MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »
Commandement du ministère de l'Intérieur dans le cyberespace

Revue de presse des cybermenaces

Centre d'analyse et de regroupement des cybermenaces

#01 – JANVIER 2025

A retenir

Le mois de décembre est marqué par plusieurs **opérations des forces de sécurité intérieure** ciblant les attaques par déni de service distribué, les rançongiciels, les services illicites de messagerie chiffrée et les distributeurs de bitcoins. Parmi les rapports publiés, celui de Palo Alto met en lumière les escroqueries associées aux grands évènements.

Les cybermenaces se déclinent sous diverses formes, allant **des attaques DdoS aux rançongiciels, en passant par les vols de données**. Par ailleurs, **les cryptoactifs** occupent une place de plus en plus importante au sein de l'actualité.

Chiffres du mois

Hameçonnage : 94 % des organisations interrogées par SOCRadar ont déclaré avoir subi des incidents de sécurité par courriel en 2024, avec des tactiques plus sophistiquées exploitant les émotions des cibles.

Cryptoactifs : selon Chainalysis, **2,2 milliards USD de fonds** ont été volés en 2024, dont 1,3 milliard USD par le groupe cybercriminel Lazarus, lié aux autorités de la Corée du Nord.

Principales cyberattaques

02 décembre, l'entreprise spécialisée dans l'entretien et la réparation des véhicules **Norauto** annonce être victime d'une **fuite de données**. Les clients ont été avertis par mail de l'intrusion. Sur des forums cybercriminels, des acteurs malveillants mettent en vente des bases de données Norauto présentées comme dérobées. Ces revendications seraient remises en cause par d'autres membres des **forums** en raison des **échantillons diffusés peu crédibles**. Usine Digitale

02 décembre, une nouvelle campagne d'**hameçonnage** (*phishing*) est en cours et vise les utilisateurs de la société **Ledger**. Les escrocs prétendent qu'une **faille de sécurité** a eu lieu et, au prétexte de « vérifier » leurs comptes, demandent aux victimes de fournir la phrase secrète de récupération de leur portefeuille de cryptoactifs. Ledger

10 décembre, **LDLC** est victime d'un **vol de données** pour la seconde fois en 2024. Dans un communiqué, la société de commerce informatique avertit ses clients, mais n'apporte pas de précision concernant le volume et le type de données concernées par l'intrusion. En mars 2024, 1,5 million de données client du groupe avaient été dérobées. LDLC

12 décembre, **Microsoft** a annoncé bloquer **7 000 attaques de mots de passe par seconde**, soit près du double du taux enregistré il y a tout juste un an. Microsoft

15 décembre, une cyberattaque visant la société de services et de conseil en informatique **ASROE de Soual** a impacté près de **30 000 agriculteurs** répartis dans 22 départements. L'**hébergeur des logiciels de gestion de troupeaux** est rendu inaccessible, obligeant les clients à déclarer sur papiers le suivi de leurs activités. Le système de sauvegarde et le serveur qui fait tourner les autres serveurs seraient **chiffrés**. La vente et le suivi des naissances sont encore impactés. France Tv Info

28 décembre, attaque par **rançongiciel** revendiquée par ***Spacebears*** contre l'entreprise **Atos**. Le géant Français du numérique **dément** dans un communiqué de presse l'intrusion et le vol de données. Aucune preuve de compromission ni aucune demande de rançon n'ont été décelées. Atos

Pour aller plus loin…

[Palo Alto] – Étude « *Suspicious Domain Registrations and Other Scams* » - Exploitation des grands évènements mondiaux par les acteurs malveillants (enregistrement de noms de domaines approchants, campagnes d'hameçonnage et autres techniques d'escroqueries).

[Cryptoast] Analyse concernant la Finance décentralisée (Decentralized Finance, DeFi) : la blockchain Polygon propose d'utiliser près d'un milliard USD en cryptoactifs stables (*stablecoins*) pour générer des intérêts liés à des prêts. Le fondateur du protocole de prêt décentralisé AAVE, qui représente plus de 450 millions USD de cryptoactifs sur Polygon, refuse la proposition, avançant des risques de sécurité.

[SOCRadar] « *Top Phishing tricks attackers use to target employees* » - le rapport présente les dernières tendances observées en matière d'hameçonnage. Les techniques semblent plus évoluées et davantage ciblées. Un focus est dédié au JOP de Paris 2024.

Faits marquants

À Paris, **treize distributeurs automatiques de bitcoins** ont été **démantelés** après une enquête de la juridiction inter-régionale spécialisée (**JIRS**) déclenchée par l'Autorité des marchés financiers (**AMF**). En cause : l'absence d'enregistrement obligatoire en tant que prestataire de services sur actifs numériques. AMF Journal du coin

Dans le cadre de l'opération internationale **PowerOFF**, impliquant **l'OFAC** et la **JUNALCO** ont démantelé **27** plateformes de **DDoS-for-hire**, connues sous le nom de ***booters***, qui permettaient à des cybercriminels de lancer des attaques par déni de service distribué (*DDoS*) contre des sites web, les rendant inaccessibles. Europol

Le 3 décembre 2024, dans le cadre d'une coopération menée avec **Europol**, les autorités françaises (dont l'Office Anti-Cybercriminalité) et néerlandaises ont démantelé un service de messagerie chiffré nommé Matrix (différent du protocole légitime matrix.org et ses diverses applications). Ce service était utilisé par près de **8 000 criminels**. Près de **2,3 millions de messages** ont pu être déchiffrés et environ **645 000 euros saisis**. The Record

Fruit de la coopération entre cybermalveillance.gouv.fr, la Police et la Gendarmerie, le **17Cyber** constitue depuis le 18 décembre une **nouvelle offre de sécurité** pour les internautes. Ce module, pouvant être directement intégré à certains sites web, permet aux **victimes de cyberattaques** de disposer d'un **premier outil de diagnostic**, de recevoir des conseils, et d'être mis en relation avec un policier ou un gendarme. Les entreprises, collectivités ou associations peuvent également être mises en relation avec des experts en cybersécurité agréés. Cybermalveillance.gouv.fr ZDnet

Informations sur la menace

Une **faille de sécurité**, désormais corrigée, permettrait à un acteur malveillant sur le chatbot de l'IA **DeepSeek**, de prendre le contrôle du compte d'une victime en exploitant une attaque par **injection de messages**. L'exploitation de cette faille détournerait la session d'un utilisateur et accéderait aux cookies et autres données associées au domaine chat.deepseek[.]com, générant la **prise de contrôle du compte**. The Hacker News

Découverte du maliciel ***DroidBot*** ciblant les systèmes d'exploitation Android. Il est commercialisé sous le modèle *Malware-as-a-Service*, pour 3 000$. Le maliciel serait conçu pour notamment attaquer les utilisateurs de **huit banques françaises**. *DroidBot* enregistre les touches tapées sur le clavier, intercepte les SMS pour rechercher des identifiants de connexion et affiche une fenêtre malveillante factice par-dessus une application bancaire ou financière. 01Net

Condamnation de deux ans avec sursis pour **l'étudiant** en informatique qui avait lancé une **attaque par bourrage d'identifiant** (*credential stuffing*) contre **Ile-de-France Mobilités** en 2023. Il a été reconnu coupable d'accès, de maintien et d'extraction frauduleuse dans un système de traitement automatisé de données, et de détention sans motif légitime d'un programme malveillant. Âgé de 20 ans, il écope d'une amende de 5 000 euros, d'une interdiction d'exercer dans la cybersécurité pendant trois ans avec sursis et doit verser 10 000 euros à Ile-de-France Mobilités. ZDNET

Le 17 décembre, l'ancien responsable de la sécurité des systèmes d'information (**RSSI**) du groupe hospitalier Grand Ouest a été **interpellé** par les enquêteurs du Centre de lutte contre les criminalités numériques (C3N) et de la Section de Recherche de Rennes. Celui-ci est mis en cause dans le cadre de l'**attaque par rançongiciel** dont la clinique La Sagesse à Rennes, appartenant à ce groupe hospitalier, avait été victime le 4 octobre. Cette cyberattaque avait alors entraîné l'interruption de plusieurs interventions chirurgicales et une rançon de 650 000 euros avait été exigée. Le Parisien

Anticipation / Réglementation

L'exercice ***Crossed Swords 2024*** de l'OTAN a débuté à Tallinn, en Estonie. Cet exercice vise à **former des spécialistes** à l'exécution d'une **chaîne d'attaque cyber offensive** dans un environnement de crise simulé. CCDCOE

Lutte contre le blanchiment de capitaux et le financement du terrorisme : le Règlement européen sur le Transfert de Fonds et de certains crypto-actifs (*Transfer of Funds Regulation II*, dit « **TFR 2** ») est **entré en vigueur** le 30 décembre 2024. L'Autorité des marchés financiers (AMF) publie une position intégrant les orientations de l'Autorité Bancaire Européenne (EBA). AMF

Hexarq, la filiale du groupe Banque Populaire Caisse d'épargne (BPCE) obtient l'agrément de Prestataire de Services sur Actifs Numériques (PSAN) auprès de l'Autorité des Marchés Financiers (AMF), après Société Générale Forge et les plateformes Deblock et GoIN. La **fourniture de services sur cryptoactifs** est désormais **encadrée** par le Règlement européen *Markets in Crypto Assets* (MiCA). AGEFI