# Gorgon Group - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:45:48 UTC

## APT group: Gorgon Group

| | | |
|---|---|---|
| Names | Gorgon Group *(Palo Alto)*<br>Subaat *(Palo Alto)*<br>ATK 92 *(Thales)*<br>TAG-CR5 *(Recorded Future)*<br>Pasty Draco *(Palo Alto)*<br>G0078 *(MITRE)* | |
| Country | Pakistan | |
| Sponsor | State-sponsored | |
| Motivation | Information theft and espionage | |
| First seen | 2017 | |
| Description | Gorgon Group is a threat group consisting of members who are suspected to be Pakistan-based or have other connections to Pakistan. The group has performed a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States.<br><br>Gorgon Group may be related to Transparent Tribe, APT 36 and may be responsible for the Aggah activity. | |
| Observed | Sectors: Government, Manufacturing.<br>Countries: Russia, Spain, Switzerland, UK, USA. | |
| Tools used | Agent Tesla, Crimson RAT, LokiBot, NanoCore RAT, NetWire RC, njRAT, QuasarRAT, RemcosRAT, RevengeRAT, Living off the Land. | |
| Operations performed | Jul 2017 | Small wave of phishing emails targeting a US-based government organization.<br>Within the 43 emails we observed, we found that three unique files were delivered, which consisted of two RTFs and a Microsoft Excel file. Both RTFs exploited CVE-2012-0158 and acted as downloaders to ultimately deliver the QuasarRAT malware family. The downloaders made use of the same shellcode, with minor variances witnessed |

| | | |
|---|---|---|
| | | between them. Additionally, the RTFs made use of heavy obfuscation within the documents themselves, making it more difficult to extract the embedded shellcode. <https://unit42.paloaltonetworks.com/unit42-tracking-subaat-targeted-phishing-attacks-point-leader-threat-actors-repository/> |
| | Feb 2018 | In addition to the numerous targeted attacks, Unit 42 discovered that the group also performed a litany of attacks and operations around the globe, involving both criminal as well as targeted attacks. Starting in February 2018, Palo Alto Networks Unit 42 identified a campaign of attacks performed by members of Gorgon Group targeting governmental organizations in the United Kingdom, Spain, Russia, and the United States. Additionally, during that time, members of Gorgon Group were also performing criminal operations against targets across the globe, often using shared infrastructure with their targeted attack operations. <https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/> |
| | Apr 2020 | Gorgon APT targeting MSME sector in India <https://www.seqrite.com/blog/gorgon-apt-targeting-msme-sector-in-india/> |
| | Jul 2020 | Advance Campaign Targeting Manufacturing and Export Sectors in India <https://www.seqrite.com/blog/advance-campaign-targeting-manufacturing-and-export-sectors-in-india/>> |
| MITRE ATT&CK | <https://attack.mitre.org/groups/G0078/> | |
| Playbook | <https://pan-unit42.github.io/playbook_viewer/?pb=pastydraco> | |

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

---