

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:44:16 UTC

APT group: FIN10

Names	FIN10 (<i>FireEye</i>) G0051 (<i>MITRE</i>)
Country	[Unknown]
Motivation	Financial crime
First seen	2016
Description	<p>(FireEye) FireEye has observed multiple targeted intrusions occurring in North America — predominately in Canada — dating back to at least 2013 and continuing through at least 2016, in which the attacker(s) have compromised organizations' networks and sought to monetize this illicit access by exfiltrating sensitive data and extorting victim organizations. In some cases, when the extortion demand was not met, the attacker(s) destroyed production Windows systems by deleting critical operating system files and then shutting down the impacted systems. Based on near parallel TTPs used by the attacker(s) across these targeted intrusions, we believe these clusters of activity are linked to a single, previously unobserved actor or group that we have dubbed FIN10.</p>
Observed	Sectors: Casinos and Gambling , Mining . Countries: Canada , USA .
Tools used	EmpireProject , KOMPROGO .
Information	< https://www2.fireeye.com/rs/848-DID-242/images/rpt-fin10.pdf >
MITRE ATT&CK	< https://attack.mitre.org/groups/G0051/ >

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=32e3ffa7-e053-4841-a072-7f314eb1637c>