CopyKittens, Slayer Kitten - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:45:12 UTC

APT group: CopyKittens, Slayer Kitten

Names	CopyKittens *(Trend Micro)* Slayer Kitten *(CrowdStrike)* G0052 *(MITRE)*	
Country	Iran	
Motivation	Information theft and espionage	
First seen	2013	
Description	CopyKittens is an Iranian cyberespionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip.	
Observed	Sectors: Defense, Education, Government, IT, Media. Countries: Germany, Israel, Jordan, Saudi Arabia, Turkey, USA.	
Tools used	Cobalt Strike, EmpireProject, Matryoshka RAT, TDTESS, Vminst, ZPP.	
Operations performed	2013	Operation “Wilted Tulip” In this report, Trend Micro and ClearSky expose a vast espionage apparatus spanning the entire time the group has been active. It includes recent incidents as well as older ones that have not been publicly reported; new malware; exploitation, delivery and command and control infrastructure; and the group’s modus operandi. We dubbed this activity Operation Wilted Tulip. <https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf>
	2015	CopyKittens has conducted at least three waves of cyber-attacks in the past year. In each of the attacks the infection method was almost identical and included an extraordinary number of stages used to avoid detection. As with other common threat actors, the group relies on social

		engineering methods to deceive its targets prior to infection. <https://s3-eu-west-1.amazonaws.com/minervaresearchpublic/CopyKittens/CopyKittens.pdf>
	Jan 2017	Breach of the Israeli newspaper Jerusalem Post As part of our monitoring of Iranian threat agents activities, we have detected that since October 2016 and until the end of January 2017, the Jerusalem Post, as well as multiple other Israeli websites and one website in the Palestinian Authority were compromised by Iranian threat agent CopyKittens. <https://www.clearskysec.com/copykitten-jpost/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0052/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
