Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:13:05 UTC

Tool: NestEgg

Names	NestEgg
Category	Malware
Type	Reconnaissance, Backdoor, Tunneling, Info stealer, Exfiltration
Description	NESTEGG is a memory-only backdoor that can proxy commands to other infected systems using a custom routing scheme. It accepts commands to upload and download files, list and delete files, list and terminate processes, and start processes. NESTEGG also creates Windows Firewall rules that allows the backdoor to bind to a specified port number to allow for inbound traffic.
Information	<https://www.documentcloud.org/documents/4834259-Park-Jin-Hyok-Complaint.html> <https://content.fireeye.com/apt/rpt-apt38> <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180231/LazarusUnderTheHood_PDF_final_for_securelist.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.nestegg>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool NestEgg

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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