Revue d'actualité de l'OSSIR

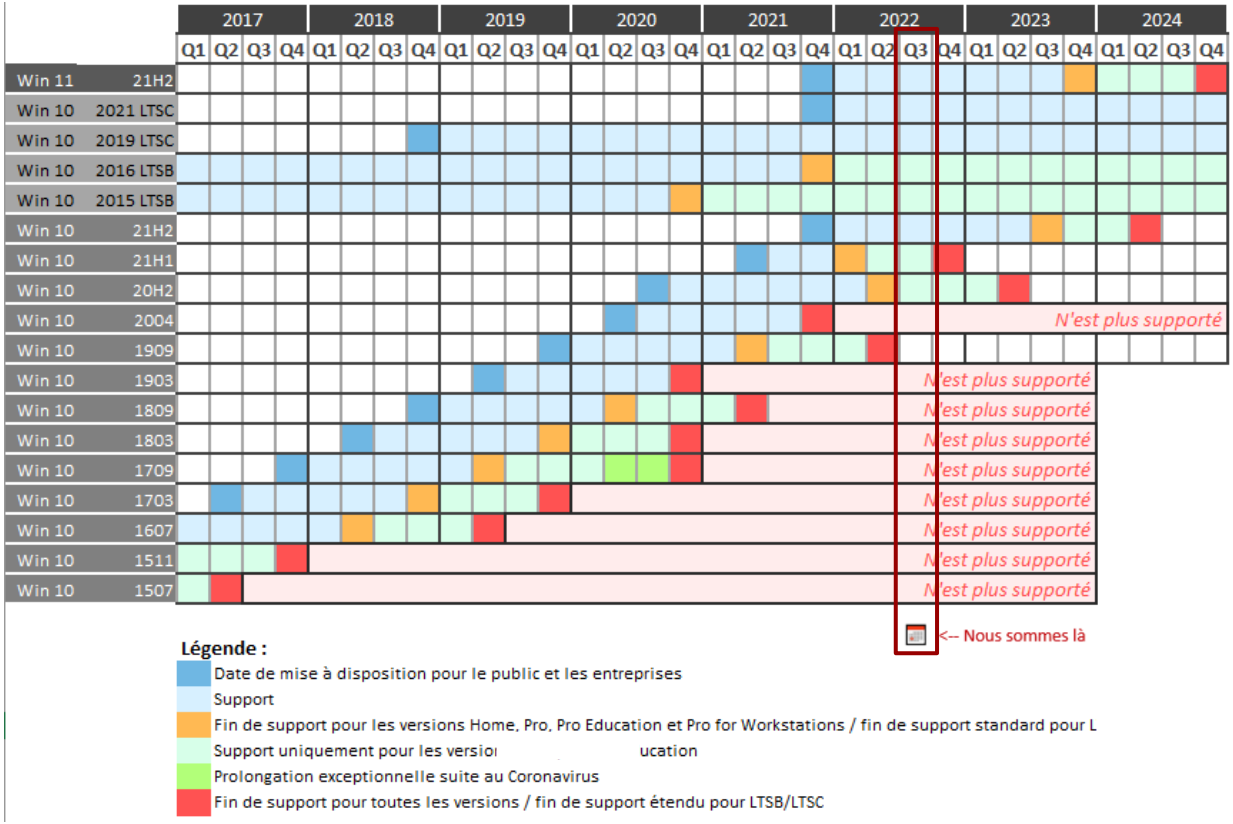
12 juillet 2022

Christophe Chasseboeuf
*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 en couleurs



Sortie	Home, Pro	Entreprise
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

Failles / Bulletins / Advisories
Microsoft - Divers

Les macros dans Office ou l'ascenseur émotionnel selon Microsoft

- Avril 2022 : macros désactivées pour les fichiers venant d'internet 🎉
  - Cf. revue du 08-02-2022 (slide 5)

    https://www.ossir.org/paris/supports/2022/2022-02-08/2022-02-08_OSSIR-20220208-v0.1.pdf
- Juin 2022 : retour en arrière sans explication 😢
  - A priori suite à des plaintes d'utilisateurs
    - Des utilisateurs d'Office comme outil ou des utilisateurs d'Office comme outil d'intrusion 😉

    https://www.bleepingcomputer.com/news/microsoft/microsoft-rolls-back-decision-to-block-office-macros-by-default/
- Juillet 2022 : en fait… si, peut-être, prochainement 🤡

  https://www.theverge.com/2022/7/11/23203554/microsoft-block-office-vba-macros-changes-temporary-statement

Failles / Bulletins / Advisories
Microsoft - Divers

Microsoft Azure AD et Granular Delegated Admin Privileges (GDAP)

- Possibilité pour les partenaires de modifier les privilèges AD de leurs clients
  - Sans leur consentement
- Pensez-y pour vos RedTeams 😉

https://www.theregister.com/2022/07/01/gdap_permissionless_change_window/

Microsoft Sharepoint, exécution de code authentifié (CVE-2022-30157)

- Exécution à la sérialisation de données des graphiques

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157

Microsoft Teams, le répertoire d'installation est modifiable par l'utilisateur

- Ce qui permet à un attaquant à privilèges limités d'y déposer une porte dérobée
- Car Teams est installé dans C:\Users\{user}\AppData\Roaming\Microsoft\Teams

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Chrome, exécution de code sur WebRTC (CVE-2022-2294)

- Exploitée dans la nature

  https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop.html

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

Apache Commons Configuration 2.4 - 2.7 (CVE-2022-33980)

- Injection de commande
- Appel avec un entête HTTP contenant une variable
  - ${script:expression} => exécution de commande
  - ${dns:record}
  - ${url:url}
  - ${sys:property}
  - ${env:var}"

https://lists.apache.org/thread/tdf5n7j80lfxdhs2764vn0xmpfodm87s

Atlassian Jira, SSRF (CVE-2022-26135)

- Belle SSRF avec :
  - GET et POST
  - Contenu Json ou pas
  - Personnalisation des entêtes

https://blog.assetnote.io/2022/06/26/exploiting-ssrf-in-jira/

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

Gitlab, Injection de commande sans authentification (CVE-2022-2185)

https://about.gitlab.com/releases/2022/06/30/critical-security-release-gitlab-15-1-1-released/

Django 3.2 et 4.0, injection SQL (CVE-2022-34265)

- Le commit :

  https://github.com/django/django/commit/54eb8a374d5d98594b264e8ec22337819b37443c

https://docs.djangoproject.com/en/4.0/releases/security/

BigBlueButton, XSS sur le nom de l'utilisateur

- Exécution du JavaScript dans le chat

https://pentests.nl/pentest-blog/stored-xss-in-bigbluebutton/

Plugin Wordpress Elementor, XSS (CVE-2022-29455)

https://rotem-bar.com/hacking-65-million-websites-greater-cve-2022-29455-elementor

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

Zimbra Mail, exécution de code à distance (CVE-2022-30333)

- Ecriture arbitraire de fichier à partir d'unrar

https://blog.sonarsource.com/zimbra-pre-auth-rce-via-unrar-0day/

OpenSSL, exécution de code (CVE-2022-2274)

- Dépassement de tampon lors du traitement d'une signature RSA sur un CPU ayant les instructions AVX-512

https://www.openssl.org/news/vulnerabilities.html

NodeJS, 7 vulnérabilités

- Dont une exécution de code (CVE-2022-32212)
- Contournement du correctifs pour la vulnérabilité CVE-2021-22884

https://securityonline.info/cve-2022-32212-node-js-arbitrary-code-execution-vulnerability/

Failles / Bulletins / Advisories
Smartphones (principales failles)

Android, contournement de l’écran de vérouillage (CVE-2022-20006)

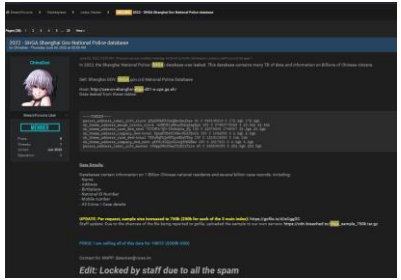
- Nécessite :
  - Un accès physique (semble évident 😉)
  - Une configuration particulière concernant les utilisateurs avec un invité (guest)

    https://medium.com/maverislabs/lock-screen-bypass-exploit-of-android-devices-cve-2022-20006-604958fcee3a

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

~~Sept cent millions~~ 1Mds de chinois et moi, et moi, et moi



- Vente d'une base de la police Chinoise contenant les données et cassiers
- Viendrait d'une publication d'un dev sur son blog contenant les creds

https://twitter.com/kendraschaefer/status/1543855989325082624

http://breached65xqh64s7xbkvqgg7bmj4nj7656hcb7x4g42x753r7zmejqd.onion/Thread-Selling-2022-SHGA-Shanghai-Gov-National-Police-database?highlight=shga

Marriott, fuite de 20Go de données

- Encore…
  - Surtout des documents de travail internes, des documents sur les hôtels et leur personnels, documents concernant certains clients
- Origine de la compromission non encore connue

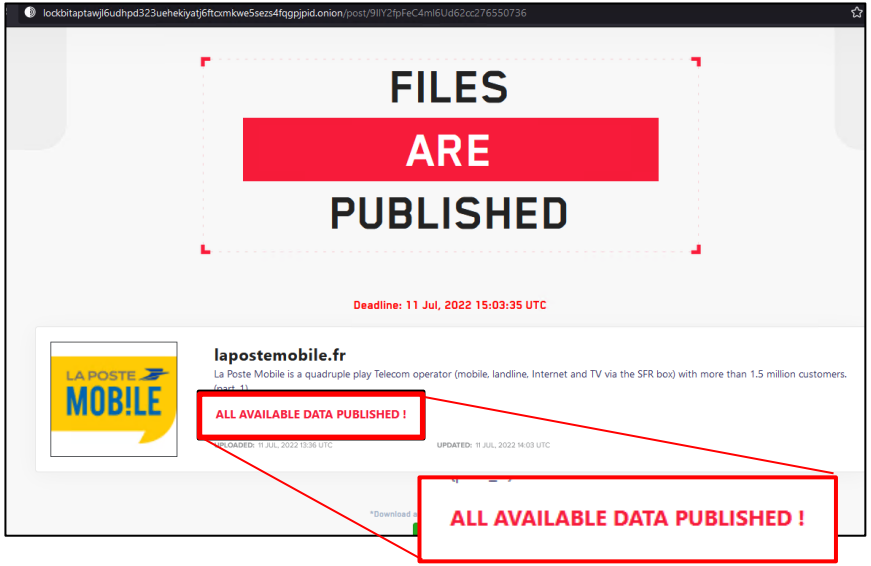
https://www.databreaches.net/exclusive-marriott-hacked-again-yes-heres-what-we-know/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Lockbit diffuse les données des utilisateurs de la Poste Mobile

- 400Mo de données : nom, prénom, numéro de tél, adresse postale, RIB,

http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion/post/9IlY2fpFeC4ml6Ud62cc276550736



Piratages, Malwares, spam, fraudes et DDoS
Piratages

Chatbot sur Messenger !!!

- 28 juin 2022 sur une campagne d'hameçonnage par chatbot sur Messenger
  - Utilisation de « Appeal now »
  - administrée par le profil @case932571902
- Une fausse double authentification en envoyant un message sur le smartphone de la victime pour donner encore plus de légitimité à leur arnaque.

https://www.numerama.com/cyberguerre/1026032-ce-chatbot-messenger-na-ete-cree-que-pour-derober-vos-identifiants-facebook.html

Cryptomonnaies, encore un vol record

- Vol de $104m chez Harmony

https://www.presse-citron.net/crypto-un-enorme-vol-vient-perturber-un-marche-deja-tres-morose/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Vol de données de 65 000 patients suite au pirage d’un comte mail

- Des employés de Kaiser Permanente s'échangeaient des données de patients
  - Par mail
  - Sans chiffrement
- Chiffrer les contenus sensibles de vos mails !
  - Et n’envoyez pas de contenu sensible par mail 😬

https://blog.malwarebytes.com/cybercrime/2022/06/email-compromise-leads-to-healthcare-data-breach-at-kaiser-permanente/

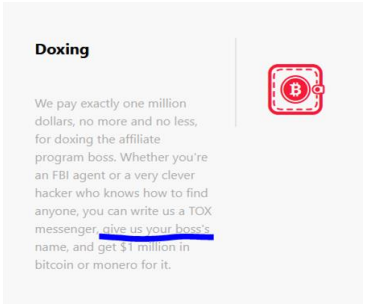
Piratages, Malwares, spam, fraudes et DDoS
Malware

Conti arrête de les rançongiciel ?

- Ou va juste changer de nom ?
  https://www.bleepingcomputer.com/news/security/conti-ransomware-finally-shuts-down-data-leak-negotiation-sites/

LockBit fait du marketing

- Revue de presse
  http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
- Bugbounty
  - sur le propre outils pour corriger les bugs, sur leur dé-anonymisation Tor...
  - $1m si vous "doxxez" les chefs des concurrents (ou vos propres chefs)
- Rachat de vulns
  http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion/bug-bounty
- Partenariats
  http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion/conditions



Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Le skimming 4.0

- Trouvé dans une boutique aux USA

  https://twitter.com/evankirstel/status/1544297283684106240

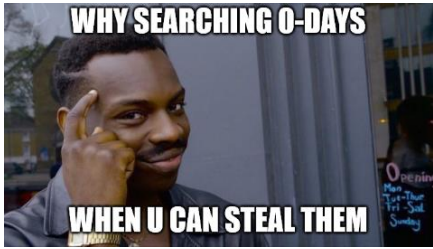
Echange des terminaux de paiement dans les restaurants

- Permettant de créditer les comptes des escrocs
- Arnaque discrète à court terme
- Astuce : personnalisez vos TPE, collez des autocollants spécifiques, marquez les…

  https://www.francelive.fr/article/france-live/arnaque-au-terminal-de-paiement-dans-les-restaurants-simple-et-terriblement-efficace-7472881/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Pourquoi chercher des vulnérabilités ? Il suffit d'être salarié HackerOne



- Un salarié vole (contrefait) des rapports de bugs
  - Et les a vendu
- Combien de fois est-ce arrivé par le passé sans que cela soit detecté ?

https://www.bleepingcomputer.com/news/security/rogue-hackerone-employee-steals-bug-reports-to-sell-on-the-side/

Rostelecom injecte de la propagande pro-russe dans les sites web en http

- Rostelecom est un opérateur Russe

https://twitter.com/MosSobyaniin/status/1544318154846998531

Prise de contrôle d'un drone grâce à ExpressLRS

- ExpressLRS protocole open source à longue portée pour envoyer des commandes
- Phase de connexion chiffrée avec MD5
  - Dont une partie du clair est prédictible

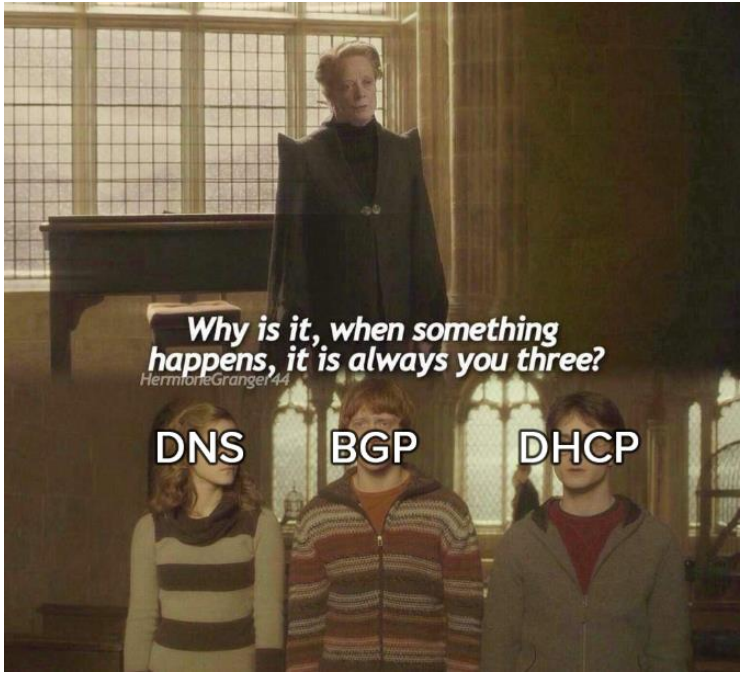
https://threatpost.com/drone-hack-expresslrs-hijacked/180133/

Piratages, Malwares, spam, fraudes et DDoS
Pannes

CloudFlare, ce coup-ci c’est BGP et non DNS

- Panne impactant 19 des datacenters de CloudFlare
- Durant 1h20
- Erreur du fait d’un déploiement BGP
  - Réalisé à 3h
  - Appliqué à 6h

https://blog.cloudflare.com/cloudflare-outage-on-june-21-2022/



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

security.txt est un standard

- Donc utilisez le 👍

  https://www.rfc-editor.org/rfc/rfc9116

Apple permet un verrouillage supplémentaire des données

- Le “Lockdown Mode” protège en plus :
  - Messages, la navigation, les connexions à un ordi, l’installation de profils de configuration
- Mais peu pratique pour l’utilisateur
  - Qui a mis un code pin sur Signal ?

  https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

- A noter qu’ils augmentent aussi leur primes au bug
  - Jusqu’à $2m pour une vulnérabilité en mode “Lockdown”

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

Sécurisez PowerShell grâce à un guide de … la NSA 😉

- Plusieurs bonnes pratiques de durcissement
- Ainsi que de détection

https://www.bleepingcomputer.com/news/security/nsa-shares-tips-on-securing-windows-devices-with-powershell/

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

Red Team TripleCross, un rootkit pour eBPF

- Développé par un étudiant
  - “à des fins éducatives uniquement” 🤣🤣🤣
- L’archi ressemble à celle de microservices

https://github.com/h3xduck/TripleCross

aaaaaaaaaaaaaaaa

https://github.com/mandiant/commando-vm

Business et Politique

Business
Monde

Recorded Future vient acquière Hatching

- un service d’analyses de logiciels malveillants
- une alternative à VirusTotal.

https://www.lemagit.fr/actualites/252522579/Recorded-Future-soffre-une-petite-perle-de-lanalyse-de-maliciels

Gaia-X a du mal à se lancer, à sortir de la théorie

- Cadre juridique incertains
- Gros acteurs américains
- Retrait de gros acteurs

https://www.lemondeinformatique.fr/actualites/lire-le-projet-europeen-gaia-x-est-bloque-au-stade-du-concept-86551.html

Business
Monde

La CNIL contrôle … le niveau de cybersécurité de sites web français

- En 2021, elle en a contrôlé 21, dont 15 ont été mis en demeure
- Les collectivités territoriales dans le viseur
- Trois mois pour se mettre en conformité à compter de juillet 2022

https://www.usine-digitale.fr/article/la-cnil-entame-un-controle-sur-le-niveau-de-cybersecurite-des-sites-web-francais.N2024492

Des hackers chez les RH

- Détecté de nombreuses attaques par rebond dans des entreprises et organisations gouvernementales
- Récupération des identifiants des services RH ou compta pour ensuite piéger un salarié en particulier

https://www.numerama.com/cyberguerre/1029360-un-hacker-se-cache-peut-etre-derriere-votre-rh.html

Droit / Juridique / Politique
Monde

En cas de piratage, les SSII / ESN devront prévenir l'ANSSI dans les 24H

- Accord provisoire de révision de la directive NIS
- En cas d'incident "majeur"

https://www.solutions-numeriques.com/les-entreprises-de-services-numeriques-devront-prevenir-lanssi-sous-24h-si-elle-subissent-une-cyberattaque/

Publication du code utilisé par le FBI pour espionner les criminels

- Le FBI a créé une fausse entreprise éditant une solution de messagerie chiffrée : Anom
- Arrestation de plus de 1 000 criminels

https://www.vice.com/en/article/v7veg8/anom-app-source-code-operation-trojan-shield-an0m

Changements de poste:

- Patrick Pailloux quitte la DT pour devenir conseiller d'Etat

https://www.vie-publique.fr/discours/285405-conseil-des-ministres-14062022-mesures-d-ordre-individuel

- Guillaume Poupard quitte l'ANSSI pour "potentiellement" le DGSE

https://www.lemondeinformatique.fr/actualites/lire-telex-guillaume-poupard-en-route-pour-la-dgse-lenovo-ouvre-une-usine-en-hongrie-adobe-prepare-une-version-freemium-de-photoshop-87095.html

Conférences

Conférences

Passée

- LeHack, 24 juin 2022
- Troopers (très très offensif), 27 juin au 1er juillet 2022
- Pass the SALT, 4-6 juillet 2022
- Hellfest 2022 🤘 *(il y'avait teeeeeeellement de gens de la cybersécurité* 😉)

A venir

- Black Hat USA, 6 au 11 aout 2022
- DefCon 20, 11 au 14 aout 2022
- Barbhack, 27 aout 2022
- BeeRumP, 16 septembre 2022
  - https://www.rump.beer/2022/
- Hexacon, 14 et 15 octobre 2022
  - par Synacktiv

Divers / Trolls velus

Divers / Trolls velus

Avisa Partners, plusieurs articles sur les pratiques controversées

- Publication d'articles d'influence sur commande

  https://www.mediapart.fr/journal/france/270622/operation-intox-une-societe-francaise-au-service-des-dictateurs-et-du-cac-40

  https://www.journaldunet.com/ebusiness/le-net/1148396-plongee-au-coeur-d-istrat-manipulateur-de-wikipedia-et-des-sites-medias/

SFR a dépose "Cloud souverain"

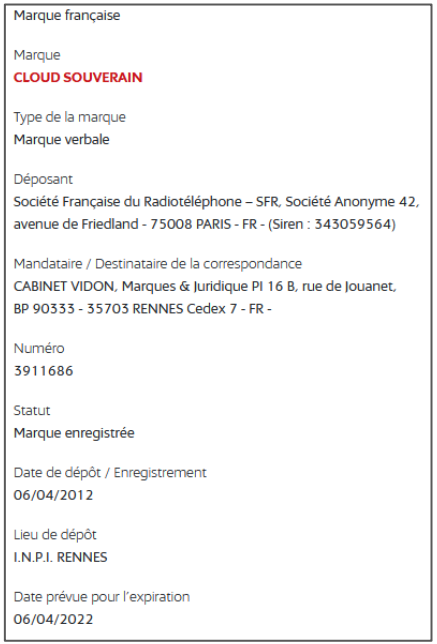
- Peu de chance que ce soit valide légalement

  https://twitter.com/SouveraineTech/status/1539863525346115585

  https://data.inpi.fr/marques/FR3911686?q=cloud%20souverain#FR3911686

- Après Thales et son "cloud de confiance"

  https://data.inpi.fr/marques/FR4772474?q=cloud%20de%20confiance#FR4772474



Marque française

Marque
CLOUD SOUVERAIN

Type de la marque
Marque verbale

Déposant
Société Française du Radiotéléphone – SFR, Société Anonyme 42, avenue de Friedland - 75008 PARIS - FR - (Siren : 343059564)

Mandataire / Destinataire de la correspondance
CABINET VIDON, Marques & Juridique PI 16 B, rue de Jouanet, BP 90333 - 35703 RENNES Cedex 7 - FR -

Numéro
3911686

Statut
Marque enregistrée

Date de dépôt / Enregistrement
06/04/2012

Lieu de dépôt
I.N.P.I. RENNES

Date prévue pour l'expiration
06/04/2022

Divers / Trolls velus

Jean-Michel Mytho est de retour

- Après "Pegazus sé lé Chinouas" *(Pegasus, de la société israélienne NSO)*

  https://jonathandata1.medium.com/pegasus-spyware-untold-chinese-engineering-samples-1-2-e5aba2a0b20b
- Après "ADB pour Android c'est une vuln critikeuh" *(ADB, l'outil de débug Android)*

  https://web.archive.org/web/20220129164409/https://github.com/jonathandata1/verizon_samsung_auto_enable_adb
- Voici "Citizenlab y zinstallent des backdoureuh"

  https://twitter.com/jonathandata1/status/1543916552050954240
- En exclu, son prochain article *"Sous Linukse l'uzer root y permet de tou kassé, c'est une backdoureuh"*

Jean-Michel Mytho peut vous tracer sur Twitter

- Plus vous tweeté, plus il peut trouver votre adresse IP
  - Il peut également vous faire gagner au loto, revenir l'être aimé et excelle dans le désenvoutement

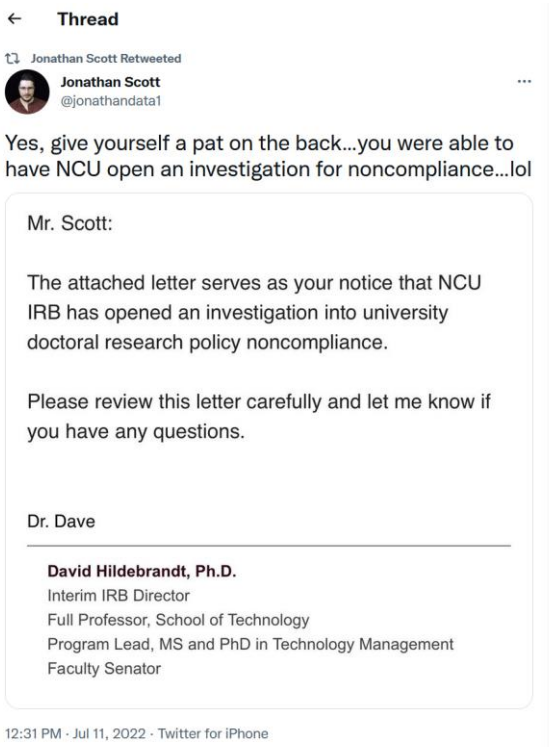
https://twitter.com/s1guza/status/1546100002472198146

Divers / Trolls velus

Jean-Michel Mytho est dans la sauce

- Ouverture d'une enquête par le comité de revue de son université

https://twitter.com/deviantollam/status/1546579921572507648



← Thread

Jonathan Scott Retweeted

Jonathan Scott
@jonathandata1

Yes, give yourself a pat on the back...you were able to have NCU open an investigation for noncompliance...lol

Mr. Scott:

The attached letter serves as your notice that NCU IRB has opened an investigation into university doctoral research policy noncompliance.

Please review this letter carefully and let me know if you have any questions.

Dr. Dave

David Hildebrandt, Ph.D.
Interim IRB Director
Full Professor, School of Technology
Program Lead, MS and PhD in Technology Management
Faculty Senator

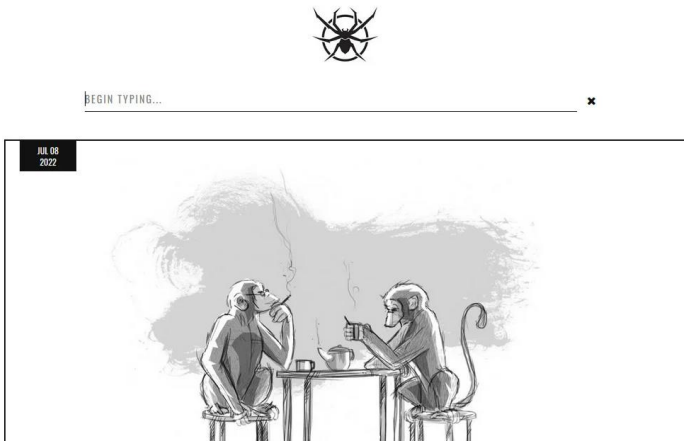
12:31 PM · Jul 11, 2022 · Twitter for iPhone

Divers / Trolls velus

Recherche des données volées !

- Qui ?
  - Deux gangs de ransomware et un groupe d'extorsion de données
- Comment ?
  - nouvelle tactique : ajouter une fonction de recherche sur le site de fuite pour faciliter la recherche de victimes ou même de détails spécifiques.
- Les extorqueurs de données commencent tout juste à explorer la fonction de recherche.

https://www.bleepingcomputer.com/news/security/ransomware-gang-now-lets-you-search-their-stolen-data/



Divers / Trolls velus

Pourquoi Synology (maintenant) c'est du solide

- Réponse courte :
  - Ils ont fait un gros effort sur la sécu
  - Et ont même sécurisé des lib open source

https://drive.google.com/file/d/1MYCNVKkNETkqS-cLJsqHE43Sfm4LZbCO/view

Cryptographie post-quantique : le NIST a choisi ses algorithmes

- Choix des algorithmes de cryptographie post-quantiques qu'il allait maintenant normaliser
  - **Kyber** pour l'échange de clés
  - **Dilithium** pour les signatures

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Vous êtes vraiment sous-payés

- Et c’est que vous bloquez les projets 😂

https://twitter.com/typesfast/status/1536406121249796096

Divers / Trolls velus

Quand tu envoies un code d'exploitation sur OpenWall…

- <<This is insane. You can't send weaponised exploits that crash email clients to public mailing lists. Please do not do this again.>>
- Publication d'un DoS sur GnuPG, avec l'exploit en pièce jointe
  - Concaténation de la même signature de nombreuses fois

https://www.openwall.com/lists/oss-security/2022/07/04/3

Les XSS c'est terminé !

- Enfin les DOM tout du moins…
- "Si" vous activez cette fonctionnalité des navigateurs :

```
Firefox: about:config#dom.security.sanitizer.enabled
Chrome: chrome://flags#enable-experimental-web-platform-features
```

https://wicg.github.io/sanitizer-api/#dom-element-sethtml

Divers / Trolls velus

LibreOffice “pas cher”

June 10, 2022

LibreOffice 7.3.4 Crack + Keygen 2022 [Mac/Win] Free Download

By Max Ward Office Tools 0 Comments

Direct Download Download Crack

LibreOffice 7.3.4 Crack

LibreOffice Crack is a powerful office suite; its clean interface and powerful tools let you unleash your creativity and grow your productivity. LibreOffice Crack embeds several applications that make it the most powerful Free & Open Source Office Suite on the market: Writer, the word processor, Calc, the spreadsheet application, Impress, the presentation engine, Draw, drawing and flowcharting application, Base, our database and database frontend, and Math for editing mathematics. Your documents will look professional and clean, regardless of their purpose: a letter, a master thesis, a brochure, financial reports, marketing presentations, technical drawings and diagrams.

https://twitter.com/TechHutTV/status/1536675787918614529

https://twitter.com/mynameisv_/status/1536961641061011456

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 ?


Bonnes Vacances