Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:11:53 UTC

Tool: ModPOS

Names	ModPOS straxbot
Category	Malware
Type	Reconnaissance, POS malware, Backdoor, Keylogger, Credential stealer
Description	(FireEye) ModPOS is highly modular and can be configured to target specific systems with components such as uploader/downloader, keylogger, POS RAM scraper and custom plugins for credential theft and other specialized functions like network reconnaissance. We believe other capabilities could also be leveraged. The modules are packed kernel drivers that use multiple methods of obfuscation and encryption to evade even the most sophisticated security controls.
Information	<https://www.fireeye.com/blog/threat-research/2015/11/modpos.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.modpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:modpos>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool ModPOS

Changed	Name	Country	Observed	
APT groups				
	Operation Black Atlas	[Unknown]	2015	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fdb9cd93-6826-440e-b2ef-04f8618c92b4