Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:59:08 UTC

Tool: reGeorg

Names	reGeorg
Category	Tools
Type	Backdoor, Tunneling
Description	The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.
Information	<https://github.com/sensepost/reGeorg> <https://sensepost.com/discover/tools/reGeorg/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1187>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.regeorg>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:regeorg>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool reGeorg

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	
	Cadet Blizzard		2020-Jun 2024	
	Dalbit		2022	
	Elephant Beetle	[Unknown]	2020	
	Gelsemium		2014-2023	

	Iridium		2018-Dec 2018	
	TaskMasters		2010-May 2021	
	Worok		2020	

8 groups listed (8 APT, 0 other, 0 unknown)

↑
