HTTPSnoop (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:05:52 UTC

win.httpsnoop (Back to overview)

HTTPSnoop

aka: TOFULOAD

Cisco Talos states that HTTPSnoop is a simple, yet effective, backdoor that consists of novel techniques to interface with Windows HTTP kernel drivers and devices to listen to incoming requests for specific HTTP(S) URLs and execute that content on the infected endpoint.

References

2023-09-19 · Cisco Talos · Arnaud Zobec, Asheer Malhotra, Caitlin Huey, Sean Taylor, Vitor Ventura
New ShroudedSnooper actor targets telecommunications firms in the Middle East with novel Implants
HTTPSnoop PipeSnoop LightBasin ShroudedSnooper

There is no Yara-Signature yet.
