BULLETIN DE VEILLE CYBER

14 janvier 2025

EDITION N°7

UNE PANNE D'INTERNET MASSIVE EN RUSSIE

[07 janvier 2025] - Une panne importante du réseau Internet russe a été reporté le 07 janvier dernier, interrompant des services populaires comme Yandex, Google, Rutube, Vkontakte, Discord et des services de paiement en ligne, principalement sur la région de Moscou. L'opérateur mobile touché est MTS qui est un des principaux du pays.

Roskomnadzor, le régulateur des communications russes, a communiqué sur l'incident en évoquant des « problèmes techniques » sans aller plus loin ni sur les causes exactes ni sur les opérateurs affectés. MTS, l'opérateur affecté, n'a également pas communiqué sur le sujet.

Rappel : La Russie est un des rares pays à disposer d'un « Internet souverain » dans le sens où le pays dispose d'équivalents nationaux aux GAFAM américains mais une telle panne pose des questions sur les limites de cette souveraineté. En effet, cette panne ouvre le débat sur la gestion du réseau par les autorités, dans un contexte de recrudescence des cyberattaques ukrainiennes et de test des autorités sur l'infrastructure du réseau.

Source : https://www.solutions-numeriques.com/la-cnil-met-orange-a-lamende/

UNE FAILLE 0-DAY EXPLOITEE SUR UN LOGICIEL DE COLLABORATION EN ENTREPRISE

[08 janvier 2025] - Mitel, une entreprise de télécommunication canadienne, a subi une cyberattaque de type 0-day et une de type RCE (Remote Code Execution) contenu dans le serveur d'Oracle (WebLogic Server). Ces attaques ont été répertoriées et indexées par l'agence américaine de la cybersécurité (CISA).

Les logiciels clients (de Mitel pour le logiciel d'entreprise et Oracle pour le logiciel client) ont déjà été mis à jour sauf pour une faille mineure. Ce type de faille est semblable à un système d'authentification, offrant une passerelle pour les hackers. D'où la nécessité d'effectuer immédiatement les mises à jour et correctifs de sécurité.

Source : https://www.theregister.com/2025/01/08/mitel_0_day_oracle_rce_under_exploit/

LE BOTNET « GAYFEMBOY » SE PROPAGE DANS LE MONDE

[08 janvier 2025] - Le botnet exploite plus de 20 failles de sécurité de type 0-day et prend le contrôle des appareils en privilégiant les routeurs (qui gèrent les routes logiques « autoroutes de l'information »). Il est basé sur le code source de Mirai, logiciel malveillant découvert en 2016, et ciblant l'Internet des Objets (IoT) et qui voit d'autres types de virus se développer avec son code source.

Le code source est public et donc complètement modifiable par d'autres hackers qui veulent l'utiliser. Le mode opératoire est d'infecter les objets IoT et orchestrer ensuite des DDoS sur les serveurs visés. Initialement rapportée en Chine par une entreprise de cybersécurité en début de semaine, l'information se répand en Europe cette semaine

Source : https://www.01net.com/actualites/milliers-routeurs-pirates-botnet-exploite-20-failles-lancer-cyberattaques.html

Alexis Szelag

LA MAISON BLANCHE LANCE UN LABEL CYBERSECURITE POUR LES APPAREILS CONNECTES

[09 janvierc 2025] - Les appareils IoT sont de plus en plus présents dans la vie quotidiennes (Alexa, caméras connectées, moniteurs pour bébé, etc.) par. contre présentent des risques de sécurité élevées. Leurs données sont stockées sur des serveurs et les transmettent (volontairement ou non) vers de pays étrangers (ex la Chine).

L'objectif du label est d'offrir la possibilité d'un choix éclairé pour les consommateurs américains en termes d'objets IoT du point de vue de leurs cybersécurités.

Cependant, le label est assez critiqué car les fabricants doivent s'auto-évaluer et ignore les défis structurels des appareils connectés (dépendance au Cloud, absence de contrôle des utilisateurs sur les données stockées en serveur)

Source : https://securite.developpez.com/actu/366570/La-Maison-Blanche-lance-un-label-de-securite-Cyber-Trust-pour-les-appareils-connectes-les-critiques-estiment-que-ce-label-offre-une-securite-limitee-valable-jusqu-a-la-prochaine-vulnerabilite/

TELEFÓNICA CONFIRME QUE SON SYSTÈME DE GESTION DES INCIDENTS INTERNES A ÉTÉ PENETRÉ

[10 janvier 2025] - L'entreprise TELEFONICA est la plus grande entreprise de télécommunication espagnole, opérant sous le nom Movistar. Elle a communiqué sur l'incident et a annoncé avoir pris les mesures nécessaires pour mettre fin à tout accès non-autorisé ainsi que pour estimer l'étendue de la fuite

La brèche dans les serveurs de l'entreprise a été permise par l'utilisation des données d'authentification d'employés compromises

Source : https://www.bleepingcomputer.com/news/security/telefonica-confirms-internal-ticketing-system-breach-after-data-leak/

UN DISPENSAIRE DE CANNABIS AMERICAIN TOUCHE PAR UNE FUITE DE DONNEES

[11 janvier 2025] - Le système de point de vente de l'entreprise a été le point d'entrée des cybercriminels (situés en Californie). Les données personnelles de plusieurs consommateurs ont été illégalement obtenues par les criminels.

Les données comprennent des informations personnelles (noms, transactions, âge, adresse, etc.) et peuvent permettre d'identifier facilement les personnes. Une demande de rançon a été envoyée mais les négociations sont encore au point mort.

Source : https://securityaffairs.com/172950/data-breach/marijuana-dispensary-stiiizy-data-breach.html

Alexis Szelag

L'ITALIE VISEE PAR UNE VAGUE D'ATTAQUE DDOS PAR DES HACKTIVISTES PRO-RUSSE

[12 janvier 2025] - L'Italie a reçu le président ukrainien, V. Zelensky ce weekend pour réaffirmer le soutien du pays à l'Ukraine contre l'invasion de la Russie.
En parallèle, le groupe de hackers pro-russes « Noname057(16) » a lancé des attaques contre des infrastructures critiques de sites institutionnels (ministères) et d'organisations privés italiennes (banques notamment).

Ce groupe est actif depuis 2022 et est spécialisé dans les cyberattaques contre des gouvernements, et des infrastructures critiques dans le monde entier, particulièrement, contre les pays engagés contre la Russie dans la guerre en Ukraine.

Ces cyberattaques ont été lancées pendant des périodes stratégiques où moins d'employés sont présents pour assurer une réponse efficace (vacances, weekends)

Source : https://securityaffairs.com/172982/hacktivism/noname057-targets-italy.html

Alexis Szelag