Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:42:29 UTC

Tool: DEADEYE

Names	DEADEYE DEADEYE.EMBED DEADEYE.APPEND
Category	Malware
Type	Downloader
Description	(FireEye) Tracking APT41 activities over the past months, we observed multiple samples that shared two unique features: the use of RC5 encryption which we don't encounter often, and a unique string "f@Ukd!rCto R$.". We track these samples as DEADEYE. DEADEYE comes in multiple variants: • DEADEYE.DOWN has the capability to download additional payloads. • DEADEYE.APPEND has additional payloads appended to it. • DEADEYE.EXT loads payloads that are already present on the system.
Information	<https://www.fireeye.com/blog/threat-research/2019/10/lowkey-hunting-for-the-missing-volume-serial-id.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S1052>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool DEADEYE

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

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