Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:15:50 UTC

Tool: TDTESS

Names	TDTESS
Category	Malware
Type	Backdoor, Info stealer, Downloader
Description	(ClearSky) TDTESS is 64-bit .NET binary backdoor that provides a reverse shell with an option to download and execute files. It routinely calls in to the command and control server for new instructions using basic authentication. Commands are sent via a web page. The malware creates a stealth service, which will not show on the service manager or other tools that enumerate services from WINAPI or Windows Management Instrumentation.
Information	<https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0164/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tdtess>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool TDTESS

Changed	Name	Country	Observed	
APT groups				
	CopyKittens, Slayer Kitten		2013-Jan 2017	
	Magic Hound, APT 35, Cobalt Illusion, Charming Kitten		2012-Jun 2025	

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