NetHelp Infostealer - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:33:44 UTC

Tool: NetHelp Infostealer

Names	NetHelp Infostealer NetHelp Striker
Category	Malware
Type	Backdoor, Info stealer
Description	(Recorded Future) The NetHelp payload was only designed to work as a service (a persistence method established by the audio dropper of matching bitness). The payload dynamically links APIs at runtime via GetProcAddress and LoadLibrary. The implant simultaneously relied on two methods of communication: creating a separate thread with an open socket to the server on port 80, as well as issuing POST requests to the C2 server with the specific User-Agent.
Information	<https://www.recordedfuture.com/redalpha-cyber-campaigns/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool NetHelp Infostealer

Changed	Name	Country	Observed	
APT groups				
	RedAlpha		2015-2021	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7db71641-766e-4bfb-90a8-2b7626e526e7