Scarlet Mimic - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:34:58 UTC

APT group: Scarlet Mimic

Names	Scarlet Mimic *(Palo Alto)* Golfing Taurus *(Palo Alto)* G0029 *(MITRE)*
Country	China
Motivation	Information theft and espionage
First seen	2015

Description	Scarlet Mimic is a threat group that has targeted minority rights activists. This group has not been directly linked to a government source, but the group's motivations appear to overlap with those of the Chinese government. While there is some overlap between IP addresses used by Scarlet Mimic and Putter Panda, APT 2, it has not been concluded that the groups are the same. (Palo Alto) The attacks began over four years ago and their targeting pattern suggests that this adversary's primary mission is to gather information about minority rights activists. We do not have evidence directly linking these attacks to a government source, but the information derived from these activities supports an assessment that a group or groups with motivations similar to the stated position of the Chinese government in relation to these targets is involved. The attacks we attribute to Scarlet Mimic have primarily targeted Uyghur and Tibetan activists as well as those who are interested in their causes. Both the Tibetan community and the Uyghurs, a Turkic Muslim minority residing primarily in northwest China, have been targets of multiple sophisticated attacks in the past decade. Both also have history of strained relationships with the government of the People's Republic of China (PRC), though we do not have evidence that links Scarlet Mimic attacks to the PRC. Scarlet Mimic attacks have also been identified against government organizations in Russia and India, who are responsible for tracking activist and terrorist activities. While we do not know the precise target of each of the Scarlet Mimic attacks, many of them align to the patterns described above.	
Observed	Countries: Tibetan and Uyghur activists as well as those who are interested in their causes.	
Tools used	BrutishCommand, CallMe, CrypticConvo, Elirks, FakeFish, FakeHighFive, FakeM, FullThrottle, HTran, MobileOrder, PiggyBack, Psylo, RaidBase, SkiBoot, SubtractThis.	
Operations performed	Aug 2022	CPR analyzes A 7-year mobile surveillance campaign targeting largest minority in China <https://blog.checkpoint.com/2022/09/22/cpr-analyzes-a-7-year-mobile-surveillance-campaign-targeting-largest-minority-in-china/>
Information	<https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0029/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=golfing-taurus>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
