

ALEMANIA Y CHEQUIA ATRIBUYEN AL GRU LA CAMPAÑA DE APT28, INCLUIDO EL HACKEO DEL SPD

El 3 de mayo de 2024, Alemania y Chequia atribuyeron a APT28, vinculado al GRU, una campaña cibernética que aprovechaba una vulnerabilidad de Outlook. En Alemania, la campaña afectó a la sede del partido SPD desde finales de diciembre de 2022, así como a empresas de defensa, logística, aeroespaciales e informáticas. También se atacó a instituciones del Estado checo. La UE y la OTAN emitieron declaraciones de apoyo.

UKRAINE EVIDENCE HUB
MÁS ALLÁ DE UCRANIA
A 15 OCT 2026

GRADO DE PRUEBA ATRIBUCIÓN OFICIAL Un Gobierno, una fiscalía, la UE, la OTAN o un órgano de las Naciones Unidas ha señalado formalmente a Rusia, a sus servicios o a sus fuerzas respaldadas por el Estado. Se trata de una posición de esa autoridad, no de una sentencia.	QUIÉN LO ESTABLECIÓ Gobierno Federal de Alemania / Ministerio Federal del Interior (3 may 2024); Ministerio de Relaciones Exteriores de Chequia (3 may 2024); declaraciones del Alto Representante de la UE y de la OTAN ese mismo día.
LO MÁS RECIENTE Desde entonces, Alemania ha atribuido otras operaciones de APT28, entre ellas el ataque de agosto de 2024 contra el proveedor de control del tránsito aéreo DFS (dic 2025).	VÍNCULO CON LA GUERRA CONTRA UCRANIA El Gobierno alemán vincula el momento de la campaña con su apoyo a Ucrania (principios de 2023).
FUENTES B Ministerio Federal del Interior de Alemania – Ciberataques atribuidos a la agencia de inteligencia militar rusa · 2024-05-03 https://bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html B Ministerio de Asuntos Exteriores de la República Checa – Declaración del Ministerio sobre los ciberataques · 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 – La OTAN y la UE condenan formalmente el ciberespionaje de APT28, vinculado a Rusia · 2024-05-03 https://securityaffairs.com/162759/apt/nato-eu-condemned-apt28-espionage.html	
QUÉ PEDIMOS A LOS ESTADOS MIEMBROS • Atribuir conjuntamente y plantearlo en el Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre seguridad de las TIC. • Aplicar el régimen de sanciones cibernéticas de la UE a las unidades responsables. • Compartir indicadores y apoyar la resiliencia de las infraestructuras críticas.	

El estado sigue cuatro grados de prueba: decisión judicial · atribución oficial · imputados · sospecha (los casos sospechosos solo figuran en la página en línea). Nivel A = tribunales, órganos de la ONU, organizaciones internacionales · B = gobiernos, fiscalías · C = medios e investigadores. Correcciones: evidence@ukraine-evidence.org



página en línea ·
correcciones