ArguePatch (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:53:02 UTC

win.arguepatch (Back to overview)

ArguePatch

Actor(s): APT28, Sandworm

During a campaign against a Ukrainian energy provider, a new loader of a new version of CaddyWiper called "ArguePatch" was observed by ESET researchers. ArguePatch is a modified version of Hex-Ray's Remote Debugger Server (win32_remote.exe).
ArguePatch expects a decryption key and the file of the CaddyWiper shellcode as command line parameters.

References

2022-09-23 · Mandiant · Mandiant Intelligence
GRU: Rise of the (Telegram) MinIOns
ArguePatch CaddyWiper XakNet

2022-04-12 · ESET Research · ESET Research
Industroyer2: Industroyer reloaded
ArguePatch CaddyWiper Industroyer INDUSTROYER2

There is no Yara-Signature yet.

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