Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:38:42 UTC

Tool: PowGoop

Names	PowGoop
Category	Malware
Type	Loader
Description	(Palo Alto) The PowGoop downloader has two components: a DLL loader and a PowerShell-based downloader. The PowGoop loader component is responsible for decrypting and running the PowerShell code that comprises the PowGoop downloader. The PowGoop loader DLL that existed in the same environment as LogicalDuckBill had a filename of goopdate.dll that was likely sideloaded by the legitimate and signed Google Update executable. The sideloading process would start with the legitimate GoogleUpdate.exe file loading a legitimate DLL with a name of goopdate86.dll. The sideloading would occur when the goopdate86.dll library loads the goopdate.dll file, which effectively runs the PowGoop loader.
Information	<https://unit42.paloaltonetworks.com/thanos-ransomware/> <https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf> <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east>
MITRE ATT&CK	<https://attack.mitre.org/software/S1046/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.powgoop>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool PowGoop

Changed	Name	Country	Observed
APT groups			

	MuddyWater, Seedworm, TEMP.Zagros, Static Kitten		2017-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5bb80638-3bd5-4921-adc9-ef529ced2d91