Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:12:02 UTC

Tool: BADNEWS

Names	BADNEWS JakyllHyde
Category	Malware
Type	Backdoor
Description	BADNEWS is malware that has been used by the actors responsible for the Patchwork campaign. Its name was given due to its use of RSS feeds, forums, and blogs for command and control.
Information	<https://unit42.paloaltonetworks.com/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/> <http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-1> <http://blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-2> <https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0128/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.badnews>

Last change to this tool card: 16 May 2021

Download this tool card in JSON format

All groups using tool BADNEWS

Changed	Name	Country	Observed
APT groups			

	Operation HangOver, Monsoon, Viceroy Tiger		2010-Jan 2020	
	Patchwork, Dropping Elephant		2013-Jun 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=47855af1-b4fe-4dc4-ad52-3e4cf90e6924