GROUPS
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
Axiom
BackdoorDiplomacy
BlackOasis
BlackTech
Blue Mockingbird
Bouncing Golf
BRONZE BUTLER
Carbanak
Chimera
Cleaver
Cobalt Group

Home > Groups > APT28

APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.[1][2] This group has been active since at least 2004.[3][4][5][6][7][8][9][10][11][12][13]

APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. [5] In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.[14] Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

ID: G0007

ⓘ Associated Groups: SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

Contributors: Sébastien Ruel, CGI; Drew Church, Splunk; Emily Ratliff, IBM; Richard Gold, Digital Shadows

Version: 3.2

Created: 31 May 2017

Last Modified: 18 October 2021

Version Permalink

Associated Group Descriptions

Name	Description
SNAKEMACKEREL	[15]
Swallowtail	[12]
Group 74	[16]
Sednit	This designation has been used in reporting both to refer to the threat group and its associated malware JHUHUGIT.[8][7][17][4]