Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:45:26 UTC

Tool: Cuba

Names	Cuba COLDDRAW
Category	Malware
Type	Ransomware
Description	Cuba is a Windows-based ransomware family that has been used against financial institutions, technology, and logistics organizations in North and South America as well as Europe since at least December 2019.
Information	<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-335a> <https://blogs.blackberry.com/en/2023/08/cuba-ransomware-deploys-new-tools-targets-critical-infrastructure-sector-in-the-usa-and-it-integrator-in-latin-america>
MITRE ATT&CK	<https://attack.mitre.org/software/S0625>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cuba>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool Cuba

Changed	Name	Country	Observed	
APT groups				
	Tropical Scorpius, RomCom		2019-Oct 2024	

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