Threat Agents/Groups Detected

For selected Attack Patterns

Valid Accounts (attack-pattern--cd2c76a4-5e23-4ca5-9c40-d5e0604f7101) (T0859)
Block Reporting Message (attack-pattern--3f1f4ccb-9be2-4ff8-8f69-dd972221169b) (T0804)
Engineering Workstation Compromise (attack-pattern--d614a9cf-18eb-4800-81e4-ab8ddf0baa73) (T0818)
Windows Remote Management (attack-pattern--c3bce4f4-9795-46c6-976e-8676300bbc39) (T1028)
Project File Infection (attack-pattern--e72425f8-9ae6-41d3-bfdb-e1b865e60722) (T0873)
Create Proxy ML dataProvider (attack-pattern--4214fc86-5feb-43b5-8ca3-a8f89057470d) (AML.T0005)
GPU Hardware (attack-pattern--680481cb-7c41-48e4-97aa-8e0dd40eb9e7) (AML.T0010.000)
Binary Padding (attack-pattern--5bfccc3f-2326-4112-86cc-c1ece9d8a2b5) (T1027.001)

Sandworm Team (G0034): 16.26%

[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

OilRig (G0049): 5.98%

[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)

stix id: intrusion-set--4ca1929c-7d64-4aab-b849-badbfc0c760d

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

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0

TEMP.Veles (G0088): 5.98%

[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

ALLANITE (G1000): 5.98%

[ALLANITE](https://attack.mitre.org/groups/G1000) is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within the United States and United Kingdom. The group's tactics and techniques are reportedly similar to [Dragonfly](https://attack.mitre.org/groups/G0035), although [ALLANITE](https://attack.mitre.org/groups/G1000)s technical capabilities have not exhibited disruptive or destructive abilities. It has been suggested that the group maintains a presence in ICS for the purpose of gaining understanding of processes and to maintain persistence. (Citation: Dragos)

stix id: intrusion-set--190242d7-73fc-4738-af68-20162f7a5aae

Aliases: ALLANITE, Palmetto Fusion

Domains: ics-attack

x_mitre_version: 1.0

FIN7 (G0046): 5.98%

[FIN7](https://attack.mitre.org/groups/G0046) is a financially-motivated threat group that has been active since 2013. [FIN7](https://attack.mitre.org/groups/G0046) has primarily targeted the retail, restaurant, hospitality, software, consulting, financial services, medical equipment, cloud services, media, food and beverage, transportation, and utilities industries in the U.S. A portion of [FIN7](https://attack.mitre.org/groups/G0046) was run out of a front company called Combi Security and often used point-of-sale malware for targeting efforts. Since 2020, [FIN7](https://attack.mitre.org/groups/G0046) shifted operations to a big game hunting (BGH) approach including use of [REvil](https://attack.mitre.org/software/S0496) ransomware and their own Ransomware as a Service (RaaS), Darkside. FIN7 may be linked to the [Carbanak](https://attack.mitre.org/groups/G0008) Group, but there appears to be several groups using [Carbanak](https://attack.mitre.org/software/S0030) malware and are therefore tracked separately.(Citation: FireEye FIN7 March 2017)(Citation: FireEye FIN7 April 2017)(Citation: FireEye CARBANAK June 2017)(Citation: FireEye FIN7 Aug 2018)(Citation: CrowdStrike Carbon Spider August 2021)(Citation: Mandiant FIN7 Apr 2022)

stix id: intrusion-set--3753cc21-2dae-4dfb-8481-d004e74502cc

Aliases: FIN7, GOLD NIAGARA, ITG14, Carbon Spider, ELBRUS, Sangria Tempest

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0