Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:39:20 UTC

Tool: ShadowNet

Names	ShadowNet
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Citizen Lab) ShadowNet malware leverages Windows Management Instrumentation (WMI), a system tool meant for administrators. Its intended usage as a tool for collecting system information and automation makes it an ideal mechanism for gathering and exfiltrating data. The use of legitimate Windows features can make it more difficult for administrators to identify activity as malicious. ShadowNet typically uses multi-layered C2 infrastructure that first connects to blog websites and then retrieves C2 information from encoded strings left on the blog. By using blog sites as intermediaries the attackers can maintain control of compromised machines even if a C2 is blocked by a network firewall or otherwise goes down. If a C2 needs to be updated the attackers can simply point the intermediaries to new servers.
Information	<https://citizenlab.ca/2015/03/tibetan-uprising-day-malware-attacks/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool ShadowNet

Changed	Name	Country	Observed	
APT groups				
	Shadow Network		2010-2010	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=93ab0ca2-e9e1-422e-b35e-04fe80d4974d