Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:07:24 UTC

APT group: Gallmaker

Names	Gallmaker *(Symantec)* G0084 *(MITRE)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2017
Description	(Symantec) Symantec researchers have uncovered a previously unknown attack group that is targeting government and military targets, including several overseas embassies of an Eastern European country, and military and defense targets in the Middle East. This group eschews custom malware and uses living off the land (LotL) tactics and publicly available hack tools to carry out activities that bear all the hallmarks of a cyber espionage campaign. The group, which we have given the name Gallmaker, has been operating since at least December 2017, with its most recent activity observed in June 2018.
Observed	Sectors: Defense, Embassies, Government. Countries: Eastern Europe and Middle East.
Tools used	Living off the Land.
Information	<https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0084/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format