MoonPeak (Malware Family)

By Fraunhofer FKIE

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.
