Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:44:23 UTC

Tool: TESDAT

Names	TESDAT
Category	Malware
Type	Loader
Description	(Trend Micro) The newer loader we later found is called TESDAT. It always loads a payload file with a ".dat" extension (like "mns.dat"). Instead of using common APIs like CreateThread to execute the decoded shellcode, it always calls an API called "SwitchToFiber," which we think is an attempt to avoid detection. Our analysis showed two variants for TESDAT loaders. It can be either an EXE file or a DLL file with an export function called "Init."
Information	<https://www.trendmicro.com/en_us/research/25/d/earth-kurma-apt-campaign.html>

Last change to this tool card: 27 June 2025

Download this tool card in JSON format

All groups using tool TESDAT

Changed	Name	Country	Observed	
APT groups				
	Earth Kurma		2020	

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