Lab 1:
Static Analysis

Tyler Hudak
INCIDENT RESPONDER

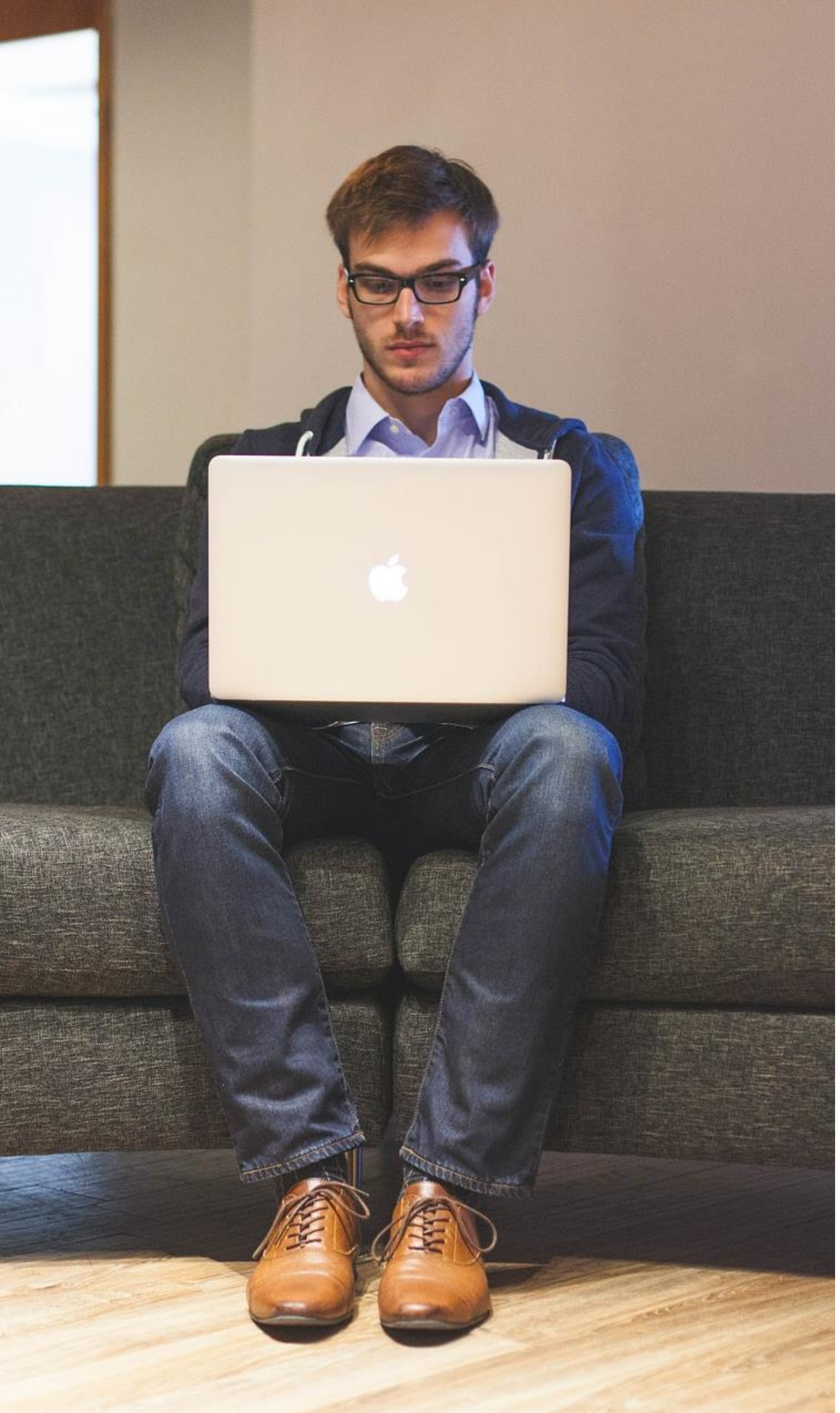
@secshoggoth

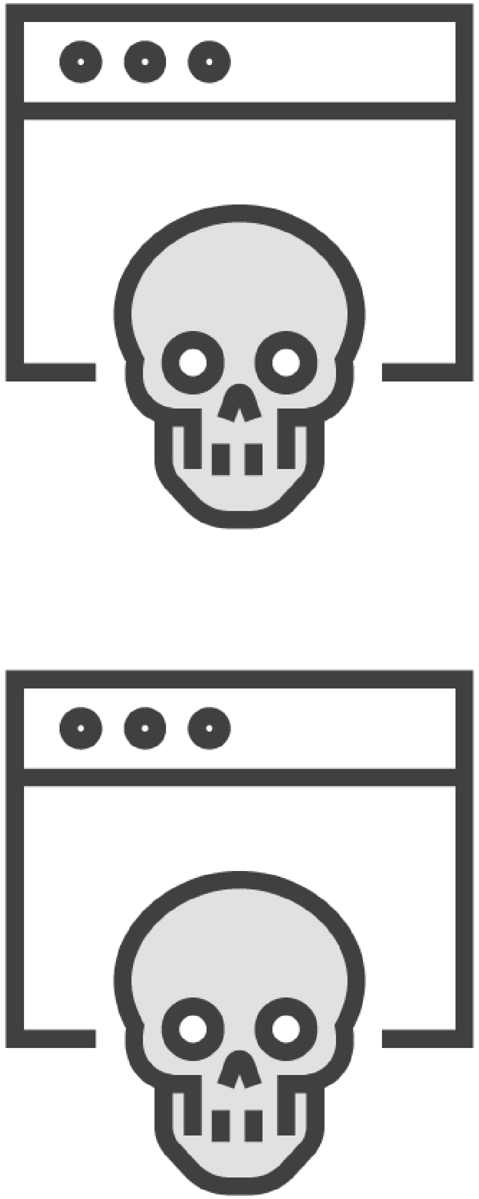
Overview

Lab Intro

Lab

Lab Discussion





Demo

Static Analysis Lab

http://bit.ly/malfund-2

- Password is “infected”

financials-xls.scr

File Identification

UPX packed executable

Microsoft Visual C++ Win32 executable

No hashes in Google or VirusTotal

financials-xls.scr

Embedded Strings

Network

- download.bravesentry.com
- 69.50.175.181

Files

- C:\Program Files\BraveSentry\BraveSentry.exe
- C:\windows\xpupdate.exe

Registry

- SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Your computer is in Danger!

financials-xls.scr

PE Header

May 7, 2007

Sections

- .text is writable

Import Address Table

- RegSetValueExA
- WriteFile
- WinExec
- wsock32.dll imported by ordinal

Resources

- Russian language

Summary

Static analysis examines without execution

File identification

Embedded strings

PE header