Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:28:11 UTC

Tool: WinorDLL64

Names	WinorDLL64
Category	Malware
Type	Backdoor
Description	(ESET) WinorDLL64 serves as a backdoor that most notably acquires extensive system information, provides means for file manipulation, and executes additional commands. Interestingly, it communicates over a TCP connection that was already established by its loader and uses some of the loader's functions.
Information	<https://www.welivesecurity.com/2023/02/23/winordll64-backdoor-vast-lazarus-arsenal/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.winordll64>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool WinorDLL64

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

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