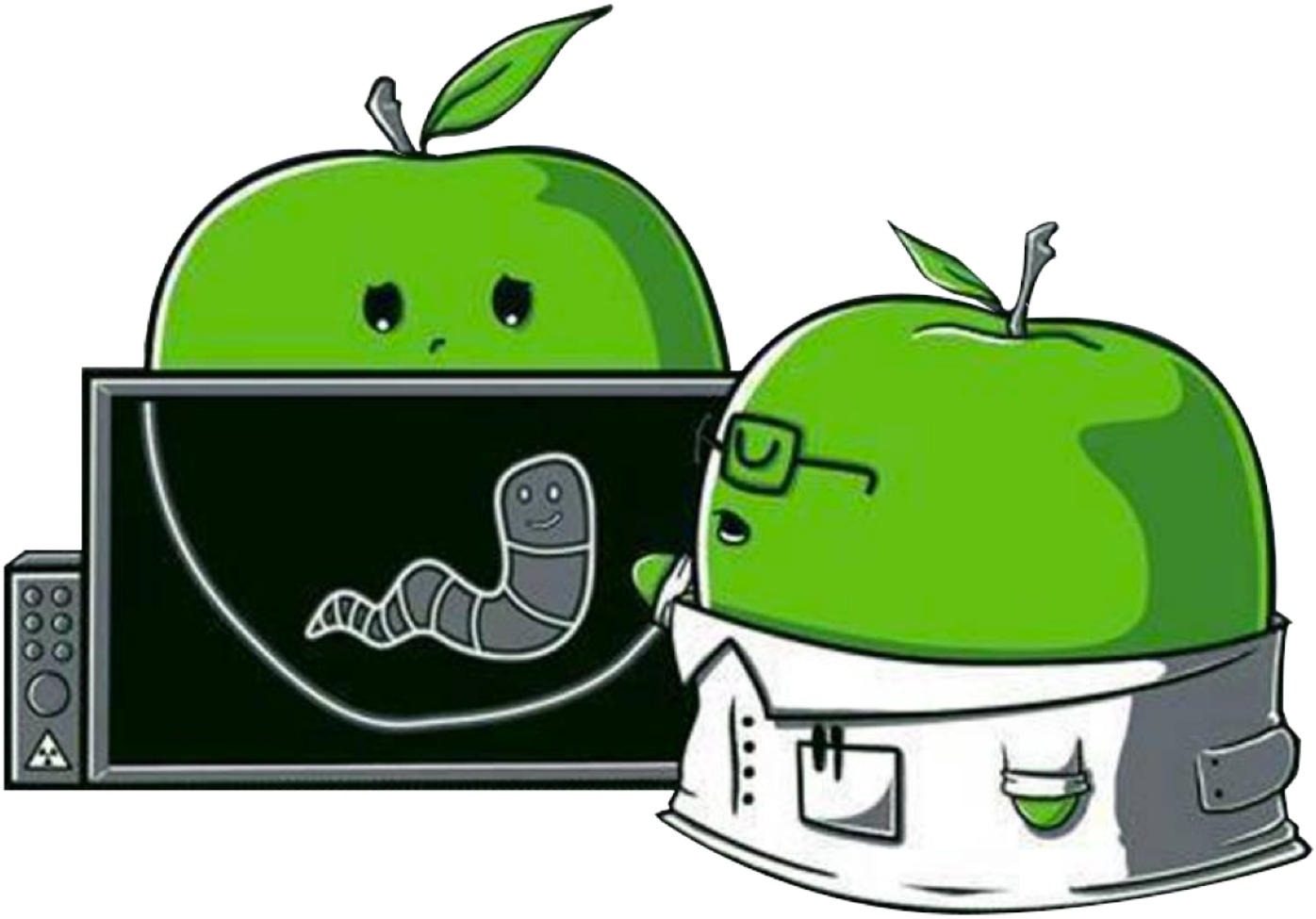


第0x4章：静态分析（简介）

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

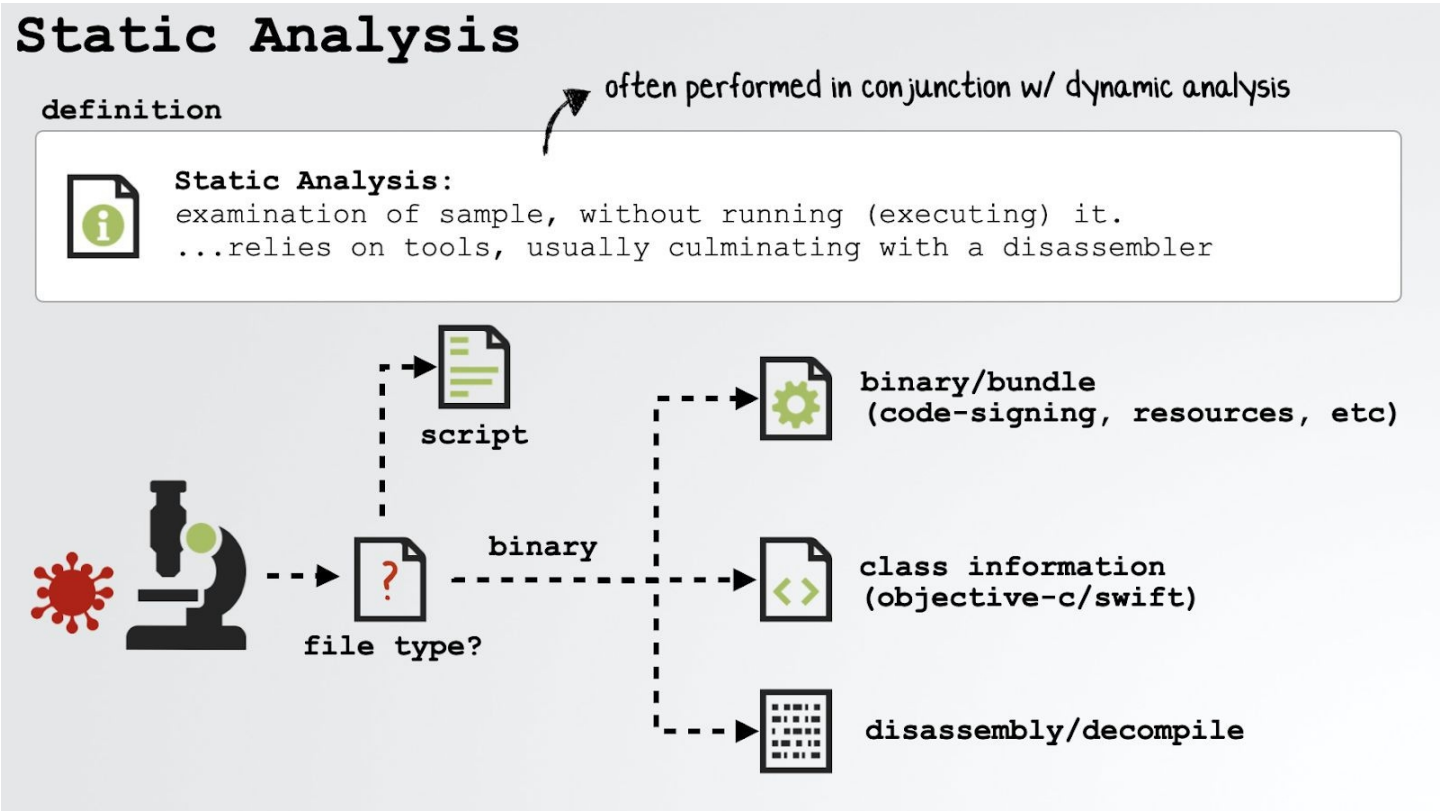
iVerify

光环隐私

静态分析（疑似）恶意软件样本涉及在没有实际运行或执行的情况下检查样本。这种分析依赖于各种静态分析工具，通常以反汇编程序或反编译程序告终。

在本章中，我们将全面介绍静态分析的方法，从基础开始，例如文件类型识别和从安装介质中提取。

一旦样本被提取出来（例如从磁盘映像或包中提取），它通常是两种形式之一：脚本或（Mach-O）二进制文件。



静态分析流程

由于其“纯文本可读性”，脚本很容易手动分析
...尽管我们仍将介绍各种分析技术，并将其应用于现实世界的macOS恶意软件样本。

另一方面，Mach-O可执行文件的二进制格式带来了一些独特的挑战，需要特定的分析工具。因此，这本书的很大一部分是专门介绍这种文件格式的内部结构和相应的静态分析工具。

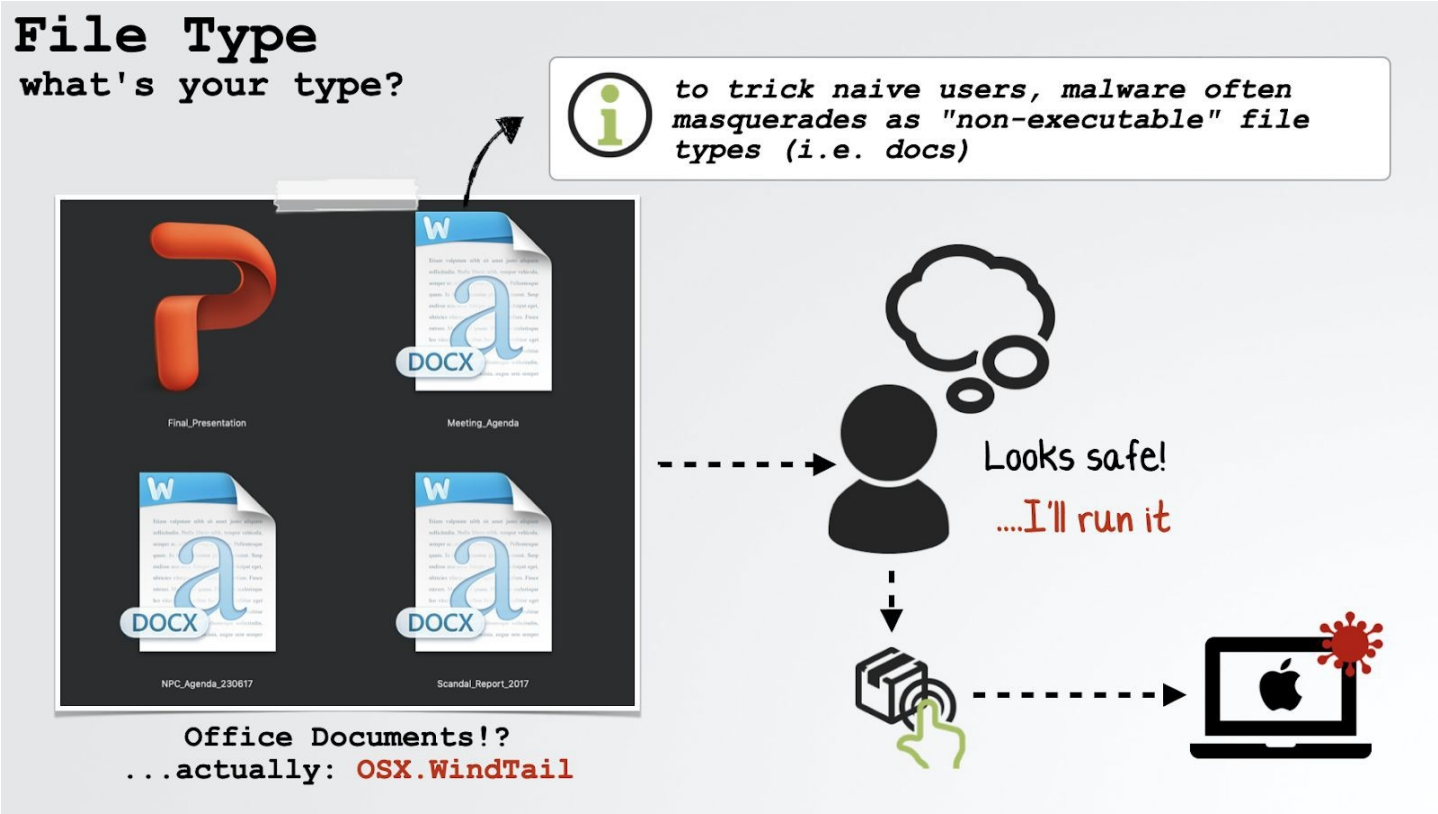
> 笔记:
>
> 静态分析计算机上的恶意软件（即不在虚拟机中）安全吗？
>
> 一般来说，静态分析是静态的 ...这意味着恶意代码永远不会运行。
>
> 尽管如此，始终在分隔的虚拟机中分析恶意软件仍然被认为是最佳实践！安全总比抱歉好，是吗？
>
> 有关设置此类VM的详细概述，请参阅:
>
> “如何在不被感染的情况下逆转macOS上的恶意软件” [1]

文件类型识别

如前所述，大多数（静态）分析工具都是特定于文件类型的。因此，分析（可能是什么）恶意文件的第一步是识别其文件类型。

通常，恶意软件作者会试图掩盖他们创建的真实文件类型，以欺骗或胁迫用户运行它。因此，不言而喻，外观可能具有欺骗性，文件类型不应仅通过其外观（图标）或其文件扩展名来识别。

例如，OSX。WindTail [2]是专门为伪装成良性的Microsoft Office文档而设计的:



伪装成Office文档的恶意软件（OSX.WindTail）

实际上，这些文件是恶意应用程序，在执行时会持续感染系统。

另一方面，恶意文件可能也没有图标，也没有文件扩展名。此外，对此类文件内容的粗略分类可能无法提供有关文件实际类型的线索。

例如，这里有一个（疑似）恶意文件，名为`VtZkT [3] ...`一些未知的二进制格式：

```
00000000  03 f3 0d 0a 97 93 55 5b  63 00 00 00 00 00 00 00  |......U[c.......|
00000010  00 03 00 00 00 40 00 00  00 73 36 00 00 00 64 00  |.....@...s6...d.|
00000020  00 64 01 00 6c 00 00 5a  00 00 64 00 00 64 01 00  |.d..l..Z..d..d..|
00000030  6c 01 00 5a 01 00 65 00  00 6a 02 00 65 01 00 6a  |l..Z..e..j..e..j|
00000040  03 00 64 02 00 83 01 00  83 01 00 64 01 00 04 55  |..d........d...U|
00000050  64 01 00 53 28 03 00 00  00 69 ff ff ff ff 4e 73  |d..S(....i.....Ns|
00000060  d8 08 00 00 65 4a 79 64  56 2b 6c 54 49 6a 6b 55  |....eJydV+lTIjkU|
00000070  2f 38 35 66 51 56 47 31  53 33 71 4c 61 52 78 6e  |/85fQVG1S3qLaRxn|
```

```
00000080  6e 42 6d 6e 4e 6c 73 4f  6c 2b 41 67 49 71 43 67  |nBmnNlsOl+AgIqCg|
00000090  4c 45 76 31 45 53 54 59  46 2b 6c 75 44 69 33 2f  |LEv1ESTYF+luDi3/|
000000a0  39 33 31 4a 4f 6b 32 72  75 47 50 74 46 7a 70 35  |931JOk2ruGPtFzp5|
```

由于静态分析工具在很大程度上是特定于文件类型的，为了继续静态分析，必须识别该文件的类型。那么，我们如何有效地识别文件的格式呢？通过macOS的内置文件命令。如手册页[4]所述，该命令有一项任务：“确定[a]文件的类型”：

```
$ man文件

FILE(1)                    通用命令手册                                FILE(1)

NAME
     文件 -- 确定文件类型
```

例如，在未知的VtZkT文件上运行file命令，会发现该文件是字节编译的Python代码：

```
$ file VtZkT

VtZkT: python 2.7字节编译
```

稍后我们将对此进行详细介绍，但知道一个文件是字节编译的python代码，这使我们能够利用特定于该文件格式的各种工具（例如，我们可以使用python反编译器重建原始python代码的可读表示）。

回到OSX。WindTail，我们可以再次使用文件实用程序来揭示恶意文件（伪装成Office文档）实际上是应用程序包，包含64位Mach-O可执行文件：

```
$ file Final_演示文稿。app/Contents/MacOS/usrnode

usrnode: Mach-O 64位可执行文件x86_64
```

下一个

在本章中，我们介绍了静态分析的概念，并重点介绍了macOS内置的文件实用程序如何有效地识别文件的真实类型。当然，这是重要的第一步，因为许多静态分析工具都是特定于文件类型的！

接下来，让我们看看在分析Mac恶意软件时可能遇到的各种文件类型。一些文件类型（例如磁盘映像）只是用来分发恶意软件，因此目标是提取恶意内容进行分析。实际的恶意软件有多种其他文件格式，如脚本和二进制文件。

对于每种文件类型，我们将简要讨论其用途，并重点介绍可用于分析所述文件格式的静态分析工具。

参考文献

1. “如何在不受感染的情况下逆转macOS上的恶意软件”
https://www.sentinelone.com/blog/how-to-reverse-macos-malware-part-one/

2. “中东网络间谍：分析WindShift的植入物：OSX.WindTail” https://objective-see.com/blog/blog_0x3B.html

3. “Mac广告软件，就像Python”
https://objective-see.com/blog/blog_0x3F.html

4. 文件实用程序
x-man-page://file