Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:23:33 UTC

APT group: FIN12

Names	FIN12 *(Mandiant)*
Country	[Unknown]
Motivation	Financial crime, Financial gain
First seen	2018
Description	(Mandiant) Today, Mandiant Intelligence is releasing a comprehensive report detailing FIN12, an aggressive, financially motivated threat actor behind prolific ransomware attacks since at least October 2018. FIN12 is unique among many tracked ransomware-focused actors today because they do not typically engage in multi-faceted extortion and have disproportionately impacted the healthcare sector. They are also the first FIN actor that we are promoting who specializes in a specific phase of the attack lifecycle—ransomware deployment—while relying on other threat actors for gaining initial access to victims. This specialization reflects the current ransomware ecosystem, which is comprised of various loosely affiliated actors partnering together, but not exclusively with one another.
Observed	Sectors: Education, Financial, Healthcare, Manufacturing, Technology. Countries: Australia, Canada, Colombia, France, Indonesia, Ireland, Philippines, South Korea, Spain, UAE, UK, USA.
Tools used	BazarBackdoor, Cobalt Strike, TrickBot.
Information	<https://www.mandiant.com/resources/fin12-ransomware-intrusion-actor-pursuing-healthcare-targets> <https://www.mandiant.com/media/12596/download>

Last change to this card: 02 November 2021

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=b43cdd5b-3411-4c5f-9190-e8de49a747e1