# Intro to Malware Analysis

A beginner’s guide to hunting digital monsters

# A Troublesome Beginning

- Computers can’t do **bad** things, they just run code
  - “Computer viruses are an urban myth, like alligators in the sewers of New York” - Peter Norton
- Began doing bad things based on mean code
  - Some seriously harmful, most just pranks
- Cyber criminals realized money to be made
  - Credential stealers
  - RAT / Bots
  - Adware
  - Droppers
  - Ransomware
  - Etc

```
                                   COMMAND.COM

ƏR▪cox
ce %2
nsert volume %‡‡‡‡‡‡‡‡‡‡≈(1 serial %2-%3
%File allocation table bad, drive %1
§Invalid COMMAND.COM
!Insert disk with %1 in drive %2
!Press any key to continue . . .
```

https://archive.org/details/malwaremuseum

# Writing malware

- Just write mean code
  - Credential stealers - grab sensitive files
  - Droppers - download or unpack a file, then execute it
  - Ransomware - find valuable files and encrypt them
- Surprisingly easy if you’ve taken classes
- Most virus authors are skiddies who steal code

# Why Analyze Malware?

- Responding to incidents
- Research cyber threats
- Pentesting payloads
- Hunting malware

Context is important!

# DANGER!

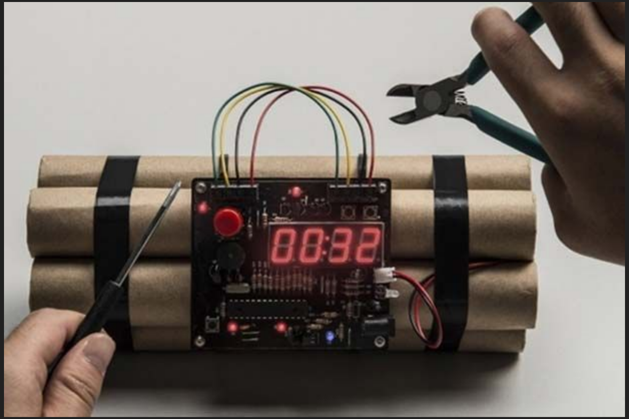
NEVER forget that these files are actively trying to harm you

- keep them in encrypted zip files whenever possible
- Def-fange URLS

# First steps

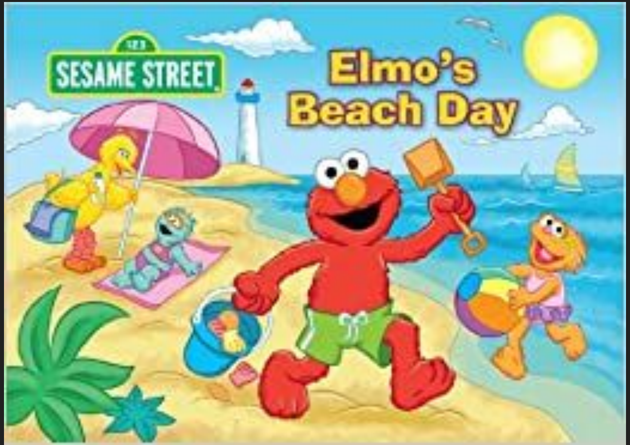
Good idea to be taking notes

1. Context
2. Calculate hash and upload to VirusTotal
3. Basic static analysis
   a. Is it packed?
   b. Strings command
   c. What language/file?
   d. Embedded files?
4. What strain/attacker? - try VT, Yara, etc
5. Consider safety of dynamic analysis



# Dynamic Analysis - put the monster in a sandbox

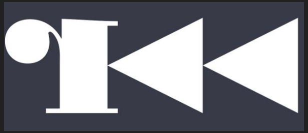
- Local VM or online sandbox
  - Local - dangerous and [more] unreliable
  - Public sandboxes: Intezer, AnyRun, Hybrid Analysis
- Results:
  - Embedded or packed files
  - Function logs
  - Packet capture (and IOCs)
  - Etc.
- Beware of imperfect executions
  - Evasive malware (shoutout to VMRay!)



# Reverse Engineering

Be careful with debuggers!

- Generally in Assembly
- May be packed or obfuscated
- Use sandbox execution as guide
- Never going to know everything (have a goal)
- Popular tools:
  - Ghidra
  - Ida Pro
  - Radare2
  - x64dbg
  - Vim/Notepad++



# Presenting Findings

- Long drawn-out process, check everything!
  - Wait 24 hrs
- Have evidence and thorough explanation
- Clearly separate potential theories
- Share what you find!
  - VirusTotal
  - Malware analysis forums/groups
  - …Twitter (sigh)
  - Blog posts

# Tools, resources, more info!

- Self Protection
    - VirtualBox - https://www.virtualbox.org/
    - TOR - https://www.torproject.org/
    - common sense
- Threat Intelligence
    - VirusTotal - https://ww.virustotal.com/
    - Att&ck Software - https://attack.mitre.org/software/
    - AnyRun Trends - https://any.run/malware-trends/
    - Security news - https://isc.sans.edu/podcast.html and https://www.thecyberwire.com/podcasts
    - DHS/CISA and US Cyber Command
- Samples:
    - VirusTotal - https://ww.virustotal.com/
    - Malware Bazaar - https://bazaar.abuse.ch/browse/
    - Hybrid Analysis - https://www.hybrid-analysis.com/file-collections
    - ur email

# Tools, resources, more info! (cont.)

- Static Analysis Tools
  - VirusTotal - https://ww.virustotal.com/
  - UnpacMe - https://www.unpac.me/
  - YAYA - https://github.com/EFForg/yaya
  - Ghidra - https://ghidra-sre.org/
  - REMnux - https://remnux.org/
  - Malware Dismantle (outdated) - https://github.com/john-faria/Malware-Dismantle-Official
  - RapidTables - https://www.rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html
  - FileInfo - https://fileinfo.com/
  - Strings, WireShark, Vim, Binwalk, etc - “apt-get install”
- Online Sandboxes
  - Intezer - https://analyze.intezer.com/analyze
  - AnyRun - https://app.any.run/
  - Hybrid Analysis - https://www.hybrid-analysis.com/
  - VirusTotal - https://www.virustotal.com/gui/url/<file hash>/behavior

# Tools, resources, more info! (cont. (cont.))

- More Info
  - Malware Analysis Bootcamp - https://www.youtube.com/playlist?list=PLBf0hzazHTGMSlOI2HZGc08ePwut6A2Io
  - MalwareHunterTeam - https://twitter.com/malwrhunterteam
  - Practical Malware Analysis - https://practicalmalwareanalysis.com/
  - MalwareAnalysisForHedgehogs - https://www.youtube.com/channel/UCVFXrUwuWxNlm6UNZtBLJ-A
  - CSC Discord - https://discord.com/channels/750111183150776402/750111904386646047

# Challenges!

- PicoCTF Reversing Archive - https://picoctf.org/index#picogym
- Binary Bomb Lab - http://zpalexander.com/binary-bomb-lab-set-up/
- MalwareTech challenges - https://www.malwaretech.com/challenges
- Flare On CTF - https://2020.flare-on.com/