Trường Đại học Công nghệ Thông tin (UIT)
Đại Học Quốc Gia Tp. HCM

BÀI TẬP 01

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: **Encrypted Virus**

Mã môn học: NT230

Học kỳ 2 - Năm học: 2023-2024

1. NỘI DUNG THỰC HIỆN

Virus mã hóa là dạng Vi-rút thực hiện mã hóa payload để trốn tránh kỹ thuật phân tích tĩnh trong nhận diện, xác định vi-rút. Tuy nhiên, để gia tăng cơ hội trốn tránh sự phát hiện của các trình nhận diện vi-rút đang dựa trên các dấu hiệu xác định trước (signature) hoặc mẫu xác định trước (code pattern), kỹ thuật tạo biến thể có thể được phát triển bên trong một chương trình độc hại. Ba dạng chính của kỹ thuật tạo biến thể vi-rút bao gồm: Oligomorphic (Dị hình), Polymorphic (Đa hình), Metamorphic (Siêu hình).

Yêu cầu thực hiện

Viết chương trình lây nhiễm virus vào tập tin thực thi (tập tin thực thi trên Windows – PE file 32 bits) có tính năng đơn giản (mục đích demo giáo dục) như yêu cầu bên dưới.

- Về chức năng, mục đích của payload (sử dụng lại phần virus cơ bản của bài tập 01):
  - Hiển thị thông điệp ra màn hình thông qua cửa sổ "pop-up" với tiêu đề cửa sổ là "Infection by NT230" và cấu trúc thông điệp là "MSSV01_MSSV02_MSSV03" (thông tin MSSV của các thành viên trong nhóm).
  - Hoàn trả chức năng gốc ban đầu của chương trình bị lây nhiễm (không phá hủy chức năng của chương trình vật chủ).
- ***Về khả năng trốn tránh việc phát hiện:***
  - Yêu cầu 01: Hiện thực virus mã hóa (encrypted virus) dùng kỹ thuật XOR.
  - Yêu cầu 02: Thực hiện tạo biến thể mã độc bên trên dùng 01 trong 03 kỹ thuật: Oligomorphic, Polymorphic, Metamorphic.

2. GỢI Ý – THAM KHẢO

Một số gợi ý thực hiện:

– Tham khảo bài giảng môn học

- Có thể dùng Python và thư viện pefile để tạo cơ chế lây nhiễm vào tập tin mục tiêu đầu tiên. Hoặc viết chương trình bằng ngôn ngữ C/C++ để tương tác lây nhiễm payload vào trong file đối tượng mục tiêu đầu tiên.
- Writing and Compiling Shellcode in C: https://www.ired.team/offensive-security/code-injection-process-injection/writing-and-compiling-shellcode-in-c
- Import Adress Table (IAT) Hooking: https://www.ired.team/offensive-security/code-injection-process-injection/import-adress-table-iat-hooking
- Fighting EPO Viruses – Endpoint Protection (Broadcom):

  https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=a86ba621-9fa1-4c0e-83c4-8833e80ecb08&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
- Process Injection: Process Hollowing:

  https://attack.mitre.org/techniques/T1055/012/
- Process Hollowing and Portable Executable Relocations:

  https://www.ired.team/offensive-security/code-injection-process-injection/process-hollowing-and-pe-image-relocations

---

Sinh viên đọc kỹ qui định, yêu cầu trình bày chung bên dưới trang này.

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, bao gồm: nguyên tắc hoạt động kèm lí giải, phân tích; quan sát thấy và kèm ảnh chụp màn hình kết quả cho các bước chi tiết (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT