# APT28

[ / ˈeɪ.piː.tiː ˈtwɛnti eɪt / ]

APT28 (Fancy Bear) is a Russian GRU-linked APT active since 2004, conducting high-risk cyber espionage, election interference, and influence operations. It targets government, defense, military, and critical infrastructure in Europe, North America, and globally, using phishing, supply chain attacks, zero-day exploits, and disinformation.

## IDENTITY

| | |
|---|---|
| Attribution | : Russian military intelligence (GRU, Unit 26165). |
| Active Since | : At least 2004. |
| Aliases | : Fancy Bear, Sofacy, STRONTIUM, Sednit, Tsar Team, Pawn Storm. |
| Motivation | : Political and military cyber espionage, election interference, and influence operations in support of Russian state objectives. |

## TTPs

| | |
|---|---|
| Initial Access | : Spear-phishing campaigns, exploitation of zero-day vulnerabilities, and credential theft. |
| Persistence | : Custom implants, scheduled tasks, compromised credentials, and backdoors for long-term access. |
| Command & Control (C2) | : Uses custom malware families, compromised infrastructure, and dynamic DNS for covert communications. |
| Malware & Tools | : X-Agent, Sednit, Sofacy implants, Zebrocy, Chopstick, GameFish, and exploitation of Microsoft Outlook vulnerabilities. |
| Techniques | : Credential harvesting, lateral movement, supply chain compromise, data exfiltration, and coordinated disinformation campaigns. |

## TARGET PROFILE

| | |
|---|---|
| Target Sectors | : Government, defense, military, transportation, NGOs, critical infrastructure, and media. |
| Geographies Targeted | : Primarily Europe (NATO, Ukraine, EU states), North America, and international organizations opposing Russian interests. |

## THREAT ASSESSMENT

| | |
|---|---|
| Risk Level | : Very High – highly capable and persistent global espionage actor. |
| Most Recent Activity | : Active during 2024–2025, exploiting Microsoft Outlook vulnerabilities to target Czech, German, and NATO government institutions. |
| Evolution | : Transitioned from simple credential theft and phishing campaigns to advanced operations involving zero-day exploitation, large-scale influence campaigns, and critical infrastructure targeting. |

## NOTABLE OPERATIONS

- **2016:** Interference in the U.S. presidential election through hacking and leaking operations.
- **2017:** Targeted French election campaigns and German political organizations.
- **2018:** Conducted cyber espionage against organizations investigating Russia's state-sponsored doping program.
- **2020:** Phishing and intrusion attempts against COVID-19 vaccine research facilities in Europe and North America.
- **2022:** Aggressive campaigns supporting Russia's invasion of Ukraine, targeting NATO defense ministries and Ukrainian infrastructure.
- **2023:** Exploited vulnerabilities in email platforms for espionage against European governments.
- **2024–2025:** Used Outlook exploits to target NATO members and EU government agencies, continuing long-term espionage campaigns.