Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:57:07 UTC

APT group: FIN5

Names	FIN5 *(FireEye)* G0053 *(MITRE)*
Country	[Unknown]
Motivation	Financial crime
First seen	2008
Description	FIN5 is a financially motivated threat group that has targeted personally identifiable information and payment card information. The group has been active since at least 2008 and has targeted the restaurant, gaming, and hotel industries. The group is made up of actors who likely speak Russian. (DarkReading) No 0days. No spear-phishing, either: The cybercriminal group tied to numerous payment card breaches including Goodwill and best known by its so-called “RawPOS” malware employed legitimate user credentials to access its targets’ networks. Researchers at FireEye here today shared their recent findings on this prolific and long-running cybercrime gang that has been the subject of multiple Visa security alerts to merchants. The RawPOS memory scraper malware has been infecting the lodging industry in epidemic proportions over the past year, and is considered one of the first memory scrapers to target point-of-sale systems. FireEye has dubbed the cybercrime gang FIN5. “One of the most unique things about FIN5 is that in every intrusion we responded to where FIN5 has been active, legitimate access was identified. They had valid user credentials to remotely log into the network,” said Barry Vengerik, principal threat analyst at FireEye. “No sexy zero-days, no remote exploits – not even spear-phishing. They had credentials from somewhere.” FIN5, which earlier this year was profiled by researchers at Trend Micro and has been in action since at least 2008, uses real credentials from the victim organization’s virtual private network, Remote Desktop Protocol, Citrix, or VNC. Vengerik says the attackers got those credentials via third parties associated with the victims’ POS systems.
Observed	Sectors: Gaming, Hospitality.

Tools used	FLIPSIDE, pwdump, RawPOS, SDelete, Windows Credentials Editor.
Information	<https://www.darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0053/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
