# Tortoiseshell, Imperial Kitten - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:34:36 UTC



## APT group: Tortoiseshell, Imperial Kitten

| | |
|---|---|
| Names | Tortoiseshell *(Symantec)*<br>Imperial Kitten *(CrowdStrike)*<br>TA456 *(Proofpoint)*<br>Curium *(Microsoft)*<br>Marcella Flores *(self given)*<br>Houseblend *(?)*<br>Crimson Sandstorm *(Microsoft)*<br>Cuboid Sandstorm *(Microsoft)*<br>Yellow Liderc *(PWC)*<br>Devious Serpens *(Palo Alto)*<br>Cobalt Fireside *(SecureWorks)* |
| Country | Iran |
| Sponsor | State-sponsored, Islamic Revolutionary Guard Corps (IRGC) |
| Motivation | Information theft and espionage |
| First seen | 2018 |
| Description | (Symantec) A previously undocumented attack group is using both custom and off-the-shelf malware to target IT providers in Saudi Arabia in what appear to be supply chain attacks with the end goal of compromising the IT providers' customers.<br><br>The group, which we are calling Tortoiseshell, has been active since at least July 2018. Symantec has identified a total of 11 organizations hit by the group, the majority of which are based in Saudi Arabia. In at least two organizations, evidence suggests that the attackers gained domain admin-level access.<br><br>Overlap has been found with Magic Hound's Subgroup: TA455, Smoke Sandstorm. |

| | | |
|---|---|---|
| Observed | Sectors: Aerospace, Defense, IT, Shipping and Logistics, Maritime and Shipbuilding.<br>Countries: Saudi Arabia, UAE, USA and Middle East. | |
| Tools used | get-logon-history.ps1, IMAPLoader, Infostealer, LEMPO, liderc, SysKit. | |
| Operations performed | Sep 2019 | Cisco Talos recently discovered a threat actor attempting to take advantage of Americans who may be seeking a job, especially military veterans.<br><https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html> |
| | Nov 2020 | I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona<br><https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media> |
| | 2022 | Yellow Liderc ships its scripts and delivers IMAPLoader malware<br><https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html> |
| | May 2023 | Operation “Fata Morgana”<br>Fata Morgana: Watering hole attack on shipping and logistics websites<br><https://www.clearskysec.com/wp-content/uploads/2023/05/Fata-Morgana-Israeli-Websites-Infected-by-Iranian-Group-1.8.pdf> |
| | Oct 2023 | IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations<br><https://www.crowdstrike.com/blog/imperial-kitten-deploys-novel-malware-families/> |
| Counter operations | Jul 2021 | Taking Action Against Hackers in Iran<br><https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/> |
| Information | <https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain><br><https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/> | |

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format