OSSIR

Revue d'actualité

08/10/2019

Préparée par

Étienne Baudin @etiennebaudin
Vladimir KOLLA @mynameisv__

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

MS19-110 Vulnérabilités dans Internet Explorer (5 CVE)

- Exploit:
  - 4 x Exécution de code à distance
  - 1 x Contournement de restrictions de sécurité
  - **Actuellement exploité dans la nature**
- Crédits:
  - Elliot Cao working Trend Micro's Zero Day Initiative (CVE-2019-1208)
  - Joshua Graham of TSS https://tsscyber.com.au (CVE-2019-1220)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-1221, CVE-2019-1236)
  - Clément Lecigne of Google's Threat Analysis Group (CVE-2019-1367)

Dont 0 communes avec IE:

MS19-111 Vulnérabilités dans Edge (1 CVE)

- Exploit:
  - 1 x Vol d'informations
- Crédits:
  - Juho Nurminen (CVE-2019-1299)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

MS19-112 Vulnérabilités dans Microsoft JET Database Engine (9 CVE)

- Affectés
  - Microsoft Office
  - Toutes versions supportées de Windows
- Exploit:
  - 9 x Exécution de code à distance
- Crédits:
  - rgod of 9sg Security Team - rgod@9sgsec.com working Trend Micro's Zero Day Initiative (CVE-2019-1240, CVE-2019-1247)
  - kdot working Trend Micro's Zero Day Initiative (CVE-2019-1241, CVE-2019-1243, CVE-2019-1246, CVE-2019-1248)
  - kdot (CVE-2019-1242)
  - rgod working Trend Micro's Zero Day Initiative (CVE-2019-1249)
  - CodeBreaker & Meysam Firouzi of STAR Labs (Security Technologies and Advanced Research Labs Pte. Ltd.) (CVE-2019-1250)

MS19-113 Vulnérabilités dans Microsoft Office (3 CVE)

- Exploit:
  - 1 x Exécution de code à distance
  - 1 x Vol d'informations
  - 1 x Contournement de restrictions de sécurité
- Crédits:
  - L4Nce working Trend Micro's Zero Day Initiative (CVE-2019-1297)
  - Ying Xinlei of Ant-financial Light-Year Security Lab (CVE-2019-1263)
  - Florent Robinet (CVE-2019-1264)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

MS19-114 Vulnérabilités dans Microsoft RDP (4 CVE)

- Exploit:
  - 4 x Exécution de code à distance
- Crédits:
  - Microsoft Platform Security Assurance & Vulnerability Research (CVE-2019-0787, CVE-2019-0788, CVE-2019-1290, CVE-2019-1291)

MS19-115 Vulnérabilités dans Microsoft Windows (23 CVE)

- Exploit:
  - 6 x Exécution de code à distance
  - 15 x Élévation de privilèges
  - 1 x Vol d'informations
  - 1 x Contournement de restrictions de sécurité
- Crédits:
  - Qixun Zhao of Qihoo 360 Vulcan Team (CVE-2019-1138)
  - ? (CVE-2019-1215, CVE-2019-1219, CVE-2019-1277, CVE-2019-1294)
  - Ryan Wincey of Securifera (CVE-2019-1267)
  - Nick Landers from Silent Break Security (CVE-2019-1268)
  - GFW Team (CVE-2019-1269)
  - Donato Ferrante, Principal Security Consultant, IOActive (CVE-2019-1270)
  - Keqi Hu from Chengdu Security Response Center of Qihoo 360 Technology Co. Ltd. (CVE-2019-1271)
  - k0shl of Qihoo 360 Vulcan team (CVE-2019-1272, CVE-2019-1289)
  - Zhiyi Zhang from Codesafe Team of Legendsec at Qi'anxin Group (CVE-2019-1217)
  - Tavis Ormandy of Google Project Zero (CVE-2019-1235)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-1237)
  - Zhiniang Peng (@edwardzpeng) of Qihoo 360 Core Security and Fangming Gu (@afang5472) (CVE-2019-1253)
  - zhong_sf of Qihoo 360 Vulcan Team (CVE-2019-1278)
  - Shih-Fong Peng (@_L4ys) of TeamT5 (CVE-2019-1280)
  - Wayne Low of Fortinet's FortiGuard Labs (CVE-2019-1287)
  - Zhiniang Peng of Qihoo 360 Core security and Fangming Gu (CVE-2019-1292)
  - Chakra team of Microsoft (CVE-2019-1298)
  - Soyeon Park from SSLab at Georgia Tech (CVE-2019-1300)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

MS19-116 Vulnérabilités dans Windows Hyper-V (2 CVE)

- Affectés
  - Windows 10
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server, version 1803
  - Windows Server, version 1903
- Exploit:
  - 1 x Déni de service
  - 1 x Vol d'informations
- Crédits:
  - ? (CVE-2019-0928)
  - Vladimir Shebaldenkov of UCloud (CVE-2019-1254)

MS19-117 Vulnérabilités dans Microsoft Graphics Component (8 CVE)

- Exploit:
  - 7 x Vol d'informations
  - 1 x Élévation de privilèges
- Crédits:
  - ? (CVE-2019-1216)
  - Mateusz Jurczyk of Google Project Zero (CVE-2019-1244, CVE-2019-1245)
  - kdot working Trend Micro's Zero Day Initiative (CVE-2019-1251, CVE-2019-1283)
  - sf (CVE-2019-1252)
  - RanchoIce of Tencent ZhanluLab (CVE-2019-1284)
  - Netanel Ben-Simon and Yoav Alon of Check Point Research (CVE-2019-1286)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

MS19-118 Vulnérabilités dans .NET Core (1 CVE)

- Exploit:
  - 1 x Déni de service
- Crédits:
  - Paul Ryman of VMware Sydney Engineering Team (CVE-2019-1301)

MS19-119 Vulnérabilités dans .NET Framework (1 CVE)

- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - Eran Shimony of CyberArk Labs (CVE-2019-1142)

MS19-120 Vulnérabilités dans ASP.NET (1 CVE)

- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - Ian Routledge (@ediblecode) (CVE-2019-1302)

MS19-121 Vulnérabilités dans Windows Kernel (4 CVE)

- Exploit:
  - 2 x Vol d'informations
  - 2 x Élévation de privilèges
- Crédits:
  - JunGu and ZiMi of Alibaba Orion Security Lab (CVE-2019-1274, CVE-2019-1293)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

MS19-122 Vulnérabilités dans Skype for Business and Microsoft Lync (1 CVE)

- Exploit:
  - 1 x Vol d'informations
- Crédits:
  - Ahmed Aaish (iqzer0) at Parallel Security Solutions (CVE-2019-1209)

MS19-123 Vulnérabilités dans Visual Studio (1 CVE)

- Exploit:
  - 1 x Vol d'informations
- Crédits:
  - pgboy of Qihoo 360 Vulcan Team (CVE-2019-1232)

MS19-124 Vulnérabilités dans Microsoft Exchange Server (2 CVE)

- Exploit:
  - 1 x Déni de service
  - 1 x Vol de session
- Crédits:
  - Nicolas Joly of Microsoft Corporation (CVE-2019-1233)
  - Abdulrahman Al-Qabandi (CVE-2019-1266)

MS19-125 Vulnérabilités dans Microsoft Exchange Server (2 CVE)

- Exploit:
  - 1 x Déni de service
  - 1 x Vol de session
- Crédits:
  - Nicolas Joly of Microsoft Corporation (CVE-2019-1233)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

MS19-126 Vulnérabilités dans Microsoft Office SharePoint (7 CVE)

- Exploit:
  - 3 x Exécutions de code à distance
  - 3 x Vol de session
  - 1 x Élévation de privilèges
- Crédits:
  - Markus Wulftange (@mwulftange) working Trend Micro's Zero Day Initiative (CVE-2019-1257, CVE-2019-1295, CVE-2019-1296)
  - Suresh C (CVE-2019-1259, CVE-2019-1261)
  - ? (CVE-2019-1260)
  - David Cioccia @davide107 ING (CVE-2019-1262)

MS19-127 Vulnérabilités dans Active Directory (1 CVE)

- Affectés
  - Windows 10
  - Windows Server 2019
  - Windows Server, version 1803,1903
- Exploit:
  - 1 x Vol de session
- Crédits:
  - Johannes Gutenberg Universität-Mainz (CVE-2019-1273

MS19-128 Vulnérabilités dans Common Log File System Driver (2 CVE)

- Exploit:
  - 1 x Élévation de privilèges
  - 1 x Vol d'informations
- Crédits:
  - bee13oy of Qihoo 360 Vulcan Team (CVE-2019-1214)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

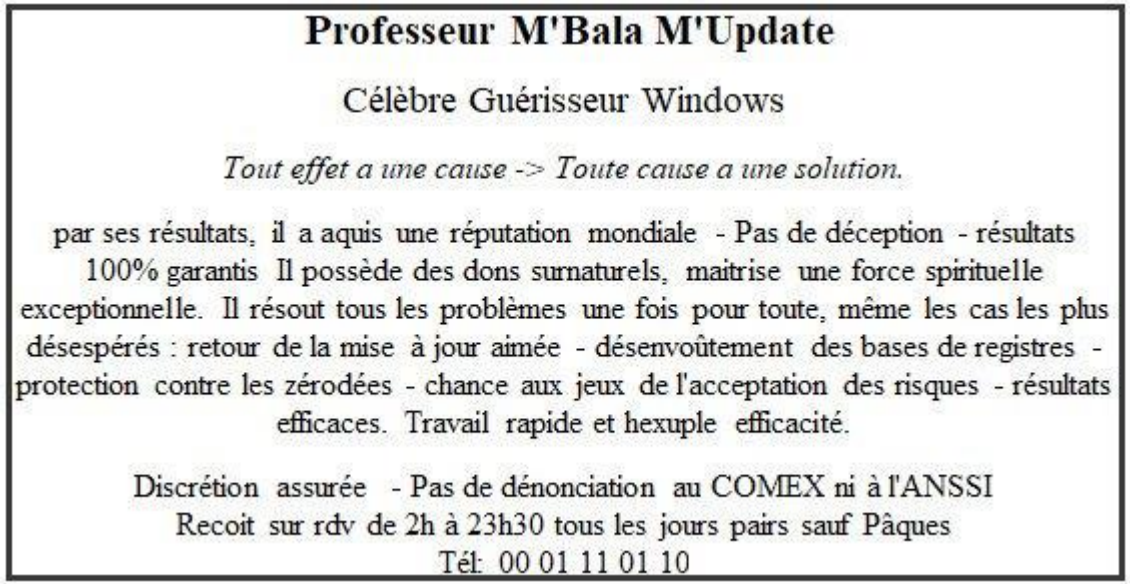
MS19-130 Vulnérabilités dans Microsoft Malware Protection Engine (1 CVE)

- Exploit:
  - 1 x Déni de service
- Crédits:
  - Charalampos Billinis of F-Secure Countercept @fsecure (CVE-2019-1255)

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Avis

Fin de support gratuit pour Windows 7, Server 2008 et 2008 R2

- 14 janvier 2020
  https://support.microsoft.com/en-us/help/4057281/windows-7-support-will-end-on-january-14-2020
  https://support.microsoft.com/en-us/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2



Professeur M'Bala M'Update

Célèbre Guérisseur Windows

Tout effet a une cause -> Toute cause a une solution.

par ses résultats, il a aquis une réputation mondiale - Pas de déception - résultats 100% garantis Il possède des dons surnaturels, maitrise une force spirituelle exceptionnelle. Il résout tous les problèmes une fois pour toute, même les cas les plus désespérés : retour de la mise à jour aimée - désenvoûtement des bases de registres - protection contre les zérodées - chance aux jeux de l'acceptation des risques - résultats efficaces. Travail rapide et hexuple efficacité.

Discrétion assurée - Pas de dénonciation au COMEX ni à l'ANSSI
Recoit sur rdv de 2h à 23h30 tous les jours pairs sauf Pâques
Tél: 00 01 11 01 10

Failles / Bulletins / Advisories
Système (principales failles)

Prise de contrôle via 2 vulnérabilités au sein d'Adobe Flash Player (APSB19-46)

- Same Origin Method Execution
- utilisation d'un espace mémoire après sa libération

https://helpx.adobe.com/security/products/flash-player/apsb19-46.html

Prise de contrôle du système à distance et contournement de sécurité via 3 vulnérabilités affectant Adobe Coldfusion (APSB19-47)

https://helpx.adobe.com/security/products/coldfusion/apsb19-47.html

(encore) **Prise de contrôle du système via une vulnérabilité au sein d'Exim**

- dépassement de tampon via l'envoi d'une commande EHLO suffisamment longue

https://www.openwall.com/lists/oss-security/2019/09/28/1

Failles / Bulletins / Advisories
Système (principales failles)

Vol d'informations via une vulnérabilité au sein de GitLab

- provenait de la fonctionnalité Group Search d'Elasticsearch
- Un attaquant pouvait accéder à des informations sensibles incluant du code, des merge requests et des commits.

https://about.gitlab.com/2019/10/02/security-release-gitlab-12-dot-3-dot-3-released/

Evasion et déni de service sur VMware ESXi

- use-after-free aboutissant à une évasion de la machine virtuelle
- erreur liée au support d'IPV6

https://www.vmware.com/security/advisories/VMSA-2019-0014.html

Orchestrateur de cloud OnApp, compromission depuis une seule VM / CVE-2019-12491

- Redirection des connexions SSH du manager

https://skylightcyber.com/2019/09/26/all-your-cloud-are-belong-to-us-cve-2019-12491/

Failles / Bulletins / Advisories
Réseau (principales failles)

Cisco

- 65 vulnérabilités pour 26 produits

https://tools.cisco.com/security/center/Search.x?publicationTypeIDs=1&firstPublishedStartDate=2019%2F09%2F10&firstPublishedEndDate=2019%2F10%2F06&limit=100

- Produits vulnérables
  - Cisco IOS
  - Cisco Adaptive Security Appliance (Déni de service)
  - Cisco Firepower Management Center
  - Cisco Unified Communications Manager
  - Cisco Unified Contact Center
  - Cisco Security Manager
  - Cisco Prime Infrastructure
  - Cisco Identity Services Engine
  - Cisco IC3000 Industrial Compute Gateway
  - Cisco FXOS
  - Cisco FTD, FMC, and FXOS
  - Cisco Firepower Threat Defense
  - Cisco Firepower System
  - Cisco Firepower Management Center
  - Cisco Email Security Appliance
  - Cisco Unified Communications Products
  - Cisco Adaptive Security Appliance
  - Cisco Firepower Threat Defense
  - Cisco Webex Meetings
  - Cisco IOS XE
  - Cisco Catalyst 4000 Series Switches TCP
  - Cisco IOx for IOS
  - Cisco IOx Application Environment
  - Cisco IOS XR
  - Cisco NX-OS
  - Cisco HyperFlex

Failles / Bulletins / Advisories
Android / iOS

Contournement de sécurité et prise de contrôle du système via 3 vulnérabilités au sein d'Apple iOS et iPadOS

- corruption mémoire et erreur logique
- accès à la liste des contacts sans authentification

https://support.apple.com/en-gb/HT210590

https://support.apple.com/fr-fr/HT210624

https://support.apple.com/en-gb/HT210603

Un nouvel outil de jailbreak d'iPhone, baptisé checkm8, a été publié en open source

- Tous les iPhones du 4S jusqu'au X concernés
- Affecte le SecureROM, en charge du démarrage de l'appareil
- Nécessite un redémarrage en DFU

https://www.igen.fr/ios/2019/09/avec-checkm8-le-jailbreak-fait-echec-et-mat-apple-110279

https://arstechnica.com/information-technology/2019/09/developer-of-checkm8-explains-why-idevice-jailbreak-exploit-is-a-game-changer/

https://github.com/axi0mX/ipwndfu

Evasion de la sandbox de Safari

- Activement exploité par eGobble pour afficher encore plus de publicités ou tenter de compromettre l'appareil

https://blog.confiant.com/massive-egobbler-malvertising-campaign-leverages-chrome-vulnerability-to-target-ios-users-a534b95a037f

Failles / Bulletins / Advisories
Android / iOS

Elévation de privilèges via une vulnérabilité 0-day au sein d'Android

- Exploitation dans la nature, POC disponible en open source
- Utilisé ou vendu par NSO Group (selon Google)

https://arstechnica.com/information-technology/2019/10/attackers-exploit-0day-vulnerability-that-gives-full-control-of-android-phones/
https://github.com/timwr/CVE-2019-2215/blob/master/poc.c
https://bugs.chromium.org/p/project-zero/issues/detail?id=1942

Use After Free sur Whatsapp pour Android

- Article **très clair** sur l'exploitation de la vulnérabilité

https://awakened1712.github.io/hacking/hacking-whatsapp-gif-rce/

Activation du micro à distance sur Signal pour Android

https://www.vice.com/en_us/article/3kx7n8/signal-bug-could-have-let-hackers-listen-to-android-users-via-microphone

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Malwares

Manque de temps…

https://awakened1712.github.io/hacking/hacking-whatsapp-gif-rce/

https://www.bleepingcomputer.com/news/security/comodo-forums-breached-data-of-over-170-000-users-up-for-grabs/

https://threatpost.com/asus-lenovo-routers-remotely-exploitable-bugs/148361/

https://blog.lastpass.com/2019/09/lastpass-bug-reported-resolved.html/

https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

https://www.darkreading.com/cloud/data-leak-affects-most-of-ecuadors-population/d/d-id/1335814

https://www.avocats-mathias.com/e-commerce/dsp2-authentification-forte

https://seclists.org/fulldisclosure/2019/Sep/31

https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

Piratages, Malwares, spam, fraudes et DDoS
Sites piratés

Rançongiciel à Sarrebourg et Sequedin

https://www.lanouvellerepublique.fr/niort/les-cyber-malfaiteurs-s-attaquent-aux-collectivites

Un rançongiciel fait perdre $95 millions à Demant (appareils auditifs)

- $7,3 pour la reconstruction du système d'information
- L’assurance ne paie que $12 millions

https://www.globenewswire.com/news-release/2019/09/26/1921031/0/en/Demant-A-S-Estimated-financial-impact-of-IT-incident-reflected-in-outlook.html

Piratages, Malwares, spam, fraudes et DDoS
Sites piratés

Plus d’infos sur l’attaque Triton, sauvé par la triple redondance

- Début en 2014 pour un sabotage en 2017
- Accès au VPN, attaque uniquement en mémoire, malware en cours de dev

https://www.industrie-techno.com/article/le-recit-par-schneider-electric-de-triton-l-attaque-qui-a-fait-trembler-l-industrie.57306

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Les “hackeurs du Darknet”

- Entre $100 et $300 pour pirater les réseaux sociaux

  https://queue.acm.org/detail.cfm?id=3365458

Serveur de Command and Control avec des paquets SYN

- La RFC permet 40 octets de données
- Peut aussi permettre l’exfiltration discrète
- Quel firewall enregistre les SYN de ports autorisés ?
  - Peut-être que le SYN-Flood pourrait le détecter

  https://thesw4rm.gitlab.io/nfqueue_c2/2019/09/15/Command-and-Control-via-TCP-Handshake/

SimJacker, exploitation vieille fonctionnalité

- Envoi de commande au “S@T Browser app” par des SMS techniques (SIM Toolkit)
- Permet d'exécuter des fonctions de la SIM
  - Géoloc, appeler, raccrocher, demander à l’utilisateur d’aller sur une page web...
- Utilisé dans la nature pour, à priori, espionner des gens

https://www.zdnet.com/article/new-simjacker-attack-exploited-in-the-wild-to-track-users-for-at-least-two-years/#ftag=CAD-00-10aag7e

WIBattack, une attaque cousine de SimJacker

- Envoi des commandes aux “Wireless Internet Browser (WIB)”

https://www.zdnet.com/google-amp/article/new-sim-card-attack-disclosed-similar-to-simjacker/

Nouveautés, outils et techniques

Crypto et Divers
Divers

DoH c’est parti (la suite dans Troll)

https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/

Contourner les Content Security Policies ?

- Merci Google Drive

  https://twitter.com/curtbraz/status/1180372698167435265?s=11

Business et Politique

Business
France

Business
International

Droit / Politique
France

Quand les ********* attaquent les ********

- Criteo affirme que Facebook privilégie sa propre régie publicitaire

  https://www.clubic.com/internet/facebook/actualite-871538-criteo-porte-plainte-facebook-france.html

Droit / Politique
International

Conférences

Conférences

Passées

- BlackHat - 3 au 9 août 2019
- BSides LasVegas - 6 - 7 août 2019
- DEFCON - 8 au 11 août 2019
- RSSIA - 23 septembre

A venir

- BruCON - 10 au 11 octobre 2019
- Assises de la sécurité - 9 au 12 octobre 2019
- Hack.lu - 22 au 24 octobre 2019
- Grehack - 15 novembre
- European Cyber Week - 19 au 22 novembre
- Sigsegv 2.0 - 30 novembre 2019 à Paris
- Botconf - 3 au 6 décembre 2019 à Bordeaux

Divers / Trolls velus

Divers / Trolls velus

Selon les EDR le modèle de détection par signature est mort

- “leurs signatures” puisqu’ils continuent à intégrer celles de Sigma (300 en open-source)
- Et sans le dire...

  https://twitter.com/cyb3rops/status/1177617812661116929?s=11

Divers / Trolls velus

IPv4 : la source est (presque) tarie

- Épuisement prévu pour pour novembre 2019
- Futures attribution au compte goutte
- Merci de rendre les IPv4 que vous n'utilisez plus
  - Propriétaires : 😎
  - RIPE: 😭

https://www.01net.com/actualites/l-epuisement-des-adresses-ipv4-est-desormais-une-realite-et-va-scleroser-le-web-1775587.html

IPv6 est la solution… ou pas

<<after now almost 12 years using, working and teaching[1]
IPv6 I've come to the conclusion that **IPv6** is a mistake and will **not work**.>>

https://www.ripe.net/ripe/mail/archives/ipv6-wg/2019-October/003352.html

Divers / Trolls velus

1.1.1.1 est il un vrai VPN ?

- VPN de CloudFlare basé sur WireGuard, servant à se protéger des MitM
- Fortement critiqué :

  https://twitter.com/notdan/status/1178339685795598336

- Mais ce n’est pas un VPN anonymisant :
- <<not designed to allow you to access geo-restricted content>>

  https://blog.cloudflare.com/announcing-warp-plus/

Divers / Trolls velus

DoH pose de nombreux problèmes

- Contournement des Proxy -> Interception SSL/TLS active est la solution
- Perte de la possibilité de faire du déchiffrement SSL/TLS -> Faux
- Les FAI ne pourront plus inspecter les requêtes DNS de mes clients
- Fuite des noms des domaines internes
- Perte de l'historique DNS (passive DNS)
- Les malwares se feront un plaisir d'utiliser DoH et… c'est déjà le cas

  https://www.zdnet.com/article/first-ever-malware-strain-spotted-abusing-new-doh-dns-over-https-protocol/

- Centralisation des requêtes DNS chez quelques fournisseurs : CloudFlare, Google…

Bortz propose un serveur DoH et DoT éthique

https://www.bortzmeyer.org/doh-bortzmeyer-fr-policy.html

https://www.bortzmeyer.org/doh-mon-resolveur.html

Divers / Trolls velus

Le Fake DeepFake

- Arnaque au président classique avec imitation d'un accent allemand
- Tout le monde parle d'utilisation de DeepFake

  https://gizmodo.com/scammer-successfully-deepfaked-ceos-voice-to-fool-under-1837835066

- Repris par des entreprises de cybersécurité sans vérifier

  https://twitter.com/search?q=%23Deepfakes%20IA%20escrocs&src=typed_query&f=live

- Der Spiegel clarifie la situation : pas de DeepFake

  https://www.spiegel.de/netzwelt/web/deepfakes-werden-erkennungsmethoden-die-naechsten-uploadfilter-a-1286373.html

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 12 novembre 2019

After Work

- oct/nov 2019

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?