MALWARE ROADMAP

By : Chris Taylor [Blue Cosmo]

SYNOPSIS:

A high level beginners guide to malware development

DISCLAIMER:

This is entirely my opinion on how to get started with malware. There is no "one clear path".

STAGE 00

Computer Science

CONCEPTS:

CONCEPTS:

- how computers work

CONCEPTS:

- how computers work
- numeric systems (binary, hex, decimal)

CONCEPTS:

- how computers work
- numeric systems (binary, hex, decimal)
    - how to convert between them

CONCEPTS:

- how computers work
- numeric systems (binary, hex, decimal)
    - how to convert between them
- processes, handles, threads

CONCEPTS:

- how computers work
- numeric systems (binary, hex, decimal)
    - how to convert between them
- processes, handles, threads
- memory, "the stack", etc

CONCEPTS:

- how computers work
- numeric systems (binary, hex, decimal)
    - how to convert between them
- processes, handles, threads
- memory, "the stack", etc
- high level understanding of machine code

PROBLEM SOLVING:

PROBLEM SOLVING:

- programming teaches you how to problem solve

PROBLEM SOLVING:

- programming teaches you how to problem solve
- learn how to google things and utilize documentatio
  chat-gpt, etc

PROBLEM SOLVING:

- programming teaches you how to problem solve
- learn how to google things and utilize documentatio chat-gpt, etc
- figure out errors on your own, and if you can't. reach to others for help

STAGE 01

Programming Fundamentals

LANGUAGE TYPES:

LANGUAGE TYPES:

1. Compiled Language

LANGUAGE TYPES:

1. Compiled Language
    - rely on a **compiler** to turn the human readable syntax into an executable file

LANGUAGE TYPES:

1. Compiled Language
    - rely on a **compiler** to turn the human readable syntax into an executable file
2. Interpreted Language

LANGUAGE TYPES:

1. Compiled Language
    - rely on a **compiler** to turn the human readable syntax into an executable file
2. Interpreted Language
    - rely on a **interpreter** to turn the human readabl syntax into machine code (executed in memory)

3 TYPES TO LEARN:

3 TYPES TO LEARN:

1. Low Level Compiled Language

3 TYPES TO LEARN:

1. Low Level Compiled Language
2. High Level Compiled Language

3 TYPES TO LEARN:

1. Low Level Compiled Language
2. High Level Compiled Language
3. Native Interpreted Language

LOW LEVEL COMPILED LANGS:

LOW LEVEL COMPILED LANGS:

- C

LOW LEVEL COMPILED LANGS:

- C
- C++

LOW LEVEL COMPILED LANGS:

- C
- C++
- C#

HIGH LEVEL COMPILED LANGS:

HIGH LEVEL COMPILED LANGS:

- Nim

HIGH LEVEL COMPILED LANGS:

- Nim
- Go

HIGH LEVEL COMPILED LANGS:

- Nim
- Go
- Rust

NATIVE INTERPRETED LANGS:

NATIVE INTERPRETED LANGS:

- PowerShell

NATIVE INTERPRETED LANGS:

- PowerShell
- Batch

NATIVE INTERPRETED LANGS:

- PowerShell
- Batch
- VisualBasicScript

NATIVE INTERPRETED LANGS:

- PowerShell
- Batch
- VisualBasicScript
- Bash (linux)

WHY NO PYTHON?

WHY NO PYTHON?

- Although Python is a interpreted language, it is not native. So it is not ideal for the deployment of malwa

WHY NO PYTHON?

- Although Python is a interpreted language, it is not native. So it is not ideal for the deployment of malwa
- However, it can be useful for malware processes tha not directly run on the target (C2, network handling, etc)

PERSONAL RECOMMENDATIONS:

PERSONAL RECOMMENDATIONS:

1. C++

PERSONAL RECOMMENDATIONS:

1. C++
2. PowerShell

PERSONAL RECOMMENDATIONS:

1. C++
2. PowerShell
3. Nim

PERSONAL RECOMMENDATIONS:

1. C++
2. PowerShell
3. Nim
4. Basic Assembly

PERSONAL RECOMMENDATIONS:

1. C++
2. PowerShell
3. Nim
4. Basic Assembly
5. Python

BUILDING OUT AN ARSENAL:

A good malware developer should never limit themselves
a few languages. Once you build a strong foundation, mo
on to learning more complex concepts.

STAGE 02

CyberSecurity Fundamentals

BASIC HACKING:

BASIC HACKING:

1. ~~Reconnaissance~~

BASIC HACKING:

1. ~~Reconnaissance~~
2. Scanning ~~& Enumeration~~

BASIC HACKING:

1. ~~Reconnaissance~~
2. Scanning ~~& Enumeration~~
3. Exploitation

BASIC HACKING:

1. ~~Reconnaissance~~
2. Scanning ~~& Enumeration~~
3. Exploitation
4. Persistence

BASIC HACKING:

1. ~~Reconnaissance~~
2. Scanning ~~& Enumeration~~
3. Exploitation
4. Persistence
5. Covering Tracks

FAMILIARIZATION WITH TOOLS:

FAMILIARIZATION WITH TOOLS:

- Metasploit

FAMILIARIZATION WITH TOOLS:

- Metasploit
- Wireshark

FAMILIARIZATION WITH TOOLS:

- Metasploit
- Wireshark
- NMAP & NCAT

FAMILIARIZATION WITH TOOLS:

- Metasploit
- Wireshark
- NMAP & NCAT
- Hashcat / John

FAMILIARIZATION WITH TOOLS:

- Metasploit
- Wireshark
- NMAP & NCAT
- Hashcat / John
- Popular malware

BASIC CRYPTOGRAPHY:

BASIC CRYPTOGRAPHY:

- basic encryption / decryption

BASIC CRYPTOGRAPHY:

- basic encryption / decryption
- different ciphers and algorithms

BASIC CRYPTOGRAPHY:

- basic encryption / decryption
- different ciphers and algorithms
  - AES, XOR, base64

BASIC CRYPTOGRAPHY:

- basic encryption / decryption
- different ciphers and algorithms
  - AES, XOR, base64
- obfuscation

STAGE 03

Networking Fundamentals

NETWORKING CONCEPTS:

NETWORKING CONCEPTS:

- Different protocols

NETWORKING CONCEPTS:

- Different protocols
  - TCP, SSH, HTTP, etc.

NETWORKING CONCEPTS:

- Different protocols
  - TCP, SSH, HTTP, etc.
- 3 Way Handshake

NETWORKING CONCEPTS:

- Different protocols
  - TCP, SSH, HTTP, etc.
- 3 Way Handshake
- Utilize protocols for remote connectivity and exfiltration

STAGE 04

Malware Development

TOPICS:

TOPICS:

- Windows API

TOPICS:

- Windows API
- Shellcode Embedding

TOPICS:

- Windows API
- Shellcode Embedding
- Process & DLL Injection

TOPICS:

- Windows API
- Shellcode Embedding
- Process & DLL Injection
- AV Evasion

TOPICS:

- Windows API
- Shellcode Embedding
- Process & DLL Injection
- AV Evasion
- Trojan Development

REVERSE ENGINEERING:

Light reverse engineering and malware analysis can go a way. It will teach you how the malware actually works an runs through the system. It will also teach you about the latest trends and techniques in development.

CONCLUSION:

Ulitmately, Malware Development is a pretty involved topic that requires a lot of fundamental knowledge to get into.

Don't be discouraged, be inspired!

THANK YOU

subscribe :D