Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:37:14 UTC

Tool: POWERSTATS

Names	POWERSTATS Valyria
Category	Malware
Type	Backdoor
Description	(Palo Alto) MuddyWater attacks are characterized by the use of a slowly evolving PowerShell-based first stage backdoor we call “POWERSTATS”.
Information	<https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/> <https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/> <https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spear-phishing-campaign.html> <https://blog.malwarebytes.com/threat-analysis/2017/09/elaborate-scripting-fu-used-in-espionage-attack-against-saudi-arabia-government_entity/> <https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/> <https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0223/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerstats>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:POWERSTATS>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool POWERSTATS

Changed	Name	Country	Observed
APT groups			

	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	

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

↑
