Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:23:16 UTC

APT group: FIN13

Names	FIN13 *(Mandiant)*
Country	[Unknown]
Motivation	Financial crime, Financial gain
First seen	2016
Description	(Mandiant) Since 2017, Mandiant has been tracking FIN13, an industrious and versatile financially motivated threat actor conducting long-term intrusions in Mexico with an activity timeframe stretching back as early as 2016. FIN13's operations have several noticeable differences from current cybercriminal data theft and ransomware extortion trends. Although their operations continue through the present day, in many ways FIN13's intrusions are like a time capsule of traditional financial cybercrime from days past. Instead of today's prevalent "smash and grab" ransomware groups, FIN13 takes their time to gather information to perform fraudulent money transfers. Rather than relying heavily on attack frameworks such as Cobalt Strike, the majority of FIN13 intrusions involve heavy use of custom passive backdoors and tools to lurk in environments for the long haul. Also see Elephant Beetle.
Observed	Countries: Mexico.
Tools used	BLUEAGAVE, BUSTEDPIPE, CLOSEWATCH, DRAWSTRING, GetUserSPNS.vbs, GoBot2, HOTLANE, JSPRAT, LATCHKEY, MAILSLOT, NIGHTJAR, nmap, PORTHOLE, PowerSploit, ProcDump, SHELLSWEEP, SIXPACK, SPINOFF, SWEARJAR, Tiny SHell.
Information	<https://www.mandiant.com/resources/fin13-cybercriminal-mexico>

Last change to this card: 25 January 2022

Download this actor card in PDF or JSON format
