WINELOADER (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:58:24 UTC

win.wineloader (Back to overview)

WINELOADER

Actor(s): APT29

There is no description at this point.

References

2025-04-15 · Checkpoint · Checkpoint Research
Renewed APT29 Phishing Campaign Against European Diplomats
GRAPELOADER WINELOADER

2024-06-19 · ANSSI · ANSSI
Malicious activities linked to the Nobelium intrusion set
WINELOADER

2024-06-03 · Binary Defense · Binary Defense, Shannon Mong
Wineloader – Analysis of the Infection Chain
WINELOADER

2024-03-22 · Mandiant · Dan Black, Luke Jenkins
APT29 Uses WINELOADER to Target German Political Parties
WINELOADER

2024-03-02 · Twitter (@SinghSoodeep) · Sudeep Singh
Tweet on WINELOADER targeting with German embassy themed lure
WINELOADER

2024-02-27 · Zscaler · Roy Tay, Sudeep Singh
European diplomats targeted by SPIKEDWINE with WINELOADER
WINELOADER SPIKEDWINE

2024-02-27 · Twitter (@greglesnewich) · Greg Lesnewich

Tweet with context on TA421 / APT29 / Midnight Blizzard / BlueBravo / Cozy Bear

WINELOADER

There is no Yara-Signature yet.
