Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:46:30 UTC

Tool: PoSlurp

Names	PoSlurp PUNCHTRACK PSVC
Category	Malware
Type	POS malware, Backdoor, Info stealer
Description	(Trend Micro) PoSlurp scrapes credit card data processed by the PoS devices, including stored and encrypted card data prior to malware infection. Once the information is extracted from the infected system, the attackers can check and verify the validity of the data offline. PoSlurp also allows the attackers to inject other commands, access files, copy log files back to the server, and delete log files, among others.
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fin8-reemerges-with-new-pos-malware-badhatch>
MITRE ATT&CK	<https://attack.mitre.org/software/S0197/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.poslurp>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PoSlurp>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool PoSlurp

Changed	Name	Country	Observed	
APT groups				
	FIN8	[Unknown]	2016-Dec 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=40074bfa-a8db-4cd2-89d4-200c99d717f2