

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:05:04 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool BLUESTEAL


Tool: BLUESTEAL

Names	BLUESTEAL
Category	Malware
Type	POS malware , Credential stealer
Description	In late 2018, Mandiant analysts observed FIN11 attempt to monetize their operations using the point-of-sale (POS) memory scraping tool BLUESTEAL.

Last change to this tool card: 20 October 2020

Download this tool card in [JSON](#) format

All groups using tool BLUESTEAL

Changed	Name	Country	Observed	
APT groups				
	FIN11	[Unknown]	2016-Mar 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=9b80b2af-9fcc-47d0-ab69-6bc0d8014f98>