LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-05 17:57:15 UTC

APT15 Cyber Espionage: Campaigns and TTPs Analysis

CVE: 5 | **URL:** 1 | **Hostname:** 2

APT15, a cyber espionage group with origins in China, has been active since approximately 2010 and has conducted numerous high-profile campaigns targeting government, diplomatic, and military sectors across North America, Europe, and the Middle East. Their operations include notable incidents such as the 2013 "moviestar" operation against European Ministries of Foreign Affairs, attacks on Indian embassy personnel in 2016, and the hacking of a US Navy contractor in 2018. Even after significant disruptions like the 2021 crackdown by Microsoft, APT15 adapted and continued its activities, notably deploying a new backdoor called Graphican in 2022 and using the ORB3 network for operations in 2023.

- 161 Subscribers

- 373,955 Subscribers

- 841 Subscribers

- 841 Subscribers

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

- 373,955 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:GoldenEagle