Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:07:52 UTC

Tool: Psylo

Names	Psylo
Category	Malware
Type	Backdoor, Exfiltration
Description	(Palo Alto) Psylo is a tool that allows threat actors to upload and download files to and from a compromised system, as well as execute commands and applications on the system. The name Psylo is an anagram from the mutex created when initially running this payload, which is 'hnxlopsyxt'. Psylo is similar to FakeM in that they are both shellcode-based, and they have similar configurations and C2 communication channels.
Information	<https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0078/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Psylo>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool Psylo

Changed	Name	Country	Observed	
APT groups				
	Scarlet Mimic		2015-Aug 2022	

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