Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:22:45 UTC

Tool: CASTLETAP

Names	CASTLETAP
Category	Malware
Type	Backdoor
Description	(Mandiant) Analysis on the FortiGate firewalls identified an additional malicious file /bin/fgfm. Analysis of /bin/fgfm determined it to be a passive backdoor, named CASTLETAP, that listened for a specialized ICMP packet for activation. The threat actor likely named the file 'fgfm' in an attempt to disguise the backdoor as the legitimate service 'fgfmd' which facilitates communication between the FortiManager and FortiGate firewalls. Once executed, CASTLETAP created a raw promiscuous socket to sniff network traffic. CASTLETAP then filtered and XOR decoded a 9-byte magic activation string in the payload of an ICMP echo request packet.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/fortinet-malware-ecosystem/>

Last change to this tool card: 26 August 2024

Download this tool card in JSON format

All groups using tool CASTLETAP

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

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