Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:57:56 UTC

Tool: SLICKSHOES

Names	SLICKSHOES
Category	Malware
Type	Reconnaissance, Dropper, Backdoor, Info stealer, Exfiltration
Description	(US-CERT) This sample is a Themida-packed dropper that decodes and drops a file 'C:\Windows\Web\taskenc.exe' which is a Themida-packed beaconing implant. The beaconing implant does not execute the dropped file nor does it schedule any tasks to run the malware. The dropped beaconing implant uses an indigenous network encoding algorithm and is capable of many features including conducting system surveys, file upload/download, process and command execution, and screen captures.
Information	<https://www.us-cert.gov/ncas/analysis-reports/ar20-045b>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.slickshoes>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:SLICKSHOES>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool SLICKSHOES

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

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