Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:04:22 UTC

Tool: GlitchPOS

Names	GlitchPOS
Category	Malware
Type	POS malware, Credential stealer
Description	(Talos) Cisco Talos recently discovered a new PoS malware that the attackers are selling on a crimeware forum. Our researchers also discovered the associated payloads with the malware, its infrastructure and control panel. We assess with high confidence that this is not the first malware developed by this actor. A few years ago, they were also pushing the DiamondFox L!NK botnet. Known as 'GlitchPOS,' this malware is also being distributed on alternative websites at a higher price than the original.
Information	<https://blog.talosintelligence.com/2019/03/glitchpos-new-pos-malware-for-sale.html> <https://cis.verint.com/2019/05/07/the-awakening-of-pos-malware-or-has-it-really-been-dormant/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.glitch_pos>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:GlitchPOS>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool GlitchPOS

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

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