Groups Detected

For selected Attack Patterns

Acquire Infrastructure (attack-pattern--0458aab9-ad42-4eac-9e22-706a95bafee2) (T1583)
Compromise Software Dependencies and Development Tools (attack-pattern--191cc6af-1bb2-4344-ab5f-28e496638720) (T1195.001)
Windows Management Instrumentation (attack-pattern--01a5a209-b94c-450b-b7f9-946497d91055) (T1047)
Socket Filters (attack-pattern--005cc321-08ce-4d17-b1ea-cb5275926520) (T1205.002)
Indicator Removal from Tools (attack-pattern--00d0b012-8a03-410e-95de-5826bf542de6) (T1066)
Archive via Utility (attack-pattern--00f90846-cbd1-4fc5-9233-df5c2bf2a662) (T1560.001)
VNC (attack-pattern--01327cde-66c4-4123-bf34-5f258d59457b) (T1021.005)

Sandworm Team (G0034): 3.29%

[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)

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): 3.29%

[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)

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): 3.29%

[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)

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

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0

Lazarus Group (G0032): 3.29%

[Lazarus Group](https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.(Citation: US-CERT HIDDEN COBRA June 2017) (Citation: Treasury North Korean Cyber Groups September 2019) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](https://attack.mitre.org/groups/G0032) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.(Citation: Novetta Blockbuster) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group](https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups, such as [Andariel](https://attack.mitre.org/groups/G0138), [APT37](https://attack.mitre.org/groups/G0067), [APT38](https://attack.mitre.org/groups/G0082), and [Kimsuky](https://attack.mitre.org/groups/G0094).

Aliases: Lazarus Group, Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Diamond Sleet

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0

Earth Lusca (G1006): 3.29%

[Earth Lusca](https://attack.mitre.org/groups/G1006) is a suspected China-based cyber espionage group that has been active since at least April 2019. [Earth Lusca](https://attack.mitre.org/groups/G1006) has targeted organizations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some [Earth Lusca](https://attack.mitre.org/groups/G1006) operations may be financially motivated.(Citation: TrendMicro EarthLusca 2022) [Earth Lusca](https://attack.mitre.org/groups/G1006) has used malware commonly used by other Chinese threat groups, including [APT41](https://attack.mitre.org/groups/G0096) and the [Winnti Group](https://attack.mitre.org/groups/G0044) cluster, however security researchers assess [Earth Lusca](https://attack.mitre.org/groups/G1006)'s techniques and infrastructure are separate.(Citation: TrendMicro EarthLusca 2022)

Aliases: Earth Lusca, TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Domains: enterprise-attack, mobile-attack

x_mitre_version: 2.0