# GIMMICK (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:11:42 UTC

- Inventory
- Statistics
- Usage
- ApiVector
- Login

win.gimmick (Back to overview)

# GIMMICK

There is no description at this point.

### References

2023-08-18 · TEAMT5 · Still Hsu, Zih-Cing Liao
Unmasking CamoFei: An In-depth Analysis of an Emerging APT Group Focused on Healthcare Sectors in East Asia
CatB Cobalt Strike DoorMe GIMMICK

2022-03-22 · Volexity · Damien Cash, Steven Adair, Thomas Lancaster
Storm Cloud on the Horizon: GIMMICK Malware Strikes at macOS
GIMMICK GIMMICK

### Yara Rules

▶ [TLP:WHITE] win_gimmick_w0 (20230802 | Detects the base version of GIMMICK in .NET.)

▶ [TLP:WHITE] win_gimmick_w1 (20230802 | Detects the macOS port of the GIMMICK malware.)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.gimmick