Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:45:30 UTC

Tool: xDll

Names	xDll
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader, Exfiltration
Description	(Positive Technologies) The backdoor is a file written in C++ and compiled in Microsoft Visual Studio using the MFC library. It also has a plausible compilation date of February 10, 2020, 6:14:37 PM.
Information	<https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/shadowpad-new-activity-from-the-winnti-group/>

Last change to this tool card: 19 October 2020

Download this tool card in JSON format

All groups using tool xDll

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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