Threat Group Cards: A Threat Actor Encyclopedia

Tool: RatankbaPOS

Names	RatankbaPOS RatabankaPOS
Category	Malware
Type	POS malware, Backdoor, Info stealer
Description	(Proofpoint) RatankbaPOS is deployed through a process injection dropper that is also capable of installing itself persistently, checking a C&C for either an update or a command to delete itself, dropping the RatankbaPOS implant to disk, and finally searching for the targeted POS process and module for injection and ultimately the theft of POS data.
Information	<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.ratankbapos>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool RatankbaPOS

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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