

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:43:18 UTC

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

Tool: Icefog

Names	Icefog Fucobha
Category	Malware
Type	Backdoor , Info stealer
Description	(Kaspersky) The “Icefog” backdoor set (also known as “Fucobha”) is an interactive espionage tool that is directly controlled by the attackers. There are versions for both Microsoft Windows and Mac OS X. In its latest incarnation, Icefog doesn’t automatically exfiltrate data, instead, it is operated by the attackers to perform actions directly on the victim’s live systems.
Information	< https://media.kaspersky.com/en/icefog-apt-threat.pdf > < http://www.kz-cert.kz/page/502 >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.icefog >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:ICEFOG >

Last change to this tool card: 13 May 2020

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

All groups using tool Icefog

Changed	Name	Country	Observed
APT groups			
	Icefog, Dagger Panda		2011-2018/2019
	RedFoxtrot		2014-Aug 2021

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.eta.ora.th/cgi-bin/listgroups.cgi?u=923f2526-abf4-4ccd-9341-afc86e2b21e8>