PNGLoad (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:41:59 UTC

PNGLoad

According to ESET Research, PNGLoad is a second-stage payload deployed by Worok on compromised systems and loaded either by CLRLoad or PowHeartBeat. PNGLoad has capabilities to download and execute additional payloads from a C&C server, which is likely how the attackers have deployed PNGLoad on systems compromised with PowHeartBeat. PNGLoad is a loader that uses bytes from PNG files to create a payload to execute. It is a 64-bit .NET executable - obfuscated with .NET Reactor - that masquerades as legitimate software.

References

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.png_load