EASYNIGHT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:55:27 UTC

win.easynight (Back to overview)

EASYNIGHT

Actor(s): APT41

FireEye describes EASYNIGHT is a loader observed used with several malware families, including HIGHNOON and HIGHNOON.LITE. The loader often acts as a persistence mechanism via search order hijacking.

Examples include a patched bcrypt.dll with no other modification than an additional import entry, in the observed case "printwin.dll!gzwrite64" (breaking the file signature).

References

2019-09-04 · FireEye · FireEye
APT41: Double Dragon APT41, a dual espionage and cyber crime operation
EASYNIGHT Winnti

2017-03-22 · Trend Micro · Cedric Pernet
Winnti Abuses GitHub for C&C Communications
EASYNIGHT APT41

There is no Yara-Signature yet.
