Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:01:30 UTC

Tool: ROCKBOOT

Names	ROCKBOOT
Category	Malware
Type	Loader
Description	(FireEye) ROCKBOOT can access and write to the compromised system's hard disk drive beneath the operating system and file system to bypass the normal MBR boot sequence and execute malware prior to the host operating system being initialized. ROCKBOOT does not contain a malicious payload but relies on a secondary payload for malicious activities, which is specified at install time.
Information	<https://paper.bobylive.com/Security/APT_Report/APT-41.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0112/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool ROCKBOOT

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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