Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:35:57 UTC

Tool: RawPOS

Names	RawPOS FIENDCRY DUEBREW DRIFTWOOD
Category	Malware
Type	POS malware, Backdoor, Info stealer
Description	(Trend Micro) Despite being one of the oldest Point-of-Sale (PoS) RAM scraper malware families out in the wild, RawPOS (detected by Trend Micro as TSPY_RAWPOS) is still very active today, with the threat actors behind it primarily focusing on the lucrative multibillion-dollar hospitality industry. While the threat actor's tools for lateral movement, as well as RawPOS' components, remain consistent, new behavior from the malware puts its victims at greater risk via potential identity theft. Specifically, this new behavior involves RawPOS stealing the driver's license information from the user to aid in the threat group's malicious activities.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/rawpos-new-behavior-risks-identity-theft/> <https://usa.visa.com/dam/VCOM/download/merchants/alert-rawpos.pdf> <https://threatvector.cylance.com/en_us/home/rawpos-malware.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0169/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rawpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:rawpos>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool RawPOS

Changed	Name	Country	Observed

APT groups

	FIN5	[Unknown]	2008	

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