Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:45:00 UTC

Tool: POOLRAT

Names	POOLRAT SIMPLESEA
Category	Malware
Type	Backdoor
Description	(Mandiant) POOLRAT is a C/C++ macOS backdoor capable of collecting basic system information and executing commands. The commands performed include running arbitrary commands, secure deleting files, reading and writing files, updating the configuration.
Information	<https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/osx.poolrat>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool POOLRAT

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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