

(Mac恶意软件的艺术) 第一卷：分析


## 第0x1部分：(Mac) 恶意软件基础

### 📝 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  
就在文档的边界上）。

 出现在屏幕上的图标

由我们的 [Friends of Objective-See](#):



[Airo](#)



[SmugMug](#)



[守护防火墙](#)



[SecureMac](#)



[iVerify](#)



[光环隐私](#)

首先，让我们讨论一下（Mac）恶意软件的各种基础主题，因为在深入研究更高级的主题之前，有这样的基础是很重要的。

在本介绍部分，我们将介绍Mac恶意软件的功能：

- 感染媒介：

恶意软件访问（即感染）系统的方式。

虽然社会工程方法目前已成为常态，但其他更具创造性和隐蔽性的感染系统方法也越来越受欢迎。

- 持久性方法：

恶意软件确保在系统启动或用户登录时由操作系统自动（重新）执行的方式。

虽然经常使用一些方法（ab），但恶意软件可以通过无数秘密手段获得持久性。

- 能力：

恶意软件的有效载荷（即其目标）。

由网络罪犯创建的恶意软件通常对经济利益感兴趣，而网络间谍（国家赞助）恶意软件则试图监视用户。