Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:59:58 UTC

Tool: GLASSES

Names	GLASSES Wordpress Bruteforcer
Category	Malware
Type	Downloader
Description	(Citizen Lab) The dropped executable connects to a website and downloads a single HTML page. The site appears to be part of a legitimate website for an eyeglasses company, suggesting that it has been compromised. The accessed page contains an anchor with an encoded command in it. The malware looks for the string in the anchor tag with the target NewRef, and then decodes it to a command. The link itself is empty, so that there is nothing to click on and it is invisible on the page. Another page on the same site, aboutus.htm, contains a different command although the URL is not apparently used by this binary. Looking through the malware code, it is evident that this is a simple downloader with only two commands.
Information	<https://citizenlab.ca/2013/02/apt1s-glasses-watching-a-human-rights-organization/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.glasses>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool GLASSES

Changed	Name	Country	Observed
APT groups			

	Comment Crew, APT 1		2006-May 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=36aef054-c9d1-43e1-bdcd-973f18961dda