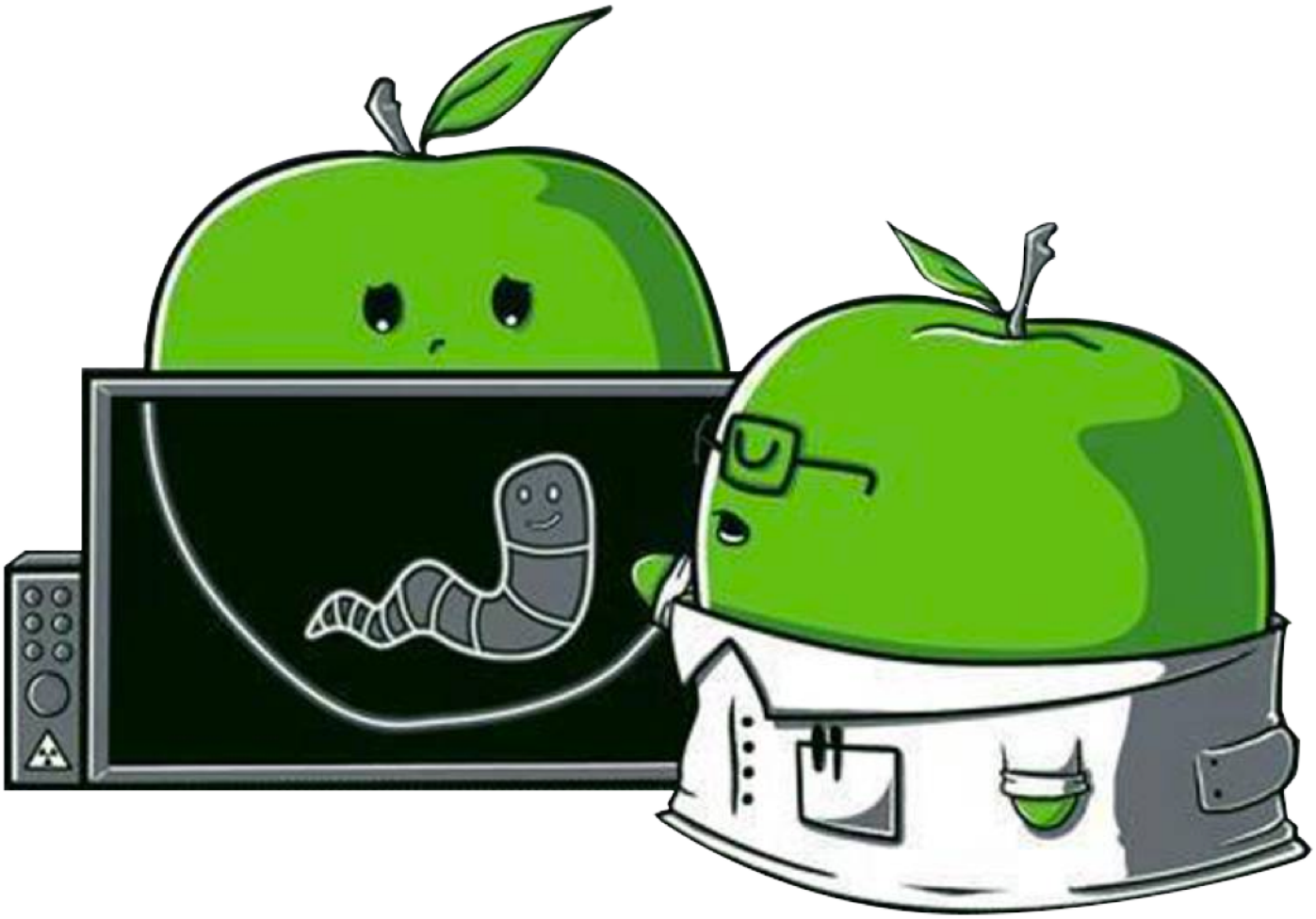


（Mac恶意软件的艺术）第一卷：分析

第0x0部分：导言

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

全面分析（Mac）恶意软件是一个多方面的话题，需要大量的知识和技能。

在这本书中，我们以实际动手的方式介绍了这些知识和技能。 此外，如果相关，会为感兴趣的读者提供指向更详细资源的链接。

从Mac恶意软件基础知识（第0x1部分）开始，我们将过渡到更高级的主题，如静态和动态分析工具和技术（第0x2部分）。最后，我们将应用本书所教的所有内容，对一个复杂的Mac恶意软件样本进行全面分析[第0x3部分]。

有了这些知识，你将很快成为一名熟练的Mac恶意软件分析师！


笔记:

如果在任何时候你觉得有点不知所措，跳到参考资料部分（附录B）。

它充满了（其他）资源，涵盖了广泛的主题，如逆向工程、macOS内部和通用恶意软件分析。

确认

首先，我要感谢我在信息安全社区的许多朋友和同事，这些年来他们的指导和支持是无价的！

我想亲自感谢Objective See的许多赞助人，他们的持续支持使这本书成为现实。

我还要感谢参与“客观之友”计划的公司和产品：

Airo AV (https://www.airoav.com/):
专门为Mac OS提供防病毒保护。





SmugMug 守护防火墙 SecureMac iVerify 光环隐私

...因为他们也帮助这本书看到了光明！

最后，感谢Runa Sandvik宝贵的输入和编辑技巧，感谢她！

> 笔记:
>
> 想支持我们吗？
>
> - 如果你是个人，请加入我们 patreon!
> - 如果你是一家公司，加入我们的“Friends of Objective-See” program!
>
> 玛哈洛

Mac vs.恶意软件

Mac电脑有恶意软件吗？如果我们相信苹果的营销声明曾经发布在 Apple.com ...apparently no!?

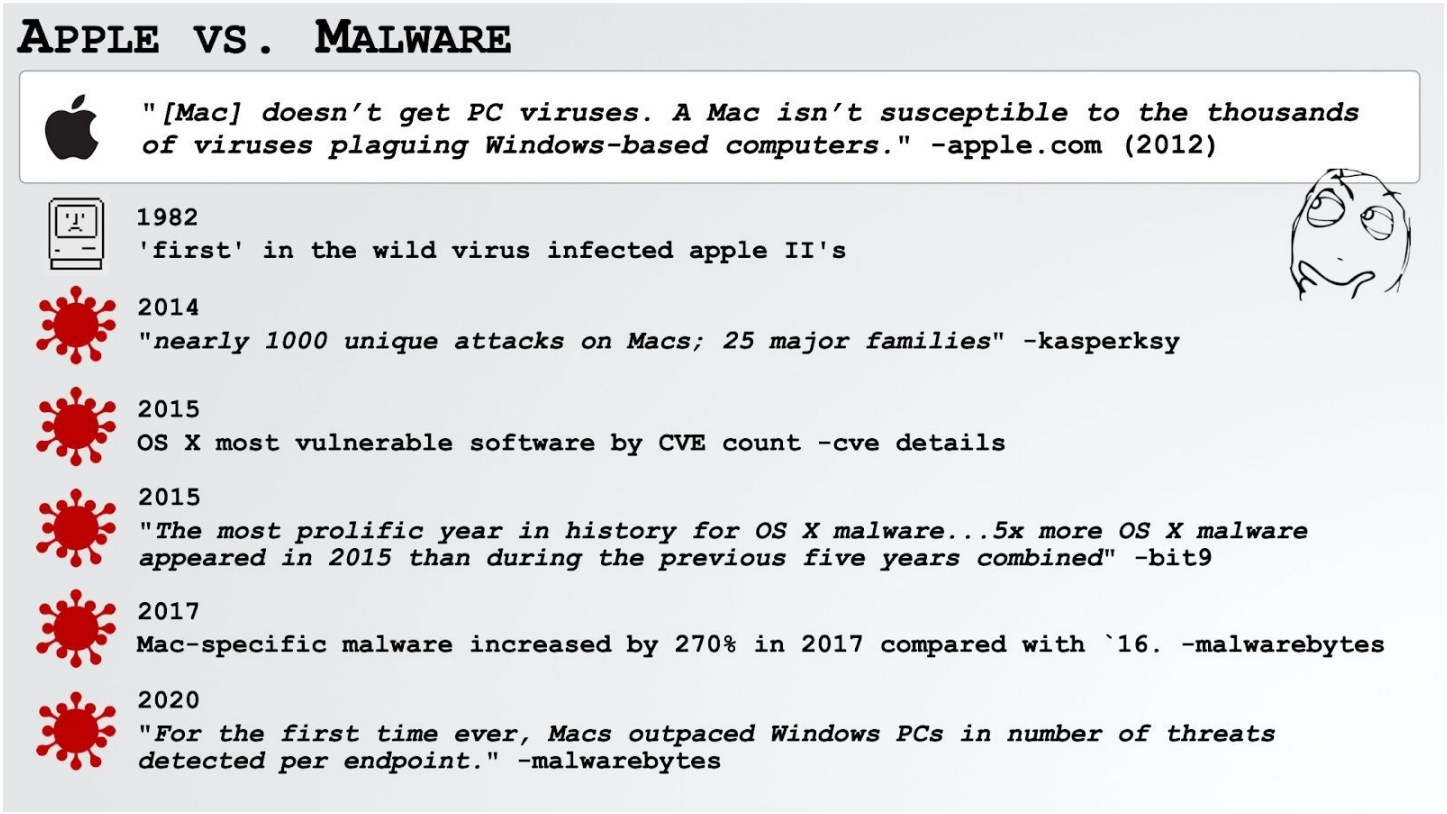
> “[Mac]不会感染电脑病毒。Mac电脑不易受到困扰Windows电脑的数千种病毒的影响。这要归功于Mac OS X中的内置防御系统，它可以让你在不做任何工作的情况下保持安全” [1]

当然，这一声明既有欺骗性，也不准确，（值得赞扬的是）早就从他们的网站上删除了[1]。

> 笔记:
>
> 这一微妙声明的“真相”在于，由于固有的跨平台不兼容（而非苹果的“防御”）：原生Windows病毒无法直接在macOS上执行。
>
> 然而，即使是这种说法也相当主观，2019年针对macOS用户的Windows广告软件样本也强调了这一点。该广告软件采用了跨平台框架（Mono），允许Windows二进制文件（.exe）在macOS上“本机”运行！
>
> 请参见:
>
> “Windows应用程序在Mac上运行，下载信息窃取软件和广告软件” [2]
>
> 而且，即使在2012年，也可能发现针对Windows和macOS的跨平台恶意软件:
>
> “一个可以同时感染Windows和Mac OS X计算机的单一恶意软件” [3]

有趣的是，苹果和恶意软件有着悠久的历史。事实上，Elk Cloner[4]“第一个家用电脑的野生病毒” [4],感染了苹果的操作系统！

从那时起，针对苹果电脑的恶意软件继续蓬勃发展（尽管程度低于Windows系统）:



苹果与恶意软件的简短时间线。

如今，Mac恶意软件的威胁越来越大也就不足为奇了 ...对最终用户和企业都是如此。

这一趋势有很多原因，但一个简单的原因是，随着苹果在全球计算机市场份额的增长，Mac电脑成为机会主义黑客和恶意软件作者越来越引人注目的目标。（据Gartner称，“苹果在2019年第一季度出货397.7万台macOS”[5]）。

换句话说：

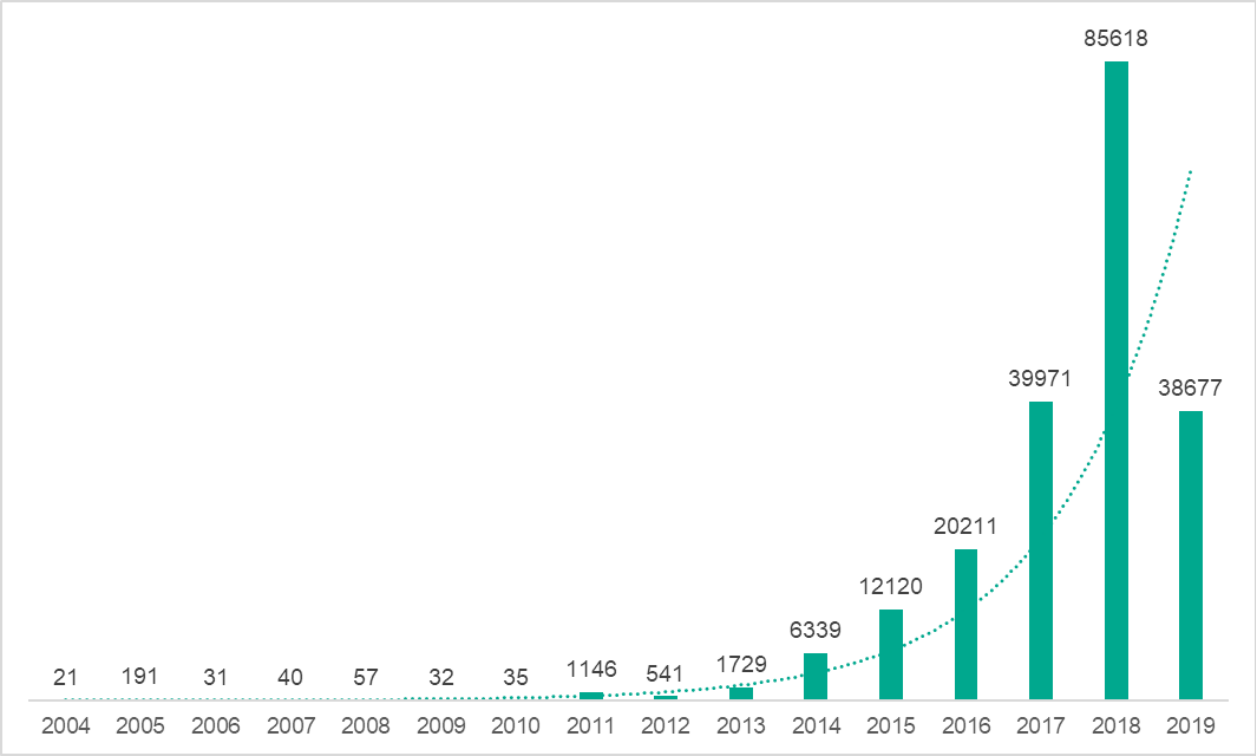
更多~~苹果~~→ 更多目标→ 更多~~多~~Mac恶意软件

还需要注意的是，尽管Mac电脑通常被认为主要是以消费者为中心的机器，但它们在企业中的普及率正在迅速增加。2020年初的一份研究这一趋势的报告大胆地指出，“Mac是一台企业机器”，并指出“苹果在企业中继续增长，其系统在《财富》500强中使用”。[6] 这种增长（不幸的是）也导致专门针对macOS企业（即工业间谍）的复杂攻击和恶意软件的同时增加。

尽管苹果的市场份额仍然（在很大程度上）落后于微软，但一些研究表明，Mac电脑同样（如果不是更多的话）受到恶意威胁的攻击。例如，Malwarebytes在他们的2020 State of Malware Report”：

> “在每个端点检测到的威胁数量上，Mac首次超过Windows PC。” [7]

卡巴斯基在2019年的一份报告《macOS用户面临的威胁》[8]中还指出，针对mac的威胁（恶意软件和广告软件）急剧上升：



“2004-2019年macOS恶意和潜在不需要的文件数量” [8]

笔记:

1. 此类统计数据通常包括广告软件（和/或“可能不需要的程序”）。
2. 恶意软件和广告软件之间的区别相当微妙，它们的区别继续模糊。因此，我们通常不会区分两者；将两者简单地称为恶意软件。
3. 当然，随着苹果提高macOS的安全性，这对苹果来说变得更加困难

> 成功感染Mac电脑的恶意软件（和广告软件）。
>
> 然而，这不太可能对有动机的恶意软件作者构成真正的障碍。

有趣的是（尽管并不意外），2020年的一份报告[9]也强调了由知识渊博的macOS黑客发起的针对Mac的独特恶意软件攻击的增长趋势：

> “以上审查的所有样本都是在过去八到十周内出现的，都是威胁行为者的证据 ...他们自己也在与苹果平台保持同步。他们不仅是将Windows恶意软件移植到macOS的参与者，而且是专门针对mac的开发人员，他们在为苹果平台编写定制恶意软件方面投入了大量资金。” [9]

如以下示例所示，这种深度和知识导致针对macOS及其用户的攻击和恶意软件的复杂性增加：

- 使用0天：
  “被火烧（fox）：Firefox 0day掉了macOS后门”

  “通过Firefox 0day,攻击者持续部署macOS二进制文件…[a]针对加密货币兑换的复杂目标攻击的持续有效载荷” [9]

- 精密瞄准：
  “在WINDSHIFT APT的尾部”

  “观察到WINDSHIFT针对特定个人发起复杂且不可预测的鱼叉式网络钓鱼攻击，很少针对公司环境” [10]

- 先进（隐形）技术：Lazarus Group Goes 'Fileless'”

  “Lazarus group继续以具有不断发展的功能的macOS用户为目标 ...[例如]一个新的样本，能够直接从内存远程下载和执行有效负载！” [11]

- 绕过（最近的）macOS安全功能：
  “新的Mac恶意软件使用‘新颖’策略绕过macOS Catalina安全性”

> “安全研究人员 ...在野外发现了一种新的Mac恶意软件，它诱使用户绕过现代macOS应用程序的安全保护。” [12]

这种攻击复杂性的增加是为了应对Mac用户变得更加敏感的威胁（阅读：不那么幼稚）和免费macOS安全工具的可用性增加，还是苹果提高macOS的核心安全性，或者两者的结合，这一点值得商榷。

Kaspersky’s 2019 “Threats to macOS users报告[8]对“Mac vs.恶意软件”的讨论进行了非常清晰和简洁的总结：

> “我们关于macOS威胁的统计数据提供了相当有说服力的证据，证明该操作系统的完全安全性仅此而已。然而，反对macOS（以及iOS）的最大理由是不受攻击是因为已经有针对这些操作系统的个人用户和此类用户组的攻击。在过去几年中，我们看到至少有八场活动的组织者基于这样的假设采取行动，即MacBook、iPhone和其他设备的用户预计不会遇到专为苹果平台创建的恶意软件。” [8]

总之，很明显Mac恶意软件将继续存在 ...它的复杂性和阴险性只会继续增加。

下一个

随着针对苹果桌面操作系统的恶意软件越来越普遍和复杂，我们必须做出回应！而且，（尽管可能是陈词滥调），知识才是真正的力量。

因此，请继续阅读！本书提供了全面理解和应对这些潜在威胁的知识。

> 笔记:
>
> 对于想深入研究或亲身实践的感兴趣读者，本书中引用的（大多数）恶意软件样本可从Objective See下载online malware collection [12].
>
> 收集标本的密码为：infect3d

...值得重申的是，本系列包含实时恶意软件，因此，请不要感染自己！

参考文献

1. “Mac电脑和恶意软件—看看苹果如何改变其营销信息” https://nakedsecurity.sophos.com/2012/06/14/mac-malware-apple-marketing-message/

2. “Windows应用程序在Mac上运行，下载信息窃取程序和广告软件” https://blog.trendmicro.com/trendlabs-security-intelligence/windows-app-runs-on-mac -downloads-info-stealer-and-adware/

3. “跨平台恶意软件利用Java攻击PC和Mac” https://www.zdnet.com/article/cross-platform-malware-exploits-java-to-attack-pcs-an d-macs/

4. 埃尔科克隆者 http://virus.wikidot.com/elk-cloner

5. “苹果在全球计算机市场的份额增长” https://www.cultofmac.com/618730/q1-2019-pc-market-apple-mac-gartner/

6. “随着Apple enterprise reach的增长，SAP对Mac的采用率翻了一番” https://www.applemust.com/mac-adoption-at-sap-double-as-apple-enterprise-reach-grow s/

7. “2020年恶意软件状况报告” https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report-1.pdf

8. “对macOS用户的威胁” https://securelist.com/threats-to-macos-users/93116/#malicious-and-unwanted-programs-for-macos

9. “四个不同的Lazarus恶意软件家族以苹果的macOS平台为目标” https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-a pples-macos-platform/

10. “被火烧（fox）第一部分：firefox 0day掉了macOS后门” https://objective-see.com/blog/blog_0x43.html

11. “在WINDSHIFT APT的尾部” https://gsec.hitb.org/materials/sg2018/D1%20COMMSEC%20-%20In%20the%20Trails%20of%20 WINDSHIFT%20APT%20-%20Taha%20Karim.pdf

12.“Lazarus Group走向‘无文件化’：远程下载和内存执行的植入”
https://objective-see.com/blog/blog_0x51.html

13.“新的Mac恶意软件使用‘新颖’策略绕过macOS Catalina安全性”
https://appleinsider.com/articles/20/06/18/new-mac-malware-uses-novel-tactic-to-byp ass-macos-catalina-security

14.Objective See的恶意软件收藏
https://objective-see.com/malware.html