Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:53:05 UTC

Tool: WndTest

Names	WndTest
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	(Cylance) WndTest is the evolution of the PVZ tool chain into a single executable. The tool chain is minimized down to a command and control communications, keystroke logging, and clipboard monitoring. The command and control still supports upgrading, downloading, and executing of applications, as well as executing batch scripts. WndTest installs as a service and has been observed attempting to impersonate Adobe Report Service. WndTest starts using PHP servers for its command and control server, some of which are listed as defaced sites.
Information	<https://www.cylance.com/content/dam/cylance/pdfs/reports/Cylance_Operation_Cleaver_Report.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.wndtest>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool WndTest

Changed	Name	Country	Observed	
APT groups				
	Cutting Kitten, TG-2889		2012-Mar 2016	

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