

oRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:25:03 UTC

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

oRAT

SentinelOne describes this as a malware written in Go, mixing own custom code with code from public repositories.

References

2022-05-23 · [Trend Micro](#) · [Daniel Lunghi](#), [Jaromír Hořejší](#)

Operation Earth Berberoka

[reptile oRAT Ghost RAT PlugX_pupy Earth Berberoka](#)

2022-05-09 · [Dinesh Devadoss](#), [Phil Stokes](#)

From the Front Lines | Unsigned macOS oRAT Malware Gambles For The Win

[oRAT](#)

2022-04-27 · [Trendmicro](#) · [Daniel Lunghi](#), [Jaromír Hořejší](#)

Operation Gambling Puppet

[reptile oRAT AsyncRAT Cobalt Strike DCRat Ghost RAT PlugX Quasar RAT Trochilus RAT Earth Berberoka](#)

2022-04-27 · [Trendmicro](#) · [Trendmicro](#)

IOCs for Earth Berberoka - MacOS

[oRAT Earth Berberoka](#)

There is no Yara-Signature yet.

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