Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:41:46 UTC

Tool: GamaPOS

Names	GamaPOS pios
Category	Malware
Type	POS malware, Credential stealer
Description	(Trend Micro) The GamaPOS threat uses a “shotgun” or “dynamite fishing” approach to get to targets, even unintended ones. This means that it launches a spam campaign to distribute Andromeda backdoors, infects systems with PoS malware, and hopes to catch target PoS systems out of sheer volume. Rough estimates show us that GamaPOS may have only hit 3.8% of those affected by Andromeda.
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/new-gamapos-threat-spreads-in-the-us-via-andromeda-botnet/> <http://documents.trendmicro.com/assets/GamaPOS_Technical_Brief.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.gamapos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:gamapos>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool GamaPOS

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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