Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:15:44 UTC

Tool: RDAT

Names	RDAT GREYSTUFF
Category	Malware
Type	Backdoor, Tunneling
Description	(Palo Alto) The adversaries compiled the RDAT payloads used in the attacks on the Middle Eastern telecommunications organization on March 1, 2020, and configured it to use a domain provided on the command line or the hardcoded domain rsshay[.]com as its C2 server. Unlike previous RDAT samples, this particular sample only uses DNS tunneling for its C2 communications with no HTTP fallback channel. This RDAT sample can only use TXT queries in its DNS tunnel.
Information	<https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/> <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020OverWatchNowheretoHide.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0495/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rdat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:rdat>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool RDAT

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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