Threat Group Cards: A Threat Actor Encyclopedia

Tool: DAVESHELL

Names	DAVESHELL sRDI
Category	Malware
Type	Dropper
Description	(Mandiant) DAVESHELL is shellcode that functions as an in-memory dropper. Its embedded payload is mapped into memory and executed.
Information	<https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.srdi>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool DAVESHELL

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

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