Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:53:58 UTC

Tool: COATHANGER

Names	COATHANGER
Category	Malware
Type	Backdoor
Description	(MIVD) The COATHANGER malware provides access to compromised FortiGate devices after installation. The implant connects back periodically to a Command & Control server over SSL, providing a BusyBox reverse shell. Notably, the COATHANGER implant is persistent, recovering after every reboot by injecting a backup of itself in the process responsible for rebooting the system. Moreover, the infection survives firmware upgrades. Even fully patched FortiGate devices may therefore be infected, if they were compromised before the latest patch was applied. Furthermore, COATHANGER is stealthy: it is hard to detect using default FortiGate CLI commands, because it hides itself by hooking most system calls that could reveal its presence, such as stat and opendir. It does so by replacing them for any process that is forced to load preload.so. Note that COATHANGER is distinct from BOLDMOVE, another RAT targeting FortiGate devices.
Information	<https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S1105>

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

All groups using tool COATHANGER

Changed	Name	Country	Observed

APT groups

	[Unnamed groups: China]		2018-Mar 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=afab8ba9-b296-4bcd-a5c4-986b185b768b