Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:05:46 UTC

Tool: MoonWind RAT

Names	MoonWind RAT MoonWind
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer
Description	(Palo Alto) The malware proceeds to collect the following victim information: • Hostname • Username • Windows version • IP address • Current time • RAM amount • Number of total drives • Number of removable drives • Unique victim identifier In total, MoonWind has 73 possibly commands that it can accept.
Information	<https://unit42.paloaltonetworks.com/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0149/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.moonwind>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:moonwind>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool MoonWind RAT

Changed	Name	Country	Observed	
APT groups				
	Nightshade Panda, APT 9, Group 27		2013-Sep 2016	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=14592f43-472d-41b2-9f29-7994c9a473fa