**Workshop Overview**

This workshop will be 50 minutes broken down into three sections: Theory, Static Analysis, and Dynamic Analysis. This workshop is for people curious about malware analysis and designed for beginners, but with the assumption that the attendees have the basic knowledge of networking and fundamentals of computer security. Each student will have their own analysis/victim virtual machine to use with analysis tools, and learn about how to glean functional information about the malware samples.

Due to infrastructure, seats will be limited to 10 per session. There will be three sessions in the morning.

**Workshop Outline**

- Malware Analysis Introduction and Slides (20 mins)
    - What is malware analysis? Why analyze malware?
    - Malware Types and Families
    - 10-second introduction to ASM, Coding Constructs, Code Logic
    - PE File Structure
    - Dynamic Vs Static Vs Sandbox Analysis
    - Triaging
    - YARA
- Static Analysis (15 mins) -- Hands-On Lab
    - Introduction to static analysis tools
        - Packer Detection
        - Insight into ELF/PE
    - Search for malicious indicators
    - Write simple YARA signatures
- Dynamic Analysis (15 Mins) -- Hands-on Lab
    - Introduction to dynamic analysis tools
        - Debuggers
        - Sysinternals
    - PCAP Analysis

**Samples used during workshop:**

- VPNFilter
- Metasploit Payloads
- Netcat
- Ransomware

**Requirements:**

- Personal Laptop with Chrome or Firefox + Flash installed, Ideally 8+GB of RAM
- Basic understanding of Networking
- Basic understanding of using virtual machines (reverting)
- Moderate understanding of Computer Security (familiarity with terms like shell (bind, reverse), and items like the registry)
- Critical thinking skills

**Bio**

Andrew Perkes is a core developer and security researcher. He is also the current instructor for IS4953 – Malware Agent Analysis at the University of Texas, San Antonio and helps coach the UTSA CCDC team. He has over 9 years of experience in computer security, which includes developing security tools, auditing, and reverse-engineering a wide range of applications (including mobile) on multiple operating systems. In previous positions he worked as a malware reverse-engineer, system administrator, and freelance pen-tester. He held a few industry certifications and is a member of a local security association called SAHA. He is currently the Vice President of the CyberDEF Dojo.