Threat Agents/Groups Detected

For selected Attack Patterns

Scheduled Task (attack-pattern--005a06c6-14bf-4118-afa0-ebcd8aebb0c9) (T1053.005)
Scheduled Task (attack-pattern--005a06c6-14bf-4118-afa0-ebcd8aebb0c9) (T1053.005)
Remote Desktop Protocol (attack-pattern--eb062747-2193-45de-8fa2-e62549c37ddf) (T1021.001)

Wizard Spider (G0102): 3.06%

[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 aresenal 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)

stix id: intrusion-set--dd2d9ca6-505b-4860-a604-233685b802c7

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

FIN7 (G0046): 3.06%

[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

Dragonfly (G0035): 3.06%

[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)

stix id: intrusion-set--1c63d4ec-0a75-4daa-b1df-0d11af3d3cc1

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): 3.06%

[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

Fox Kitten (G0117): 3.06%

[Fox Kitten](https://attack.mitre.org/groups/G0117) is threat actor with a suspected nexus to the Iranian government that has been active since at least 2017 against entities in the Middle East, North Africa, Europe, Australia, and North America. [Fox Kitten] (https://attack.mitre.org/groups/G0117) has targeted multiple industrial verticals including oil and gas, technology, government, defense, healthcare, manufacturing, and engineering. (Citation: ClearkSky Fox Kitten February 2020)(Citation: CrowdStrike PIONEER KITTEN August 2020)(Citation: Dragos PARISITE)(Citation: ClearSky Pay2Kitten December 2020)

stix id: intrusion-set--c21dd6f1-1364-4a70-a1f7-783080ec34ee

Aliases: Fox Kitten, UNC757, Parisite, Pioneer Kitten, RUBIDIUM, Lemon Sandstorm

Domains: enterprise-attack

x_mitre_version: 2.0