Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:40:45 UTC

Tool: Nautilus

Names	Nautilus
Category	Malware
Type	Backdoor
Description	Nautilus is very similar to Neuron both in the targeting of mail servers and how client communications are performed. This malware is referred to as Nautilus due to its embedded internal DLL name “nautilus-service.dll”, again sharing some resemblance to Neuron. The Nautilus service listens for HTTP requests from clients to process tasking requests such as executing commands, deleting files and writing files to disk.
Information	<https://threatpost.com/turla-compromises-iranian-apt/149375/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.nautilus>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Nautilus

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	
	Turla, Waterbug, Venomous Bear		1996-2024	

2 groups listed (2 APT, 0 other, 0 unknown)