

第0x0C章：案例研究（OSX.EvilQuest）

📝 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

欢迎来到最后一章！现在是时候应用我们学到的所有知识，全面分析一个有趣的macOS恶意软件样本：OSX。邪恶探索。

📝 笔记:

你将通过配合这一章获得最大的收获！
要加入，请下载OSX。Objective See Mac恶意软件系列的EvilQuest:

<https://objective>

背景

奥斯。DevilQuest于2020. 夏天被Dinesh Devadoss (@dineshdina04. 发现。在一条推文中，他分享了各种散列信息，并指出它被冒充为“谷歌软件更新程序” [1. ,它的勒索软件功能，以及（不幸的）防病毒引擎没有检测到:



Dinesh_Devadoss
@dineshdina04

...

#macOS #ransomware impersonating as Google
Software Update program with zero detection.

MD5:

522962021E383C44AFBD0BC788CF6DA3
6D1A07F57DA74F474B050228C6422790
98638D7CD7FE750B6EAB5B46FF102ABD

并不是每天都会发现一个新的Mac恶意软件，尤其是一个（最初）未被发现，但却有盗窃用户文件的倾向的恶意软件。

...而且，正如我们将看到的，我们的分析将揭示更多的潜在能力！

感染载体

在分析（新的）恶意软件样本时，分析的首要目标之一通常是回答以下问题：“恶意软件如何感染Mac系统？”就像生物病毒一样，识别样本的感染载体通常是了解其潜在影响以及阻止其持续传播的最佳方式。

正如我们在第0x1章“感染载体”中看到的，恶意软件作者采用了各种策略，从简单的社会工程攻击到强大的0天攻击。

Dinesh的推文[1]没有具体说明OSX是如何工作的。EvilQuest能够感染macOS用户。然而，Malwarebytes的托马斯·里德指出，这些恶意软件是在流行的torrent网站上共享的流行macOS软件的盗版版本中发现的。

他特别指出：

“Twitter用户 ...昨天，在得知俄罗斯一个专门分享torrent链接的论坛上有一个明显恶意的小飞贼安装程序可供下载后，我发了这条消息。一篇帖子为Little Snitch提供了一个torrent下载，很快就有很多评论说下载的内容包含恶意软件。事实上，我们发现它不仅是恶意软件，而且是一种通过盗版传播的新Mac勒索软件。” [2]

andrejka29
Experience: 26 days
4 posts


09-Jun-20 14:24 (21 days ago, rev. 27-Jun-20 00:55)

Little Snitch 4.5.2 [Intel]

Year : 2020
Version : 4.5.2
Developer : Objective Development
Developer site : <http://obdev.at>
Platform : Intel only
Interface language : English
Tablet : The program has been treated (does not require data entry / enter any data)
System requirements : Mac OS X 10.11+, compatible with Mac OS X 10.15

Updated!
Description : Little Snitch is one of the most popular programs for monitoring and blocking the traffic of various applications and services.

The application warns you when the program tries to establish an outgoing connection. You can allow or deny the connection by setting access rules for future connections. These rules reliably prevents the sending of sensitive data without your knowledge. Little Snitch runs in the background and can detect network activity of viruses, malware and other malicious programs.



Screenshots

Screenshots of the About window

Download

Download the distribution by magnet link • 59.3 MB

Your Internet Provider and Government can see what you are downloading.
Don't forget to hide your IP with VPN to avoid fines and lawsuits!

[NordVPN](#) • [ExpressVPN](#) • [Private internet access](#) • [Airvpn](#) • [IPVanish](#)

The site does not distribute or store electronic versions of works, but merely provides access to a user-created directory of links to torrent files that contain only hash lists

[How to download?](#) (registration is required to download .torrent files)

[Profile] [PM]

盗版版的小飞贼感染了OSX。邪恶探索[2]

分发被恶意木马攻击的盗版（或破解）应用程序是针对macOS用户进行感染的一种相当常见的方法。虽然不是最复杂的方法，但它相当有效，因为一部分用户不喜欢付费软件，而是寻找盗版替代品 ... 可能会被感染。其他成功（ab）使用同一感染载体的Mac恶意软件包括OSX。iWorm [3]，OSX。Shlayer [4]和OSX。BirdMiner [5]。

当然，这种感染媒介需要用户交互。因此，为了感染OSX。用户必须从其中一个torrent网站下载并运行（受感染的）应用程序。

📝 笔记:

为了阻止（或至少反击）这种病毒以及其他“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。

distribute已被苹果检查是否存在恶意组件。” [6]

... 尽管这已经被多次检讨[7]。

分析（分类）

如前所述，OSX。EvilQuest被分发到各种盗版应用程序中。在本章中，我们将重点介绍一个与流行的DJ应用程序“Mixed In Key”恶意打包并通过各种torrent站点分发的示例。

📝 笔记:

该应用程序的创建者谈到了该应用程序的受欢迎程度，并指出，“世界顶级DJ和制作人使用混音键来帮助他们的混音听起来完美。” [7]

该应用程序的合法副本价格为58美元，并通过其创建者的网站（mixedinkey.com）直接分发。

回想一下，应用程序实际上是捆绑包（一种特殊的目录结构），在分发之前必须打包。OSX的样本。我们在这里分析的EvilQuest是作为一个磁盘映像分发的（看起来是这样的），混合在键8中。dmg。该文件的SHA-256哈希为：B34738E181A6119F23E930476AE949FC0C7C4DED6EFA003019FA946C4E5B287A。

当第一次被发现时，这个OSX。VirusTotal上的任何反病毒引擎都没有将EvilyQuest样本标记为恶意[9]

b34738e181a6119f23e930476ae949fc0c7c4ded6efa003019fa946c4e5b287a

Help 🔍 ⬆️ 📁 🗨️ Patrick War...

0
/ 58

Community Score

✓ No engines detected this file

b34738e181a6119f23e930476ae949fc0c7c4ded6efa003019fa946c4e5b287a

Mixed In Key 8.dmg

dmg

10.38 MB

Size

2020-06-26 22:13:59 UTC

3 days ago

DMG

... 尽管现在，它被广泛检测为包含恶意软件。

5

给定一个潜在的恶意文件，我们讨论了使用file实用程序来识别文件类型 ...许多分析工具都是特定于文件类型的。

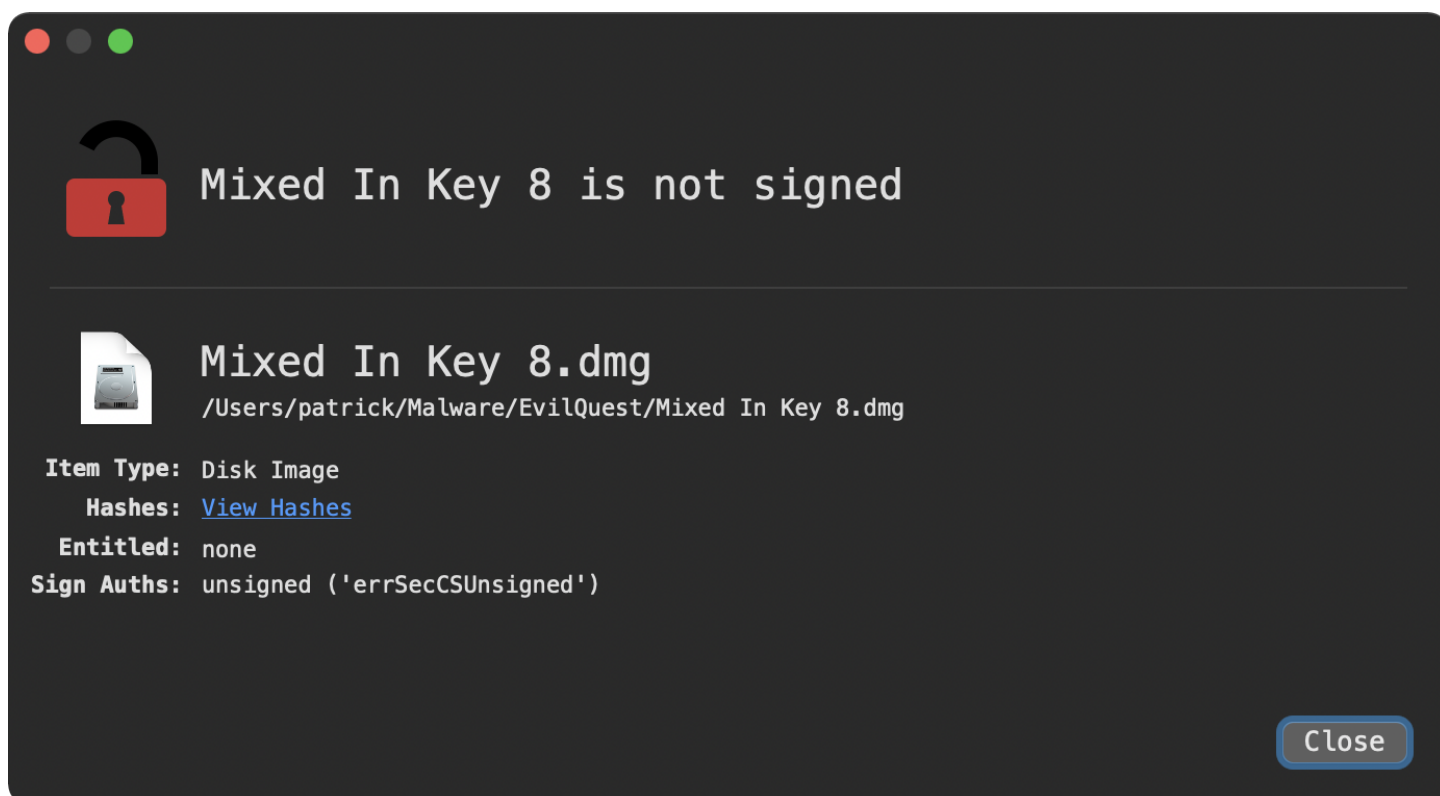
因此，在分析键8中的混合。dmg文件进一步，让我们运行文件实用程序：

```
$ file "EvilQuest/Mixed In Key 8.dmg"
```

Oops,看起来文件实用程序“错误识别”了文件 ...正如著名的macOS研究人员乔纳森·莱文所解释的那样，这其实并不令人惊讶：“由于zlib头，用zlib压缩的[磁盘图像]经常错误地显示为“VAX COFF”[10]

然而，Objective See的“WhatsYourSign” [11]实用程序显示项目的代码签名信息，也可用于识别文件的类型。

请注意，在下面的WhatsYourSign窗口中，键8中的“项目类型”字段确认为Mixed。dmg确实是一个磁盘映像，正如预期的那样：



(你的标志是什么)

您可以通过macOS的hdiutil实用程序手动装载磁盘映像（以便提取其内容）：

```
$ hdiutil附加“OSX.EvilQuest/Mixed In Key  
8.dmg”  
/dev/disk2 GUID partition scheme
```

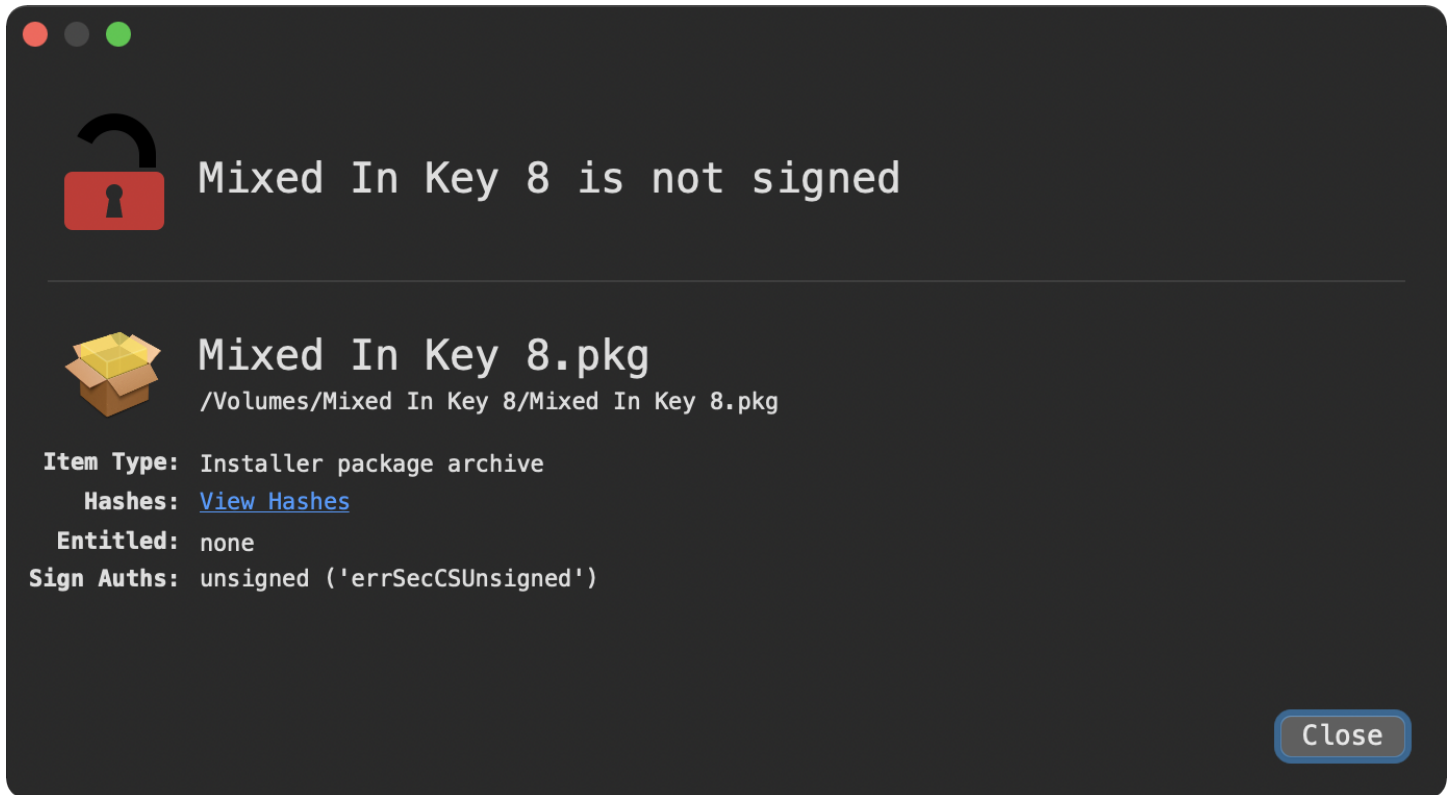
📝 笔记:

您也可以尝试挂载可疑的磁盘映像，因为hdiutil实用程序将无法挂载无效的文件（即不是磁盘映像），并显示以下错误消息：

一旦装入（到/Volumes/Mixed In Key 8/），列出磁盘映像的内容就会显示一个文件 ...一个名为Mixed的安装程序包，包含在密钥8中。背包：

```
$ ls “/数量/混合在
```

我们再次使用WhatsYourSign来确认文件的类型（“项目类型：安装程序包存档” ... 又称作pkg），并检查包的签名状态。没有签名：



未签名
(通过WhatsYourSign)

也可以通过pkgutil实用程序从终端检查包裹签名（或缺少签名）。请把车开过去 --检查签名和包裹路径：

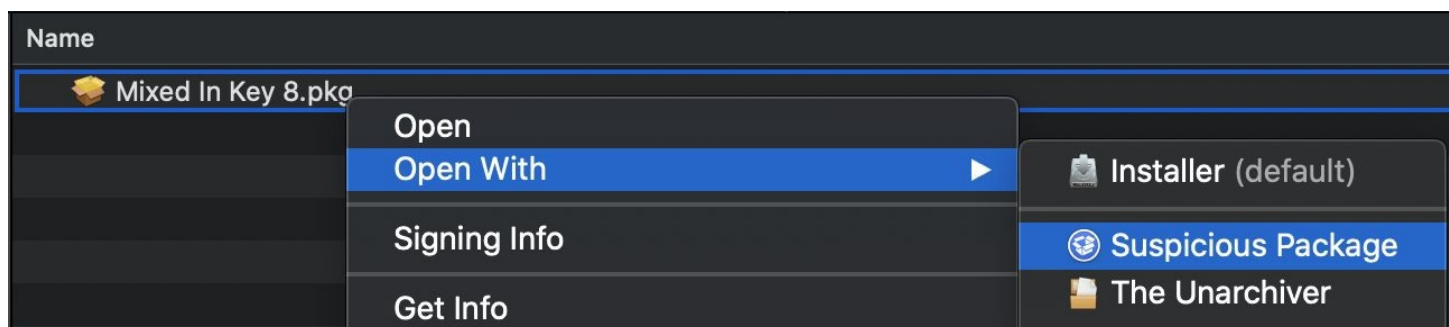
```
$ pkgutil --检查签名"/Volumes/Mixed In  
Key 8/Mixed In Key 8.pkg"包"Mixed In
```

由于软件包未签名，macOS将在允许打开之前提示用户：

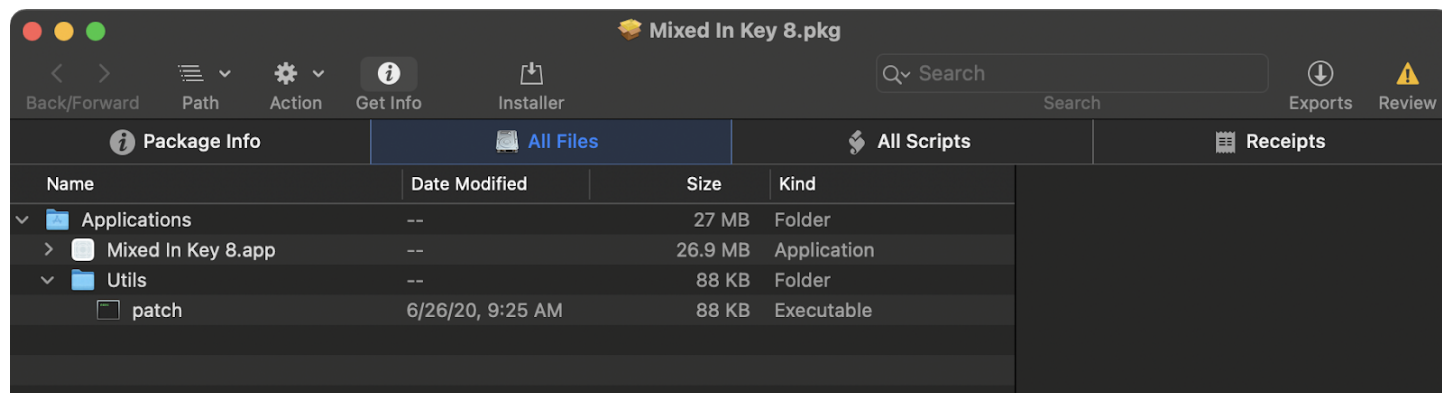


然而，试图盗版软件的用户很可能会忽略这一警告，继续前进 ...无意中确保感染开始！

在第0x5章“非二进制分析”中，我们讨论了使用可疑包[11]实用程序来探索包（.pkgs）的内容。在这里，我们用它来打开混合键8。背包：



在“所有文件”选项卡中，我们将在键8中找到一个名为Mixed的应用程序。应用程序和一个名为patch的可执行文件：



我们将简短地对这些文件进行分类，但首先我们单击可疑软件包中的“所有脚本”选项卡，其中显示了一个简单的安装后脚本：

```
01 #!/bin/sh
02 mkdir /Library/mixednkey
03
04 mv /Applications/Utils/patch /Library/mixednkey/toolroomd
05 rmdir /Application/Utils
06
07 chmod +x /图书馆/混搭店/工具房
08
09 /Library/mixednkey/toolroomd &
```

混合在8号键中。pkg的安装后脚本

请记住，安装软件包时，也会（自动）执行任何安装后脚本。因此，当特洛伊木马混合在密钥8中时。如果安装了pkg，也将执行其安装后脚本中的以下命令：

1. `mkdir /Library/mixednkey`
创建一个名为/Library/mixednkey的目录。
2. `mv /Applications/Utils/patch /Library/mixednkey/toolroomd`
将补丁二进制文件（已“安装”到/Applications/Utils/patch）移动到新创建的/Library/mixednkey目录中 ...作为名为toolroom的二进制文件。
3. `rmdir /Application/Utils`
删除/Applications/Utils/目录（在安装过程之前创建）。