Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:27:39 UTC

Tool: Headlace

Names	Headlace
Category	Malware
Type	Backdoor, Dropper, Loader, Downloader, Info stealer, Credential stealer, Exfiltration
Description	(IBM) Headlace is a multi-component malware including a dropper, a VBS launcher and a backdoor using MSEdge in headless mode to continuously download secondary payloads, likely to exfiltrate credentials and sensitive information.
Information	<https://securityintelligence.com/x-force/itg05-ops-leverage-israel-hamas-conflict-lures-to-deliver-headlace-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.headlace>

Last change to this tool card: 17 January 2024

Download this tool card in JSON format

All groups using tool Headlace

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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