
# Mach-O Malware Analysis: Combatting Mac OSX/iOS Malware with Data Visualization

INCOMPLETE DRAFT: PLEASE SEE LAST PAGE FOR FINAL PPTX

Remy Baumgarten

Security Engineer at ANRC Services

https://www.linkedin.com/in/remybaumgarten

Website: anrc-services.com

Twitter: @anrctraining

# About me

ANRC

- Mobile malware talks/ tutorials
- Present: Research and development (ANRC Services)
- Past: Malware team (Booz Allen Hamilton)
- past: secure dna

# Why a new tool?

- Examining and evaluating the existing tools available to help decipher the Mach-O format.
- Finding working examples of security products equipped to process Mach-O malware.
- Attempting to find a tool that could analyze these files regardless of the underlying architecture.
- Researching a better way to view the file internals of Mach-O files.

# TOOLS THAT ANALYZE MACH-O

| Tool | Graphic | Multiple Architectures | Network Security Aware | Easy to Understand | Ease of Use |
|---|---|---|---|---|---|
| IDA Pro | Yes (sometimes) | Yes | No | No | No |
| otool | No | Yes | No | No | No |
| class-dump | No | Objc Only | No | Yes | Yes |
| Machoview | Yes | Yes | No | No | Yes |
| ptool | No | Yes (old/no support) | No | No | Yes |
| otool-ng | No | Yes (old/no support) | No | No | No |
| hopper | Yes (sometimes) | Yes | No | No | No |

Figure 1. Evaluation of existing Mach-O tools (Green=Meets Need, Red=Does Not Meet, Yellow=Some Need Met)

We wanted to fuse the best features of all of these programs and add a focus on network security.

Ultimately the goal is to help the network defender understand the Mach-O file format better and provide a method to effectively and efficiently analyze a particular binary for malicious behavior.

# Introducing Mach-O Viz

- Mach-O Viz presents a Mach-O binary visually
- In turn this makes it easier for anyone to see how the file is constructed
- Visual representation from the header through the load commands and into all its corresponding segments
- Interactive so you can zoom into segments for more detail

# Design Features

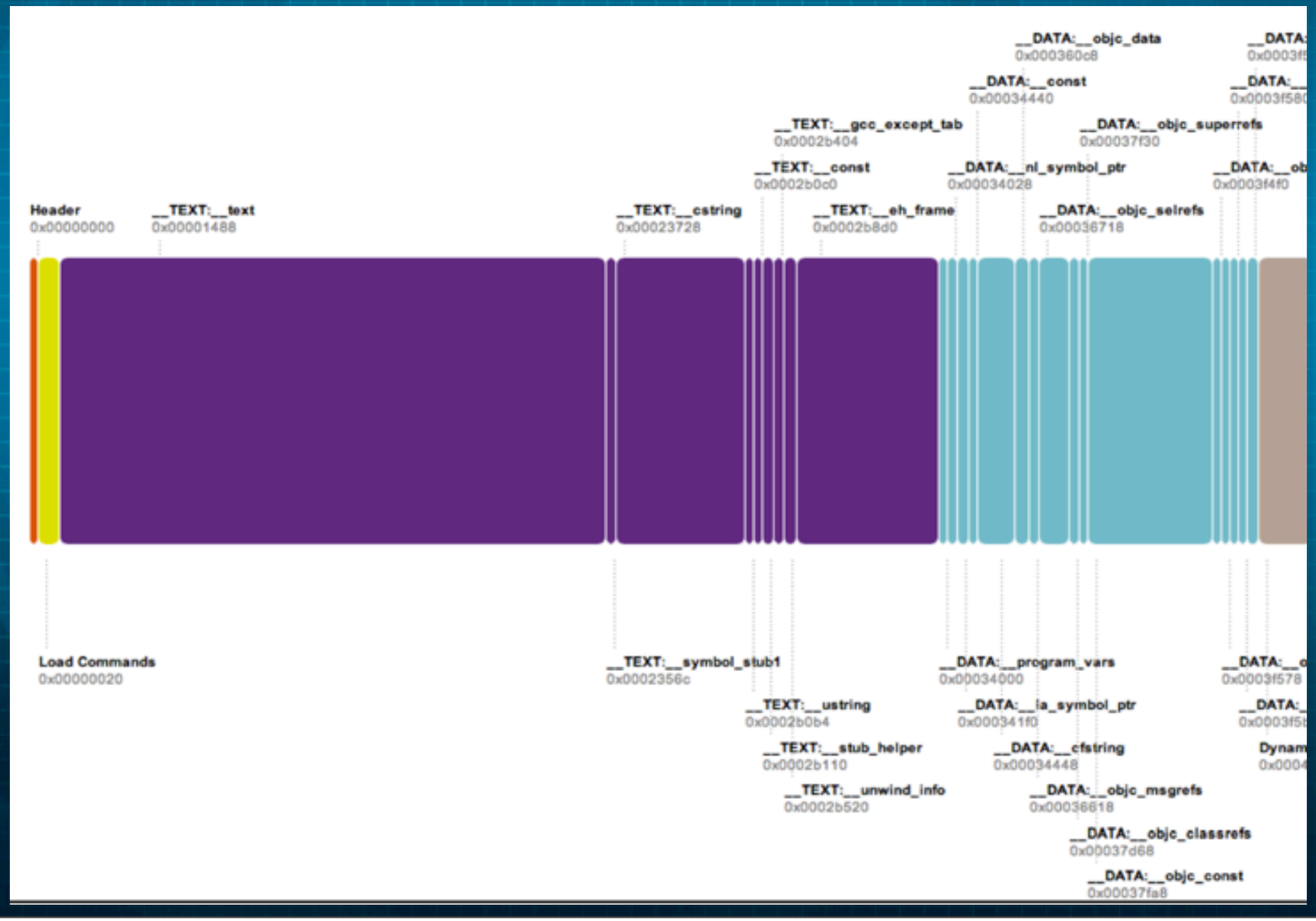
- In addition, to visualizing the file format itself:
- we wanted a powerful back-end graph visualization and analytics system for graphing the binary's disassembly
- Currently supports i386, x86_64 and ARM6/7.
- We wanted to keep this program not only as visual as possible but also accessible:
- Only a web browser is required to perform interactive analysis

# Design Features

- Use any client capable of running HTML5/JavaScript, thereby significantly increasing the types of devices that could make use of Mach-O Viz.
- Keep the back-end as “Mac” as possible. We wanted to rely on Apple’s updates of the Mach-O spec and its tools, such as otool, in their native environment. This would keep Mach-O Viz updated and relevant by default.
- Gain access to the LLVM disassembler for the most accurate ASM we can feed into our analytics engine.
- Make use of as many Open Source utilities that added benefit as possible.

# File Structure Visualization

- Major Segments at the top level of the file
- Drilling down possible by clicking Segment

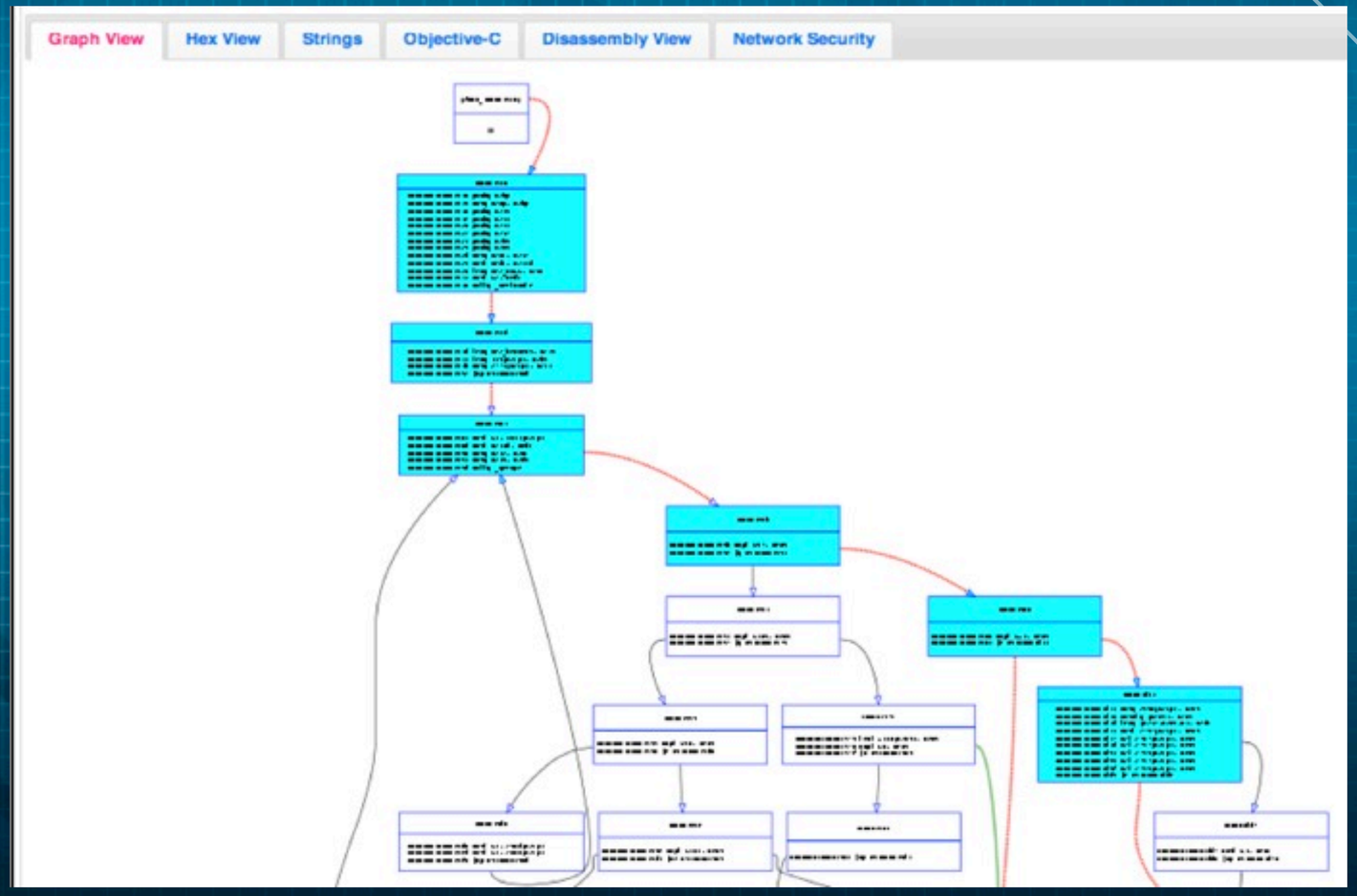


# File Structure Visualization

- Here you can see the load commands
- Specific values for macho file format are viewed this way

# Graph View

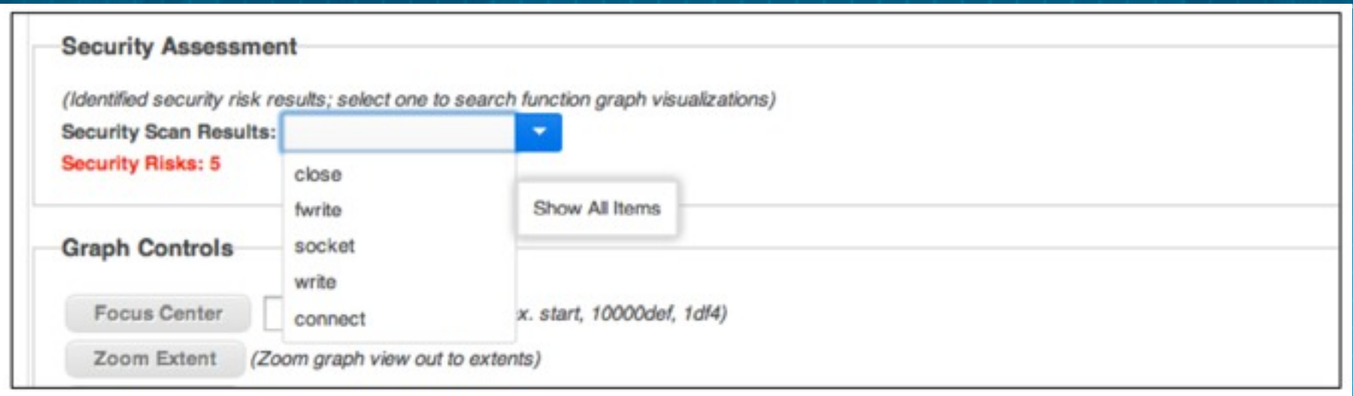
- Offers an IDA like interface
- This is done via parsing out otool disassembly with perl into graphviz charts
- Then placing into html as SVG with JS and CSS



# Security Analysis

- Identifying code segments which are using API's and Functions flagged as Security Risks.
- Identifying and automatically generating network and static file signatures for the binary.
- Mach-O Viz does this in 2 ways:
  - a) By detecting network domains, ip addresses, urls & web protocols embedded in the binary.
  - b) Calculating a unique binary signature for the file itself using Mach-O MAGIC value in the file's header plus a unique 16 bytes from the binary's String Table.

# Security Analysis




- Results take you directly to code for instant analysis
- File Signature is then created

# Final slides available

- http://machoviz.anrc-services.com/slides.zip