Rewterz Threat Alert – GIMMICK Malware - Active IOCs - Rewterz

Published: 2022-03-25 · Archived: 2026-04-05 17:09:56 UTC

Severity

High

Analysis Summary

GIMMICK Malware is a newly discovered malware used by a Chinese espionage threat actor called “Storm Cloud”. GIMMICK is a macOS variant of the malware and reserachers previously discovered a Windows version of the malware as well. The malware is written in Objective C and uses Google Drive (and other public cloud hosting services) for C2 channels. And the malware is configured to communicate with its C2 server on working days to blend in with network traffic in the target environment. The Chinese APT group has been targeting Tibetan organizations and individuals since at least 2018.

Impact

- Data Loss
- File Encryption
- Financial Loss

Indicators of Compromise

MD5

- 23699799f496b8e872d05f19d2b397f8
- 66c52c5bc096e15d984ae12fa0589b2f

SHA-256

- 2a9296ac999e78f6c0bee8aca8bfa4d4638aa30d9c8ccc65124b1cbfc9caab5f
- b554bfe4c2da7d0ac42d1b4f28f4aae854331fd6d2b3af22af961f6919740234

SHA-1

- fe3a3e65b86d2b07654f9a6104c8cb392c88b7e8
- 038e6c73d7235d9942ba9f4cc48cf2626c940dc7

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.
