Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:31:10 UTC

Home > List all groups > List all tools > List all groups using tool UDPoS

Tool: UDPoS

Names	UDPoS
Category	Malware
Type	POS malware, Credential stealer
Description	(Forcepoint) Point of Sale malware has been around for some time and has been deployed against a broad range of businesses from retailers to hotel groups. However, this appears to be a new family which we are currently calling 'UDPoS' owing to its heavy use of UDP-based DNS traffic. At the time of writing, it's unclear whether the malware is currently being used in campaigns in the wild, although the coordinated use of LogMeIn-themed filenames and C2 URLs, coupled with evidence of an earlier Intel-themed variant, suggest that it may well be.
Information	<https://www.forcepoint.com/blog/x-labs/udpos-exfiltrating-credit-card-data-dns> <https://threatmatrix.cylance.com/en_us/home/threat-spotlight-inside-udpos-malware.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.udpos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:udp%20pos>

Last change to this tool card: 24 May 2020

Download this tool card in JSON format

All groups using tool UDPoS

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=d1b2544d-3721-4d8f-91e6-5d777a5f56d9