Trường ĐH Công nghệ Thông tin –
ĐHQG TP. HCM

Cơ chế hoạt động của mã độc

NT230 – Malware's Modus Operandi

NT230 - Malware's Modus Operandi

WELCOME
BACK
AND
GOOD LUCK
THIS SEMESTER

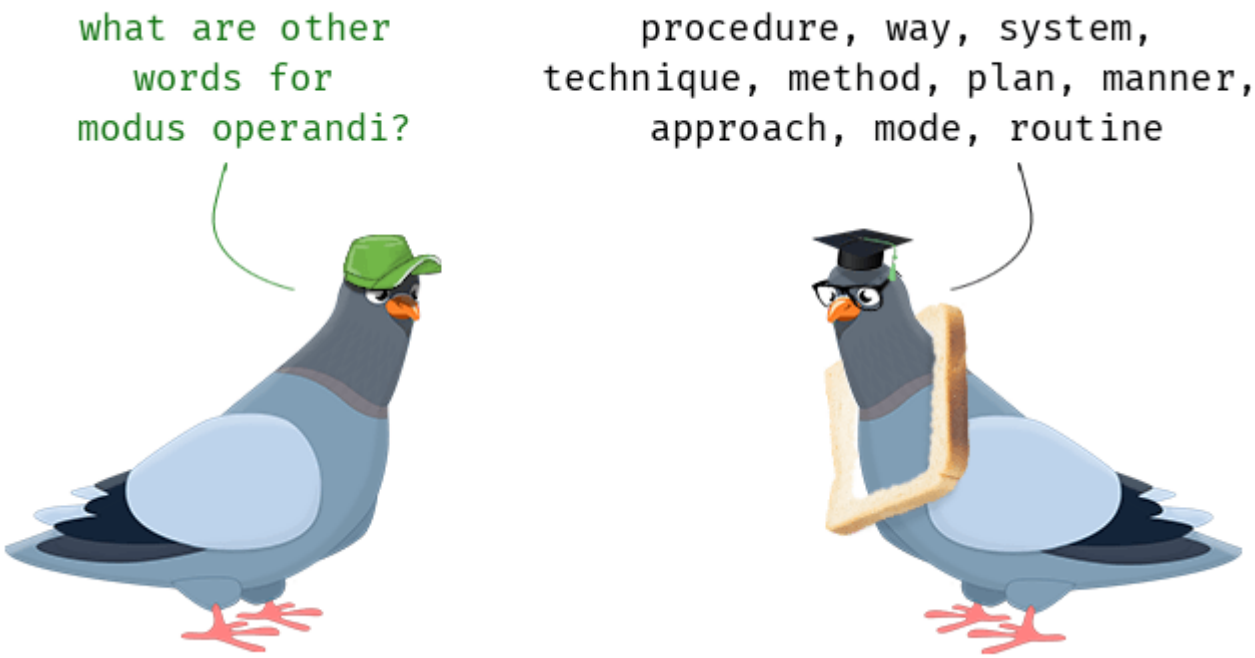
NT230 - Cơ chế hoạt động của mã độc

Bài giảng lý thuyết – 02.2023
Email: duypt@uit.edu.vn

Buổi 01 - Giới thiệu nội dung

- **Giảng viên lý thuyết:**
  - TS. Phạm Văn Hậu
  - ThS. Phan Thế Duy
- **Giảng viên thực hành:**
  - KS. Đoàn Minh Trung
  - CN. Nguyễn Hữu Quyền
  - ThS. Nghi Hoàng Khoa

Tổng quan


what are other words for modus operandi?
procedure, way, system, technique, method, plan, manner, approach, mode, routine


MALWARE

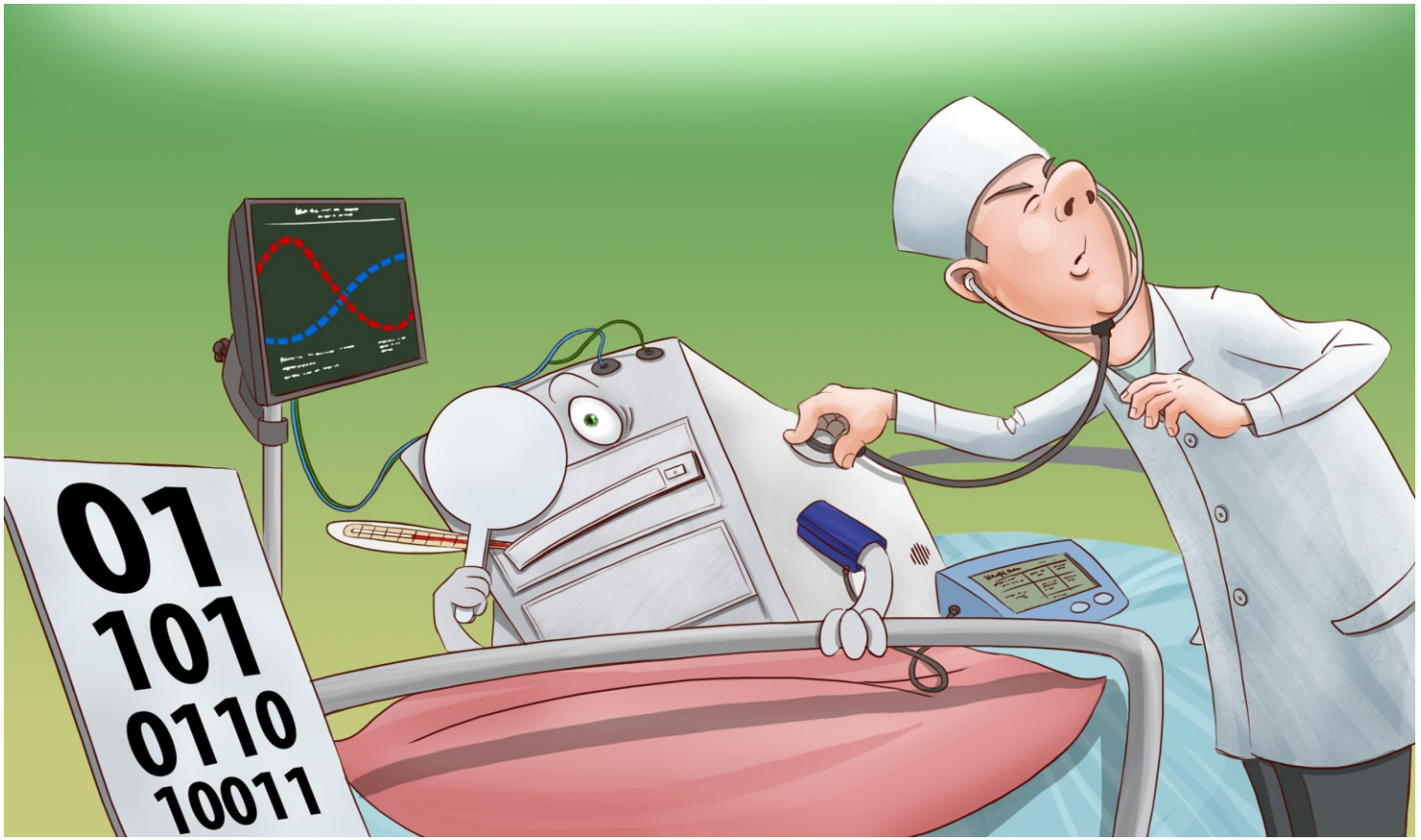
Khảo sát kiến thức

Mã độc (Malware) là gì?

Khảo sát kiến thức

Các nguyên nhân bị lây nhiễm mã độc?

Khảo sát kiến thức

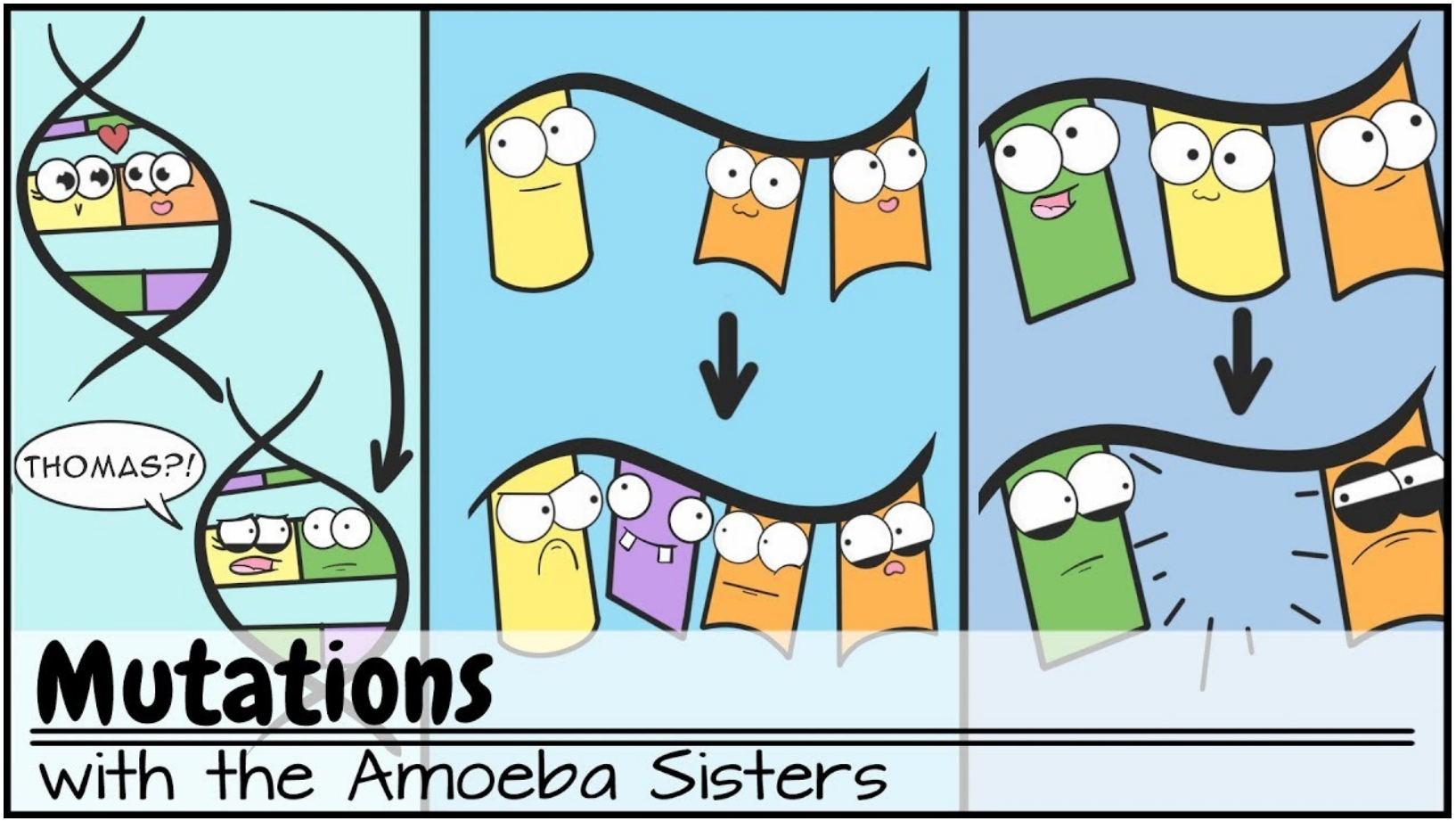


Các dấu hiệu bị lây nhiễm mã độc?

Khảo sát kiến thức

Các thể loại của mã độc?

Khảo sát kiến thức



Phương pháp biến đổi của mã độc đột biến?

Khảo sát kiến thức

Phương pháp nào giúp xác định, phân tích và ngăn chặn, loại bỏ mã độc?

Khảo sát kiến thức

- Mã độc
- Virus máy tính
- Sâu máy tính (worm)
- Phần mềm lừa đảo
- Rootkit
- Macro virus
- Mã độc đột biến

- Botnet
- Hoạt động & cơ chế lây nhiễm của mã độc
- Cơ chế trốn tránh phát hiện

Mục tiêu

- **Mục tiêu:**

  Trang bị những kiến thức cơ bản về cơ chế hoạt động của các loại mã độc, phần mềm độc hại, virus máy tính.

Nội dung môn học (2016-2021)

- Các khái niệm tổng quan về mã độc máy tính
- Cấu trúc tập tin thực thi (PE- Portable Exe)
  - Virus máy tính
  - Chèn payload
- Khai thác:
  - Stack overflow
  - Format String
- Sâu máy tính (worm)
- Rootkit
- Các kỹ thuật mã hóa, rối mã, đột biến của virus
- Khai thác:
  - ARC injection
  - Tấn công ROP (Return-oriented programming)
  - Off-by-one

Nội dung môn học (2022)

- Các khái niệm tổng quan về mã độc máy tính
- Cấu trúc tập tin thực thi (PE- Portable Exe)
  - Virus máy tính
  - Chèn payload
- Sâu máy tính (worm), Botnet
- Các kỹ thuật mã hóa, rối mã (obfuscation) của mã độc
  - Encrypted/packed virus: Packing/unpacking, Decryptor, Protector
  - Đột biến mã độc: Polymorphic (Đa hình), Oligomorphic (Dị hình), Metamorphic (Siêu hình)
- Các kỹ thuật chống phân tích, chống phát hiện:
  - Anti-Disassembly
  - Anti-Debugging
  - Anti-VM & Anti-Sandbox
- Rootkit:
  - Kernel basics & Kỹ thuật cơ bản của Rootkit
  - Rootkit Anti-Forensics & Covert Channel
- Các phương pháp trốn tránh cơ chế phát hiện tự động:
  - Anti-Anti Virus (Anti-AV)
- Các loại mã độc trên nền tảng khác: Android, macro,…

Nội dung môn học (2023)

- Các khái niệm tổng quan về mã độc máy tính
- Cấu trúc tập tin thực thi (PE- Portable Exe) + Windows Internal
- Virus máy tính
  - Định nghĩa, khái niệm về virus máy tính
  - Một số dạng virus lây nhiễm qua tập tin: Chèn payload (Code and Process Injection), DLL Injection, Process Hollowing, …
- Sâu máy tính (worm), Botnet
- Các kỹ thuật mã hóa (encrypted), rối mã (obfuscation) của mã độc
  - Encrypted/packed virus: Packing/unpacking, Decryptor, Protector
  - Đột biến mã độc: Polymorphic (Đa hình), Oligomorphic (Dị hình), Metamorphic (Siêu hình)

Nội dung môn học (2023)

- Các kỹ thuật chống phân tích, chống phát hiện (Armoring Techniques):
  - Anti-Disassembly
  - Anti-Debugging
  - Anti-VM & Anti-Sandbox
- Các phương pháp trốn tránh cơ chế phát hiện tự động (Evasion Technique):
  - Anti Virus Evasion
  - Network IDS Evasion
  - Sandbox Evasion
- Mã độc phi mã (Fileless Malware)
- Stealth & Rootkit:
  - Kernel basics & Kỹ thuật cơ bản của Rootkit
  - Rootkit Anti-Forensics & Covert Channel
- Các loại mã độc trên nền tảng khác: Android, Macro, Image, Brower Hijacking,…

Đánh giá môn học: Quá trình

Bài tập, các chủ đề nâng cao

- Quiz: các câu hỏi về nội dung bài học (cá nhân)
- Assignment: 05 bài tập (nhóm/cá nhân)
- Project (đồ án): 01 chủ đề seminar (nhóm)

Đánh giá môn học: Thực hành

6 buổi thực hành về các nội dung liên quan

- Làm theo nhóm đồ án đã đăng ký
- Tất cả các thành viên đều tham gia

Đánh giá môn học: Cuối kỳ

Cách đánh giá bao gồm:

- Thi lý thuyết (Trắc nghiệm + Tự luận): 90 phút
  - Tự luận: (4đ)
    - ✓ Kiến thức cơ bản và vận dụng: **02 câu**
    - ✓ Mô tả đồ án môn học: **01 câu**
  - Trắc nghiệm (6đ): **40 câu hỏi** (4 lựa chọn)

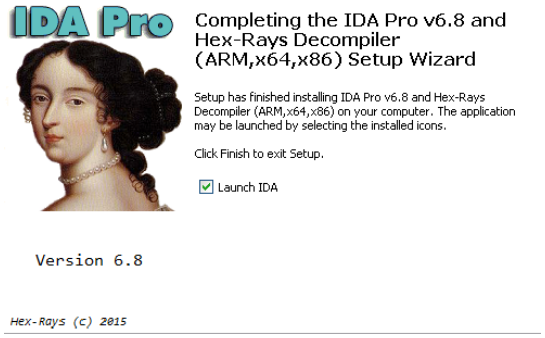
Yêu cầu

- Đến lớp đúng giờ
- Tìm hiểu trước bài giảng + Tích cực thảo luận
- Bài tập + câu hỏi trên lớp + Challenge: Điểm quá trình **(30%)**
- Cuối kỳ: **40%**
- Làm nhóm (đối với thực hành): (30%)
  - Không ghi nhóm → sao chép
  - GV hỏi bất kỳ thành viên

Các công cụ hỗ trợ

- IDA Pro
- OllyDBG
- …..

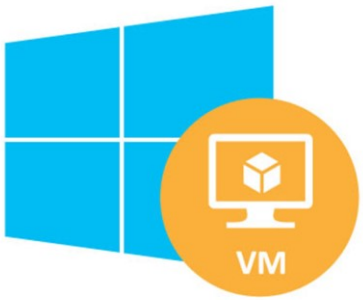
- Ghidra
- WinDbg
- …..



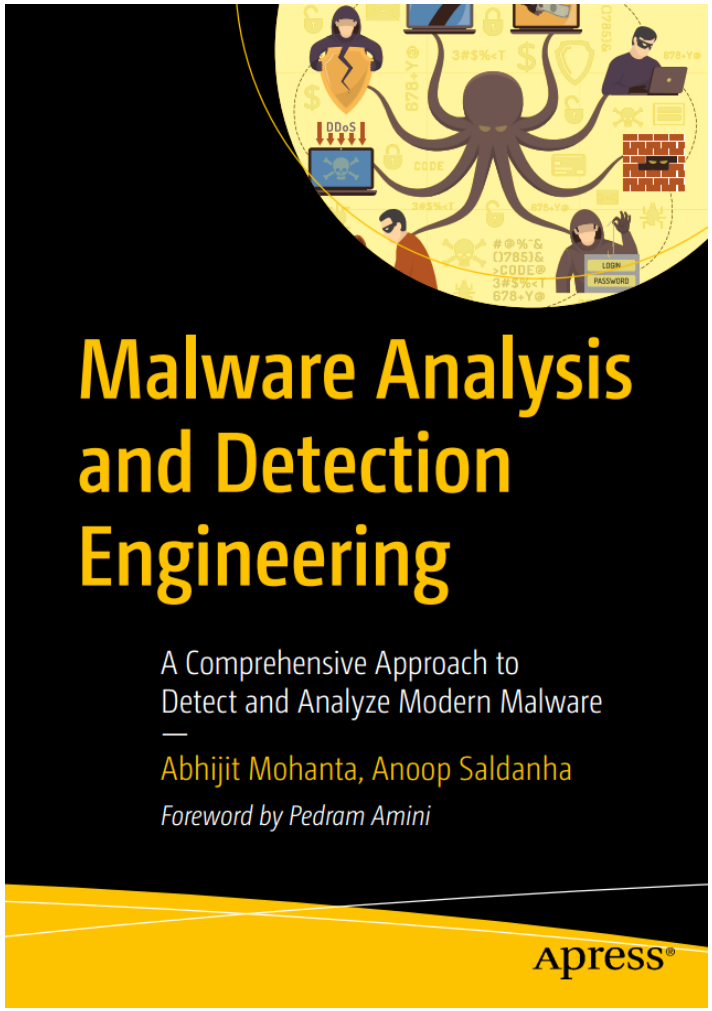
OllyDbg

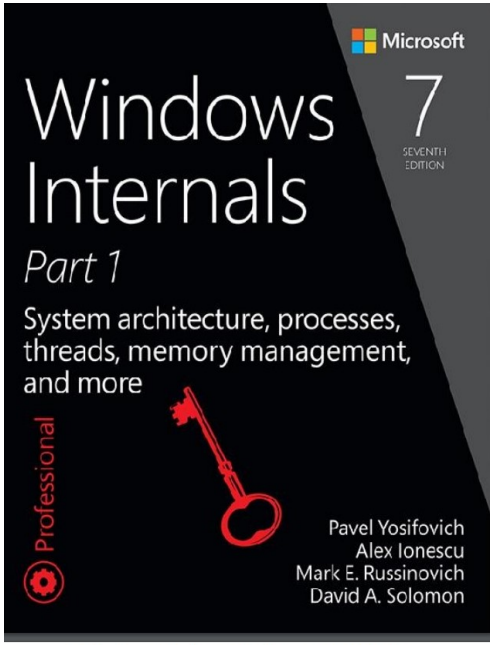
Lưu ý

- Cài đặt các công cụ hỗ trợ trên máy ảo
- Cảnh giác với các phần mềm, công cụ phiên bản crack
- Thực hiện các thao tác, chỉnh sửa mã độc trên máy ảo
- **KHÔNG NÊN** sử dụng môi trường máy thật cá nhân.
  - FLARE VM - The Windows Malware Analysis Distribution

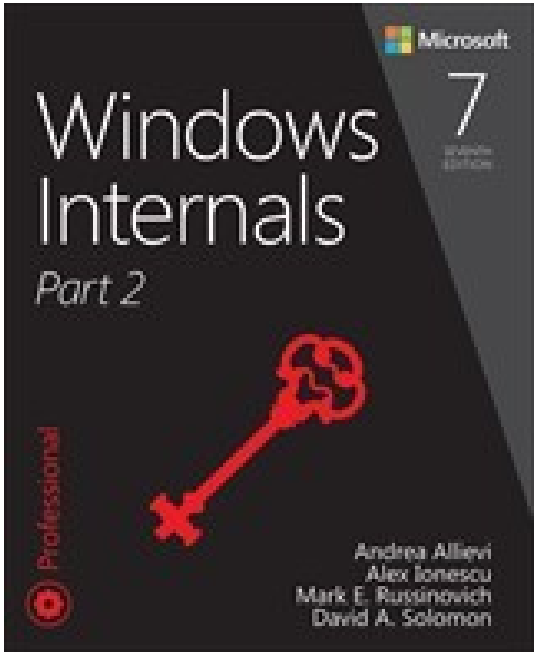


Tài liệu tham khảo

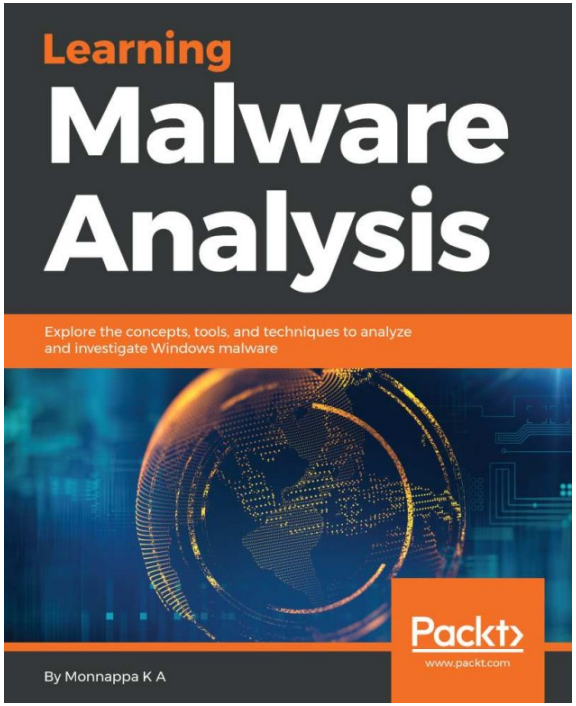


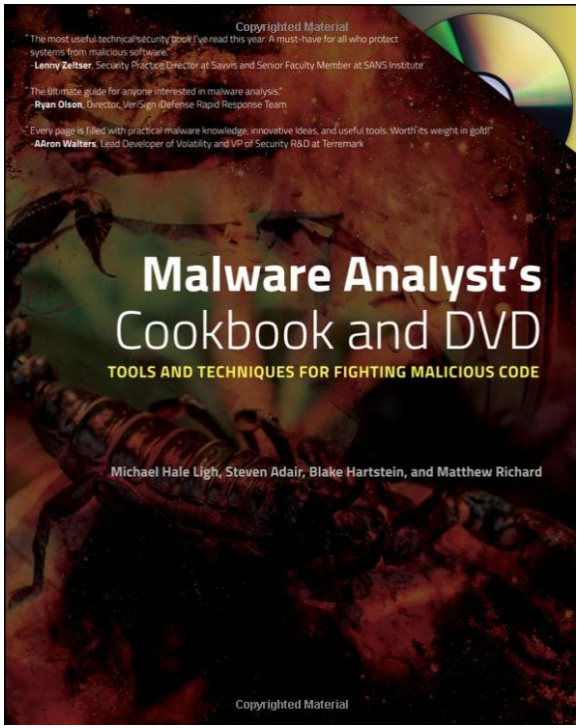


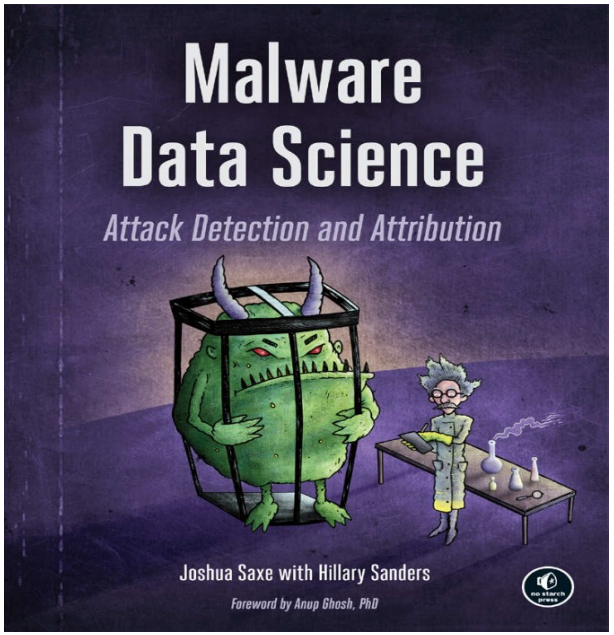
Windows Internals Seventh Edition



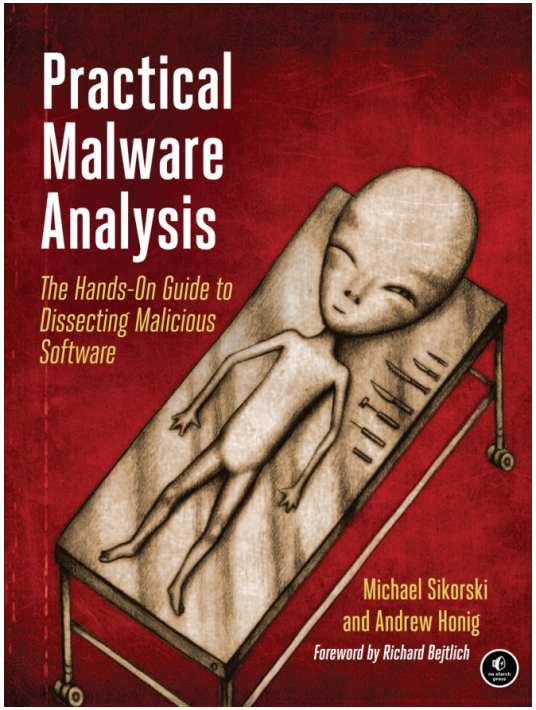
Tài liệu tham khảo

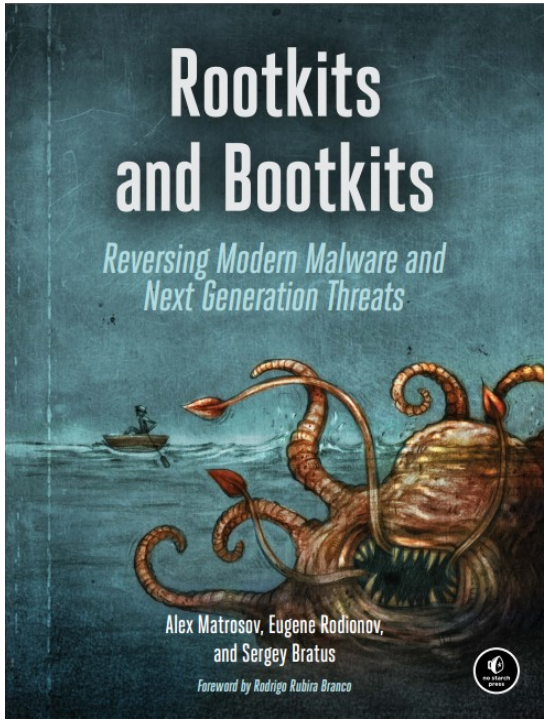


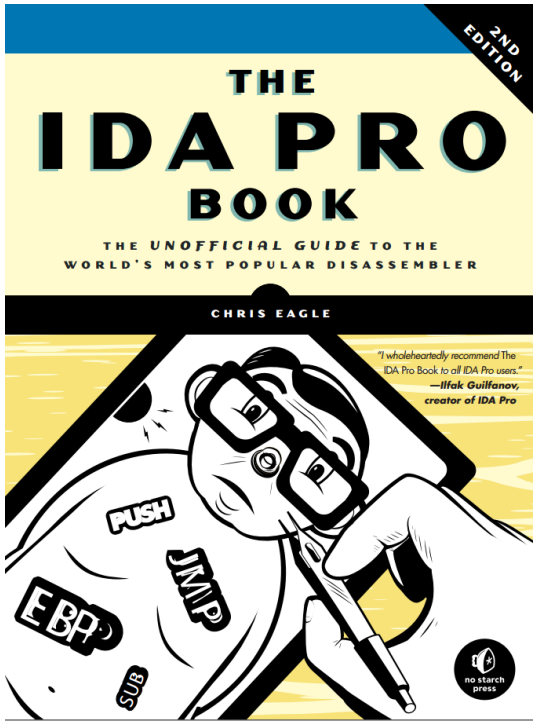




Tài liệu tham khảo



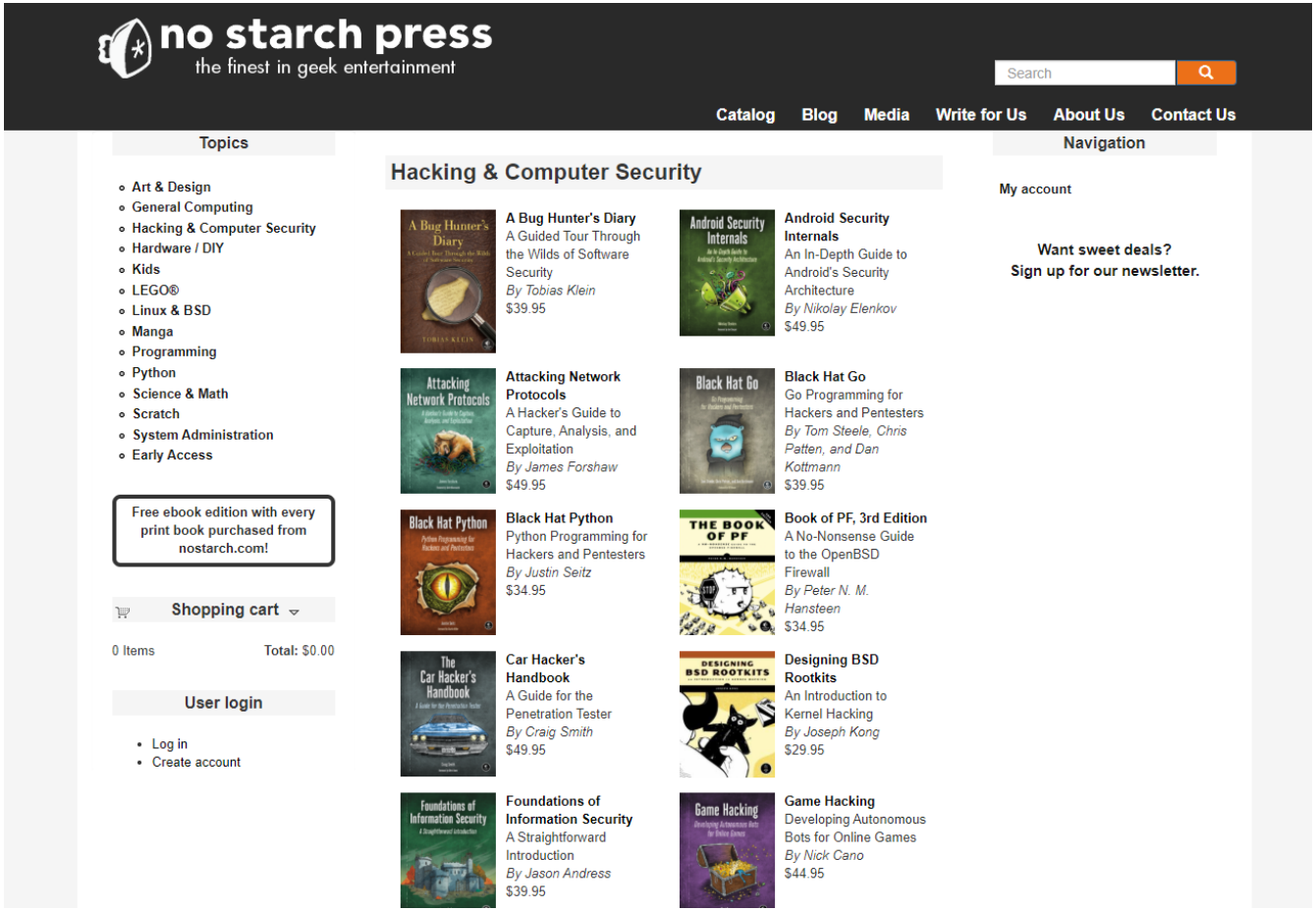




Tài liệu tham khảo

- Website: https://sites.google.com/a/uit.edu.vn/malware mechanism/
- Thư mục OneDrive của môn học:

Tài liệu tham khảo



- Nhà xuất bản No Starch Press có nhiều sách hay về Hacking & Computer Security: https://nostarch.com/catalog/security

NT230 – Malware's Modus Operandi

Cơ chế hoạt động của mã độc

Email: inseclab@uit.edu.vn

Trường ĐH Công nghệ Thông tin - ĐHQG TP. HCM