

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:43:11 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool PylangGhost

Tool: PylangGhost

Names	PylangGhost
Category	Malware
Type	Backdoor
Description	<p>(Talos) As the Golang variant of the RAT is already well-documented, this blog focuses on the Python version and the similarities between the two. The initial stage consists of a command line which the fake webpage tells the unsuspecting user to copy, paste and execute.</p> <p>The command line uses either PowerShell Invoke-WebRequest or curl to download a ZIP file containing the PylangGhost modules as well as Visual Basic Script file. This script is responsible for unzipping the Python library stored in the “lib.zip file” and launching the trojan by running a renamed Python interpreter using the file “nvidia.py” as the Python program to run.</p>
Information	< https://blog.talosintelligence.com/python-version-of-golangghost-rat/ >

Last change to this tool card: 28 June 2025

Download this tool card in [JSON](#) format

All groups using tool PylangGhost

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Operation Contagious Interview		2020-Jul 2025	

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