Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:12:33 UTC

Tool: PICKPOCKET

Names	PICKPOCKET
Category	Malware
Type	Credential stealer
Description	(FireEye) PICKPOCKET is a credential theft tool that dumps the user's website login credentials from Chrome, Firefox, and Internet Explorer to a file. This tool was previously observed during a Mandiant incident response in 2018 and, to date, solely utilized by APT34.
Information	<https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.pickpocket>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:PICKPOCKET>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool PICKPOCKET

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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