Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:07:28 UTC

Tool: LogPOS

Names	LogPOS
Category	Malware
Type	POS malware, Credential stealer
Description	(securitykitten) In most POS variants, one process scrapes memory from other processes and writes discovered track data to a log. Because LogPOS injects code into various processes and has each of them search their own memory, it can't use a log, since they can't all open the same file with write access at once. Instead, it uses mailslots.
Information	<https://securitykitten.github.io/2015/11/16/logpos-new-point-of-sale-malware-using-mailslots.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.logpos>

Last change to this tool card: 22 May 2020

Download this tool card in JSON format

All groups using tool LogPOS

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

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