Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:31:56 UTC

Tool: Punkey

Names	Punkey PunkeyPOS Punkey POS pospunk poscardstealer
Category	Malware
Type	POS malware, Credential stealer
Description	(Trustwave) During a recent United States Secret Service investigation, Trustwave encountered a new family of POS malware, that we named Punkey. It appears to have evolved from the NewPosThings family of malware first discovered by Dennis Schwarz and Dave Loftus at Arbor Networks. While this malware shares some commonalities with that family, it departs from the standard operating procedure of the previous versions rather dramatically. In a blog post, TrendMicro also detailed recently compiled versions of the NewPOSthings family that bear a closer resemblance to NewPOSthings than Punkey. This suggests that multiple actors may be using similar source code, or the malware is being customized as a service for targeted campaigns.
Information	<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/new-pos-malware-emerges-punkey/> <https://www.pandasecurity.com/mediacenter/malware/punkeypos/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.punkey_pos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:punkey>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool Punkey

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=0f1accf5-8212-45a5-a3a3-ec852eb28065