SerialVlogger (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:31:48 UTC

win.serialvlogger (Back to overview)

SerialVlogger

Actor(s): APT41

This malware is protected using VMProtect and related to the loading of KEYPLUG.

References

2020-10-12 · Malwarebytes Labs · Hossein Jazi, Jérôme Segura, Malwarebytes Threat Intelligence Team, Roberto Santos
Winnti APT group docks in Sri Lanka for new campaign
DBoxAgent SerialVlogger Winnti

There is no Yara-Signature yet.
