Final Project in NT230 course – Malware's Modus Operandi

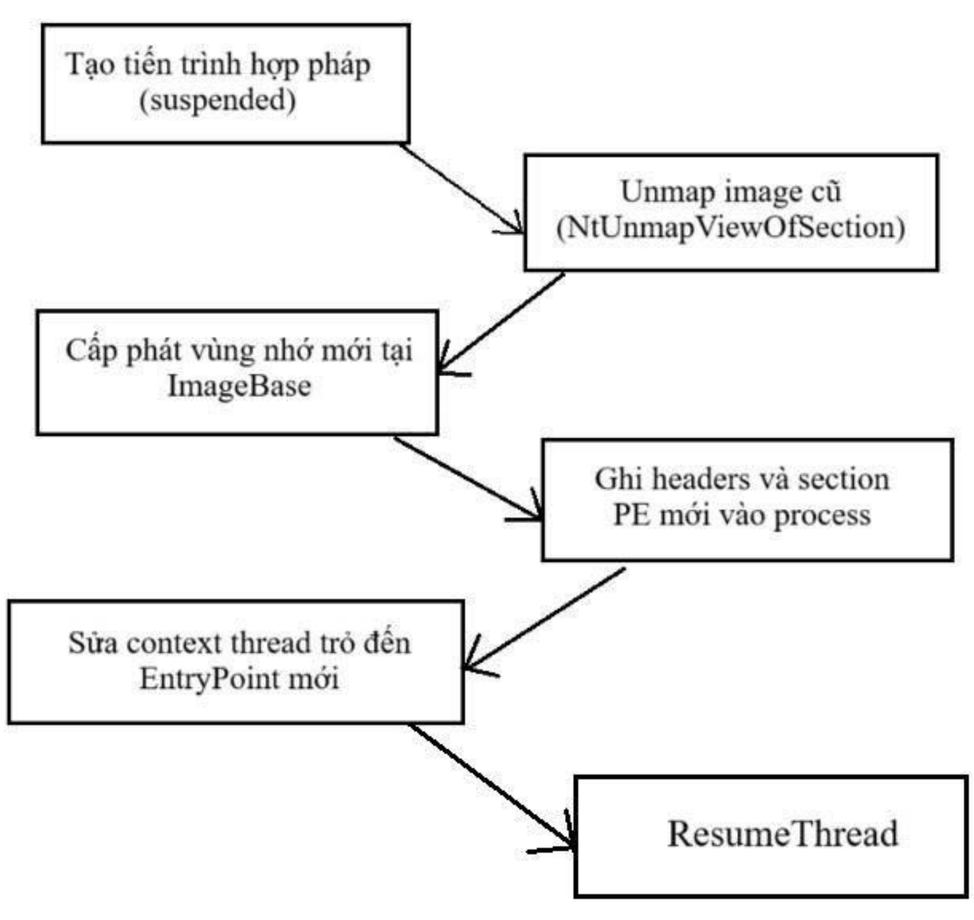
PROCESS HOLLOWING

Thành viên nhóm: Tôn Thất Bình (21520639) - Nguyễn Văn Hào (20521293) - Phạm Trần Hiếu (21520236) - Đặng Quốc Hưng (21520882)

Mã nhóm: CK17, Mã đề tài: S10

Tổng quan

Process Hollowing là kỹ thuật cho phép kẻ tấn công thực thi mã độc trong một tiến trình hợp pháp bằng cách tạo process ở trạng thái suspended, hollow/unmap bộ nhớ rồi ghi mã độc vào, sau đó resume.



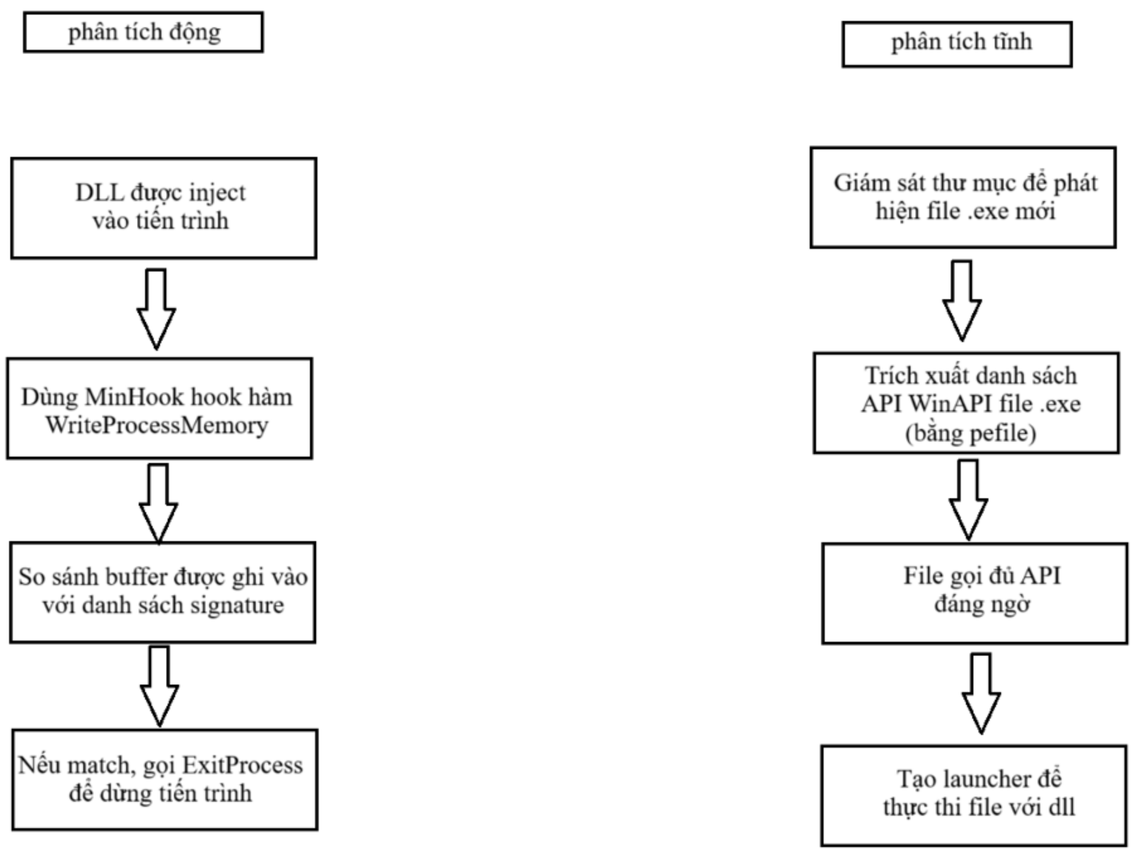
A. Mô phỏng tấn công

1. Tạo tiến trình nạn nhân ở trạng thái suspended
2. Giải phóng vùng nhớ image gốc của tiến trình nạn nhân sử dụng NtUnmapViewOfSection
3. Cấp phát vùng nhớ mới trong tiến trình nạn nhân bằng VirtualAllocEx
4. Ghi header và section của file PE độc hại vào tiến trình nạn nhân bằng WriteProcessMemory
5. Sửa context của thread chính trỏ tới entry point mới bằng Get/SetThreadContext
6. Khởi chạy tiến trình với mã mới bằng ResumeThread

B. Bypass Windows Defender

- Dynamic API resolution: Dùng GetProcAddress để lấy địa chỉ hàm tại runtime, tránh bị phát hiện qua bảng import.
- Memory-only injection: Tạo tiến trình hợp pháp (vd. notepad.exe) ở trạng thái suspended, ghi shellcode mã hóa vào memory, chỉ giải mã khi thực thi.
- XOR shellcode: Payload được XOR, giải mã tại runtime trong memory, tránh bị nhận diện tĩnh.
- Không drop file/process lạ: Toàn bộ hoạt động diễn ra trong memory tiến trình hợp pháp, giảm dấu vết trên đĩa.

C. Giám sát và Phát hiện



KẾT LUẬN

- Đã thực thi mã độc thành công trong vỏ bọc của một tiến trình hợp pháp, không sinh process lạ
- Đã phát hiện và ngăn chặn process hollowing thành công thông qua phân tích API được gọi và hook WriteProcessMemory
- Đã có thể né tránh phát hiện của window defender thành công

Hướng phát triển

- Kết hợp thêm sandbox phân tíchgiúp phát hiện các tiến trình có vỏ bọc hợp pháp nhưng hành vi thực hiện nguy hiểm.
- Kết hợp thêm kỹ thuật anti-vm, anti debug, anti hook giúp né tránh phát hiện tốt hơn