Module C1: FILE HANDLING TECHNIQUES

**Module Description:** SRE often involves files of unknown origin and/or functionality. Many of these are binary files, but files that are commonly viewed as benign (e.g., Office documents, PDFs, audio/video files) can also be malicious if used in the wrong context. In the context of static analysis such files are often considered to be safe as long as they are not opened or executed, but that can be a dangerous and misguided assumption. Anti-virus (AV) software often examines all files on a system, file system explorers generate and display previews of files, and operating systems index and gather metadata from files. The large majority of this happens without user interaction, and often involves automated parsing of the file metadata and/or content in ways that have historically been vulnerable to exploitation. In addition, the transmission of files of unknown origin and/or functionality is similarly complex, as common tools for transferring data (e.g., email and file sharing services such as Dropbox) often examine file attachments and can also result in suspicious or dangerous files being transferred outside a safe environment. The module will cover techniques by which files of unknown origin and/or functionality can be safely moved, stored, and examined by static analysis tools (i.e., not including execution, which is covered in module D1).

**Prerequisite Knowledge:** This module is intended to be a follow-up to Module B1: Approaches to SRE

**Length of Completion**: Module – More than 4 and less than 10 hours

**Level of Instruction:** This module intended to be an advanced undergraduate or graduate course for technical majors.

**Learning Setting:** This module is intended for in-class.

**Lab Environment:** VMs and containers that include the exercises and challenge materials to ensure consistency and ease of deployment.

**Lab Tasks:** The objective of this lab is to allow you to use the Honeypot instance you created in class to acquire and investigate real malware samples in the wild. It also provides an opportunity to deploy additional honeypots.

**Lab Files that are Needed:** All files are contained in the VMs.

# learning outcomes

MODULE learning oUTCOMES

Upon successful completion of this module, the student should be able to:

1. Explain various approaches to acquire, transfer, and store malware sample.
2. Recognize and differentiate between the options available for transfer and storage of malware samples.
3. Identify and evaluate the techniques for acquiring malware samples.

# module Details

**Interconnection:** This module is part of a 15-week Software Reverse Engineering (SRE) Course. The 15 modules are:

* Module A1: x86 and x64 architectures and assembly languages
* Module A2: ARM architectures and assembly languages
* Module A3: "Forward Engineering"
* Module B1: Approaches
* **Module C1: Techniques for the safe handling of files of unknown origin and /or functionality**
* Module C2: Basic static analysis tools.
* Module C3: Disassemblers and Decompilers
* Module D1: Sandboxing and other techniques for the safe execution/opening of files of unknown origin and /or functionality.
* Module D2: Basic dynamic analysis tools.
* Module D3: Debuggers
* Module D4: Network Traffic Analysis
* Module D5: Patching binaries
* Module E1: Obfuscation and Anti-SRE
* Module F1: Non-Binary SRE

**Instructional Files and Online Resources Needed:**

PowerPoint file: SRE-C1-Lecture.pptx

Lab Environment: SRELNX-2.ova (Format may vary)

Lab Narrative: SRE-C1-Lab.docx

Supplementary Reading:

Sikorski, M. & Honig, A. (2012). *Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software.* San Francisco:No Starch Press.

Eagle, C. (2011). *The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (2nd ed.).* San Francisco:No Starch Press.

**Assessment:**

The learning objectives are assessed through the following methods:

1. ASKs: There are questions in the note sections for the instructor to involve the students in the lesson and assess their grasp of the concepts.
2. LABs: There are lab exercises associated with this lesson

# lessons

**Warm Up:** See SRE-C1-Lecture.pptx

**Lesson:** See SRE-C1-Lecture.pptx

**Active Learning Activity:** See SRE-C1-Lab.docx