

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:45:27 UTC

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

Tool: WindTail

Names	WindTail
Category	Malware
Type	Backdoor
Description	(Carbon Black) One of the custom macOS backdoors employed by this group has been named WindTail and is typically delivered via email in a zip file containing an application masquerading as an Office document.
Information	< https://www.carbonblack.com/2019/01/18/tau-threat-intelligence-notification-windtail-osx/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S0466/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/osx.windtail >

Last change to this tool card: 30 December 2022

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

All groups using tool WindTail

Changed	Name	Country	Observed
APT groups			
	WindShift	[Unknown]	2018

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f81b4f3d-e2db-4fb6-847c-a5fae410e157>