Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:23:09 UTC

Tool: Powersing

Names	Powersing
Category	Malware
Type	Backdoor, Info stealer
Description	(Kaspersky) • Stage 0's role is to extract and execute the next element of the chain, as well as a decoy document embedded inside the LNK file to display to the user. This creates the illusion of having clicked on a real document and ensures the victim doesn't get suspicious. • Stage 1 is a PowerShell script containing C# assembly designed to connect to a dead drop resolver (more on this in the next paragraph) and obtain cryptographic material used to decode the last stage of the chain by extracting a "DLL" file from the shortcut and locating a Base64-encoded list of URLs at a fixed offset. This establishes persistence by creating a shortcut (using the dropped icon) in the Windows startup folder pointing to the VBE startup script. • Finally, on stage 2, the actual malware implant used to take control of the victim's machine. It connects to one of the dead drop resolvers to get the address of the real C&C server and enters a loop that looks for orders every few seconds. • Upon system restart, the VBE startup script – which closely resembles stage 0 – is automatically executed, once again leading all the way to Powersing stage 2. Communications with the C&C server involve the exchange of JSON-encoded objects. Powersing only has two tasks: • Capture periodic screenshots from the victim's machine, which are immediately sent to the C&C server (two built-in commands allow operators to change screenshot quality and periodicity) • Execute arbitrary Powershell scripts provided by the C&C
Information	<https://securelist.com/deathstalker-mercenary-triumvirate/98177/>

Last change to this tool card: 27 August 2020

Download this tool card in JSON format

All groups using tool Powersing

Changed	Name	Country	Observed	
APT groups				
	Deceptikons, DeathStalker	[Unknown]	2012-Jun 2020	

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