Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:57:54 UTC

Tool: NewsReels

Names	NewsReels
Category	Malware
Type	Backdoor, Exfiltration
Description	The NEWSREELS malware family is an HTTP based backdoor. When first started, NEWSREELS decodes two strings from its resources section. These strings are both used as C2 channels, one URL is used as a beacon URL (transmitting) and the second URL is used to get commands (receiving). The NEWSREELS malware family is capable of performing file uploads, downloads, creating processes or creating an interactive reverse shell.
Information	<https://www.fireeye.com/blog/threat-research/2014/01/tracking-malware-import-hashing.html> <http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.newsreels>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool NewsReels

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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