Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:44:23 UTC

Tool: Jason

Names	Jason
Category	Malware
Type	Credential stealer
Description	Jason is a graphic tool implemented to perform Microsoft exchange account brute-force in order to “harvest” the highest possible emails and accounts information. Distributed in a ZIP container (a copy is available here) the interface is quite intuitive: the Microsoft exchange address and its version shall be provided (even if in the code a DNS-domain discovery mode function is available). Three brute-force methods could be selected: EWS (Exchange Web Service), OAB (Offline Address Book) or both (All). Username and password list can be selected (included in the distributed ZIP file) and threads number should be provided in order to optimize the attack balance.
Information	<https://marcoramilli.com/2019/06/06/apt34-jason-project/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.jason>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Jason

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=63a5c1de-3df9-4c7f-8fd3-134b26c2866f