Voir la version en ligne

OPEN
NOUVELLE-CALEDONIE
ORGANISATION DES PROFESSIONNELS DE L'ÉCONOMIE NUMÉRIQUE

Février 2023

Blague artificielle par Chat GPT:

Pourquoi les hackers préfèrent-ils travailler la nuit?
Parce qu'ils aiment éteindre les lumières avant de pénétrer dans le système!

« JENESUISPASUNEDATA», L'UFC-QUE CHOISIR en action

A l'occasion de la journée dédié à la protection des données le 25 janvier l'UFC-Que choisir a lancé une campagne de sensibilisation avec son site www.jenesuispasunedata.fr pour aider les internautes à reprendre le contrôle de leurs données personnelles.

En savoir +

Cyber Resilience Act: La Commission européenne propose de nouvelles normes de Cybersécurité!

Avec ce texte, la Commission veut mettre en place des règles communes de cybersécurité pour les fabricants et les développeurs de produits comportant des éléments numériques, du matériel aux logiciels.

Le jeudi 15 septembre 2022, la Commission européenne a proposé un nouveau projet de loi baptisé « Cyber Resilience Act ». Ce texte a pour objectif d'établir des règles de cybersécurité communes pour l'ensemble des « produits comportant des éléments numériques ».

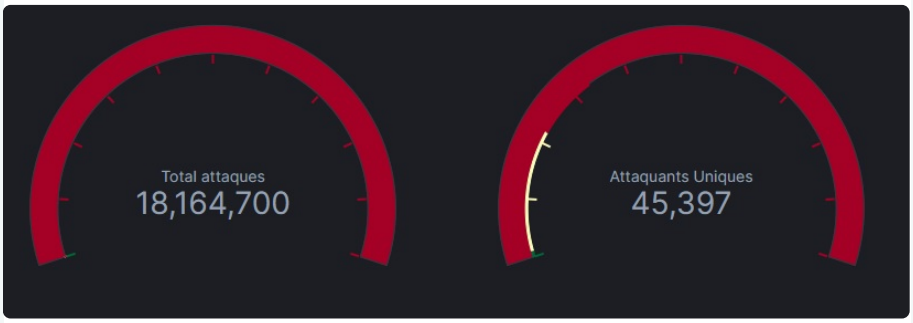
En savoir +

Cybersécurité : les prévisions pour 2023 ne sont pas réjouissantes

L'entreprise de cybersécurité américaine Trellix prévoit des pics de cyberattaques causés par les conflits géopolitiques en Asie et en Europe, ainsi qu'une intensification de l'hacktivisme

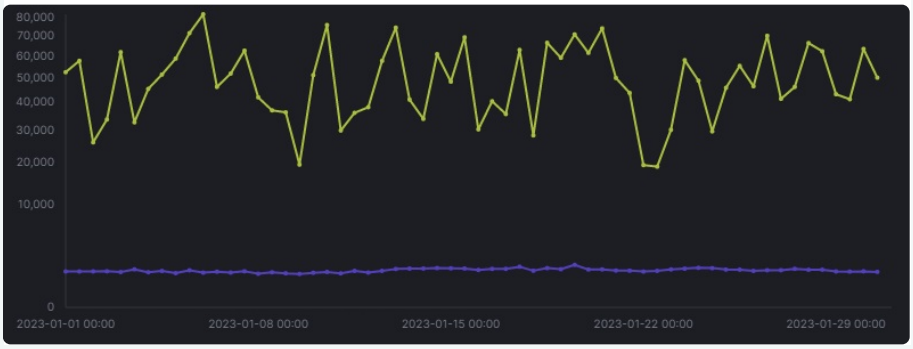
En savoir +

CHIFFRES ET TENDANCES EN NOUVELLE-CALEDONIE



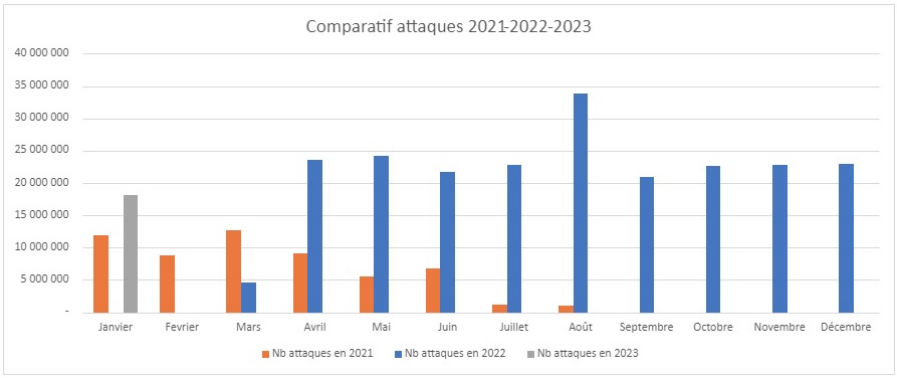
Via le honeypot, nous avons recensé sur le mois de décembre, 18 164 700 attaques en Nouvelle-Calédonie avec plus de 45 000 attaquants uniques.

Sur le graphique ci-dessous, vous pouvez constater l'évolution des attaques sur la période (courbe bleue) et des attaquants (courbe verte).



Période	Nb attaques	Tendance	Nb attaque/jours	Nb d'attaquants	moyen d'attaques / attaquants
janv-22	0		-		
févr-22	0		-		
mars-22	4 601 331	+100,00%	148 430	27674	166
avr-22	23 513 687	+411,02%	783 790	38657	608
mai-22	24 171 784	+2,80%	779 735	45679	529
juin-22	21 706 605	-10,20%	723 554	51334	423
juil-22	22 851 039	+5,27%	737 130	45375	504
août-22	33 840 381	+48,09%	1 091 625	43 352	781
sept-22	20 916 944	-38,19%	697 231	40 740	513
oct-22	22 716 197	+8,60%	732 781	41 379	549
nov-22	22 784 586	+0,30%	759 486	39 547	576
déc-22	22 901 003	+0,51%	738 742	43104	531
janv-23	18 164 700	-20,68%	585 958	45397	400
Total	**238 168 257**	**Attaques moyenne jour**	**598 343**	**42 022**	**507**

On constate qu'en janvier 2023, le nombre d'attaques est significativement moins important que fin 2022, mais que le nombre d'attaquants est plus important.



Le top 10 des ports attaqués

Ports	Nb d'attaques	Pourcentage	Description
445	814020	60,69	SMB Partage de fichiers et Microsoft DS Active Directory
22	166397	12,41	SSH Accés administration à distance et transfert de fichiers
5900	161923	12,07	VNC/RFB Accés ordinateur à distance
3389	69619	5,19	RDP Accés ordinateur à distance (Microsoft)
23	46717	3,48	TELNET communications texte non chiffrés
25	25159	1,88	SMTP Transfert de courier email
110	22110	1,65	POP3 Récupération de courrier email
443	13263	0,99	HTTPS Site et application Web en SSL/TLS
1433	11572	0,86	Utilisé par le serveur SQL de Microsoft.
80	10549	0,79	HTTP Site et application Web

Le nombre d'attaques a atteint un pic au début du mois de décembre 2022 (1,180 millions d'attaques en une journée). Pourtant en progression régulière depuis plusieurs années, le nombre d'attaques a chuté durant le mois de décembre 2022 et janvier 2023.
Le nombre d'attaques reste tout de même dans la moyenne de l'année 2022 (entre 600 000 et 700 000 attaques par jour).

Cette réduction du nombre d'attaques depuis début décembre 2022 s'explique essentiellement par une diminution très importante du nombre d'attaques provenant de Russie. Faut-il y voir les conséquences des conflits sur le Dark Web russe ?

L'ACTUALITÉ DE LA CYBERMALVEILLANCE

Le FBI et Europol abattent le site des hackers qui ont attaqué Altice

La plateforme de revendication et de vente des données des hackers de Hive est indisponible. Elle a été fermée par le FBI et Europol. Ce collectif était responsable de la cyberattaque contre le groupe Altice (SFR, BFM, RMC).

En savoir +

Panocrim 2023 du Clusif : la cybercriminalité change de dimension

Ransomware, MFA, cyberguerre, quantique, le panorama des menaces réalisé par le Clusif est complet. Il montre aussi qu'avec la guerre en Ukraine, la cybercriminalité s'est renforcée et adaptée à ce contexte. Il est donc nécessaire d'anticiper et de se préparer comme le montre l'équipe sécurité des JO Paris 2024

En savoir +

Les cyberattaques visent des cibles plus faciles, comme les TPE ou les sous-traitants, d’après l'Anssi

Les petites entreprises, les collectivités territoriales et les établissements publics de santé sont les premières cibles des cybercriminels, constate l’Agence nationale de la sécurité des systèmes d’information dans son rapport annuel 2022. Les attaquants se veulent de plus en plus discrets, en visant les équipements périphériques, comme les pare-feux ou les routeurs.

En savoir +

LA GAZETTE CYBER !

- WordPress : un nouveau malware exploite une vingtaine de failles !.En savoir +
- L'Anssi dévoile son panorama des cybermenaces en 2022. En savoir +
- Salve mondiale de cyberattaques via une faille ESXi. En savoir +

VOUS ÊTES VICTIME D'UNE CYBERATTAQUE ?

Si vous êtes victime d'une cyberattaque, voici les choses à faire :

- Déconnectez-vous d'internet
- Faites un balayage de votre ordinateur au moyen de votre logiciel antivirus pour vérifier s'il est infecté et, le cas échéant, éliminez le virus
- Procédez à une restauration complète de votre ordinateur si besoin
- Faites appel à un expert si vous croyez que le fonctionnement de votre ordinateur est toujours compromis
- Modifiez tous vos mots de passe

Procédez ensuite au dépôt de plainte au commissariat ou à la gendarmerie. Ils vous redirigeront vers les services spécifiques de lutte contre la cybercriminalité :

- Conservez des images de ce que vous voyez en utilisant la fonction « Imprimer écran ». Ces captures d'écran pourraient éventuellement aider l'enquête
- Listez tous les préjudices subis
- Munissez-vous de tous les éléments qui vous semblent pertinents : traces informatiques qui vous font penser à une attaque, fichier encrypté suite au virus, etc

Une enquête sera menée à la suite de votre dépôt de plainte.

LES BONNES PRATIQUES CYBER !

Particulier ou professionnel, découvrez les bonnes pratiques à appliquer en matière de cybersécurité !

Je découvre

CENTRE GOUVERNEMENTAL DE VEILLE

Retrouvez l'ensemble des alertes de sécurité, les menaces et incidents, les avis de sécurité, les indicateurs de compromission, les durcissements et recommandations, et les bulletins d'actualité du CERT.

Consultez

OPEN NC
Station N
Rue du Commandant Babo
98800 Nouméa
contact@open.nc

Vous n'êtes pas inscrit à la newsletter ? Inscrivez-vous en ligne