
# BULLETIN DE VEILLE N°4

ANPT-2019-BV-04

*« Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication » -James Scott*

Août 2019

# Alertes de sécurité

## Smartphone

### Un nouveau ransomware est en train de se propager par SMS

01 août 2019

Les chercheurs de l'entreprise ESET ont découvert un nouveau ransomware baptisé ***Android/Filecoder.c.*** Il a pour principale particularité de se diffuser par SMS et ne cible pour le moment que les systèmes Android.

D'après les chercheurs d'ESET, la principale originalité de ce ransomware viendrait de son mode de diffusion. En effet, une fois le terminal infecté, ce dernier s'arrangerait pour récupérer le contenu du carnet d'adresses de l'utilisateur afin de s'envoyer lui-même aux contacts stockés dedans. Les utilisateurs recevraient alors des SMS génériques contenant des liens malveillants, des liens pointant directement vers le programme d'installation du malware.

Il est recommandé de mettre à jour le système d'exploitation Android et de ne pas télécharger des fichiers APK en dehors des boutiques officielles. Il est aussi recommandé de ne pas cliquer sur les liens suspects envoyés par SMS.

***Source :*** *http://bit.ly/30BWYpK*

### Failles critiques dans des Antivirus sous Android

02 août 2019

Lors de récents tests, un grand nombre d'applications antivirus Android gratuites populaires ont révélé des failles de sécurité et des problèmes de confidentialité - y compris une vulnérabilité critique qui expose les carnets d'adresses des utilisateurs, et une autre faille grave qui permet aux attaquants de désactiver complètement la protection antivirus. […] parmi ces produits, AEGISLAB, BullGuard, dfndr et VIPRE.

Les utilisateurs de VIPRE sont exposés à une faille critique permettant la récupération des contacts y compris les noms complets, photos et informations personnelles sensibles et cela lors de la synchronisation automatique. […] la faille est causée par une mauvaise implémentation de la procédure de contrôle pendant la synchronisation sur cloud. […] Une autre faille critique permet à un attaquant d'envoyer des alertes frauduleuses en capturant la requête générée lorsqu'un virus est détecté puis en modifiant l'ID de l'utilisateur et autres paramètres.

L'application BullGuard mettait ces utilisateurs vulnérables à un attaquant désactivant la protection antivirus à distance de plus d'une faille de type XSS pouvant être exploitée pour détourner des sessions, collecter des données personnelles ou utiliser le site Web comme plate-forme pour des campagnes de phishing. […]

L'utilisateurs du tableau de bord de AEGISLAB risquaient d'être victimes d'une grave faille XSS permettant l'exécution de code malveillant à travers plusieurs paramètres d'entré non contrôlés.

Les fournisseurs ont mis à jour leurs produits pour corriger ces failles. Il est recommandé de les appliquer.

D'autre antivirus pour mobile n'ont pas réussi à détecter des virus basics lors des tests. Parmi ces applications : AEGISLAB Antivirus Free, Antiy AVL Pro Antivirus & Security, Brainiacs Antivirus System, Fotoable Super Cleaner, MalwareFox Anti-Malware, NQ Mobile Security & Antivirus Free, Tap Technology Antivirus Mobile, et Zemana Antivirus & Security […].

Concernant l'aspect « protection de la vie privée », de nombreuses applications gratuites affichent des publicités ciblées. […] Selon l'analyse réalisée, dfndr était le pire en terme de trackers publicitaires. […] il demande notamment la permission d'accéder, de lire, et d'écrire des contacts, de consulter le carnet d'adresse et de saisir l'identifiant unique et le numéro de téléphone de l'appareil.

Il est recommandé de vérifier les permissions demandées par toute application avant l'installation en refusant en cas de permissions suspects.

***Source :*** *https://threatpost.com/critical-bug-android-antivirus/146927/*

## Bluetooth

### Une faille Bluetooth critique expose des millions d'appareils à des attaques d'écoute clandestine

16 août 2019

Une nouvelle vulnérabilité divulguée (CVE-2019-9506) dans les paramètres du noyau de Bluetooth peut être exploitée pour intercepter et manipuler des communication/trafic Bluetooth entre deux périphériques vulnérables.

La faille affecte la procédure/protocole de négociation des clés d'encryptions. Les détails concernant l'attaque sont décrits sur cet article.

Des tests ont été réalisés sur des puces de différents fabricants tels que Intel, Broadcom, Appl et Qualcomm et ont été toutes vulnérables. Selon les chercheurs, tout appareil Bluetooth conforme aux normes est vulnérable.

Cependant, afin que l'attaque réussisse, les conditions suivantes doivent être réunies :

- L'attaquant doit être physiquement à proximité du ou des dispositifs visés
- Ne peut être menée que lors de la négociation d'une connexion entre des appareils jumelés. Les sessions existantes ne peuvent pas être attaquées
- Elle est conditionnée dans une fenêtre temporelle étroite
- Les deux dispositifs doivent être vulnérables pour que l'attaque fonctionne

Microsoft a publié les correctifs dans le cadre des « mise à jour du mardi » du mois d'août 2019.

Cisco a découvert plusieurs dispositifs affectés, les correctifs sont en cours.

Apple a corrigé la faille dans les mises à jours de sécurité de juillet pour iOS, mcOS, tvOS and watchOS. Blackberry, Johnson Controls, Lenovo et Intel ont publié des avis à ce sujet.

A10 Networks, Juniper, Oracle et VMWare ne sont pas impactés.

***Source*** : *https://www.helpnetsecurity.com/2019/08/16/bluetooth-cve-2019-9506/*

## Intel

### Une vulnérabilité dans l'Utilitaire d'identification des processeurs Intel® pour Windows

13 août 2019

Une vulnérabilité de sévérité moyenne, référencée CVE-2019-11163, dans l'utilitaire Intel® Processor Identification Utility, en ses version antérieur à 6.1.0731, pour Windows peut entraîner une élévation de privilèges, un déni de service ou une divulgation d'informations.

Des mises à jour ont été publiées sur le site officiel de Intel pour corriger ces vulnérabilités.

***Source :*** *https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00281.html*

## Cisco

### Cisco corrige six bugs critiques dans les équipements et les commutateurs UCS

22 août 2019

Cisco Systems met en garde contre six vulnérabilités critiques affectant un large éventail de ses produits, notamment sa gamme de serveurs Unified Computing System et ses commutateurs intelligents de la série 220 pour petites entreprises. Dans toutes les instances de vulnérabilités, un attaquant distant non authentifié pourrait prendre le contrôle du matériel ciblé.

Quatre bugs critiques ( CVE-2019-1938 , CVE-2019-1935 , CVE-2019-1974 et CVE-2019-1937) affectent les composants du système d'informatique unifiée (UCS) de Cisco. Chacun a un indice de gravité critique et un score CVSS de 9,8.

Et deux bogues d'exécution de code à distance affectant les commutateurs intelligents de la série 220 pour petite entreprise. Dans les deux cas, un attaquant distant non authentifié peut provoquer un dépassement de mémoire tampon et exécuter du code arbitraire pour prendre le contrôle du système d'exploitation du commutateur.

Le code d'exploitation public pour les deux bogues critiques (CVE-2019-1913 et CVE-2019-1912 ) est disponible en ligne, mais aucun incident n'a été signalé.

***Source :*** *https://threatpost.com/cisco-patches-six-critical-bugs/147585/*

## Lenovo

### Vulnérabilité critique dans Lenovo Solution Center

23 août 2019

Une vulnérabilité a été signalée dans le logiciel LSC (Lenovo Solution Center) préinstallé sur les PC d'ancien modèles. La vulnérabilité est une faille d'escale de privilèges qui peut être utilisée pour exécuter du code arbitraire sur un système ciblé, recouvrant des privilèges de niveau Administrateur ou SYSTEM. La version affectée, v. 03.12.003, n'est plus supportée depuis novembre 2018 (officiellement déclarée End Of Life) mais elle est toujours présente en téléchargement sur le site officiel.

Lenovo a publié un bulletin de sécurité concernant ce bogue et a recommandé aux utilisateurs de passer à un utilitaire similaire appelé Lenovo Vantage.

***Source :*** *https://threatpost.com/bug-found-in-pre-installed-software/147657/*

## Microsoft

### Corruption mémoire sur serveur DHCP sous Microsoft Windows Server 2008 SP2

14 août 2019

Une vulnérabilité classée critique, identifiée par CVE-2019-1213, a été découverte dans Microsoft Windows Serveur 2008 SP2. Un attaquant peut exploiter cette vulnérabilité en envoyant un paquet modifié au serveur DHCP lui permettant d'exécuter du code arbitraire à distance.

Il est recommandé de mettre à jour le système qui corrige cette vulnérabilité en modifiant la manière dont les paquets réseaux sont traités.

***Source*** : *https://vuldb.com/?id.139905*

### Multiples vulnérabilités dans Microsoft Remote Desktop Services

14 août 2019

Lors de la publication mensuelle de ses correctifs, Microsoft a corrigé plusieurs vulnérabilités affectant les services de bureau à distance (Remote Desktop Services, RDS). Parmi les failles corrigées, quatre d'entre elles, critiques, permettent une exécution de code arbitraire à distance. Selon l'éditeur, elles touchent les systèmes Windows 7 SP1, Server 2008 R2 SP1, Server 2012, Windows 8.1, Server 2012 R2 ainsi que toutes les versions supportées de Windows 10, cela incluant les versions serveur.

Ces vulnérabilités identifiées comme CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 et CVE-2019-1226 peuvent être exploitées sans authentification et sont considérées comme étant d'une criticité similaire à la faille CVE-2019-0708 corrigée au mois de mai par l'éditeur.

Microsoft a également publié un article de blogue revenant sur deux de ces failles, CVE-2019-1181 et CVE-2019-1182. Celui-ci incite les utilisateurs à mettre à jour leurs systèmes dans les plus brefs délais et met en garde contre le risque d'utilisation de ce type de vulnérabilité dans la propagation de malware.

***Source :*** *https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-012/*

### Elévation de privilège dans Windows

13 août 2019

Une vulnérabilité de type élévation de privilèges, référencée CVE-2019-1190 a été publiée par Microsoft. Un attaquant peut exploiter avec succès la vulnérabilité présente dans la manière dont le noyau de Windows gère les objets en mémoire et pourrai exécuter du code avec des permissions élevées.

Pour exploiter la vulnérabilité, un attaquant authentifié localement pourrait exécuter une application spécialement conçue à cet effet.

Les systèmes affectés sont Windows 10 et serveur 2019 dont les versions sont listées dans le bulletin officiel.

Il est recommandé d'appliquer les mises à jours correctives de cette vulnérabilité, disponibles sur le lien du bulletin.

***Source*** : *https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1190*

### Microsoft corrige 93 failles de sécurité dans sa mise à jour du Mardi, aout 2019

13 août 2019

Microsoft a publié son récapitulatif mensuel des mises à jour de sécurité connu sous le nom de Patch Tuesday.

Ce mois-ci, Microsoft a corrigé 93 failles de sécurité, dont 29 classées critiques et 64 classées importantes, et a publié deux avis de sécurité avec des mesures d'atténuation pour deux problèmes de sécurité touchant les produits et services de l'entreprise.

La mise à jour comprend des correctifs pour plusieurs failles permettant l'exécution de code à distance, notamment celle du composant Remote Desktop Service (RDS), celle incluse dans Ms Edge, deux failles présentes dans Hyper-V, six autres dans Ms Graphics, une dans Outlook, deux affectant Ms Word, deux dans le client DHCP de Windows, deux dans le vieux composant Scripting Engine et un dans le moteur VBScript.

Les mises à jour d'autres produit ont été aussi inclus dans le récapitulatif, notamment celles d'Adobe, de VMware et de SAP

A l'occasion, Microsoft a rappelé aux utilisateurs de Windows 7 et serveur 2008 R2 que ces produits ne seront plus pris en charge et ne recevront plus de mise à jour à partir du 14 janvier 2020.

***Source :*** *https://zd.net/2ZvktU7 ;*
***Détails CVE et correctifs :*** *http://bit.ly/2PggM0A*

## Kaspersky

### Vulnérabilité dans les produits Kaspersky

16 août 2019

Une vulnérabilité a été découverte dans les produits Kaspersky permettant à un attaquant de provoquer une atteinte à la confidentialité des données et une injection de code à distance (XSS).

Les produits affectés sont : Anti-Virus 2019, Internet Security 2019, Total Security 2019, Kaspersky Free Anti-Virus 2019, Small Office Security 6.

Un patch a été publié pour corriger cette vulnérabilité. Il est recommandé de l'appliquer dans les plus brefs délais.

***Source :*** *https://support.kaspersky.com/general/vulnerability.aspx?el=12430#160819*

## Adobe

### Multiples vulnérabilités dans les produits Adobe

08 août 2019

De multiples vulnérabilités ont été découvertes dans Adobe Acrobat, Adobe Reader et Adobe Photoshop CC. L'exploitation réussie de la plus grave de ces vulnérabilités pourrait permettre à un attaquant de prendre le contrôle du système affecté. Selon les privilèges associés à l'utilisateur, l'attaquant pourrait installer des programmes, afficher, modifier ou supprimer des données, ou créer de nouveaux comptes avec tous les droits d'utilisateur. Si cette application a été configurée pour avoir moins de droits d'utilisateur sur le système, l'exploitation pourrait avoir moins d'impact que si elle était configurée avec des droits administratifs.

Les versions affectées listées dans les bulletins officiels.

Il est recommandé de mettre à jour les applications et de s'assurer des droits minimaux accordés pour leur lancement.

***Source :*** *http://bit.ly/2U8arTT*

## VLC

### Multiples vulnérabilités découvertes dans VLC media player

19 août 2019

Plusieurs vulnérabilités ont été publiées et corrigées dans VLC Media Player en sa version 3.0.7.1 et antérieur.

L'exploitation de ces failles permet à un attaquant de provoquer un déni de service ou d'exécuter du code malveillant à distance avec les droits d'utilisateur cible.

Ces vulnérabilités listées dans le bulletin sur le site officiel peuvent être exploitées simplement en ouvrant un fichier vidéo (.MKV) malveillant.

Il est recommandé de mettre à jour le logiciel à la version 3.0.8 en restant vigilant sur la source des vidéos ouvertes.

***Source :*** *https://www.videolan.org/security/sb-vlc308.html*

## Linux /Unix

### Une backdoor dans Webmin pendant plus d'un an

10 août 2019

Une vulnérabilité critique (CVE-2019-15107) a été découverte dans Webmin, l'interface web open source pour la gestion des systèmes Linux et UNIX. Elle a été publiée lors de la conférence internationale Defcon qui s'est tenue du 9 au 11 août 2019 à las vegas, US.

La faille de sécurité réside dans la page de réinitialisation du mot de passe et permet à un attaquant distant non authentifié d'exécuter des commandes arbitraires avec des privilèges root sur les serveurs affectés simplement en ajoutant une commande pipe ("|") dans l'ancien champ du mot de passe via des requêtes POST.

Les responsables du projet ont révélé que la faille n'était pas le résultat d'une erreur de codage commise par les programmeurs mais le résultat d'un pirate inconnu qui a réussi à injecter la backdoor dans le build du projet et qui a persisté pendant plus d'un an (versions 1.882 à 1.921).

Un exploit a été publié lors de la même conférence avec une démonstration en direct.

Il est recommandé de mettre à jour l'application et de vérifier sa configuration par défaut.

***Source :*** *https://thehackernews.com/2019/08/webmin-vulnerability-hacking.html ;*
***Exploit :*** *http://bit.ly/2NAUi8n*

## Libreoffice

### Multiples vulnérabilités dans LibreOffice

16 Août 2019

De multiples vulnérabilités ont été découvertes dans LibreOffice. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité. Les vulnérabilités sont référencées : CVE-2019-9850, CVE-2019-9851, CVE-2019-9852.

Les versions antérieures à 6.2.6 et 6.3.0 sont affectées.

Il est recommandé d'appliquer les correctifs mentionnés dans les bulletins de l'éditeur.

***Source :*** *https://www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-401/*

## PHP

### Multiples vulnérabilités dans PHP

02 août 2019

De multiples vulnérabilités ont été découvertes dans PHP (CVE-2019-11041, CVE-2019-11042) dont l'exploitation réussie de peut permettre à un attaquant d'exécuter du code arbitraire, selon les privilèges associés à l'application. L'échec de l'exploitation pourrait entraîner un déni de service.

Les versions affectées sont : PHP 7.1 antérieur à 7.1.31, PHP 7.2 antérieur à 7.2.21 et PHP 7.3 antérieur à 7.3.8

Il est recommandé de mettre à jour l'application à sa dernière version et d'appliquer le principe du moindre privilège pour les utilisateurs ainsi que les applications en exécution.

***Source :*** *http://bit.ly/2Hw0pqG*

# Actualité

### Google : mots de passe hackés toujours en utilisation

16 août 2019


Google a publié les résultats d'une étude à grande échelle sur les habitudes en matière de mots de passe qui montre pourquoi les pirates utilisent des attaques par mot de passe sur les comptes en ligne : de nombreux utilisateurs restent avec le même mot de passe, même lorsqu'ils sont avertis que celui-ci a été compromis.

Le « password Spraying » est une technique de brute force de mots de passe qui consiste à rassembler un grand nombre de noms d'utilisateurs de comptes et tenter de s'authentifier avec un nombre restreint des pires mots de passe [..] cette méthode a été utilisée pour pirater la société Tech Citrix et voler 6To d'information.

Les chercheurs de Microsoft ont révélé que les cinq principaux éléments utilisés dans l'attaque sont : 123456, password, 00000000, 1qaz2wsx et a123456.

Les données de Google sur les habitudes en matière de mots de passe proviennent de son étude sur chacun des 670 000 utilisateurs de Chrome qui ont installé son extension Password Checkup.

Quant à la façon dont les utilisateurs réagissent aux alertes de violation de mot de passe, l'étude a donné des résultats mitigés. Google a constaté que 25,7 % de ses alertes, totalisant 81 368, n'ont pas déclenché un changement de mot de passe de la part des utilisateurs. Cependant, il a également constaté que 26,1 % des alertes, totalisant 82 761, ont donné lieu à un changement de mot de passe.

Les changements de mots de passe qui en résultent sont mixtes, mais ils ont conduit à un mot de passe plus fort [..] 94 % des nouveaux mots de passe sont au moins plus forts que les anciens, même si une grande partie est encore devinable.

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

### Android va corriger près de 200 failles de Sécurité

26 Août 2019

Android 10 (anciennement Android Q) sera l'occasion pour Google de corriger pas moins de 193 failles de sécurité qui sont répertoriées dans le dernier bulletin de sécurité d'Android Open Source Project (AOSP). Toutes ces failles de sécurité, dont la gravité est qualifiée de « modérée », vont de l'élévation des privilèges, en passant par l'exécution du code à distance, la divulgation d'informations et le déni de service. Deux d'entre elles sont dans l'environnement d'Android lui-même, deux autres se trouvent au niveau de sa bibliothèque et 24 dans le framework, a relevé Forbes. 68 failles sont présentes dans le framework média et 97 dans le système d'Android.

Elles seront toutes corrigées par le patch Android 10 qui sera diffusé à partir du 1er septembre. [..] Android 10 introduira également une série de nouveautés et améliorations de sécurité et de confidentialité qui permettront par exemple de définir quand les applications peuvent accéder à la géolocalisation, comment elles peuvent accéder à l'appareil photo du smartphone ou encore les empêcher d'activer ou désactiver le Wi-Fi sans avertir l'utilisateur.

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

### Microsoft a publié la version bêta du nouvel Edge - et offre des récompenses allant jusqu'à 30.000 $ pour la recherche de vulnérabilités

20 août 2019

Microsoft lance un appel de bug Hunt afin de déceler tout problème de sécurité dans la version bêta de son nouveau navigateur Edge sur le code Chromium open-source de Google, avant de le pousser officiellement en mise à jours.

[...] Microsoft a également étendu son programme Edge bug -bounty existant pour inclure maintenant le « Microsoft Edge Insider Bounty », visant à résoudre les problèmes de sécurité dans cette dernière version. […] Ils invitent les chercheurs à révéler toute vulnérabilité à fort impact qu'ils pourraient trouver dans la prochaine version de Microsoft Edge, basée sur Chrome, et recevoir une récompense pouvant atteindre 30 000 $ US pour des failles admissibles sur les canaux Dev et Beta. […] les failles concernées comprennent celles de type élévation de privilèges, exécution de code, divulgation d'information et autres...

L'ancienne version de Edge étant en fin de vie, la nouvelle version chromium est en phase de test depuis plusieurs mois […] son lancement officiel est prévu pour fin 2019 début 2020.

***Source :*** *https://threatpost.com/microsoft-rewards-chromium-edge-beta-flaws/147542/*

***Détail bounty :*** *https://www.microsoft.com/en-us/msrc/bounty-new-edge?rtc=1*

### Un nouveau label européen des objets connectés

19 août 2019

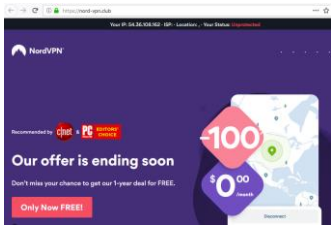

« IoT Qualified as Secured » IQS est le label de cyber sécurité nouvellement sorti de chez Digital Security, spécialiste français de la sécurité des objets connectés. En 2016, l'ENISA, l'agence de la sécurité des objets connectés de l'Union Européenne, avait déjà publié un référentiel de sécurité pour ce genre de produits [..]. Le label possède deux niveaux : standard et avancé. Pour l'obtenir, le produit proposé doit correspondre à une série de 20 à 30 exigences d'ordre technique dont

la liste complète et descriptive est téléchargeable sur le site https://iqs-label.com/. Une labélisation qui se veut être une garantie à la fois technique et relative aux données. Une fois accordée, elle sera valide pour deux ans.

***Source :*** *http://bit.ly/2U6BIpT*

## Site VPN populaire cloné pour propager des Malwares

21 août 2019




Des chercheurs au « Doctor Web virus lab » ont découvert que des cybercriminels avaient créé un clone du site Web qui appartenait au service de réseau privé virtuel NordVPN. Ce site web nord-vpn.club, actuellement inaccessible, était presque identique au site officiel de nordvpn.com.

Pour rendre le site cloné plus légitime et s'assurer qu'il passe les contrôles de sécurité du navigateur, il avait un certificat SSL valide émis par l'autorité de certification ouverte Let's Encrypt.

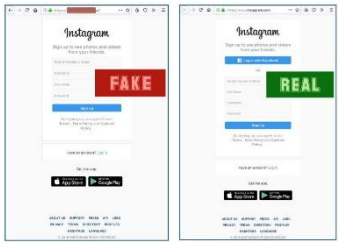
Les visiteurs du faux site web ont été invité à télécharger le client de NordVPN. Le vrai programme est installé mais le cheval de trois Win32.Bolik.2 été téléchargé en plus infectant le système de l'utilisateur.

A l'aide de ce malware, les attaquants peuvent effectuer des injections web, intercepter du trafic, enregistrer les frappes clavier et voler des informations sensibles.

***Source :*** *https://www.techspot.com/news/81539-popular-vpn-site-cloned-spread-malware.html*

## Utilisateurs d'Instagram victimes d'une compagne de phishing

25 août 2019




Les utilisateurs d'Instagram sont victimes d'une nouvelle compagne de phishing qui utilise des alertes d'authentification combinées à ce qui ressemble aux codes d'authentification à deux facteurs pour tromper les victimes potentielles à introduire leurs données sensibles sur de faux sites.

[..] ici, les attaquants utilisent de fausses alertes indiquant que quelqu'un a essayé de se connecter au compte de la cible, et demandent ainsi qu'il confirme son identité au moyen d'une page de connexion liée dans le message. La page de redirection est un parfait clone de la page d'authentification Instagram, vérifiée par certificat SSL légitime et affichant un cadenas vert pour palier à toute suspicion d'authenticité.

Afin d'éviter de tomber dans le piège de l'hameçonnage Instagram comme celui-ci, il est recommandé de ne jamais saisir les informations de connexion si la page qui le demande n'appartient pas au site instagram.com.

Cependant, si l'utilisateur s'est fait voler ses identifiants Instagram lors d'une telle attaque, ou si son compte a été piraté mais qu'il peut encore y accéder d'une manière ou d'une autre, il doit vérifier en premier lieu si son adresse mail et son numéro de téléphone sont toujours associés au compte. Changer par la suite le mot de passe est primordial.

***Source :*** *https://www.ehackingnews.com/2019/08/instagram-users-fall-victim-to-yet.html*

## Une nouvelle campagne de phishing utilise de faux CV pour distribuer Quasar RAT

27 août 2019

Une nouvelle campagne de phishing distribue Quasar RAT sur les systèmes Windows via de faux documents de CV protégés par mot de passe.

Quasar RAT est un outil d'administration à distance capable d'ouvrir des connexions de bureau distant, d'enregistrer des saisies claviers, de voler des informations d'identification, de prendre des captures d'écran, d'enregistrer des vidéos à partir de webcams, de télécharger ou d'exfiltrer des fichiers et de gérer des processus sur des ordinateurs infectés […].

Les courriels de phishing incluent un document Microsoft Word malveillant déguisé en document protégé par mot de passe. Le mail invite les utilisateurs à ouvrir le CV en entrant le mot de passe "123".

Une fois ouvert, le faux CV leur demandera d'activer les macros qui démarrera le processus d'infection.

***Source :*** *http://bit.ly/347f19q*

## Nouvelles Dragonblood vulnérabilités découvertes dans le standard Wifi WPA3

03 août 2019

En avril de l'année en cours, deux chercheurs en sécurité ont divulgué des détails sur cinq vulnérabilités (appelées Dragonblood) de la norme de sécurité et d'authentification Wifi WPA3 récemment lancée par l'Alliance Wifi.

Le 02 du mois d'août, les mêmes chercheurs ont révélé deux bugs supplémentaires sur dans les recommandations de sécurité créées pour atténuer les attaques initiales Dragonblood. [..] Tout comme celles d'avril, ces vulnérabilités permettent aux attaquants de divulguer des informations provenant des opérations cryptographique et ainsi brute forcer le mot de passe réseau du Wifi.

Les deux vulnérabilité référencées CVE-2019- 13377 et CVE-2019-13456 impact le mécanisme d'échange de clé et le protocole EAP-pwd respectivement. Les détails sont présents sur le lien fourni.

Les chercheurs ont déclaré avoir signalé ces deux nouveaux bogues à l'Alliance WiFi. [..] Ils ont également critiqué l'Alliance pour son processus fermé de développement de standards qui ne permet pas à la communauté open-source de contribuer et empêcher l'introduction de vulnérabilités dans standard.

Il est à noter que c'est les mêmes chercheurs belges qui ont découvert l'attaque KRACK qui a cassé le standard d'authentification WiFi WPA2 et forcé la WiFi Alliance à développer le standard WPA3, qu'elle a lancé en juin 2018.

Des détails sur les deux nouvelles vulnérabilités de sont disponibles dans une version mise à jour du livre blanc Dragonblood.

***Source :*** *https://zd.net/2Lf6lFh*

## Une nouvelle famille de Ransomware cible les utilisateurs du jeu Fortnite

20 août 2019


Surnommé Syrk, le nouveau ransomware récemment découvert tente de monétiser la popularité du jeu en se faisant passer pour un outil de piratage de jeu pour Fortnite. Une fois exécuté, le malware commence à crypter les fichiers sur la machine de la victime, en y ajoutant l'extension.Syrk.

L'attaquant tente d'amener les utilisateurs à payer la rançon le plus rapidement possible en supprimant des fichiers toutes les deux heures.

Une fois exécuté, le ransomware tente également de désactiver Windows Defender et User Account Control (UAC) par le biais d'un ajustement au registre, et tente d'assurer la persistance. Il surveille également le système à la recherche d'outils qui pourraient mettre fin à son processus, tels que Task Manager, Procmon64 et ProcessHacker. Il tente également d'infecter les clés USB connectées au système pour se propager davantage.

Cependant, des chercheurs en cyber sécurité ont découvert deux méthodes pour déchiffrer les données, car les fichiers nécessaires à cela sont présent dans la machine infectée aussi bien que des fichiers contenant l'ID et le mot de passe nécessaires pour le décryptage.

***Source*** : *https://www.securityweek.com/open-source-based-ransomware-targets-fortnite-players*

## Les pirates veulent 2,5 millions de dollars de rançon suite à une attaque Ransomware au Texas

21 août 2019


L'attaque qui a ciblé plusieurs institutions gouvernementales du Texas avec des ransomware la semaine dernière a peut-être été perpétrée en compromettant un fournisseur de services gérés (MSP). L'attaquant a exigé une rançon collective de 2,5 millions de dollars, selon le maire d'une municipalité.

Selon le Département des ressources d'information (DIR), le nombre de victimes a été fixé à 22. [..] Les noms de toutes les municipalités touchées par le malware ne sont toujours pas dévoilées.

Le malware a été déployé, selon toute vraisemblance, par le biais du logiciel d'administration utilisé par le fournisseur de services gérés (MSP) pour le support technique.

***Source*** : *http://bit.ly/2MG7yZo*

## Hostinger fuite d'information - Réinitialise le mot de passe de 14 millions d'utilisateurs

26 aout 2019


Le fournisseur d'hébergement Web populaire, a été victime d'une brèche massive de données, qui a conduit à la réinitialisation des mots de passe de tous ses clients par mesure de précaution.

Dans un article publié dans son blog, Hostinger révèle qu'un tiers, non autorisé, a piraté l'un de ses serveurs et a eu accès à des mots de passe hachés et d'autres données associés à ses millions de clients.

L'incident s'est produit le 23 août lorsque des pirates ont trouvé un jeton d'autorisation sur l'un des serveurs de l'entreprise et l'ont utilisé pour accéder à une API système interne, sans avoir besoin de nom d'utilisateur ni de mot de passe. [..]

La base de données de l'API héberge les informations personnelles de près de 14 millions de clients Hostinger, y compris leurs noms d'utilisateur, e-mails, mots de passe hachés, prénoms et adresses IP.

Il convient de noter que l'entreprise a utilisé l'algorithme SHA-1 faible pour hacher les mots de passe des clients, ce qui a facilité la tâche aux pirates. De plus, l'authentification à deux facteurs n'est pas disponible.

***Source*** : *https://thehackernews.com/2019/08/web-hosting-hostinger-breach.html?m=1*

## Une opération illégale de crypto-monnaie expose des informations sensibles d'une centrale nucléaire ukrainienne

23 août 2019

Les médias locaux ont rapporté que le service de sécurité de l'Ukrain (SBU) a découvert du matériel informatique non autorisé à la centrale nucléaire de l'Ukrain du Sud. [..] les enquêteurs ont découvert que des travailleurs menaient une opération d'extraction de cryptomonaie en utilisant le réseau électrique de la centrale pour alimenter leurs équipements. [..] de plus, ces mêmes équipements ont été connectés au réseau intranet de la centrale et à internet ce qui aurait entraîné la divulgation d'informations confidentielles sur la sécurité physique de l'installation. Ce type d'information représenterait un secret d'État.

Les enquêteurs ont découvert des cartes vidéo, des commutateurs, des dispositifs de stockage, des blocs d'alimentation, des cartes mères, des câbles et d'autres accessoires dans la pièce d'où l'opération a eu lieu.

[..] Un responsable a déclaré que l'opération n'avait probablement pas été détectée pendant des mois, voire plus, exposant les infrastructures critiques à des « problèmes de sécurité potentiellement catastrophiques » ajoutant à cela que même avec les politiques et les règlements les plus stricts au monde, tout est théorique si une surveillance continuelle des activités inhabituelles n'est pas assurée.

***Source*** : *https://www.ehackingnews.com/2019/08/the-guards-at-ukrainian-nuclear-power.html*

## Plugins WordPress attaqués par une campagne de redirection malveillante

27 août 2019


Les plugins WordPress, point faible potentiel du système de gestion de contenu, sont souvent la cible d'attaques. Une nouvelle campagne exploite une sélection d'anciennes et de nouvelles vulnérabilités dans plusieurs plug-ins pour rediriger le trafic de sites Web légitimes vers d'autres domaines. Plusieurs plugins individuels de NicDark et de Simple 301 Redirects Addon - ont été corrigés, ont déclaré des chercheurs en sécurité de WordFence […]. Des indicateurs

de compromis (IOC) pour la campagne en cours ont été publiés par Wordfence, qui a également mis à jour les règles de pare-feu pour se protéger contre ces attaques.

Les 20 principales adresses IP associées à cette campagne sont répertoriées dans la source.

***Source :*** *http://bit.ly/2L3lGu2*

### Des scripts de détournement de clic sur plus de 600 sites Web populaires détectés

27 août 2019

Des chercheurs de Microsoft Research, de l'Université chinoise de Hong Kong, de l'Université nationale de Séoul et de la Pennsylvania State University ont découvert des scripts de détournement de clics malveillants qui interceptent les clics d'utilisateurs sur au moins 613 sites Web populaires.

L'équipe de recherche a détecté des scripts de détournement de clic sur des sites Web en créant un outil appelé Observer. Cet outil analyse la liste des 250 000 principaux sites Web Alexa les plus populaires pour détecter la présence de scripts de détournement de clics qui interceptent les clics de l'utilisateur.

«OBSERVER se concentre sur trois actions fondamentales sur lesquelles le code JavaScript peut s'appuyer pour intercepter les clics: 1) modifier un lien hypertexte existant dans une page; 2) créer un nouveau lien hypertexte dans une page; et 3) l'enregistrement d'un gestionnaire d'événements dans un élément HTML pour accrocher un clic d'utilisateur », ont déclaré les chercheurs dans leur document de recherche […].

Les chercheurs recommandent aux organisations de veiller à l'intégrité des liens et des clics afin d'empêcher l'interception des clics par des hyperliens et des gestionnaires d'événements […].

***Source :*** *http://bit.ly/2MGoAa7*

# Evènements

### #LOI1807DZ, mise en œuvre.

### Chapitre 3 > Assurer la confidentialité de vos données !

***Jeudi 01 Aout 2019, Alger, Algérie***

*http://urlz.fr/afgs*

Un workshop sur comment préserver la confidentialité des données, qu'elles se trouvent sur ordinateur de bureau, ordinateur portable, tablette, disque dur, média amovible, fichier, système de messagerie électronique ou application cloud (dont SaaS), pour collaborer en toute confiance.

### Blackhat

***3-8 août 2019, Las Vegas, USA***

*https://www.blackhat.com/us-19/*

Black Hat USA, qui en est à sa 22eme édition, est le plus important événement mondial sur la sécurité de l'information, offrant aux participants les toutes dernières nouveautés en matière de recherche, de développement et de technologie. Elle débute par quatre jours de formations techniques (3-6 août) suivis d'une conférence principale de deux jours (7-8 août) avec Briefings, Arsenal, Business Hall, et plus encore.

Les vidéos des conférences peuvent être visionnées sur la chaine Black Hat USA 2019

### DEF CON

***8-11 août 2019, Las Vegas, USA***

*https://www.defcon.org/html/defcon-27/dc-27-index.html*

DEF CON est la convention Hacker la plus connue à travers le monde. Tenue chaque année à Las Vegas aux USA. La première s'est déroulée en juin 1993.

L'évènement consiste en de multiples conférences traitant de sujets liés aux ordinateurs ou au piratage informatique, de concours de crochetage de serrures, de robotique ou encore l'une des compétitions les plus connues *Capture The Flag (CTF)*. Celle-ci se joue sur deux fronts ; défendre et protéger son réseau en corrigeant ses failles en tentant de compromettre le réseau des équipes adverses. Les vidéos techniques des intervenants peuvent être visionnées sur la chaine DEFCONConference.

### HITB GSEC

***26th - 30th août 2019, Singapore***

*https://gsec.hitb.org/sg2019/*


HITBSecConf ou la Hack In The Box Security Conference est un événement annuel incontournable dans les calendriers des chercheurs et professionnels de la sécurité à travers le monde. Tenue chaque année, c'est est une plate-forme de discussion et de diffusion des questions de sécurité informatique de la prochaine génération. Ses événements comprennent deux jours de formation et une conférence de deux jours sur plusieurs thèmes mettant en lumière des conférences techniques de pointe données les experts les plus respectés de l'industrie de la sécurité informatique.

| | |
|---|---|
| **Reference** | ANPT-2019-BV-04 |
| **Titre** | Bulletin de veille N°4 |
| **Date de version** | 28 août 2019 |
| **Contact** | ssi@anpt.dz |