Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:40:03 UTC

APT group: Group5

Names	Group5 *(Citizen Lab)* G0043 *(MITRE)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2015
Description	(SecurityWeek) A threat actor using Iranian-language tools, Iranian hosting companies, operating from the Iranian IP space at times was observed targeting the Syrian opposition in an elaborately staged malware operation, Citizen Lab researchers reveal. The operation was first noticed in late 2015, when a member of the Syrian opposition flagged a suspicious email containing a PowerPoint slideshow, which led researchers to a watering hole website with malicious programs, malicious PowerPoint files, and Android malware. The threat actor was targeting Windows and Android devices of well-connected individuals in the Syrian opposition, researchers discovered. They called the actor Group5, because it targets Syrian opposition after regime-linked malware groups, the Syrian Electronic Army (SEA), Deadeye Jackal, ISIS (also known as the Islamic State or ISIL), and a group linked to Lebanon did the same in the past.
Observed	Countries: Syria.
Tools used	DroidJack, NanoCore RAT, njRAT.
Information	<https://www.securityweek.com/iranian-actor-group5-targeting-syrian-opposition>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0043/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format