Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:24:10 UTC

Tool: SPOONBEARD

Names	SPOONBEARD
Category	Malware
Type	Dropper
Description	(FireEye) In May 2019, a SPOONBEARD-packed SCRAPMINT sample was uploaded to VirusTotal. Based on several Mandiant incident response cases, we believe SCRAPMINT has been used by multiple actors to conduct POS malware operations including FIN6. Between August and December 2019, we identified SPOONBEARD samples that delivered AZORult or VIDAR credential theft malware. It is plausible that FIN11 used these credential stealers; however, both AZORult and VIDAR have been sold on underground forums and are used by multiple actors. In late 2019 and early 2020, we identified SPOONBEARD samples that delivered SLOWROLL and JESTBOT respectively. SLOWROLL is a backdoor associated with TEMP.TruthTeller (aka Silent Group) post-compromise activity.

Last change to this tool card: 20 October 2020

Download this tool card in JSON format

All groups using tool SPOONBEARD

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

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