Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:34:18 UTC

Tool: RedXOR

Names	RedXOR
Category	Malware
Type	Backdoor
Description	(Intezer) The backdoor masquerades itself as polkit daemon. We named it RedXOR for its network data encoding scheme based on XOR. The malware was compiled on Red Hat Enterprise Linux.
Information	<https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.redxor>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool RedXOR

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

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