Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:21:57 UTC

APT group: Polonium

Names	Polonium *(Microsft)* Plaid Rain *(Microsoft)* Incendiary Jackal *(CrowdStrike)* G1005 *(MITRE)*	
Country	Lebanon	
Motivation	Information theft and espionage	
First seen	2022	
Description	(Microsoft) MSTIC assesses with high confidence that POLONIUM represents an operational group based in Lebanon. We also assess with moderate confidence that the observed activity was coordinated with other actors affiliated with Iran's Ministry of Intelligence and Security (MOIS), based primarily on victim overlap and commonality of tools and techniques. Such collaboration or direction from Tehran would align with a string of revelations since late 2020 that the Government of Iran is using third parties to carry out cyber operations on their behalf, likely to enhance Iran's plausible deniability. POLONIUM has targeted or compromised more than 20 organizations based in Israel and one intergovernmental organization with operations in Lebanon over the past three months. This actor has deployed unique tools that abuse legitimate cloud services for command and control (C2) across most of their victims. POLONIUM was observed creating and using legitimate OneDrive accounts, then utilizing those accounts as C2 to execute part of their attack operation.	
Observed	Sectors: Engineering, Defense, IT, Manufacturing, Media, Telecommunications. Countries: Israel, Lebanon.	
Tools used	CreepyDrive, CreepySnail, DeepCreep, FlipCreep, MegaCreep, PapaCreep, TechnoCreep.	
Operations performed	Sep 2022	POLONIUM targets Israel with Creepy malware <https://www.welivesecurity.com/2022/10/11/polonium-targets-israel-creepy-malware/>

		<https://www.deepinstinct.com/blog/polonium-apt-group-uncovering-new-elements>
Information	<https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G1005/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
