Subgroup: DEV-0270, Nemesis Kitten - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:06:31 UTC

APT group: Subgroup: DEV-0270, Nemesis Kitten

Names	DEV-0270 *(Microsoft)* Nemesis Kitten *(CrowdStrike)* DireFate *(BAE Systems)* Yellow Dev 23 *(PWC)* Yellow Dev 24 *(PWC)* Lord Nemesis *(OP Innovate)*	
Country	Iran	
Motivation	Financial gain	
First seen	2022	
Description	A subgroup of Magic Hound, APT 35, Cobalt Illusion, Charming Kitten. (Microsoft) Microsoft threat intelligence teams have been tracking multiple ransomware campaigns and have tied these attacks to DEV-0270, also known as Nemesis Kitten, a sub-group of Iranian actor PHOSPHORUS. Microsoft assesses with moderate confidence that DEV-0270 conducts malicious network operations, including widespread vulnerability scanning, on behalf of the government of Iran. However, judging from their geographic and sectoral targeting, which often lacked a strategic value for the regime, we assess with low confidence that some of DEV-0270's ransomware attacks are a form of moonlighting for personal or company-specific revenue generation.	
Observed		
Tools used	Impacket, WmiExec, Living off the Land.	
Operations performed	Nov 2023	Lord Nemesis Strikes: Supply Chain Attack on the Israeli Academic Sector <https://op-c.net/blog/lord-nemesis-strikes-supply-chain-attack-on-the-israeli-academic-sector/>

Information	<https://www.microsoft.com/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/>

Last change to this card: 10 March 2024

Download this actor card in PDF or JSON format
