Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:28:37 UTC

Tool: BOLDMOVE

Names	BOLDMOVE
Category	Malware
Type	Backdoor
Description	(Mandiant) With BOLDMOVE, the attackers not only developed an exploit, but malware that shows an in-depth understanding of systems, services, logging, and undocumented proprietary formats. Malware running on an internet-connected device can enable lateral movement further into a network and enable command and control (C2) by tunneling commands in and data out of a network.
Information	<https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw>
MITRE ATT&CK	<https://attack.mitre.org/software/S1184>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.boldmove> <https://malpedia.caad.fkie.fraunhofer.de/details/win.boldmove>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool BOLDMOVE

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

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