Revue d'actualité de l'OSSIR

11 Avril 2023

Par ordre alphabétique :
Christophe Chasseboeuf
Jérémy De Cock
Vladimir Kolla

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de mars 2023, 80 vulnérabilités, dont :

- Exploitées dans la nature :
  - 1 zero-day critique (CVE-2023-23397) :
    - Exfiltration du condensat du mot de passe depuis un avis de réunion

      https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/
  - Contournement des sécurités Excel (CVE-2023-23398)

    https://packetstormsecurity.com/files/171752/Microsoft-Excel-Spoofing.html
- Les plus critiques ou les plus intéressantes :
  - Windows, exécution (rare) de code à la réception d'un paquet ICMP (CVE-2023–23415)

    https://doublepulsar.com/a-look-at-cve-2023-23415-a-windows-icmp-vulnerability-mitigations-which-is-not-a-cyber-meltdown-78a9f7e3e538
  - Windows, élévation locale de privilèges (CVE-2023-21768)

    https://github.com/xforcered/Windows_LPE_AFD_CVE-2023-21768

Failles / Bulletins / Advisories
Microsoft - Divers

Le zombie Internet Explorer, c'est enfin la fin… enfin…

- IE encore présent dans certains composants
- Fin annoncée pour le 13 juin 2023
  - Mais possible dès le 23 mai 2023 avec les mises à jour facultatives

https://www.neowin.net/news/microsoft-is-permanently-killing-off-internet-explorer-today/

Exécution de code dans Word (CVE-2023-21716)

- Dépassement de tampon du tas à partir d'un RTF dans la librairie wwlib
  - Si l'on précise un trop grand nombre de polices de caractères
  - Fonctionne avec le mode de prévisualisation d'outlook ou word
- Corrigé dans le bulletin du 14 fév. 2023
- PoC publié le 5 mars 2023

https://qoop.org/publications/cve-2023-21716-rtf-fonttbl.md

Failles / Bulletins / Advisories
Microsoft - Divers

Blocage (futur) **de très nombreuses techniques de contournement de KASLR**

- Suppression d'infos sensibles de tous les API NtQuery

  https://twitter.com/yarden_shafir/status/1644766236415258633

Planter cmd.exe ? Facile comme 339 839 907 caractères A

- Plante sous Windows 11

  https://www.exploit-db.com/exploits/51348

Failles / Bulletins / Advisories
Microsoft - Divers

AADConnect, mieux vaut prévenir que guérir

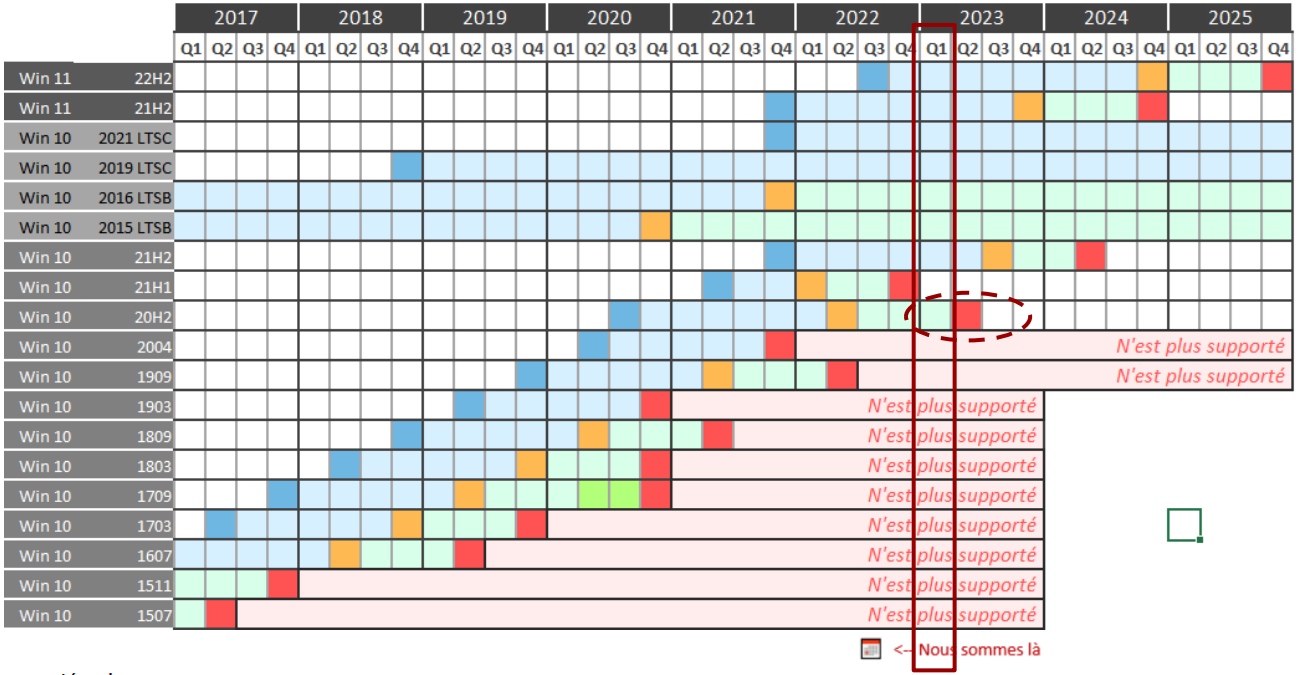
- Chaque version sera mise hors service **12 mois** à partir de la nouvelle disponible
- **Aucun support** fourni sur les versions hors service
- Version 2.1.1.0 hors service depuis mars 2023

https://admin.microsoft.com/Adminportal/Home#/dirsyncmanagement

https://learn.microsoft.com/fr-fr/azure/active-directory/hybrid/reference-connect-version-history#retiring-azure-ad-connect-1x-versions

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



Sortie	Home, Pro	Entreprise
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 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 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	10 mai 2022**
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	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
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	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

Elévation de privilèges avec `systemctl status`

- CVE-2023–26604 (CVSS 7.8)
  - Si le terminal n'est pas assez grand, les infos en sortie sont affichées avec `less` (vs `cat`)
  - `less` a la capacité d'exécuter des commandes (comme un shell `!sh`)
  - `/usr/bin/systemctl status <something>` dans */etc/sudoers* 🏆
- Mettez à jour Systemd vers la **version 247 minimum**

https://medium.com/@zenmoviefornotification/saidov-maxim-cve-2023-26604-c1232a526ba7

RCE sur ClamAV

- CVE-2023-20032 (CVSS 9.8)
  - **Heap overflow** réalisable lors de l'analyse de partition HFS+
  - Permet d'exécuter du code arbitraire avec les privilèges du processus ClamAV
  - Réalisable sans être authentifié
- Mettez à jour ClamAV vers la **version 1.0.1**

https://thehackernews.com/2023/02/critical-rce-vulnerability-discovered.html

Failles / Bulletins / Advisories
Systèmes

CVE sur les imprimantes HP, spécifique mais critique

- CVE-2023-1707 (CVSS 9.1)
- Impacte 50 modèles ssi …
  - … ils tournent sur le firmware FutureSmart version 5.6
  - … ils ont IPsec activé
- Permet à un utilisateur non authentifié d'effectuer une MitM
  - Un patch devrait sortir d'ici 85 jours, soyez patients !
- C'est quand même important de sécuriser ses imprimantes 😉

https://www.bleepingcomputer.com/news/security/hp-to-patch-critical-bug-in-laserjet-printers-within-90-days/

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

2 extensions Wordpress pouvant être critiques

- Elementor Pro
  - 12 millions de sites web impactés
  - Versions <= 3.11.6 affectées
  - Permet à un simple utilisateur de créer un créer un compte admin

  https://thehackernews.com/2023/04/hackers-exploiting-wordpress-elementor.html
- WooCommerce
  - 500k sites web impactés
  - Versions >= 4.8.0 et <= 5.6.1 affectées
  - Permet à une personne non authentifiée d'usurper un compte admin

  https://thehackernews.com/2023/03/critical-woocommerce-payments-plugin.html

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

2 CVEs importantes du côté de Zoom

- CVE-2023-22885 (CVSS 9.6)
  - Clients Zoom et Zoom Rooms
  - Versions < 5.13.5 impactées sur toutes les plateformes
  - RCE possible suite à un Trust Boundary Violation
- CVE-2023-22883 (CVSS 7.8)
  - Clients Zoom
  - Versions < 5.13.5 impactées sur Windows et macOS (uniquement)
  - Elévation de privilèges possible durant le processus d'installation

https://securityonline.info/zoom-fixes-two-high-risk-security-cve-2023-22885-cve-2023-22883-flaws/

https://github.com/patrickhener/CVE-2023-22855 (exploit python)

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

Injection SQL sur le module Paypal de PrestaShop

- CVE-2023-28843 (CVSS 9.8)
  - Versions comprises entre la 3.12.0 et 3.16.3 (inclus) du module affectés
  - Prestashop 1.6 uniquement concerné
- Permet à un attaquant à distance d'obtenir des accès admin

https://github.com/202ecommerce/paypal/security/advisories/GHSA-66pc-8gh8-mx7m

Failles / Bulletins / Advisories
Apple

Vulnérabilités exploitées dans la nature sur iOS 16.3

- Activement exploitées dans la nature
  - CVE-2023-23529, exécution de code dans le navigateur
  - CVE-2023-23514, élévation locale de privilèges

https://support.apple.com/en-us/HT213635

Failles / Bulletins / Advisories
Vulns' du vendredi 😢

Vulnérabilités critique sur JavaScript VM2 (CVE-2023-29017)

- Bibliothèque de cloisonnement (sandboxing) utilisée par NodeJS et plein d'autres
  - Nécessite au moins une XSS
- PoC

https://gist.github.com/seongil-wi/2a44e082001b959bfe304b62121fb76d

Vulnérabilités critique sur macOS et iOS (CVE-2023-28205 et CVE-2023-28206)

- Activement exploitées dans la nature
  - CVE-2023-28205, exécution de code dans le Safari (basé sur WebKit)
  - CVE-2023-28206, élévation locale de privilège

iOS 16.4 impacté, mettre à jour en iOS 16.4.1 https://support.apple.com/en-us/HT213720

iPadOS 16.4 impacté, mettre à jour en iPadOS 16.4.1 https://support.apple.com/en-us/HT213720

macOS Ventura 13.3 impacté, mettre à jour en macOS Ventura 13.3.1 https://support.apple.com/en-us/HT213721

Failles / Bulletins / Advisories
Réseau (principales failles)

Fortinet FortiOS

- CVE-2022-41328 (CVSS 7.1) - **Path Traversal**
- Permet à un attaquant de lire et écrire sur le système Linux via la CLI de **FortiManager**
  - … qui ne devrait pas être exposée 🙅‍♂️
- Moyen de persistance mis en place
  - Le fichier */sbin/init* est modifié et le fichier */bin/fgfm* est créé
- Systèmes affectés :
  - FortiOS versions 7.2.x antérieures à 7.2.4
  - FortiOS versions 7.0.x antérieures à 7.0.10
  - FortiOS versions 6.x antérieures à 6.4.12

https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-001/

https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis

https://thehackernews.com/2023/03/chinese-hackers-exploit-fortinet-zero.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
DDoS

Un record pour les DDoS 

- 71 millions de requêtes par seconde
- 30k adresses IP détournées
- Sites de crypto et sociétés de jeux-vidéos ciblés

https://www.numerama.com/cyberguerre/1271018-71-millions-de-requetes-par-seconde-un-nouveau-record-pour-une-attaque-ddos.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de DNA Diagnostics Center

- Vol de données ADN de 2,1 millions de personnes
  - Stockées sur des serveurs d'une entreprise achetée précédemment

https://www.01net.com/actualites/adn-21-millions-personnes-pirate-negligence.html

Secteur de la santé

- CHU de Brest
  https://www.usine-digitale.fr/article/le-chu-de-brest-victime-d-une-cyberattaque.N2110326
- Saint-Pierre (Belgique)

LastPass

- Compromission du poste personnel d'un dev à partir d'un logiciel "média" non à jour
- Ajout d'un keylogger, compro du coffre-fort pro de mots de passe
- Accès au stockage externe des coffres-forts des clients
  https://www.nextinpact.com/lebrief/71117/lastpass-pirates-sont-entres-par-lordinateur-dun-developpeur

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage du forum de Kodi

- Kodi, lecteur multimédia, multiplateforme
  - Fuite des messages privés, condensats des mots de passe, mail…
- Forum basé sur MyBB

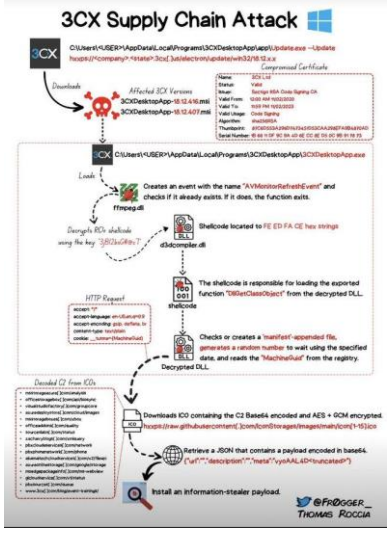
https://kodi.tv/article/important-kodi-forum-data-breach/

3CX, compromission de la chaîne d'approvisionnement

- Inclusion d'une librairie vérolée
  - Vol des mots de passe, jetons d'API, cookies…
- Alerte sur le forum, non prise au sérieux par l'éditeur 🤦‍♂️
- Attaque attribuée à la Corée du Nord

https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/

https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/



Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Clés privées de MSI volées

- Attaque revendiquée par Money Message
- Rançon de 4 millions de $ demandée
- Codes sources volés (1.5 To de données) de différents outils de MSI …
  - ERP
  - Logiciels et firmwares
- Et surtout les clés privées de MSI !!!
  - Attaque par supply chain à venir ?

https://twitter.com/lukolejnik/status/1644635717300101120

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Rorschach, le nouveau ransomware du moment

- Le plus rapide actuellement
  - 4 minutes 30 pour chiffrer 220k fichiers VS 7 minutes pour LockBit v.3
  - Pourquoi ? Il chiffre uniquement une partie de chaque fichier
- ++ ?
  - Désactive le firewall de Windows
  - Efface les journaux des événements Windows
  - Crée une GPO pour se propager vers d'autres machines (lorsqu'il est exécuté sur le DC)
- Petit tip gratuit :
  - Vous ne risquez rien si votre machine utilise une langue faisant partie de la Communauté des Etats indépendants (comme la Russie 😁)

https://securityaffairs.com/144425/cyber-crime/rorschach-ransomware-fast-encryption.html

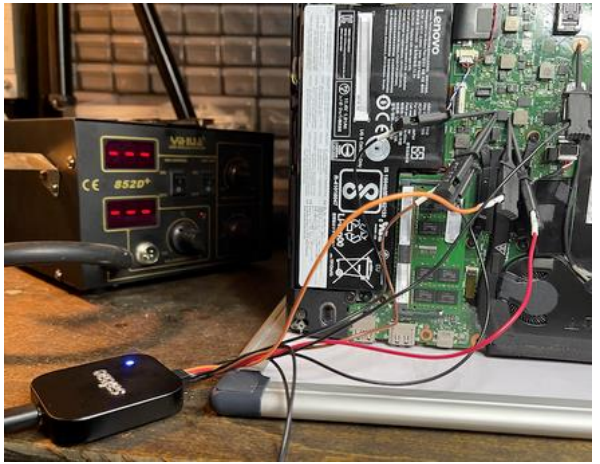
Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Récupérer le code exécuté sur un FPGA cloud

- Récupération possible du code source, des clefs de chiffrement…
  https://infosec.exchange/@hovav/110135084960548532

Récupérer la clef Bitlocker

- Fortement inspiré d'un article de 2021
  https://dolosgroup.io/blog/2021/7/9/from-stolen-laptop-to-inside-the-company-network
- Bus SPI (Serial Peripheral Interface) non chiffré
  https://astralvx.com/stealing-the-bitlocker-key-from-a-tpm/



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Clonage d'une voix à partir d'une IA 😳

- Et accès à un compte bancaire
  - Oh surprise, oh révolution… personne ne s'y attendait 😲
  - Orange Labs le faisait déjà avec le produit commercial **Kagedo** en 2008
    - Devenu Voxygen en 2011
  - Baidu Deep Voice, depuis 2017

    http://research.baidu.com/Blog/index-view?id=91
- Répétez après moi : **<<la biométrie c'est de l'identification, pas de l'authentification>>**

  https://www.nextinpact.com/lebrief/1189

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

ChatGPT, fuite des conversations

- Accès aux titres des conversations des autres

  https://www.engadget.com/chatgpt-briefly-went-offline-after-a-bug-revealed-user-chat-histories-115632504.html
- Mais c'est pareil avec DeepL, Google Translate, les json beautifier…

Vol des données du service d'imigration des USA

- Stocké dans un AWS S3, protégé par un couple identifiant/mot de passe ultra solide
  - Admin:Password1
- VX Underground contacté pour le rachat ou la revente

  https://twitter.com/vxunderground/status/1642875346235129856

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

Vulkan files, sous-traitant du FSB et GRU

https://www.nextinpact.com/lebrief/71371/les-vulkan-files-revelent-outils-dun-prestataire-cyber-renseignement-russe

https://blog.sekoia.io/sekoia-io-analysis-of-the-vulkanfiles-leak/

https://clement-briens.com/2023/04/01/meet-the-fsb-contractor-0day-technologies/

https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

Documents des services secrets US

- Publiés sur Twitter, Reddit, 4chan…
- Beaucoup de documents sensibles…
  - Avec « quelques » manipulations dedans comme la modification du nombre de pertes ukrainiennes
- Oh surprise, les USA espionnent leur alliés

https://www.rfi.fr/fr/am%C3%A9riques/20230409-les-%C3%A9tats-unis-enqu%C3%AAtent-sur-des-fuites-de-documents-class%C3%A9s-secrets

Blue Team Les vulnérabilités des fournisseurs de Cloud

- Pas de CVE, déjà corrigées (normalement 😉), impossible à tester/rejouer
  - Exploitée dans la nature ? Aucune idée…
- Référentiel d'une partie de ces vulnérabilités

https://securitylabs.datadoghq.com/cloud-security-atlas/

https://www.cloudvulndb.org/results?q=

Blue Team Suis-je vulnérable à la CVE-2022-47522 ?

- Cette vuln' permet d'intercepter le trafic vers d'autres clients au niveau de la couche MAC
  - Elle bypass l'isolation AP
  - Et bypass également le DAI (Dynamic ARP inspection)
- MacStealer développé pour tester si un client Wi-Fi est vulnérable

https://github.com/vanhoefm/macstealer

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

Blocage d'extensions du côté de OneNote

- 120 extensions de fichiers vont être bloquées
  - Pour limiter l'intégration de fichiers malveillants dans un fichier OneNote
- Dont .vbs, bat, .exe, .ps1, etc.
- Prendra effet dès la version 2304 (prévue pour fin avril 2023) de Microsoft 365, Office >= 2016

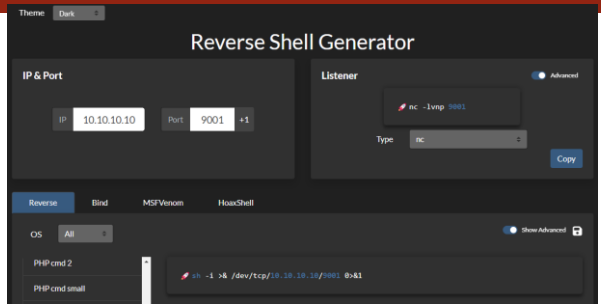
https://support.microsoft.com/en-us/office/blocked-attachments-in-outlook-434752e1-02d3-4e90-9124-8b81e49a8519#:~:text=File%20types%20blocked%20in%20Outlook

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

Red Team Générer vos Reverse Shell en ligne

- Pour tout type d'OS
- nc, pwncat, rustcat, socat, msfconsole, etc. disponibles
- Disponible sur Github

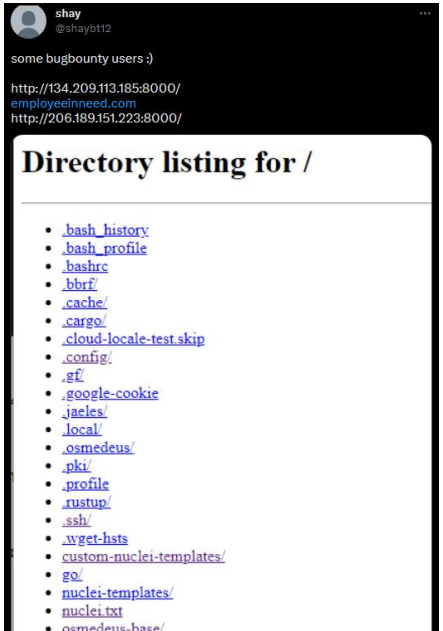
https://www.revshells.com/



Le chasseur de prime… qui se fait chasser

- Publication sur Twitter d'un répertoire ouvert
  - Contenant tous les outils de REDVAULT SECURITY
  - 100% open source
- Twitter == Divulgation Éthique !!?

https://twitter.com/shaybt12/status/1644593596690038784



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

Red Team Exécuter du PS sans être détecté via une archive WinRAR SFX

- Utilisé avec utilman.exe = déploiement d'une backdoor
  - L'archive contient un fichier texte vide qui sert de leurre
  - Ce procédé permet d'abuser les options de configuration de WinRAR et d'exécuter PS
- Technique déjà exploité, alors :
  - Surveillez les comportements des archives SFX
  - Surveillez la clé de registre *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options* (utilisée pour configurer utilman.exe)

https://www.bleepingcomputer.com/news/security/winrar-sfx-archives-can-run-powershell-without-being-detected/

https://socradar.io/hackers-exploit-winrar-sfx-archives-to-install-backdoors-undetected/

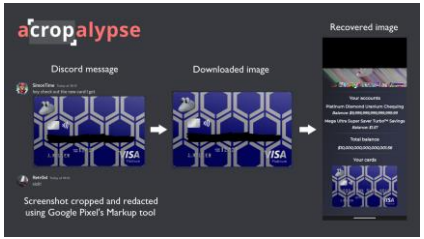
Mots de passe par défaut en CLI

- Recherche en ligne de commande, pratique 😁

https://github.com/ihebski/DefaultCreds-cheat-sheet

C’est l’aCropalypse sur les Google Pixel

- 0-day trouvée sur l’outil d’édition des captures d’écran
  - Poussée par Android Pie en 2018
- Si une image est recadrée depuis cet outil
  - Possible d'afficher la versions **non recadrées** et non modifiées
- Les outils de capture de Windows 10 et 11 partiellement vulnérables
- Suite ?
  - Correctifs disponibles pour Pixel et Windows
  - Certains comme Twitter tronquent déjà automatiquement les images téléchargées



https://github.com/infobyte/CVE-2023-21036 (détecter acropalypse et nettoyer les captures d’écran)

https://securityaffairs.com/143748/hacking/google-pixel-acropalypse-flaw.html

https://issuetracker.google.com/issues/180526528?pli=1

Business et Politique

Business
France

RCCP

- Référentiel de Compétences Cyber pour les Prestataires
  - groupe AFNOR, le Campus régional de Cybersécurité et de Confiance numérique Nouvelle Aquitaine (C3NA) et le Centre de Formation de l'ANSSI (CFSSI)

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillancegouvfr-referentiel-de-competences-cyber-afnor-c3na-cfssi

Business
Monde

Faillite de la SVB

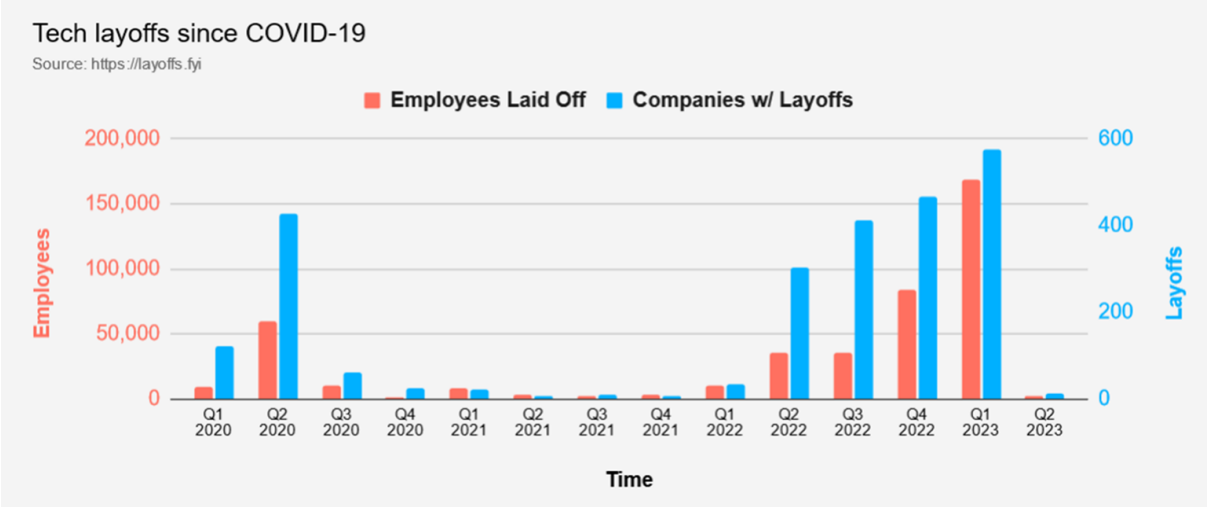
- Silicon Valley Bank
  - En quelques semaines, c'était fini
  - 2ème plus grande faillite bancaire de l'histoire des USA
  - Quid de la Tech Industry et des startups ensuite !!!

https://www.reuters.com/business/finance/svb-financial-seeks-bankruptcy-protection-2023-03-17/

https://www.nelsonmullins.com/storage/iStfJqDLksUfHmp9TXzqi5ASOXUv3LKYQAEuuqrY.pdf

Licenciement de la Tech

- Ça augmente !!!
  https://layoffs.fyi/



Business
Monde

Gandi acheté par Strikwerda Investments

- Gandi, cette perle française (dns, hébergement, vps…)
  - Fusionné avec Total Webhosting, va devenir https://your.online/
- Risque d'augmentation de prix et baisse de qualité

https://www.nextinpact.com/article/71103/gandi-fusionne-avec-total-webhosting-solutions-tws-pour-devenir-your-online-et-cela-inquiete

Free rachète iTrust 😳

- << [...] solution Cyber XPR, seule solution 100 % française à garantir le niveau de protection le plus élevé et la souveraineté totale>> 🤦‍♂️

https://www.clubic.com/connexion-internet/fai-free-box-freebox/actualite-463983-free-se-lance-dans-la-cybersecurite-voila-comment.html

Business
Monde

Sesame IT lève 10m€

- Sonde “Jizo” qualifiée
- Félicitations à toute l’équipe !

https://www.usine-digitale.fr/article/sesame-it-leve-dix-millions-d-euros-pour-sa-solution-de-detection-des-cyberattaques.N2116051

Alcyonie lève 10m€

- Conseil en gestion de crise cyber
- Félicitations à toute l’équipe !

https://alcyconie.com/alcyconie-cyberk1/

Droit / Juridique / Politique
Monde

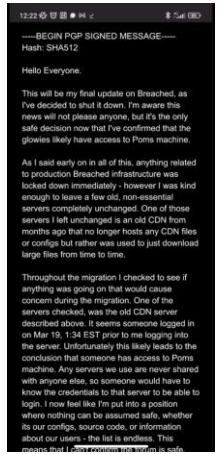
Arrestation de l’administrateur de Breached.to, par le FBI

- Breached.to, remplacant de RaidForums
  - L’admin était un américain : Conor Brian Fitzpatrick, Alias “Pompompurin“
  - Seul chef d’inculpation “préparation pour commettre un délit d’effraction dans un SI“

https://www.lemonde.fr/pixels/article/2023/03/18/cybercriminalite-le-gestionnaire-du-plus-grand-forum-de-vente-de-donnees-volees-arrete-aux-etats-unis_6166040_4408996.html

- Tous les **vendeurs** de “recherche dans le Darknet” en panique

- Admin reprise par “Baphomet” **?**
  - Finalement non, toute la base a été récupérée par le FBI ---------->



https://breached.co/member.php

http://breached65xqh64s7xbkvqgg7bmj4nj7656hcb7x4g42x753r7zmejqd.onion/index.php

Démantèlement de Genesis Market par Interpol

- Arrestation de 119 personnes dans 17 pays (3 en FR)

https://www.lemonde.fr/pixels/article/2023/04/05/europol-demantele-l-une-des-plus-grandes-plates-formes-de-hackeurs-en-ligne_6168391_4408996.html

Droit / Juridique / Politique
Monde

Arrestation des pirates des impôts

- Compromission de 2 000 comptes et remplacement du RIB
  - Avec paramétrage de travaux (isolation…) pour bénéficier de remboursements
- Indices
  - IP suspectes due à des coupures du VPN du cyberdélinquant
  - Le 1er compte à avoir été paramétré pour les remboursements était… celui du complice

https://www.nextinpact.com/lebrief/71324/le-pirate-impots-trahi-par-microcoupures-son-vpn

Droit / Juridique / Politique
Monde

Analyse du contenu des communications (encore…)

- Le retour des projets de loi “à la con” de gens qui n’y connaissent rien
- L'angleterre le tente avec le projet de loi Online Safety Bill

  https://en.wikipedia.org/wiki/Online_Safety_Bill
  - Et Signal ne coopéra pas

    https://www.nextinpact.com/lebrief/71092/signal-pourrait-cesser-fournir-ses-services-dans-pays-sattaquant-au-chiffrement
- L'EU le tente avec une proposition de règlement basé sur l'IA…
  - La fameuse IA magique qui règle tout, désenvoute et apporte la chance au jeu
  - Inefficace et bourré de faux positifs

    https://www.nextinpact.com/article/71104/la-commission-europeenne-veut-surveiller-integralite-web-mails-et-messageries-chiffrees

L'état va devoir limiter le recours aux SSII/ESN et cabinets de conseil

- Ré-internaliser les compétences
  - Réduire les risques de dépendance et perte de maîtrise
- Aurait pu aussi être mis dans la section “Troll”

  https://www.legifrance.gouv.fr/download/pdf/circ?id=45407

Droit / Juridique / Politique
Monde

LPM 2024, déclaration des incidents de sécurité par les éditeurs

- A l'Anssi et aux utilisateurs en France

  https://www.linforme.com/tech-telecom/article/cyberattaque-l-anssi-pourra-exiger-le-blocage-des-sites-sans-passer-par-le-juge_536.html
- L’ANSSI pourra bloquer un nom de domaine lié à une cyberattaque
  - N’aura pas besoin de décision de justice
  - Uniquement un contrôle préalable de l’Arcep sera effectué

  https://www.usine-digitale.fr/article/cyberattaque.N2119866

Droit / Juridique / Politique
Monde

TikTok, plus personne n'en veut

- Selon l'ANSSI tchèque : <<menace pour la cybersécurité>>
  https://www.nextinpact.com/article/71206/lanssi-tcheque-qualifie-tiktok-menace-pour-cybersecurite
- Banni des agences fédérales américaines et canadiennes
  https://www.bfmtv.com/tech/tiktok/la-maison-blanche-ordonne-aux-agences-federales-de-bannir-tik-tok-de-leurs-appareils-d-ici-fin-mars_AD-202302280032.html
  https://www.bfmtv.com/tech/tiktok/apres-les-etats-unis-le-canada-interdit-l-application-tik-tok-sur-les-telephones-gouvernementaux_AD-202302280088.html
- Interdit sur les téléphones des parlementaires européens et employés
  https://www.bfmtv.com/tech/tiktok/apres-la-commission-le-parlement-et-le-conseil-europeen-interdisent-tik-tok-pour-leurs-employes_AV-202303010259.html
- Banni des députés danois
  https://www.bfmtv.com/tech/tiktok/risque-d-espionnage-le-parlement-danois-demande-aux-deputes-de-desinstaller-tik-tok_AD-202302280410.html
- Interdit sur les appareils gouvernementaux (uniquement) au Royaume-Uni
  https://www.lemonde.fr/pixels/article/2023/03/16/le-royaume-uni-interdit-tiktok-sur-les-appareils-gouvernementaux_6165739_4408996.html
- Idem en Australie
  https://www.nextinpact.com/lebrief/71402/les-ministres-australiens-interdits-tiktok-a-leur-tour
- Interdit sur les fournis par l'état français aux agents publics
  https://twitter.com/jnbarrot/status/1639219001459986432
  - N'écoutez pas les incompétents qui n'ont:
    - Jamais vu de vraie flotte mobile (avec ses contournements, ses usages pro sur perso, ses erreurs de conf/durcissement, ses smartphones dépréciés car renouveler une flotte mobile ça coûte cher…)
    - Pas lu la presse ces 10 dernières années (les députés utilisent Telegram…)
      https://twitter.com/ygini/status/1639610969650282496

Droit / Juridique / Politique
Monde

Remontée “éthique” de vuln désormais légalement autorisé en Belgique

- Avant ?
  - Trouver une faille et la signaler -> **interdit**
- Maintenant ?
  - Trouver une faille et la signaler dans les 72 heures -> **autorisé**
  - Hameçonnage, attaques par force brute, DDos, suppression de données, backdoor… -> **interdit**
  - Décrire publiquement une faille découverte -> **interdit**

Un décret qui interdit l'usage de logiciels espions commerciaux

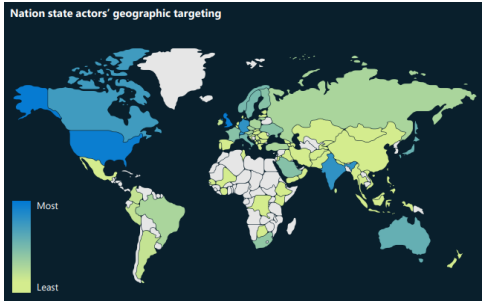
- Interdisant aux agences (fédérales) d'utiliser des logiciels espions commerciaux
  - Type Pegasus de NSO Group
  - Australie, Canada, Costa Rica, Danemark, France, Nouvelle-Zélande, Norvège, Suisse, Suède, Royaume-Uni et États-Unis
- Ces pays “ont” leurs propres capacités offensives (USA en tête)

https://www.nextinpact.com/article/71198/onze-pays-dont-france-sengagent-a-enrayer-proliferation-logiciels-espion-utilises-a-fins-politiques

Publications
Monde

Rapport Microsoft Digital Defense 2022

- 1ère place accordée aux **rançongiciels** (*contrôlés par l'homme*)
  - ⅓ des cibles sont compromises avec succès
  - 5% d'entre-elles reçoivent une demande de rançon
- Le nombre d'attaques de mots de passe a augmenté de 74%
  - 921 attaques / seconde
- 90% des attaques russes détectées visaient des États membres de l'OTAN
- Les secteurs les plus touchés par les attaques étatiques sont :
  - ESN (22%)
  - Think Tank et ONG (17%)
  - Établissements d'enseignement (14%)
  - Gouvernements (10%)



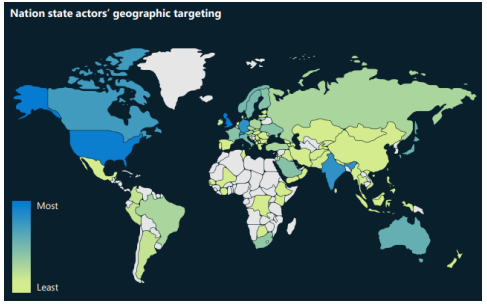
- 52% des entreprises utilisent **peu ou pas du tout de solution EDR**
- L'**IOT ciblé** en masse !
  - 100 millions d'attaques répertoriées en mai 2022 contre les dispositifs de gestion
  - Multiplication x5 par rapport à 2021

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Publications
Monde

Rapport Microsoft Digital Defense 2022

- 1ère place accordée aux **rançongiciels** (*contrôlés par l'homme*)
  - ⅓ des cibles sont compromises avec succès
  - 5% d'entre-elles reçoivent une demande de rançon
- Le nombre d'attaques de mots de passe a augmenté de 74%
  - 921 attaques / seconde
- 90% des attaques russes détectées visaient des États membres de l'OTAN
- Les secteurs les plus touchés par les attaques étatiques sont :
  - ESN (22%)
  - Think Tank et ONG (17%)
  - Établissements d'enseignement (14%)
  - Gouvernements (10%)



- 52% des entreprises utilisent **peu ou pas du tout de solution EDR**
- L'**IOT ciblé** en masse !
  - 100 millions d'attaques répertoriées en mai 2022 contre les dispositifs de gestion
  - Multiplication x5 par rapport à 2021

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Conférences

Conférences

Passée

- JSSI, mardi 14 mars « La transformation de la Cybersécurité »
  https://www.ossir.org/conference/jssi-2023/
- CORI&IN, 5 avril 2023, à Lille
  - En parallèle du FIC
- FIC, 5 au 7 avril 2023, à Lille

A venir

- BotConf, 11 au 14 avril 2023 à Strasbourg #BoufConf / #BouffeConf
- SSTIC, 7 au 9 juin 2023 😎🤩🥳
  - A vos clavier
- Le Hack, 30 Juin au 2 juillet 2023 à Paris
- Pass the Salt, 3 au 5 juillet 2023 à Lille
- Barbhack, ?? aout 2023 à Toulouse

Divers / Trolls velus

Divers / Trolls velus

Découverte de Team Jorge

- Société de désinformation israélienne, avec des capacités de :
  - Créer des comptes sur les réseaux sociaux et populariser des mensonges
  - Soudoyer de vrais journalistes et diffuser des mensonges
- Jorge est en réalité “Tal Hanan”
- Influence de médias français comme BFMTV

https://www.lemonde.fr/pixels/article/2023/02/15/revelations-sur-team-jorge-des-mercenaires-de-la-desinformation-operant-dans-le-monde-entier_6161842_4408996.html

https://www.francetvinfo.fr/monde/story-killers/soupcon-d-ingerence-a-bfmtv-derriere-le-cas-de-rachid-m-barki-l-enquete-story-killers-revele-le-role-d-une-agence-de-desinformation-israelienne_5659016.html

https://forbiddenstories.org/story-killers/team-jorge-disinformation/

Divers / Trolls velus

FIC 2023

- Précédemment…
  - Annulation du Ministère des Armées

    https://www.lalettrea.fr/action-publique_executif/2023/03/01/apres-les-armees-la-gendarmerie-nationale-reconsidere-sa-participation-au-fic,109919190-eve
- Puis…
  - L'ANSSI, Cybermalveillance, Bercy annoncent ne pas aller au FIC

    https://www.nextinpact.com/lebrief/71351/lanssi-renonce-elle-aussi-a-tenir-son-stand-au-forum-international-cybersecurite-fic

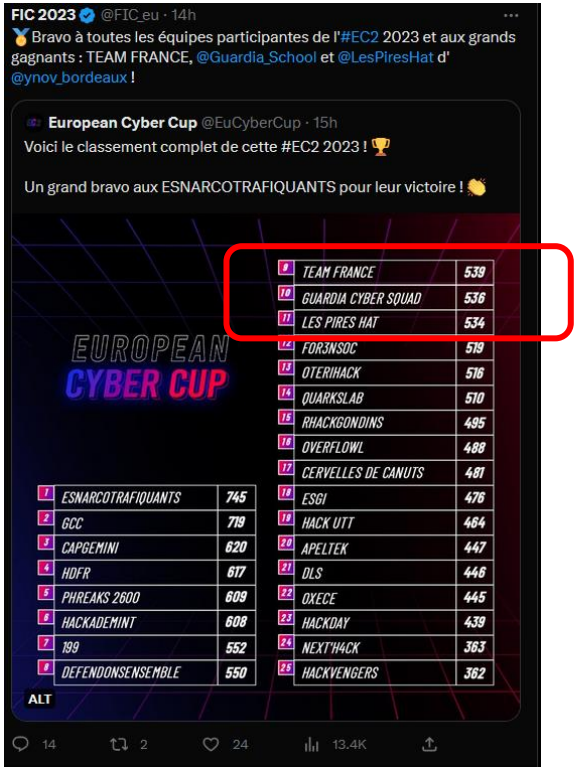
    https://www.lalettrea.fr/action-publique_executif/2023/03/22/les-agents-de-bercy-prives-de-fic,109926355-bre
  - La gendarmerie nationale pourrait ne plus participer au FIC

    https://www.nextinpact.com/lebrief/71131/la-gendarmerie-prendrait-ses-distances-avec-forum-international-cybersecurite
  - L'État boycotte le salon de la cybersécurité

    https://amp-lefigaro-fr.cdn.ampproject.org/c/s/amp.lefigaro.fr/secteur/high-tech/l-etat-boycotte-le-salon-de-la-cybersecurite-20230331

Divers / Trolls velus

FIC 2023, suffit d'être 9eme pour gagner le CTF



https://twitter.com/FIC_eu/status/1644027535846416390

https://twitter.com/LesPiresHat/status/1644083171011747841

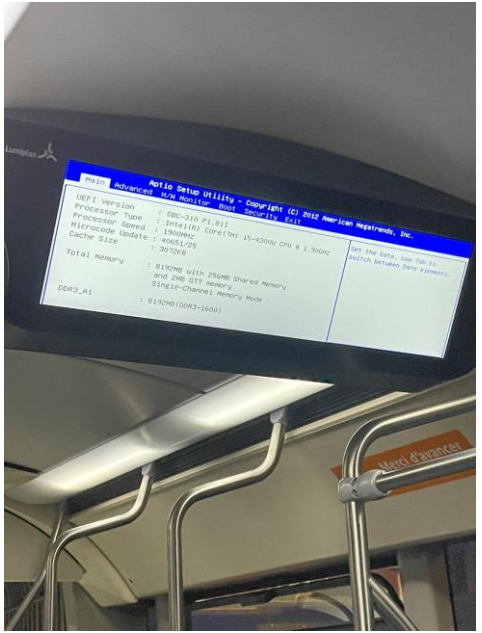
Divers / Trolls velus

Le Campus Cyber, totem de la cyber française…

- Après le partenariat avec le fond d'investissement de la NSA (Paladin Capital Group)
  https://twitter.com/CampusCyberFr/status/1580230774032171013
- Voici le partenariat avec Palo Alto (éditeur israélo-américain)
  https://www.cybersecurite-solutions.com/palto-alto-networks-renouvelle-son-partenariat-avec-le-campus-cyber/

Les ordinateurs dans les bus RATP, anciens mais puissants

- BIOS affiché sur un écran d'informations d'un bus
  - Processeur : Intel Core i5-4300U, cadencé à 1,90 GHz
  - RAM : 8 Go
- Reste qu'à brancher un clavier et une souris (ou 🎮)
  https://twitter.com/gmillour_/status/1635393361703211008/photo/1



Divers / Trolls velus

Ma religion m'interdit Apple et Microsoft

- Une nouvelle embauchée demande à n'utiliser que Linux
  - Que feriez vous ?

https://www.reddit.com/r/sysadmin/comments/11g9y9q/ga_employee_claims_she_cant_use_microsoft_windows/

Apple, vous avez pensé à mettre à jour vos câbles ?

- Mise à jour du firmware des câbles USB-C des MacBook M2

https://www.macworld.com/article/1514105/macbook-air-pro-magsafe-cable-firmware-update.html

Wi-R, l'antenne c'est vous !

- Exploite les champs électro quasi statiques (EQS)
  - Portée jusqu'à 5 mètres (avec conducteur)
  - Bande passante jusqu'à 1Mb/s
  - Consomme 100 fois moins par rapport au Wi-Fi et au Bluetooth

https://www.generation-nt.com/actualites/wi-antenne-wifi-bluetooth-2033439

https://www.ouest-france.fr/leditiondusoir/2023-02-16/qu-est-ce-le-wi-r-cette-alternative-au-bluetooth-qui-utilise-notre-corps-comme-une-antenne-33cc373e-7583-4981-948b-1f786f2b9416

Divers / Trolls velus

Plus de Cloud, plus de NAS Western Digital chez toi !

- Panne du portail d'authentification de Western Digital
  - Plus possible d'accéder à son NAS, chez soi… sur son réseau… dans son appart 🙅‍♂️

https://www.itpro.co.uk/security/cyber-attacks/370369/western-digital-suffers-cyber-attack-shuts-down-systems

- Rappelez vous en 2020, panne du Cloud AWS = plus d'aspirateur ni de sonnette

https://www.bbc.com/news/technology-55087054

Vidéo des Tesla échangées entre salariés

- Après le partage des vidéos des aspirateurs robots…
- Les salariés de Tesla s'échangeaient les vidéos prises par les voitures
  - Dont des accidents
  - Et le garage d'Elon Musk

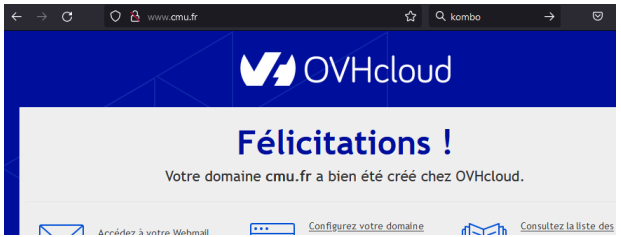
https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/

Divers / Trolls velus

Qui veut faire de l'hameçonnage facile ?

- CMU remplacé par CSS (Complémentaire santé solidaire)
  - **cmu.fr** remplacé par **complementaire-sante-solidaire.gouv.fr**
  - **cmu.fr** non renouvelé…

https://twitter.com/canardenchaine/status/1628377573452402689



Divers / Trolls velus

News autour de GPT-4 ?

- Microsoft va intégrer GPT-4 dans Microsoft 365

  https://www.lemonde.fr/pixels/article/2023/03/16/microsoft-annonce-l-integration-de-la-technologie-gpt-4-dans-ses-outils-word-excel-outlook-et-teams_6165789_4408996.html
- GPT-4 manipule un humain pour résoudre un test CAPTCHA

  https://www.numerama.com/tech/1306066-gpt-4-a-persuade-un-humain-de-resoudre-un-test-captcha-pour-lui.html
- Le nom de ChatGPT sur Bing est Sydney (mais fallait pas le dire)

  https://www.numerama.com/tech/1267298-bing-avec-chatgpt-est-trop-bavard-il-devoile-son-vrai-nom-et-ses-consignes-secretes.html
- Microsoft Security Copilot, l’assistant cybersécurité from Microsoft

  https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot

  https://thehackernews.com/2023/03/microsoft-introduces-gpt-4-ai-powered.html

Divers / Trolls velus

Troll “master class”

- Un commercial de Sophos pavane
  - Profitant d’un drame cyber au CHU Saint-Pierre (Belgique) 🤬
- Le DSI le recadre
  - Le CHU “avait” Sophos

Stephane Odent · 3rd+ — + Follow
CIO at CHU Saint-Pierre
23h ·

L’occasion fait le larron…. Bravo Sophos! En tout cas leur antivirus ne nous a pas protégé et nous plombe sérieusement…

Ceci dit, il faut en effet prendre la cybersécurité très au sérieux et se protéger contre une menace grandissante et de plus en plus agressive et efficace.

See translation

Karim Boudekhan · 3rd+ — + Follow
Enterprise Account Manager
BELUX SOPHOS
5d ·

N'attendez pas qu'il soit trop tard!
Encore un hospital qui est la cible de cyberattaques.

Le CHU Saint-Pierre de Bruxelles a fermé son service d'urgence due à une cyberattaque 🔥🔥🔥.

Avec nos solutions et services de Sophos, cette attaque aurait été neutralisée par notre équipe d'experts dédiée.

Managed Detection and Response fournit des résultats supérieurs en matière de cybersécurité. Sophos Managed Detection and Response est un

Most relevant

Stephane Odent · 2nd — 1d
CIO at CHU Saint-Pierre

Pour ajouter du piment à cette histoire, Karim Boudekhan a fini par trouver mon adresse e-mail et m'a proposé les services du rapid response team, 7 jours après l'attaque 🤔 Heureusement qu'on ne les ... ...see more

See translation

Like · 74 | Reply · 18 Replies

Load previous replies

Le Top arbitraire de l’année écoulée

Version sous forme d’article de blog : https://patrowl.io/blog-le-top-arbitraire-de-lannee-ecoulee-2022-2/

Divers / Trolls velus

Le voici… enfin…

- Avec un très léger retard (de 2,5 mois)
- Il sent l'odeur des **larmes séchées** 😢 de RSSI vaporisées par la chaleur des **détonations** de **vulnérabilités** 💥

Il répond à LA grande question :

- Qu'est ce qui a caractérisé l'année 2022 ?

Divers / Trolls velus

2022, à nouveau une année des vulnérabilités majeures ?

- Nouvelles manières d'exploiter **Log4J** (cf. revue du 2022-01-11 et 2022-02-08)
- **Spring4Shell**, injection de code Java (CVE-2022-22963, cf. revue du 2022-04-12)
- Vulnérabilités majeures chez les fournisseurs de Cloud :
  - **AWS** CloudFormation (cf. revue du 2022-02-08).
  - **Azure** Automation Account, permettant de récupérer les jetons des autres clients (cf. revue du 2022-03-08)
- **ProxyNotShell**, que Microsoft aura mis 3 mois à corriger (cf. revue du 2022-10-11)
- **Zimbra** pris pour cible avec des exploitations de 0-days (cf. revue du 2022-02-08, 2022-07-12, 2022-09-13, 2022-10-11)

Divers / Trolls velus

2022, toujours une année de vulnérabilités sur les CPU ?

- **SQUIP** / Side Channel Vulnerability, touchant les CPU AMD Zen 1, 2 et 3 (cf. 2022-09-13)
- **AEPIC** Leak / Architecturally Leaking Uninitialized Data from the Microarchitecture, touchant les CPU Intel de 10eme, 11eme et 12eme generation (cf. 2022-09-13)
- **RetBleed**, touchant les CPU Intel et AMD (cf. 2022-09-13)
- **Phantom JMPS**, touchant les CPU Intel et AMD (cf. 2022-09-13)
- **PACMAN**, touchant les CPU Apple M1 (cf. 2022-09-13)

Divers / Trolls velus

2022, l'année de la fin des compromissions de poste de travail à cause des macros Office ?

- Macros Office sont désactivées par défaut
  - Annoncé en février (cf. revue du 2022-02-08)
  - Rocambolesque série de blocages et de retours en arrière
- Mais il reste beeeaaauuucoup de techniques
  - DDE
  - Schémas d'appel (ms-msdt://)
  - XLL
  - OneNote
  - Chaines improbables (url > .zip > .iso > .lnk > .bat > .dll)

Divers / Trolls velus

2022, toujours et encore une année des compromissions des chaînes d'approvisionnement (supply chain) ou fournisseurs ?

- StellarParticle et CozyBear, piratage de services/applications exposés sur Internet, accès au tenant Azure, vol de cookie pour contourner les MFA… (cf. revue du 2022-02-08)
- Serpent, ciblant des entreprises et ministères français (cf. revue du 2022-04-12)
- Le piratage de CircleCI et vol de TOUS les secrets de TOUS les clients (cf. revue du 2023-01-10)
- Les réseaux GSM espionnés par un groupe Chinois utilisant « Poison Ivy » (cf. revue du 2022-04-12)
- Twilio permettant ensuite aux attaquants de compromettre des comptes Signal, Okta, Telegram… (cf. revue du 2022-09-13)
- Bug bounty HackerOne avec des salariés contrefaisant des rapports pour voler et revendre les vulnérabilités (cf. revue du 2022-07-12)

Divers / Trolls velus

2022, la continuité du piratage des interfaces d'administration exposées sur Internet, en général sur des solutions de sécurité ?

- Piratage de firewall et VPN **WatchGuard** par Cyclops Blink (Sandworm) (cf. revue du 2022-03-08)
- Piratage en masse de firewall **Fortinet** (cf. revue du 2022-11-08)
- Contournement de l'authent sur le portail d'admin des **Palo Alto** (CVE-2022-0030)
- Prise de contrôle des VPN SSL **SonicWall** par une requête web triviale (cf. revue du 2022-02-08)
- Injection de code à distance et sans authent sur les **F5 BigIP** (cf. revue du 2022-06-14)
- Injection de commande à distance et sans authent sur les firewalls **Zyxel** par une simple requête POST avec un JSON (CVE-2022-30525) (cf. revue du 2022-06-14)
- Exécution de code à distance et sans authent sur les firewalls **Sophos** par une simple requête POST avec un caractère unicode (CVE-2022-1040) (cf. revue du 2022-06-14)
- Nombreuses vulnérabilités critique sur les solutions de **Palo Alto** comme l'XDR **Cortex** (cf. revue du 2022-02-08)
- **Manage Engine** avec des vulns triviales comme la prise de contrôle par une simple requête web (CVE-2021-44515) (cf. revue du 2022-02-08)

Divers / Trolls velus

2022, année des vulns critiques similaires à celles des années 2000 ?

- Atlassian Confluence, injection de commande à distance sans authent (CVE-2022-26134) (cf. revue du 2022-06-14)
- Atlassian **Confluence**, encore un compte caché avec un mot de passe en dur (cf. revue du 2022-10-11)
- Atlassian **Jira**, injection de requête web (SSRF) triviale (CVE-2022-26135) (cf. revue du 2022-07-12)
- **GitLab**, mot de passe en dur « 123qweQWE!@#00 » pour l'authent externe (cf. revue du 2022-02-08)
- **Grafana** 8.4.3, lecture arbitraire de fichier avec un path traversal trivial (CVE-2022-32275) (cf. revue du 2022-06-14)
- **Apache**, lecture et écriture arbitraire de mémoire datant de… 20 ans (cf. revue du 2022-09-13)
- **pfSence**, exécution triviale de commande sans authentification (cf. revue du 2022-10-11)
- **GLPI**, injection triviale de commande (cf. revue du 2022-11-08)

Divers / Trolls velus

2022, la confirmation que les cybercriminels n'ont pas d'âme ?

- L'hôpital Corbeil-Essonnes, bloquant tout le système d'information (cf. revue du 2022-09-13)
- Le Département Indre et Loire, créant des problèmes sur les versements des allocations (cf. revue du 2022-09-13)
- Hôpital de Castelluccio à Ajaccio qui a bloqué des services critiques (cf. revue du 2022-06-14)
- Groupement hospitalier de la région Grand Est (GHT Cœur Grand Est) avec le vol de données de patients (cf. revue du 2022-06-14)
- Groupements d'Intérêt Public (cf. revue du 2022-06-14)
- Hôpital Corbeil-Essonnes (cf. revue du 2022-09-13)

Rassurez-vous, le groupe LockBit s'est excusé suite à la compromission d'un hôpital d'enfants au Canada 🤦‍♂️ (cf. revue du 2023-01-10)

Divers / Trolls velus

2022, une année de la reprise des codes de la « startup nation » par les cybercriminels ?

- **LockBit** a annoncé :
  - Un programme de **bugbounty**
  - Un programme de rachat de vulnérabilités
  - Des partenariats
  - Du recrutement… (cf. revue du 2022-07-12)

Divers / Trolls velus

2022, une année surprenante avec des attaquants de 16 ans utilisant des techniques basiques !!?

- **Lapsus$**, piratage de :
  - **Nvidia** et sorti 1To de données, les comptes de l'AD avec condensat NTLM… (cf. revue du 2022-02-08)
  - **Samsung** et sorti 200Go de données dont des codes source sensibles (cf. revue du 2022-02-08)
  - **Microsoft** et la sorti de beaucoup de code source dont Bing mais coupé rapidement car le groupe a annoncé la fuite en temps réel (cf. revue du 2022-04-12)
  - Mais aussi **Ubisoft**, **Okta**, **Uber**, **Rockstar…**

Divers / Trolls velus

2022, une année confirmant que oui, un antivirus et un EDR, cela se contourne ?

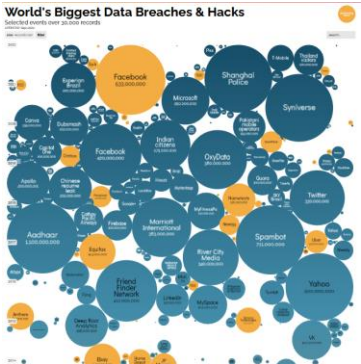
- Toutes les semaines, des techniques de contournement sont publiées

Divers / Trolls velus

2022, encore une année de vols de données, publications de fuites de données… ?

- Literies **Emma**, vol des informations de 97 000 clients (cf. revue du 2022-04-12)
- Base de données de 1 Milliards de **Chinois** venant de leur police avec des données personnelles et leur casier (cf. revue du 2022-07-12)

- Base de données des clients la **Poste Mobile**, publiée par Lockbit (cf. revue du 2022-07-12)
- Base de données des utilisateurs de **TikTok** (cf. revue du 2022-09-13)
- Liste de tous les clients du micro-SOC d'**Orange CyberDefense** (cf. revue du 2022-09-13)
- Données **d'Altice** et enquêtes de journalistes sur la famille Drahi (cf. revue du 2022-09-13)
- Base de données de 5,4 millions d'utilisateurs de **Twitter** + n° de gsm (cf. revue du 2022-09-13)
- Base de données de 233 millions d'utilisateurs de **Twitter** (cf. revue du 2023-01-10)
- Base de données de 257 millions d'utilisateur de **Deezer** (cf. revue du 2023-01-10)



https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Divers / Trolls velus

2022, une nouvelle année de collecte de vos données personnelles, sans limite ?

- Cisco **WebEx** vous écoutait même quand le micro est coupé (cf. revue du 2022-06-14)
- Les **iPhones** ne s'éteignaient jamais « Evil never sleeps » (cf. revue du 2022-04-12)
- Les photos intimes prises par des **aspirateurs robots** sont sorties sur Facebook (cf. revue du 2023-01-10)

Divers / Trolls velus

2022, une année rassurante avec de nombreuses saisies, arrestations et sanctions ?

- Beaucoup d'amendes
  - L'annonce que **Google Analytics** n'était pas conforme au RGPD (cf. revue du 2022-04-12)
  - La condamnation de **Dedalus** Biologie à une amende de 15m€ (cf. revue du 2022-06-14)
  - Les multiples amendes contre **ClearView AI** (7,5 m£ en Angleterre ; 20m€ en Italie ; mise en demeure en France) (cf. revue du 2022-06-14)
  - Amende de 390m€ contre **Meta** par la CNIL Irlandaise (cf. revue du 2023-01-10)
  - Amende de 8m€ contre **Apple** pour traçage publicitaire (cf. revue du 2023-01-10)
- Arrestations
  - RaidForums ainsi que nulled.to et eleaks mais rapidement remplacés (cf. revue du 2022-03-08)
  - Emotet
  - Place de marché Hydra (Dmitry Pavlov) (cf. revue du 2022-06-14)
  - Auteur de Raccoon Stealer, grâce aux publications Instagram de sa copine (cf. revue du 2022-11-08)
  - Arnaqueurs au CPF a été arrêté (cf. revue du 2022-12-08)
  - Le RSSI de Uber condamné pour avoir caché une compromission importante et payé la rançon avec le bidget du big bounty

Divers / Trolls velus

2022, une année florissante pour les fusions, rachats et levées de fond en cybersécurité ?

- Côté rachats :
  - NeoSoft a acquis **CONIX** (cf. revue du 2022-03-08)
  - Google a acquis **Mandiant** pour $5Mds (cf. revue du 2022-03-08)
  - Schwarz Group a acquis **XM Cyber** pour $700 millions
  - Framatome a acquis **Cyberwatch** (cf. revue du 2022-06-14)
  - IBM a acquis **Randori** (!=RandoriSec) (cf. revue du 2022-06-14)
  - UnaBiz (Singapour) a acquis le français **Sigfox** et conservé 110 salariés sur 174 (cf. revue du 2022-06-14)
  - Broadcom a acquis VMware (cf. revue du 2022-06-14)
  - Thales a acquis S21sec et Excellium (Luxembourg) (cf. revue du 2022-06-14)
  - Orange Cyber Défense a racheté les entreprises Suisses SCRT et Telsys (cf. revue du 2022-12-08)

- Côté levées :
  - Patrowl a levé 2m€ en seed 🍼🐣
  - Thetris a levé 44m€ (cf. revue du 2022-11-08)
  - Citalid a levé 12m€ (cf. revue du 2022-11-08)

Divers / Trolls velus

2022, l'année des succès de la France en cyber ?

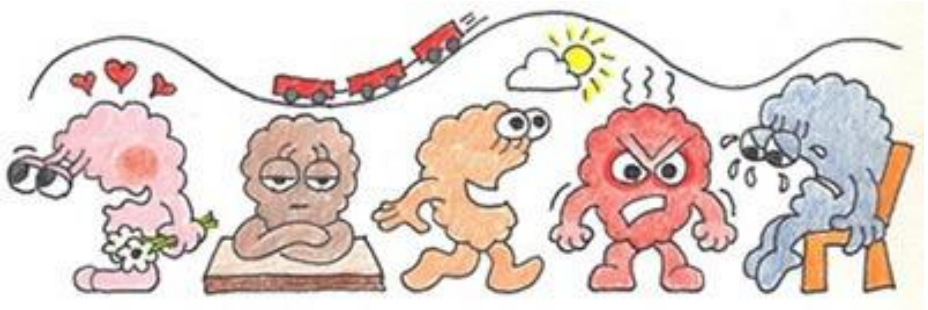
- Synacktiv, succès lors de compétitions internationales comme les Pwn2Own, Pwn2Own Vancouver (cf. revue du 2022-02-08, du 2022-04-12)
- Outils français = références mondiales :
  - **ADeleg**, pour auditer vos délégations Active Directory (cf. revue du 2022-06-14)
  - **CrackMapExec**, pour auditer vos systèmes d'information interne, avec des mises à jour dingues quasiment tous les mois
  - **PingCastle**, toujours présent, toujours la référence pour analyser la sécurité de votre Active Directory

Divers / Trolls velus

2022, l'année du grand débat concernant les assurances cyber ?

Ascenseur émotionnel d'annonces *(ou montagnes russes émotionnelles pour coller avec l'illustration)*:

- **L'AMRAE**, qui a annoncé que l'assurance cyber pourrait disparaître (cf. revue du 2022-02-08)
- **Générali** qui a annoncé ne pas rembourser les rançons (cf. revue du 2022-02-08)
- La **Lloyd**, pas de remboursement pour les victimes d'attaques étatiques (cf. revue du 2022-09-13)
- Mais… **Bercy** veut autoriser l'indemnisation des rançons, sous condition (cf. revue du 2022-09-13)



Divers / Trolls velus

2022, la confirmation que non, le cloud n'est pas exempt de pannes majeures ?

- **AWS**, impactant impactant Twitch, Zoom, Playstation Network, Xbox Live, Hulu, League of Legends… (cf. revue du 2022-01-11)
- **Atlassian** efface les données de 400 clients suite à une mauvaise manipulation (cf. revue du 2022-06-14)
- **CloudFlare**, passe touchant 19 dataceners pendant 1h20 à cause d'une erreur BGP et non DNS (cf. revue du 2022-07-12)
- Microsoft **Teams**, avec une incapacité à faire tourner le service (cf. revue du 2022-09-13)
- **Google** UK, à cause de la chaleur de l'été (cf. revue du 2022-09-13)
- **Azure**, à cause de DNS (cf. revue du 2022-09-13)

Divers / Trolls velus

Excellente année 2023 et… bonnes fêtes de Pâques 🤣

- 2023, l'année des réponses des textes et images…
  - générées par « deep learning » ?
  - Au top de la **kalitéy**

Prochaines réunions

Prochaine réunion

- Mardi 9 mai

After Work

- Euh… un after-quoi !!?
- Si vous avez des adresses de bars, contactez nous
  - Vidéo projecteur
  - Possibilité de privatiser
  - Bière + buffet campagnard 😁

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées

- Contactez-nous