Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:45:54 UTC

Tool: PingPull

Names	PingPull
Category	Malware
Type	Backdoor
Description	(Palo Alto) PingPull has the capability to leverage three protocols (ICMP, HTTP(S) and raw TCP) for command and control (C2). While the use of ICMP tunneling is not a new technique, PingPull uses ICMP to make it more difficult to detect its C2 communications, as few organizations implement inspection of ICMP traffic on their networks. This blog provides a detailed breakdown of this new tool as well as the GALLIUM group's recent infrastructure.
Information	<https://unit42.paloaltonetworks.com/pingpull-gallium/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1031/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.pingpull>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool PingPull

Changed	Name	Country	Observed	
APT groups				
	Gallium		2018-Jun 2022	

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