Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:25:28 UTC

Tool: SessionManager

Names	SessionManager
Category	Malware
Type	Backdoor
Description	(Palo Alto) SessionManager is a unique custom backdoor that allows its operators to run commands, as well as uploading files to and downloading them from the web server. This threat also allows attackers to use the web server as a proxy to communicate with additional systems on the network.
Information	<https://unit42.paloaltonetworks.com/rare-possible-gelsemium-attack-targets-se-asia/> <https://securelist.com/the-sessionmanager-iis-backdoor/106868/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.session_manager>

Last change to this tool card: 13 October 2023

Download this tool card in JSON format

All groups using tool SessionManager

Changed	Name	Country	Observed	
APT groups				
	Gelsemium		2014-2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6bb6d05c-cfa7-40a7-91c2-92d94b3e2f38