Alina POS - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:09:50 UTC

Tool: Alina POS

Names	Alina POS Track alina_eagle alina_spark aline_joker katrina
Category	Malware
Type	POS malware, Reconnaissance, Credential stealer
Description	(Trustwave) Alina is a well-documented family of malware used to scrape Credit Card (CC) data from Point of Sale (POS) software. We published a series of in-depth write-ups on the capabilities Alina possesses as well as the progression of the versions. Xylitol has a nice write-up on the Command and Control (C&C) aspects of Alina.
Information	<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/alina-pos-malware-sparks-off-a-new-variant/> <https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina--Casting-a-Shadow-on-POS/> <https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina--Following-The-Shadow-Part-1/> <https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina--Following-The-Shadow-Part-2/> <http://www.xylibox.com/2013/02/alina-34-pos-malware.html> <https://www.xylibox.com/2013/10/inside-malware-campaign-alina-dexter.html> <https://blog.trendmicro.com/trendlabs-security-intelligence/two-new-pos-malware-affecting-us-smbs/> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://www.secureworks.com/research/point-of-sale-malware-threats> <https://blog.centurylink.com/alina-point-of-sale-malware-still-lurking-in-dns/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.alina_pos>

Last change to this tool card: 02 July 2020

Download this tool card in JSON format

All groups using tool Alina POS

Changed	Name	Country	Observed	
APT groups				
	Operation Black Atlas	[Unknown]	2015	

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

↑
