

# Malware Analysis - Agniane Stealer, Native Stub to .NET Unpacking

Published: 2023-08-19 · Archived: 2026-04-05 18:42:35 UTC

We trace API calls of a packed native file using hasherezade's tiny\_tracer and discover that it unpacks a .NET payload. Using x64dbg we unpack the .NET assembly and find it unreadable, among others due to dr4k0nia's XOR string obfuscation. ...

...mer

---

Source: <https://www.youtube.com/watch?v=-KJ0HlvmV10>