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

BÀI TẬP 02

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: **Advanced Virus Techniques**

Mã môn học: NT230 - Modus Operandi of Malware

Học kỳ 2 - Năm học: 2022-2023

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).

Ngoài ra, một số virus cũng có thể trang bị cho mình các kỹ thuật nhận diện môi trường chạy (environmental keying) hay các kỹ thuật chống phân tích động (anti-VM/anti-sandbox) để tránh việc "hiện nguyên hình" trên môi trường giả lập (máy ảo (Virtual machine - VM), hộp cát cô lập (sanboxing)) của các nhà khoa học phân tích mã độc. Các kỹ thuật chống phân tách (anti-disassembly), hay chống gỡ lỗi (anti-debugger) cũng đóng một vai trò quan trọng trong các nguyên lý hoạt động của các chương trình virus phức tạp. Điều này hướng tới việc trốn tránh các trình nhận diện vi-rút, làm gia tăng công sức và tiêu tốn thời gian hơn của người phân tích, xác định mã độc. Việc hiểu được các nguyên lý này cho phép các kỹ thuật viên phân tích chương trình phần mềm độc hại có giải pháp tổ chức, phối hợp các kỹ thuật với nhau một cách hiệu quả để điều tra, xác định hành vi hay nhận biết các chương trình độc hại.

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). 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).

Về khả năng trốn tránh việc phát hiện:

a) Tìm hiểu nguyên lý phát hiện sandbox (thí dụ như Cuckoo Sandbox,…).
Hiện thực lại mã độc chống phân tích động (trang bị thêm cho payload ban đầu) khả năng nhận biết môi trường (environmental sensivity):
   + Chạy trong môi trường máy ảo,
   + Chạy trong môi trường sandbox,
   + Có khả năng phát hiện đang bị gỡ lỗi (debugging),

Một khi nhận biết đang bị đặt trong môi trường phân tích, nó sẽ không thực hiện hành vi, không thể hiện bản chất của mình (vd: payload không thực thi đoạn mã mục tiêu cho trước, dừng chương trình…).
Các nhóm sinh viên chọn 2 cách thức khác nhau trong mỗi kỹ thuật anti-debugging, anti-VM và anti-sandbox để hiện thực tính năng trên.

b) Hiện thực virus mã hóa (encrypted virus) dùng kỹ thuật XOR.

Lưu ý:

+ *Sinh viên chương trình Tài năng thực hiện* ***tất cả các yêu cầu a, b.***
+ *Sinh viên chương trình Đại trà, Chất lượng cao thực hiện* ***yêu cầu a.***

2. GỢI Ý – THAM KHẢO

Một số gợi ý thực hiện:

– Tham khảo bài giảng môn học

– Writing and Compiling Shellcode in C: https://www.ired.team/offensive-security/code-injection-process-injection/writing-and-compiling-shellcode-in-c

– Environmental Keying: https://attack.mitre.org/techniques/T1480/001/#:~:text=Environmental%20keying%20may%20be%20used,decrypt%20the%20payload%20before%20execution.

– Anti-debugger: https://www.apriorit.com/dev-blog/367-anti-reverse-engineering-protection-techniques-to-use-before-releasing-software

– Anti-debugging and anti-VM techniques and anti-emulation: https://resources.infosecinstitute.com/topic/anti-debugging-and-anti-vm-techniques-and-anti-emulation/

– Detecting Malware and Sandbox Evasion Techniques: https://sansorg.egnyte.com/dl/j0Svu3JMja

– Sandbox detection and evasion techniques. How malware has evolved over the last 10 years: https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/

- Malware Sandbox Evasion: Techniques, Principles & Solutions: https://www.apriorit.com/dev-blog/545-sandbox-evading-malware
- CATCH ME IF YOU CAN!—DETECTING SANDBOX EVASION TECHNIQUES : https://www.usenix.org/conference/enigma2020/presentation/guibernau
- Evolution of Malware Sandbox Evasion Tactics – A Retrospective Study : https://www.mcafee.com/blogs/other-blogs/mcafee-labs/evolution-of-malware-sandbox-evasion-tactics-a-retrospective-study/
- Anti-VM and Anti-Sandbox Explained: https://www.cyberbit.com/blog/endpoint-security/anti-vm-and-anti-sandbox-explained/

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 .DOCX và .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