Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:40:50 UTC

Tool: BRICKSTORM

Names	BRICKSTORM
Category	Malware
Type	Backdoor
Description	(NVISO) BRICKSTORM provides attackers with file manager and network tunneling capabilities. As a notable difference to Mandiant's BRICKSTORM report, the Windows samples discussed here are not equipped with command execution capabilities. Instead, adversaries have been observed using network tunneling capabilities in combination with valid credentials to abuse well-known protocols such as RDP or SMB, thus achieving similar command execution
Information	<https://blog.nviso.eu/wp-content/uploads/2025/04/NVISO-BRICKSTORM-Report.pdf>

Last change to this tool card: 21 April 2025

Download this tool card in JSON format

All groups using tool BRICKSTORM

Changed	Name	Country	Observed	
APT groups				
	UNC5221, UTA0178		2022-Mar 2025	

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