Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:53:27 UTC

Tool: HYPERSCRAPE

Names	HYPERSCRAPE
Category	Malware
Type	Exfiltration
Description	(Google) HYPERSCRAPE requires the victim's account credentials to run using a valid, authenticated user session the attacker has hijacked, or credentials the attacker has already acquired. It spoofs the user agent to look like an outdated browser, which enables the basic HTML view in Gmail. Once logged in, the tool changes the account's language settings to English and iterates through the contents of the mailbox, individually downloading messages as .eml files and marking them unread. After the program has finished downloading the inbox, it reverts the language back to its original settings and deletes any security emails from Google. Earlier versions contained the option to request data from Google Takeout, a feature which allows users to export their data to a downloadable archive file.
Information	<https://blog.google/threat-analysis-group/new-iranian-apt-data-extraction-tool/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hyperscrape>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool HYPERSCRAPE

Changed	Name	Country	Observed	
APT groups				
	Magic Hound, APT 35, Cobalt Illusion, Charming Kitten		2012-Jun 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1274a300-b39b-48f0-8648-8e0f46fe91fe