Pro POS - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:52:09 UTC

Tool: Pro POS

Names	Pro POS
Category	Malware
Type	POS malware, Backdoor, Credential stealer, Rootkit, Tunneling
Description	(Talos) Pro PoS is simple-to-use PoS malware that is available for purchase, enabling multiple threat actors to easily take advantage of this malware to target businesses. The functionality of Pro PoS seems fairly extensive according to recent press releases. These claims include the following: 1. Tor support 2. Rootkit functionalities 3. Mechanisms to avoid antivirus detection 4. Polymorphic engine
Information	<https://blog.talosintelligence.com/2015/12/pro-pos.html>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:pro%20pos>

Last change to this tool card: 13 June 2020

Download this tool card in JSON format

All groups using tool Pro POS

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

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