Leafminer, Raspite - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:38:47 UTC

APT group: Leafminer, Raspite

Names	Leafminer *(Symantec)* Raspite *(Dragos)* Flash Kitten *(CrowdStrike)* G0077 *(MITRE)*
Country	Iran
Motivation	Information theft and espionage
First seen	2017
Description	(Symantec) Symantec has uncovered the operations of a threat actor named Leafminer that is targeting a broad list of government organizations and business verticals in various regions in the Middle East since at least early 2017. The group tends to adapt publicly available techniques and tools for their attacks and experiments with published proof-of-concept exploits. Leafminer attempts to infiltrate target networks through various means of intrusion: watering hole websites, vulnerability scans of network services on the internet, and brute-force/dictionary login attempts. The actor's post-compromise toolkit suggests that the group is looking for email data, files, and database servers on compromised target systems. (Dragos) Analysis of Raspite tactics, techniques, and procedures (TTPs) indicate the group has been active in some form since early- to mid-2017. Raspite targeting includes entities in the US, Middle East, Europe, and East Asia. Operations against electric utility organizations appear limited to the US at this time. Raspite leverages strategic website compromise to gain initial access to target networks. Raspite uses the same methodology as Berserk Bear, Dragonfly 2.0 and Allanite in embedding a link to a resource to prompt an SMB connection, from which it harvests Windows credentials. The group then deploys install scripts for a malicious service to beacon back to Raspite –controlled infrastructure, allowing the adversary to remotely access the victim machine.

Observed	Sectors: Energy, Financial, Government, Transportation. Countries: Israel, Kuwait, Lebanon, USA and Europe and East Asia.
Tools used	Imecab, LaZagne, Mimikatz, PhpSpy, Sorgu.
Information	<https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east> <https://dragos.com/resource/raspite/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0077/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
