Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:03:10 UTC

Tool: RegDuke

Names	RegDuke
Category	Malware
Type	Backdoor
Description	(ESET) A recovery first stage, which uses Dropbox as its C&C server. The main payload is encrypted on disk and the encryption key is stored in the Windows registry. It also relies on steganography as above.
Information	<https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0511/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool RegDuke

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

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