Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:23:38 UTC

Tool: PowerSpritz

Names	PowerSpritz
Category	Malware
Type	Dropper, Downloader
Description	(Proofpoint) PowerSpritz is a Windows executable that hides both its legitimate payload and malicious PowerShell command using a non-standard implementation of the already rarely used Spritz encryption algorithm. PowerSpritz decrypts a legitimate Skype or Telegram installer using a custom Spritz implementation with the key “Znxkai@if8qa9w9489”. PowerSpritz then writes the legitimate installer to disk in the directory returned by GetTempPathA either as a hardcoded filename such as SkypeSetup.exe or, in some versions, as the filename returned by GetTempFileNameA. The installer is then executed to trick the potential victim into thinking they downloaded a legitimate, working application installer or update. Finally, Spritz uses the same key to decrypt a PowerShell command that downloads the first stage of PowerRatankba.
Information	<https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powerspritz>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool PowerSpritz

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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