Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:08:27 UTC

Tool: PhanDoor

Names	PhanDoor
Category	Malware
Type	Backdoor
Description	(AhnLab) Phandoor was used from January 2016 to the summer of 2017. It is characterized by having the string 'S^%' main character strings. (E.g. S^%s\cmd.exe, S^nehomegpa.dll) However, some variants found in 2017 did not contain character string, 'Anonymous?' When Phandoor is executed, it initializes and tries to connect to C&C server. At this time, the string 'Anonymous?' is s check whether that the server is functioning properly. After that, it receives commands from the C&C server such as to execute the cmd.exe file.
Information	<https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus%2
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.phandoor>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Phandoor>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool PhanDoor

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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