29 avril 2025 - ÉDITION N°22

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

POUR LA PREMIÈRE FOIS, LA FRANCE ATTRIBUE OFFICIELLEMENT DES ATTAQUES CYBER À LA RUSSIE

Du 29 avril 2025

Pour la première fois, **la France a désigné officiellement la Russie** comme responsable de **cyberattaques** menées contre ses intérêts. Le ministère de l'Europe et des Affaires Étrangères s'est exprimé publiquement sur les réseaux, notamment en la personne du ministre Jean-Noël Barrot, qui a accusé le **renseignement militaire russe (GRU)** d'être à l'origine de cyberattaques contre « *une dizaine d'entités françaises depuis 2021.* » Le GRU a ainsi ciblé la **campagne présidentielle d'Emmanuel Macron** en 2017, la chaîne **TV5 Monde** en 2015 et des structures liées aux **Jeux olympiques** de Paris 2024.

Dans le viseur : le **mode opératoire APT28**, connu des experts, et l'**unité 20728 du GRU**, citée pour la première fois publiquement. L'attribution s'appuie sur un **rapport de l'ANSSI** réalisé avec la DGSE, la DGSI et la DGA.

Source :

- **Le Monde :** https://www.lemonde.fr/international/article/2025/04/29/la-france-attribue-pour-la-premiere-fois-officiellement-des-cyberattaques-a-la-russie_6601713_3210.html

L'ANSSI PUBLIE LE BILAN DU VOLET CYBERSÉCURITÉ DE FRANCE RELANCE

Du 28 avril 2025

Le volet cybersécurité du plan France Relance est un **succès**, selon le bilan publié par l'ANSSI, qui présente les travaux entrepris par l'Agence en 2024.

Ce programme des parcours de cybersécurité a permis de **renforcer la sécurité de 945 acteurs publics** (collectivités, établissements de santé, entités publiques), tout en dynamisant l'écosystème national de la cybersécurité.

En effet, sur les 100 millions d'euros investis dans le programme, 40 millions ont été investis pour l'acquisition de produits de cybersécurité français et européens, dont **33 millions dédiés à des solutions françaises** ! Au total, 197 prestataires ont été mobilisés sur l'ensemble du territoire national.

Sources :

- **Cyber.gouv.fr** : https://cyber.gouv.fr/actualites/bilan-du-volet-cybersecurite-de-france-relance-un-defi-reussi

OUVERTURE DU LOCKED SHIELDS 2025, LA FRANCE FAIT ÉQUIPE AVEC LA POLOGNE

Du 28 avril 2025

La **15e édition de Locked Shields** a débuté le 28 avril et se poursuivra jusqu'au 09 mai 2025.

Locked Shields est l'**exercice de Lutte Informatique Défensive (LID) international** le plus sophistiqué à ce jour, organisé par le Centre d'excellence pour la cyberdéfense en coopération de l'**OTAN** (CCDCOE).

Cet exercice majeur vise à entraîner les équipes à la défense informatique en situation de crise, en favorisant la coopération entre nations. Cette année, **la France**, représentée par les les cybercombattants du ministère des Armées et de l'ANSSI, **fait équipe avec la Pologne !**

À noter, la participation de **quatre écoles françaises** : EPITA, ENSIBS, Ecole 2600 et ESGI. Cocorico !

Sources :

- **COMCYBER** : https://www.defense.gouv.fr/comcyber/evenements/locked-shields-2025
- **CCDCOE** : https://ccdcoe.org/exercises/locked-shields/

LES PAYS-BAS ALERTENT SUR UNE ESCALADE DES CYBERATTAQUES RUSSES

Du 28 avril 2025

Le **service de renseignement militaire néerlandais (MIVD)** alerte sur une escalade des cyberattaques russes visant à déstabiliser les Pays-Bas.

Dans son dernier rapport annuel, le MIVD révèle une **tentative inédite de cybersabotage contre une infrastructure publique critique**, sans dégâts mais hautement symbolique.

D'autres attaques ont visé des **partis politiques** et des **services de transport** en pleine période électorale. La MIVD soupçonne également des reconnaissances en mer du Nord autour de **câbles internet**. « *Ce rapport annuel confirme que nous vivons dans une zone grise entre la guerre et la paix* », a déclaré le ministre de la Défense Ruben Brekelmans.

Source :

- **InCyber News** : https://incyber.org/article/pays-bas-vises-par-tentative-cybersabotage-russe/
- **MIVD** : https://www.defensie.nl/actueel/nieuws/2025/04/22/russische-brutaliteit-om-samenleving-te-ontwrichten-neemt-toe

DÉPENDANCE NUMÉRIQUE : 80% DES DÉPENSES EUROPÉENNES EN LOGICIELS ET CLOUD PARTENT VERS LES ÉTATS-UNIS

Du 25 avril 2025

La dépendance numérique de l'Europe coûte cher : **264 milliards d'euros s'envolent chaque année** vers les États-Unis, selon une étude commandée par le **Cigref**, qui regroupe les plus grandes entreprises et administrations publiques françaises.

Autrement dit, ce sont **80% des dépenses** liées aux logiciels et services cloud à usage professionnel en Europe qui profitent à des entreprises comme Microsoft ou Google. Aux États-Unis, ces activités représentent pas moins de 2 millions d'emplois. L'étude envisage qu'en 2035, **si 15% de ces dépenses restaient en Europe, elles généreraient environ 500 000 emplois.**

Sources :

- **Cigref** : https://www.cigref.fr/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe
- **Usine Digitale** : https://www.usine-digitale.fr/article/la-dependance-numerique-aux-etats-unis-coute-264-milliards-d-euros-par-an-a-l-europe.N2231200

VIGINUM : UNE DOCTRINE « OPEN CTI » POUR STRUCTURER LA LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION (LMI)

Du 24 avril 2025

VIGINUM, le service français de vigilance contre les ingérences numériques étrangères, a publié sa doctrine « Open CTI » pour structurer la **Lutte contre les Manipulations de l'Information (LMI)**.

Ce document définit un cadre méthodologique visant à capitaliser les connaissances sur les campagnes de désinformation, en s'appuyant sur la plateforme open-source OpenCTI, initialement conçue pour la cybersécurité et désormais adaptée à la **menace informationnelle**.

Elle permet de modéliser des éléments tels que les narratifs, les modes opératoires et les indicateurs techniques, facilitant ainsi la **collaboration entre les différents acteurs** engagés dans la LMI.

Source :

- **SGDSN** : https://www.sgdsn.gouv.fr/publications/guide-dutilisation-dopencti-pour-la-lutte-contre-les-manipulations-de-linformation

LES GROUPES DE RANSOMWARE-AS-A-SERVICE DIVERSIFIENT LEURS OFFRES POUR SÉDUIRE PLUS DE CYBERCRIMINELS

Du 24 avril 2025

Le **Ransomware-as-a-Service (RaaS)** est un **modèle commercial criminel** où des développeurs conçoivent des rançongiciels qu'ils louent ou vendent à d'autres cybercriminels, leurs « affiliés ». Selon une **étude de Secureworks**, DragonForce et Anubis, deux acteurs majeurs du RaaS, ont **repensé leur modèle d'affiliation** pour séduire davantage de cybercriminels.

DragonForce propose une infrastructure clé en main – outils, leak site sur Tor, support technique – et permet à ses affiliés de créer leur propre marque.

Anubis offre trois options : un chiffrement classique, une extorsion basée sur le vol de données, et une aide à l'extorsion de victimes déjà compromises, avec des parts de rançon pour les affiliés de 80%, 60% ou 50%.

Source :

- **Secureworks** : https://www.secureworks.com/blog/ransomware-groups-evolve-affiliate-models