

L'ALLEMAGNE ET LA TCHÉQUIE ATTRIBUENT AU GRU UNE CAMPAGNE D'APT28, DONT LE PIRATAGE DU SPD

Le 3 mai 2024, l'Allemagne et la Tchéquie ont attribué à APT28, lié au GRU, une cybercampagne exploitant une vulnérabilité d'Outlook. En Allemagne, la campagne a visé le siège du SPD à partir de fin décembre 2022, ainsi que des entreprises des secteurs de la défense, de la logistique, de l'aérospatiale et de l'informatique. Des institutions de l'État tchèque ont également été ciblées. L'UE et l'OTAN ont publié des déclarations de soutien.

UKRAINE EVIDENCE HUB
AU-DELÀ DE L'UKRAINE
AU 15 OCT. 2026

DEGRÉ DE PREUVE

ATTRIBUTION OFFICIELLE

Un gouvernement, un procureur, l'UE, l'OTAN ou un organe de l'ONU a formellement désigné la Russie, ses services ou ses forces soutenues par l'État. Il s'agit d'une position de cette autorité, non d'un jugement.

QUI L'A ÉTABLI

Gouvernement fédéral allemand / Ministère fédéral de l'intérieur (3 mai 2024) ; Ministère tchèque des affaires étrangères (3 mai 2024) ; déclarations du Haut Représentant de l'UE et de l'OTAN le même jour.

DERNIÈRES NOUVELLES

L'Allemagne a depuis attribué d'autres opérations d'APT28, dont l'attaque d'août 2024 contre le prestataire du contrôle aérien DFS (déc. 2025).

LIEN AVEC LA GUERRE CONTRE L'UKRAINE

Le Gouvernement allemand rattache le calendrier de la campagne à son soutien à l'Ukraine (début 2023).

SOURCES

- B** Ministère fédéral allemand de l'Intérieur – Des cyberattaques attribuées au service de renseignement militaire russe · 2024-05-03
<https://bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html>
- B** Ministère tchèque des Affaires étrangères – Déclaration du MAE sur les cyberattaques · 2024-05-03
https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html
- C** Security Affairs – L'OTAN et l'UE condamnent officiellement le cyberespionnage d'APT28, lié à la Russie · 2024-05-03
<https://securityaffairs.com/162759/apt/nato-eu-condemned-apt28-espionage.html>

CE QUE NOUS DEMANDONS DES ÉTATS MEMBRES

- Attribuer conjointement et porter la question devant le Groupe de travail à composition non limitée des Nations Unies sur la sécurité du numérique.
- Appliquer le régime de sanctions cyber de l'UE aux unités responsables.
- Partager les indicateurs et renforcer la résilience des infrastructures critiques.

Le statut suit quatre degrés de preuve : décision de justice · attribution officielle · mis en accusation · soupçonné (les cas soupçonnés ne figurent que sur la page en ligne). Niveau A = juridictions, organes de l'ONU, organisations internationales · B = gouvernements, parquets · C = médias et enquêteurs. Rectificatifs : evidence@ukraine-evidence.org



page en ligne ·
rectificatifs