UNPACK

Công cụ chính: DIE - Detect It Easy, CFF Explorer, x32dbg (Scylla), Resource Hacker (import resource)
Một số thao tác chung:

- Detect loại packer (DIE)
    - Unpack1: UPX packer
    - Unpack2: Petite 2.X
    - Unpack3: ASPack 2.12-2.42
    - Unpack4: FSG 2.0, chạy trên Win 7
    - Unpack5: MPRESS2.19
    - Unpack6: VMProtected
    - Unpack7: FSG-Win XP
    - Unpack8: ASProtect 1.23-2.56
- Cấp quyền chạy cho section (CFF Explorer)
- Run script trên x32dbg
- Dump, import IAT, fix dump file (Scylla)

Unpack1

Sử dụng CFF để unpack

Unpack2,3,4,5

Thủ thuật tìm OEP: pushad popad
Break point hardware tại esp address, chạy để tìm OEP (dựa vào đặc điểm nhận dạng) / sử dụng script.

Unpack6

Đoạn chương trình chính (chứ OEP) được sinh ra bằng VirtualProtect (chạy 17 lần để sinh hết). Sử dụng script để tìm OEP (hoặc mò tay :)))).
Pattern: ***"E8 ?? ?? ?? ?? "***.
File được dump bị thiếu resource Dialog; sử dụng Resource Hacker để import resource từ file gốc.

Unpack7

Sử dụng ***attack*** trong x32dbg để bỏ qua các phần anti debug.
Tìm OEP bằng cách tìm pattern ***"E8 ?? ?? ?? ?? E9"*** trong section đầu tiên. Ghi nhớ OEP của chúng ta :> (đặt breakpoint luôn cho lẹ :<).
Để anti các antidebug dùng ScyllaHide, rồi tìm đến OEP đã nhớ địa chỉ từ bước trước nếu chưa đặt breakpoint :< . Nhanh chóng chạy và dump file.

Unpack8

Run đến VirtualFree
Run script chờ em nó tìm OEP hộ :<