Fancy Bear Hackers (APT28): Targets & Methods | CrowdStrike

By Editorial Team

Archived: 2026-04-05 14:53:44 UTC

The nation-state adversary group known as FANCY BEAR (also known as APT28 or Sofacy) has been operating since at least 2008 and represents a constant threat to a wide variety of organizations around the globe. They target aerospace, defense, energy, government, media, and dissidents, using a sophisticated and cross-platform implant.

FANCY BEAR's code has been observed targeting conventional computers and mobile devices. To attack their victims, **they typically employ both phishing messages and credential harvesting using spoofed websites.** FANCY BEAR has demonstrated the ability to run multiple and extensive intrusion operations concurrently. In the blog post, Bears in the Midst, CrowdStrike CTO Dmitri Alperovitch details the **adversary's operations against U.S. political organizations**. At the same time that operation was occurring, this actor was involved in extensive operations targeting European military organizations. This adversary has dedicated considerable time to developing **their primary implant known as XAgent,** and to leverage proprietary tools and droppers such as **X-Tunnel, WinIDS, Foozer and DownRange**. Their main implant has been ported across multiple operating systems for conventional computers as well as mobile platforms. This group is also known for **registering domains that closely resemble domains of legitimate organizations** they plan to target in order to establish phishing sites that spoof the look and feel of the victim's web-based email services, with the intention of harvesting their credentials.

Fancy Bear's Targets

FANCY BEAR is a Russian-based threat actor whose **attacks have ranged far beyond the United States and Western Europe.** The group has been observed targeting victims in multiple sectors across the globe. Because of its extensive operations against defense ministries and other military victims, FANCY BEAR's profile **closely mirrors the strategic interests of the Russian government**, and may indicate affiliation with Главное Разведывательное Управление (Main Intelligence Department) or GRU, Russia's premier military intelligence service. FANCY BEAR has also been linked publicly to **intrusions into the German Bundestag and France's TV5 Monde TV station in April 2015.**

Other Known Russia-Based Adversaries

- Cozy Bear
- Venomous Bear
- Voodoo Bear

Curious about other nation-state adversaries? *Visit our threat actor center to learn about the new adversaries that the CrowdStrike team discovers.*

Learn More

- To learn more about using threat intelligence to defend your enterprise, protect your endpoints and proactively hunt sophisticated threat actors, visit the **CrowdStrike Falcon® Intelligence page**.
- **Want the insights on the latest adversary tactics, techniques, and procedures (TTPs)?** Download the *CrowdStrike 2021 Global Threat Report.*
