

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:14:01 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool DAVESHELL

## Tool: DAVESHELL

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

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	
<b>APT groups</b>				
	<a href="#">Lazarus Group, Hidden Cobra, Labyrinth Chollima</a>		2007-May 2025	

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b010508c-af27-4b52-811f-f39fc585f9ae>