

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:34:21 UTC

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



Tool: DOUBLEFANTASY

Names	DOUBLEFANTASY DoubleFantasy VALIDATOR
Category	Malware
Type	Reconnaissance , Downloader
Description	(Kaspersky) The Equation Group’s DoubleFantasy implant is a validator-style Trojan which sends basic information about the system to the attackers. It also allows them to upload a more sophisticated Trojan platform, such as EQUATIONDRUG or GRAYFISH . In general, after one of these sophisticated platforms are installed, the attackers remove the DoubleFantasy implant. In case the victim doesn’t check out, for example, if they are a researcher analysing the malware, the attackers can simply choose to uninstall the DoubleFantasy implant and clean up the victim’s machine.
Information	< https://securelist.com/equation-group-from-houston-with-love/68877/ > < https://www.antiy.com/response/FROM EQUATION TO EQUATIONS.pdf >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/elf.doublefantasy > < https://malpedia.caad.fkie.fraunhofer.de/details/win.doublefantasy >

Last change to this tool card: 28 December 2022

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

All groups using tool DOUBLEFANTASY

Changed	Name	Country	Observed	
APT groups				
	Equation Group		2001-Aug 2016	

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=7e44cd7d-5496-4c09-9a9f-d823f9637796>