PipeSnoop (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:40:57 UTC

win.pipesnoop (Back to overview)

PipeSnoop

aka: TOFUPIPE

Cisco Talos states that PipeSnoop can accept arbitrary shellcode from a named pipe and execute it on the infected endpoint.

References

2024-09-19 · Mandiant · Mark Lechtik, Matan Mimran, Sarah Bock, Stav Shulman
UNC1860 and the Temple of Oats: Iran’s Hidden Hand in Middle Eastern Networks
CRYPTOSLAY PipeSnoop TEMPLEDOOR UNC1860

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.
