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

BÀI TẬP 02

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: **File Infecting Virus**

Mã môn học: NT230

Học kỳ 2 - Năm học: 2023-2024

1. NỘI DUNG THỰC HIỆN

Vi-rút lây nhiễm tệp (file infecting virus) là một loại phần mềm độc hại lây nhiễm vào các tệp thực thi với mục đích gây ra thiệt hại vĩnh viễn hoặc khiến chúng không thể sử dụng được. Vi-rút lây nhiễm tệp sẽ ghi đè mã hoặc chèn mã bị nhiễm vào tệp thực thi. Tệp lây nhiễm vi-rút hay còn gọi là virus lây nhiễm qua tập tin, thường sao chép mã của chúng vào các chương trình thực thi như tập tin .COM và .EXE, v.v.

Hầu hết các phần mềm lây nhiễm tập tin chỉ đơn giản là sao chép và lây lan, nhưng một số lại vô tình làm hỏng các chương trình máy chủ lưu trữ. Ngoài ra còn có những virus lây nhiễm qua tập tin ghi đè lên các tập tin máy chủ lưu trữ nhằm phá hủy. Các phần mềm độc hại dựa trên cơ chế lây nhiễm vào tập tin có nhiều dạng payload khác nhau từ loại có khả năng phá hủy cao (chẳng hạn như định dạng lại ổ cứng), đánh cắp thông tin người dùng và trốn tránh việc phát hiện (sử dụng các kỹ thuật ẩn giấu tinh vi để che giấu sự tồn tại), hoặc lành tính (chẳng hạn như hiển thị thông báo ra màn hình máy tính nạn nhân).

Yêu cầu thực hiện

Yêu cầu 01: Trình bày hiểu biết của em về các kỹ thuật làm rối mã cơ bản, được liệt kê trong buổi 06. Ví dụ minh hoạ về các kỹ thuật đó.

Yêu cầu 02: 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:

- 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 "**MSSV1-MSSV2-MSSV3".** Lưu ý: không có dấu "".
- Hoàn trả chức năng gốc ban đầu của chương trình bị lây nhiễm (không phá hủy chức năng của chương trình vật chủ).
- Tóm lại: một tập tin bị nhiễm virus sẽ in ra thông điệp khi người dùng kích hoạt chương trình, cố gắng lây nhiễm sang tập tin khác trong cùng thư mục, rồi thực

thi chức năng ban đầu của tập tin. Đối với việc lây nhiễm sang một tập tin khác, nếu đối tượng là một tập tin đã bị nhiễm, chương trình virus sẽ bỏ qua. Nếu đối tượng là tập tin không bị nhiễm, hoạt động lây nhiễm payload vào tập tin thực thi sẽ được kích hoạt.

Về cách lây nhiễm:

- *Mức yêu cầu 01 - RQ01 (5đ):*
  - Trình bày được khái niệm về các kỹ thuật làm rối mã và cho ví dụ minh hoạ.
  - Thực hiện chèn mã độc vào process bình thường bằng kỹ thuật process hollowing hoặc sử dụng section .reloc trong tập tin thực thi để tiêm payload của virus.
- Mức yêu cầu 02 - RQ02 (2đ): Virus đạt được như yêu cầu RQ01 và có khả năng lây nhiễm qua các file thực thi khác cùng thư mục khi người dùng kích hoạt tập tin vật chủ.
- *Mức yêu cầu 03 - RQ03 (3đ):* Thay vì thay đổi Entry-point của chương trình, Hãy áp dụng lần lượt 02 chiến lược lây nhiễm trong nhóm kỹ thuật Entry-Point Obscuring (EPO) virus – che giấu điểm đầu vào thực thi của mã virus (virus code) cho Virus đã thực hiện ở RQ01/RQ02. Một số dạng EPO-virus có thể xem xét để thực hiện yêu cầu này bao gồm:
  - Call hijacking EPO virus
  - Import Address Table-replacing EPO virus.
  - TLS-based EPO virus.

2. GỢI Ý – THAM KHẢO

Một số gợi ý thực hiện:

– Tham khảo bài giảng môn học và các tài liệu tham khảo được trích dẫn.

– 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/offensivesecurity/code-injection-process-injection/writing-and-compiling-shellcode-in-c

– Import Adress Table (IAT) Hooking: https://www.ired.team/offensivesecurity/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-processinjection/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).
- Nộp báo cáo theo deadline được giao.

Báo cáo:

- File .PDF. Tập trung vào nội dung và yêu cầu được giao.
- 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_MSSV1_MSSV2.

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_20129212_21029282..*
- 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