Talking Malware Analysis with MITRE

Jonathan Jones | Michael Long

MITRE

Meet the MITRE Conversation Starters

We are Comp Sci Aggies

- **Michael Long**
  - Cyber Security Engineer
  - BS and MS in Computer Science

- **Jonathan Jones**
  - Cyber Security Engineer
  - BS and MS (SFS) in Computer Science

MITRE

Why we are here

- MITRE is looking to engage with Students at NCATSU with real world challenges and activites.
- Discuss high level topics with students in various areas related to Cyber Security/Cyber Operations

Initial topic: Malware Analysis

- We want to be able to explain the *who, what, how, and why* at a high level
- Assist in developing subject matter expertise among students who may be interested in this area of cyber security
- Any questions about malware analysis after presentation let us know!

Malware Analysis

The Syllabus

1. What is Malware Analysis & Why Does it exist?
2. Malware Types
3. How To Perform Analysis
4. Static Analysis
5. Dynamic Analysis
6. More Tools
7. Quick Tip
8. Demo(s)

Malware Analysis

What is Malware Analysis & Why Does it exist?

- **What**
  - *"The art of dissecting malware to understand how it works, host to identify, and how to defeat or eliminate it"*
    - Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software 1st Edition (Michael Sikorski, Andrew Honing)
    - Studying the malicious behavior of software
    - Monitoring malicious software in a controlled environment

- **Why**
  - To assess damage to systems
  - Discover indicators of compromises
    - C2 (command-and-control)
  - Understanding of intruders
    - Is this an advanced persistent threat (APT), or
    - Crimeware
  - Determine the purpose of the malware

Malware Analysis

Malware Types

- **Virus**
- **Worm**
- **Trojan**
- **Backdoor**
- **Remote Access Trojan (RAT)**
- **Ransomware**
- **Bot**
- **Downloader**
- **Dropper**
- **Potentially Unwanted Programs (PUP)**
  - Adware
  - Spyware

Malware Analysis

How To Perform Analysis

Safety 1st: Controlled Environment = Safe Environment

- **Never use your everyday use computer(s)**
  - Use an old computer
    - Physical Machine where you can use clonezilla to restore to pristine state
  - Access to VirtualBox, VMWare?
    - VMs allow the use of snapshots and reverts
  - Access to an OS?
    - Windows, Linux

- **Analysis Type**
  - Static (code) Analysis
    - Examining file attributes
    - Examining disassembled code
  - Dynamic (behavioral) Analysis
    - Run the malware - observe its impacts on the system
    - Run the malware in a debugger to examine the malware's inner workings
  - Memory Analysis
    - Analyzing computer's RAM for artifacts

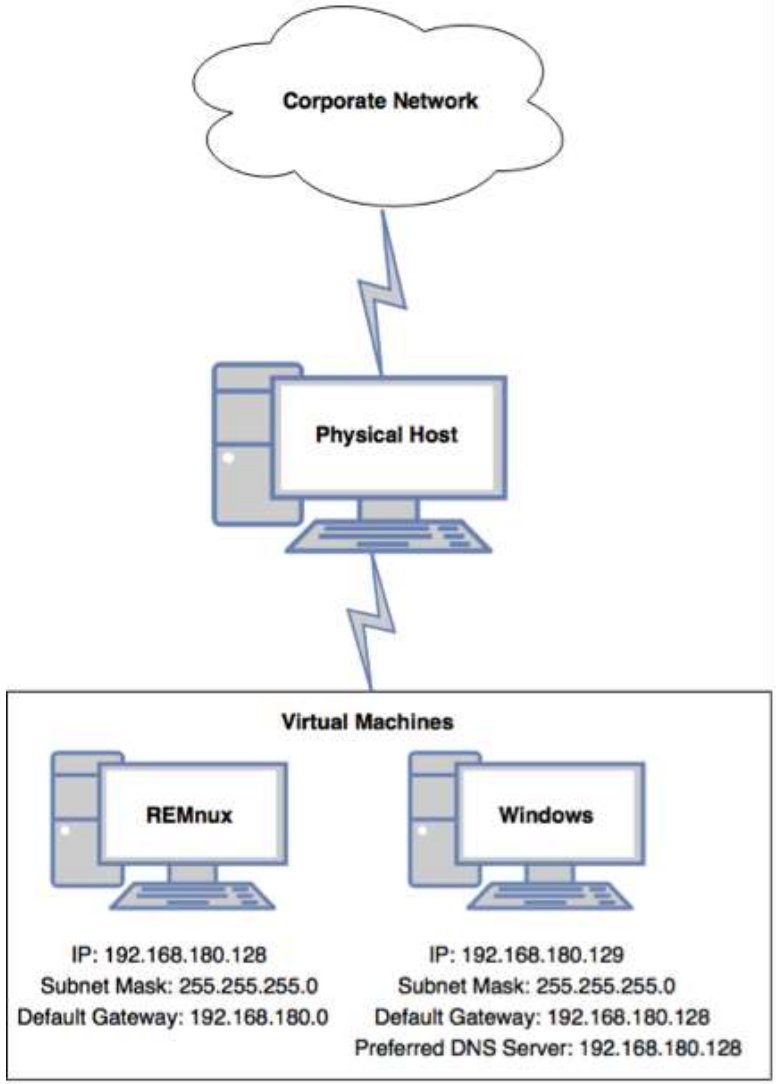
MITRE

Malware Analysis

How To Perform Analysis

Safety 1st: Controlled Environment = Safe Environment

- **Suggested Lab Environment**
  - **Physical Machine**
    - Host OS should not be Windows
  - **Virtual Environment**
    - Windows VM
    - REMnux VM
      - Reverse-Engineering Malware Linux
  - **Networking**
    - Only allow network connections between the VMs
    - Never allow traffic to go out
  - **Tips**
    - Password protect malware samples in compressed file
    - Always take a snapshot of environment
      - Initial setup snapshot of VMs is ideal



MITRE

Malware Analysis

How To Perform Analysis

Safety 1st: Controlled Environment = Safe Environment

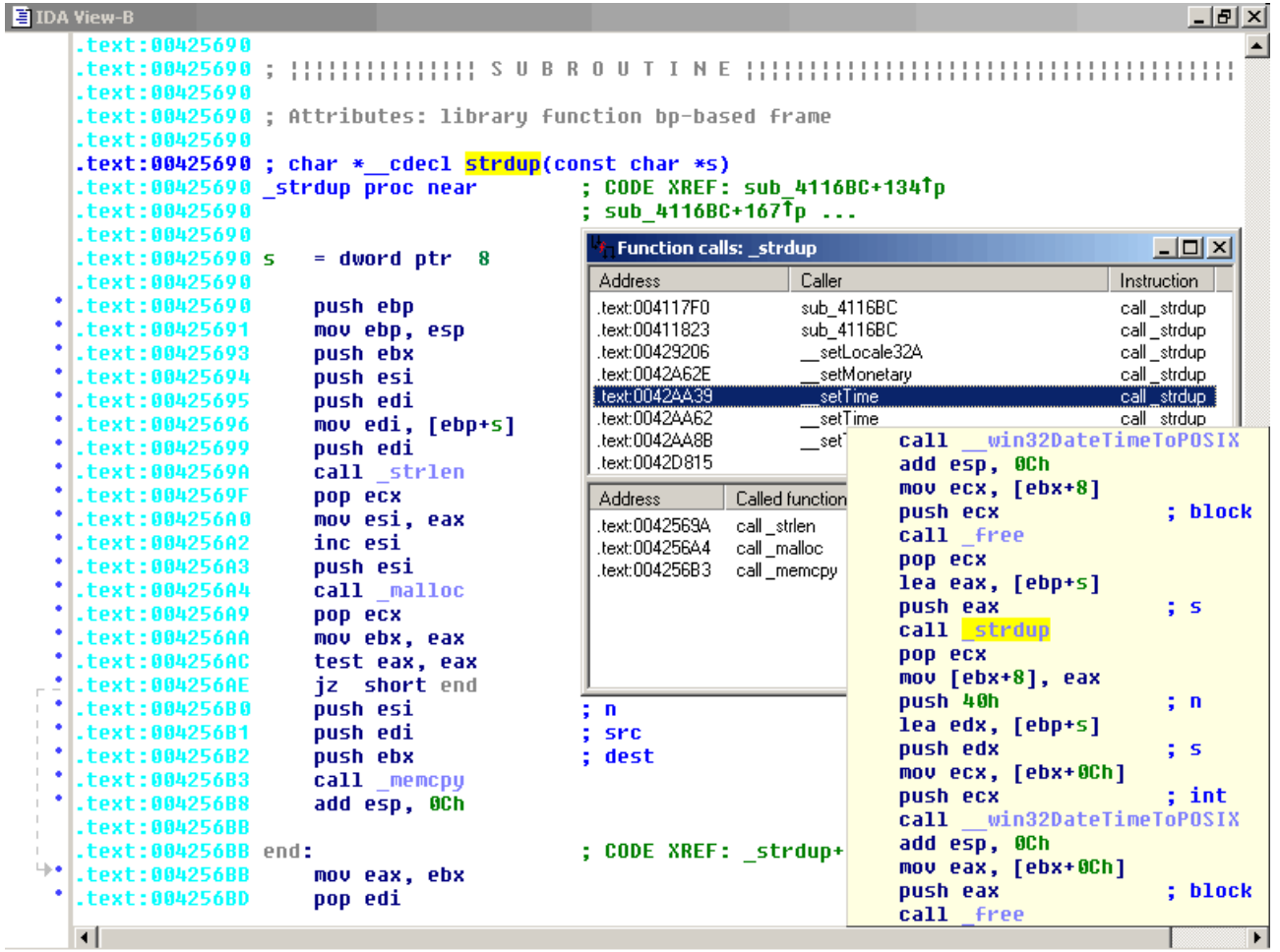
- **Advanced static analysis**
  - Deep inspection of code to understand the inner workings of the malware
    - Reverse-engineering with a disassembler
    - Complex, requires understanding of assembly code
- **Advanced Dynamic Analysis**
  - Run code in a debugger
  - Examines internal state of a running malicious executable

Malware Analysis

Static Analysis

Safety 1st: Controlled Environment = Safe Environment

- **Tools we can use**
  - Anti-Virus Engines
  - Hash (md5, sha1, sha256)
  - YARA
  - Strings
  - IDA Pro
  - PEView
  - PEiD
  - And many more



Malware Analysis

Dynamic Analysis

Safety 1st: Controlled Environment = Safe Environment

- **Tools**
  - FireEye (costs)
  - Cuckoo (Free)
  - WireShark (Free)
  - SysInternals (Free)
  - Process Hacker
- **What we look for**
  - IP Addresses
  - Services/Processes
  - Registry Changes
  - File System Changes

Malware Analysis

More Tools

- **Multiscanner**
  - Developed by MITRE
  - Combines Static and Behavioral Analysis
  - Hosted on Github
    - It's **FREE!!!**

- **VirusTotal**
  - Submit Files for Analysis
  - Be careful for what you submit
    - Paid members can download
  - Threat Actors submit samples

Malware Analysis

Quick Tip

- **Don’t Get Caught in Details**
  - Focus on key features
- **Try Several Tools**
  - If one tool fails, try another
    - MITRE does not endorse a specific tool. Find one which works best for you.
  - Don’t get stuck on a hard issue, move along
- **Malware authors are constantly raising the bar**
  - Malware Analysis requires continuous learning
    - Work with peers, public forums, research
  - Come to MITRE

DEMO

Resources

- **Practical Malware Analysis, Black Hat 2007**
  - Kris Kendall and Chad McMillan

- **Awesome-Malware-Analysis**
  - A curated list of awesome malware analysis tools and resources
  - Github Project

- **MITRE**
  - Solving Problems for a Safer World
  - Do you have what it takes? Apply here

Resources

- **Free Training**
  - http://opensecuritytraining.info/
- **REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware**
  - https://remnux.org/
- **Lenny Zeltser**
  - https://zeltser.com/

MITRE

MITRE is a not-for-profit organization whose sole focus is to operate federally funded research and development centers, or FFRDCs. Independent and objective, we take on some of our nation's—and the world's—most critical challenges and provide innovative, practical solutions.

Learn and share more about MITRE, FFRDCs, and our unique value at www.mitre.org