

Hatef Wiper - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:04:44 UTC

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

Tool: Hatef Wiper

Names	Hatef Wiper
Category	Malware
Type	Wiper
Description	<p>(Intezer) The malware wipes key system paths across all connected drives, focusing on directories within “Users,” “Program Files,” “Program Files (x86),” and “Windows,” employing the ProcessDirectory method to enumerate all files within these paths recursively. Once files are deleted, and directories are left empty, it uses an incorrectly spelled method, DeleteDrirectorys, to remove these now-obsolete directories.</p> <p>During its operation, the wiper sends periodic updates to a predetermined Telegram chat, likely to inform its controllers about the ongoing progress or notify them when the task is completed. The dispatched information comprises the external IP address of the infected computer, the hostname, a timestamp, and a count of “Undeleted files” within critical file system locations such as the Windows directory and Program Files directories. This count is formatted to show the number of files that the malware has not managed to delete up to that point. This communication strategy serves as a means of real-time reporting on malicious activities, offering the attackers updates and insights into the efficacy of their attack.</p>
Information	< https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/ >

Last change to this tool card: 16 January 2024

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

All groups using tool Hatef Wiper

Changed	Name	Country	Observed
Other groups			
	Handala Hack Team	[Unknown]	2023-Dec 2023

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=d582c66b-480c-41d3-9211-20a615163a5b>