Cherry Picker - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:59:59 UTC

Tool: Cherry Picker

Names	Cherry Picker Cherry Picker POS CherryPicker POS cherrypickerpos cherrypicker cherry_picker
Category	Malware
Type	POS malware, Credential stealer
Description	(Trustwave) For the last five years Trustwave has been monitoring a threat across a number of forensic cases that we have dubbed 'Cherry Picker'. This targeted Point of Sale (PoS) memory scraper has enjoyed a very low detection rate in the wild for quite some time. Cherry Picker uses a new memory scraping algorithm, a file infector for persistence, and cleaner malware that removes all traces of the infection from target systems. This sophisticated functionality and highly targeted victims have helped the malware remain under the radar of many AV and security companies. This post will expose the functionality of Cherry Picker and hopefully help organizations provide protection from this threat.
Information	<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/shining-the-spotlight-on-cherry-picker-pos-malware/> <https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Memory-Scraping-Technique-in-Cherry-Picker-PoS-Malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0107/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cherry_picker>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:cherry%20picker>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Cherry Picker

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=617bd0a3-821e-43b4-9619-a6fd084d1439