Chisel (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 15:48:53 UTC

win.chisel (Back to overview)

Chisel

Chisel is an open-source project by Jaime Pillora (jpillora) that allows tunneling TCP and UDP connections via HTTP. It is available across platforms and written in Go. While benign in itself, Chisel has been utilized by multiple threat actors. It was for example observed by SentinelOne during a PYSA ransomware campaign to achieve persistence and used as backdoor.
Github: https://github.com/jpillora/chisel

References

2024-11-04 · Securonix · Den Iyzvyk, Tim Peck
CRON#TRAP: Emulated Linux Environments as the Latest Tactic in Malware Staging
Chisel

2022-09-12 · Arctic Wolf · Alex Ammons, Arctic Wolf Labs Team, Markus Neis, Ross Phillips, Steven Campbell, Teresa Whitmore
Chiseling In: Lorenz Ransomware Group Cracks MiVoice And Calls Back For Free
Chisel Lorenz

2022-04-18 · SentinelOne · James Haughom
From the Front Lines | Peering into A PYSA Ransomware Attack
Chisel Chisel Cobalt Strike Mespinoza

There is no Yara-Signature yet.
