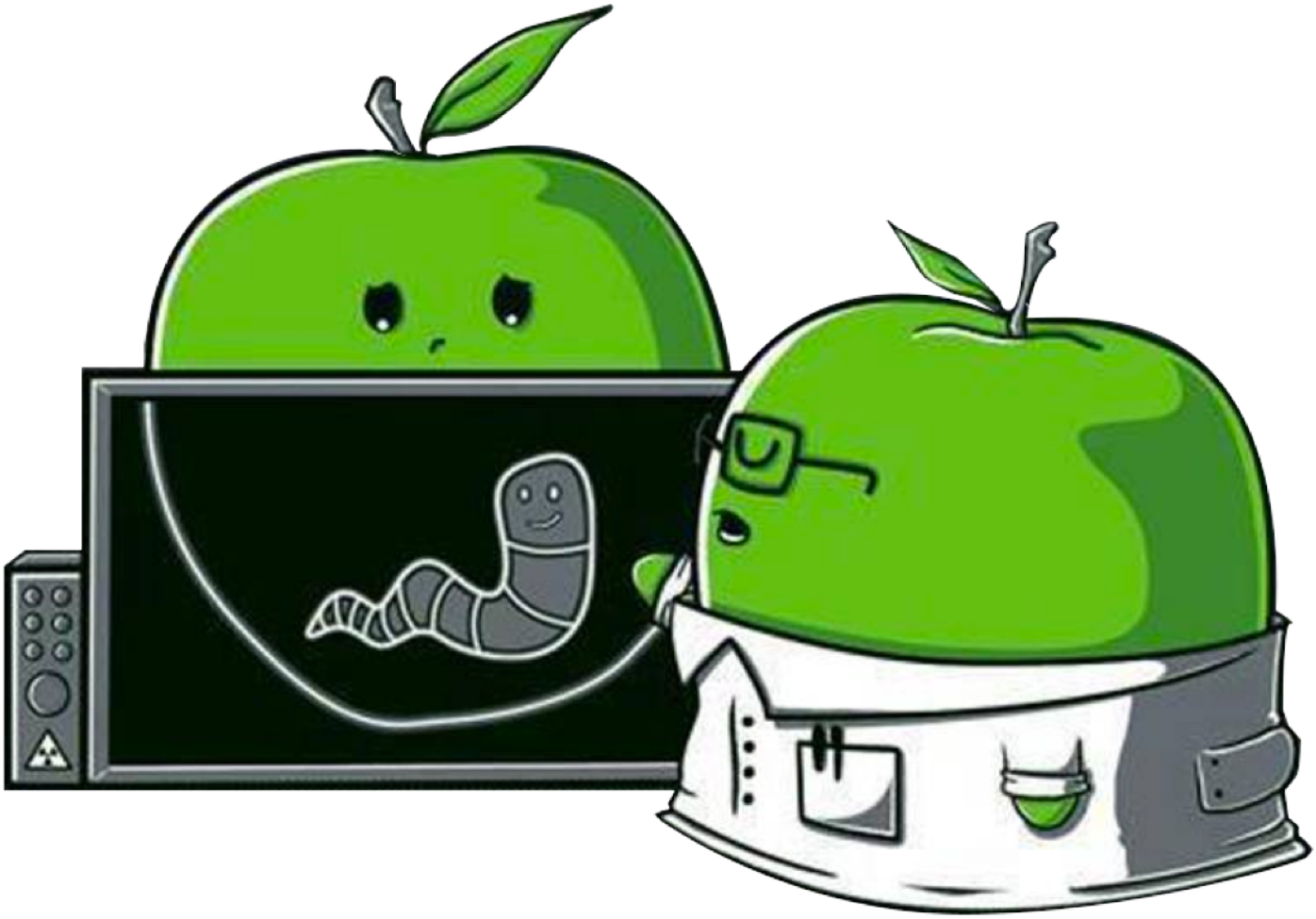


（Mac恶意软件的艺术）第一卷：分析

第0x1章：感染媒介

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

恶意软件的感染载体是指它访问（即感染）系统的方式。

多年来，恶意软件作者一直依赖各种机制，从社会工程技巧到先进的远程0天攻击。

在这里，我们将讨论Mac恶意软件作者使用的一些最常见的技术（ab）。

到目前为止，用恶意代码感染Mac用户最常见的方法是欺骗或强迫用户感染自己 ...换句话说，直接下载并运行恶意代码（而不是远程攻击）。

如前所述，需要诱骗用户（直接）感染恶意软件的几种常见社会工程攻击包括:

- 虚假更新
- 假申请
- 特洛伊木马程序
- （受感染的）盗版应用程序

笔记:

为了阻止（或至少反击）这些“用户辅助”感染媒介，苹果在macOS 10.15（Catalina）中引入了应用程序公证要求。

这些要求确保苹果在允许在macOS上运行之前已经扫描（并批准）了所有软件:

“公证让用户更加相信，你发行的开发者id签名软件已经被苹果检查过是否存在恶意组件。” [1]

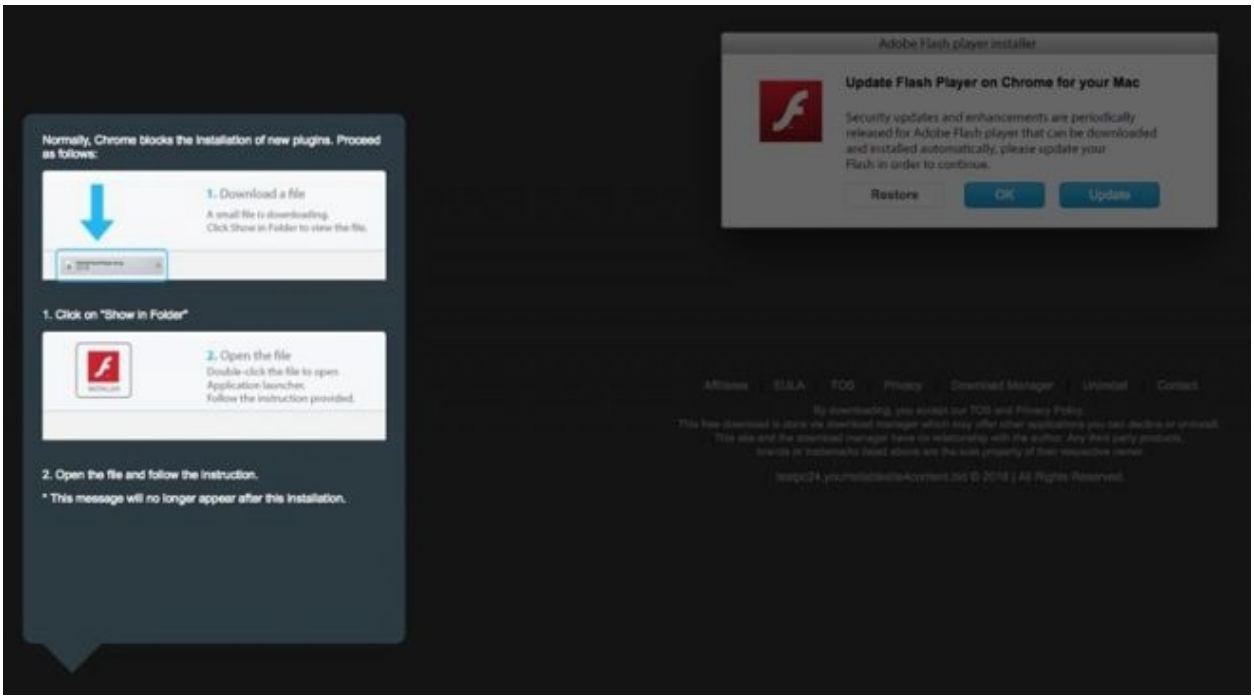
尽管并非绝对正确，但这是对抗基本macOS感染媒介的一个极好的步骤 ...尽管恶意软件作者已经很快适应了。[2]

虚假更新（通过浏览器弹出窗口）

如果你是Mac用户，在浏览网页时可能会遇到恶意弹出窗口。“更新你的Flash播放器”尖叫一个模式浏览器弹出链接到下载（完全）不令人惊讶的是不是一个合法的Flash更新，而是恶意软件或广告软件。

这种强迫用户感染自己的常见方法包括恶意网站（尤其是那些提供“免费”（视频）内容的网站）或合法网站上的恶意广告，显示误导性的弹出窗口。

广告软件，如OSX。Shlayer [3]特别喜欢这种感染载体：



假冒Flash播放器更新（ OSX.Shlayer）[3]

不幸的是，有一定比例的Mac用户会受到这种类型的攻击，认为更新是“必需的”，从而在过程中感染自己。

> 笔记:
>
> 为了直接响应macOS Catalina的公证要求，攻击涉及

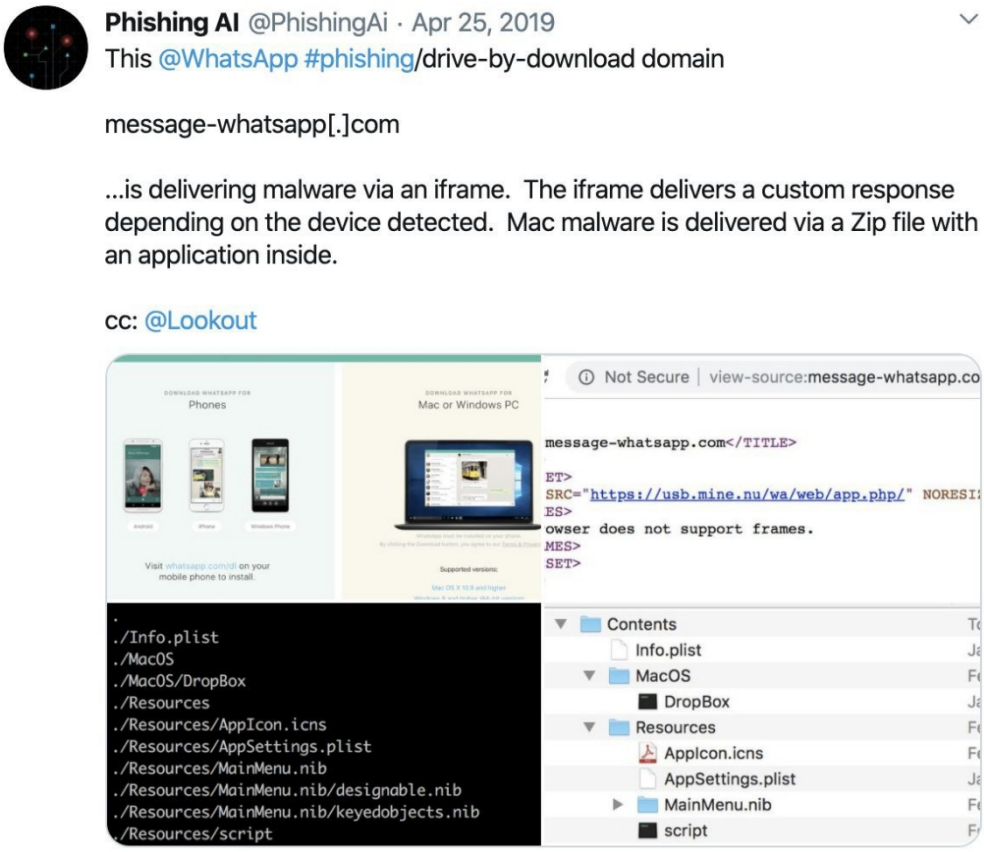
奥斯。Shlayer，现在利用“用户辅助”公证绕过。 有关详细信息，请参阅：

“新的Mac恶意软件使用‘新颖’策略绕过macOS Catalina安全” [2]

假申请

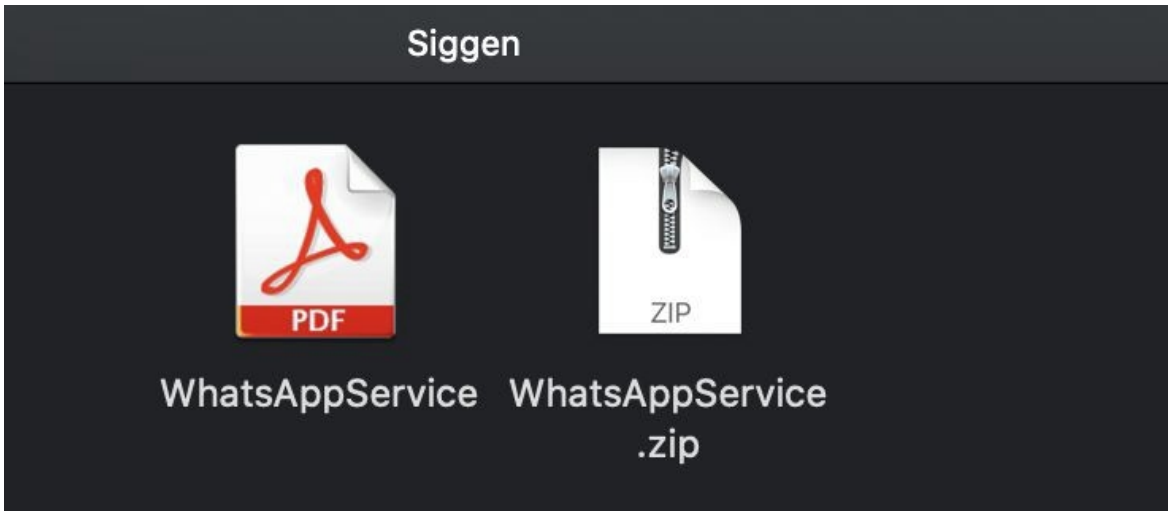
攻击者非常喜欢通过假应用程序攻击Mac用户。此感染向量依赖于强制用户下载并运行伪装成合法内容的恶意应用程序。

例如，OSX。Siggen [4][5]通过模仿流行的WhatsApp消息应用程序，瞄准macOS用户。正如@PhishingAi在推文中所解释的，一个iFrame托管在消息whatsapp[.]com将：“交付...包含[恶意]应用程序的zip文件“[6]



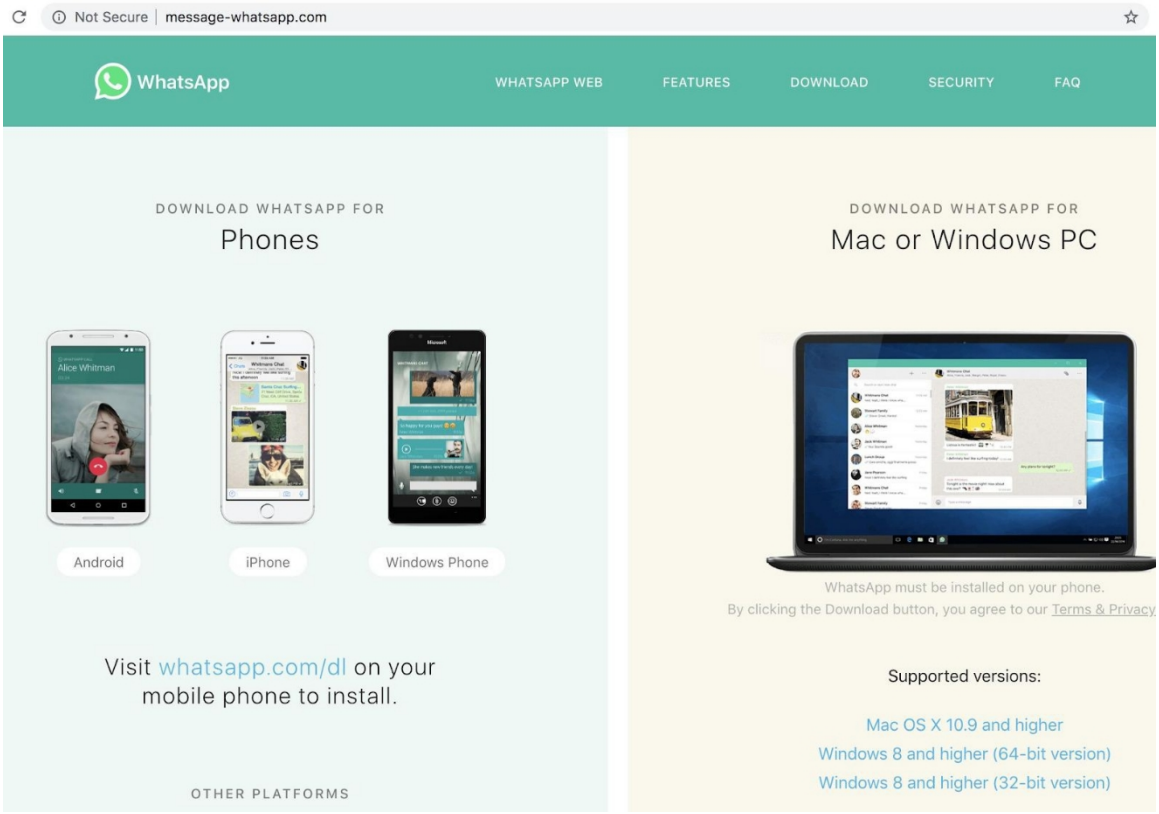
OSX的初步细节。西格根[6]

正如@PhishingAi所指出的，下载的是一个名为WhatsAppWeb的zip存档。拉链 ...这（惊喜，惊喜）不是官方的WhatsApp应用程序，而是一个名为WhatsAppService的恶意应用程序:



WhatsAppService
(OSX.Siggen)

作为whatsapp[.]的信息com网站看起来（有些）合法，也许普通用户不会注意到任何错误，会下载并运行假应用程序，从而感染自己:



message-whatsapp[.]com

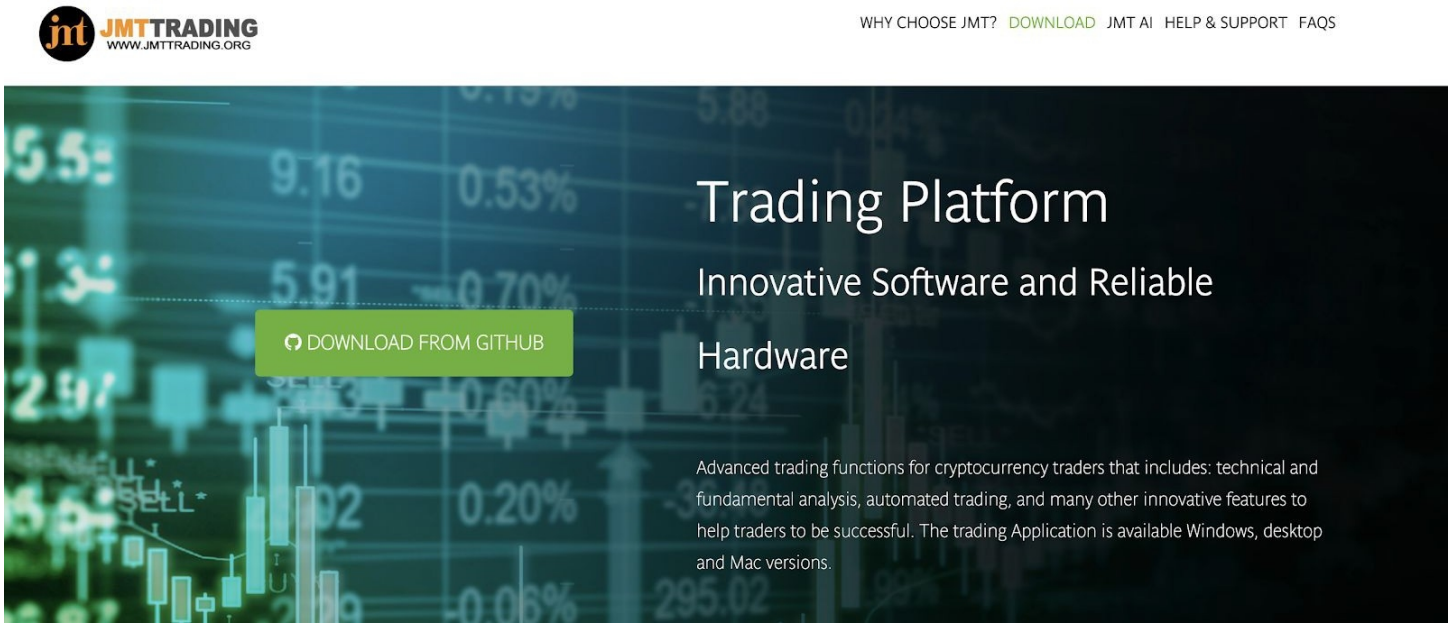
笔记:

1. 通过网站，消息whatsapp[.]com会自动下载。zip文件（包含恶意软件），用户仍需手动解压并执行恶意软件

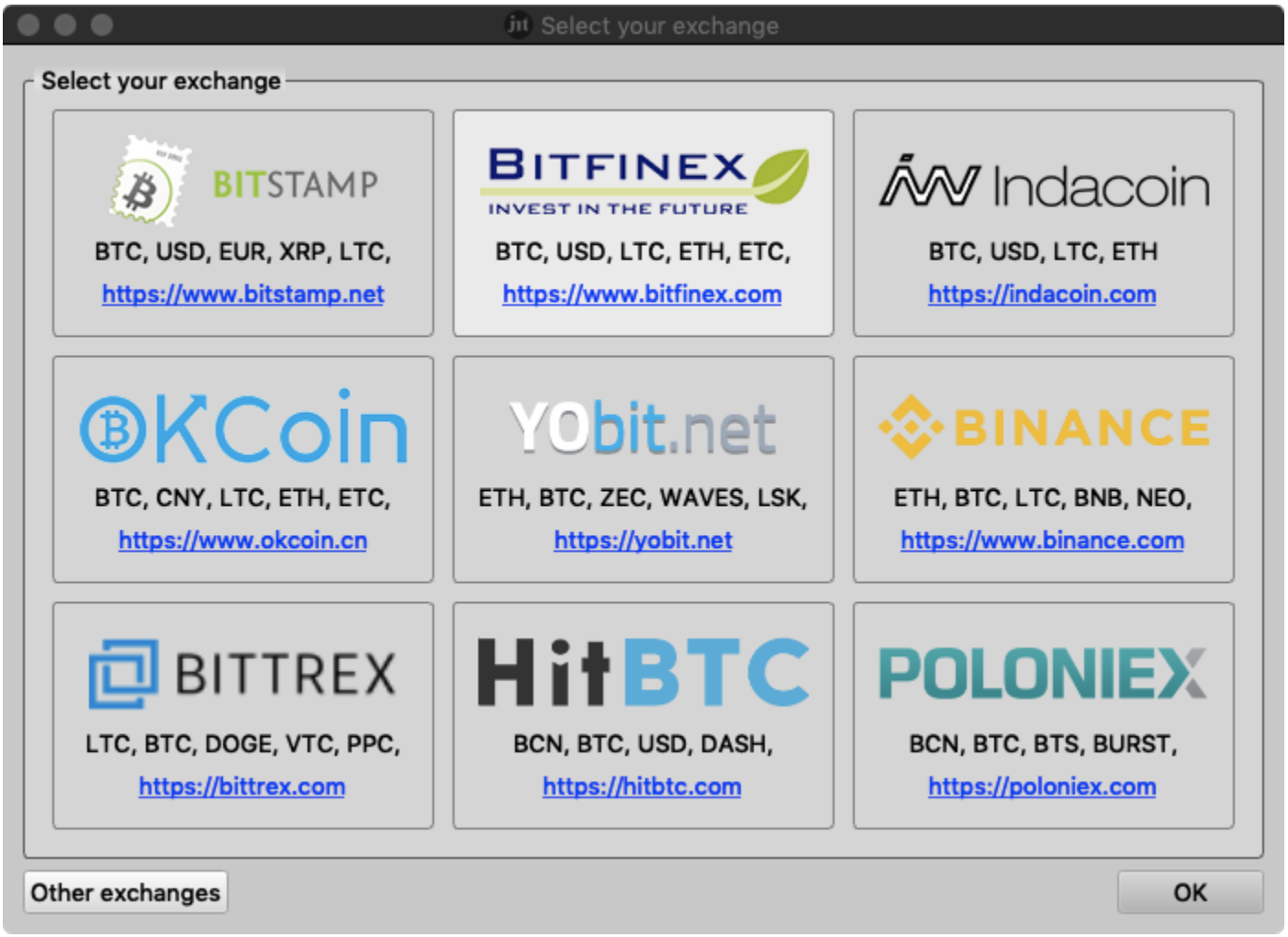
2. 此外，由于恶意应用程序没有签名，macOS（特别是Gatekeeper）会阻止它。（有关Gatekeeper及其在帮助阻止恶意软件和保护macOS用户方面的基础作用的更多信息，请参阅：Gatekeeper Exposed" [7]).

特洛伊木马程序

假设你是一家流行的加密货币交易所的员工，刚刚收到一封电子邮件，要求查看一个新的加密货币交易应用程序："JMTTrader"。电子邮件中的链接会将你带到一个外观合法的公司网站，并链接到（声称是）新应用程序的源代码和预构建的二进制文件：



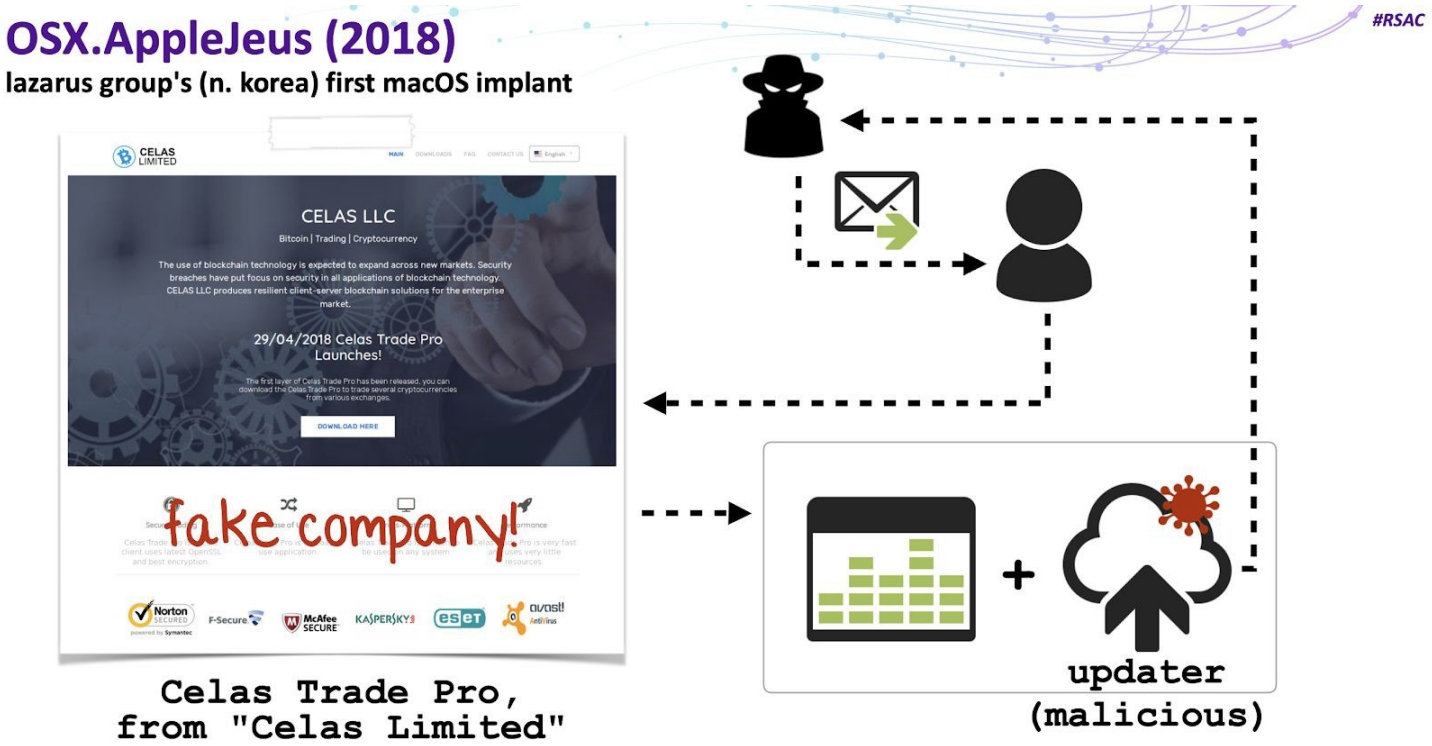
下载、安装并运行应用程序后，`JMTTrader`。应用程序（仍然）没有出现任何问题：



特洛伊加密货币交易应用程序（感染Lazarus Group backdoor）

不幸的是，虽然应用程序的源代码很原始，但JMTTrader的预构建安装程序。该应用程序被一个恶意后门偷偷地安装了特洛伊木马。在安装过程中，持续安装后门[8]。

这种特定的攻击归因于臭名昭著的Lazarus APT组织，该组织利用这种相当复杂（多方面）的社会工程方法感染Mac用户（大约从2018年开始）：



另一个特洛伊木马程序（感染Lazarus Group backdoor）

笔记:

有关Lazarus集团攻击的更多详细信息，以及他们对这种感染媒介的总体倾向，请参阅：

“传递AppleJeus”[8]

盗版（破解）应用程序

更复杂的攻击（仍然需要高度的用户交互）涉及将恶意软件打包到破解或盗版应用程序中。在这种攻击场景中，恶意软件作者将首先破解流行的商业软件（比如Photoshop等），取消版权或许可限制。然后，他们会将恶意软件注入（现已破解）软件包，然后再将其分发给毫无戒备的公众。下载并运行此类破解应用程序的用户将被感染。

利用这种感染媒介的Mac恶意软件包括OSX。通过“理想OS X应用程序的盗版版本（如Adobe Photoshop和Microsoft Office）” [8]传播的iForm，这些应用程序已上传到流行的torrent网站“海盗湾”:

Type	Name (Order by: Uploaded, Size, ULed by, SE, LE)
Applications (Mac)	Adobe Photoshop CS6 for Mac OSX Uploaded 07-26 23:11, Size 988.02 MiB, ULed by aceprog
Applications (Mac)	Parallels Desktop 9 Mac OSX Uploaded 07-31 00:19, Size 418.43 MiB, ULed by aceprog
Applications (Mac)	Microsoft Office 2011 Mac OSX Uploaded 07-20 19:04, Size 910.84 MiB, ULed by aceprog
Applications (Mac)	Adobe Photoshop CS6 Mac OSX Uploaded 07-26 23:18, Size 988.02 MiB, ULed by aceprog

包含OSX的盗版应用程序。我形成

> 笔记:
>
> 有关OSX如何运行的技术细节。下载并运行盗版应用程序后，iForm会持续感染Mac用户，请参阅:
>
> “入侵核心：iWorm的感染载体和持久性机制” [9]

最近，OSX。BirdMiner（也称为OSX.LoudMiner）也通过“VST Crack”网站上的盗版（破解）应用程序进行分发。著名Mac恶意软件分析师托马斯·里德（Thomas Reed）表示:

> “在高端音乐制作软件Ableton Live的破解安装程序中发现了Bird Miner”[10]

ESET还分析了该恶意软件[11],并讨论了其感染机制。 具体而言，他们的研究发现了近100个盗版应用程序，所有这些应用程序都与数字音频/虚拟演播室技术（VST）有关，（比如破解的Ableton Live软件包）包含BirdMiner恶意软件。

当然，下载并安装这些盗版应用程序的用户会感染恶意软件。

自定义URL方案