Đại Học Quốc Gia Tp. HCM

Trường Đại học Công nghệ Thông tin (UIT)

BÀI TẬP 03

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: **Hijacking Execution Techniques**

Mã môn học: NT230 - Modus Operandi of Malware

Học kỳ 2 - Năm học: 2023-2024

1. NỘI DUNG THỰC HIỆN

Các kỹ thuật hijacking được các nhóm tin tặc, kẻ tấn công sử dụng rất phổ biến và có mặt hầu hết ở các báo cáo phân tích về mã độc. Việc hiểu được các kỹ thuật hijacking là rất quan trọng trong việc phân tích hành vi và phát hiện mã độc. Cho đến hiện tại, có rất nhiều kỹ thuật hijacking khác nhau, nhằm vượt qua sự phát hiện của các AV, kẻ tấn công đã xây dựng nhiều phương pháp độc đáo, với rất nhiều kỹ thuật vượt trội. Theo MITRE ATT&CK, nhóm các kỹ thuật này có ID: T1574, và các kỹ thuật con được liệt kê đều có các yếu tố nâng cao về mặt kỹ thuật. Việc hiểu biết về kỹ thuật này và dựng lại các lab để phân tích là rất quan trọng.

Yêu cầu thực hiện

Tìm hiểu một trong các kỹ thuật được liệt kê tại MITRE ATT&CK: https://attack.mitre.org/techniques/T1574/. Yêu cầu các nhóm trình bày lại bằng tiếng việt về kỹ thuật được chọn. Mô tả rõ cách thức triển khai, demo lại bằng cách lập trình C/C++ hoặc ngôn ngữ tương tự. Xây dựng lab sử dụng máy ảo Windows 10/11 (Tắt Windows Defender).

Yêu cầu:

- Hiểu và mô tả rõ ràng về mặt lý thuyết kỹ thuật được chọn. (2 điểm)

- Vận dụng lý thuyết để lập trình mã độc (định dạng DLL hoặc tương tự kỹ thuật được chọn) và xây dựng lab đơn giản trên máy ảo Windows 10/11 (Tắt Windows Defender). (3 điểm)

- Chức năng của mã độc: Mở một tiến trình có sẵn trên máy: notepad.exe, calc.exe,... (2 điểm)

- Chức năng nâng cao:

  - Mã độc có thể tự khởi chạy khi máy tính được mở lại. (2 điểm)
  - Có khả năng lẩn tránh Windows Defender (Trên máy ảo Windows 10/11 không tắt Windows Defender). (1 điểm)

Lưu ý:

- Việc thực hiện bài tập này nhằm hiểu biết rõ hơn về các kỹ thuật được các nhóm tin tặc và kẻ tấn công sử dụng. Không nhằm mục đích tấn công hay mang yếu tố xấu, ảnh hưởng đến người khác, mọi hành vi chia sẻ, phát tán công khai có thể vi phạm Luật An ninh mạng Việt Nam, lưu ý các nhóm phải bảo mật mã nguồn và chỉ sử dụng trong phạm vi môn học này tránh các rủi ro khác.

- Việc thực hiện lẩn tránh Windows Defender trên Windows 10/11 là một hành vi nguy hiểm, các nhóm lưu ý thực hiện trên máy ảo, có snapshot máy ảo trước khi chạy mã độc và revert lại khi bị phát hiện, có thể gửi mail cho thầy để tham khảo thêm ý kiến.

- Nộp bài theo yêu cầu ở trang cuối, nếu không tuân thủ sẽ coi như không làm.

2. GỢI Ý – THAM KHẢO

Một số gợi ý thực hiện:

- https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/dll-hijacking
- https://elliotonsecurity.com/perfect-dll-hijacking/#new-techniques
- https://unit42.paloaltonetworks.com/dll-hijacking-techniques
- https://hijacklibs.net/
- https://attack.mitre.org/techniques/T1574/
- https://www.mandiant.com/resources/blog/abusing-dll-misconfigurations
- https://juggernaut-sec.com/dll-hijacking/
- https://www.ired.team/offensive-security/privilege-escalation/t1038-dll-hijacking
- https://cocomelonc.github.io/pentest/2021/09/24/dll-hijacking-1.html

---

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**) đã thực hiện theo yêu cầu và tương tự các bài tập trước
- Sinh viên báo cáo kết quả thực hiện và nộp bài theo deadline.

Báo cáo:

- File.PDF. Tập trung vào trọng tâm được yêu cầu.
- 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_MSSV.

  *Ví dụ: [*NT101.K11.ANTT*]-Exe03_20192821.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP kèm với thư mục source code với cùng tên file báo cáo.

– Đặt mật khẩu cho file nén có chứa source code bên trong và có readme đầy đủ mô tả code và comment trong code. Source code không chứa các folder x64, .vs, debug, ... gây nặng và không cần thiết.

– Nộp file báo cáo trên theo thời gian đã đặt tại courses.uit.edu.vn.

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

HẾT