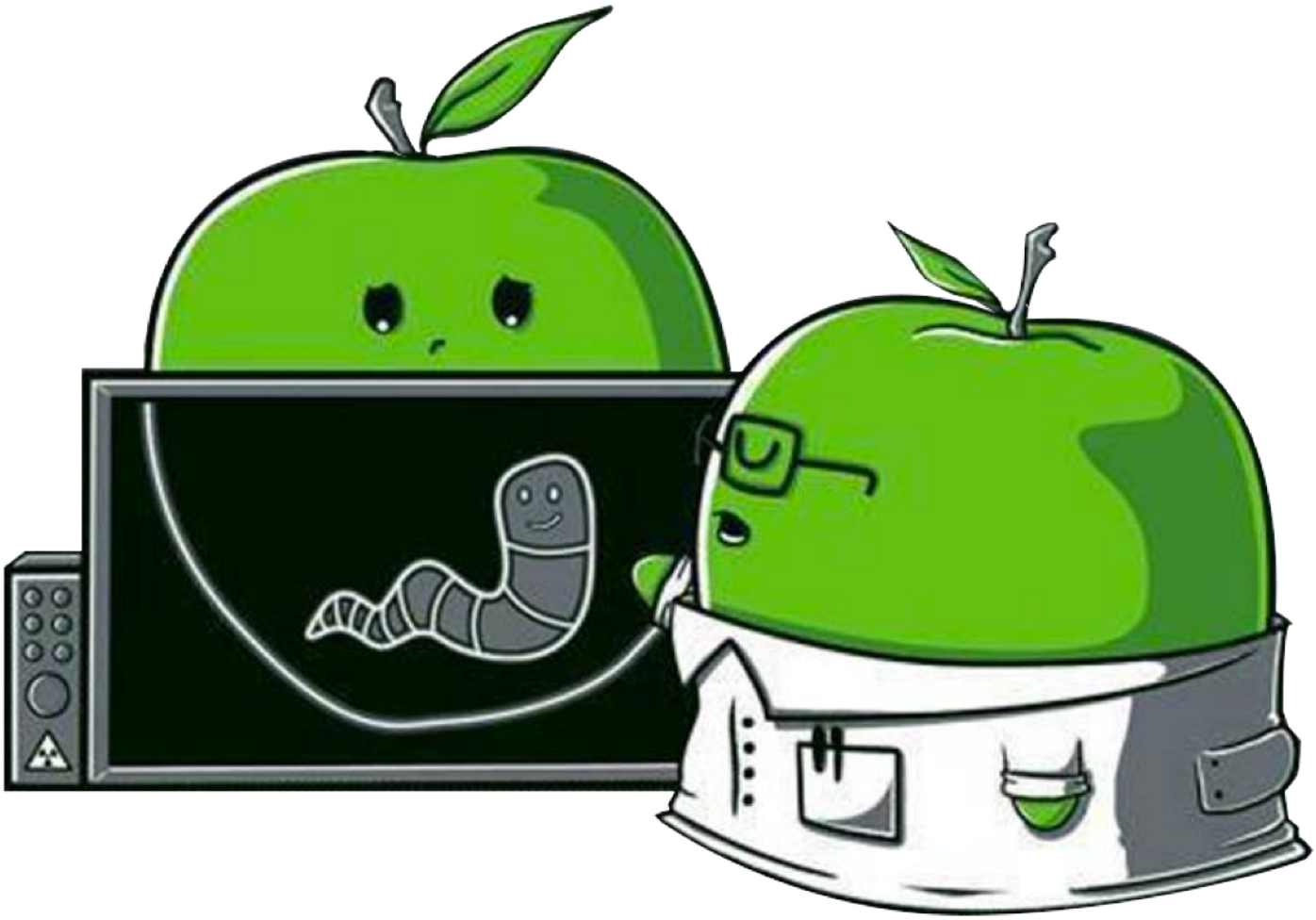


第0x8章：动态分析

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）。

在前几章中，我们讨论了静态分析的方法 ...利用（静态）分析工具深入了解和理解恶意文件和二进制文件的方法。根据定义，这种分析涉及静态地检查所述项目，而不是实际运行或执行它们。

然而，通常情况下，为了（被动地）观察恶意文件的行为和动作，简单地执行恶意文件可能更有效。当恶意软件作者实施了专门设计用于使静态分析复杂化甚至阻碍静态分析的机制时，尤其如此 ...例如加密嵌入的字符串和/或配置信息。奥斯。Windtail [1]提供了一个示例；其命令和控制服务器的地址（通常是恶意软件分析人员会试图发现的）是base64编码和AES加密的:

```
01 r14 = [NSString stringWithFormat:@"%@", [self
02 yoop:@"F5Ur0CCFMO/fWHjecxEqGLy/xq5gE98ZviUSLrtFPmGyV7vZdBX2PYYAIfmUcgXHjNZe3ibndAJ
03 Ah1fA69AHwjVjD0L+Oy/rbhmw9RF/OLs="]];
04
05 rbx = [[NSMutableURLRequest alloc] init];
06 [rbx setURL:[NSURL URLWithString:r14]];
07
08 [[[NSString alloc] initWithData:[NSURLConnection sendSynchronousRequest:rbx
09 returningResponse:0x0 error:0x0] encoding:0x4] isEqualToString:@"1"]
```

加密的命令和控制服务器地址（OSX.WindTail）

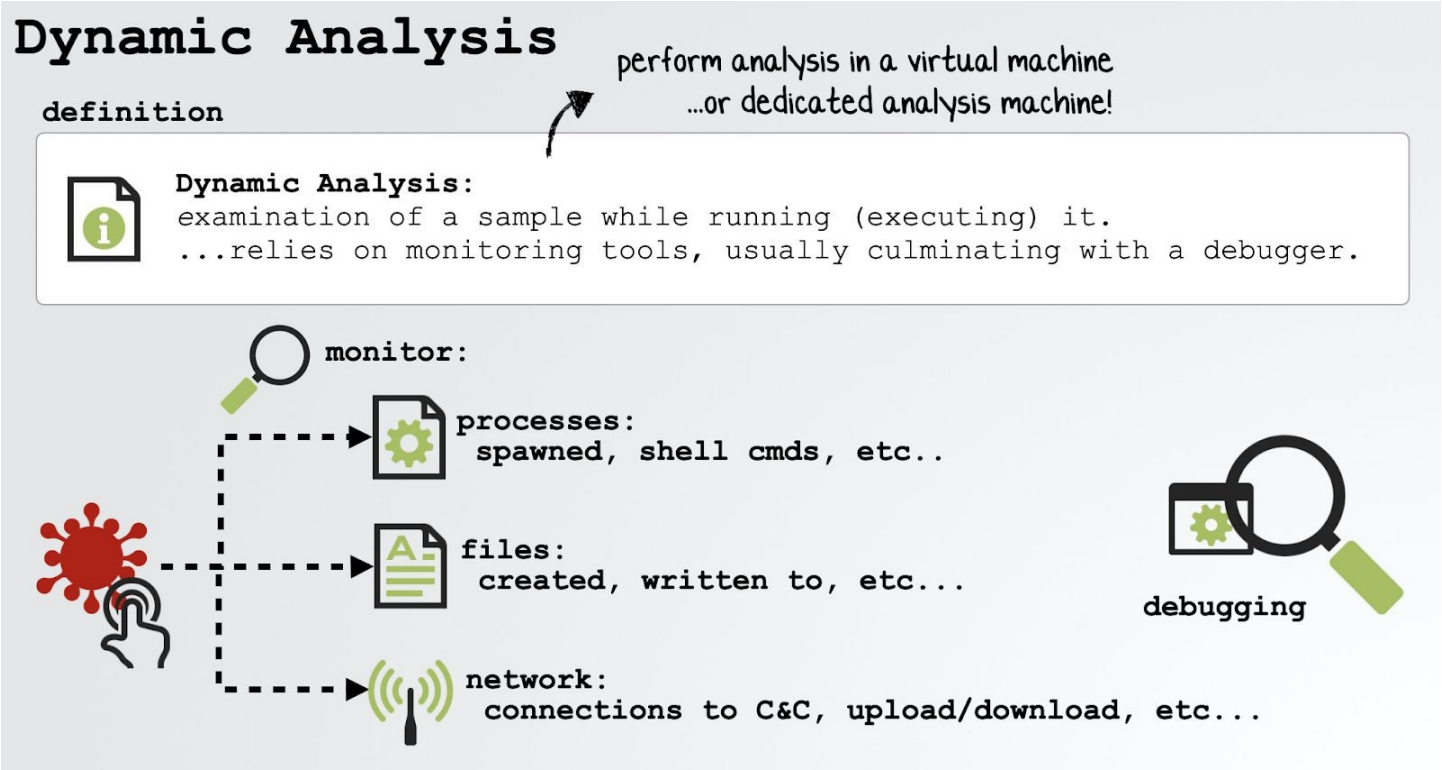
现在，可以手动解码和解密“F5Ur0CCFMO/fWHjecxE”...9RF/OLs=“string（因为加密密钥在恶意软件中是硬编码的）。然而，当恶意软件试图建立连接时，简单地执行恶意软件并通过动态分析工具（如网络监视器）被动地确定服务器的地址要容易得多。

在本章中，我们将深入探讨动态分析方法，作为被动观察和理解Mac恶意软件样本的一种手段。

我们将首先关注:

- 过程监控
- 文件监控
- 网络监控

在讨论这些监控工具和技术之后，我们将研究更高级的动态分析技术，例如调试恶意二进制文件。



动力分析

笔记:

在本书的这一部分中，我们将讨论涉及执行恶意软件（观察其行为）的动态分析方法。因此，请始终在分隔的虚拟机中执行此类分析，或者最好在专用恶意软件分析机上执行此类分析。

...换句话说，不要在主（基本）系统上执行动态分析！

有关为（macOS）恶意软件分析设置虚拟机的详细“操作方法”，请参阅：

“如何在不被感染的情况下逆转macOS上的恶意软件” [2]

参考文献

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

2. “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/