

Groups Detected

Sandworm Team (G0034): 10.04%

[Sandworm Team](<https://attack.mitre.org/groups/G0034>) is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) This group has been active since at least 2009.(Citation: iSIGHT Sandworm 2014)(Citation: CrowdStrike VODOO BEAR)(Citation: USDOJ Sandworm Feb 2020)(Citation: NCSC Sandworm Feb 2020) In October 2020, the US indicted six GRU Unit 74455 officers associated with [Sandworm Team] (<https://attack.mitre.org/groups/G0034>) for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide [NotPetya] (<https://attack.mitre.org/software/S0368>) attack, targeting of the 2017 French presidential campaign, the 2018 [Olympic Destroyer](<https://attack.mitre.org/software/S0365>) attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019.(Citation: US District Court Indictment GRU Unit 74455 October 2020)(Citation: UK NCSC Olympic Attacks October 2020) Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as [APT28](<https://attack.mitre.org/groups/G0007>).(Citation: US District Court Indictment GRU Oct 2018)

Aliases: Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Seashell Blizzard, FROZENBARENTS

Domains: enterprise-attack, ics-attack, mobile-attack

x_mitre_version: 4.0

Wizard Spider (G0102): 3.69%

[Wizard Spider](<https://attack.mitre.org/groups/G0102>) is a Russia-based financially motivated threat group originally known for the creation and deployment of [TrickBot](<https://attack.mitre.org/software/S0266>) since at least 2016.

[Wizard Spider](<https://attack.mitre.org/groups/G0102>) possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals.(Citation: CrowdStrike Ryuk January 2019)(Citation: DHS/CISA Ransomware Targeting Healthcare October 2020)(Citation: CrowdStrike Wizard Spider October 2020)

Aliases: Wizard Spider, UNC1878, TEMP.MixMaster, Grim Spider, FIN12, GOLD BLACKBURN, ITG23, Periwinkle Tempest, DEV-0193

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0

Dragonfly (G0035): 3.69%

[Dragonfly](<https://attack.mitre.org/groups/G0035>) is a cyber espionage group that has been attributed to Russia's Federal Security Service (FSB) Center 16.(Citation: DOJ Russia Targeting Critical Infrastructure March 2022) (Citation: UK GOV FSB Factsheet April 2022) Active since at least 2010, [Dragonfly]

(<https://attack.mitre.org/groups/G0035>) has targeted defense and aviation companies, government entities, companies related to industrial control systems, and critical infrastructure sectors worldwide through supply chain, spearphishing, and drive-by compromise attacks.(Citation: Symantec Dragonfly)(Citation: Secureworks IRON LIBERTY July 2019)(Citation: Symantec Dragonfly Sept 2017)(Citation: Fortune Dragonfly 2.0 Sept 2017)(Citation: Gigamon Berserk Bear October 2021)(Citation: CISA AA20-296A Berserk Bear December 2020)(Citation: Symantec Dragonfly 2.0 October 2017)

Aliases: Dragonfly, TEMP.Isotope, DYMALLOY, Berserk Bear, TG-4192, Crouching Yeti, IRON LIBERTY, Energetic Bear, Ghost Blizzard, BROMINE

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0

OilRig (G0049): 3.69%

[OilRig](<https://attack.mitre.org/groups/G0049>) is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. The group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.(Citation: FireEye APT34 Dec 2017)(Citation: Palo Alto OilRig April 2017)(Citation: ClearSky OilRig Jan 2017)(Citation: Palo Alto OilRig May 2016)(Citation: Palo Alto OilRig Oct 2016)(Citation: Unit42 OilRig Playbook 2023)(Citation: Unit 42 QUADAGENT July 2018)

Aliases: OilRig, COBALT GYPSY, IRN2, APT34, Helix Kitten, Evasive Serpens, Hazel Sandstorm, EUROPIUM

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0

APT29 (G0016): 3.69%

[APT29](<https://attack.mitre.org/groups/G0016>) is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).(Citation: White House Imposing Costs RU Gov April 2021)(Citation: UK Gov Malign RIS Activity April 2021) They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. [APT29](<https://attack.mitre.org/groups/G0016>) reportedly compromised the Democratic National Committee starting in the summer of 2015.(Citation: F-Secure The Dukes)(Citation: GRIZZLY STEPPE JAR)(Citation: CrowdStrike DNC June 2016)(Citation: UK Gov UK Exposes Russia SolarWinds April 2021) In April 2021, the US and UK governments attributed the [SolarWinds Compromise] (<https://attack.mitre.org/campaigns/C0024>) to the SVR; public statements included citations to [APT29] (<https://attack.mitre.org/groups/G0016>), Cozy Bear, and The Dukes.(Citation: NSA Joint Advisory SVR SolarWinds April 2021)(Citation: UK NSCS Russia SolarWinds April 2021) Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.(Citation: FireEye SUNBURST Backdoor December 2020)(Citation: MSTIC NOBELIUM Mar 2021)(Citation: CrowdStrike SUNSPOT Implant January 2021)(Citation: Volexity SolarWinds)(Citation: Cybersecurity Advisory SVR TTP May 2021)(Citation: Unit 42 SolarStorm December 2020)

Aliases: APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTIRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune, UNC3524, Midnight Blizzard

Domains: enterprise-attack

x_mitre_version: 6.0