge dans Microsoft Office 2019 et Office 365 ProPlus.

Selon Sophos, ces vulnérabilités sont dues à plusieurs types d'erreurs de programmation différentes (débordement de tampon, confusion de type, utilisation après libération, débordement d'entier et déréférence de pointeur nul).

Les dernières versions d'Office sont exposées à six vulnérabilités décrites dans un avis Autodesk annonçant des correctifs pour CVE-2020-7080 à CVE-2020-7085. Pour plus de détails veuillez consulter l'avis complet de Microsoft ici

Source : *https://bit.ly/3aIcTXN*

Microsoft fait face à 4 bugs sous un exploit actif dans le Patch Tuesday d'Avril

14 avril 2020

Microsoft a publié 113 correctifs dans une mise à jour importante. Microsoft a déclaré que 4 de ces failles sont activement exploitées et deux de ces dernières ont déjà été rendues publics.

Parmi les principales vulnérabilités corrigées par Microsoft est CVE-2020-0968. Celle-ci est une faille de corruption de mémoire de niveau critique sur Internet Explorer, ayant été exploitée dans la nature. D'après les explications de Threatpost Satnam Narang, un ingénieur principal de recherche chez Tenable, de nombreux scénarios d'exploitation de cette vulnérabilité existent […]. Un pirate peut inciter l'utilisateur par ingénierie sociale à se diriger vers un site web qui contient du code malveillant appartenant au pirate ou encore un site web compromis avec le code malveillant injecté.

Deux des bugs activement exploités constituent des problèmes RCE (Remote Code Execution) majeurs pour la bibliothèque Windows Adobe Type Manager. La première faille est CVE-2020-1020 qui a déjà été rendue public. La faille est causée par la mauvaise gérance de la police multi-maître (format PostScript Adobe Type 1) par la bibliothèque. D'après Dustin Childs, avec ZDI (Zero Day Initiative), les pirates ont la possibilité d'utiliser ce bug dans l'exécution du code sur les systèmes affectés s'ils arrivent à persuader l'utilisateur de visualiser une police spécialement conçue.

La seconde vulnérabilité est CVE-2020-0938. C'est une faille RCE affectant le rendu de police OpenType dans Windows. Là aussi, le pirate aurait la possibilité d'exécuter du code sur un système ciblé dans le cas où l'utilisateur visualise la police spécialement conçue.

Les détails sur les autres bugs sont disponibles ici.

Source : *https://bit.ly/35fGOFz*

Une vulnérabilité de PowerPoint permet une cyberattaque par survol de la souris

Un chercheur en cyber sécurité, nommé Mandar Satam, tire la sonnette d'alarme sur un éventuel nouveau vecteur d'attaque qui permet à un attaquant de manipuler un fichier PowerPoint pour télécharger et installer un logiciel malveillant, simplement en survolant un lien hypertexte. Cette technique exigerait que la victime accepte une boite de dialogue contextuelle pour l'exécution ou l'installation d'un programme.

Selon ce chercheur, une éventuelle attaque risquerait le contournement de la restriction de PowerPoint qui consiste à ne pas pouvoir ajouter un fichier distant à l'action HyperLink. Il a également déclaré que le pirate aura la possibilité de manipuler le texte de la boite de dialogue qui contient le nom du fichier, et ceci dans le but d'afficher d'autres textes tels que "Windows Update.bat" ou "Chargement... Please Wait.exe".

D'après un porte-parole de Microsoft, les clients doivent adopter de bonnes mesures et pratiques de cyber sécurité, et rester vigilants avant de cliquer sur des liens qui mènent vers des pages Web, permettant d'ouvrir des fichiers inconnus ou accepter des transferts de fichiers.

Le chercheur a créé une attaque de preuve de concept dont les détails techniques sont disponibles ici.

Source : *https://bit.ly/2SdqyEn*

Firefox

Mozilla : correction de deux vulnérabilités zero-day dans Firefox

14 avril 2020

Des correctifs pour deux failles critiques, largement exploitées sur internet, ont été apportés dans la dernière version de Firefox.

Les navigateurs concernés sont Firefox 74.0.1 et Firefox ESR 68.6.1. Une alerte a été publiée par US Cybersecurity and Infrastructure Security Agency (CISA) encourageant les administrateurs ainsi que les utilisateurs à appliquer les correctifs nécessaires partagés sur l'avis. Les pirates ont exploité les failles CVE-2020-6819 et CVE-2020-6820 lors d'attaques ciblées. Ces dernières risqueraient de provoquer une faille de type corruption de la mémoire que les pirates peuvent utiliser dans l'exécution de code arbitraire ou encore pour activer les capacités d'exécution de code à distance.

Mozilla n'a pas fourni de détails sur la façon dont les attaquants exploitent ces failles ou sur leurs cibles. Pour plus de détails, veuillez consulter l'avis complet ici.

Source : *https://bit.ly/3f1bMPh*

WordPress

Bug du plugin WordPress permet aux pirates de créer des comptes administrateur

27 avril 2020

Il est conseillé aux propriétaires de WordPress de sécuriser leurs sites Web en mettant à jour le plug-in « real time find and replace » pour empêcher les attaquants d'injecter du code

malveillant dans leurs sites et de créer des comptes administrateur en exploitant une faille Stored XSS. Le plugin WordPress real time find and replace est installé sur plus de 100000 sites et permet aux utilisateurs de remplacer temporairement le texte et le contenu de code sur leurs sites en temps réel sans avoir à entrer dans le code source des sites et à apporter des modifications permanentes.

La vulnérabilité affecte toutes les versions de *real time find and replace* jusqu'à 3.9. Un attaquant peut profiter des fonctionnalités du plugin pour remplacer tout contenu sur un site ciblé par du code malveillant, comme détaillé dans un rapport publié aujourd'hui par l'analyste de menace Wordfence Chloe Chamberland.

Malheureusement, malgré la réponse rapide du développeur et la disponibilité du correctif de sécurité au cours des cinq derniers jours, un peu plus de 27000 de tous les utilisateurs ont mis à jour leurs installations du plugin vers 4.0.2 - la dernière version sans bug.

Source : *https://bit.ly/2KFZJzU*

OpenSSL

OpenSSL corrige une vulnérabilité DoS

21 avril 2020

OpenSSL a publié une mise à jour de sécurité pour OpenSSL qui corrige une vulnérabilité de haute gravité, identifiée comme CVE-2020-1967, qui peut être exploitée par des attaquants pour lancer des attaques par déni de service (DoS).

La vulnérabilité affecte les versions OpenSSL 1.1.1d, 1.1.1e et 1.1.1f, et elle a été corrigée avec la version 1.1.1g.

L'organisation a souligné que les anciennes versions 1.0.2 et 1.1.0 ne sont pas affectées par la vulnérabilité, mais ces versions ne sont plus prises en charge et ne reçoivent plus de mises à jour. Les utilisateurs de ces versions doivent passer à OpenSSL 1.1.1.

Source : *https://bit.ly/2KwiNR3*

IBM

Un chercheur dévoile 4 bugs Zero-Day dans le logiciel de sécurité d'entreprise d'IBM

21 avril 2020

Un chercheur en cybersécurité a rendu public aujourd'hui les détails techniques et le PoC pour 4 vulnérabilités non corrigées zero-day affectant un logiciel de sécurité d'entreprise proposé par IBM après que la société ait refusé de reconnaître la divulgation soumise de manière responsable.

Le produit premium concerné en question est IBM Data Risk Manager (IDRM) qui a été conçu pour analyser les actifs d'informations commerciales sensibles d'une organisation et déterminer les risques associés.

Le chercheur a publié deux modules *Metasploit* pour le contournement de l'authentification, l'exécution de code à distance et le téléchargement de fichiers arbitraires.

Un porte-parole d'IBM a déclaré à *The Hacker News* qu'une erreur de processus a entraîné une réponse incorrecte au chercheur qui a signalé cette situation à IBM. « Nous avons travaillé sur des étapes d'atténuation et elles seront discutées dans un avis de sécurité qui sera publié. »

Source : *https://bit.ly/3eVCL5L*

Vmware

VMware corrige une vulnérabilité critique

17 avril 2020

Une vulnérabilité critique du produit de gestion vCenter de VMware a permis à un utilisateur du même réseau de créer à distance un compte administrateur, a révélé une étude de Guardicore Labs. La vulnérabilité référencée CVE-2020-3952 , dont les détails étaient disponibles lorsque VMWare a publié un patch la semaine dernière, a été classée par VMware elle-même comme CVSS v3 10.0, le plus haut niveau.

Le fournisseur de virtualisation a publié une note d'information et un correctif le 9 avril expliquant qu'un acteur malveillant ayant un accès réseau au port 389 sur un déploiement vmdir affecté peut être en mesure d'extraire des informations très sensibles telles que les informations d'identification de compte administratif qui pourraient être utilisées pour compromettre vCenter Server ou d'autres services qui dépendent de vmdir pour l'authentification. Différents vecteurs d'attaque tels que la création de nouveaux comptes administratifs contrôlés par des attaquants sont également possibles.

Source : *https://bit.ly/3549FNe*

Réseaux sociaux

Une faille TikTok cause un téléchargement de fausses vidéos vers les comptes utilisateurs

Une faille dans l'application TikTok a été découverte par des développeurs de Mysk Inc permettant le téléchargement de fausses vidéos sur les comptes des utilisateurs. Selon ces développeurs, ce bug existe à cause de la transmission des données de TikTok sur http. Ceci accorde la possibilité aux pirates d'effectuer des attaques MiTM (Man in The Middle) et d'avoir le contrôle sur les vidéos et les photos des utilisateurs.

Selon les chercheurs, TikTok s'est basée sur les réseaux de distribution de contenu CDN pour distribuer des données transmettant les médias via http. Ceci risque de compromettre la confidentialité des utilisateurs. Les données transmises via le protocole non sécurisé peuvent être facilement interceptées par des outils tels que Wireshark.

TikTok n'a pas encore partagé de correctif et l'application utilise encore http sur les plateformes Android et iOS. TikTok pour iOS (VERSION 15.5.6) et TikTok pour Android (version 15.7.4) utilisent toujours http non chiffré pour se connecter au CDN TikTok.

Source : *https://bit.ly/2W1nM1G*

Actualité

Comment le confinement a ouvert la voie aux pirates VPN

20 avril 2020

Le confinement mondial dû à l'épidémie de COVID-19 a contraint les particuliers et les entreprises à utiliser des VPN en grand nombre dans le monde pour protéger les activités de navigation des regards indiscrets sur les connexions Wi-Fi publiques / privées. Un VPN est également requis lorsque quelqu'un essaie d'accéder à des sites géo-restreints. Dans de nombreux pays, les chiffres d'utilisation des VPN ont explosé.

Des chercheurs ont découvert que les groupes de pirates informatiques manipulent les utilisateurs pour télécharger et installer des logiciels malveillants en se faisant passer pour un client VPN légitime. De plus, certains VPN sont simplement une arnaque disponible sur le Chrome Store, Android Play Store ou à d'autres endroits.

Les noms de domaines utilisés par ces faux VPN sont : nordfreevpn[.]com et vpn4test[.]net

La semaine dernière, Google a supprimé de playstore une application VPN Android 'SuperVPN' - téléchargée plus de 100 millions de fois - avec une vulnérabilité critique qui menaçait les utilisateurs d'une attaque MITM.

Source *: https://bit.ly/2y8HYGP*

Les attaques ransomware « Double Extorsion » atteignent leur pic

16 avril 2020

Le procédé du ransomware nommé « double extorsion » a vu le jour vers la fin de l'année 2019 par les opérateurs Maze et plusieurs cybercriminels l'ont utilisé derrière les familles de ransomwares Clop, DopplelPaymer et Sodinokibi.

Selon le responsable du renseignement sur les menaces chez Check Point Research « Lotem Finkelsteen », la double extorsion est une tendance croissante et claire aux cyberattaques de ransomwares. Plusieurs attaques de ce genre ont eu lieu durant le premier trimestre de 2020.

En Novembre 2019, la grande entreprise américaine de personnel de sécurité Allied Universal a été attaquée par un ransomware « double extorsion ». La société n'a pas accepté de payer la rançon de Maze d'une valeur de 300 Bitcoins (2.3 millions de dollars), les pirates ont menacé d'utiliser des données sensibles extraites des systèmes de la société, et plusieurs de ses e-mails et certificats de nom de domaine dans une compagne de spam au nom d'Allied Universal.

Suite à cela, 700 Mo de données ont été divulguée, ainsi que des contacts, des certificats de chiffrement, des dossiers médicaux etc, et les pirates ont demandé une rançon plus élevée que la précédente de 50%.

A présent, les chercheurs déclarent que TA2101, soit le groupe derrière le rançongiciel Maze, a fini par créer une page Web spéciale répertoriant les identités des victimes non coopératives et publiant des échantillons de données volées régulièrement.

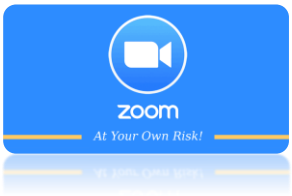
Des experts soulignent que les attaques de « double extorsion » continueront à cibler les victimes de ransomware en cette année 2020, en particulier les hôpitaux qui sont actuellement hautement exposés suite à la pandémie du coronavirus facilitant ainsi le travail des pirates.

Il est recommandé à toutes les institutions de se protéger et de suivre les bonnes pratiques pour éviter et surtout empêcher les attaques de ransomwares, en sauvegardant les fichiers et les données, en formant les employés et en s'assurant d'appliquer les mises à jours nécessaires.

Source *: https://bit.ly/2Yc7InC*

Vous utilisez Zoom ? Voici les risques de confidentialité à surveiller

02 avril 2020



Le coronavirus a provoqué une augmentation de l'activité du travail à domicile, Zoom est rapidement devenu l'application de vidéoconférence de choix. Et avec cette popularité, les risques de confidentialité s'étendent à un plus grand nombre d'utilisateurs. Des fonctionnalités intégrées de suivi de l'attention aux récentes hausses du "Zoom-bombing" (où des participants non invités entrent et perturbent les réunions), les pratiques de sécurité de Zoom attirent davantage l'attention .

Les experts de la confidentialité ont déjà exprimé des préoccupations au sujet de Zoom: en 2019, le logiciel de visioconférence a connu à la fois un scandale de piratage de webcam et un bug qui permettait aux utilisateurs d'espionner et de rejoindre potentiellement des réunions vidéo auxquelles ils n'avaient pas été invités . Ce mois-ci, l'Electronic Frontier Foundation a averti les utilisateurs travaillant à domicile des fonctionnalités de confidentialité intégrées du logiciel.

Plus d'informations sur les problèmes de sécurité de zoom par ici.

Source *: https://cnet.co/3eZqTQw*

Des lecteurs USB malveillants infectent 35000 ordinateurs avec un botnet de crypto-mining

24 avril 2020

Des chercheurs en cybersécurité d'ESET ont déclaré avoir supprimé une partie d'un botnet de logiciels malveillants comprenant au moins 35000 systèmes Windows compromis que les attaquants utilisaient secrètement pour exploiter la crypto-monnaie Monero […].

Le botnet, nommé «VictoryGate», est actif depuis mai 2019, les infections étant principalement signalées en Amérique latine, en particulier au Pérou représentant 90% des appareils compromis. "L'activité principale du botnet est l'exploitation de la crypto-monnaie Monero", a déclaré ESET. " Les victimes comprennent des organisations des secteurs public et privé, y compris des institutions financières."

Selon les chercheurs d'ESET, VictoryGate se propage via des périphériques amovibles tels que des clés USB qui, lorsqu'ils sont connectés à la machine victime, installent une charge utile malveillante dans le système. De plus, le module communique également avec le serveur de commande et de contrôle (serveur C2) pour recevoir une charge utile secondaire.

Source : *https://bit.ly/2S7PBnV*

Fin de support décalée pour des produits Microsoft

Microsoft a annoncé le report de nombreuses dates de fin de support de quelques produits, et ceci pour faciliter la tâche des administrateurs systèmes durant cette période de pandémie. Les utilisateurs pourront donc toujours recouvrir à ces versions.

Dans le but de simplifier la tâche à ses clients et de limiter les opérations de migration ainsi que les mises à jour des produits, complexe en ces temps suite au télétravail imposé par la pandémie, Microsoft a déclaré retarder la date de fin de support de quelques produits. Tous les changements se résument sur une page spéciale de support que Microsoft a publié.

Les divers produits affectés par ces changements sont mentionnés ici. Selon Microsoft, les changements ne devront pas affecter le reste des produits ainsi que les autres versions. L'entreprise précise également qu'au vue de cette situation, elle se réserve le droit d'apporter des modifications et des mises à jour des informations en rapport avec la fin de support des applications.

Source : *https://bit.ly/2SikhCT*

La suppression de 49 extensions malveillantes de cryptomonnaie par Google

10 avril 2020

49 extensions de cryptomonnaie ont été retirées du Chrome Web Store par Google étant donné qu'elles contenaient du code malveillant volant des mots de passe, des clés privées ainsi que d'autres informations qui permettent des attaques de force brute.

Happy Denley, qui est le directeur de la sécurité de la plateforme MyCrypto, est celui qui a découvert ces extensions malveillantes. D'après ce directeur, ces extensions malveillantes ont été placées par la même personne ou le même groupe basé en Russie.

Les extensions malveillantes avaient un fonctionnement similaire à celui des extensions légitimes. Mais l'ensemble des données saisies par la victime pendant les procédures de configuration étaient envoyées aux serveurs des pirates, ou bien à un formulaire Google. Ce qui est dommage, c'est que les victimes ne peuvent pas récupérer les fonds volés à cause de la nature de la majorité des crypto-monnaies. Il faut néanmoins être prudent, car le pirate n'a pas encore été trouvé et d'autres extensions malveillantes pourraient apparaitre sur le Chrome Web Store.

Source : *https://bit.ly/3eWY5rD*

Les sociétés pétrolières et gazières ciblées par des attaques de ransomware et d'exploitation de vulnérabilité

27 avril 2020

Deux campagnes de spear-phishing différentes ont été lancées entre le 31 mars et le 12 avril 2020, fournissant le cheval de Troie de spyware "Agent Tesla".

La première campagne a utilisé des spams se faisant passer pour la compagnie pétrolière d'État égyptienne Enppi, ciblant des organisations aux États-Unis, en Malaisie, en Iran, en Afrique du Sud, à Oman et en Turquie.

La deuxième campagne a utilisé des courriers électroniques indésirables provenant d'une société de transport maritime et a exploité des informations légitimes sur un pétrolier / chimiste pour cibler des organisations aux Philippines.

Selon un rapport de Bitdefender, depuis octobre 2019, les cyberattaques sur le secteur de l'énergie, et en particulier le pétrole et le gaz, augmentent régulièrement sur une base mensuelle […].

Ces attaques avaient des caractéristiques particulières telles que :

- Habituellement, les cyberattaquants préfèrent cibler les vulnérabilités des systèmes de contrôle industriels (ICS) ou d'autres applications matérielles ou logicielles, comme cela s'est produit dans le cas d'APT41.
- Les attaques impliquant l'agent Tesla ont été menées via des e-mails de spearphishing.
- Pendant l'ère épidémique de COVID-19, les sociétés pétrolières et gazières sont obligées de passer à une connectivité d'accès à distance pour maintenir leurs opérations.

Le 5 Avril, la grande société algérienne d'hydrocarbures Sonatrach a aussi été victime d'une attaque par le fameux groupe de ransomware nommé Maze, qui a ciblé plusieurs dizaines de sociétés dans le monde. Suite à cette attaque, plusieurs données sensibles ont été cryptées sur les serveurs de la compagnie et d'autres ont été dérobées afin d'extorquer de l'argent à la compagnie algérienne. Les détails sont disponibles dans l'article publié sur l'application News NATP installable depuis play store ;

Source : https://bit.ly/3bHi0sF

Evènements

Evènement du mois

Cisco Live Virtual Event APJC

1-2 Avril 2020

https://bit.ly/35j7Z2i

Un événement d'apprentissage en ligne s'est déroulé en deux jours. Des conférences ainsi que plus de 25 sessions techniques et démonstrations de solutions ont été présentées sur les dernières innovations technologiques de Cisco, proposées par des experts mondiaux de Cisco dans les domaines de la mise en réseau, de la cybersécurité, du centre de données, de la collaboration, du fournisseur de services et bien plus.

Fortinet Webinaries

https://bit.ly/2zHGy6F

Plusieurs webinaries ont été organisés en ce mois par Fortinet traitant des solutions de sécurité réseau, de sécurité web, d'authentification, de sécurité de la messagerie, de la protection contre les ransomware...etc. Une gamme de produits et de services dédiés à la sécurité des sites distants et à la protection de la périphérie réseau.

Infos ANPT

Durant la crise sanitaire provoquée par la pandémie du covid-19, plusieurs Startups en partenariat avec l'Agence Nationale de Promotion et de Développement des Parcs Technologiques -ANPT- se sont mobilisées pour contribuer à la lutte contre la propagation du virus et l'accompagnement des citoyens dans leur confinement instauré par l'état et cela à travers le développement de différentes solutions technologiques dont :

La Startup @MadrassaNet publie des cours en ligne pour les différentes classes d'examens.

Une nouvelle version d'E-Tabib intégrant des services de téléconsultation disponibles gratuitement pour les médecins et les patients.

La Startup Golden a lancé une application COVINFO pour la sensibilisation et la prévention du Coronavirus COVID- 19.

La Startup TECHGRAPH a mis en place un système baptisé COROVID RESCUE dont le but est de constituer une base de données au niveau du Ministère de la Santé pour identifier les citoyens atteints et suspects à l'aide d'un QR Code.

Plusieurs conférences Live ont aussi été diffusées sur le Développement Personnel, le Management et le Leadership.

Diffusion d'une compagne de sensibilisation sur le « *phishing* ».

Une compagne de vulgarisation/sensibilisation sur les différents types de malwares

https://bit.ly/2SnpRno

Reference	ANPT-2020-BV-04
Titre	Bulletin de veille N°4
Date de version	30 avril 2020
Contact	ssi@anpt.dz