Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:49:35 UTC

Tool: Dtrack

Names	Dtrack TroyRAT Preft
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	Dtrack is a Remote Administration Tool (RAT) developed by the Lazarus group. Its core functionality includes operations to upload a file to the victim's computer, download a file from the victim's computer, dump disk volume data, persistence and more. A variant of Dtrack was found on Kudankulam Nuclear Power Plant (KNPP) which was used for a targeted attack.
Information	<https://securelist.com/my-name-is-dtrack/93338/> <https://securelist.com/dtrack-targeting-europe-latin-america/107798/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0567/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dtrack>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:DTrack>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool Dtrack

Changed	Name	Country	Observed
APT groups			

	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	
	Wassonite		2018-Oct 2019	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5a3e9d46-de22-4cd7-af31-cc7ea1079471