

# MoonPeak (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:34:48 UTC

win.moonpeak ([Back to overview](#))

## MoonPeak

---

According to Cisco Talos, this RAT is derived from the open source XenoRAT.

### References

2024-08-21 · [Cisco Talos](#) · [Asheer Malhotra](#), [Guilherme Venere](#), [Vitor Ventura](#)

MoonPeak malware from North Korean actors unveils new details on attacker infrastructure

[MoonPeak XenoRAT UAT-5394](#)

There is no Yara-Signature yet.

---

---

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.moonpeak>