Threat Agents/Groups Detected

For selected Attack Patterns

Direct (attack-pattern--c5960919-9111-4243-a5e0-ea912bea59d5) (AML.T0051.000)
Modify Controller Tasking (attack-pattern--09a61657-46e1-439e-b3ed-3e4556a78243) (T0821)
Command-Line Interface (attack-pattern--24a9253e-8948-4c98-b751-8e2aee53127c) (T0807)
Obtain Capabilities (attack-pattern--6b015680-e5f2-4f11-9fe1-74472713cb19) (AML.T0016)

Sandworm Team (G0034): 50.0%

[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 VOODOO 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)

stix id: intrusion-set--381fcf73-60f6-4ab2-9991-6af3cbc35192

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

TEMP.Veles (G0088): 50.0%

[TEMP.Veles](https://attack.mitre.org/groups/G0088) is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing [TRITON](https://attack.mitre.org/software/S0609), a malware framework designed to manipulate industrial safety systems.(Citation: FireEye TRITON 2019)(Citation: FireEye TEMP.Veles 2018)(Citation: FireEye TEMP.Veles JSON April 2019)

stix id: intrusion-set--9538b1a4-4120-4e2d-bf59-3b11fcab05a4

Aliases: TEMP.Veles, XENOTIME

Domains: enterprise-attack, ics-attack

x_mitre_version: 1.4