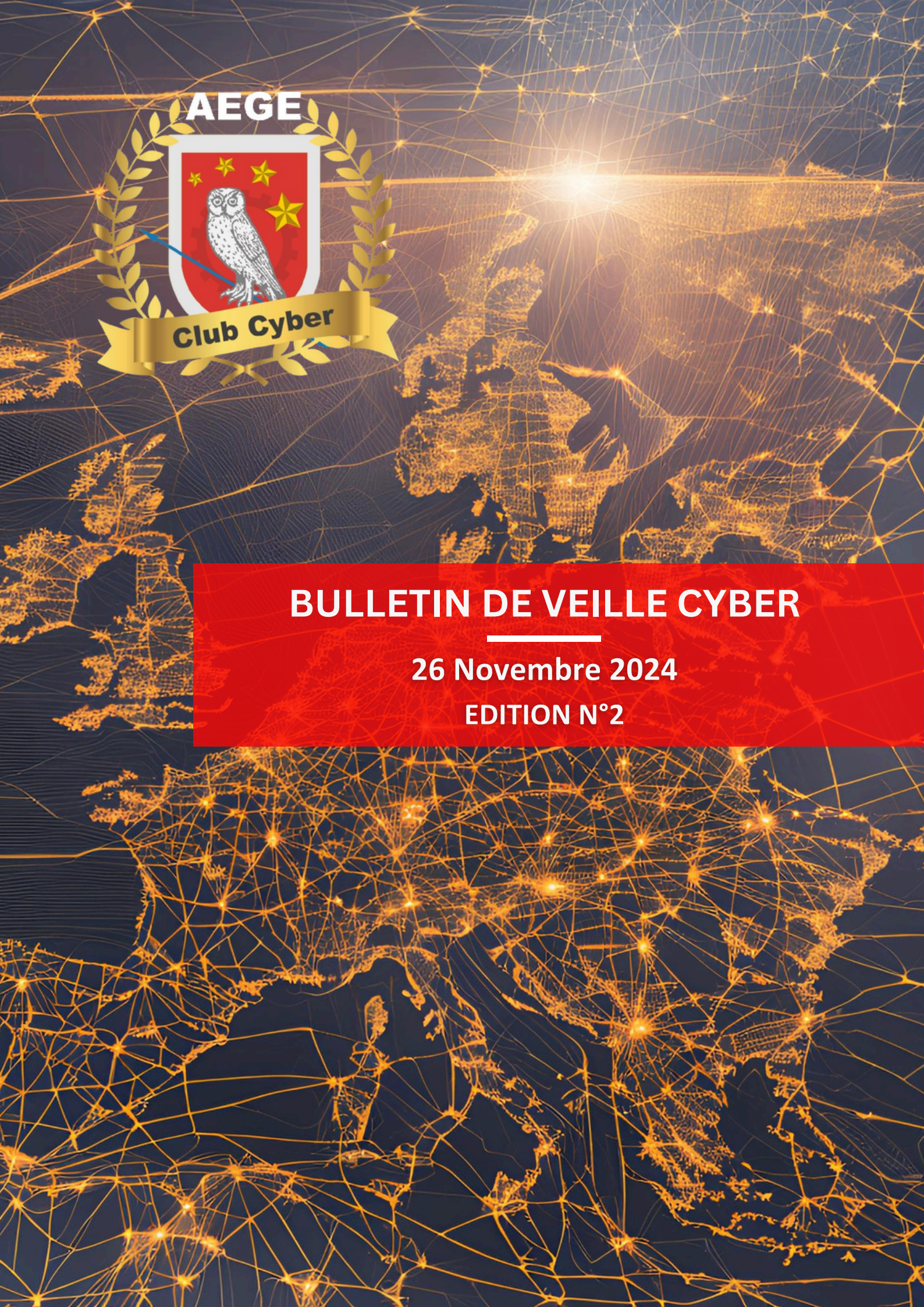
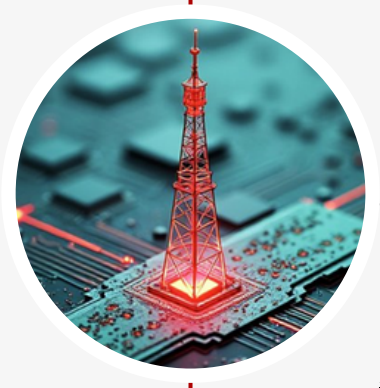


BULLETIN DE VEILLE CYBER

26 Novembre 2024

EDITION N°2

ESPIONNAGE DES RÉSEAUX TÉLÉCOM PAR SIGTRAN



[20 NOVEMBRE 2024] - De nombreuses cyberattaques affiliées à un groupe de cyber-espionnage lié à la Chine ont visés des entités de télécommunications en Asie du Sud et en Afrique depuis au moins 2020.

Ce groupe est suivi par l'entreprise CrowdStrike qui l'a nommé Liminal Panda. Ce dernier possède une connaissance approfondie des réseaux de télécommunications et des liens entre les différents fournisseurs.

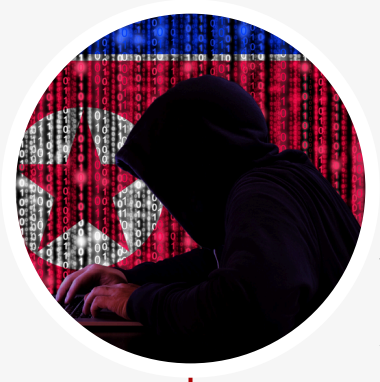
Liminal Panda utilise des outils qui lui facilite l'accès clandestin aux SI, le « *command and control* » (C2) ainsi que l'exfiltration de données.

Sources : https://thehackernews.com/2024/11/china-backed-hackers-leverage-sigtran.html

https://www.sekoia.io/fr/glossaire/command-control-c2/

VOL DE 10 MILLIONS DE DOLLARS GRÂCE À L'IA

[22 ET 23 NOVEMBRE 2024] - Sapphire Sleet aurait volé pour environ 10 millions de dollars de cryptomonnaies grâce à des campagnes d'ingénierie sociale s'étalant sur plus de six mois.



Microsoft aurait identifié la création de faux profils LinkedIn se faisant passer pour des recruteurs et des chercheurs d'emplois pour générer des revenus illicites permettant de contourner les sanctions internationales pesant sur la Corée du Nord.

L'IA a été utilisée pour la modification des photos et de documents volés aux victimes grâce à Faceswap ainsi que la modification de voix.

Sources : https://thehackernews.com/2024/11/north-korean-hackers-steal-10m-with-ai.html

https://www.microsoft.com/en-us/security/blog/2024/11/22/microsoft-shares-latest-intelligence-on-north-korean-and-chinese-threat-actors-at-cyberwarcon/

DÉPLOIEMENT DE HATVIBE ET CHERRYSPY

[21 ET 22 NOVEMBRE 2024] - TAG-110 et APT28 ont été identifiés dans des campagnes de cyber-espionnage visant des entités en Asie Centrale, Asie de l'Est et en Europe.

HATVIBE et CHERRYSPY ont été utilisés pour atteindre des institutions gouvernementales, des établissements d'éducation ainsi que des groupes soutenant les droits de l'Homme.

Plus précisément, HATVIBE est utilisé pour déployer CHERRYSPY, une porte dérobée en Python pour l'exfiltration de données et l'espionnage.
Le CERT-UA date la première utilisation à mai 2023. Depuis, 62 victimes ont été identifiées dans 11 pays différents.

Sources : https://www.recordedfuture.com/research/russia-aligned-tag-110-targets-asia-and-europe

https://thehackernews.com/2024/11/russian-hackers-deploy-hatvibe-and.html

Ghita Rachidi

CYBERATTAQUES EN FRANCE : DIRECT ASSURANCE, SFR, LE POINT ET MEDIBOARD

[21 NOVEMBRE 2024] - Le même pirate « *Near* » serait à l'origine de plusieurs vols de données :

- Direct Assurances : vol de données dont les IBAN.
- Mediboard : les données personnelles et médicales de 758 912 français ont été dérobées dont nom, prénom, adresse, ordonnances, numéro de téléphone, médecin traitant.
- SFR : vol de données de 150 782 clients dont les IBAN.
- Le Point : vol de données de 915 000 abonnés du média.

Sources : https://www.clubic.com/actualite-544418-cyberattaques-de-sfr-direct-assurance-le-point-et-donnees-medicales-tous-ont-ete-pirates-par-le-meme-hacker-qui-reclame-des-sommes-derisoires.html

https://www.usine-digitale.fr/article/direct-assurance-victime-d-une-cyberattaque-les-donnees-de-15-000-clients-derobees.N2222978

DES HACKERS CHINOIS ATTAQUENT LINUX GRÂCE AU LOGICIEL MALVEILLANT WOLFSBANE

[21 NOVEMBRE 2024] - Une nouvelle porte dérobée Linux nommée « *WolfsBane* » a été découverte et serait utilisée par le groupe cybercriminel chinois *Gelsemium*.

W*olfsBane* est un logiciel malveillant utilisant un rootkit open-source modifié pour échapper à la détection. La tendance à l'augmentation des cyberattaques visant Linux est sûrement lié au renforcement de la sécurité des systèmes Windows.

De ce fait, les groupes de pirates informatiques se concentrent davantage sur les vulnérabilités des systèmes connectés à Internet dont la plupart fonctionnent sous Linux.

Source : https://www.bleepingcomputer.com/news/security/chinese-gelsemium-hac

https://www.kaspersky.fr/resource-center/definitions/what-is-rootkitkers-use-new-wolfsbane-linux-malware/

MITRE – PUBLICATION DES 25 FAILLES LOGICIELLES LES PLUS DANGEREUSES DE 2024

[21 NOVEMBRE 2024] - Les faiblesses logicielles font référence aux défauts, bogues, vulnérabilités et erreurs trouvés dans le code, l'architecture, la mise en œuvre ou la conception du logiciel.

Afin de réaliser le classement de cette année, MITRE a noté chaque faiblesse en fonction de sa gravité et de sa fréquence après avoir analysé 31 770 enregistrements CVE signalisées entre 2023 et 2024 ainsi que les failles de sécurité ajoutées au classement de la CISA.

Sources : https://www.silicon.fr/Thematique/cybersecurite-1371/Breves/Top-25-CWE-2024-la-methodo-evolue-et-le-classement-465122.htm

https://fr.techtribune.net/d2/tendance-actuelle/mitre-partage-les-25-faiblesses-logicielles-les-plus-dangereuses-de-2024/951084/

Ghita Rachidi