LevelBlue - Open Threat Exchange

By AlienVault

Archived: 2026-04-05 14:40:45 UTC

CVE: 6 | **FileHash-MD5:** 2 | **FileHash-SHA256:** 85 | **YARA:** 1 | **Hostname:** 71

Over the past seven months, Unit 42 has been investigating a series of attacks we attribute to a group we have code named “Scarlet Mimic.” 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.
