

德国和捷克将包括入侵社民党在内的APT28攻击活动归咎于格鲁乌

2024年5月3日，德国和捷克将一场利用Outlook漏洞的网络攻击活动归咎于与格鲁乌有关联的APT28。在德国，该活动自2022年12月下旬起攻击了社会民主党总部以及国防、物流、航空航天和信息技术企业。捷克国家机构也成为攻击目标。欧盟和北约发表了支持声明。

UKRAINE EVIDENCE HUB
乌克兰境外
截至 2026年10月15日

证明程度

官方归因

某国政府、检察机关、欧盟、北约或联合国机构已正式点名俄罗斯、其情报部门或其国家支持的部队。这是该机构的立场，而非判决。

认定方

德国联邦政府/联邦内政部（2024年5月3日）；捷克外交部（2024年5月3日）；欧盟高级代表和北约当天发表的声明。

最新

此后，德国又将APT28的其他行动归咎于俄罗斯，包括2024年8月对空中交通管制机构DFS的攻击（2025年12月）。

与对乌克兰战争的关联

德国政府将该活动的时间与其对乌克兰的支持（2023年初）联系起来。

来源

B 德国联邦内政部——网络攻击被追溯至俄罗斯军事情报机构 · 2024-05-03
<https://bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html>

B 捷克外交部——外交部关于网络攻击的声明 · 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——北约和欧盟正式谴责与俄罗斯有关联的APT28网络间谍活动 · 2024-05-03
<https://securityaffairs.com/162759/apt/nato-eu-condemned-apt28-espionage.html>

我们的诉求

(致会员国)

- 联合归因，并在联合国信息和通信技术安全问题不限成员名额工作组提出。
- 对相关责任单位适用欧盟网络制裁制度。
- 共享威胁指标，支持关键基础设施的韧性。

状态分为四个证明程度：法院认定 · 官方归因 · 已起诉 · 涉嫌（涉嫌案例仅列于网站页面）。A级 = 法院、联合国机构、国际组织 · B级 = 政府、检察机关 · C级 = 媒体和调查人员。更正：evidence@ukraine-evidence.org



网站页面 · 更正