Revue d'actualité de l'OSSIR

11 juillet 2023

Christophe Chasseboeuf
*Vladimir Kolla @mynameisv_*
Jérémy De Cock

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de juin 2023, 78 😨 vulnérabilités, dont :

- Exploitées dans la nature :
  - Elévation de privilèges dans **SharePoint** (CVE-2023-29357)
    - Peut être chainé avec une autre vulnérabilité pour contourner l'authentification
- Les plus critiques ou les plus intéressantes
  - Exécutions de code à distance sur le service multicast **PGM** (RFC 3208) (CVE-2023-29363, CVE-2023-32014 et CVE-2023-32015)
    - En lien avec Microsoft Message Queuing (MSMQ)
    - cf. MS08-036 pour PGM
  - Executions de code à distance sur **.Net** (CVE-2023-24897, CVE-2023-24895, CVE-2023-33126, CVE-2023-33128)
  - Exécution de code à la lecture d'une **vidéo** (CVE-2023-29370)

Failles / Bulletins / Advisories
Microsoft - Divers

Les signatures de fichier OOXML (Office) sont cassées

- Juste en ajoutant un sig1.xml dans l'archive, le fichier est considéré comme signé
- Et sinon, il y'a plusieurs autres méthodes

https://www.theregister.com/2023/06/13/office_open_xml_signatures/

Teams, envoie de malware depuis des comptes externes

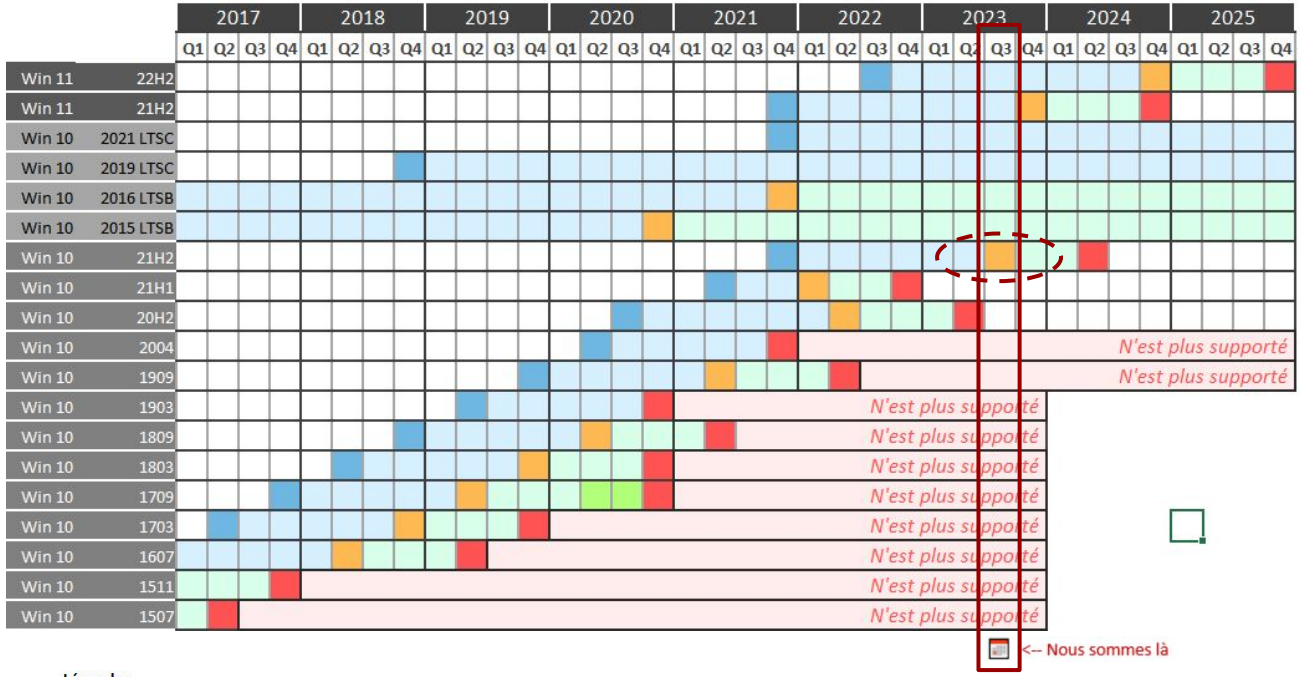
- Si la configuration n'a pas été durcie (et autorise les communications externes)
- Modification des identifiants "dans" la requête POST
  - Le fichier est stocké dans le SharePoint de la cible
- Pas un problème urgent selon Microsoft

https://labs.jumpsec.com/advisory-idor-in-microsoft-teams-allows-for-external-tenants-to-introduce-malware/

https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/microsoft-teams-bug-allows-malware-delivery-from-external-accounts/amp/

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

StackRot, une faille sur le noyau Linux

- CVE-2023-3269 (CVSS 7.8)
  - Vulnérabilité autour du sous-système qui gère la mémoire
  - Privesc possible 🪜
- Version 6.1 à 6.4 affectées
  - Debian 12 tourne actuellement sur la 6.1

https://github.com/lrh2000/StackRot

Snap-confine, élévation locale de privilèges (CVE-2021-44731)

- Installé par défaut sur Ubuntu
- “Race condition”

https://github.com/deeexcee-io/CVE-2021-44731-snap-confine-SUID/blob/main/snap_confine_LPE.sh

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

Plugin WordPress: WooCommerce, fuite des commandes (CVE-2023-34000)

- Avec Stripe Payment Gateway (CVSS 7.5)
  - Permet de récupérer le détail des commandes passées par ce plugin
  - Sans nécessité d'être authentifié !
- Faille qui affecte toutes les versions < 7.4.1

https://nvd.nist.gov/vuln/detail/CVE-2023-34000

Plugin WordPress: ultimate member (CVE-2023-3460)

- Accès admin sans authentification

https://github.com/gbrsh/CVE-2023-3460/blob/main/exploit.py

Nombreuses vulnérabilités sur la plateforme d'e-learning Chamilo

- Injection de commande, SSRF, XSS…
- Bravo à RandoriSec

https://www.randorisec.fr/chamilo-1.11.18-multiple-vulnerabilities

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

OpenFire, contournement de l'authentification de la console d'admin (CVE-2023-32315)

- Juste en manipulant l'URL de création d'un utilisateur
- OpenFire = serveur Jabber/XMPP

https://github.com/izzz0/CVE-2023-32315-POC/blob/main/main.py

Vulnérabilité nOAuth

- Prise de contrôle du compte de la cible via son mail ! (et OAuth mal implémenté)
  - Identification via le mail (mutable et non vérifié) + Azure AD OAuth multi-tenants = 💣
- Beaucoup d'applis vulnérables : à la première position… Grafana (CVE-2023-3128)

https://www.descope.com/blog/post/noauth (article des chercheurs + démo)

https://www.it-connect.fr/vulnerabilite-dans-grafana-mettez-a-jour-des-que-possible-si-vous-utilisez-lauthentification-azure-ad/ (explication de la CVE Grafana + liste des versions patchées)

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

MOVEit, injection SQL (CVE-2023-35708)

- https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023

MOVEit, encore des vulnérabilités (CVE-2023-36934 , CVE-2023-36932, CVE-2023-36933)

- SQLi pre-auth

https://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023

Failles / Bulletins / Advisories
Réseau (principales failles)

RCE sur les routeurs ASUS

- **Nouveau firmware disponible** depuis le 06/19/2023
- Ce dernier corrige 9 failles de sécurité dont
  - CVE-2022-26376 : corruption de mémoire dans le firmware Asuswrt entraînant une RCE
  - CVE-2018-1160 : faiblesse dans l'implémentation de Netatalk entraînant une RCE
- Une dizaine de routeurs Wi-Fi et systèmes Wi-Fi Mesh impactés
- **Mettez à jour** ou sinon désactivez les services accessibles depuis le WAN !

https://www.asus.com/content/asus-product-security-advisory/

Cisco Nexus 9000 (en mode ACI)

- Lecture et Modification des flux inter-site chiffrés (si MitM)
  - Pas de correctif prévu, merci de vous débrouiller tout seul 😲
  - <<Cisco has not released and will not release software updates>>
- ACI = solution de SDN de Cisco

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX

Failles / Bulletins / Advisories
Réseau (principales failles)

Fortinet FortiNAC, RCI pre-auth (CVE-2022-39952)

- Injection de commande sans authentification

https://frycos.github.io/vulns4free/2023/06/18/fortinac.html

Fortinet VPN SSL, RCE (CVE-2023-27997)

- Cf. revue de juin
- Exploitée dans la nature
  - Si vous n'avez pas mis à jour… dépêchez vous
  - Et investiguez !

https://www.theregister.com/2023/06/12/fortinet_fixes_critical_rce_bug/

Zyxel, RCI pre-auth (CVE-2023-27992)

- Injection de commande sans authentification
  - Zyxel doit surement faire un concours avec Fortinet

https://thehackernews.com/2023/06/zyxel-releases-urgent-security-updates.html

Failles / Bulletins / Advisories
Autre (principales failles)

Vulnérabilités macOS et iOS exploitées dans la nature

- CVE-2023-32439 et CVE-2023-32435, exécution de code dans Safari
- CVE-2023-32434, élévation locale de privilèges
- Impactés :
  - iOS 16.5 => iOS 16.5.1 https://support.apple.com/en-us/HT213814
  - iOS 15.7.6 => 15.7.7 https://support.apple.com/en-us/HT213811
  - iPasOS 16.5 => iOS 16.5.1 https://support.apple.com/en-us/HT213814
  - iPadOS 15.7.6 => 15.7.7 https://support.apple.com/en-us/HT213811
  - macOS Ventura 13.4 => 13.4.1 https://support.apple.com/en-us/HT213813
  - macOS Monterey 12.6.6 => 12.6.7 https://support.apple.com/en-us/HT213810
  - macOS Big Sur 11.7.7 => 11.7.8 https://support.apple.com/en-us/HT213809

Encore une vulnérabilité macOS et iOS (Safari)

- CVE-2023-37450, exécution de code dans Safari
- Mise à jour Rapid Security Response (RSR) de 2,7mo
- Impactés :
  - iOS 16.5.1 et iPadOS 16.5.1 => iOS 16.5.1(a) https://support.apple.com/en-us/HT213823
  - macOS Venture 13.4.1 => 13.4.1(a) https://support.apple.com/en-us/HT213825

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Global CyberAttacks in the US

- MOVEit plateforme attaquée le 28 mai
- Vague de cyberattaques aux USA
- Exposition Louisiana, Oregon, …

https://edition.cnn.com/2023/06/29/politics/us-health-department-cyberattack/index.html

'Toitoin' Campaign

- Chaîne d'infection en plusieurs étapes
- Cible : Amazon EC2

https://edition.cnn.com/2023/06/29/politics/us-health-department-cyberattack/index.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages

#BlackCat / #ALPHV

- Passage par du “Malverting”
- Dernière cibles :
  - Barts Health NHS Trust (UK)
  - Bangladesh Krishi Bank

https://heimdalsecurity.com/blog/massive-data-breach-affects-uk-hospital-group/

https://www.trendmicro.com/en_us/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-lever.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0723_IRMalvertisement-TW

https://twitter.com/ido_cohen2/status/1678413187857670153

https://izoologic.com/2023/07/10/alphv-strikes-bangladesh-krishi-bank-with-a-massive-data-breach/

TOP TARGETED COUNTRIES:
USA: 43
Canada: 5
UK: 3
Colombia: 3
Netherlands: 2
Australia: 1

TOP ACTIVE GROUPS:
-CLOP: 56
-Play: 36
-Lockbit: 19
-Akira: 17
-**BlackCat**: 15
-8Base: 14

Total Victims: 88

Hits Map:

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Cyberattaque au CHU de Rennes

- Potentielle exfiltration de données dû à un compte VPN SSL d'un prestataire
  https://www.usine-digitale.fr/article/le-chu-de-rennes-victime-d-une-cyberattaque-des-donnees-derobees.N2146632

Cyberattaque au CHU de Brest

- Le retour d'expérience dans le prochain NoLimitSécu 😁

TSMC piraté par Lockbit

- Compromission par un sous-traitant/fournisseur (Kinmax)
  https://techcrunch.com/2023/06/30/tsmc-confirms-data-breach-after-lockbit-cyberattack-on-third-party-supplier/

Kromsec annonce avoir piraté des données du ministère français de la justice

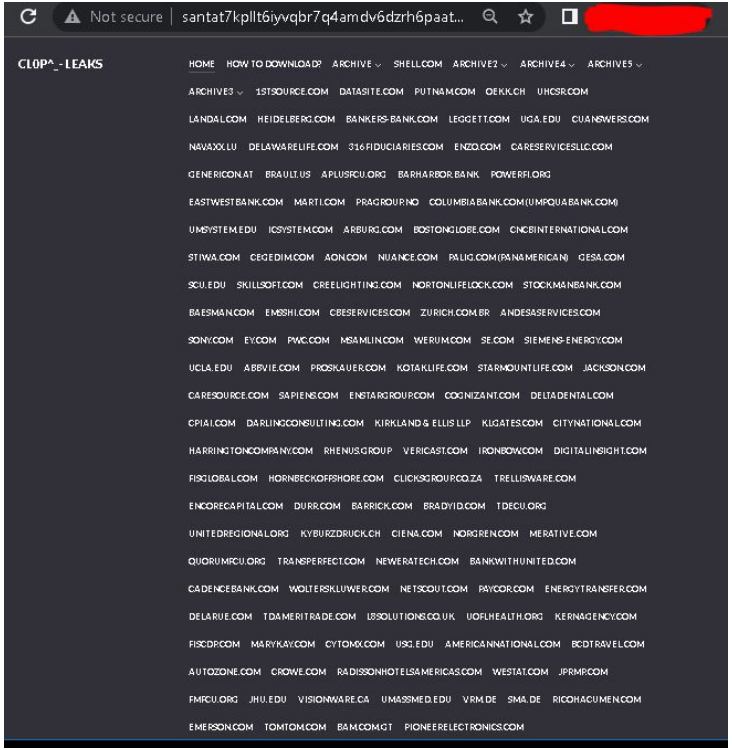
- Le ministère réfute
- Les captures d'écran font penser à un backup, un sous-traitant, un gros cabinet d'avocats…
  - Dont les données liées à l'affaire Nahel

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Cl0p publie une liste de 231 victimes

- Qui ont refusé de payer
- Dont beaucoup aux USA

https://twitter.com/vxunderground/status/1677442776105975808



DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

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

Leak de 101 000 comptes ChatGPT

- Etude menée par Group-IB
  - 100k logs de malwares info-stealer
  - 101k comptes volés entre juin 2022 et mai 2023
  - ~ Environ 45% en provenance d'Asie
- Historique important et critique quand on sait l'usage qui est fait avec l'outil

https://www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials/

Piratages, Malwares, spam, fraudes et DDoS
DDoS

DDoS contre Blizzard

- Panne des services de Diablo IV

  https://twitter.com/BlizzardCS/status/1673082677115666440

  https://eu.battle.net/support/en/article/99037

- Infographie de l'ANSSI sur les DDoS

  https://www.ssi.gouv.fr/uploads/ddos_infographie_anssi.pdf

DDoS contre Microsoft et panne de Microsoft 365

- Attaque niveau 7 par "Storm-1359"

  https://www.theregister.com/2023/06/19/microsoft_365_outage_ddos_cause/

Piratages, Malwares, spam, fraudes et DDoS
Publication

TOP (2)5 faiblesses logicielles MITRE 2023

Rang	ID	Nom	Score	CVE connues	Range en 2022
1	CWE-787	Out-of-bounds Write	63.72	70	0
2	CWE-79	Cross-site Scripting	45.54	4	0
3	CWE-89	SQL Injection	34.27	6	0
4	CWE-416	Use After Free	16.71	44	+3
5	CWE-78	OS Command Injection	15.65	23	+1

https://cwe.mitre.org/top25/

Piratages, Malwares, spam, fraudes et DDoS
Pirater les pirates

Près de 6% des transactions Monero sont désanonymisables

- Erreur dans l'algorithme de mixage
  - Mixage non réalisé tous les 10 blocs

https://www.cointribune.com/une-faille-de-confidentialite-sur-monero/

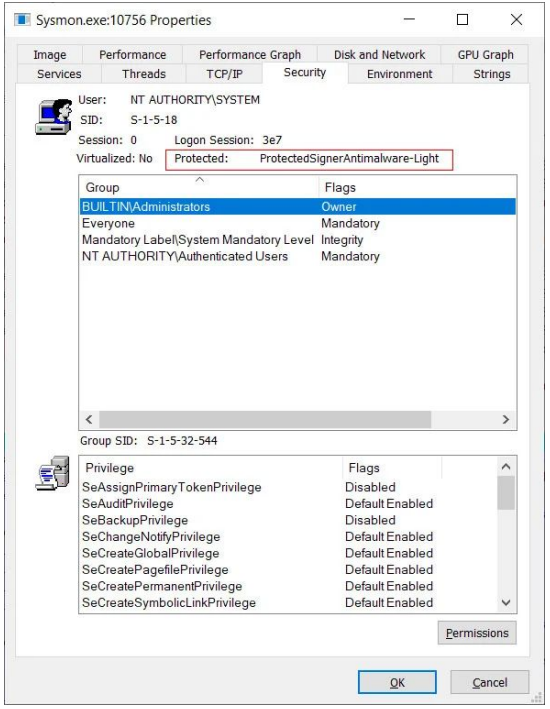
Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Blue Team Nouvelle version de Sysmon !

- **Sysinternals**, la boîte à outils INCROYABLE fournie par Microsoft
  - DebugView (affiche l'information de débogage)
  - ProcessMonitor (affiche les processus et les logiciels en cours)
  - PsExec (remplacement de Telnet pour l'exécution à distance)
  - Et beaucoup d'autre…
- Deux fonctionnalités importantes avec le passage à la **version 15**
  - 1) Exécution de Sysmon dans un processus protégé ---------->
  - 2) Détecter les nouveaux fichiers exécutables

https://live.sysinternals.com/ (liste des outils présents dans sysinternals)

https://github.com/Sysinternals (sysinternals en projet open-source pour Linux)



Blue Team Snappy, l'ennemi des rogue AP

- Permet d'identifier une usurpation d'@MAC et de SSID
  - Calcule l'empreinte SHA256 d'un AP à un instant T
  - Empreinte différente à T+1 → Rogue AP
- Développé en Python

https://github.com/SpiderLabs/snappy

Nouvelle version de crackmapexec 6.0.0

- Dump DPAPI
- Collecte Bloodhound
- …

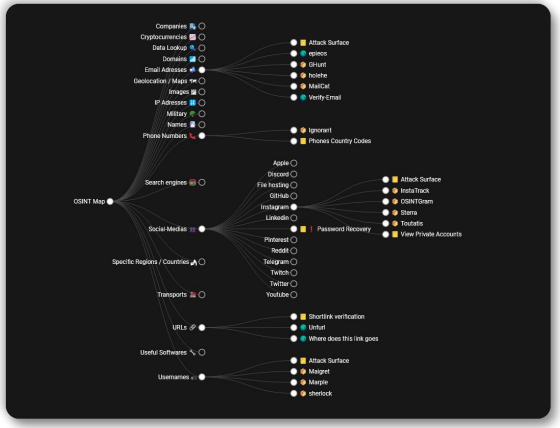
https://github.com/mpgn/CrackMapExec/releases/tag/v6.0.0

DFIR / OSINT
Techniques & outils

Mindmap pour l'OSINT

- Disponible ici : http://map.malfrats.industries/
- Version à jour de https://osintframework.com/

https://github.com/Malfrats/OSINT-Map (version GitHub)

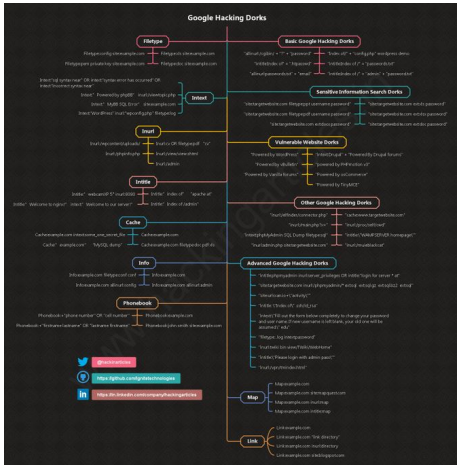


Carte heuristique pour Google DORKS

- Mise en forme de tags de recherche sous Google avec des exemples

https://twitter.com/DailyOsint/status/1678404233463201793

https://github.com/Ignitetechnologies/Mindmap/tree/main/Google%20Dorks



Nouveautés
Divers

Passkeys chez Apple, Microsoft et Google

- Gestionnaire de passkeys pour…
  - Windows Hello
  - Les comptes Google
  - Les comptes Apple ID
- Passkey ?
  - Mot de passe **0** - Paire de clés **1**
  - `<< Le début de la fin du mot de passe >>` annoncé par Google

https://www.lemonde.fr/pixels/article/2022/09/12/fini-les-mots-de-passe-les-passkeys-expliques-en-trois-questions_6141237_4408996.html

Business et Politique

Droit / Juridique / Politique
Monde

Avisa retire ses plaintes contre Reflets, Nextinpact…

- Suite aux articles reprenant médiapart
- Avisa se renomme en “Forward” et scinde ses activités
- Conserve le FIC qui passe de **F**orum **I**nternational de la **C**ybersécurité à **F**orum **inC**yber

https://www.portail-ie.fr/univers/business-development-innovation-et-start-up/2023/avisa-partners-scinde-ses-activites-annonce-la-naissance-de-forward-et-securise-le-fic-2024/

Arrestation Nikita Kislitsin

- Ancien responsable de la sécurité des réseaux pour l'une des plus grandes entreprises russes de cybersécurité (Group-IB),
  - Vols de mots de passe Formspring, LinkedIn et Dropbox

https://krebsonsecurity.com/2022/07/a-retrospective-on-the-2015-ashley-madison-breach/

Droit / Juridique / Politique
Monde

Le chef de l’équipe Sandworm identifié

- “Selon” les renseignements américains
- Sandworm = Fancy Bear = APT28 (Blackout electrique en Ukraine, NotPetya, Piratage des JO 2018…)
- Arrêté en 2018 en Hollande avec saisie de son matériel puis relâché

https://www.wired.com/story/russia-gru-sandworm-serebriakov/

Bouygues poursuit son assureur

- Et réclame 20m€ suite au piratage de Maze

https://www.linforme.com/tech-telecom/article/cyberattaque-bouygues-construction-poursuit-ses-assureurs_770.html

Conférences

Conférences

Passée(s)

- **DefConParis**, lundi 19 juin 2023 à Paris
- **Le Hack**, 30 juin au 2 juillet 2023 à Paris
- **Pass the Salt**, 3 au 5 juillet 2023 à Lille

À venir

- **Barbhack,** 26 août 2023 à Toulon
- **Black Hat USA**, 5-10 août 2023 à Las Vegas
- **DefCon**, 10-13 août 2023 à Las Vegas

Divers / Trolls velus

Divers / Trolls velus

Le TJ des agents de l'ANSSI augmente

- Passe de 1000 à 1200€/jour

  https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036739823

Divers / Trolls velus

Encore un OS souverain…

- Et ClipOS !!?

  https://www.senat.fr/amendements/2022-2023/778/Amdt_87.html

Les avocats de plus en plus ciblés

- https://www.numerama.com/cyberguerre/1428430-les-avocats-de-plus-en-plus-cibles-par-les-hackers-alerte-lanssi.html

Le CESIN inquiet des notations cyber

- Scans sauvages des périmètres… approximatifs
- Notes à leur bon vouloir
- Vente des notes

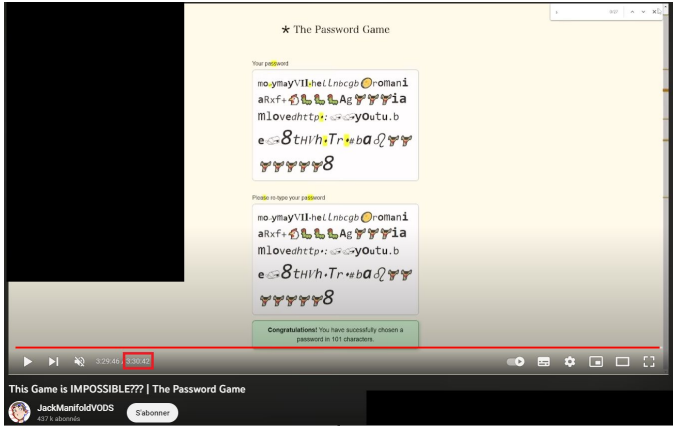
  https://www.lemagit.fr/actualites/366542234/Le-Cesin-sinquiete-de-la-notation-de-la-posture-de-cybersecurite

Divers / Trolls velus

Générer son mot de passe de façon ludique (ou pas)

- Jeu “The Password Game” développé par Neal Agarwal
- **35 règles** à respecter pour gagner 🏆
- Des règles simples…
  - Respecter un nombre minimum de caractères
  - Inclure des chiffres
  - Inclure des minuscules et des majuscules
- D’autres un peu moins …
  - Taper le meilleur coup dans une certains positions d'échecs en utilisant la notation algébrique
  - Insérer l'URL d'une vidéo YouTube d'une longueur spécifiée
- À vous de jouer → https://neal.fun/password-game/

https://www.youtube.com/watch?v=aTCK-GgIlOI



Divers / Trolls velus

DarkBERt, la version obscure de ChatGPT

- Modèle basé sur RoBERTa basé sur BERT, basé sur ?
- Apprentissage issue de **5,83 Go de texte brut obsures**
- Mais un apprentissage tout de même “éthique”
  - Les données personnelles sensibles trouvées ont été supprimées du set initial
  - Fichiers et vidéos supprimées également

https://arxiv.org/abs/2305.08596

Les utilisateurs de LastPass en panique !

- MFA réinitialisée **de force**
- Mesure prise suite aux incidents de 2022
- Pas mal de problèmes
  - Utilisateurs bloqués dans une loop
  - Impossible de contacter le support Premium (puisqu’il faut être connecté)
  - MasterPW invalide

https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass%2Fwhy_do_i_have_to_reset_my_authenticator_app.html&_LANG=enus

Divers / Trolls velus

Trahison chez Red Hat

- Code source de RHEL **uniquement** accessible aux clients de Red Hat
- Version publique diffusable via CentOS Stream
- Contrat de licence de RHEL → code **non partageable** !
  - Un gros problème pour les forks : Rocky Linux, Alma Linux, etc.

https://www.redhat.com/en/blog/furthering-evolution-centos-stream

Après MSN et MySpace… Skyblog 🪦

- Plateforme fondée en 2002 par Skyrock
- 17ème site le plus visité au monde en 2007
- Pensez à backuper votre skyblog avant 21 août 2023 !

https://lequipe-skyrock.skyrock.com/3356709252-Comment-sauvegarder-ton-blog.html

Divers / Trolls velus

TikTok banni en France ?

- Devrait être banni en France dès le 1er janvier 2024
  - Pour cause d'un manque de mesures de transparence
  - Et puis… par mise en évidence de collectes massives déjà réalisée aussi 😅 #2022
- Sauf si TikTok :
  - clarifie sa nature de ses relations avec les autorités chinoises
  - se conforme au droit européen en matière de protection des données
  - contrôle réellement l'âge des utilisateurs
  - met en place une modération efficace pour lutter contre la désinformation
  - Etc.

(encore 6 mois, bon courage)

https://www.tomsguide.fr/tiktok-interdit-en-france-des-le-1er-janvier-2024-pour-des-raisons-de-securite-nationale/

Prochaines réunions

Prochaine réunion

- Mardi 13 septembre

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