CDDS (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:18:30 UTC

osx.cdds (Back to overview)

CDDS

aka: Macma

Google TAG has observed this malware being delivered via watering hole attacks using 0-day exploits, targeting visitors to Hong Kong websites for a media outlet and a prominent pro-democracy labor and political group.

References

2024-08-02 · Volexity · Ankur Saini, Paul Rascagnères, Steven Adair, Thomas Lancaster
StormBamboo Compromises ISP to Abuse Insecure Software Update Mechanisms
CDDS DUSTPAN MgBot

2021-11-15 · SentinelOne · Phil Stokes
Infect If Needed | A Deeper Dive Into Targeted Backdoor macOS.Macma
CDDS

2021-11-11 · Objective-See · Patrick Wardle
OSX.CDDS a sophisticated watering hole campaign drops a new macOS implant!
CDDS

2021-11-11 · Google · Erye Hernandez, Google Threat Analysis Group
Analyzing a watering hole campaign using macOS exploits
CDDS

There is no Yara-Signature yet.
