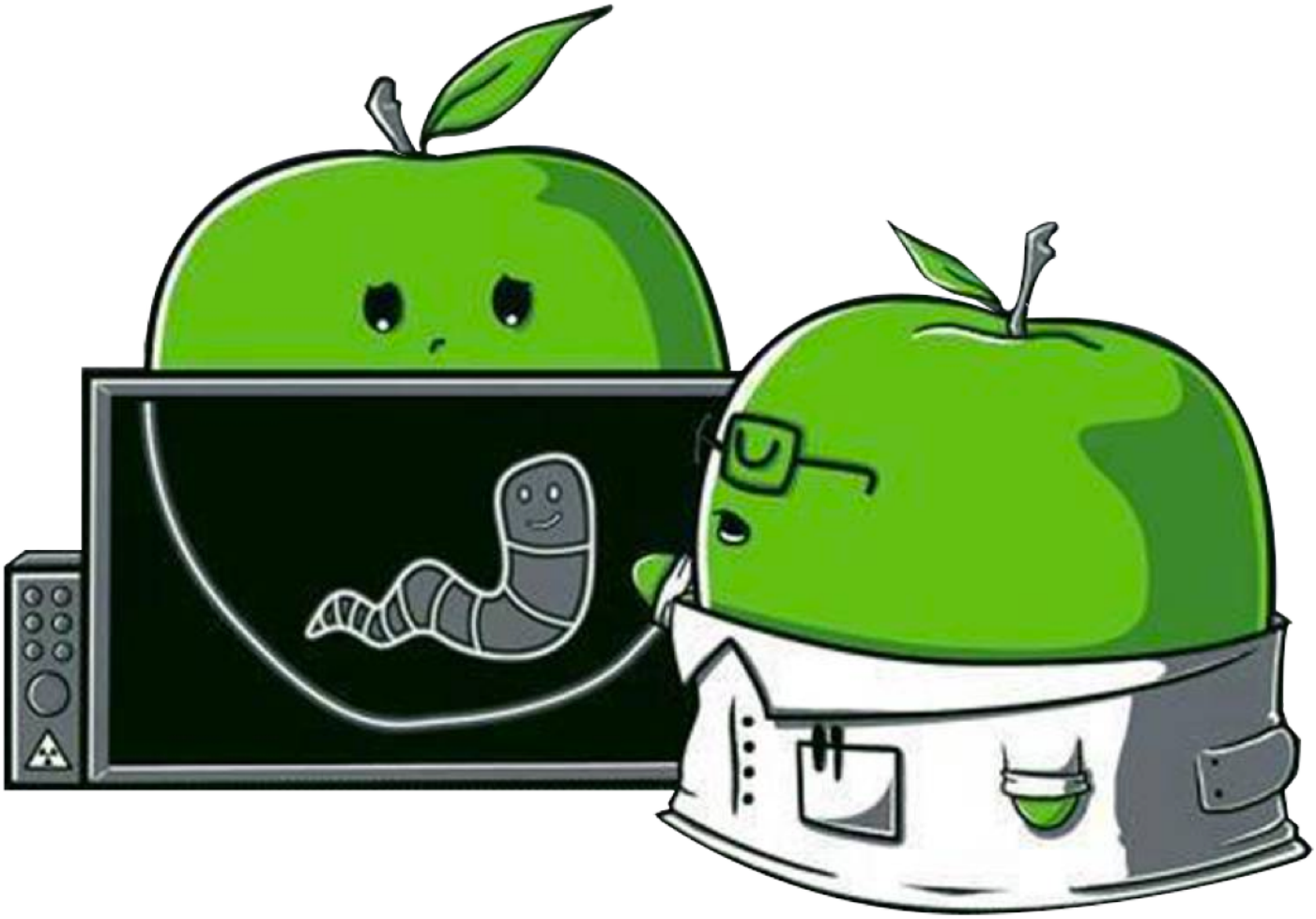

(The Art of Mac Malware) Volume 1: Analysis

Part 0x2: (Mac) Malware Analysis

📝 Note:

This book is a work in progress.

You are encouraged to directly comment on these pages ...suggesting edits, corrections, and/or additional content!

To comment, simply highlight any content, then click the icon which appears (to the right on the document's border).

Armed with a foundational knowledge of Mac malware's infection vectors, persistence mechanisms and capabilities, let's now discuss how to effectively analyze a malicious (or suspected to be) sample!

In order to effectively analyze samples, we'll cover both static and dynamic approaches:

- Static Analysis:
  The examination of a sample (without running/executing it), via various tools often culminating with a disassembler or decompiler.

- Dynamic Analysis:
  The examination of a sample (while running/executing it), via various monitoring tools often culminating with a debugger.

Via these analysis techniques, we'll be able to ascertain if a sample is indeed malicious and, if so, answer questions such as:

- *"What infection vector does it utilize to infect Mac users?"*
- *"What (if any) persistence mechanism is used to maintain access?"*
- *"What are its (ultimate) objectives and capabilities?"*

With the answers to these questions, we can understand what threat the malware poses to Mac users, as well as create both detection and prevention mechanisms to thwart the malware!