PRIVATELOG (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:30:44 UTC

PRIVATELOG

Malware that abuses the Common Log File System (CLFS) to store/hide a second stage payload via registry transaction files.

References

2022-05-04 · Cybereason · Akihiro Tomita, Assaf Dahan, Chen Erlich, Daniel Frank, Fusao Tanida, Niv Yona, Ofir Ozer
Operation CuckooBees: A Winnti Malware Arsenal Deep-Dive
PRIVATELOG Spyder STASHLOG Winnti

2022-05-04 · Cybereason · Akihiro Tomita, Assaf Dahan, Chen Erlich, Daniel Frank, Fusao Tanida, Niv Yona, Ofir Ozer
Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques
PRIVATELOG Spyder STASHLOG Winnti

2021-09-03 · Twitter (@ESETresearch) · ESET Research
Twitter thread on SPARKLOG, a launcher component for PRIVATELOG along with STASHLOG
PRIVATELOG STASHLOG

2021-09-01 · FireEye · Adrien Bataille, Blaine Stancill
Too Log; Didn't Read — Unknown Actor Using CLFS Log Files for Stealth
PRIVATELOG STASHLOG

Yara Rules

▶ [TLP:WHITE] win_privatelog_w0 (20230119 | Detects possible hijack of legitimate prntvpt.dll based on missing export)

Download all Yara Rules

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