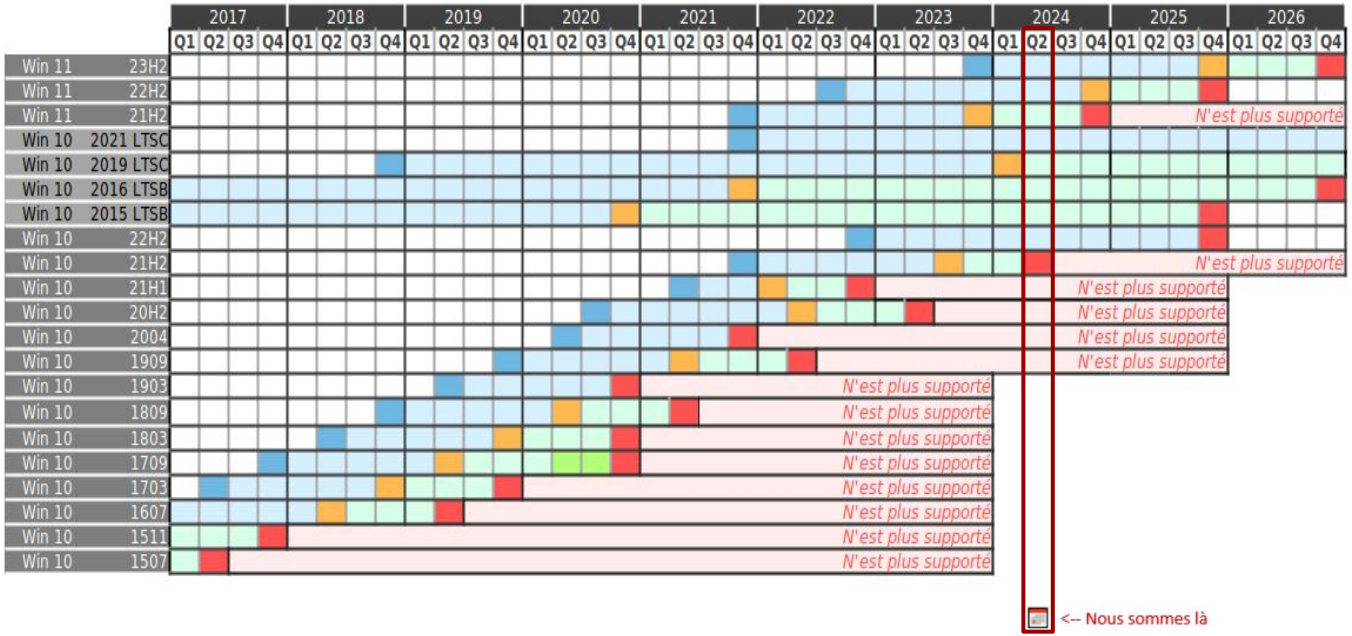
Revue d'actualité de l'OSSIR

09 juillet 2024

Jérémy De Cock
Melchior Courtois

Rappel du support Windows en couleurs

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Workstation***



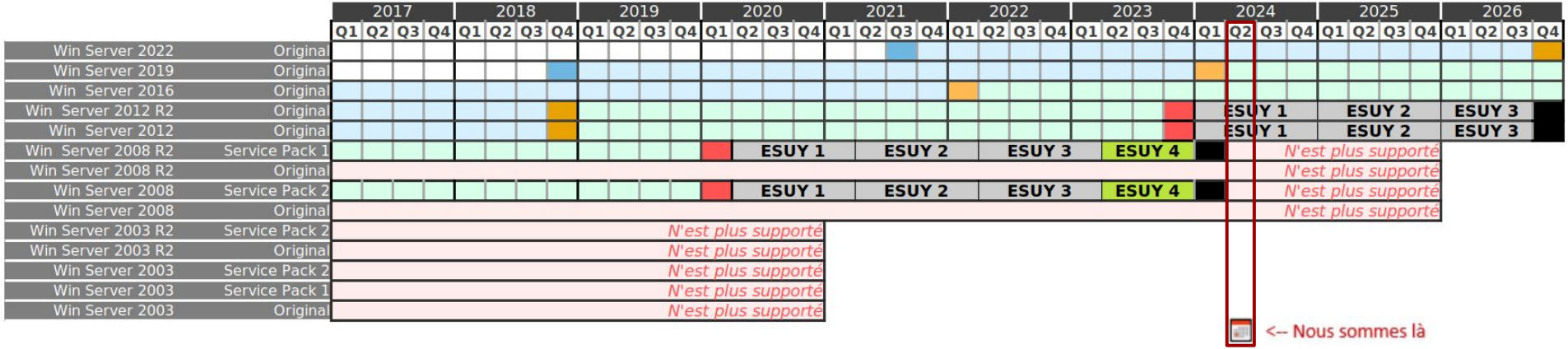
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 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

LTSB : **L**ong-**T**erm **S**ervicing **B**ranch
LTSC : **L**ong-**T**erm **S**ervicing **C**hannel

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Server***



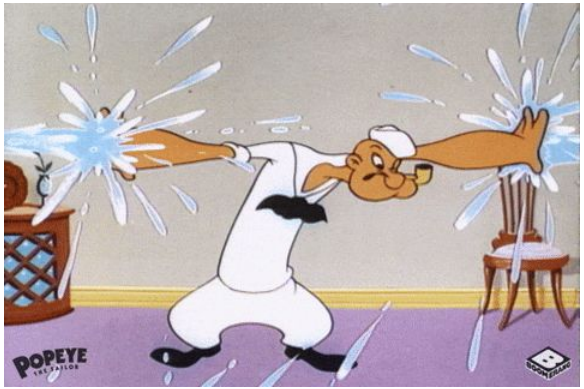
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 30 octobre 2012	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 22 février 2011	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
jeudi 22 octobre 2009	mardi 9 avril 2013		
mercredi 29 avril 2009	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
mardi 6 mai 2008	mardi 12 juillet 2011		
mardi 13 mars 2007	mardi 14 juillet 2015		
dimanche 5 mars 2006	mardi 14 avril 2009		
mardi 13 mars 2007	mardi 14 juillet 2015		
mercredi 30 mars 2005	mardi 14 avril 2009		
mercredi 28 mai 2003	mardi 10 avril 2007		

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour la version standard
- Support étendu pour LTSB/LTSC
- Fin de support étendu pour LTSB/LTSC
- X Extension d'une ou plusieurs années (ESUY)
- X Extension disponible uniquement avec Azure (Microsoft Entra ID)
- Fin de support pour la ou les extensions supplémentaires

ESYC : **E**xtended **S**ecurity **U**pdate **Y**ear

Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de juin, 51 vulnérabilités patchées dont

- 1 vulnérabilité de type 0-day :
  - [**CVE-2023-50868**] DNSSEC, déni de service
    - Présente dans le mécanisme NSEC3
    - Augmentation de la charge du CPU → DoS
    - Affecte tous les Windows Server ≥ 2012 (mais n'est pas exploitée dans la nature)
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2024-30080**] MSMQ, exécution de code à distance
    - Affecte Windows 10 & 11 ainsi que tous les Windows Server ≥ 2008
  - [**CVE-2024-30078**] Driver WiFi, exécution de code à distance unauthenticated 0-clic 😱
    - Seul prérequis : la machine ciblée doit détecter le réseau sans-fil malveillant
      - Critique dans les lieux publics…
    - Toutes les versions ≥ Windows 10 et Windows Server 2008 sont affectées
  - [**CVE-2024-30103**] Outlook, exécution de code à distance 0-clic
    - Message ouvert ou prévisualisé (panneau de prévisualisation d'Outlook) = ☠️
    - Contournement des listes de blocage du registre Outlook + création de DLL malveillantes
    - Affecte Microsoft 365 Apps for Enterprise et les versions Office 2016, 2019 et LTSC 2021

https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2024-patch-tuesday-fixes-51-flaws-18-rces/

Failles / Bulletins / Advisories
Systèmes

Faille critique sur les routeurs ASUS


CVE-2024-3080

- Accès à distance possible sans authentification requise
- 7 modèles affectés
  - XT8 (ZenWiFi AX XT8)
  - XT8_V2 (ZenWiFi AX XT8 V2)
  - RT-AX88U
  - RT-AX58U
  - RT-AX57
  - RT-AC86U
  - RT-AX68U
- Mettez à jour leur firmware, sinon n'exposez tout simplement pas votre routeur 😀
  - Interface d'administration, DMZ, redirection de ports, service VPN, etc;

https://www.bleepingcomputer.com/news/security/asus-warns-of-critical-remote-authentication-bypass-on-7-routers/

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

2 x RCE + 1 x Privesc sur VMware vCenter

- [CVE-2024-37079] Type << heap-overflow >>
  - Présente dans l'implémentation du protocole DCERPC
- [CVE-2024-37080] Type << heap-overflow >> (again)
  - Présente directement dans le protocole DCERPC
- [CVE-2024-37081] Mauvaise configuration de **sudo**
  - Elévation de privilège permettant de devenir **root**
- Affectent les versions 7.0 et 8.0 de vCenter + 4.x et 5.x pour la Cloud Foundation

https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-vcenter-rce-vulnerability-patch-now/

Response Matrix:

VMware Product	Version	Running On	CVE	CVSSv3	Severity	Fixed Version	Workarounds
vCenter Server	8.0	Any	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081	9.8, 9.8, 7.8	Critical	8.0 U2d	None
vCenter Server	8.0	Any	CVE-2024-37079, CVE-2024-37080	9.8, 9.8	Critical	8.0 U1e	None
vCenter Server	7.0	Any	CVE-2024-37079, CVE-2024-37080, CVE-2024-37081	9.8, 9.8, 7.8	Critical	7.0 U3r	None

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

Mise à jour de ChatGPT pour macOS

- Stockage des conversations en clair en local dans l'application
  - Risque de fuite de données par logiciel malveillant
- Application disponible sur le site OpenAI et non sur l'AppStore
  - Contourne les contrôles de sécurité (sandboxing) réalisés habituellement

https://www.it-connect.fr/vous-utilisez-application-chatgpt-sur-macos-mettez-la-a-jour-maintenant/

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

RegreSSHion, la faille qui fait transpirer vos serveurs SSH

CVE-2024-6387

- RCE unauthenticated en tant que root 😱 😱 😱
  - Race condition dans la configuration par défaut de sshd
- Affecte tous les systèmes Linux basés sur la glibc
  - = 14 millions de serveurs OpenSSH #Shodan
  - Versions comprises de OpenSSH entre la 8.5p1 et la 9.7p1 (ou < 4.4p1)
- Faille déjà patchée en 2006 (**CVE-2006-5051**) et ré-introduite en octobre 2020
- Pour vous protéger ?
  - Définir **LoginGraceTime** à **0** ou tout simplement, montez de version !

https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

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

Faille critique sur LibreOffice


CVE-2024-5261

- Possibilité d'utiliser LibreOffice en tant que bibliothèque
  - Convertir, visualiser et interagir avec des documents
  - = Mode LibreOfficeKit
- Vérification de la certification TLS désactivée ???
  - Option **CURLOPT_SSL_VERIFYPEER** définie sur **false**
  - Critique pour la récupération de ressources distantes (interception & manipulation)
- Impacte les versions inférieures à la 24.2.4

https://securityonline.info/cve-2024-5261-cvss-10-libreoffice-patches-critical-vulnerability-in-libreofficekit/

Failles / Bulletins / Advisories
Smartphones (principales failles)

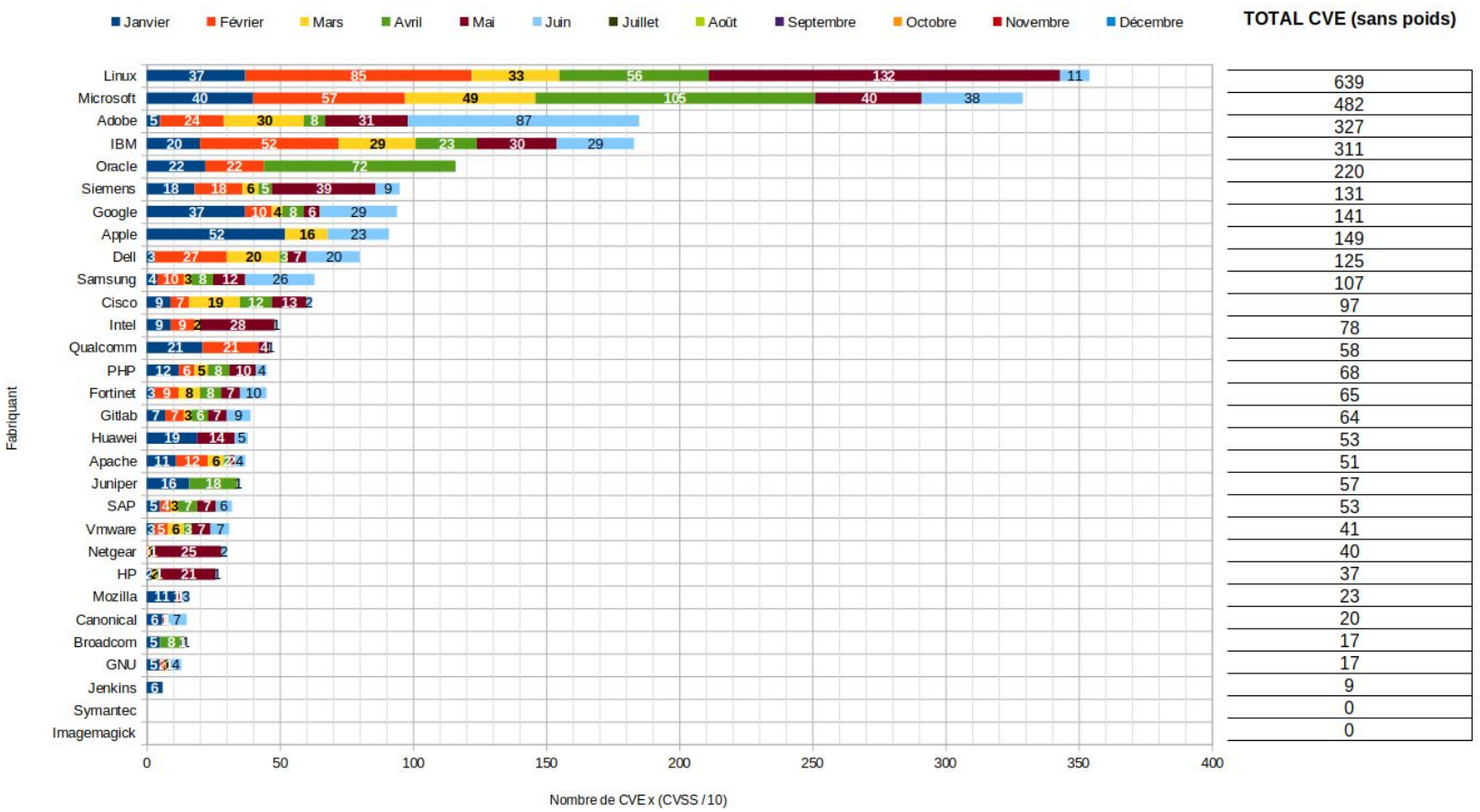
Plus de 50 vulnérabilités découvertes sur les appareils Pixel (Google)


CVE-2024-32896

- Une plus importante que les autres : **CVE-2024-32896**
  - Elévation de privilèges nécessitant une interaction utilisateur
  - Fortement exploitée dans la nature
  - Pas plus d'information pour le moment…
- Toutes ces vulnérabilités corrigées dans le patch de juin (2024-06-05)

https://www.securityweek.com/google-warns-of-pixel-firmware-zero-day-under-limited-targeted-exploitation/

Failles / Bulletins / Advisories
Stats du mois



TOTAL CVE (sans poids)
639
482
327
311
220
131
141
149
125
107
97
78
58
68
65
64
53
51
57
53
41
40
37
23
20
17
17
9
0
0

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Retour sur le piratage des Cisco Nexus

CVE-2024-20399

- 0-day exploitée en avril dernier dans les systèmes NX-OS des switch Nexus
  - Exploitation associée à Velvet Ant, cybercriminels sponsorisés par l'État chinois
- Prérequis de la faille : Avoir un accès administrateur au système
  - Permet d'exécuter des commandes en root et de prendre le contrôle de l'appareil compromis
- Bulletin et liste des équipements safes disponible par Cisco :

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP

Liste des produits vulnérables ——————————>

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Switches (standalone mode)

https://www.it-connect.fr/faille-de-securite-switchs-cisco-nexus-cve-2024-20399/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Cyberattaque chez TeamViewer

- Intrusion détectée le 26 juin – Investigation en cours
  - `<< Environnement interne de TeamViewer totalement indépendant de l'environnement du produit >>`
- Groupe russe APT29 suspecté

https://www.it-connect.fr/cyberattaque-chez-teamviewer-intrusion-sur-le-reseau-juin-2024/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Suite chez TeamViewer (5 jours après)

- Confirmation de l'attaque par APT29 /Midnight Blizzard
  - Récupération des identifiants d'un salarié
  - Copie des données de l'annuaire comprenant noms, contacts et mots de passe chiffrés
  - `<< TeamViewer affirme avoir d'ores et déjà fait le nécessaire pour renforcer les méthodes d'authentification de ses employés. >>`

https://www.it-connect.fr/cyberattaque-teamviewer-mots-de-passe-voles-mais-ce-ne-sont-pas-ceux-des-utilisateurs/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Retour de Medusa – Android

- Aussi connu sous le nom de TangleBot; apparu en mai 2020 pour la première fois
- Pas de réelle activité depuis 2023; réveil en mai 2024
  - Accessible actuellement en tant que MAAS (Malware as a Service)
  - Nouvelle fonctionnalitée présente par rapport à la version de 2020 : désinstallation d'application, copie d'écran,... et moins de permissions à donner donc plus discret.
- Campagne visant 7 pays dont la France, le Canada et les Etats-Unis

https://www.it-connect.fr/trojan-bancaire-medusa-cible-android-dans-7-pays-dont-la-france/

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

400 Go de données médicales

- 3 juin : ransomware sur les grands hôpitaux anglais comme King's College Hospital et St Thomas
  - Impact majeur et report de + 1500 opérations
  - Demande de rancon (50 millions d'euros) et fuite des données en ligne
- Fuite de ses données dans la nuit du 20 juin sur le site et le canal Telegram du groupe Qilin (appartenance russe)

https://www.lemonde.fr/pixels/article/2024/06/21/pres-de-400-gigaoctets-de-donnees-personnelles-de-patients-britanniques-publiees-en-ligne-apres-un-piratage_6242026_4408996.html

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

Sport2000, fuite de 4.3 millions de données

- Données très détaillées (34 points d'informations)
  - Prénom, nom, mail, date de naissance, adresse postale, n° mobile…
- Attaque subie le 19 avril 2024
  - Le groupe français Epsilon en serait à l'origine

https://www.zdnet.fr/actualites/sport-2000-des-donnees-clients-en-vente-suite-a-une-intrusion-391087.htm

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

Disney, fuite de 2.5 Go de données par des fans du club Penguin

- Serveur Confluence de Disney ciblé
  - Vengeance des fans
- Données internes plus ou moins importantes
  - 😲 Centaine de PDF sur Club Penguin
  - 😲 Documentation de divers projets commerciaux et logiciels de Disney
  - 😵 Points de terminaison d'API, informations de connexion vers des buckets S3
- Données qui auraient été volées début juin 2024

https://www.bleepingcomputer.com/news/security/club-penguin-fans-breached-disney-confluence-server-stole-25gb-of-data/

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Plusieurs sites gouvernementaux victimes de DDoS

- 14 sites 🇫🇷 ciblés
  - Police National, Légifrance, INSEE, Service Public, Ministères de l'Ecologie et de la Culture
  - Certains HS pendant 48 heures…
- Attaques orchestrées par des russes
  - Groupe d'hacktivistes NoNameO57(16)
- Actions effectuées dans le cadre du projet DDoSia
  - Regroupe plusieurs milliers d'utilisateurs sur Telegram

https://www.01net.com/actualites/cyberattaque-russe-contre-la-france-plusieurs-sites-du-gouvernement-sont-hors-service.html

https://www.sekoia.io/fr/glossaire/ddosia/ (plus d'infos sur DDoSia)

Piratages, Malwares, spam, fraudes et DDoS
Publication

Augmentation massive de phishing, merci ChatGPT 🤖

- Etude réalisée par SOCRadar
- Augmentation de 4.151% de courriers malveillants
  - Augmentation de 856% entre 2023 et 2024
- Dû à quoi ?
  - Templates réalisés par LLM
  - Dans n'importe quelle langue
  - Kit de phishing ? (c'est pas nouveau)

https://socradar.io/phishing-in-2024-4151-increase-since-chatgpt/ (étude)

https://www.it-connect.fr/campagne-phishing-microsoft-365-secteur-finance-onnx/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Rapport d'OVH sur les DDOS

- Augmentation du nombre d'attaque DDOS
  - De + en + fréquentes et de + en + fortes
  - Attaque record le 25 mai, max 2.5 Tbps
- Nombreux appareils compromis MikroTik
  - + de 100 000 équipements accessibles depuis Internet
  - Sont équipés d'une fonction exploitable pour le DDOS : "Bandwidth test" permettant d'envoyer plusieurs millions de paquets par seconde
- OVH a contacté l'entreprise MikroTik pour transmettre ses informations

https://www.it-connect.fr/ovhcloud-attaque-ddos-record-botnet-equipements-reseau-mikrotik/

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

Red Team Le fameux boitier Basilisk, qu'est-ce qu'il vaut ?

- Si vous voulez le tester vous-même
  - Ici pour 577$: https://ringtail.ch/products/basilisk-automatic-ethernet-ghosting
- Tout le trafic provenant de la machine 💀 est modifié en temps réel
  - Son adresse MAC est remplacée par celle de la machine 👼
    - Également dans les paquets ARP et DHCP
  - Et inversement au moment de la réception des réponses

  = Trafic masqué !

- Le trafic provenant de la machine 👼 n'est pas altéré
- Autres mesures / promesses...
  - Aucun trafic envoyé de la machine 💀 tant que l'@ MAC de la machine 👼 n'est découverte
  - Contournement du NAC et MAC whitelisting 😲
  - Fonctionne avec un début Ethernet 10/100 Mo
  - Chaque port physique dispose d'une mémoire tampon circulaire de 32 Ko
- Passez au 802.1AE (MACSec) !

Business et Politique

Business
Monde

Etat-Unis : bannissement de Kaspersky

- Interdiction effective à partir du 29 septembre 2024
  - Les entreprises ont 3 mois pour migrer vers d'autres solutions → non conformité = risque de sanctions civiles et pénales
- Kaspersky assure ne pas être impliqué dans la moindre activité représentant une menace pour la sécurité des États-Unis
  - `<< L'entreprise a l'intention de poursuivre toutes les options légales disponibles pour préserver ses activités et ses relations actuelles. >>`

https://www.it-connect.fr/les-etats-unis-ont-pris-la-decision-de-bannir-editeur-russe-kaspersky/

Business
Monde

Accord de plaider-coupable pour Julian Assange

- Fondateur de WikiLeaks, a dénoncé les crimes de guerres des Etats-Unis ; jugé coupable d'espionnage
- Procédure rapide permettant de juger rapidement un coupable reconnaissant les faits
  - Reconnaît sa participation à un « complot pour obtenir et divulguer des informations relevant de la défense nationale »
  - Accord conclu avec la justice américaine après avoir purgé des années de prison en Angleterre

https://www.lemonde.fr/pixels/article/2024/06/25/le-lanceur-d-alerte-julian-assange-conclut-un-accord-de-plaider-coupable-avec-la-justice-americaine_6243463_4408996.html

Droit / Juridique / Politique
National

OpenDNS quitte la France 👋

- Suite des demandes de Canal+ (cf. OSSIR 05/2024)
- Décision de justice prise fin juin :
  - Demande aux DNS alternatifs de bloquer l'accès à plus d'une centaine de sites
  - Article L.333-10 du code du sport français
- OpenDNS n'est pas trop d'accord…
  - `<< À compter du 28 juin 2024, en raison d'une décision de justice en France [...] et d'une décision de justice au Portugal [...], le service OpenDNS n'est actuellement pas disponible pour les utilisateurs en France et dans certains territoires français et au Portugal. Nous nous excusons pour la gêne occasionnée >>`

https://next.ink/142507/contraint-de-bloquer-des-noms-de-domaine-opendns-decide-de-quitter-la-france/

Opérations internationales

Opérations internationales

Après les opérations Cronos et Endgame : Morpheus

- Réalisée en juin 2024 et coordonnée par Europol
  - + Allemagne, Australie, Canada, Pays-Bas, Pologne, USA & UK
  - + partenaires privés
- Démantèlement de plus de 600 serveurs Cobalt Strike 👏👏👏
  - Sur 690 adresses IP signalées !
- D'autres opérations déjà réalisées
  - Emma (vs réseaux de distribution de dropper), GoldDust (vs REvil), etc.
  - Année productive !

https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-global-action-against-criminal-abuse-of-cobalt-strike

Conférences

Conférences

Passée(s)

- **Pass The Salt**, 03 au 05 juillet 2024 à Lille
- **LeHack** « Compile », 05 au 07 juillet 2024 à Paris (20ème édition !)

À venir

- **Barbhack**, 31 août 2024 à Toulon
- **Black Hat USA**, 03 au 08 août 2024 à Las Vegas
- **DefCon**, 12 au 13 août 2024 à Las Vegas

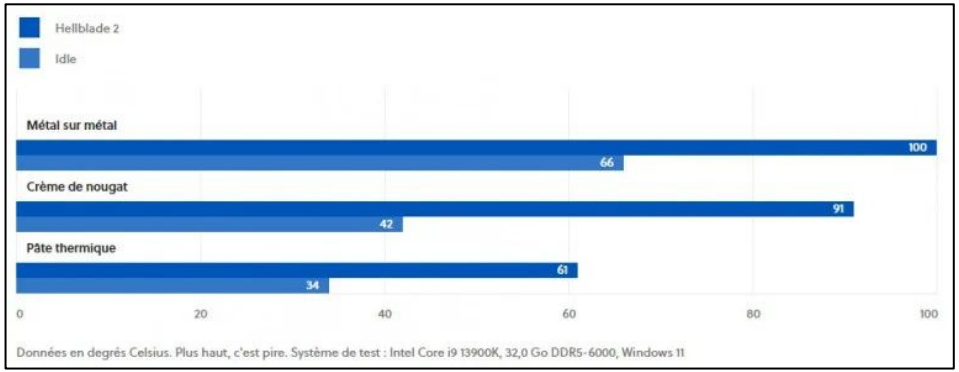
Divers / Trolls velus

Divers / Trolls velus

Bonne idée de remplacer de la pâte thermique par de la crême de nougat ?

- Idée fournie par Gemini #Google
  - Et c'est pas la seule : dentifrice, côtons humides, vaseline, fromage…
- Thermal Grizzly Kryonaut **vs** Crême de nougat ?
  - Aucun dommage irréversible sur le court terme
  - Et c'est loin d'être une solution miracle (sans surprise)

https://www.jeuxvideo.com/news/1895539/ce-joueur-a-remplace-la-pate-thermique-de-son-pc-par-de-la-creme-de-nougat-il-a-voulu-ecouter-les-conseils-d-une-ia.htm



Divers / Trolls velus

CrowdSec participe à sa manière à la sécurisation de la France pendant les JOs

- Accès complètement **gratuit** à une blacklist de plusieurs milliers d'@ IP
  - IP les plus actifs (derniers 30 jours) ciblant différentes entités 🇫🇷
  - Permettrait de réduire de 80% le volume d'alertes au niveau des SOC
- Liste mise à jour régulièrement et accessible via la CLI de CrowdSec
  - Intégrable facilement à n'importe quel pare-feu

https://app.crowdsec.net/blocklists/665d96cf0a60f8f3808a5d5c?utm_source=press&utm_medium=organic&utm_campaign=olympics (blacklist)

https://www.crowdsec.net/press-releases/crowdsec-renforce-des-jeux-olympiques-et-paralympiques-de-paris-2024

Divers / Trolls velus

Moshi, le nouveau rival de ChatGPT ?

- Développée par Kyutai (6 mois d'existence)
  - Cofondée par Xavier Niel, Rodolphe Saadé et Eric Schmidt
- IA conversationnelle à << la réactivité et à la latence inédites >>
  - Fonctionne en temps réel (grosse différence avec ChatGPT)
  - Elle coupe la parole, module le son de sa voix (vraie voix), imite des émotions
  - Ne parle qu'en anglais pour l'instant
- Modèle de 7 milliards de paramètres (Helium)
  - + Code de compression audio Mimi, etc.
- Conçu et entraîné en France !!!
  - Sur le supercalculateur Nabu23 (Scaleway)
- Le code et les modèles vont être mis en open-source 🎁
  - Licence Apache ou MIT (encore en discussion pour chercher la plus permissive)

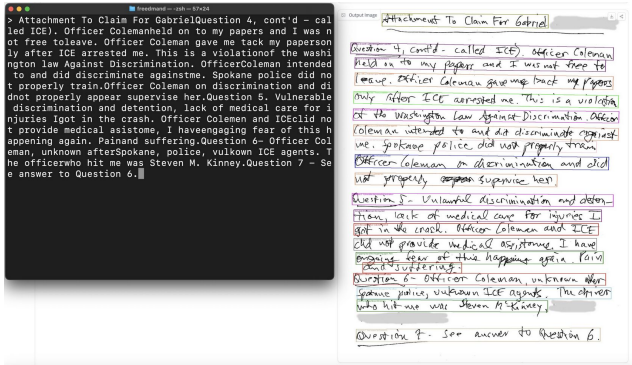
https://www.lesnumeriques.com/intelligence-artificielle/moshi-le-premier-assistant-vocal-ia-en-temps-reel-au-monde-est-made-in-france-n223813.html

Divers / Trolls velus

OCR 2.0 - Florence 2

- Modèle open-source développé par Microsoft
- OCR totalement fonctionnel !
- Démo disponible en ligne : https://huggingface.co/spaces/gokaygokay/Florence-2

https://x.com/dylfreed/status/1803502158672761113



FIN

Prochaine réunion ?

- RDV le **mardi 10 septembre 2024**

Accéder aux différents supports ?

Replays

Slides

https://www.youtube.com/@OSSIR

https://www.ossir.org/support-des-presentations/