

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:35:27 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool HATVIBE



Tool: HATVIBE

Names	HATVIBE
Category	Malware
Type	Loader
Description	(The Hacker News) Opening the document and enabling macros results in the execution of an encoded HTML Application (HTA) named HATVIBE, which sets up persistence on the host using a scheduled task and paves the way for a Python backdoor codenamed CHERRYSPY , which is capable of running commands issued by a remote server.
Information	< https://thehackernews.com/2024/07/ukrainian-institutions-targeted-using.html > < https://cert.gov.ua/article/6280129 >

Last change to this tool card: 27 August 2024

Download this tool card in [JSON](#) format

All groups using tool HATVIBE

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

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1c242d91-b9d1-40af-972a-ecf002dbde30>