Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:54:16 UTC

Tool: FastPOS

Names	FastPOS
Category	Malware
Type	POS malware, Backdoor, Keylogger, Credential stealer
Description	(Trend Micro) How do the components make the entire system work? The main file extracts all components and passes control to the main service (serv32.exe). The main service creates and monitors a central communication medium and directly sends all received information to the C&C server. The keylogger components (Kl32.exe/Kl64.exe) hook the keyboard then communicate with the main service to send logged keystrokes to the C&C server. The RAM scraper modules monitor processes and scan for credit card track data, which are then sent to the main service.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/fastpos-updates-in-time-for-retail-sale-season/> <http://documents.trendmicro.com/assets/Appendix%20-%20FastPOS%20Updates%20in%20Time%20for%20the%20Retail%20Sale%20Season.pdf> <http://documents.trendmicro.com/assets/fastPOS-quick-and-easy-credit-card-theft.pdf> <https://www.bankinfosecurity.com/fastpos-malware-creator-pleads-guilty-to-federal-charges-a-14751>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.fast_pos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:fastpos>

Last change to this tool card: 02 August 2020

Download this tool card in JSON format

All groups using tool FastPOS

Changed	Name	Country	Observed

Other groups

	Infraud Organization	[Various]	2010-Jul 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=367c3161-847f-4f81-a69f-d70fa65db070