Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:40:30 UTC

Tool: LOADOUT

Names	LOADOUT
Category	Malware
Type	Downloader
Description	(Mandiant) LOADOUT is an obfuscated VBScript-based downloader which harvests extensive information from the infected system. The harvested information is then sent to a command-and-control (C2) server. C2 server responses for LOADOUT infections delivered Griffon, a JavaScript-based downloader which retrieves additional JavaScript modules using HTTP or DNS and executes them in memory.
Information	<https://www.mandiant.com/resources/evolution-of-fin7>

Last change to this tool card: 05 April 2022

Download this tool card in JSON format

All groups using tool LOADOUT

Changed	Name	Country	Observed	
APT groups				
	FIN7		2013-Jul 2024	

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