Revue d'actualité de l'OSSIR

13 Juin 2023

Christophe Chasseboeuf
Jérémy De Cock
*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de mai 2023, 38 vulnérabilités, dont :

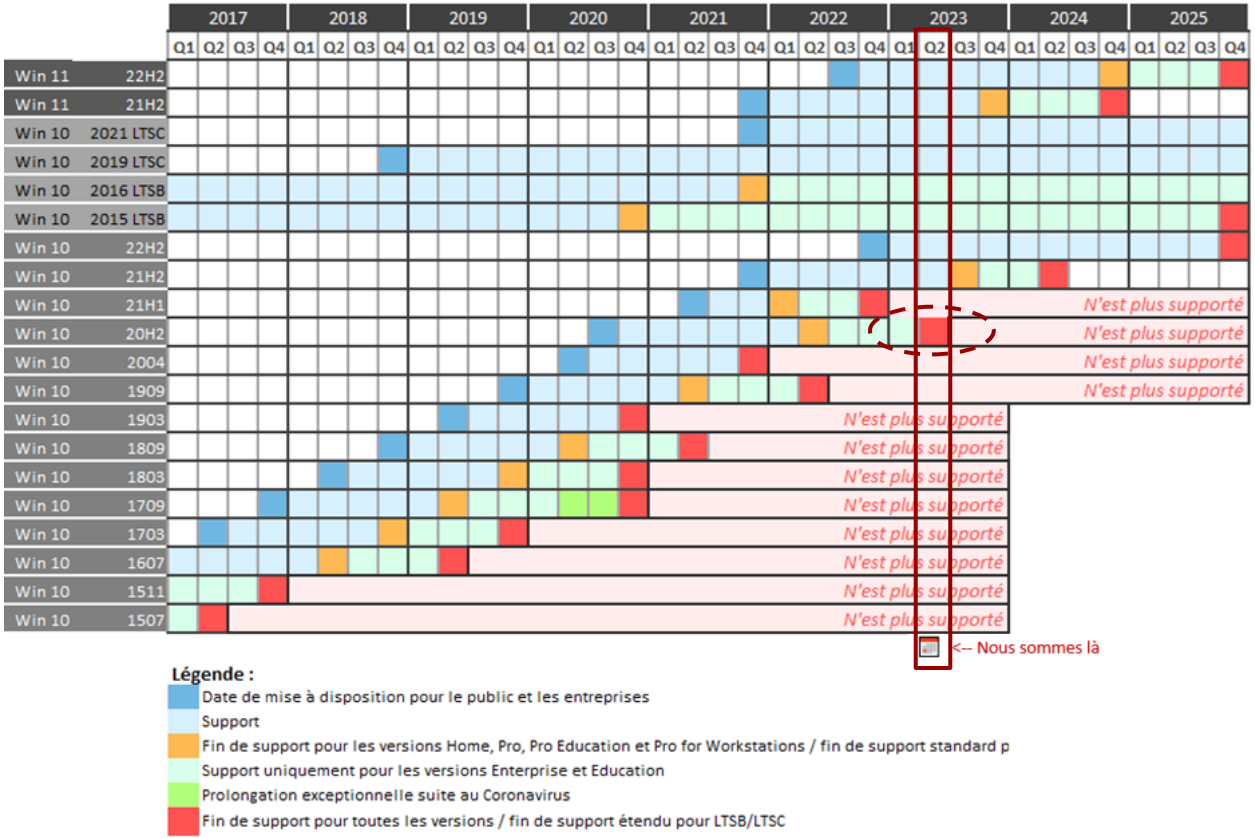
- Exploitées dans la nature :
  - Elevation locale de privilèges (CVE-2023-29336) :

    https://github.com/numencyber/Vulnerability_PoC/blob/main/CVE-2023-29336/poc.cpp
  - Contournement de Secure Boot par exécution d'un code auto signé dans l'UEFI (CVE-2023-24932)
    - *Exploitée par BlackLotus pour contourner le correctif de CVE-2022-21894 (cf. revue de 2023-05-09)*
    - *Le correctif nécessite une activation manuelle pour appliquer la liste de révocation des*

      https://support.microsoft.com/en-us/topic/kb5025885-how-to-manage-the-windows-boot-manager-revocations-for-secure-boot-changes-associated-with-cve-2023-24932-41a975df-beb2-40c1-99a3-b3ff139f832d
  - Exécution de code à l'ouverture d'un fichier RTF contenant un objet OLE (CVE-2023-29325)
- Les plus critiques ou les plus intéressantes
  - Exécution de code à l'ouverture d'un mail depuis **Outlook** (CVE-2023-29325)
  - Elévation de privilèges depuis **Sysmon** 😳 (CVE-2023-29343)
  - Exécution de code à la lecture d'une vidéo **AV1** (CVE-2023-29340 et CVE-2023-29341)
  - Exécution de code à distance dans **SharePoint** (CVE-2023-24955)
  - Exécution de code sur le pilote **BlueTooth…** à distance 😨(CVE-2023-24947)
  - Exécution de code à l'ouverture d'un fichier RDP (CVE-2023-24905)
  - Exécution de code à distance sur le service Message Queuing (CVE-2023-24943)
  - Exécution de code à distance sur le protocole de tunneling SSTP (CVE-2023-24903)
  - Exécution de code à distance sur LDAP (CVE-2023-28283)

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 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 18 octobre 2022	mardi 14 octobre 2025	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
Navigateurs (principales failles)

Chrome, 3eme 0-day exploitée dans la nature

- Après CVE-2023-2033 (confusion de type dans V8) et CVE-2023-2136 (dépassement d'entier)
- Voici CVE-2023-3079 (encore une confusion de type dans V8)
  - Découverte par Google **car** exploitée dans la nature

https://chromereleases.googleblog.com/2023/06/stable-channel-update-for-desktop.html

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

GoLang <1.20.5 et <1.19.10, plusieurs vulnérabilités

- CVE-2023-29402, injection sur le nom du module s'il contient \n
- CVE-2023-29403, élévation de privilèges si le programme a le bit suid
- CVE-2023-29404, injection si un module spécifié l'option "#cgo LDFLAGS"

https://groups.google.com/g/golang-announce/c/q5135a9d924

KeePass <2.54, récupération de la clef maître en mémoire (CVE-2023-32784)

- Directement en mémoire, dans le swap, dans le fichier d'hibernation
- Liée à une faible des fenêtres de saisie de Windows (TextBox et TextBox.PasswordChar)
- PoC:

https://github.com/vdohney/keepass-password-dumper

https://keepass.info/news/n230603_2.54.html

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

N8n, plusieurs vulnérabilités critiques (CVE-2023-27562, CVE-2023-27563, CVE-2023-27564)

- Path traversal
- Contournement de l'authentification
- Elévation de privilèges

https://www.synacktiv.com/sites/default/files/2023-05/Synacktiv-N8N-Multiple-Vulnerabilities_0.pdf

Oracle WebLogic, exécution de code sans authentification (CVE-2023-21839)

- Utilisation de la connexion JNDI (log4j…) vers LDAP
  - Retour d'une URL vers une site où vous hébergez votre class Java malveillante
- Code d'exploitation

https://packetstormsecurity.com/files/172882/cve_2023_21839_weblogic_rce.rb.txt

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

RCE sur la librairie Python ReportLab PDF (CVE-2023-33733)

- Bibliothèque Python qui permet de générer des fichiers PDF à partir d'une entrée HTML
- Vulnérabilité qui permet de bypasser les restrictions de la sandbox
  - Manque de vérifications du côté de la fonction rl_safe_eval
  - Possibilité d'exécuter du code sur le système au moment de la génération en PDF

https://security.snyk.io/vuln/SNYK-PYTHON-REPORTLAB-5664897

https://github.com/c53elyas/CVE-2023-33733 (PoC)

Faille critique sur GitLab (CVE-2023-2825)

- Faille critique (CVSS 10) qui permet d'exploiter un Path Traversal
  - Permet à un utilisateur non authentifié de lire le contenu de fichiers sensibles
- Version 16.0.0 de GitLab Community Edition et Enterprise Edition vulnérable

https://securityonline.info/cve-2023-2825-critical-bug-in-gitlab-with-cvss-score-of-10/

https://github.com/Occamsec/CVE-2023-2825

Failles / Bulletins / Advisories
Réseau (principales failles)

Nessus, multiples vulnérabilités (CVE-2021-20031)

- Plusieurs vulnérabilités authentifiées dans libxml2
  - Corruption de mémoire et potentielle exécution de code
  - Relativement complexes à exploiter

https://www.tenable.com/security/tns-2023-20

Zyxel, multiples vulnérabilités critiques

- Injection de commande avant authentification sur IKE (CVE-2023-28771)
  https://attackerkb.com/topics/N3i8dxpFKS/cve-2023-28771/rapid7-analysis
- Exécution de code par une lecture de fichier et prédiction du mot de passe ‘supervisor’ (CVE-2023-28770)
  https://packetstormsecurity.com/files/172277/zyxel_lfi_unauth_ssh_rce.rb.txt

Failles / Bulletins / Advisories
Réseau (principales failles)

Fortinet, RCE pre-auth sur le VPN (CVE-2023-27997)

- Tweet le dimanche 11/06 et plein d'articles… référençant le tweet
  - Tweet d'une personne "fiable"
    https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/
    https://thehackernews.com/2023/06/critical-rce-flaw-discovered-in.html
    https://www.securityweek.com/fortinet-patches-critical-fortigate-ssl-vpn-vulnerability/
  - Les articles citent Olympe Cyberdefense, société FR inconnues 🤔
    - Avec son offre "**Talos**" (ils vont être contents chez Cisco Talos)
- Correctif "à priori" en 6.2.15, 6.4.13, 7.0.12 et 7.2.5 mais :
  - **Rien** dans le PSIRT Fortinet 🤔
    https://www.fortiguard.com/psirt
  - **Rien** dans les releases notes Fortinet 🤔
    https://docs.fortinet.com/document/fortigate/7.2.5/fortios-release-notes/760203/introduction-and-supported-models
    https://docs.fortinet.com/document/fortigate/7.0.12/fortios-release-notes/760203/introduction-and-supported-models
    https://docs.fortinet.com/document/fortigate/6.4.13/fortios-release-notes/760203/introduction-and-supported-models
    https://docs.fortinet.com/document/fortigate/6.2.15/fortios-release-notes/760203/introduction-and-supported-models
  - **Rien** sur le MITRE (CVE reserved) 🤔
- N'est-ce pas le rôle de l'éditeur d'alerter publiquement sur la criticité de la vuln !!?
  - Et donc d'informer les DSI sur l'urgence à mettre à jour

Maj du 13/06
- Vuln officialisée
  https://www.fortiguard.com/psirt/FG-IR-23-097

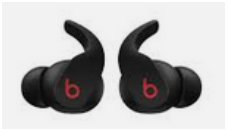
Failles / Bulletins / Advisories
Réseau (principales failles)

Faille dans Cisco Secure Client (CVE-2023-20178)

- Permet d'obtenir les droits SYSTEM sur Windows
  - Sans interaction utilisateur
  - Dangereuse en local (CVSS 7.8)
- Versions Secure Mobility avant 4.10MR7 et Secure Client < 5.0MR2 concernées → MAJ
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-csc-privesc-wx4U4Kw

Failles / Bulletins / Advisories
Smartphones (principales failles)

Mettez à jour vos écouteurs



- Beats Fit et Beats Fit Pro
- AirProd, AirPods Pro et AirPods Max
- Usurpation de l’identité de la source lors d’un appairage ou jumelage (CVE-2023-27964)
    - https://support.apple.com/en-us/HT213752

Failles / Bulletins / Advisories
Autre (principales failles)

Des millions de carte mère Gigabytes avec une porte dérobée… panique !!!

- En fait… pas vraiment 😂
- Fonctionnalité “dégueulasse” de mise à jour du firmware
  - Peut être utilisée par un malware pour persister et installer son propre firmware

https://eclypsium.com/blog/supply-chain-risk-from-gigabyte-app-center-backdoor/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Barracuda, brulez vos appliances ESG (Email Security Gateway Appliance) **!!!**

- Vulnérabilité 0day exploitée depuis… octobre 2022 (CVE-2023-2868)
  - Injection de commande à distance
  - Corrigé en mai 2023
- Soupçons le 18 mai
  - Appel à Mandiant pour analyser
  - Le 19, identification de la compromission
  - Les attaquants ont installés une porte dérobée inspirée d'un vieil outil public (cd00r)

https://www.bleepingcomputer.com/news/security/barracuda-says-hacked-esg-appliances-must-be-replaced-immediately/

- Barracuda pourrait remplacer gratuitement les boîtiers infectés
  https://www.it-connect.fr/impacte-par-la-faille-zero-day-dans-lappliance-barracuda-demandez-un-nouveau-boitier/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Injection SQL chez MOVEit Transfer exploitée depuis 2021

- Logiciel de transfert de fichiers sécurisé
- Injection SQL découverte (CVE-2023-34362) permettant l'envoi de code arbitraire
  - Exploitée depuis 2021 par le groupe de ransomware Clop 🇷🇺 (selon Kroll 🇺🇸)
  - Toutes les branches ont un patch disponible (2020.1.x → 2023.0.0)
- Audit de sécurité mené ensuite
  - Plusieurs injections SQL critiques trouvées = CVE-2023-35036

https://www.it-connect.fr/le-ransomware-clop-connait-la-faille-zero-day-dans-moveit-transfer-depuis-2021/

Deepfake de Vladimir Poutine

- Diffusé pendant 40 minutes en Russie le 5 juin
  - Suite à un piratage des antennes de TV et de radio à Moscou
- Le (faux) président déclare l'invasion ukrainienne en Russie

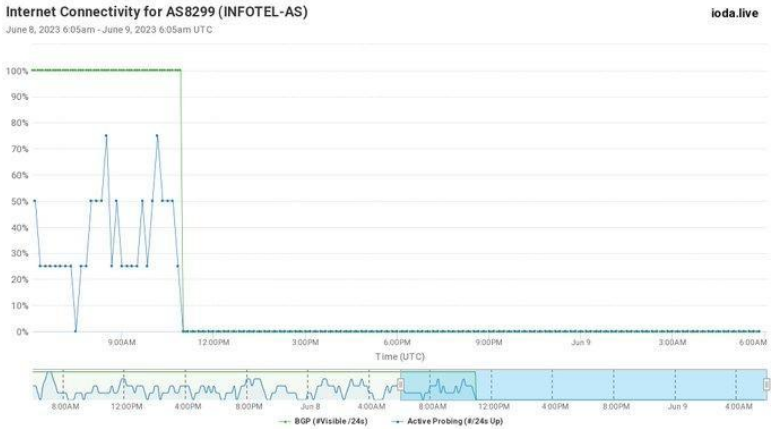
https://twitter.com/nexta_tv/status/1665701461865447424

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage du réseau telecom Russe (infotel)

- Gros impact sur le réseau bancaire
  - Plus de 36h de panne
- A priori piraté par hacktivistes pro-ukraine

https://twitter.com/igorsushko/status/1667046475220795392



Piratages, Malwares, spam, fraudes et DDoS
Malware

Désactivation de Snake, opération Medusa du FBI

- Semblerait lié au FSB (à l'origine des outils Turla et Uroburos)
  - Daterait de plus de 20 ans et serait l'un des principaux outils du FSB

https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network

- Opération MEDUSA, communication avec le C&C et envoie d'un ordre de se désactiver
- Rapport impressionnant de détails techniques :
  - TTP, identifiants MITRE ATT&CK
  - Règles Yara et Suricata
  - Les clefs de base de registre à regarder pour identifier une infection
  - Un plugin Volatility en Python pour analyser une capture mémoire et détecter Snake

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

- Publié le 9 mai, date du « jour de la victoire » (signature de la capitulation Allemande en 1945)
  - Message passé aux Russes: on vous voit depuis 20 ans
    - Ou juste pour les faire douter : quel crédit donner aux infos rapportées si les américains étaient au courant
- Réponse Russe ?
  - Annoncer que l'opération "Triangulation" est américaine
  - Kaspersky a utilisé MVT :)

https://securelist.com/operation-triangulation/109842/

https://www-fsb-ru.translate.goog/fsb/press/message/single.htm!id=10439739@fsbMessage.html?_x_tr_sch=http&_x_tr_sl=ru&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=wapp

Piratages, Malwares, spam, fraudes et DDoS
Malware

Kaspersky victime de Triangulation (malware)

- Plusieurs Iphone chez Kaspersky infectés par Triangulation
- Quelques découvertes après l'analyse de l'équipe …
  - Propagation par IMessage invisible
  - Exploitation de code dès la réception sans aucun clic nécessaire
  - Elévation de privilèges et compromission des données sur l'appareil
- Systèmes iOS < 15.7 vulnérables

https://www.schneier.com/blog/archives/2023/06/operation-triangulation-zero-click-iphone-malware.html

https://github.com/KasperskyLab/triangle_check/releases (outil de vérification)

Piratages, Malwares, spam, fraudes et DDoS
Malware

Predator d'Intellexa analysé

- Cible Android
- Analysé par Citizen Lab, puis Google et enfin Talos !
- Contient des exploits pour 5 vulnérabilités assez anciennes:
  - CVE-2021-37973, exécution de code dans Chrome
  - CVE-2021-37976, fuite de données dans Chrome (contournement d'ASLR)
  - CVE-2021-38000, permet de faire traiter des URL par une autre application que Chrome
  - CVE-2021-38003, exécution de code dans Chrome
  - CVE-2021-1048, élévation locale de privilèges dans Linux
  - Pas de grande fraîcheur mais l'écosystème android est complexe…
- Vendu à l'Arabie saoudite, l'Arménie, l'Égypte, la Grèce, l'Indonésie, Madagascar, le sultanat d'Oman et la Serbie

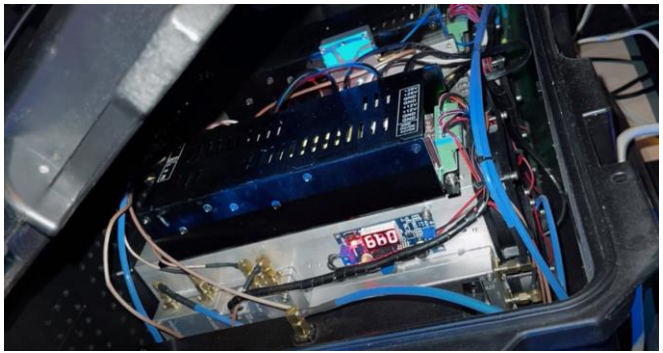
https://www.lemondeinformatique.fr/actualites/lire-le-spyware-predator-pour-ios-et-android-disseque-90568.html

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Arnaqueurs au SMS

- <<Elle se fait arrêter sous stup' avec un IMSI Catcher dans le coffre>>
- Envoie massif de SMS (~war driving) + collecte de n°
  - CPAM, Mon Compte Formation, banque…
  - ~~Faille~~ fonctionnalité du protocole 2G
- Réseau sans tête
  - Beaucoup d'arnaqueurs indépendants en IdF
  - Dont des lycéens

https://www.leparisien.fr/faits-divers/paris-a-16-ans-le-pirate-20-proposait-des-kits-de-phishing-destines-aux-escrocs-14-04-2023-DOY2OWG7GVB6XAPFVXPVMHTJJE.php

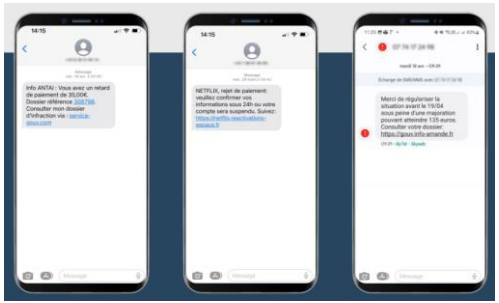


- Vidéo de micode

https://www.youtube.com/watch?v=6Jv0EzXdQbk

  - Basée sur les travaux de tad et son outil StalkPhish
    https://github.com/t4d/StalkPhish
  - Ne faites PAS ça chez vous !!!!

https://www.bouyguestelecom.fr/choisir-bouygues-telecom/stop-arnaque#Description



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

Voyageurs du monde, publication de 10 000 passeports

- Piratage par Lockbit
  - Réutilisation d'un mot de passe (password reuse)
- Publication de plus de 10 000 passeports
- Réponses de l'agence de voyage:
  - <<`ce n'est que 1% de ce que nous avons`>> Quoiiiiiiiiiiiiii !!?
  - <<`ce ne sont que des copies`>> donc c'est pas grave !!?

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/l-agence-voyageurs-du-monde-victime-d-une-cyberattaque-ils-font-les-malins-pour-pas-grand-chose-rassure-le-pdg-du-groupe_5871401.html

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Encore une panne Microsoft 365 (EX571516)

- 8h de panne !
  - La 7eme de l'année

https://www.lemondeinformatique.fr/actualites/lire-une-7eme-panne-pour-microsoft-365-90637.html

Grosse panne de 10h chez Datadog

- Mise à jour de systemd et systemd-networkd a effacé les routes réseau entre les conteneurs
- Panne de 10 000 noeuds kubernetes, et c'est long à démarrer
- Analyse juste avec les informations publiques :
  https://newsletter.pragmaticengineer.com/p/inside-the-datadog-outage
- Rapport officiel publié bien après :
  https://www.datadoghq.com/blog/2023-03-08-multiregion-infrastructure-connectivity-issue/

Google, incendie dans le Datacenter parisien europe-west9-a

- Potentiellement du fait d'une pompe de refroidissement défectueuse
- Panne car 2 zones sur 3 dans ce DC et de corum pour la reprise
  - Impact sur BigTable

https://www.lebigdata.fr/data-center-panne

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Bug sur les SSD SanDisk

- Perte d'accès soudain aux données sur les SSD Sandisk
  - Modèles Extreme et Extreme Pro, 2 et 4 To, sortis après novembre 2022 affectés
  - Pas plus d'informations sur le pourquoi
- Mise à jour du firmware pour le modèle 4 To prochainement disponible
  - Pas plus d'infos pour le modèle 2 To

https://www.it-connect.fr/a-cause-dun-bug-les-ssd-portables-sandisk-deviennent-illisibles/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Feuille de route du Numérique en Santé

- Avec un volet Cyber:
  - Améliorer la résilience (CARE)
  - Faire des exercices de crise
  - Ré-internaliser les experts

https://sante.gouv.fr/actualites/actualites-du-ministere/article/lancement-de-la-feuille-de-route-du-numerique-en-sante-2023-2027

https://sante.gouv.fr/IMG/pdf/feuille_de_route_du_numerique_en_sante_2023-2027.pdf

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

Red Team Outil pour aider à trouver des drivers faillibles

- Permettant de “tuer” d’autres processus
  - Simple recherche à partir d’une liste JSON
- Peut être utiliser pour “tuer” un AV ou EDR

https://github.com/xalicex/LOLDrivers_finder

Red Team Des codes d’exploitation de CVE

- Moteur de recherche

https://cvexploits.io/

- Attention aux codes piégés

https://github.com/0xDarv1n/ssh-privesc-poc

https://github.com/0xDarv1n/apache-2.4.57-rce-poc-exploit

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

Red Team Contourner AMSI simplement…

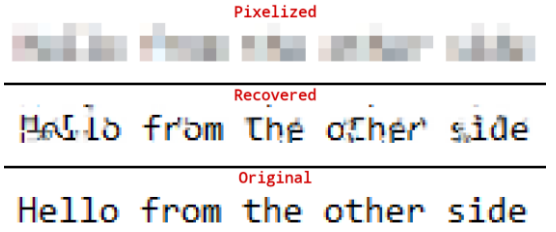
- En créant une DLL amsi.dll contenant l'export "AmsiScanBuffer 🥷♂
  - Puis vous lancer votre code malveillant dans le même répertoire

https://twitter.com/eversinc33/status/1666121784192581633

Images pixélisées ? Pas si secure …

- Outil permettant de retrouver le texte sur une image pixelisée
  - Uniquement celles créées avec un filtre de boîte linéaire
- Le rectange noir reste une valeur sûre 😎

https://github.com/beurtschipper/Depix



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

NON, je ne veux pas de tes cookies !

- Permet de contourner les paywalls en ligne
- Exemple avec marmiton.org
  - https://12ft.io/proxy?&q=https%3A%2F%2Fwww.marmiton.org
- Le site a été désactivé plusieurs fois
  - Il renvoyait une erreur HTTP 451 (Indisponible pour des raisons légales)
  - Paywalls, cookie walls et log walls on en parle ?
- Ne fonctionne malheureusement pas partout
  - KO du côté Bloomberg, The New York Times et The Athletic

https://12ft.io/

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

CVSSv4 te voilà… ou presque

- Permet d’évaluer les risques via un score (CVSS)
- Se base sur plusieurs mesures :
  - Facilité d'exploitation
  - Impact sur la confidentialité, intégrité, disponibilité
  - Niveau requis d'interaction de l'utilisateur
- Quoi de nouveau ?
  - En autre, se concentré beaucoup plus sur la complexité de l’attaque
  - Plusieurs étapes nécessaires ? Exploits connus dans la nature ?

https://www.first.org/cvss/v4-0/

Nouveautés
Divers

OWASP : API Top 10

- Release candidate
- https://github.com/OWASP/API-Security/tree/master/2023/en/src
  1. *broken-object-level-authorization*: **Fuite** d'info sur des API
  2. *broken-authentication*: Contournement de l'**authentification**
  3. *broken-object-property-level-authorization*: Mauvaise gestion de l'**autorisation** sur des **objets**/données
  4. unrestricted-resource-consumption: Absence de **limites** du nombre d'appels
  5. *broken-function-level-authorization*: Mauvaise gestion de l'**autorisation** sur des appels de **fonctions**
  6. server-side-request-forgery: **SSRF**, on aime 😉
  7. *security-misconfiguration*: Défaut de **configuration**
  8. *lack-of-protection-from-automated-threats*: Absence de blocage des attaques automatisées
     i. Ressemble beaucoup au 4
  9. *improper-assets-management*: Inventaire des actifs non à jour
  10. *unsafe-consumption-of-apis*: Manque/absence de sécurisation des appels API
      i. Semble rassembler un peu toutes les techniques d'injection

Business et Politique

Business
Monde

Sekoia.io lève 35m€

- Avec la caisse des dépôts, Bright Pixel, Omnes, Seventure et BNPP
  - Après une série A de 10m€ (include dedans?)

    https://www.usine-digitale.fr/article/sekoia-leve-10-millions-d-euros-pour-accelerer-la-commercialisation-de-sa-plateforme-de-cybersecurite.N1013229

https://www.linkedin.com/posts/sekoia_sekoiaio-just-raised-a-record-breaking-35m-activity-7067016388736868352-P-42

Droit / Juridique / Politique
Monde

Activer un téléphone à distance

- Afin de le localiser et écouter ce qui est dit
  - Enquête sur un crime ou délit puni de +5 ans de zonzon
- Adopté par le Sénat

https://www.actu-juridique.fr/justice/pure-folie-estime-v-niore-a-propos-de-lactivation-a-distance-des-telephones-portables/

Droit / Juridique / Politique
Monde

Clearview AI, encore une amende de la CNIL

- Déjà une amende de 20m€ en xxx, cf. revue 2022-01-11, 2022-06-14
  - Avec une astreinte de 100k€/jour en cas de non effacement des données des français
- Réponse de Clearview : RANAFOUT' !
  - Ils ne seraient pas capable de retrouver la nationalité des personnes dans leur base
- CNIL is back : liquidation de l'astreinte pour 5,2m€
  - Affaire à suivre…

https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-liquide-lastreinte-prononcee-lencontre-de-clearview-ai

Microsoft XBox, amende de $20m aux USA

- Collecte des données personnelles d'enfants de moins de 13 ans
- Car pas de blocage de création de compte pour les enfants

https://kotaku.com/xbox-microsoft-ftc-illegal-fine-glitch-childres-profile-1850509207

L’observatoire

Observatoire
Rapport

Panorama des cybermenaces Maritimes 2022

- Par le France Cyber Maritime (M-CERT) et Own

  https://www.own.security/analyses

  https://share.own.security/s/tgL26oYXPQgL8d7

Conférences

Conférences

Passée

- SSTIC, 7 au 9 juin 2023 😎🤩🤑

A venir

- 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
- Barbhack, 26 août 2023 à Toulon

Divers / Trolls velus

Divers / Trolls velus

Tu penses qu’il triche aux échecs avec un plug anal ?

- Pirate-le avec ton Flipper Zero

  https://twitter.com/HTTP_Lovecraft/status/1656029332593098761

Divers / Trolls velus

TLD .zip, super idée !

https://github.com/kubernetes/kubernetes/archive/refs/tags/@v1271.zip

- Vous cliquez sur lequel ? ----------> https://github.com/kubernetes/kubernetes/archive/refs/tags/v1.27.1.zip
  - @ + caractères unicode U+2044 (⁄) et U+2215 (∕)

https://medium.com/@bobbyrsec/the-dangers-of-googles-zip-tld-5e1e675e59a5

L'Iran se met au processeur Quantique

- Grosse révolution…
- Ou pas !

https://twitter.com/GLNoronha/status/1666885129082396679

Divers / Trolls velus

Drama sur le CTF…

- CTF PWNME avec une petite indispo au début, vite corrigée et stabilisée
- Tout à basculé quand la direction a décidé de tout migrer en plein milieu du CTF

  https://twitter.com/Atlas453_/status/1656740040855154718

  https://web.archive.org/save/https://twitter.com/Atlas453_/status/1656740040855154718

Pendant qu'il fait la promo du livre de ses récits hallucinés

- Certains ne tombent pas dans le panneau

  https://twitter.com/gabrielthierry/status/1661279708095422464

  https://www.marianne.net/societe/big-brother/cybernegociateur-ou-escroc-letonnante-confession-dun-hacker-francais-avant-son-proces

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

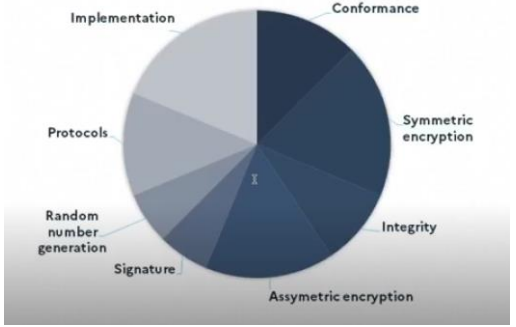
- Sa mise en examen suit son cours
  - **Extorsion** en **bande organisée**, passible de 20 ans de prison et de 150 000 euros d'amende

Divers / Trolls velus

Tous à la crypto !

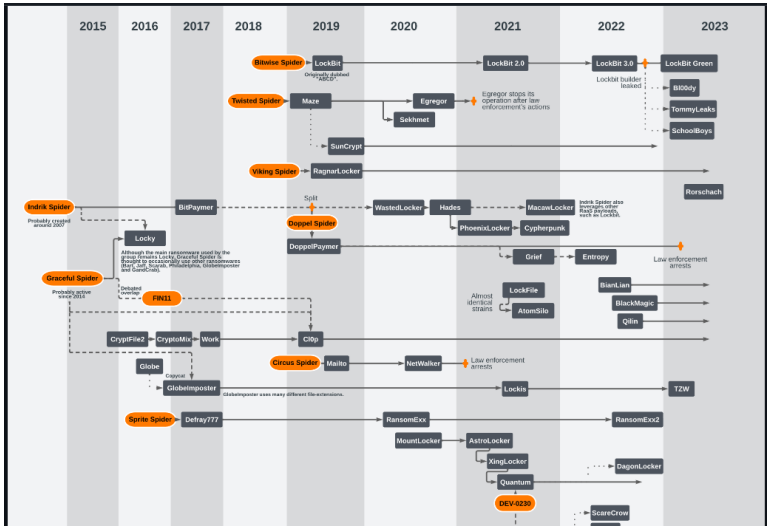
- Plateforme d'apprentissage mis à disposition par l'**ANSSI**
- Application de messagerie (Element) vulnérable sur **36 points**

https://github.com/ANSSI-FR/cry-me



Frise chronologique des groupes de rançongiciels

https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf



Divers / Trolls velus

2FA obligatoire sur PyPI

- Dépôt de plus de 200 000 paquets Python
  - Convoité par les attaquants (supply chain)
- MFA obligatoire sur les comptes dev en fin d'année 2023
  - Clé de sécurité ou application d'authentification (TOTP)

https://www.silicon.fr/pypi-mfa-466329.html

Compte Google inactif depuis + 2 ans = inactif = 🗑

- Permet de lutter contre le vol de compte
  - Ancien compte = mot de passe faible + MFA désactivé
- Toutes les données de ces comptes seront supprimées (ou déplacées 🤭)
  - Données venant de Google Drive, Google Photos, Gmail, YouTube, etc.

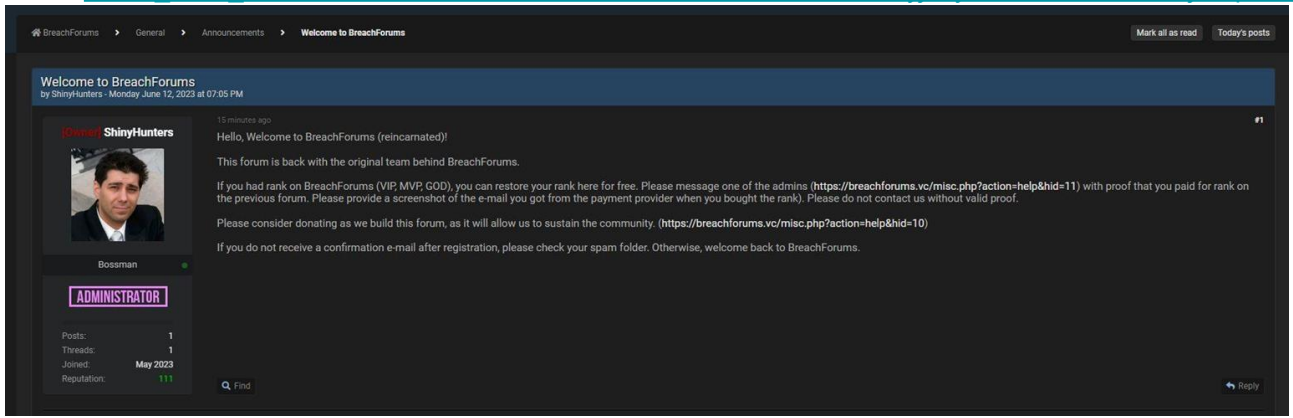
https://www.it-connect.fr/attention-google-va-supprimer-les-comptes-inactifs-depuis-plus-de-deux-ans/

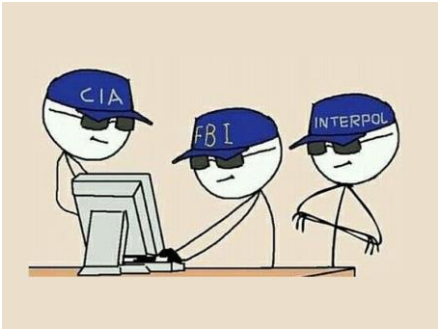
Divers / Trolls velus

Breachforum is back or FBI is ready

- Fermé le **22 mars 2023**
  - Administrateur “Pompompurin” arrêté par le FBI
  - Tentative de reprise par Baphomet qui a fini par abandonner
- **3 mois** après : ré-ouverture !
  - Annonce réalisée par un membre de ShinyHunters
  - Reprise de grande gratuitement
- Ça sent le piège Faut-il qu’il soit en place ---------->

https://media.licdn.com/dms/image/D4E22AQEXtY2DiNQ2Fw/feedshare-shrink_2048_1536/0/1686597806354?e=1689206400&v=beta&t=zWhyjb4y0nc0E-oxwAuKYr5jWxpU6rVQ0yF5gxh2sTM





Divers / Trolls velus

Au revoir Cortana !

- Microsoft annonce la fin de support pour 2023
- Préfère se concentrer sur ses nouveaux bébés
  - Windows Copilot pour Windows 11
  - Windows 365 Copilot
  - Bing IA

https://support.microsoft.com/en-us/topic/end-of-support-for-cortana-in-windows-d025b39f-ee5b-4836-a954-0ab646ee1efa

L’armée américaine recrute ! Sur 4chan :)

- Plusieurs postes incitant à rejoindre l’armée trouvés sur 4chan
  - Difficile de confirmer la source

https://twitter.com/LookAtMyMeat1/status/1636900998714122241

https://www.numerama.com/cyberguerre/1409480-larmee-americaine-tenterait-de-recruter-sur-le-polemique-forum-4chan.html

Divers / Trolls velus

Comment ce site n'est-il pas encore coupé !!?

- Accès à de très nombreuses fuites de données
  - Indexées dans une base de données
- Site créé pour contrarier Peter Kleissner qui vend des recherches dans des fuites de données

https://search.illicit.services/

Liste des 200 sociétés les mieux sécurisées

- Classement fait par Forbes, basé sur les notes de SecurityScorecard
  - N°1 Intel
  - N°4 Palantir
- La meilleure idée du monde
  - 3…2…1…attaquez !

https://www.forbes.com/lists/most-cybersecure-companies/

Prochaines réunions

Prochaine réunion

- Mardi 11 juillet

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