Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:23:50 UTC

Tool: GooseEgg

Names	GooseEgg
Category	Exploits
Type	Loader
Description	(Microsoft) The GooseEgg binary—which has included but is not limited to the file names justice.exe and DefragmentSrv.exe—takes one of four commands, each with different run paths. While the binary appears to launch a trivial given command, in fact the binary does this in a unique and sophisticated manner, likely to help conceal the activity.
Information	<https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gooseegg>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool GooseEgg

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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