Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:20:05 UTC

Tool: BlueShell

Names	BlueShell
Category	Malware
Type	Backdoor
Description	According to AhnLab, BlueShell is a backdoor malware developed in Go language, published on Github, and it supports Windows, Linux, and Mac operating systems. Currently, the original Github repository is presumed to have been deleted, but the BlueShell source code can still be obtained from other repositories. It features an explanatory ReadMe file in Chinese, indicating the possibility that the creator is a Chinese user.
Information	<https://asec.ahnlab.com/en/47455/> <https://asec.ahnlab.com/en/56941/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.blueshell>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool BlueShell

Changed	Name	Country	Observed	
APT groups				
	Dalbit		2022	

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