Revue d'actualité de l'OSSIR

11 octobre 2022

Christophe Chasseboeuf
*Vladimir Kolla @mynameisv_*

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de septembre 2022 très très chaud !

- **IKE**, Exécution de code à distance (CVE-2022-34721 et CVE-2022-34722)
  - CVSS: 9.8/10, exploité dans la nature
  - Exploit stable : https://github.com/78ResearchLab/PoC/tree/main/CVE-2022-34721
- API de journalisation (**CLFS**), élévation locale de privilèges (CVE-2022-37969)
  - CVSS: 7.8/10, découvert par (Mandiant, Zscaler, Crowdstrike) exploité dans la nature
- **IPv6**, Exécution de code à distance (CVE-2022-34718)
  - CVSS: 9.8/10, paquet routable

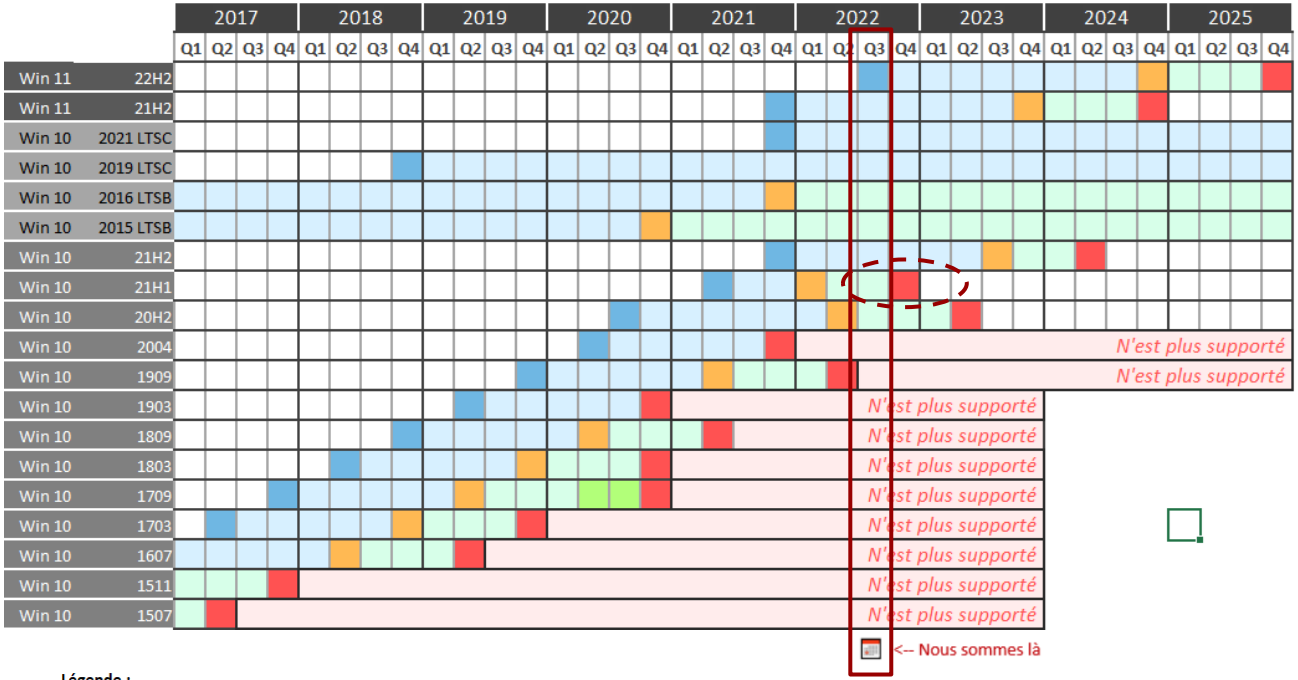
Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Attendez… c'est pas fini…

- **Visual Studio**, exécutions de code, protégez à vos développeurs 👍(CVE-2022-35777, CVE-2022-35825, CVE-2022-35826, CVE-2022-35827)
- **Exchange**, élévations de privilèges
- VPN « **PPP** », exécution de code à distance et sans authentification (CVE-2022-30133)
- **Bluetooth**, exécution de code à distance et sans authentification (CVE-2022-30144)
  - Désactivez le Bluetooth de votre ordi par défaut, c'est une bonne pratique
- **NFS**, exécution de code à distance et sans authentification 😱 (CVE-2022-34715)
- **SMB**, exécution de code à distance et sans authentification client et serveur 😳 (CVE-2022-35804)
- **Excel**, contournement des restrictions, à utiliser dans un phishing (CVE-2022-33631)
- **Fax**, élévation locale de privilèges… 2022… le Fax…🤦♂ (CVE-2022-34690)
- **Spooler** d'impression, encore des vulnérabilités 🤯 (CVE-2022-35755, CVE-2022-35793)
- **Hyper-V**, évasion de machine virtuelle (CVE-2022-34696)
- **Credential Guard**, contournement 🤦♀(CVE-2022-34709)
- Windows **Hello**, contournement de l'authentification 🤦♂ (CVE-2022-35797)
- **Secure Boot**, contournements 🤦♀(CVE-2022-34301 et CVE-2022-34303)
- Chromium-Edge, 16 vulnérabilités

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

macOS, la vérification des certificats était cassée (CVE-2022-26766)

- Depuis des années
- Possibilité de générer une chaîne certificat valide et de signer une application
  - Avec l’extension appleCertificateExtensions

https://worthdoingbadly.com/coretrust/

https://github.com/zhuowei/CoreTrustDemo/blob/main/badcert/makecerts.sh

Failles / Bulletins / Advisories
Systèmes

macOS / iOS, élévation locale de privilèges (CVE-2022-32917)

- Activement exploitée dans la nature
  - Dans des chaînes d'exploitation 1-click et 0-click
- Beaucoup d'autres vulnérabilités corrigées :
  - iOS 15.7 https://support.apple.com/en-us/HT213445
  - iOS 16 https://support.apple.com/en-us/HT213446
  - iPadOS 15.7 https://support.apple.com/en-us/HT213445
  - macOS Big Sur 11.7 https://support.apple.com/en-us/HT213443
  - macOS Monterey 12.6 https://support.apple.com/en-us/HT213444

iOS < 16.0.3 , l'email qui casse tout (CVE-2022-22658)

- Si l'expéditeur est: `""@example.com`

  https://support.apple.com/en-us/HT213480

Failles / Bulletins / Advisories
Les 0-days du vendredi (ou commencer passer un mauvais week-end)

Vendredi 30 septembre 2022

Exchange, *ProxyNotShell*, exécution de code à distance (CVE-2022-41040 et CVE-2022-41082)

- SSRF depuis l'autodiscover, permettant d'appeler PowerShell *(seconde vuln)*
    - Découvert par une "blue team" **car** exploitée dans la nature
  - **Correctif** : non disponible, contournement dans l'article de Microsoft
    - Le blocage sur ".*autodiscover\.json.*\@.*Powershell.*" est contournable par ".." au lieu de "@"

      https://twitter.com/wdormann/status/1576922677675102208
  - **Exploitée** : activement et massivement dans la nature ⚠
- SSRF :

  `https://mail.monexchange.com/autodiscover/autodiscover.json?@attaquant.com/&Email=autodiscover/autodiscover.json%3f@attaquant.com`

  ou

  `https://mail.monexchange.com/autodiscover/autodiscover.json?@outlook.com/&Email=autodiscover/autodiscover.json%3f@monexchange.com`

  https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

  https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
- Correctif ce jour à 18h GMT

Failles / Bulletins / Advisories
Les 0-days du vendredi (ou commencer passer un mauvais week-end)

Vendredi 7 octobre 2022

Zimbra, exécution de code à distance (CVE-2022-41352)

- Path traversal à la décompression (*comme CVE-2022-30333*) d'un .cpio par l'antivirus amavis
  - **CVSS**: 9.8/10
  - **Versions**: Zimbra Collaboration 8.8.15 et 9.0 sur Debian, RedHat et CentOS mais pas Ubuntu (par défaut) ;
  - **Correctif** : non disponible pour l'instant, installez « pax »

    https://blog.zimbra.com/2022/09/security-update-make-sure-to-install-pax-spax/
  - **Exploitée**: activement et massivement dans la nature ⚠
  - **Mitre ATT&CK**: T1574.010

FortiOS, prise de contrôle à distance (CVE-2022-40684)

- Contournement de l'authentification sur le portail web d'admin
  - Fortinet a communiqué l'info discrètement à ses clients "joignables"
  - **CVSS**: 9.6/10
  - **Versions**: FortiOS 7.0.0 à 7.0.6 et 7.2.0 à 7.2.1, FortiProxy 7.0.0 à 7.0.6 et 7.2.0
  - **Correctif** : disponible, mais ne jamais exposer un portail d'admin sur internet, **JAMAIS →**
  - **Exploitée** : exploitée par des groupes spécifiques et pas encore massivement
  - **Mitre ATT&CK**:T1548.002

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

Base de données Redis, exécution de code à distance (CVE-2022-35951)

- Dépassement de mémoire du tas
  - En appellant la commande XAUTOCLAIM avec un COUNT trop grand

  https://github.com/redis/redis/security/advisories/GHSA-5gc4-76rx-22c9

Atlassian Confluence, application "Questions For Confluence" (CVE-2022-26138)

- Compte caché (pour des migrations cloud) avec mot de passe en dur :
  - User: `disabledsystemuser`
  - Password: `disabled1system1user6708`

https://github.com/alcaparra/CVE-2022-26138

BitBucket, injection de commande sans authentification (CVE-2022-36804)

- Avec une simple commande :

```
# git archive --prefix xd --exec='echo pew#' --remote=file:///tmp/ -- blah
-> execve('/bin/sh','-c','echo pew# /tmp')
```

https://blog.assetnote.io/2022/09/14/rce-in-bitbucket-server/

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

Python, path traversal

- Vuln veille de 15 ans, 350 000 projets open source vulnérables… Panique !
- Ou pas…
  - “Path traversal” sur les archives .tar documenté depuis 15 ans

https://www.bleepingcomputer.com/news/security/unpatched-15-year-old-python-bug-allows-code-execution-in-350k-projects/
https://docs.python.org/3/library/tarfile.html

> **Warning:** Never extract archives from untrusted sources without prior inspection. It is possible that files are created outside of *path*, e.g. members that have absolute filenames starting with `"/"` or filenames with two dots `".."`.

Teams, stockage des jetons de session en clair

- Stockage en clair dans une base SQLite… Panique !
- Ou pas…
  - Nécessite une première prise de contrôle à distance
  - Si l’host est compromis, c’est TRES compliqué de protéger un jeton

https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/

- Mais Teams reste sensible : SharePoint, OneDrive…

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

Teams, GIFShell

- Utiliser Teams comme canal de communication C2
- Avec des images GIF :
  - Téléchargées par Microsoft
  - Non scannées par les AV/EDR

https://medium.com/@bobbyrsec/gifshell-covert-attack-chain-and-c2-utilizing-microsoft-teams-gifs-1618c4e64ed7

pSence, exécution de commande sans authentification

- En ajoutant une règle sans authentification
- Avec une commande shell dans le nom

```
"name": '../../../tmp/rules.packages.|'+cmd+'|'
```

https://ssd-disclosure.com/ssd-advisory-pfsense-post-auth-rce/

Magento, exécution de commande sans authentification (CVE-2022-24086)

- Par un simple paramètre

```
{{var this.getTemplateFilter().addAfterFilterCallback("system").filter("ls")}}
```

https://support.magento.com/hc/en-us/articles/4426353041293-Security-updates-available-for-Adobe-Commerce-APSB22-12-

Failles / Bulletins / Advisories
Smartphones (principales failles)

Whatsapp, exécution de code à distance (CVE-2022-36934 et CVE-2022-27492)

- Exécution de code par dépassements d'entier lors d'un appel vidéo CVE-2022-36934
- Exécution de code par dépassements d'entier à l'ouverture d'une vidéo CVE-2022-27492

https://www.whatsapp.com/security/advisories/2022/

Apple, élévation locale de privilèges (CVE-2022-32917)

- Exploitée dans la nature pour des chaînes d'exploitation 0-click ou 1-click
- Touche tous les OS d'Apple:
  - iOS 15.7 https://support.apple.com/en-us/HT213445
  - iPadOS 15.7 https://support.apple.com/en-us/HT213445
  - macOS Big Sur 11.7 https://support.apple.com/en-us/HT213443
  - macOS Monterey 12.6 https://support.apple.com/en-us/HT213444

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage de Rockstar (serveur de dev?)

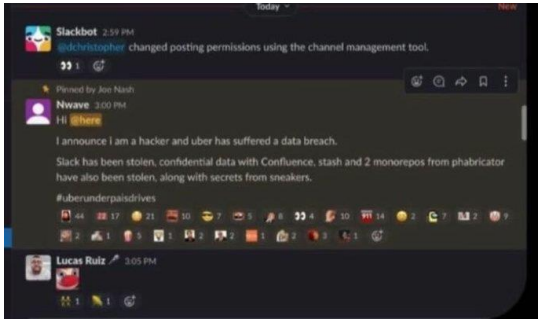
- Vol et publication de 90 vidéos de GTA 6
- Chantage à la publication du code source

https://www.lemondeinformatique.fr/actualites/lire-piratage-de-gta-6-et-uber-un-adolescent-arrete-au-royaume-uni-88127.html

Piratage de Uber

- Accès initial par le VPN d'un salarié (jeton ou login/pass)
- Script contenant un identifiant et mot de passe admin
  - Compromission des ESXi, AWS, GCP, OneLogin, SentinelOne...
- Ajout de moquerie sur le Slack, les rapports de bugbounty...

https://thehackernews.com/2022/09/uber-claims-no-sensitive-data-exposed.html



Rockstar et **Uber, arrestation d'un suspect**

- Anglais de 17 ans qui a plaidé non coupable
- "À priori" lié à Lapsus

https://www.usine-digitale.fr/article/un-adolescent-de-17-ans-arrete-pour-les-piratages-d-uber-et-rockstar-games.N2048312

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Facebook a été piraté, 1 millions de mots de passe en fuite…

- Ou pas 😋
- 400 app mobiles malveillantes identifiées sur les “stores”
  - 45 chez Apple et 355 chez Google
  - Ces app volent tout ce qu’elles peuvent
    - Jetons de session
    - Mots de passe, dont Facebook
    - …

https://www.bloomberg.com/news/articles/2022-10-07/facebook-warning-1-million-about-stolen-usernames-passwords

L’Iran pirate l’Albanie

- Rançongiciel visant les infra du gouvernement en juillet
- Suite à l’organisation d’une réunion d’opposants au régime iranien (annulé)

https://www.lemonde.fr/pixels/article/2022/09/07/l-albanie-rompt-ses-relations-diplomatiques-avec-l-iran-apres-une-cyberattaque_6140624_4408996.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Auth0 / Okta, fuite des codes sources de 2020 et avant

- Fuite de données en 2020 liée à une erreur de configuration
  - Désactivation de la ligne de conf activant la sécurité d'ELK par un admin de Cap Gemini
- Jugé à Singapour
  - Nom de l'admin cité partout sur internet 😢

https://auth0.com/blog/auth0-code-repository-archives-from-2020-and-earlier/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

CommonSpirit Health (USA) victime

- Retards dans les opérations chirurgicales, reprogrammation de rendez-vous

  https://www.nbcnews.com/tech/security/ransomware-attack-delays-patient-care-hospitals-us-rcna50919?cid=sm_npd_nn_tw_ma

Killnet cible les aéroports états-uniens

- 15 sites Web d'aéroports américains touchés par DDoS

  https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet

Piratages, Malwares, spam, fraudes et DDoS
Les groupes d'attaquants

Brute Ratel utilisé par les cybercriminels

- Après **Metasploit**, après **Cobalt Strike**, après **Immunity Canva**…
  - En version "warez"

https://www.lemondeinformatique.fr/actualites/lire-l-outil-de-test-d-intrusion-brute-ratel-dans-les-mains-des-cybercriminels-87331.html
https://twitter.com/BushidoToken/status/1575054022784208897

Lazarus, nouvelles activités

- Exploitation de vulnérabilités dans VMWare Horizon
  - Elevation de priviège depuis un pilote Dell (CVE-2021-21551)
- Persistance sur le long terme

https://blog.talosintelligence.com/2022/09/lazarus-three-rats.html

Fancy Bear et PowerPoint

- Utilisation d'un modèle de slides de l'OCDE
  - Activation de la charge utile lors d'une projection et si la souris bouge
  - Exécution de PowerShell avec SyncAppvPublishingServer

https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Piratage des PS4 et PS5

- Grâce à une vulnérabilité dans l'émulateur PS2 (lecture/écriture arbitraire)
- Seul code utilisant encore le JIT
  https://cturt.github.io/mast1c0re.html

Attaque BYOVD - Rançongiciel BlackByte

- Apportez votre propre pilote vulnérable
  https://fr.techtribune.net/securite/blackbyte-ransomware-abuse-dun-pilote-windows-vulnerable-pour-desactiver-les-solutions-de-securite/453793/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Ikea Tradfri - Un éclairage sur l'IOT

- Du contrôle dans l'air

  https://www.cnetfrance.fr/news/ikea-tradfri-une-faille-permet-de-controler-les-eclairages-intelligents-a-distance-39948150.htm

Binance balance

- Piratage et vol de 2 millions de Smart Chain BNB

  https://cryptoast.fr/hack-chain-prime-plusieurs-millions-dollars-pour-attraper-pirate/

Piratages, Malwares, spam, fraudes et DDoS
Vulnérabilités

Akamai - Mauvaise configuration

- Empoisonnement du cache avec du contenu arbitraire
  - Gain de $ 46 000

https://portswigger.net/daily-swig/researchers-net-46k-for-akamai-misconfiguration-vulnerability

VM2 sandbox en Javascript (CVE-2022-36067)

- Très utilisé pour Node.js
- Evasion de la Sandbox
  - CVSS **10.0**/10

https://github.com/advisories/GHSA-mrgp-mrhc-5jrq

https://nvd.nist.gov/vuln/detail/CVE-2022-36067

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

Razer, l'erreur de configuration à 7m€

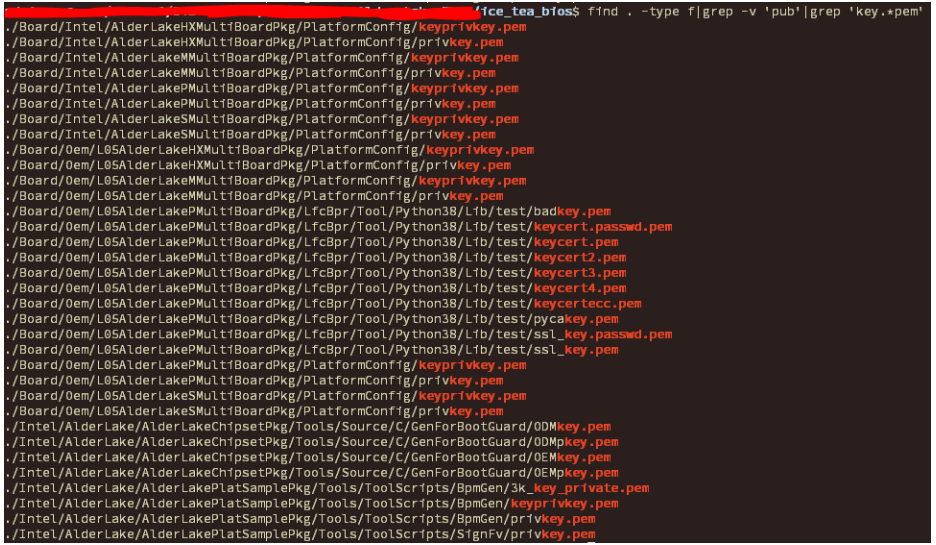
- Fuite de données en 2020 liée à une erreur de configuration
  - Désactivation de la ligne de conf activant la sécurité d'ELK par un admin de Cap Gemini
- Jugé à Singapour
  - Nom de l'admin cité partout sur internet 😢

https://www.lemondeinformatique.fr/actualites/lire-un-ex-employe-de-capgemini-a-l-origine-de-la-fuite-de-donnees-de-razer-87584.html

Publication du code source d'Intel Alder Lake

- Archi CPU de 12eme génération
- Publication de 2,8Go (compressé) sur github
- Source pour matériel Lenovo
  - "Avec" les clefs privées UEFI

https://hardenedvault.net/blog/2022-10-08-alderlake_fw-leak/



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

Hôpital de Corbeil-Essonnes, suite du piratage par Lockbit

- Publication d'une partie des données par les cybercriminels

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/enquete-cyberattaque-a-l-hopital-de-corbeil-essonnes-des-donnees-tres-confidentielles-ont-ete-divulguees_5395618.html

Fuite du "packer" Bl00dy de Lockbit

- Accompagné d'un "keygen"

https://www.bleepingcomputer.com/news/security/leaked-lockbit-30-builder-used-by-bl00dy-ransomware-gang-in-attacks/

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

Cobalt, XSS (CVE-2022-39197)

- Injection d'HTML et donc de Javascript dans le serveur Cobalt
  - Sur le champ "username"

https://github.com/burpheart/cve-2022-39197/blob/main/poc.py

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

Blue Team PersistenceSniper

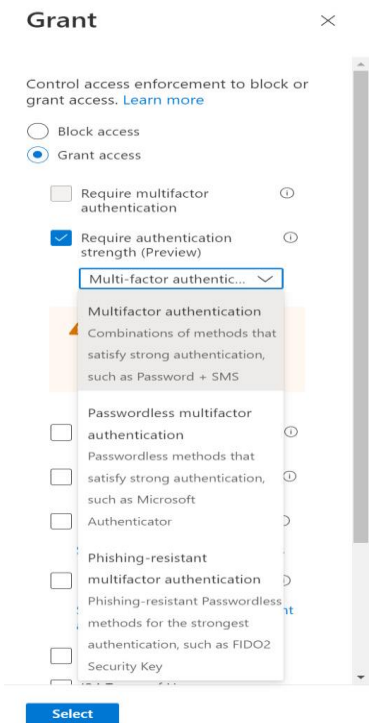
- Un petit script PowerShell pour identifier des persistances (34 techniques)
  - Connues… et basiques mais c'est toujours ça

https://github.com/last-byte/PersistenceSniper

Azure permet enfin de sélectionner son MFA par "résistance"

- Tous les MFA ne se valent pas

https://twitter.com/kennethvs/status/1577647568946925568



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

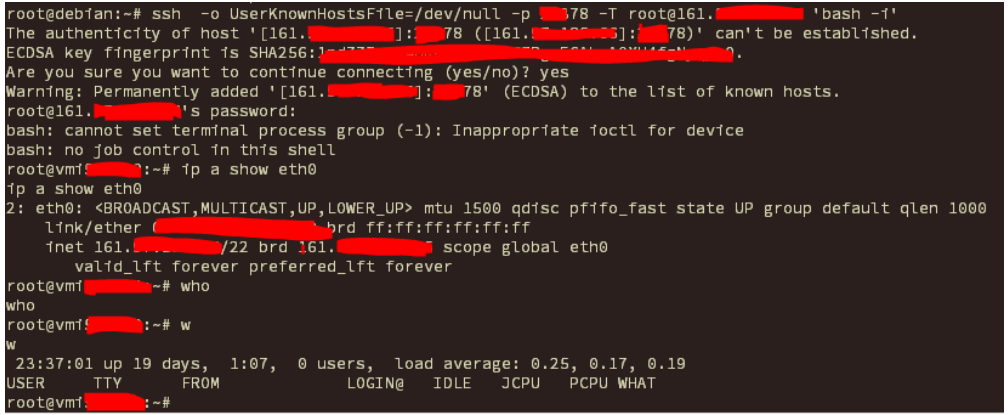
Jean-Michel DISCRET se fait un proxy pour un C2

- En utilisant les commentaires de VirusTotal

  https://github.com/D1rkMtr/VirusTotalC2

- Il le fait aussi avec github ;)

  https://github.com/D1rkMtr/githubC2



Red Team Cacher sa session SSH

- C’est une fonctionnalité

```
ssh -o UserKnownHostsFile=/dev/null -T user@target.com 'bash -i'
```

https://twitter.com/alh4zr3d/status/1578406155453276160

Business et Politique

Business
Monde

Levée de fond pour Patrowl

- Levée de 2 millions d'euros
  - Leader français du Pentest as-a-Service
  - Préparation d'une série A pour entrer sur le marché américain en 2023

https://www.finyear.com/Patrowl-leve-2M-et-conforte-sa-place-de-leader-francais-du-Pentest-as-a-Service_a48108.html

ChapsVision met la main sur Deveryware

- Et lève plus de 100 millions d'euros
  - Création d'un géant du traitement des données de masse dans le secteur de la cybersécurité

https://www.usine-digitale.fr/article/chapsvision-met-la-main-sur-deveryware-pour-creer-un-geant-du-traitement-des-donnees-de-masse.N2046402

Business
Monde

CrowdSec lève aussi

- Levée de 14 millions d'euros
  - plate-forme de cybersécurité open source

https://www.opensourceforu.com/2022/10/crowdsec-a-french-open-source-cybersecurity-business-raises-13-7-million/

SOC qui n’en veut

- SPIE lance son offre SOC
  - service 100 % français

https://www.spie.com/fr/actualites/france-spie-lance-son-offre-security-operations-center-et-renforce-son-positionnement-dacteur-de-la-cybersecurite

Business
Monde

Mailinblack s’ouvre …

- Entrée de Apax et NewAlpha Verto au capital
  - Démocratiser une cybersécurité performante et accessible

https://www.finyear.com/Mailinblack-s-allie-aux-fonds-francais-Apax-et-NewAlpha-Verto-et-dispose-de-50M-pour-ses-operations-de-croissance_a48003.html

Campus Cyber

- De Altarea à La Française REM
  - 26 500 mètres carrés, connu sous le nom de tour Eria
  - Valorisation de l’ensemble atteint les 320 M€ et rendement à 4.1%

https://www.cfnewsimmo.net/Les-Alertes-de-CFNEWS-IMMO/Le-Campus-Cyber-plus-grande-acquisition-des-SCPI-de-La-Francaise-REM-447417

Droit / Juridique / Politique
Monde

Uber, le RSSI jugé et condamné

- Il a caché une cyber attaque importante
- Et… a payé la rançon avec le budget BugBounty

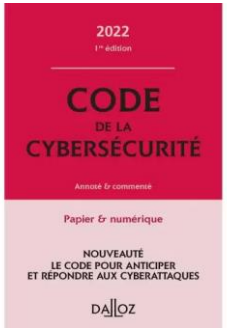
https://www.nytimes.com/2022/10/05/technology/uber-security-chief-joe-sullivan-verdict.html

#MonBudgetMonChoix

Le code de la cybersécurité est sorti

- Chez Dalloz

https://www.boutique-dalloz.fr/code-de-la-cybersecurite-p.html



Droit / Juridique / Politique
Monde

Google propose de la Cyber Assurance

- Pour les clients de son cloud “GCP”
  - Analyse proactive de sa sécurité
  - Proposition d’une liste d’assureurs avec des meilleurs prix

https://cloud.google.com/risk-protection-program

Assurance Cyber = Ascenseur émotionnel, la suite…

- Bercy veut autoriser l’indemnisation des rançons (cf. revue du 2022-09-13)
- CESIN est contre (et heureusement…)

  https://www.lemagit.fr/actualites/252525535/Cyberattaques-le-Cesin-vent-debout-contre-lindemnisation-des-rancons
- NCSC (~= ANSSI anglaise)

  `<<nous n'encourageons ni ne tolérons le paiement des demandes de rançon aux organisations criminelles>>`
- ICO (~=CNIL anglaise)

  `<<S'engager avec les cybercriminels et payer des rançons ne fait qu'encourager d'autres criminels>>`

  https://thestack.technology/ransom-payments-stop-or-get-busted/
- Mais qui est pour !!?

Droit / Juridique / Politique
Monde

Le directeur de la BSI, renvoyé

- BSI ~= ANSSI Allemande
- Accusé de lien avec la Russie

https://www.lemagit.fr/actualites/252525911/Allemagne-le-patron-du-BSI-menace-apres-des-allegations-de-liaisons-dangereuses

https://www.lemonde.fr/pixels/article/2022/10/10/le-responsable-de-l-agence-de-cybersecurite-allemande-en-passe-d-etre-revoque_6145176_4408996.html

Droit / Juridique / Politique
France

Guardia Cybersecurity School

- Sur Lyon et Paris
  - Un Bachelor de développeur informatique option cybersécurité
  - Un Master of Science en cybersécurité,

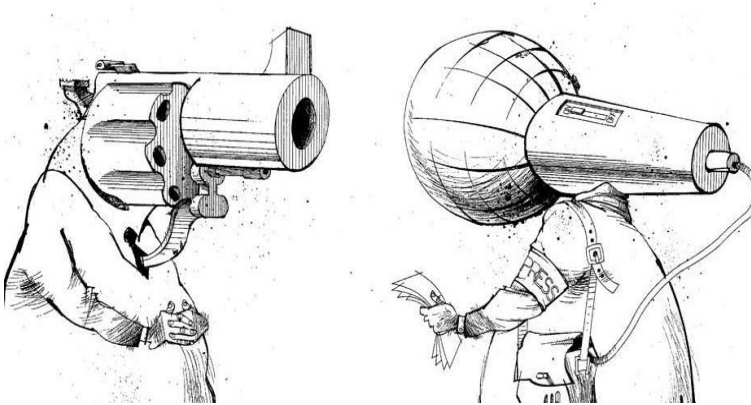
https://lejournaldeleco.fr/guardia-cybersecurity-school-a-la-pointe-de-la-securite/

Droit / Juridique / Politique
Monde

Avisa attaque en justice Nextinpact, Arrêt sur Image, Mediapart, l'ADN et Reflets

- Suites aux révélations concernant les pratiques d'influence d'Avisa
- Communément nommée dans le milieu "procédure bâillon"
  - Effet Streisand à venir ?

https://www.nextinpact.com/blog/70040/next-inpact-attaque-en-justice-par-avisa-partners



Altice gagne en justice face à Reflets

- Piratage d'Altice par Hive
  - Publications de documents par les cybercriminels
- Analyse et publication d'articles sur les paradis fiscaux, le train de vie de Drahi…
- Décision de justice :
  - Pas de nouvel article mais les anciens peuvent rester
  - Revient à une forme de censure

https://www.lemonde.fr/economie/article/2022/10/07/la-justice-interdit-a-reflets-info-de-publier-de-nouveaux-articles-a-propos-d-altice-tires-de-donnees-piratees_6144794_3234.html

Droit / Juridique / Politique
Monde

La CIA utilisait un canal de communication non sécurisé avec ses sources

- Années 2010, faux sites web pour les communications cachées (**Cov**ert **Com**munications)
  - Cassé par le contre espionnage Iranien
  - Et par les Chinois
  - Chaque site avait le même Javascript, très caractéristique
- Les sources de la CIA ont finies assassinées ou emprisonnées
- Leur COVCOM était aussi indéxé par Google

https://twitter.com/thegrugq/status/1058376118292475904

Les vulnérabilités utilisées par les groupes Chinois…

- Selon les USA
- Des vieilleries allant jusqu'à 2019
  - Mais toujours non mise à jour 😱

https://www.bleepingcomputer.com/news/security/us-govt-shares-top-flaws-exploited-by-chinese-hackers-since-2020/

Vendor	CVE	Vulnerability Type
Apache Log4j	CVE-2021-44228	Remote Code Execution
Pulse Connect Secure	CVE-2019-11510	Arbitrary File Read
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Atlassian	CVE-2022-26134	Remote Code Execution
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
F5 Big-IP	CVE-2020-5902	Remote Code Execution
VMware vCenter Server	CVE-2021-22005	Arbitrary File Upload
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution
Buffalo WSR	CVE-2021-20090	Relative Path Traversal
Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution
Hikvision Webserver	CVE-2021-36260	Command Injection
Sitecore XP	CVE-2021-42237	Remote Code Execution
F5 Big-IP	CVE-2022-1388	Remote Code Execution
Apache	CVE-2022-24112	Authentication Bypass by Spoofing
ZOHO	CVE-2021-40539	Remote Code Execution
Microsoft	CVE-2021-26857	Remote Code Execution
Microsoft	CVE-2021-26858	Remote Code Execution
Microsoft	CVE-2021-27065	Remote Code Execution
Apache HTTP Server	CVE-2021-41773	Path Traversal

Conférences

Conférences

Passée

- FranSec : 13 et 14 septembre 2022
- DefCon Paris : 29 septembre 2022

A venir

- Les Assises : 12 au 15 octobre 2022
- HexaCon : 14 et 15 octobre 2022
- Unlock your brain : 4 et 5 novembre 2022
- Black Alps : 15 et 16 novembre 2022
- C&SAR : 15 et 16 novembre 2022
- ECW : 15 à 17 novembre 2022
- CCC : décembre 2022

Challenges

European Cybersecurity Challenge

- 28 équipes nationales à Vienne
  - Les danois 1er

https://www.informatiquenews.fr/une-medaille-de-bronze-pour-la-france-a-leuropean-cybersecurity-challenge-89407

Divers / Trolls velus

Divers / Trolls velus

macOS, mais où est passée la CVE

- Les applications malveillantes peuvent contourner les contrôles (CVE-2022-32910)

Printer-Friendly View

CVE-ID	
CVE-2022-32910	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	

https://www.jamf.com/blog/jamf-threat-labs-macos-archive-utility-vulnerability/

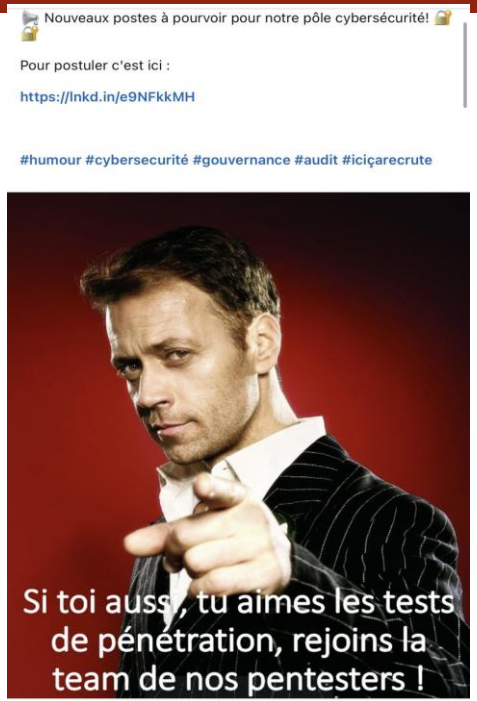
https://thehackernews.com/2022/10/details-released-for-recently-patched.html

Divers / Trolls velus

Jean-Michel BEAUF s’étonne de ne pas recruter des filles

- Annonce de recrutement sur Linkedin
- “Légèrement” malaisante

https://www.l4m.fr/emploi/offre/62300-lens-62110-henin-beaumont-soc-analyst-584073



Twitter, l’ancien RSSI continue ses révélations

- Beaucoup de problèmes
  - Pas de lutte contre les bots
  - 50% des employés peuvent accéder à toutes les données, sans contrôle
  - Certains salariés sont des agents des rens’
  - Nombreuses vulnérabilités connues depuis des années mais pas corrigées

https://www.theverge.com/2022/8/23/23317857/twitter-whistleblower-zatko-security-spam-safety

Divers / Trolls velus

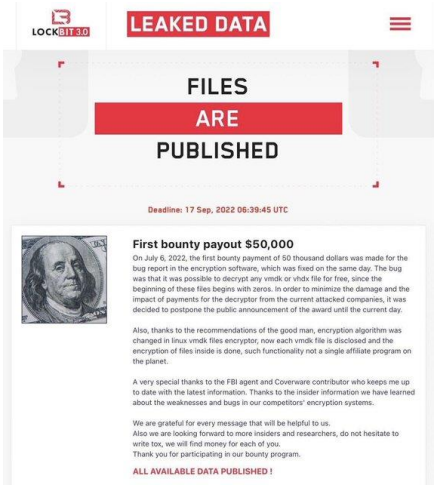
Quand l'essence des groupes électrogène de ton DC prennent feu

https://twitter.com/AnonOpsSE/status/1570724233742786560

LockBit, paiement de leur première prime de bug bounty

- Vulnérabilité sur leur chiffrement des ESXi

https://twitter.com/BushidoToken/status/1571088895697387520



Divers / Trolls velus

Les correcteurs orthographiques font fuiter vos mots de passe

- Pour les navigateurs Chrome et Edge
  - Envoyés sur les serveurs des éditeurs

https://www.01net.com/actualites/le-correcteur-orthographique-de-chrome-et-edge-fait-fuiter-vos-mots-de-passe.html

Passer de l'IA aux stats #AITheNewBayesian

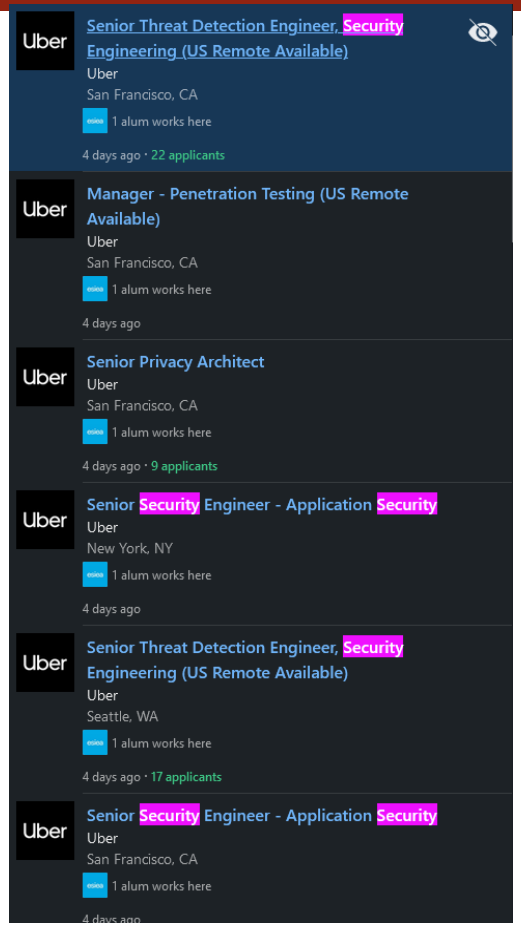
<<L'intelligence artificielle [...] apprentissage automatique [...] apprentissage statistique>>

https://www.europeanscientist.com/fr/opinion/le-tournant-cognitif-de-la-cybersecurite-changement-de-paradigme-et-prolegomenes-a-la-cybersecurite-cognitive/

Divers / Trolls velus

Que faire quand on se fait pirater ?

- Publier des offres d'emploi en cybersécurité
  - Dès le lendemain (capture du 20/09)



Prochaines réunions

Prochaine réunion

- Mardi 8 novembre 2022

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 ?