Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:19:51 UTC

Tool: TinyPOS

Names	TinyPOS
Category	Malware
Type	POS malware, Backdoor, Info stealer
Description	(Forcepoint) It all starts with the delivery of a small loader called TinyLoader, an obfuscated executable withsimple -yet powerful- downloader functionality. Upon execution, it will first brute force its own decryption key (a 32-bit value, meaning this takes a fraction of second on modern PCs) before using this to decrypt the main program code. Code-wise the POS component is very similar to the loader, except there is no additional encryption, as whenever it is delivered the operators are almost certain -due to the pre-filtering above- that a valuable target has been identified. This component works like any other POS memory scraper: opening processes based on either a predefined black or whitelist of process names, creating a new thread for each matching one and scanning their full memory range for Track 1 and Track 2 credit card data. If such data is found, first it will be verified by the Luhn algorithm for integrity, then it will be encrypted by a pre-defined key (another 32 or 64-bit value stored in the POS binary itself) and either sent to yet another C2 identified, again, by IP/port combination or it will be saved locally.
Information	<https://www.forcepoint.com/sites/default/files/resources/files/report-tinypos-analysis-en.pdf> <https://blog.talosintelligence.com/2019/11/c2-with-it-all.html> <https://www.carbonblack.com/2020/05/21/tau-technical-report-new-attack-combines-tinypos-with-living-off-the-land-techniques-for-scraping-credit-card-data/> <https://github.com/carbonblack/tau-tools/tree/master/malware_specific/TinyPOS>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Tinypos>

Last change to this tool card: 26 May 2020

Download this tool card in JSON format

All groups using tool TinyPOS

Changed	Name	Country	Observed	
APT groups				
	Tiny Spider	[Unknown]	2015-2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=2698c733-ab93-4b51-acc8-3265209d0005