

# Analyzing and Unpacking Qakbot Using Binary Ninja Automation

## Part 2

Published: 2024-02-09 · Archived: 2026-04-05 16:49:30 UTC

In this stream we continued the development of our static unpacker using Binary Ninja scripting. We then used pefile and Binary Refinery to extract the final Qakbot payload. We then stumbled across an advanced payload that we extracted using our unpacker that used indirect syscalls, that we began to analyze using binary ninja, and eventually unpacked the final PE dynamically. ...

...mer

---

Source: <https://www.youtube.com/watch?v=utqaGgnb5yM>