Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:01:15 UTC

Tool: PwnPOS

Names	PwnPOS
Category	Malware
Type	POS malware, Credential stealer
Description	(Trend Micro) PwnPOS is one of those perfect examples of malware that's able to fly under the radar all these years due to its simple but thoughtful construction; albeit not being future proof. Technically, there are two components of PwnPOS: 1) the RAM scraper binary, and 2) the binary responsible for data exfiltration. While the RAM scraper component remains constant, the data exfiltration component has seen several changes – implying that there are two, and possibly distinct, authors. The RAM scraper goes through a process' memory and dumps the data to the file and the binary uses SMTP for data exfiltration.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/pwnpos-old-undetected-pos-malware-still-causing-havoc/> <https://www.brimorlabsblog.com/2015/03/and-you-get-pos-malware-nameand-you-get.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pwnpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PwnPOS>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool PwnPOS

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=2dae9d51-6708-44f3-9253-21bc4262d92f