BULLETIN DE VEILLE N°04

ANPT-2021-BV-04

«Il n'y a pas de solution miracle avec la cybersécurité, une défense en couches est la seule défense viable» -James Scott -

Avril 2021

Alertes de sécurit

Microsoft

Vulnérabilité Zero-day dans Desktop Window Manager exploitée dans la nature

16 mars 2021

Un nouvel exploit Zero-day dans Desktop Windows Manager a été découvert par les experts en cybersécurité de Kaspersky.

La vulnérabilité référencée CVE-2021-28310 est utilisé dans la nature, potentiellement par des cybercriminels. Il s'agit d'un exploit d'élévation de privilèges (EoP), trouvé dans Desktop Window Manager, permettant aux attaquants d'exécuter du code arbitraire sur la machine victime. Il est probablement combiné avec d'autres exploits pour échapper aux sandboxes ou afin d'obtenir des privilèges système pour un accès ultérieur.

Il est fortement recommandé d'installer immédiatement les correctifs que Microsoft a publiés le 13 avril.

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

WhatsApp

WhatsApp, de nouveaux bugs qui pourraient permettre aux attaquants de pirater votre téléphone à distance

14 avril 2021

WhatsApp a récemment corrigé deux vulnérabilités de sécurité dans son application de messagerie pour Android qui auraient pu être exploitées pour exécuter du code malveillant à distance sur l'appareil et même exfiltrer des informations sensibles […].

Les failles permettent une attaque de type « man-in-the-disk » qui permet à des attaquants de compromettre une application en manipulant certaines données échangées entre celle-ci et le stockage externe.

Pire encore, le code malveillant peut être utilisé pour accéder à toute ressource stockée dans la zone de stockage externe non protégée, y compris celles de WhatsApp. Il s'est avéré que celle-ci est utilisée pour enregistrer les détails de la clé de session TLS dans un sous-répertoire, entre autres, et par conséquent, exposer des informations sensibles. Des informations à toute application configurée pour lire ou écrire à partir du stockage externe.

« Tout ce qu'un attaquant a à faire est d'inciter la victime à ouvrir un document HTML en pièce jointe », a déclaré Chariton Karamitas, chercheuse à Census Labs. « WhatsApp rendra cette pièce jointe dans Chrome, via un fournisseur de contenu, et le code Javascript de l'attaquant pourra voler les clés de session TLS stockées. »

Pour se défendre contre de telles attaques, Google a introduit une fonctionnalité appelée « stockage limité » dans Android 10, qui donne à chaque application une zone de stockage isolée sur l'appareil de manière à ce qu'aucune autre application installée sur le même appareil ne puisse accéder directement aux données enregistrées par d'autres applications.

Source : *https://bit.ly/3xan4pF*

Juniper

Une faille RCE critique permet aux attaquants de compromettre les périphériques réseau Juniper

20 avril 2021

Juniper Networks a corrigé une vulnérabilité critique dans Junos OS, qui pourrait permettre à un attaquant de prendre le contrôle à distance des appareils affectés ou de les perturber.

Ce problème affecte Junos OS 15.1X49, 15.1, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3. Juniper SIRT déclare qu'il n'est au courant d'aucune exploitation malveillante de cette vulnérabilité.

La faille référencée CVE-2021-0254 peut être exploitée par un attaquant distant non authentifié pour exécuter du code arbitraire d'un périphérique vulnérable ou pour déclencher une condition DoS. La vulnérabilité peut être exploitée en envoyant des paquets spécialement conçus au système ciblé.

Un attaquant pourrait provoquer la faille pour installer une porte dérobée sur un appareil vulnérable ou pour modifier sa configuration. Une mise à jour est disponible pour résoudre le problème.

Source : *https://bit.ly/3er4dId*

Google

Google lance un correctif pour une vulnérabilité zero-day dans Chrome

21 avril 2021

Google a publié une mise à jour pour son navigateur Web Chrome qui corrige une série de failles de sécurité, y compris une vulnérabilité zero-day connue pour être activement exploitée par des acteurs malveillants. Les bugs affectent les versions Windows, macOS et Linux du navigateur populaire.

La vulnérabilité zero-day référencée CVE-2021-21224 récemment révélée découle d'un bug de confusion de type dans le moteur JavaScript V8 utilisé dans Chrome et d'autres navigateurs Web basés sur Chrome.

Les utilisateurs des systèmes concernés devraient mettre à jour Google Chrome vers la version 90.0.4430.85 pour résoudre le problème.

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

Mysql

MySQL pour Windows est vulnérable à l'élévation des privilèges

20 avril 2021

MySQL pour Windows contient une vulnérabilité d'élévation de privilèges due à l'utilisation d'une OPENSSLDIR variable qui spécifie un emplacement où un utilisateur Windows non privilégié peut créer des fichiers.

La vulnérabilité référencée CVE-2021-2307 pourrait permettre à un utilisateur non privilégié d'exécuter du code arbitraire avec les privilèges SYSTEM sur un système Windows avec le logiciel MySQL vulnérable installé.

Cette vulnérabilité est corrigée dans les versions 8.0.24 et 5.7.34 du programme d'installation de MySQL Windows.

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

Apple

Apple corrige un bug critique de macOS après son utilisation dans la nature

26 avril 2021

Apple a corrigé une vulnérabilité zero-day dans macOS exploitée dans la nature par le malware *Shlayer* afin de contourner les contrôles de sécurité de File Quarantine, Gatekeeper et Notarization d'Apple et télécharger des charges utiles malveillantes de deuxième étape.

Les créateurs de Shlayer ont déjà réussi à obtenir leurs charges utiles malveillantes via le processus de notarisation automatisé d'Apple .

La vulnérabilité référencée CVE-2021-30657 permettait de contourner les protections d'Apple, notamment les exigences de notarisation. Elle aurait été exploitée par au moins un groupe criminel. Apple a corrigé le bug dans les versions bêta de macOS Big Sur 11.3.

Un autre bug zero-day référencé CVE-2021-30661de WebKit Storage exploité dans la nature a aussi été corrigé par Apple. La vulnérabilité permet aux attaquants d'exécuter du code arbitraire.

La liste des appareils concernés comprend ceux exécutant : Apple Watch Series 3 et versions ultérieures ainsi que iPhone 6s et versions ultérieures, iPad Pro (tous les modèles), iPad Air 2 et versions ultérieures, iPad 5e génération et versions ultérieures, iPad mini 4 et versions ultérieures et iPod touch (7e génération)

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

Pulse Secure

Des pirates exploitent Pulse Secure zero-Day

20 avril 2021

La vulnérabilité critique de contournement d'authentification zero-day référencée CVE-2021-22893 est actuellement exploité dans la nature sans la disponibilité d'un correctif à ce jour.

Au moins deux acteurs malveillants ont été à l'origine d'une série d'intrusions visant des organisations de défense, gouvernementales et financières aux États-Unis et ailleurs. Et cela en exploitant les vulnérabilités critiques des périphériques VPN Pulse Secure pour contourner les protections d'authentification multifactorielles et perturber les réseaux d'entreprise.

VPN Pulse Secure a publié des atténuations temporaires pour remédier à la vulnérabilité d'exécution arbitraire de fichiers, tandis qu'un correctif devrait être mis en place début mai.

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

SonicWall

3 Exploits Zero-Day affectent SonicWall Enterprise Email Security Appliances

20 avril 2021

SonicWall a corrigé trois vulnérabilités de sécurité critiques dans son produit de sécurité de messagerie (ES) hébergé et sur site qui sont activement exploitées dans la nature.

Référencées comme CVE-2021-20021 et CVE-2021-20022, les failles ont été découvertes et signalées à l'entreprise par la filiale Mandiant de FireEye le 26 mars 2021, après que la société de cybersécurité ait détecté une activité de shell web post-exploitation sur un système accessible par Internet dans l'environnement d'un client où l'application ES de SonicWall s'exécutait sur une installation Windows Server 2012. Une troisième faille (CVE-2021-20023) identifiée par FireEye a été divulguée à SonicWall le 6 avril 2021 […].

L'attaquant a exploité ces vulnérabilités, avec une connaissance approfondie de l'application SonicWall, pour installer une porte dérobée, accéder aux fichiers et aux e-mails et se déplacer latéralement dans le réseau de l'organisation victime.

SonicWall a publié des correctifs pour corriger les problèmes et a communiqué ces mesures d'atténuation aux clients et partenaires."

Source : *https://bit.ly/3dW6exZ*

Actualité

Facebook : une fuite massive de données, 2,8 milliards d'utilisateurs sont concernés

21 avril 2021

Après que **533** millions d'utilisateurs Facebook ont été touchés par l'un des gros piratages de l'histoire du réseau social, ce dernier pourrait subir une nouvelle fuite de données de grande ampleur. Un outil repéré par un chercheur en cybersécurité est capable de relier 5 millions d'adresses mail par jour à des comptes publics et/ou privés. Intitulé « Facebook Email Search v1.0 », il se propage actuellement sur divers forums de hacking […].

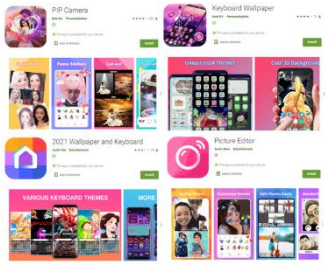
L'outil est actuellement utilisé pour pirater des comptes Facebook et prendre le contrôle de pages, groupes ainsi que des « comptes publicitaires, évidemment pour obtenir des gains financiers ». En seulement quelques minutes, l'outil parvient à obtenir plusieurs milliers d'adresses mail, simplement à partir de quelques noms de compte […].

Le chercheur à l'origine de la découverte conclut en disant que « il ne s'agit pas seulement d'une immense atteinte à la vie privée. Cela va résulter en une nouvelle fuite gigantesque de données, notamment des adresses mail. Elle va permettre à des personnes malveillantes non seulement de relier les adresses mail aux identifiants utilisateurs, mais aussi d'ajouter ces dernières aux numéros de téléphone étant apparus dans de précédentes fuites ».

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

Applications malveillantes dans Google Play Store détournent les notifications par SMS

21 avril 2021



De nombreuses applications frauduleuses ont fait leur chemin vers Google Play Store, ciblant les utilisateurs d'Android en Asie du Sud-Ouest et dans la péninsule arabique à hauteur de plus de 700000 téléchargements. Ces applications malveillantes dans Google Play Store détournent les notifications de messages SMS pour commettre une fraude à la facturation.

Se faisant passer pour des éditeurs de photos, des fonds d'écran, des puzzles, des skins de clavier et d'autres applications liées à l'appareil photo, les logiciels malveillants intégrés dans ces applications frauduleuses détournent les notifications des SMS, puis effectuent des achats non autorisés. Ces applications se révèlent être frauduleuses après les validations [..].

Ces menaces qui tirent parti de Notification Listener continueront de prospérer. Cependant, il est essentiel de prêter attention aux applications qui demandent des autorisations liées aux SMS et des autorisations d'écoute de notification

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

Les attaquants peuvent masquer les avertissements par e-mail de l'expéditeur externe avec HTML et CSS

22 avril 2021

Les produits de sécurité de messagerie tels que les passerelles de messagerie d'entreprise sont souvent configurés pour afficher l'avertissement «expéditeur externe» à un destinataire lorsqu'un e-mail arrive de l'extérieur de l'organisation.

Les administrateurs informatiques imposent l'affichage de ces avertissements pour protéger les utilisateurs contre les e-mails de phishing et d'escroquerie provenant de sources non fiables.

Cependant, cette semaine, un chercheur a montré un moyen assez simple que les expéditeurs d'e-mails peuvent utiliser pour contourner cette protection appliquée par les produits de sécurité des e-mails.

En ajoutant juste quelques lignes de code HTML et CSS, le chercheur Louis Dion-Marcil a montré comment un expéditeur externe pouvait cacher l'avertissement même d'un message électronique […].

Le chercheur dit qu'il ne s'agit pas d'un bug dans aucune application client de messagerie en soi, et qu'il est indépendant du client.

Indépendamment du fait qu'un e-mail contienne l'avertissement «expéditeur externe» ou non, les utilisateurs doivent faire attention avant d'ouvrir des liens ou des pièces jointes dans les e-mails qu'ils reçoivent.

Source *: https://bit.ly/2R4XA7j*

Comment la micro-segmentation crée une bataille difficile pour les intrus

22 avril 2021

L'un des plus grands dangers est qu'après avoir pris pied dans un réseau d'entreprise, un acteur attaquant prudent peut progressivement se déplacer latéralement à travers celui-ci et augmenter son accès et ses privilèges tout en restant indétectable […].

La mise en œuvre d'une approche du moindre privilège s'est avérée être un moyen efficace de contrer cette menace, obligeant l'intrus à faire beaucoup plus de travail pour accéder aux données et aux systèmes critiques. Mieux encore, les politiques de confiance zéro qui exigent que chaque utilisateur ou système soit vérifié en fonction de facteurs de risque tels que l'emplacement et l'appareil.

La micro-segmentation du réseau joue un rôle central dans la réalisation de stratégies de confiance zéro en limitant sévèrement le mouvement latéral d'un attaquant et en bloquant sa capacité à naviguer sur le réseau. La division des

environnements réduit efficacement la surface d'attaque disponible pour les adversaires et offre un contrôle extrêmement granulaire de tous les environnements de cloud et de centre de données, jusqu'à être en mesure de séparer les charges de travail individuelles. Plus il est difficile pour l'acteur de la menace de se déplacer, plus il devra rester longtemps dans le réseau avant d'atteindre son objectif, ce qui augmentera en fin de compte la probabilité qu'il soit détecté […].

La capacité, même pour une simple politique de séparation environnementale, de ralentir considérablement la progression des intrus sur le réseau signifie que la micro-segmentation devrait être un élément essentiel de toute stratégie de sécurité.

Source *: https://bit.ly/32VIeoA*

L'industrie des télécommunications face à une augmentation des attaques DDoS

21 avril 2021

Le secteur des télécommunications est confronté à une menace accrue d'attaques par déni de service distribué (DDoS), selon un nouveau rapport.

La nouvelle étude de Cloudflare détaille les attaques DDoS et les tendances pour le premier trimestre de 2021.

Parmi les résultats transcrit, la société d'infrastructure et de sécurité Web note que l'industrie des télécommunications a été le secteur le plus ciblé au cours des trois premiers mois de l'année 2021.

Le secteur a fait un bond «significatif» de la sixième place au quatrième trimestre 2020 pour devenir la cible numéro un des DDoS au premier trimestre 2021, suivi du secteur des services aux consommateurs et du secteur de la sécurité et des enquêtes.

«De nombreuses organisations ont des liaisons montantes fournies par leurs fournisseurs de services avec une capacité de bande passante inférieure à 1 Gbit / s.

«En supposant que leur interface réseau publique dessert également un trafic légitime, vous pouvez voir comment même les attaques DDoS inférieures à 500 Mbps peuvent facilement détruire les propriétés Internet.»

Le rapport complet est disponible sur le blog Cloudflare .

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

Cloud … soyons prêts !

50 entreprises nommées fournisseurs de confiance par Cloud Security Alliance

23 avril 2021

La Cloud Security Alliance (CSA) a annoncé jeudi la sélection d'une première série de «fournisseurs de confiance» pour la sécurité du cloud.

Dans une annonce à la presse , le groupe a déclaré qu'une «marque de confiance» de fournisseur de cloud de confiance serait affichée sur le registre CSA Security, Trust, Assurance & Risk (STAR) de chaque organisation. L'ASC espère que cela aidera les équipes de sécurité à identifier les fournisseurs de cloud qui démontrent un engagement envers une sécurité holistique. Plus de 50 prestataires ont été pré-qualifiés pour le groupe inaugural […].

Pour devenir un fournisseur cloud de confiance CSA, les entreprises doivent répondre aux critères suivants :

- Avoir une entrée à jour dans le registre CSA Security, Trust, Assurance & Risk (STAR) .
- Au moins un membre actuel du personnel doit avoir obtenu le certificat CSA of Cloud Security Knowledge (CCSK) .
- Inscrivez-vous en tant que membre corporatif et faites du bénévolat au moins 20 heures par an auprès de l'ASC pour des activités telles que des groupes de travail de recherche , des événements de chapitre, des articles de blog et d'autres travaux pour le bien de la communauté Cloud.

Source *: https://bit.ly/3dWcm9t*

Top 10 des outils de sécurité cloud Open Source pour protéger les données contre les pirates

25 avril 2021

Ces outils de sécurité dans le cloud sont utiles pour tous les modèles publics et privés tels que SaaS, PaaS, laaS, etc. Ceci est entièrement construit et fonctionne grâce à des technologies open source.

Top 10 des outils de sécurité cloud Open Source :

- Osquery
- GoAudit.
- Grapl
- OSSEC
- Suricata
- Zeek / Bro
- Panthère
- Kali Linux
- PacBot
- Security Monkey

Source *: https://bit.ly/3vnmoq8*

Bon à savoir !

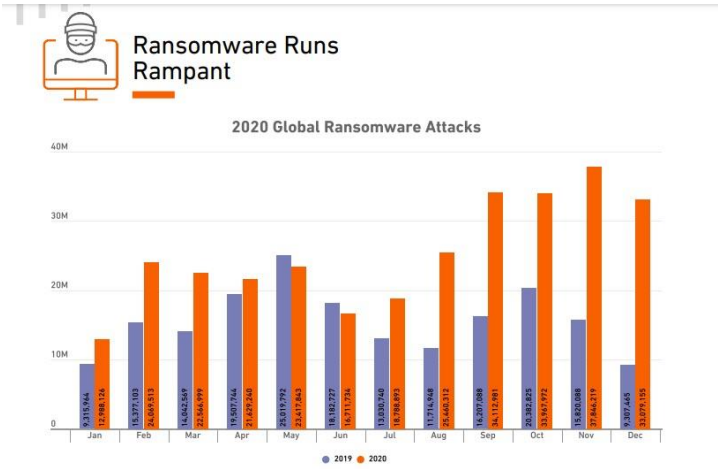
Récapitulatif sur les cybermenaces 2020, Rapport Sonicwall 2021

2020 a été une année historique pour notre façon de travailler. Les organisations ont dû fermer leurs bureaux, les employeurs ont dû apprendre à être plus flexibles et les employés ont dû comprendre comment travailler à domicile. Le changement rapide de notre façon de travailler a offert de nombreuses opportunités aux cybercriminels.

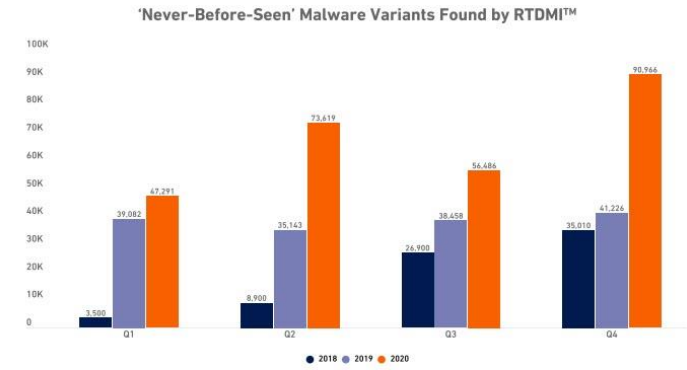
Le rapport mondial sur les menaces SonicWall, largement considéré comme l'une des sources les plus fiables au monde sur la cybersécurité mondiale, montre 188 hacks pour chaque clin d'œil au cours des douze derniers mois, soit un total de 5,6 milliards d'attaques de logiciels malveillants.

Les principales conclusions du rapport SonicWall sont les suivantes :

Les Ransomwares atteignent de nouveaux sommets avec des attaques de plus en plus ciblées



Plus de variantes de malwares «never-before-seen» identifiées

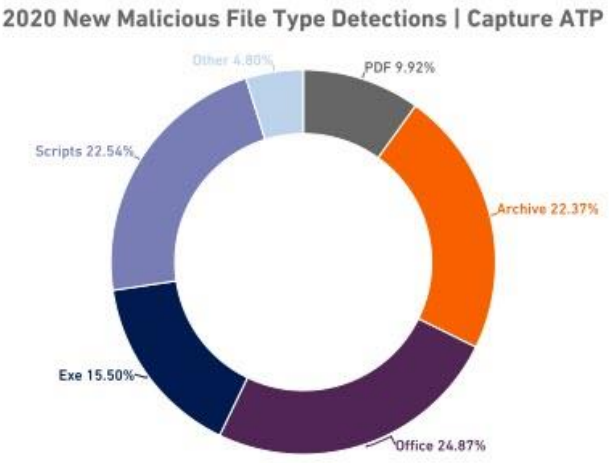


Les fichiers Office malveillants dépassent les fichiers PDF préférés de l'année précédente

Le cryptojacking revient alors que la crypto-monnaie bat des records

Les malwares IoT augmentent à mesure que la pandémie crée un réseau potentiel de perturbations

Les tentatives d'intrusion se manifestent à mesure que les schémas d'attaque changent



[Cliquez ici](#) pour télécharger le rapport sur les cybermenaces SonicWall 2021

Evènements

Evènements du mois

ALFM Action Line C5: Multidimensional cybersecurity measures15

20 avril 2021, Online

https://bit.ly/3sYrVC6

L'évaluation de la cybersécurité est essentielle pour soutenir une prise de décision éclairée, et une variété d'indices mesurant la maturité, la capacité, l'engagement, l'exposition au risque ou la capacité à répondre aux incidents ont émergé des secteurs public et privé.

Ce webinaire d'une heure a mis en vedette un panel diversifié d'experts pour une discussion sur la cybersécurité. Parmi les points discutés :

- Comment le travail de ces experts devrait-il et ne devrait-il pas être utilisé pour améliorer la cybersécurité ?
- Défis actuels dans la construction des données et des indices
- Comparabilité entre les États, les économies et les personnes.

Cliquer ici pour accéder à l'enregistrement du panel.

Evènements à venir

Women in Cyber Mentorship

08 Mars - Août 2021, Online

https://bit.ly/2R642Lk

L'Union internationale des télécommunications (UIT), le Forum de réponse aux incidents et des équipes de sécurité (FIRST) et EQUALS, le partenariat mondial pour l'égalité entre hommes et femmes à l'ère numérique dont l'UIT est un co-fondateur, organisent conjointement le programme Women in Cyber Mentorat pour l'autonomisation des femmes dans le secteur de la cybersécurité. Le programme engage des modèles et des leaders dans ce domaine et les met en relation avec des femmes talentueuses du monde entier.

Le programme de Women in Cyber Mentorship est un programme en trois parties qui comprend des cercles de mentorat mensuels guidés avec des activités de soutien, y compris une série de webinaires inspirants et des cours de formation techniques et non techniques. Toutes les activités seront livrées en ligne sur une période de six (6) mois, de mars à août 2021.

Reference	ANPT-2021-BV-04
Titre	Bulletin de veille N°04
Date de version	30 Avril 2021
Contact	ssi@anpt.dz