Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:55:40 UTC

Tool: RGDoor

Names	RGDoor
Category	Malware
Type	Backdoor, Info stealer
Description	RGDoor is a malicious Internet Information Services (IIS) backdoor developed in the C++ language. RGDoor has been seen deployed on webservers belonging to the Middle East government organizations. RGDoor provides backdoor access to compromised IIS servers.
Information	<https://unit42.paloaltonetworks.com/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/> <https://researchcenter.paloaltonetworks.com/2017/09/unit42-striking-oil-closer-look-adversary-infrastructure/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0258/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rgdoor>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool RGDoor

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=260ce10a-405e-4723-a836-5430dcf54336