

WindTail (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:02:46 UTC

osx.windtail ([Back to overview](#))

WindTail

Actor(s): [WindShift](#)

There is no description at this point.

References

2019-12-12 · [Virus Bulletin](#) · [Patrick Wardle](#)

Cyber espionage in the Middle East: unravelling OSX.WindTail
[WindTail](#)

2019-04-24 · [SpecterOps](#) · [Richie Cyrus](#)

Introducing Venator: A macOS tool for proactive detection
[AppleJeus WindTail](#)

2019-04-08 · [SANS Cyber Security Summit](#) · [Taha Karim](#)

Trails of WindShift
[WindTail ZhMimikatz](#)

2019-01-15 · [Objective See](#) · [Patrick Wardle](#)

Middle East Cyber-Espionage: analyzing WindShift's implant: OSX.WindTail (part 2)
[WindTail](#)

2018-12-20 · [Objective-See](#) · [Patrick Wardle](#)

Middle East Cyber-Espionage: analyzing WindShift's implant: OSX.WindTail (part 1)
[WindTail](#)

2018-08-30 · [Forbes](#) · [Thomas Brewster](#)

Hackers Are Exposing An Apple Mac Weakness In Middle East Espionage
[WindTail](#)

2018-01-01 · [DarkMatter](#) · [Taha K.](#)

IN THE TRAILS OF WINDSHIFTAPT
[WindTail WindShift](#)

There is no Yara-Signature yet.

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/osx.windtail>