AEGE

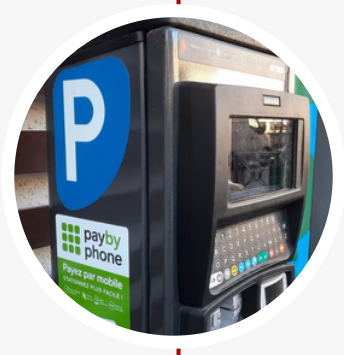
Club Cyber

BULLETIN DE VEILLE CYBER

03 Décembre 2024

EDITION N°3

LA CYBER CRIMINALITÉ DE PLUS EN PLUS PRÉSENTE DANS LA VIE RÉELLE



[24 NOVEMBRE 2024] - Les hackeurs utilisent de façon croissante des supports matériels comme **les QR Code** afin d'inciter les usagers à payer pour des parcmètres. Cela met en lumière l'idée que les menaces en ligne ne se limitent pas aux systèmes numériques, mais qu'elles s'étendent également aux aspects plus tangibles de la vie quotidienne.

Par le passé, ces escrocs recouraient à la méthode du "**skimming**", consistant à installer des dispositifs en plastique sur les distributeurs automatiques de billets des banques, précisément à l'emplacement destiné à l'insertion des cartes de crédit.

En **octobre 2024**, des stickers aux allures de QR code ont fleuri sur au moins **161 horodateurs à Nice**. Le site www.pbp-player.info qui apparaissait, imite de manière flagrante le site officiel.

Sources : Les conseils pratiques de Cyber malveillance.gouv / Conseils contre la cyber malveillance dans la vie réelle

PLUSIEURS GRANDES SOCIÉTÉS AU RALENTI APRÈS UNE CYBERATTAQUE CONTRE UN LOGICIEL DE SUPPLY CHAIN

[21 NOVEMBRE 2024] - L'éditeur américain de logiciels de supply chain Blue Yonder a été victime d'une **attaque par ransomware**. Des enseignes comme Starbucks, Sainsbury's ou encore BIC ont subi de lourdes perturbations.

Blue Yonder, une société américaine fournit des logiciels dans la supply chain pour plus de 3000 grandes entreprises dans 76 pays.
Les dégâts sont principalement au **Royaume-Uni** et aux **Etats-Unis**. Des entreprises comme Morissons ont dû mettre des systèmes de secours pour faire face aux défaillances dans sa gestion des produits dans ses entrepôts.

Ces entreprises sont particulièrement ciblés par les cybercriminels. Leur objectif est d'infiltré les systèmes de plusieurs clients à partir d'une unique porte d'entrée.

Sources : Les cyberattaques dans la supply chain / Article de Forbes sur le sujet

LA RUSSIE SERAIT PRÊTE À LANCER UNE CYBER GUERRE CONTRE LE ROYAUME-UNI

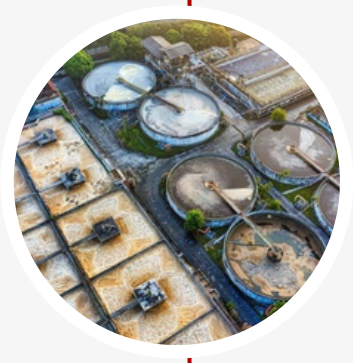
[24 NOVEMBRE 2024] - La Russie pourrait utiliser des attaques cyber pour diminuer le soutien du Royaume-Uni et de ses alliés à l'Ukraine.
Le chancelier, Pat McFadden, l'un des responsables de la **Sécurité Nationale britannique,** aurait évoqué ce type de menace. Plus particulièrement venant de l'Unité 29155 qui aurait déjà mené de nombreuses attaques au Royaume-Uni et en Europe.
Cette cyber guerre a pour objectif de déstabiliser les capacités de l'Ukraine.
Les attaques les plus préoccupantes touchent les **réseaux électriques** et les **entreprises britanniques**.
Au Royaume-Uni, ces dernières semaines, une série de cyberattaques ont été menées contre plusieurs conseils municipaux, dont certaines ont été revendiquées par un **groupe de pirates informatiques (pro-russes et russes)**.

Sources : Article de la BBC

Edwin Barancira

L'ANSSI DRESSE UN PANORAMA DES MENACES CYBER DANS LE SECTEUR DE L'EAU

[28 NOVEMBRE 2024] - Le secteur de l'eau intéresse de plus en plus les cyber criminels.



En février 2021, la Floride a mis en lumière la fragilité du secteur de l'eau. Un peu plus de trois ans après, l'ANSSI a décidé de se pencher sur la question en publiant un rapport. On apprend qu'entre janvier 2021 et août 2024, **46 entités du secteur** de la gestion de l'eau ont été touchées par un évènement de sécurité.

Plusieurs exemples qui montrent l'hétérogénéité du secteur de l'eau en termes de statuts (régie, syndicat intercommunal, société privée), des tailles variées et une maturité diverse sur la sécurité des SI. Si on ajoute à cela des installations industrielles vieillissantes et dispersées, il s'agit d'autant de brèches pour les attaquants.

Dans son rapport, l'ANSSI évoque l'**aspect géopolitique du secteur de l'eau** avec une recrudescence de l'hakctivisme pendant la période des Jeux Olympiques. En mars 2024, le groupe Cyber Army of Russia a revendiqué la prise de contrôle à distance de la **centrale hydroélectrique** de Courlon-sur-Yonne dans le département de l'Yonne en France. L'agence a finalement constaté que les attaquants avaient ciblé un moulin dans la Marne, géré par un particulier.

Sources : Panorama des menaces dans le secteur de l'eau

LE GROUPE DE HACKER RUSSE ROM COM EST PARVENU À EXPLOITER UNE FAILLE ZÉRO DAY SUR MOZILLA ET MICROSOFT

[28 NOVEMBRE 2024] - Les chercheurs en cybersécurité de la société slovaque ESET ont découvert deux **vulnérabilités 0-day** dans des produits de Mozilla Firefox et de Windows. Dans un rapport, ils expliquent que ces deux failles, combinées sous forme d'exploit 0-clic (sans interaction de l'utilisateur), ont permi à des hackers russes de cibler plusieurs centaines d'appareils en **Europe** et en **Amérique du Nord**.

La première faille détectée par ESET, intitulée CVE-2024-9680, présente un **score de sévérité critique (CVSS à 9,8)**. Il s'agit d'un bug d'utilisation dans la fonctionnalité de chronologie d'animation de Mozilla Firefox, permettant d'exécuter un code malveillant dans le sandbox (environnement isolé) du navigateur. La deuxième, d'un score de sévérité 8,8, est liée à une erreur d'élévation des privilèges dans la fonctionnalité du planificateur de tâches Windows.

Sources : Article de l'Usine Digitale / Le contenu du rapport de Eset