

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:18:21 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool MajikPOS

Tool: MajikPOS

Names	MajikPOS
Category	Malware
Type	POS malware , Backdoor , Credential stealer
Description	<p>(Trend Micro) While other PoS malware FastPOS (its updated version), Gorynych and ModPOS also feature multiple components with entirely different functions like keylogging, MajikPOS's modular tack is different. MajikPOS needs only another component from the server to conduct its RAM scraping routine.</p> <p>MajikPOS is named after its command and control (C&C) panel that receives commands and sends exfiltrated data. MajikPOS's operators use a combination of PoS malware and remote access Trojan (RAT) to attack their targets, to daunting effects. MajikPOS is a reflection of the increasing complexity that bad guys are predicted to employ in their malware to neuter traditional defenses.</p>
Information	<p><https://blog.trendmicro.com/trendlabs-security-intelligence/majikpos-combines-pos-malware-and-rats/></p> <p><https://documents.trendmicro.com/assets/majikpos-combines-pos-malware-and-rats-to-pull-off-its-malicious-tricks.pdf></p> <p><https://blog.group-ib.com/majikpos_treasurehunter_malware></p>
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.majik_pos >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:MajikPOS >

Last change to this tool card: 18 November 2022

Download this tool card in [JSON](#) format

All groups using tool MajikPOS

Changed	Name	Country	Observed
---------	------	---------	----------

Unknown groups

	_ [Interesting malware not linked to an actor yet] _			
--	------------------------------------------------------------------------	--	--	--

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e22b0666-2e62-4214-a1d0-1ff6d2832fd9>