Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:47:07 UTC

Tool: AbaddonPOS

Names	AbaddonPOS
Category	Malware
Type	POS malware
Description	(Proofpoint) Proofpoint threat researchers recently detected a new addition to PoS malware landscape. Named AbaddonPOS by Proofpoint researchers, this sample was initially discovered as it was being downloaded in the process of a Vawtrak infection. This use of additional payloads to enhance attack capabilities offers another example of efforts by threat actors to expand their target surfaces through the delivery of multiple payloads in a single campaign, in this case by including potential PoS terminals. This post will analyze AbaddonPOS; discuss the observed infection vectors; and expose, details on the downloader used to retrieve this new PoS malware. We will also provide evidence to demonstrate that the downloader malware and PoS malware are closely related, perhaps even written by the same actor or actors.
Information	<https://www.proofpoint.com/us/threat-insight/post/AbaddonPOS-A-New-Point-Of-Sale-Threat-Linked-To-Vawtrak> <https://threatpost.com/new-pos-malware-pinkkite-takes-flight/130428/> <https://www.proofpoint.com/us/threat-insight/post/abaddonpos-now-targeting-specific-pos-software>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.abaddon_pos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:abaddonpos>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool AbaddonPOS

Changed	Name	Country	Observed

APT groups

	FIN6, Skeleton Spider	[Unknown]	2015-Oct 2021	
	TA530	[Unknown]	2016-Nov 2016	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1e27e4a7-2583-4e55-9fe3-ffee54333563