Lab 2:
Dynamic Analysis

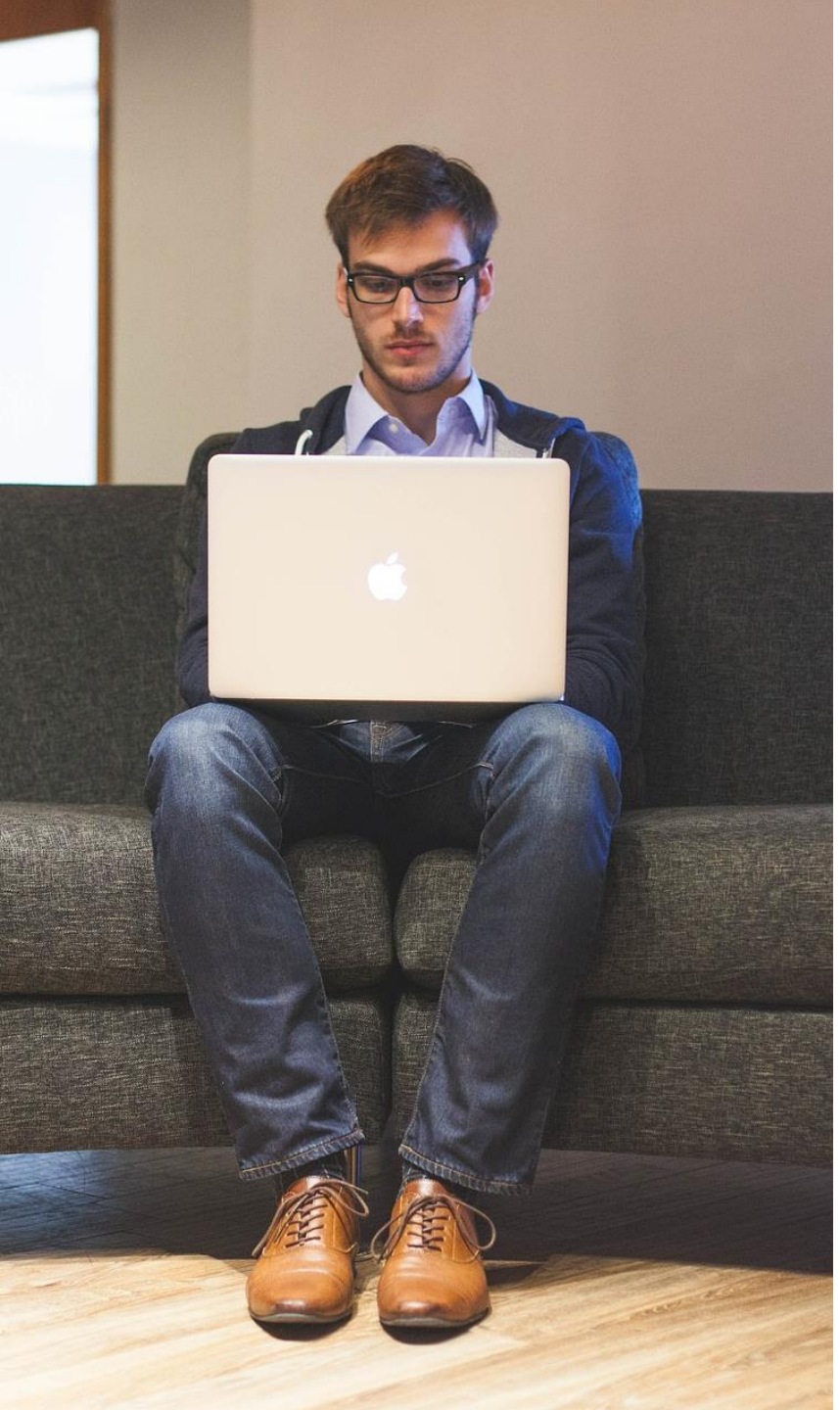
Tyler Hudak
INCIDENT RESPONDER

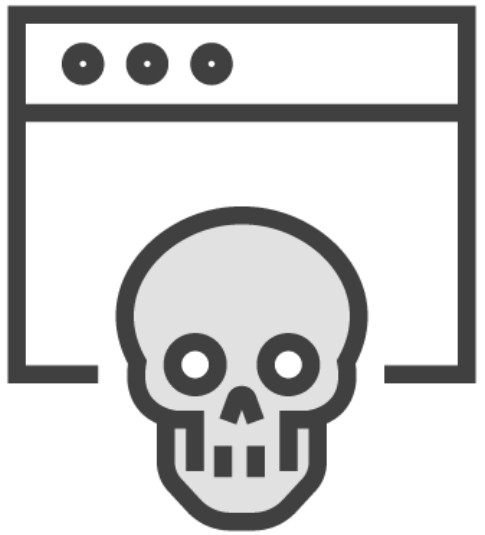
@secshoggoth

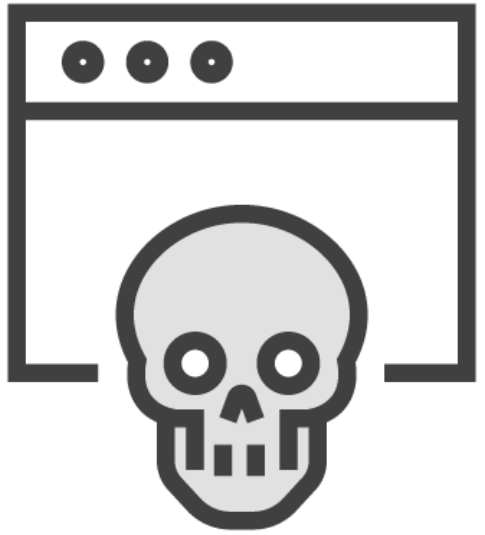
Overview

Dynamic Analysis Lab

Lab Discussion







financials-xls.exe

Recap

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

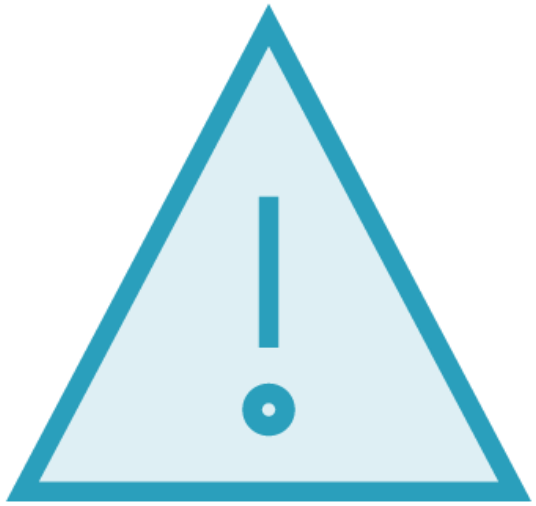
Your computer is in Danger!

Demo

Dynamic Analysis Lab

http://bit.ly/malfund-2

- Password is “infected”



financials-xls.exe

Behavior Monitoring

File System:

- C:\windows\xpupdate.exe
- Install.dat

Registry

- Two persistence keys in HKCU
- Created install version key

Network

- Attempted to download from download.bravesentry.com

Summary

System changes

Behavior monitoring