Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:41:04 UTC

Tool: JackPOS

Names	JackPOS
Category	Malware
Type	POS malware, Reconnaissance, Backdoor, Credential stealer, Botnet
Description	(Trustwave) Overall, this malware is quite rudimentary. A number of bugs (some of which I've mentioned in this blog post) show a lack of sophistication and, possibly, a rush on the author's part. There are a number of artifacts that link this malware family to others we've seen. The blacklist of process names is extremely similar to the ones discovered in the Alina POS malware family. Additionally, the installation path very much reminds me of the early Dexter variants. It's certainly likely that because these malware families' code has been leaked online, the author used at least some of this code as a basis for JackPOS. While the malware technically has a command and control (C&C) component to it, overall it's quite limited and not nearly as robust as other examples seen in the past. I mentioned originally that I wanted to see if JackPOS brought something special to the table. I'm going to have to answer that question with a resounding 'no' in this particular case. However, while this family does not bring any innovative characteristics to the POS malware scene, as history has taught us, it should still very much be considered a real threat.
Information	<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/jackpos-the-house-always-wins/> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://threatpost.com/points-of-sale-poorly-secured-facing-sophisticated-attacks/106027/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.jackpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:jackpos>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool JackPOS

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=067de1ba-dafb-4c9b-9d60-50a4953d65d8