Threat Group Cards: A Threat Actor Encyclopedia

Tool: Reshell

Names	Reshell
Category	Malware
Type	Backdoor
Description	(Palo Alto) Following the creation of the users and the reconnaissance activity, the attackers attempted to execute a previously undocumented .NET backdoor, which they named windows.exe. We named this threat Reshell based on its program database (PDB) path.
Information	<https://unit42.paloaltonetworks.com/alloy-taurus-targets-se-asian-government/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.reshell>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool Reshell

Changed	Name	Country	Observed	
APT groups				
	Earth Krahang		2022	
	Gallium		2018-Jun 2022	

2 groups listed (2 APT, 0 other, 0 unknown)