Revue d'actualité de l'OSSIR

12 septembre 2023

Jérémy De Cock
Christophe Chasseboeuf
Vladimir Kolla

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

2 mois == 219 failles dont 8 “0-day” (ou 7 ?)

- Juillet…
  - Windows MSHTML (CVE-2023-32046) → Privesc à distance
  - Windows SmartScreen (CVE-2023-32049) → Contourner la protection SmartScreen
  - Service de rapport d'erreur Windows (CVE-2023-36874) → Privesc en local
  - Microsoft Outlook (CVE-2023-35311) → Contourner certaines mesures de protection
  - Utilisation malveillante de pilotes signés par Microsoft (ADV230001) → Provenant de comptes compromis
  - Office et Windows HTML (CVE-2023-36884) → RCE from doc malveillante (#RomCom)
- Août …
  - .NET et Visual Studio (CVE-2023-38180) → DOS
  - Microsoft Office (ADV230003) → Correctif arrivé pour la CVE-2023-36884 !

https://www.it-connect.fr/patch-tuesday-juillet-2023-132-failles-de-securite-corrigees-dont-6-failles-zero-day/

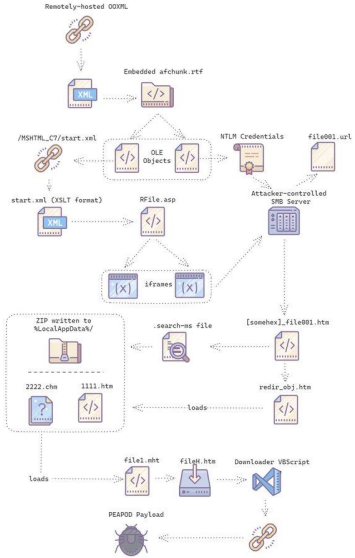
https://www.it-connect.fr/patch-tuesday-aout-2023-87-failles-de-securite-corrigees-dont-2-failles-zero-day/

Failles / Bulletins / Advisories
Microsoft - Divers

Execution de code dans Office, la cousine de Folina (CVE-2023-36884)

- Publié en juillet, pas de correctif en juillet
  - « There is either no solution available or it is impossible to apply. »
  - Exploité dans la nature
- La chaine d'exploitation

  https://twitter.com/r00tbsd/status/1679042071477338114
- Contournements :
  - Avoir Defender pour Office
  - Avoir InTune et activer l'option "Block all Office applications from creating child processes"
  - Activer l'option en PowerShell
    - Pensez à ajouter OneNote, oublié par Microsoft (`"OneNote.exe", "OneNotem.exe"`)



https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-all-office-applications-from-creating-child-processes

Failles / Bulletins / Advisories
Microsoft - Divers

Vol de clé MSA critique à Microsoft

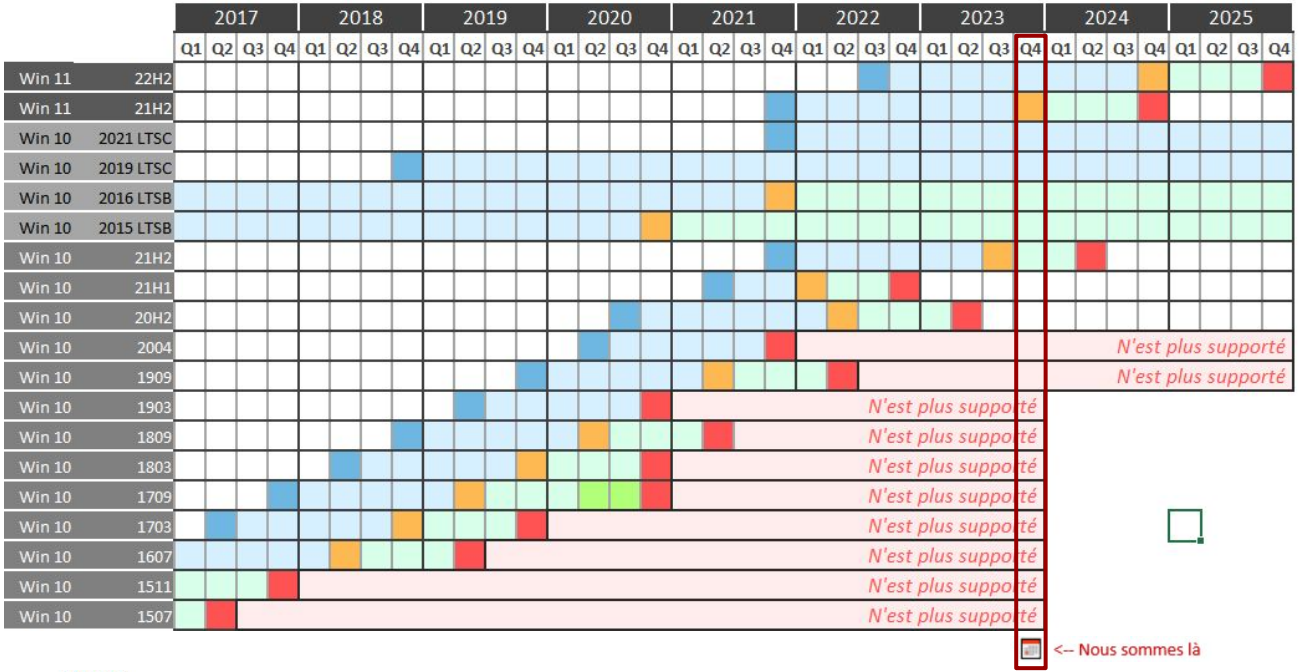
- Effectué par le groupe Storm-0558
- À permis de compromettre les comptes de messagerie de 25 organisations
  - Dont des agences fédérales américaines
- Clé de signature permettant de falsifier des jetons d'authentification pour l'**ensemble du service Cloud de Microsoft**
  - Et également les applications qui utilisent la fonctionnalité "Se connecter avec Microsoft"
  - Exploitation d'un problème de validation (`GetAccessTokenForResourceAPI`)
- Comment cela est-il arrivé ?
  - Compromission d'un compte ingénieur > accès au réseau de Microsoft > accès à l'environnement de débogage où la clé MSA se trouvait "accidentellement" (#crashdump)
- Volée depuis **avril 2021** ???

https://www.bleepingcomputer.com/news/microsoft/hackers-stole-microsoft-signing-key-from-windows-crash-dump/

https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

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

2 PrivEsc dans le noyau Linux d'Ubuntu

- CVSS 7.8
- Module OverlayFS en cause
  - CVE-2023-32629 : fonction `ovl_copy_up_meta_inode_data` qui peut être exploitée
  - CVE-2023-2640 : même chose avec une autre fonction inconnue
- 40% des utilisateurs sont impactés
- Versions impactées : 6.2.0 (Ubuntu 23.04), 5.19.0 (Ubuntu 22.10), etc.

https://www.wiz.io/blog/ubuntu-overlayfs-vulnerability

macOS, iOS, encore des 0days exploitées dans la nature en "0-click"

- CVE-2023-41064 : RCE depuis une image (reçue par iMessage?) avec le composant ImageIO
- CVE-2023-41061 : RCE lors du traitement d'un fichier par PassKit avec le composant Wallet
  - Coupons, cartes d'embarquement, papiers d'identité, clés de voiture ou de maison, titres de transport,...
- Découvert par Citizen Lab
- Mettez à jour (iOS 16.6 en 16.6.1, macOS Ventura 13.5.1 en 13.5.2)

https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Nouvelle 0-day sur Chrome

- CVE-2023-2136 (CVSS 9.6)
  - Integer overflow dans la bibliothèque graphique 2D Skia
  - Peut permettre une évasion de la sandbox de Chrome
- Version patchée : 112.0.5615.137

https://nvd.nist.gov/vuln/detail/CVE-2023-2136

Encore une faille du côté du plugin WP WooCommerce

- CVE-2023-28121 (CVSS 9.8)
  - Contournement de l'authentification qui permet une exécution de code
    - En tant que simple utilisateur ou en tant qu'admin !
- Faille exploitée en masse : 1.3 millions d'attaques en 2 jours ! (sur 157k sites)
- Versions vulnérables : 4.8.0 à 5.6.1

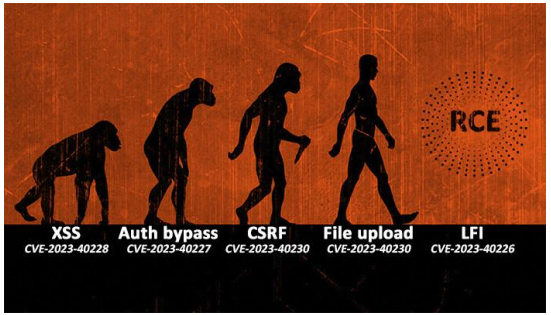
https://nvd.nist.gov/vuln/detail/CVE-2023-28121

Failles / Bulletins / Advisories
Navigateurs (principales failles)

OmniSpace, exécution de code à distance (CVE-2023-40226, CVE-40227, CVE-40228, CVE-40229, CVE-40230)

- “From automated XSS to RCE”
  - 5 CVE : XSS, Contournement de l’authentification, CSRF, téléversement de fichiers et LFI

https://www.patrowl.io/fr/blog-omnispace-from-automated-xss-to-rce-cve-2023-40228



WordPress Media Library Assistant, exécution de code à distance (CVE-2023-4634)

- LFI + téléversement arbitraire + fichier polyglotte = RCE

https://www.patrowl.io/blog-wordpress-media-library-rce-cve-2023-4634

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

Vulnérabilité dans Python urllib (CVE-2023-24329)

- CVSS 7.5
- Présente dans la librairie urllib et sa méthode urlparse() pour découper une URL
- Permet de contourner certains contrôles comme des listes de blocage
  - Exploitation : débuter une URL par un espace (0x20)
  - Version < 3.11.4

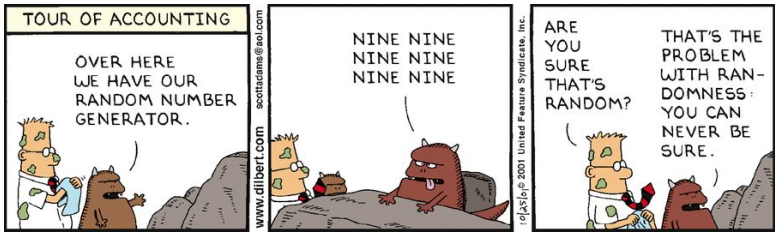
https://nvd.nist.gov/vuln/detail/CVE-2023-24329

https://thehackernews.com/2023/08/new-python-url-parsing-flaw-enables.html

Vulnérabilité dans Libbitcoin Explorer : Milk Sad (CVE-2023-39910)

- Générateur d'aléa (bx seed) sortant 32 bits d'aléa au lieu de 128, 192 ou 256
  - Servant pour la bi-clef de chiffrement du porte monnaie

https://milksad.info/



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

Attention à votre usage de `ssh-agent` (CVE-2023-38408)

- CVSS 9.8
- Met en cache les clés privées pour l'authentification par clé publique SSH
- RCE lors d'un transfert d'agent vulnérabile via OpenSSH
  - Raison : faiblesse venant du support de ENABLE_PKCS11
    - Transmission de bibliothèques partagées entre le client et le serveur
    - Effet de bord sur certaines librairies lors du dlclose() immédiat après le dlopen()
  - Version < 9.3p2

https://nvd.nist.gov/vuln/detail/CVE-2023-38408
https://github.com/snowcra5h/CVE-2023-38408

Exposition des clefs de signature des paquets Grafana

- Ecriture de la clef privée + "pass phrase" en clair, dans un fichier de log
  - A cause d'un vieux script de leur CI/CD
- Changez vos clefs :)

https://grafana.com/blog/2023/09/06/grafana-security-update-post-incident-review-and-timeline-for-gpg-signing-key-rotation/

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

RCE sur PaperCut (CVE-2023-39143)

- CVSS 9.8
- 2 path traversal qui permettent d'uploader, lire ou supprimer des fichiers
  - Raison : faiblesse venant de l'option qui autorise l'intégration des périphériques externes
  - Version < 22.1.3
- Comment tester ?
  - *curl -w "%{http_code}" -k --path-as-is "https://<IP>:<port>/custom-report-example/..\..\..\deployment\sharp\icons\home-app.png"*
  - Ou avec un PoC : https://github.com/horizon3ai/CVE-2023-27350
- Exploitée en masse par Clop et LockBit

https://nvd.nist.gov/vuln/detail/CVE-2023-39143

https://www-bleepingcomputer-com.translate.goog/news/security/new-papercut-critical-bug-exposes-unpatched-servers-to-rce-attacks/?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en

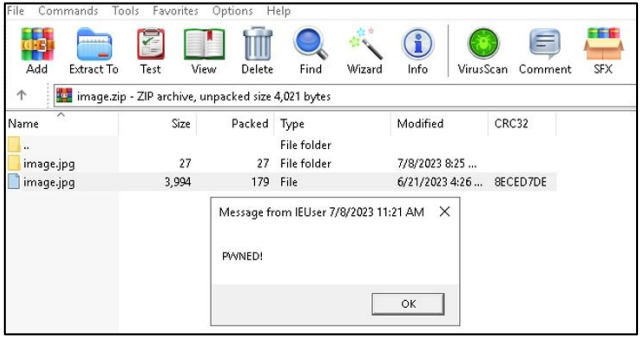
Failles / Bulletins / Advisories
Applications / Framework / … (principales failles)

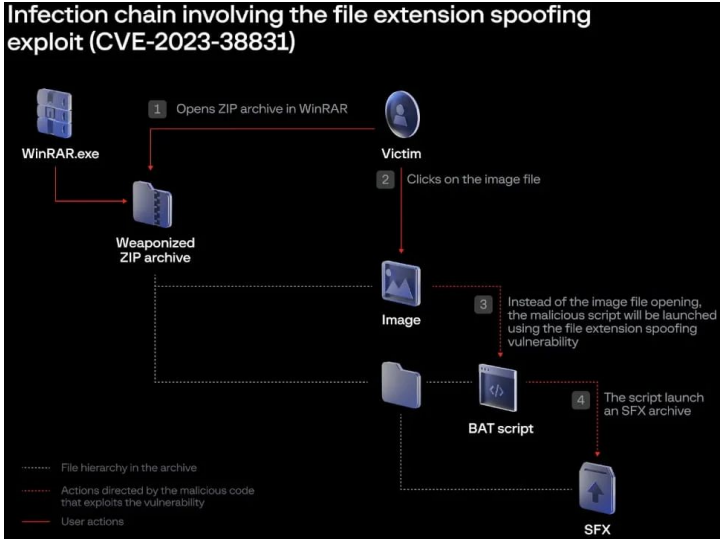
0-day sur WinRAR (CVE-2023-38831)

- CVSS 7.8
- Usurpation de nom d'extension de fichier
  - Exploitation : "image.jpg .cmd"
  - Version < 6.23
- Exploitée en masse depuis Avril (installation de DarkMe, GuLoader…)

https://nvd.nist.gov/vuln/detail/CVE-2023-38831

https://github.com/b1tg/CVE-2023-38831-winrar-exploit (exploit)





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

Faille sur les serveurs Ivanti Sentry (CVE-2023-38035)

- CVSS 9.8
- Port 8443 exposé = vous êtes vulnérables
  - Raison : API sensibles utilisables par un attaquant non-authentifié (RCE)
  - Version <= 9.18.0
- 500 serveurs vulnérables et exposés selon Shodan

https://github.com/horizon3ai/CVE-2023-38035 (exploit)

Vulnérabilité critique pour Citrix (CVE-2023-3519)

- CVSS 9.8
- Serveur configuré comme passerelle (VPN, virtual server, ICA Proxy, CVPN, RDP Proxy) ou comme serveur virtuel AAA = vous êtes vulnérables
- RCE sans plus d'informations techniques…
- 15.000 serveurs vulnérables et exposés selon Shodan

https://www.it-connect.fr/cve-2023-3519-faille-zero-day-corrigee-dans-citrix-adc-et-citrix-gateway/

https://www.gatewatcher.com/cve-2023-3519-citrix-adc-gateway/ (quelques IoC)

Failles / Bulletins / Advisories
Réseau (principales failles)

À l'attaque de vos ampoules 💡 (CVE-2023-38906, CVE-2023-38908, CVE-2023-38909)

- Ampoule connectée Tapo L530E et son application mobile impactées
  - Possible de récupérer le SSID et le mot de passe du réseau utilisé (ampoule)
  - Possible de prendre le contrôle de l'application et du compte utilisateur utilisé (appli)
- Mais pas que …
  - Checksum d'un secret partagé trouvé en dur dans le code de l'application
  - Possible de capturer les clés RSA et ainsi de visualiser le trafic échangé en clair
- Correctifs pas encore disponible 😢

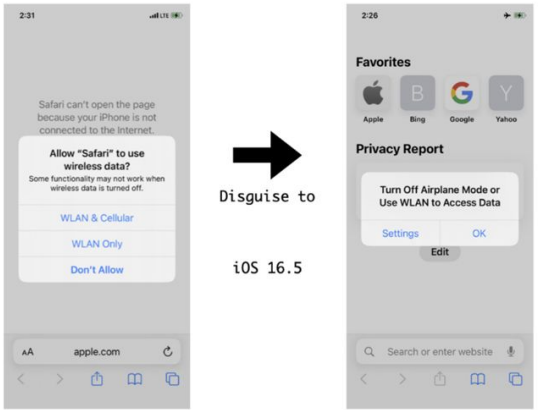
https://www.tp-link.com/us/support/faq/3722/

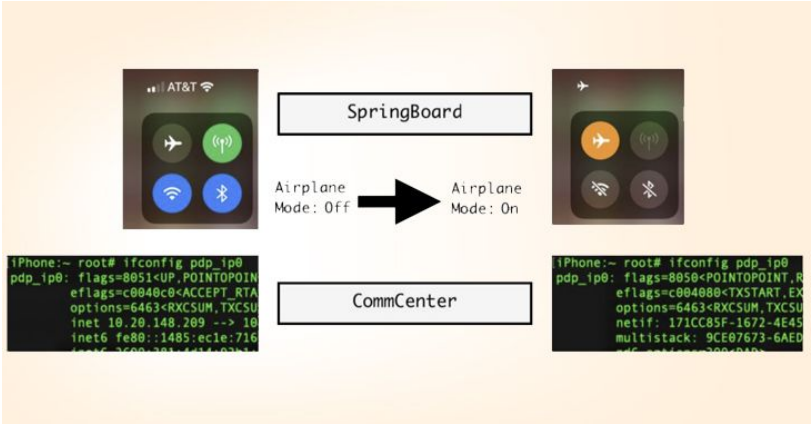
Failles / Bulletins / Advisories
Smartphones (principales failles)

Faux mode avion sur iOS 16

- Icône activée et coupure réseau pour toutes les applications sauf celle de l'attaquant ?
- Mode avions =
  - Réseau cellulaire désactivé et inutilisable **uniquement** côté user space
  - Actions effectuées via **com.apple.CommCenter** (bloquer) et **SpringBoard** (informer)
  - Base SQL qui enregistre l'état pour chaque appli (id bundle = 8 → appli bloquée)
    - Et pour un cheval de Troie alors ?

https://www.jamf.com/blog/fake-airplane-mode-a-mobile-tampering-technique-to-maintain-connectivity/





Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Malware

Nettoyage des ordinateurs infectés par Qakbot depuis … les serveurs C2 de Qakbot !

- Trojan bancaire (2008) puis dérivation vers le download de ransomware (2023)
  - Cf. revue d'actualité cyber de l'OSSIR du mois de Mai
- Infrastructures saisies par le FBI fin août
  - 700.000 appareils infectés
  - Clés de chiffrement utilisées pour communiquer avec les serveurs C2 récupérées
  - Intervention du FBI pour désinstaller le malware sur ces appareils
    - Outil propagé depuis un poste infecté pour communiquer avec tous les serveurs C2 de niveau 1
    - Module "supernode" utilisé par Qakbot remplacé par celui créé par le FBI
      - Nouvelles clés de chiffrement utilisées afin d'exclure les opérateurs de Qakbot de leur infrastructure
      - DLL Windows personnalisée utilisée pour émettre la commande "`QPCMD_BOT_SHUTDOWN`" au malware
    - Aucune suppression des fichiers Qakbot et des moyens de persistance utilisés
  - Base de données des informations volées partagées avec HaveIBeenPwned et la police néerlandaise
- Participation de la France, de l'Allemagne et des Pays-Bas (26 août 2023)

https://www.bleepingcomputer.com/news/security/how-the-fbi-nuked-qakbot-malware-from-infected-windows-pcs/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Phishing en utilisant les sous-domaines de onmicrosoft.com

- Exploité en masse par le groupe APT-29 (Midnight Blizzard)
  - Utilisent des tenants Microsoft 365 compromis
  - Cible les organisations gouvernementales, ainsi que les domaines de l'industrie, de l'informatique et les médias
- Etapes :

1. Avoir un domaine comme "teamsprotection.onmicrosoft.com"
2. Envoyer une invitation en tant que "Microsoft Identity Protection"
3. Pousser l'utilisateur à entrer un code précis dans son application mobile "Microsoft Authenticator"
4. Jeton de l'utilisateur obtenu, compte compromis !

Indicators of compromise

Indicator	Type	Description
msftprotection.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
identityVerification.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
accountsVerification.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
azuresecuritycenter.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain
teamsprotection.onmicrosoft[.]com	Domain name	Malicious actor-controlled subdomain

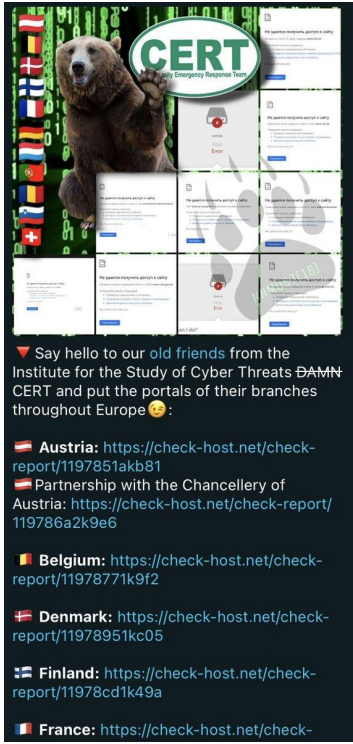
https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

Piratages, Malwares, spam, fraudes et DDoS
DDoS

Attaques en masse contre les CERT européens

- CERT EU, CIRCL, CERT-FR…
- Déni de service distribué “basique”
- Pas de conséquence sérieuse si ce n’est une indisponibilité des sites

https://twitter.com/ValeryMarchive/status/1699731606301278406



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Deviner vos mots de passe grâce au son généré par vos frappes au clavier

- CoANet développé par des chercheurs britanniques
  - Classificateur d'images
  - Utilise des représentations graphiques des ondes et des spectrogrammes
- Sujet du test : Apple MacBook Pro
  - Au travers d'un appel cellulaire (Iphone 13) : 95% de succès
  - Au travers d'un appel Zoom : 93% de succès
  - Au travers d'un appel Skype : 91,7% de succès
- Recommandations ?
  - Mots de passe aléatoires, usage du MFA
  - Avoir une saisie au clavier différente à chaque fois (impossible)
  - Générer des bruits de frappe au clavier ou appliquer un filtre pour supprimer ces bruits

https://www.it-connect.fr/voler-des-donnees-a-partir-du-bruit-genere-par-la-saisie-au-clavier-cest-possible/

Contournement du chiffrement de disque Luks + TPM

- La TPM c'est pas mal mais c'est **contournable**
- Préférez une solution avec un mot de passe qui déchiffre la vraie clef
  - Algo lent type PDKDF2 avec beaucoup de rotations

https://pulsesecurity.co.nz/advisories/tpm-luks-bypass

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

VirusTotal, fuite de données concernant 5 600 utilisateurs

- Téléversement d'un CSV contenant cette liste "sur" VirusTotal
  - Utilisateurs "premium"
    - Agences de renseignements, cyber command US, FBI, NSA, CERT… du beau monde !

https://www.bleepingcomputer.com/news/security/virustotal-apologizes-for-data-leak-affecting-5-600-customers/

Discord.io, fuite de données concernant 760 000 utilisateurs

- Service indépendant des serveurs Discord
- Vol de la base de données suite à une faille sur leur site ?
  - Clé d'API, identifiants, mots de passe hashés (bcrypt), adresses, etc.

https://www.bleepingcomputer.com/news/security/discordio-confirms-breach-after-hacker-steals-data-of-760k-users/

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

419 Dating, fuite de données concernant 260 000 utilisateurs (340 GB)

- Pas que des adresses mail et des localisations
  - Egalement des images, des chats privés, des audios et des logs !
- Données accessibles sur un bucket AWS S3 vulnérable
- L'application *from Hong Kong* a été retirée des stores mobiles depuis…

https://www.scmagazine.com/news/dating-app-spills-340gb-of-steamy-data-and-260000-user-profiles

Leak de Parcoursup ? "Enfaîte" non 😜

- Leak d'une soixantaine de dossiers
- La victime n'est pas Pacoursup, mais un lycée de l'académie de Rennes !
  - Victime de tentatives d'extraction de la base de données de leur site

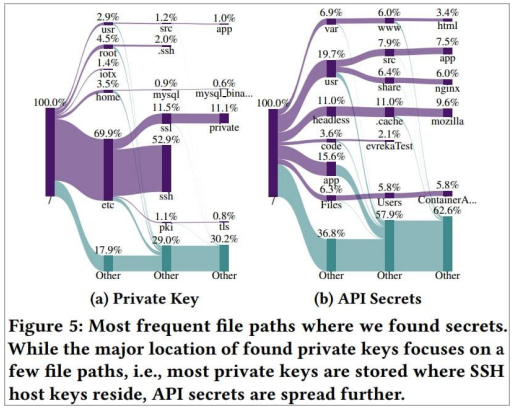
https://euro.dayfr.com/business/599459.html

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

Données sensibles dans des dizaines de milliers d'images chez Docker Hub

- Analyse de 337,171 images
- 8.5% contiennent des clefs privées, clefs d'API, mots de passe…

https://www.bleepingcomputer.com/news/security/thousands-of-images-on-docker-hub-leak-auth-secrets-private-keys/



(a) Private Key (b) API Secrets

Figure 5: Most frequent file paths where we found secrets. While the major location of found private keys focuses on a few file paths, i.e., most private keys are stored where SSH host keys reside, API secrets are spread further.

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

Énorme fuite du côté de Pôle Emploi (10 millions d'allocataires)

- Faille du côté de leur prestataire Majorel (#MOVEit)
  - S'occupe du traitement des documents des demandeurs d'emploi inscrits
- Données des demandeurs inscrits en février 2022
  - Mais également de certains plus anciens ?
  - Fiches d'identité, numéro de sécurité sociale…

https://www.lebigdata.fr/fuite-pole-emploi

Fuite de 130k clients ENGIE

- Fuite motivée par la "hausse du prix du gaz"
- Faille n-day utilisée sur un sous-domaine de engie.fr (ma prime économie d'énergie)
- Nom, prénom, adresse mail, ville, n° téléphone, n° client Engie, etc.

https://www.numerama.com/cyberguerre/1486298-engie-victime-dune-fuite-de-donnees-clients-110-000-personnes-sont-concernees.html

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

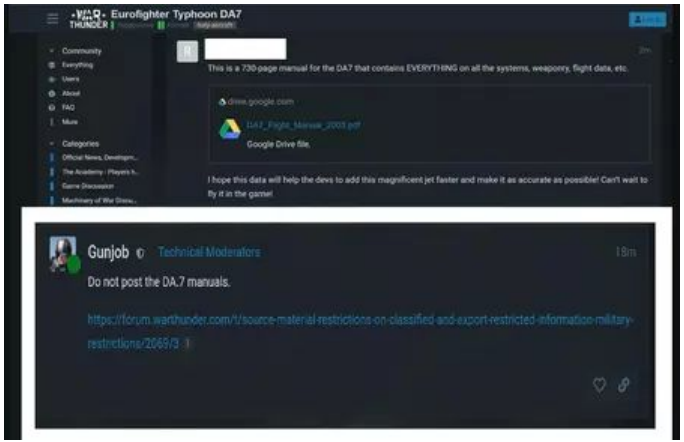
Le nouveau Jack Teixeira anglais

- Après Discord (avril), le forum du jeu-vidéo War Thunder
  - Jeu avec des assets réalistes (chars de combat, avions de chasse, navires de guerre)
- Fan de l'avion Typhoon version DA7 = leak d'un document classifié de 730 pages

`<< J'espère que ces informations vont pouvoir aider les développeurs à ajouter ce magnifique avion et ce de la meilleure manière possible. J'ai hâte de pouvoir le faire voler dans le jeu. >>`

- Semble provenir de l'Army Equipment Support Publication (AESP) #UK

https://www.journaldunet.com/solutions/dsi/1524407-war-thunder/



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

Suite de la cyberattaque du CHU de Rennes

- Fin juin : intrusion dans son SI
- Fin juillet : leak de 300 Go
  - Fonctionnement du CHU
  - Données médicales associés aux patients
- Selon le CHU, les patients impactés sont ceux du Centre de Soins Dentaires, des salles techniques de cardiologie et de leurs laboratoires

https://www.ouest-france.fr/bretagne/rennes-35000/direct-cyberattaque-au-chu-de-rennes-suivez-la-conference-de-presse-de-lhopital-2d460e76-11a2-11ee-a958-484ef579d2df

USA - Ministère de la santé et des services sociaux

- Aucun système ou réseau n'ait été compromis
- Exploitation de la vulnérabilité du logiciel MOVEit

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

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

Ville de Betton victime de Medusa

- Connu pour la double extorsion
  - Exfiltration des données suivie du chiffrement des données sur les machines
  - 100 000€ demandés dans un premier temps
- Environ 5 000 victimes = ½ de la ville
  - Pièces justificatives
  - Avis d'imposition
  - Factures, etc.
- Données accessibles sur le site vitrine du groupe… gratuitement ☹️

  https://twitter.com/_SaxX_/status/1699713382918607060

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

Des pirates piratés

- Plus de 100 000 cybercriminels infectés par un malware
  - Avec fuite de leurs identifiants et mots de passe de forums
  - Surement du fait d'un info-stealers
- Les cybercriminels aussi ont besoin de formation et de sensibilisation 😂

https://www.phonandroid.com/plus-de-100-000-hackers-se-sont-fait-voler-leurs-identifiants-sur-des-forums-de-cybercriminels.html

Blue Team PingCastle 3.1 est sorti !!!

- Audit de la sécurité AD et ~~AzureAD~~ Entra ID

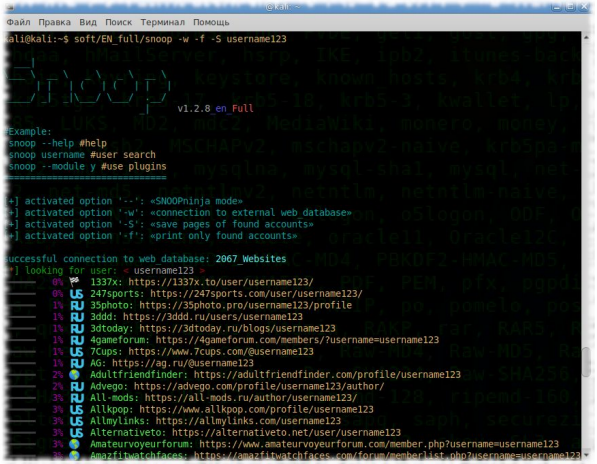
  https://twitter.com/mysmartlogon/status/1687165985017511942

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

Red Team Snoop, Sherlock mais en plus grand !

- 350 sites sur Sherlock VS 3100 sites sur Snoop
- Fait par un Russe, donc ⅓ de sites russes…

https://github.com/snoopppr/snoop/blob/master/README.fr.md



Red Team Testez vos formulaires d'upload !

- Upload_Bypass (nom de l'outil)
- Permet de tester les mécanismes d'upload sur vos sites
  - Webshell, eicar ou un répertoire
- N'inclut pas de bypass de captcha

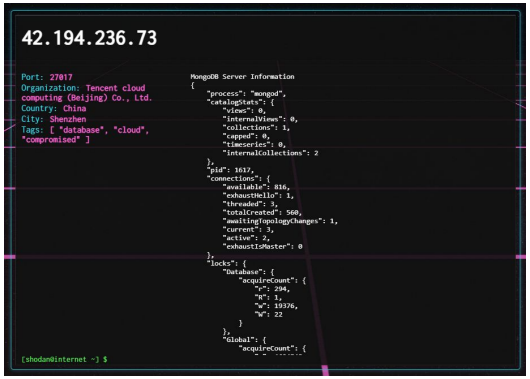
https://github.com/sAjibuu/upload_bypass

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

Red Team Shodan 2000

- Façon retro-futuristic d'explorer
  des équipements nouvellement découverts

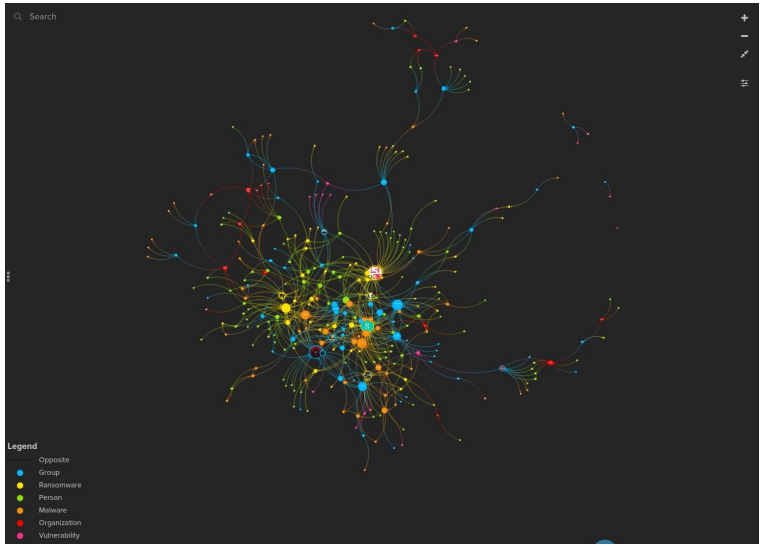
  https://2000.shodan.io/#/



Mind map utile en CTI

- Connexions concernant…
  - Groupes, organisations et personnes
  - Ransomwares, malwares et vulnérabilités
- Pays concernés : Russie, Chine et Iran
- Description, discussion, metrics…

https://kumu.io/pancak3/cybercrime-ops-demo#cybercrime-ops-demo



Nouveautés
Divers

Oodrive concurrence Office 365

- Suite collaborative complète
  - Pour traiter les contenus sensible

https://www.lemagit.fr/actualites/366544475/Oodrive-sort-son-alternative-a-Office-365

Business et Politique

Business
Monde

RadioFrance et **FranceInfo** parlent d'**Avisa Partners**

- << Avisa Partners ou la manipulation de l'opinion >>

  https://www.radiofrance.fr/franceinter/podcasts/secrets-d-info/secrets-d-info-du-samedi-02-septembre-2023-8381160

- << Avisa Partners : dans les coulisses de la sulfureuse agence d'influence soupçonnée de désinformation >>

  https://www.francetvinfo.fr/economie/medias/enquete-avisa-partners-dans-les-coulisses-de-la-sulfureuse-agence-d-influence_6035825.html

Droit / Juridique / Politique
Monde

BPI se lance dans le cyber diagnostic

- Evaluation des risques pour les PME
- **4** jours et **4** étapes, pour **4 4**00€ HT dont 50% payé par BPI
  - Ça fait beaucoup de 4 😁

https://www.bpifrance.fr/catalogue-offres/cybersecurite/diag-cybersecurite

Le ST(SI)² devient l'ANFSI

- La DSI commune police et gendarmerie change de nom
  - Devient une direction du numérique
- Le nom reste toujours imprononçable

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047989004

https://www.republik-it.fr/decideurs-it/gouvernance/naissance-de-l-agence-du-numerique-des-forces-de-securite-interieure.html

Droit / Juridique / Politique
Monde

LPM 2024-2030 adoptée le 13/07/2023

- Takedown/sinkhole DNS (2321-2-3)
- Dé-anonymisation whois (2321-3-1)
- Possibilité de forcer les éditeurs à communiquer sur leurs vulnérabilités (2321-4-1)
- Plus d'informations le mois prochain avec Marc-Antoine LEDIEU

https://www.defense.gouv.fr/actualites/lpm-2024-2030-definitivement-adoptee-parlement

https://www.defense.gouv.fr/sites/default/files/ministere-armees/Livret%20de%20pr%C3%A9sentation%20de%20la%20Loi%20de%20programmation%20militaire%202024-2030%20%286%20avril%202023%29.pdf

https://www.linkedin.com/posts/marc-antoine-ledieu-a040917_lpm-n2023-703-du-1er-aout-2023-aspects-cyber-activity-7092510621409128448-JcYW/

Droit / Juridique / Politique
Monde

Zoom va entraîner son IA avec vos données !

- Informations sur les clients, données de télémétrie et diagnostics, etc.
- Vous avez signés les CGU, alors vous acceptez cela !

> << Vous consentez à ce que Zoom accède, utilise, collecte, crée, modifie, distribue, traite, partage, entretienne et stocke les données générées par le service à toutes fins, dans la mesure et de la manière autorisées par la loi applicable, y compris à des fins [...] d'apprentissage automatique ou d'intelligence artificielle. >>

- Zoom rassure : “le contenu audio, vidéo ou de chat n’est pas utilisé”
- Mise à jour effective depuis le 27 juillet

https://www.it-connect.fr/zoom-va-entrainer-son-ia-avec-certaines-donnees-des-utilisateurs-et-cest-obligatoire/

Conférences

Conférences

Passée(s)

- Black Hat USA, 5-10 août 2023 à Las Vegas
  - Toutes les conférences : https://github.com/onhexgroup/Conferences/tree/main/Black%20Hat%20USA%202023%20slides
- DefCon, 10-13 août 2023 à Las Vegas
- Barbhack, 26 août 2023 à Toulon

À venir

- Hack in Paris, 25-29 septembre 2023 à Paris

Divers / Trolls velus

Divers / Trolls velus

Vous revenez de la Black Hat et/ou de Defcon…

- Si j'étais vous, je vérifierais si mon hôtel est dans la liste…
  - Des hôtels contrôlés ayant des puces de lit !

https://www.newsweek.com/bed-bugs-las-vegas-strip-hotels-1819456

- Pas de punaise, super !
  - Et la légionellose ?
    - Pour ceux qui sont passé par le Caesars Palace

https://twitter.com/jmcmurry/status/1695450627294502958

- Pas de punaise, ni de légionellose, super !
  - Et le COVID ?

https://twitter.com/manhack/status/1692507709440962851

Divers / Trolls velus

Scaleway pirate les sites web !!!

- Ils ont potentiellement une attaque depuis une IP Scaleway
  - Et accusent nommément la personne référencées dans le WHOIS 🤦
- On dirait une blague de 1er avril… un 21 août 🤔

```
<< les adresses IP sont fermées à l'accès >>
<< Scaleway tente quotidiennement de pirater le site Web >>
<< Nous les avons signalé à la gendarmerie française et européenne de la cybersécurité >>
```

https://www.linkedin.com/posts/runwaymagazineofficial_scaleway-mickaelmarchand-hebergeur-activity-7099274056645922816-VmTh/

https://web.archive.org/web/20230821080237/https://www.linkedin.com/posts/runwaymagazineofficial_scaleway-mickaelmarchand-hebergeur-activity-7099274056645922816-VmTh/

Lidl : Pat Patrouille ou Porn Patrouille ?

- Rappel de gâteaux “Pat Patrouille” avec une URL dont le domaine n’a pas été renouvelé
  - Suite à la fermeture de l’entreprise

    https://web.archive.org/web/20210728000139/https://www.appykidsco.com/
- Domaine récupéré par un site porno chinois

https://www.lidl.co.uk/static/assets/Paw_Patrol_Public_Recall_poster-500790.pdf

Divers / Trolls velus

Arrêtez tout, voici LA solution pour TOUT sécuriser !

- << Oubliez les proxy et les antivirus, utilisez plutôt ce logiciel révolutionnaire >>
- Ah non, c'est juste une publi-rédaction de 01Net pour vendre du NordVPN 🤦‍♂️
  - Rappels : ces VPN ne servent à rien ! *(sauf à contourner les restrictions Netflix)*

https://www.01net.com/bons-plans/oubliez-les-proxy-et-les-antivirus-utilisez-plutot-ce-logiciel-revolutionnaire.html

Mathis Hammel publie sur Twitter une vuln critique

- Impactant un site de rencontre d'extrême droite
- Une personne lui demande de "dézinguer" un site de musulmans
  - Il accepte 😮
- Baptiste Robert critique sa démarche, lui reprochant ce que lui même fait tout le temps

https://twitter.com/MathisHammel/status/1685635946878742528

https://twitter.com/fs0c131y/status/1685675774928384000

Divers / Trolls velus

Filigrane sur vos documents, par le gouvernement

- Ajoutez un filigrane sur des documents
  - Limite les arnaques de vol de dossier de loc'
    - Et ouverture de crédits à la conso
  - Votre PDF ou image est converti en un PDF avec des images
- Je recommande : `Usage:dossier de location truc, Date:juillet 2023`
- Pratique pour vos dossiers de location, prêt, ouverture de compte, dossiers administratif…
  - Par contre, ce n'est pas du chiffrement !

https://filigrane.beta.gouv.fr/

Un résumé de ShadowBrokers

- Très complet avec toutes leurs communications, les leaks, les victimes collatérales…

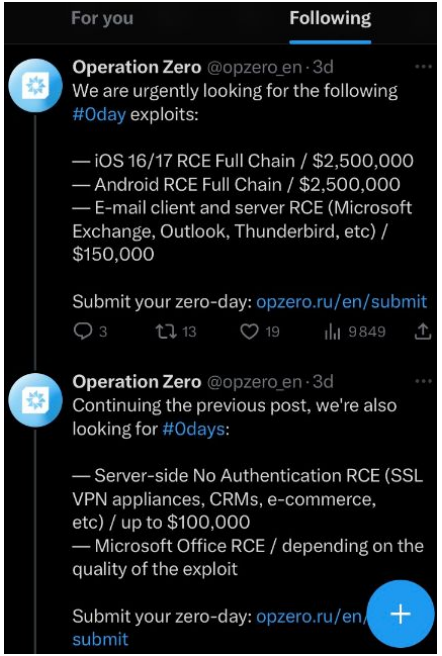
https://hack2interesting.com/the-shadow-brokers/

Divers / Trolls velus

Quelqu'un à reçu une grosse commande de 0days…

- Et n'a pas de stock !
- Achats de :
  - iOS/Android : $2,5m
  - Exchange, Outlook, Thunderbird : $150k
- Qui est Operation Zero ?
  - <<Our **clients** are Russian private and government organizations **only**>>
  - Devinez à quoi vont servir ces 0days…

https://twitter.com/opzero_en/status/1685621799311048705



Le Forrester liste les 3 dépenses à éviter en cyber

- Evitez les "appliances" on-premise, tous sur le cloud… américain
- Evitez le conseil à faible valeur ajoutée, liée à des projets (!!?)
- Evitez les outils de GRC

https://www.larevuedudigital.com/les-3-investissements-a-eviter-en-securite-pour-les-rssi-selon-forrester-research/

Divers / Trolls velus

Google collecte les données des apps de SMS et téléphonie

- A partir de la télémétrie
  - Ils savent qui communique avec **qui** et **quand**
- Les gens en passe de découvrir qu'Apple collecte TOUT

https://social.jesuislibre.net/@tuxicoman/108040078812453944

Un emoji qui vaut cher ! 💵 💵 💵

- Selon un juge au Canada :
  - `<<l'emoji pouce levé est une façon non traditionnelle de signer un document >>`
- Une affaire qui a coûté 82.000 dollars canadien pour un agriculteur

https://www.huffingtonpost.fr/international/article/l-emoji-pouce-leve-peut-etre-utilise-pour-signer-un-contrat-selon-la-justice-canadienne_220358.html

Divers / Trolls velus

Suite de l’arrestation de Pompompurin

- Ancien administrateur de BreachForums
  - Arrêté par le FBI en Mars 2023
  - Sujet évoqué dans la présentation de l’OSSIR en Avril
- 3 charges contre lui, il plaide coupable
  - Conspiration en vue de commettre une fraude sur des dispositifs d'accès
  - Fraude au moyen d'un dispositif d'accès - sollicitation non autorisée
  - Possession de pornographie enfantine
- Peine maximale : 40 ans de prison + 750k$, réponse le 17/01/2023 !

Divers / Trolls velus

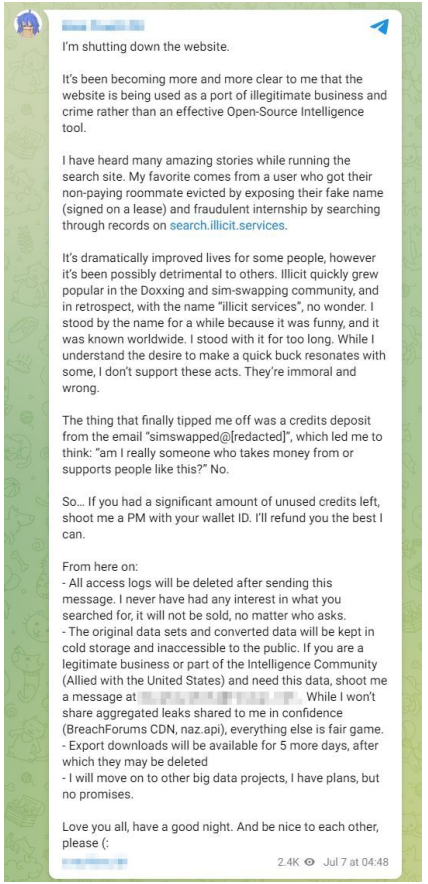
RIP deux légendes

- Kevin Mitnick (alias *Le Condor*)
  - Ancien pirate informatique repenti (Nokia, Pacific Bell, etc.)
  - Film Cybertraque vivement conseillé !
- Bram Moolenaar (:wq!)
  - Créateur de VIM (> Nano)

search.illicit déjà fermé (prévisible)

- Sujet évoqué dans la présentation de l'OSSIR de Juin
- Site fermé courant juillet par Peter Kleissner (son créateur)
  - `<<It's been becoming more and more clear to me that the website is being used as a port of illegitimate business and crime rather than an effective Open-Source Intelligence tool >>`
- Se propose [d'essayer] de rembourser les utilisateurs ayant encore des crédits sur le site et assure qu'il n'y aura pas de suite

https://www.zataz.com/le-projet-illicit-services-ferme-ses-portes-14-milliards-de-fuites-disparaissent/



I'm shutting down the website.

It's been becoming more and more clear to me that the website is being used as a port of illegitimate business and crime rather than an effective Open-Source Intelligence tool.

I have heard many amazing stories while running the search site. My favorite comes from a user who got their non-paying roommate evicted by exposing their fake name (signed on a lease) and fraudulent internship by searching through records on search.illicit.services.

It's dramatically improved lives for some people, however it's been possibly detrimental to others. Illicit quickly grew popular in the Doxxing and sim-swapping community, and in retrospect, with the name "illicit services", no wonder. I stood by the name for a while because it was funny, and it was known worldwide. I stood with it for too long. While I understand the desire to make a quick buck resonates with some, I don't support these acts. They're immoral and wrong.

The thing that finally tipped me off was a credits deposit from the email "simswapped@[redacted]", which led me to think: "am I really someone who takes money from or supports people like this?" No.

So... If you had a significant amount of unused credits left, shoot me a PM with your wallet ID. I'll refund you the best I can.

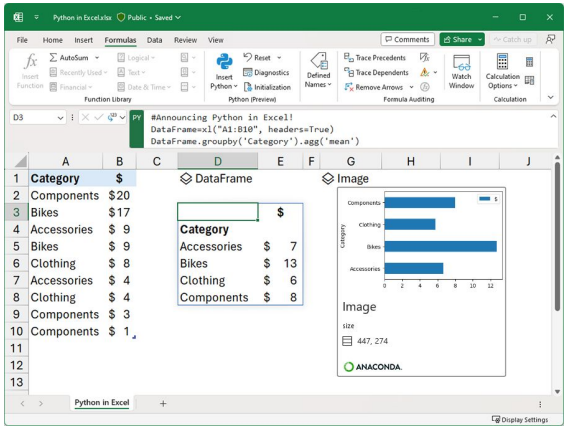
From here on:
- All access logs will be deleted after sending this message. I never have had any interest in what you searched for, it will not be sold, no matter who asks.
- The original data sets and converted data will be kept in cold storage and inaccessible to the public. If you are a legitimate business or part of the Intelligence Community (Allied with the United States) and need this data, shoot me a message at [redacted] While I won't share aggregated leaks shared to me in confidence (BreachForums CDN, naz.api), everything else is fair game.
- Export downloads will be available for 5 more days, after which they may be deleted
- I will move on to other big data projects, I have plans, but no promises.

Love you all, have a good night. And be nice to each other, please (:

2.4K Jul 7 at 04:48

Divers / Trolls velus

Python arrive sur Excel (macros 2.0 ?)



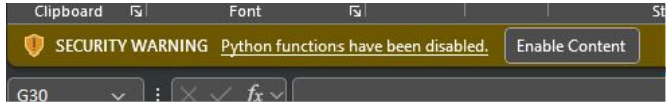
- Machine learning, analyses prédictives…
- Reverse-Shell ? Exfiltration de données ?
  - Code exécuté dans le Cloud dans un conteneur isolé (Azure)
    - Minage de bitcoin ? 😈
  - Aucun accès au poste et au réseau
  - Safe ? (non)

    https://twitter.com/two06/status/1696448565743108319?s=46&t=ZJaAuSPxDh8LIZXGARxqbg

- Actuellement en Beta (**version 16.0.16818.2000**)

  https://support.microsoft.com/en-us/office/data-security-and-python-in-excel-33cc88a4-4a87-485e-9ff9-f35958278327

Clé de registre **à ajouter**



Divers / Trolls velus

Anonfiles ferme ses portes

- Service de partage de fichiers promettant un anonymat complet
- Après la coupure des accès vers leur proxy (par le fournisseur)
  - Pour cause d'abus avec la plateforme
    - Exfiltration de données
    - Propagation de malwares, etc.
  - << `plusieurs pétaoctets plus tard` >>
  - Malgrés un "tri sélectif et automatisé" des fichiers uploadés

https://www.bleepingcomputer.com/news/security/file-sharing-site-anonfiles-shuts-down-due-to-overwhelming-abuse/

Divers / Trolls velus

Adieu les certificats TLS > 90 jours (Chromium Projects)

- Après Safari qui était passé à un an en 2020…
- De 13 mois à 90 jours pour Chrome OS et Google Chrome
- Leur but ?
  - <<Promouvoir l'automatisation>>
  - <<Rationaliser et améliorer les pratiques de validation des domaines>>
  - <<Se préparer à un monde post-quantique>>
- Entrée en vigueur en fin 2024 (si approuvé par le CA/Browser Forum)

https://www.darkreading.com/operations/enterprises-must-prepare-now-for-shorter-tls-certificate-lifespans

Divers / Trolls velus

Ajout du chiffrement résistant au quantique dans Chrome 116

- Prise en charge de **X25519Kyber768** dans les échanges TLS
- Sera utilisé pour le partage des secrets de chiffrement symétrique
  - X25519 = accord de clé lors de l'établissement d'une connexion TLS
  - Kyber-778 = KEM (validé par le NIST)
- Déja adopté par Cloudfare, Amazon Web Services et IBM

https://thehackernews.com/2023/08/enhancing-tls-security-google-adds.html

Teams va quitter Microsoft 365 dans l'UE

- Mesure qui prendra effet à partir du 1er octobre
  - Pour cause de pratique anticoncurrentielle
  - Possible d'avoir Teams avec le suite pour 5€ en plus (- 2€ sur l'abonnement mensuel)
- Microsoft promet d'intégrer des applications concurrentes et de renforcer sa documentation technique ainsi que les services de support !

https://www.silicon.fr/microsoft-debranche-teams-sur-office-365-et-microsoft-365-dans-lue-470864.html

Divers / Trolls velus

Clé FIDO2 from Google résistante à l'informatique quantique

- Nouveau schéma de signature hybride
  - Combinaison de ECDSA et de Dilithium
  - Version de ce dernier basée en Rust (20 ko)
- Mise au point dans le cadre d'OpenSK

  https://github.com/google/OpenSK (firmware de la clé)

  https://www.bleepingcomputer.com/news/security/google-released-first-quantum-resilient-fido2-key-implementation/

Prochaines réunions

Prochaine réunion

- Mardi 10 octobre

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