Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:28:04 UTC

Tool: Okrum

Names	Okrum
Category	Malware
Type	Backdoor, Exfiltration
Description	(ESET) The functionality of the Okrum backdoor is not unlike the other backdoors operated by the Ke3chang group The commands allow the attackers to download and upload files, execute binaries or run shell commands. The backdoor can also update itself to a newer version and can adjust the time it sleeps after each backdoor command.
Information	<https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0439/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.okrum>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Okrum

Changed	Name	Country	Observed	
APT groups				
	Ke3chang, Vixen Panda, APT 15, GREF, Playful Dragon		2010-Oct 2024	

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