Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:10:01 UTC

Tool: CenterPOS

Names	CenterPOS Cerebrus
Category	Malware
Type	POS malware, Backdoor, Credential stealer
Description	(FireEye) CenterPOS malware was initially discovered in September 2015 in a directory filled with other POS malware, including NewPoSThings, two Alina POS variants known as “Spark” and “Joker,” and BlackPOS. This CenterPOS sample (171c4c62ab2001c2f2394c3ec021dfa3) contains an internal version of “1.7” and is a memory scraper that iterates through running processes in order to extract payment card information. The payment card information is transferred to a command and control (CnC) server via HTTP POST:
Information	<https://www.fireeye.com/blog/threat-research/2016/01/centerpos_an_evolvi.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.centerpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:CenterPOS>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool CenterPOS

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=af2af621-086d-4b01-af40-c4e0a406ccba