Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:00:27 UTC

Tool: RtPOS

Names	RtPOS
Category	Malware
Type	POS malware, Reconnaissance, Backdoor, Credential stealer
Description	(Booz Allen) RtPOS is unique in comparison to other fully featured POS malware like Project Hook and TreasureHunter, in that it has no native exfiltration capability. While other POS malware families are perfectly capable of sending captured Track1 and Track2 data to a C2 server, RtPOS merely saves the data locally. As this activity is similar to some POS utilities, this is likely intended to reduce the network activity footprint of RtPOS and ensure the malware remains undetected for longer, thus earning the controllers a healthier profit. The RtPOS malware is also simplistic in features, largely automated in operation, and lacks many of the features that more mature POS malware families do. The lack of a network exfiltration feature, interaction and user commands, as well as a dropper component hints at more serious implications: in order for RtPOS to execute and in order to retrieve the captured payment card data, the attackers would have existing access to the victim's machine(s). RtPOS may simply be an in-development POS malware family, though review and analysis suggests RtPOS is a post-compromise tool instead of a standalone malware, and may even be part of a larger, heretofore unidentified tool set.
Information	<https://www.boozallen.com/c/insight/blog/new-point-of-sale-malware-family-uncovered.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rtpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:RtPOS>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool RtPOS

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ab3b05c0-27a8-4225-bc9c-8ccc5b4796c1