ADCG Malware Challenge 2

Due January 24th

Introduction

Congratulations! You have successfully landed a job as a malware analysts at Initech. The management was particularly impressed with your data mining skills and looks forward to seeing what you can produce. They have high hopes, so make them proud!

In your interview, you proved that you had what it takes to identify benign and malicious malware from a given sample set. This is great news and with that knowledge you are confident that you can revolutionize the antivirus industry. Hell, even most academic papers use that metric, it has to be solid right?

Phase 1

Introduction

Your mentor has assigned you with a few training exercises to develop an understanding of malware.

Homework

Write a report for three samples from the following list. The report should just be long enough to cover the core points. I.e. a few sentences for each of the following questions:

1) What is the purpose of the malware?
2) Who is the actor?
3) What are some interesting techniques used?
4) Was the malware tool successful?
5) What did the defenders do wrong, right, or how did they respond?

Malware list:

1) Zeus-Citadel
2) Crypto-Locker
3) Conficker
4) Mirai
5) Lazarus[1]

[1] https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

6) Mediyes

Phase 2

Introduction

Ohh no! Initech never cared about security and assumed it was just added overhead. Unfortunately, during a recent audit for insurance it was reported that their security practices were severely lacking. In fact, Initech's network is a hotbed for malware and they are denied coverage and further funding until their problem is better managed.

Management has turned to you to help figure out how big of a problem they have.

Dataset

2 sets of JSON newline delimited files. They contain results for PEInfo and Objdump respectively. The Objects sha256 is the pivot.

Deliverables

Create a presentation to present to the company board. Your presentation should:

1) Using PEInfo, identify the number of malware families. Additionally, provide a graphical depiction.
2) Take 3 samples. One from three clusters.
    a) Identify the malware
        i) Are there signatures from Virustotal?
    b) Explain the malware at a high level. (remember you are briefing the board)
    c) Highlight any concerns.
    d) Using Objdump, write a similarity detection algorithm that identifies similar malware.
        i) Are there differences with the original cluster?
3) Identify any serious concerns and provide a recommendation to mitigate the problem

Grading

The board is composed of your peers. They will evaluable your presentation for the following:

1) Ability to transfer knowledge to the audience
2) Ability to focus on important facts and results
3) General presentation skills (slide quality, presentation pace and speech quality...)