Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:31:43 UTC

Tool: PowerRatankba

Names	PowerRatankba QUICKRIDE.POWER
Category	Malware
Type	Backdoor, Info stealer
Description	(Proofpoint) a PowerShell-based malware variant that closely resembles the original Ratankba implant. We believe that PowerRatankba was likely developed as a replacement in Lazarus Group's strictly financially motivated team's arsenal to fill the hole left by Ratankba's discovery and very public documentation earlier this year.
Information	<https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf> <https://www.riskiq.com/blog/labs/lazarus-group-cryptocurrency/> <https://blog.trendmicro.com/trendlabs-security-intelligence/lazarus-campaign-targeting-cryptocurrencies-reveals-remote-controller-tool-evolved-ratankba/> <https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/> <https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.power_ratankba>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PowerRatankba>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool PowerRatankba

Changed	Name	Country	Observed
APT groups			

	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

↑
