Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:31:48 UTC

Tool: FindPOS

Names	FindPOS PoSeidon
Category	Malware
Type	POS malware, Backdoor, Keylogger, Credential stealer
Description	(Palo Alto) The malware in question has the ability to scrape memory for track data, exfiltrate any discovered data via HTTP POST requests, and in some instances log keystrokes. While the malware family uses many common techniques witnessed in previous malware families targeting POS devices, the prevalence and continued development of this malware demonstrates a threat to those running Windows-based point of sale terminals.
Information	<https://unit42.paloaltonetworks.com/findpos-new-pos-malware-family-discovered/> <https://blogs.cisco.com/security/talos/poseidon>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.findpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:FindPOS>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool FindPOS

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

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