Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:25:54 UTC

Tool: GpUpdates.exe

Names	GpUpdates.exe
Category	Malware
Type	Dropper
Description	(Epic Turla) The droppers are misidentified as packed by Armadillo but in reality they're built using now defunct Chilkat software, 'Zip2Secure' to create self-extracting executables. The packing alone has led the droppers to be detected under generic AV detections but the subcomponents have low-to-no detections at this time. The Zip2Secure configuration entrusts the distribution of the files contained therein to 'Distribute.exe', which places the files and silently registers the subcomponents with regsvr32.exe.
Information	<https://www.epicturla.com/blog/the-lost-nazar>

Last change to this tool card: 24 April 2020

Download this tool card in JSON format

All groups using tool GpUpdates.exe

Changed	Name	Country	Observed	
APT groups				
	Nazar		2008	

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