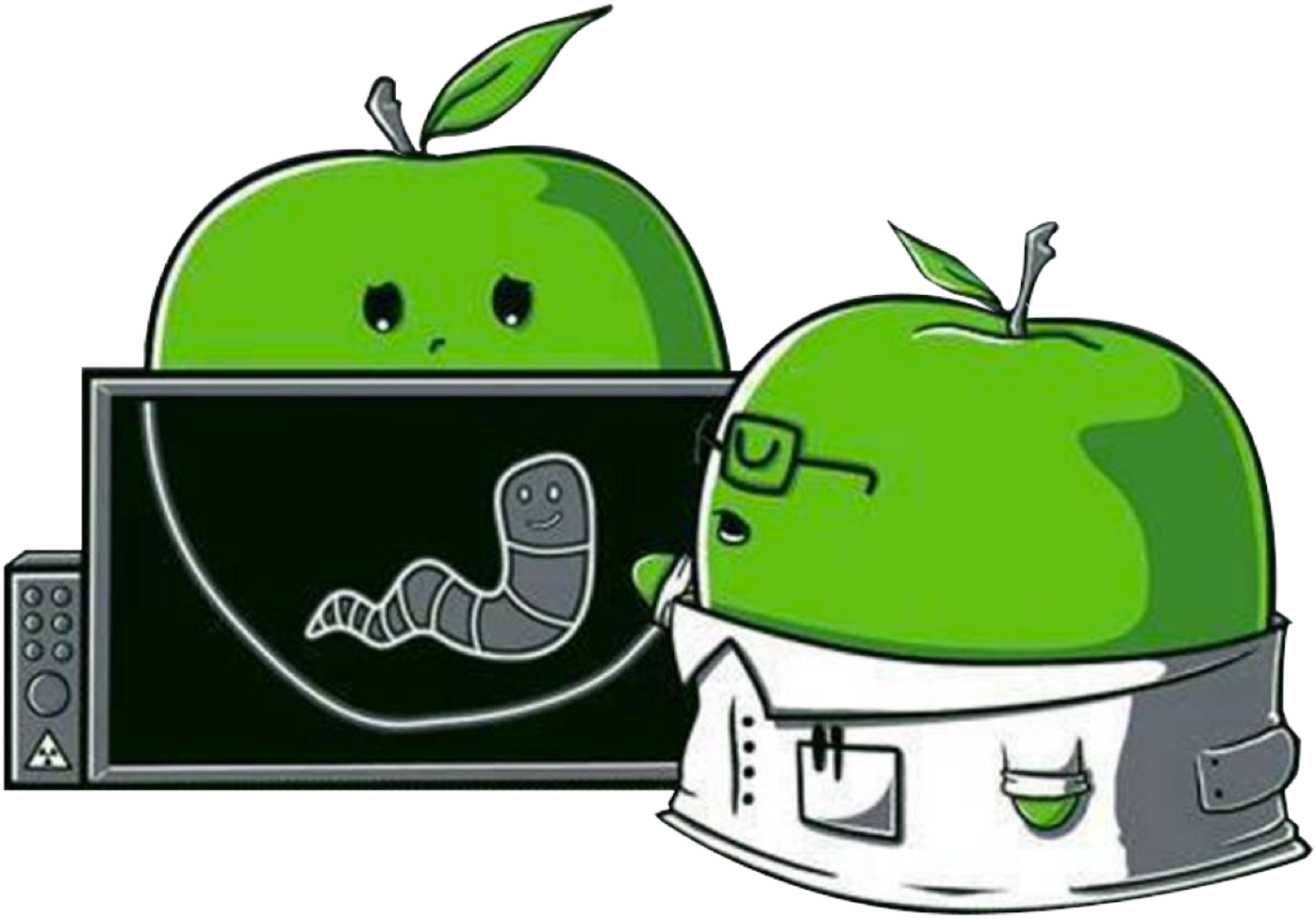

第0x2部分：（Mac）恶意软件分析

笔记:

这本书正在进行中。

我们鼓励您直接在这些页面上发表评论 ...建议编辑、更正和/或其他内容！

要发表评论，只需突出显示任何内容，然后单击 出现在屏幕上的图标
就在文档的边界上）。

由我们的 Friends of Objective-See:


Airo


SmugMug


守护防火墙


SecureMac

iVerify

光环隐私

有了Mac恶意软件感染载体、持久性机制和功能的基础知识，现在让我们讨论如何有效地分析恶意（或疑似）样本！

为了有效地分析样本，我们将介绍静态和动态方法:

- 静力分析:
  通过各种工具对样本进行的检查（不运行/执行），通常以反汇编程序或反编译程序告终。

- 动力分析:
  通过各种监控工具对样本进行的检查（在运行/执行样本时），通常以调试器结束。

通过这些分析技术，我们将能够确定样本是否真的是恶意的，如果是，我们将回答以下问题：:

- “它利用什么感染媒介感染Mac用户？”
- “使用什么（如果有的话）持久性机制来维护访问？”
- “其（最终）目标和能力是什么？”

有了这些问题的答案，我们可以了解恶意软件对Mac用户构成的威胁，并创建检测和预防机制来阻止恶意软件！