


Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:44:17 UTC

[Home](#) > [List all groups](#) > Tracer Kitten

APT group: Tracer Kitten

Names	Tracer Kitten (<i>CrowdStrike</i>)
Country	 Iran
Motivation	Information theft and espionage
First seen	2020
Description	<p>(CrowdStrike) In April 2020, OverWatch discovered Iran-based adversary TRACER KITTEN conducting malicious interactive activity against multiple hosts at a telecommunications company in the Europe, Middle East and Africa (EMEA) region. The actor was found operating under valid user accounts, using custom backdoors in combination with SSH tunnels for C2. The adversary leveraged their foothold to conduct a variety of reconnaissance activities, undertake credential harvesting and prepare for data exfiltration.</p> <p>Telecommunications is currently the third most frequently targeted vertical. This industry still remains firmly within the crosshairs for targeted attacks, the motivations of which are likely associated with espionage and data theft objectives.</p>
Observed	Sectors: Telecommunications . Countries: Europe, Middle East and Africa.
Tools used	
Information	< https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf >

Last change to this card: 31 December 2022

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=cabd014b-5087-4ff8-b0c8-74202e82fa1d>