Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:30:43 UTC

Tool: QUADAGENT

Names	QUADAGENT
Category	Malware
Type	Backdoor, Tunneling
Description	(Palo Alto) Once the QUADAGENT payload has executed, it will use rdppath[.]com as the C2, first via HTTPS, then HTTP, then via DNS tunneling, each being used as a corresponding fallback channel if the former fails.
Information	<https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0269/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.quadagent>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:QUADAGENT>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool QUADAGENT

Changed	Name	Country	Observed	
APT groups				
	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0951e35a-f91b-43e8-936a-e6b6f1439555