# APT 33, Elfin, Magnallium - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:46:58 UTC



## APT group: APT 33, Elfin, Magnallium

| | |
|---|---|
| Names | APT 33 *(Mandiant)*<br>Elfin *(Symantec)*<br>Magnallium *(Dragos)*<br>Holmium *(Microsoft)*<br>ATK 35 *(Thales)*<br>Refined Kitten *(CrowdStrike)*<br>TA451 *(Proofpoint)*<br>Cobalt Trinity *(SecureWorks)*<br>Peach Sandstorm *(Microsoft)*<br>Yellow Orc *(PWC)*<br>Curious Serpens *(Palo Alto)*<br>G0064 *(MITRE)* |
| Country | Iran |
| Sponsor | State-sponsored, Iranian Islamic Revolutionary Guard Corps (IRGC) |
| Motivation | Information theft and espionage, Sabotage and destruction |
| First seen | 2013 |
| Description | (FireEye) When discussing suspected Middle Eastern hacker groups with destructive capabilities, many automatically think of the suspected Iranian group that previously used SHAMOON – aka Disttrack – to target organizations in the Persian Gulf. However, over the past few years, we have been tracking a separate, less widely known suspected Iranian group with potential destructive capabilities, whom we call APT33. Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government.<br><br>APT33 has targeted organizations – spanning multiple industries – headquartered in the United States, Saudi Arabia and South Korea. APT33 has shown particular interest in organizations in the aviation sector involved in both military and |

| | | |
|---|---|---|
| | commercial capacities, as well as organizations in the energy sector with ties to petrochemical production.<br><br>APT 33 seems to be closely related to OilRig, APT 34, Helix Kitten, Chrysene since at least 2017. | |
| Observed | Sectors: Aviation, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Manufacturing, Media, Oil and gas, Petrochemical, Telecommunications and others.<br>Countries: Iran, Iraq, Israel, Saudi Arabia, South Korea, UAE, UK, USA. | |
| Tools used | AutoIt backdoor, DarkComet, DistTrack, EmpireProject, FalseFont, Filerase, JuicyPotato, LaZagne, Mimikatz, NanoCore RAT, NetWire RC, PoshC2, PowerBand, PowerSploit, POWERTON, PsList, PupyRAT, QuasarRAT, RemcosRAT, Ruler, SHAPESHIFT, StoneDrill, Tickler, TURNEDUP, Living off the Land. | |
| Operations performed | Mar 2019 | Attacks on Multiple Organizations in Saudi Arabia and U.S.<br>The Elfin espionage group (aka APT33) has remained highly active over the past three years, attacking at least 50 organizations in Saudi Arabia, the United States, and a range of other countries.<br><https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage> |
| | Jul 2019 | US Cyber Command has issued an alert via Twitter today about threat actors abusing an Outlook vulnerability to plant malware on government networks.<br>The vulnerability is CVE-2017-11774, a security bug that Microsoft patched in Outlook in the October 2017 Patch Tuesday.<br><https://www.zdnet.com/article/us-cyber-command-issues-alert-about-hackers-exploiting-outlook-vulnerability/> |
| | Nov 2019 | More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting<br><https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/> |
| | Feb 2023 | Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets<br><https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/> |

| | | |
|---|---|---|
| | Nov 2023 | Microsoft: Hackers target defense firms with new FalseFont malware <https://www.bleepingcomputer.com/news/security/microsoft-hackers-target-defense-firms-with-new-falsefont-malware/> |
| | Apr 2024 | Peach Sandstorm deploys new custom Tickler malware in long-running intelligence gathering operations <https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/> |
| Information | <https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html><br><https://en.wikipedia.org/wiki/Elfin_Team> | |
| MITRE ATT&CK | <https://attack.mitre.org/groups/G0064/> | |
| Playbook | <https://pan-unit42.github.io/playbook_viewer/?pb=oilrig> | |

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

---

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=958e1f46-a2b6-4beb-8cb0-ddc90c08368e