Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:21:54 UTC

Tool: PosCardStealer

Names	PosCardStealer
Category	Malware
Type	POS malware, Credential stealer
Description	(Panda Security) The first attack we were able to analyze took place September 30, 2015 and affected 30 PoS systems. The malware was installed using PowerShell, a popular Windows tool. With this tool the file (MD5: 0B4F921CF2537FCED9CAACA179F6DFF4) was executed, with an internal date of creation for two days before (28/09/2015 17:07:59) and compiled with C++ visuals. The installer's job is to infect the system with malware that is specifically designed for PoS systems. To do this, it uses different techniques in function with the PoS software installed on the system. In concrete, it looks for brain.exe (pertaining to Dinerware) and scpwin.exe processes, and installs the malware as follows depending on which of the two it finds.
Information	<https://www.pandasecurity.com/mediacenter/malware/poscardstealer-malware-pos/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.poscardstealer>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool PosCardStealer

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=2d486642-f5ab-4f5f-8248-8a3085e06c82