Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:04:17 UTC

Tool: HemiGate

Names	HemiGate
Category	Malware
Type	Backdoor
Description	(Trend Micro) HemiGate is a backdoor used by Earth Estries. Like most of the tools used by this threat actor, this backdoor is also executed via DLL sideloading using one of the loaders that support interchangeable payloads. K7AVMScn.exe from K7 Computing is the sideloading host utilized by this backdoor, while the loader poses as K7AVWScn.dll. The main backdoor is an encrypted file named taskhask.doc, and another encrypted file named taskhask.dat serves as the configuration file.
Information	<https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html> <https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hemigate>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool HemiGate

Changed	Name	Country	Observed	
APT groups				
	Salt Typhoon, GhostEmperor		2020-Feb 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3a8b91fe-b0df-4e6c-a005-be144bbc6440