Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:37:42 UTC

Tool: Agent Racoon

Names	Agent Racoon
Category	Malware
Type	Backdoor
Description	(Palo Alto) This malware family is written using the .NET framework and leverages the domain name service (DNS) protocol to create a covert channel and provide different backdoor functionalities. Threat actors have used this along with the other two tools in multiple attacks targeting organizations across the U.S., Middle East and Africa. Its C2 infrastructure dates back to 2020.
Information	<https://unit42.paloaltonetworks.com/new-toolset-targets-middle-east-africa-usa/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_racoon>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool Agent Racoon

Changed	Name	Country	Observed	
APT groups				
	Operation Diplomatic Specter		2022	

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