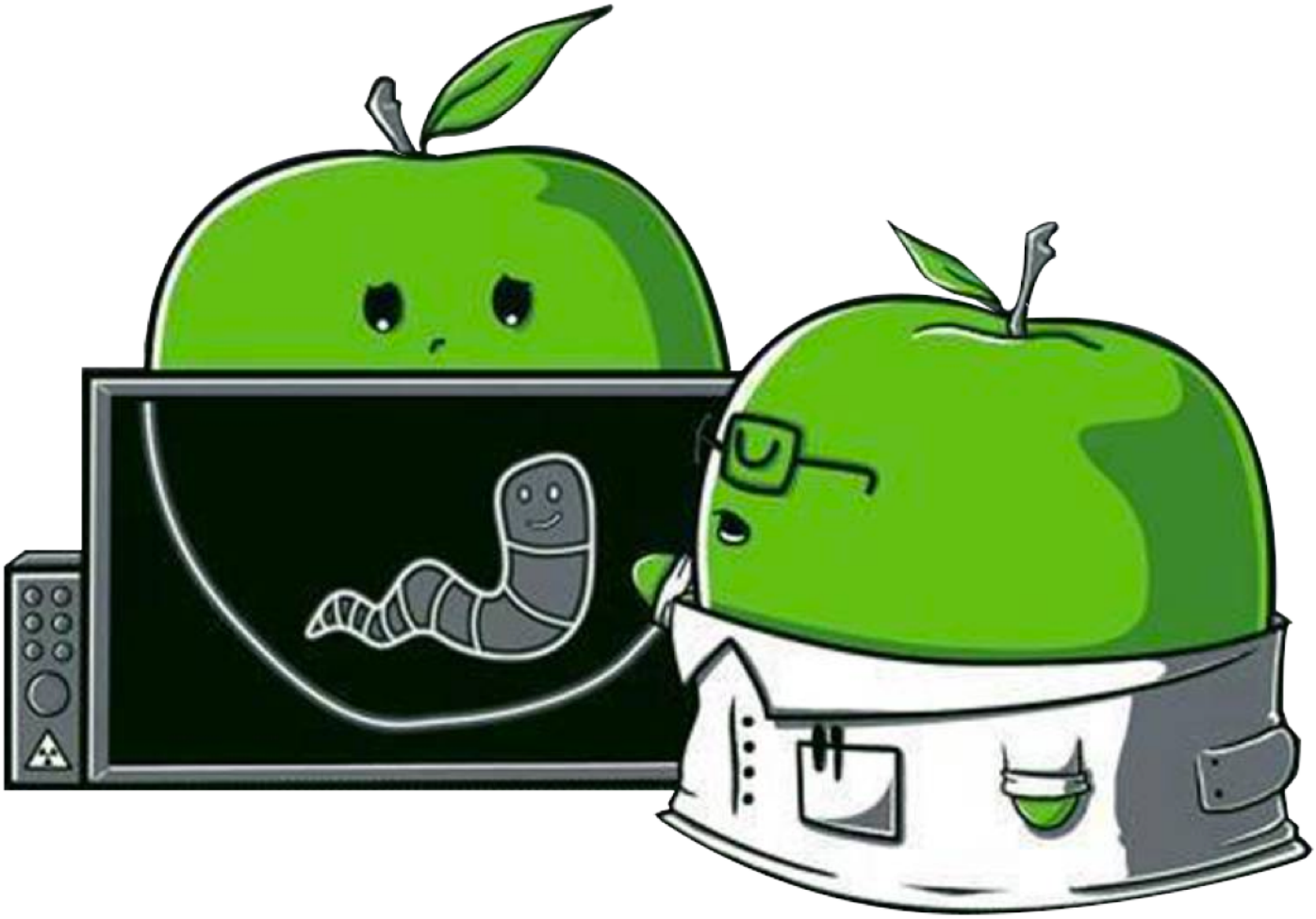


（Mac恶意软件的艺术）第一卷：分析

第0x3章：能力

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

那么，一旦一个恶意软件感染了一个系统，并且（可选地）持续存在，它会做什么呢？当然，这取决于恶意软件的目标！

在本章中，我们将介绍Mac恶意软件的常见功能，包括:

- Surveying/reconnaissance
- 与广告软件相关的劫持和注射
- 加密货币挖掘
- 远程炮弹
- 远程执行
- 远程下载/上传
- 文件加密
- ...还有更多！

在深入讨论Mac恶意软件的有效载荷之前，需要注意的是，恶意软件的有效载荷在很大程度上取决于其类型。一般来说，Mac恶意软件可以分为两大类：（网络）犯罪和（网络）间谍活动。网络犯罪分子设计的恶意软件主要由一个因素驱动：金钱！因此，属于这一类别的恶意软件试图通过显示广告、劫持搜索结果、挖掘加密货币或加密用户文件以获取赎金来为恶意软件作者赚钱。另一方面，为监视受害者而设计的恶意软件（例如，由三个字母的间谍机构设计的）更有可能包含（更隐蔽的）有效载荷，其特点是能够从系统麦克风上录制音频，或者暴露一个交互式外壳，允许远程攻击者执行任意命令。

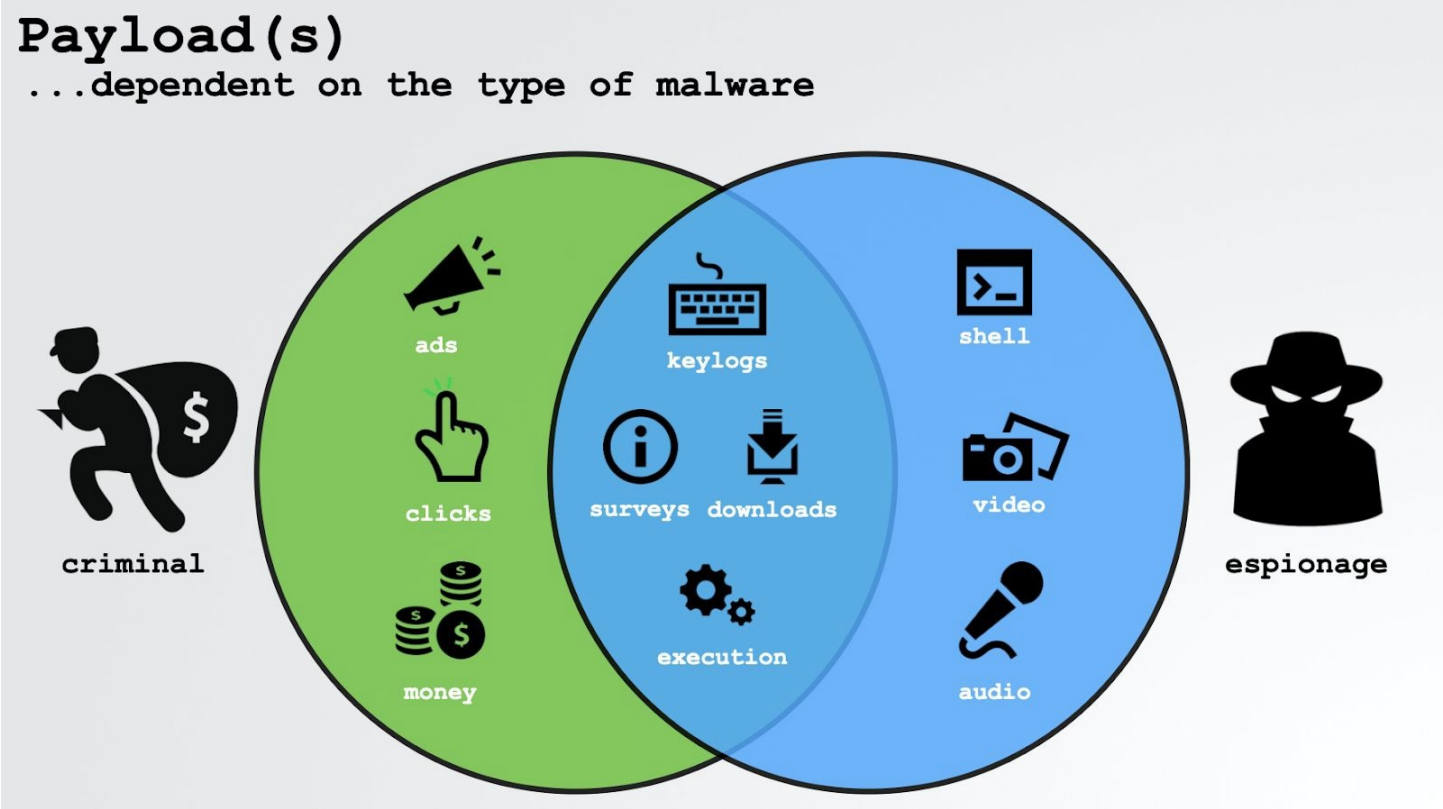
 笔记:

还有其他（较小）种类的macOS恶意软件，例如专为:

- “黑客行动主义”

- 破坏（即刮水器）
- 变态行为（即网络摄像头捕捉）

当然，这两大类别之间的有效载荷和能力存在重叠。例如，下载和执行任意二进制文件的能力对所有恶意软件作者来说都是一种吸引人的能力，因为它提供了更新或动态扩展其恶意创建的手段。



恶意软件分类

Survey/Reconnaissance

在以犯罪为导向和以间谍为导向的能力重叠中，我们发现（除其他外），**“调查”**通常，当恶意软件（和广告软件）感染系统时，它会首先检查并查询其环境。这通常有两个主要原因：

1. 这项调查让恶意软件深入了解其**“环境”**，这可能会推动后续决策。例如，如果检测到第三方安全工具，恶意软件可能会选择不持续感染系统。或者，如果它发现自己在运行

使用非root权限时，它可能会尝试升级其权限（或者干脆跳过需要此类权限的操作）。

2. 此调查可能会传回攻击者的命令和控制（C&C）服务器。在这里，调查中收集的信息可能会被攻击者用来唯一地识别受感染的系统（通常通过某些特定于系统的唯一标识符），和/或识别感兴趣的受感染目标（计算机）。在后一种情况下，最初看似不分青红皂白的攻击感染了数千个系统（或更多！），实际上可能是一场针对性很强的活动，根据调查信息，攻击者对大多数受感染的系统不感兴趣。

> 笔记:
>
> 一个（非Mac）广泛但目标明确的攻击例子涉及流行的Windows产品CCleaner:
>
> “数十万台计算机被一个极为常见的安全软件的损坏版本渗透，永远不会有好的结局。但现在越来越清楚的是，最近的CCleaner恶意软件爆发的结果到底有多糟糕。研究人员现在相信，背后的黑客不仅致力于大规模感染，但针对的是试图进入至少18家科技公司网络的有针对性的间谍活动。”
>
> “CCleaner恶意软件的惨败针对至少18家特定的科技公司”[1]

让我们简要介绍一下在实际macOS恶意软件样本中发现的一些特定调查功能。

首先是OSX。质子[2]。一次是OSX。Proton已经进入Mac系统，它首先调查该系统，以确定是否安装了任何第三方防火墙。如果发现一个，恶意软件将不会持续感染系统，而是简单地退出！

调查逻辑包括检查是否存在与（常见）macOS防火墙产品相关的文件，例如属于LittleSnitch防火墙的内核扩展:

```
01  //0x51: 'LittleSnitch.kext'
02  rax = [*0x10006c4a0 objectAtIndexedSubscript:0x51];
03
04  //检查文件是否存在
05  rdx = rax;
```

```
06  如果（[rbx fileExistsAtPath:rdx]！= 0x0）goto文件存在；
07
08  //exit!
09  fileExists:
10   rax = exit(0x0);
11   返回rax；
```

用于检测LittleSnitch OSX的调查

。质子

这样的防火墙产品会提醒用户OSX的存在。当它试图连接到其命令和控制服务器时。因此，恶意软件的作者们决定，与其进行风险检测，不如干脆退出（并跳过持续感染系统）更明智！

OSX.MacDownloader [3] 是另一个包含调查功能的Mac恶意软件样本。然而，与OSX不同。Proton的目标是向（远程）攻击者提供有关受感染系统的详细信息：

> “MacDownloader收集有关受感染系统的信息，包括用户的活动钥匙链，然后将其上载到C2. 滴管还记录正在运行的进程、已安装的应用程序以及通过假系统首选项对话框获取的用户名和密码。”[4]

转储Objective-C类信息（我们将在第0x6章[TODO]中介绍）揭示负责执行和过滤调查的各种方法：

```
$ class dump“addone flashplayer.app/Contents/MacOS/Bitdefender广告软件删除工具”

...
- (id)getKeychainsFilePath;
- (id)getInstalledApplicationsList;
- (id)getRunningProcessList;
- (id)getLocalIPAddress;
- (void)saveSystemInfoTo:(id)arg1 withRootUserName:(id)arg2 andRootPassword:(id)arg3;
- (BOOL)SendCollectedDataTo:(id)arg1 withThisTargetId:(id)arg2;
```

在OSX之前。MacDownloader将调查发送给攻击者，并将其保存到名为applist的文件中。txt（in /tmp）。在虚拟机中运行恶意软件可以让我们“捕获”调查结果：

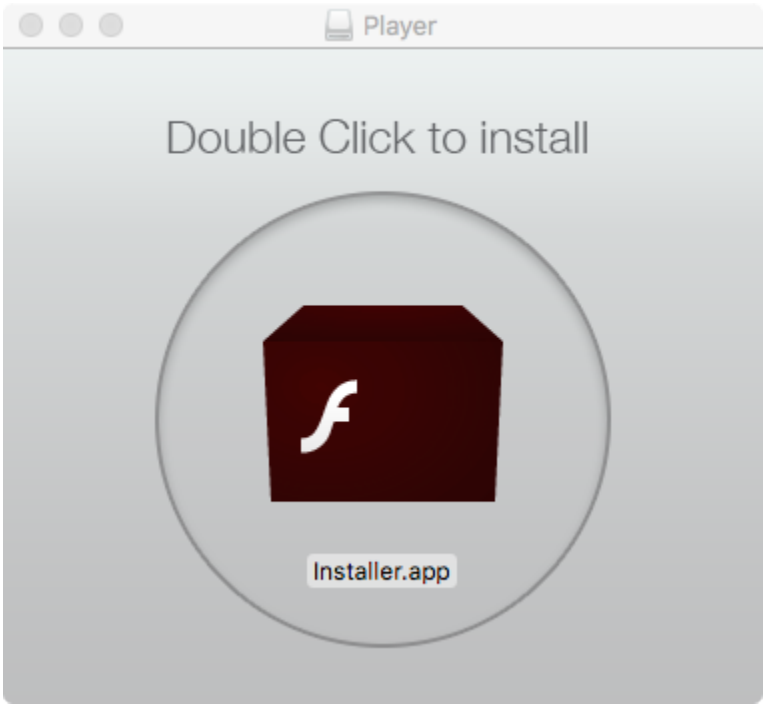
```
$ cat /tmp/applist.txt
“操作系统版本：Darwin users-Mac.local 16.7.0 Darwin内核版本16.7.0: Thu Jun 15 17:36:27 PDT
2017；根目录：xnu-3789.70.16~2\/RELEASE_X86_64 X86_64”，

“Root用户名：\“user\”，“Root密码
：\“hunter2\”，
...

[
"Applications\/App%20Store.app\/",
"Applications\/Automator.app\/",
"Applications\/Calculator.app\/",
"Applications\/Calendar.app\/",
"Applications\/Chess.app\/",
...
]

“进程名称为：Dock\t PID: 254从运行: 文件：\/\/\/System\/Library\/CoreServices\/Dock
。app\/Contents\/MacOS\/Dock”，“进程名为：Spotlight\t PID: 300从:
文件：\/\/\/System\/Library\/CoreServices\/Spotlight。app\/Contents\/MacOS\/Spotlight”，“
进程名称为：Safari\t PID: 972从运行:
file:\/\/\/Applications\/Safari.app\/Contents\/MacOS\/Safari",

...
```

与广告软件相关的劫持和注射

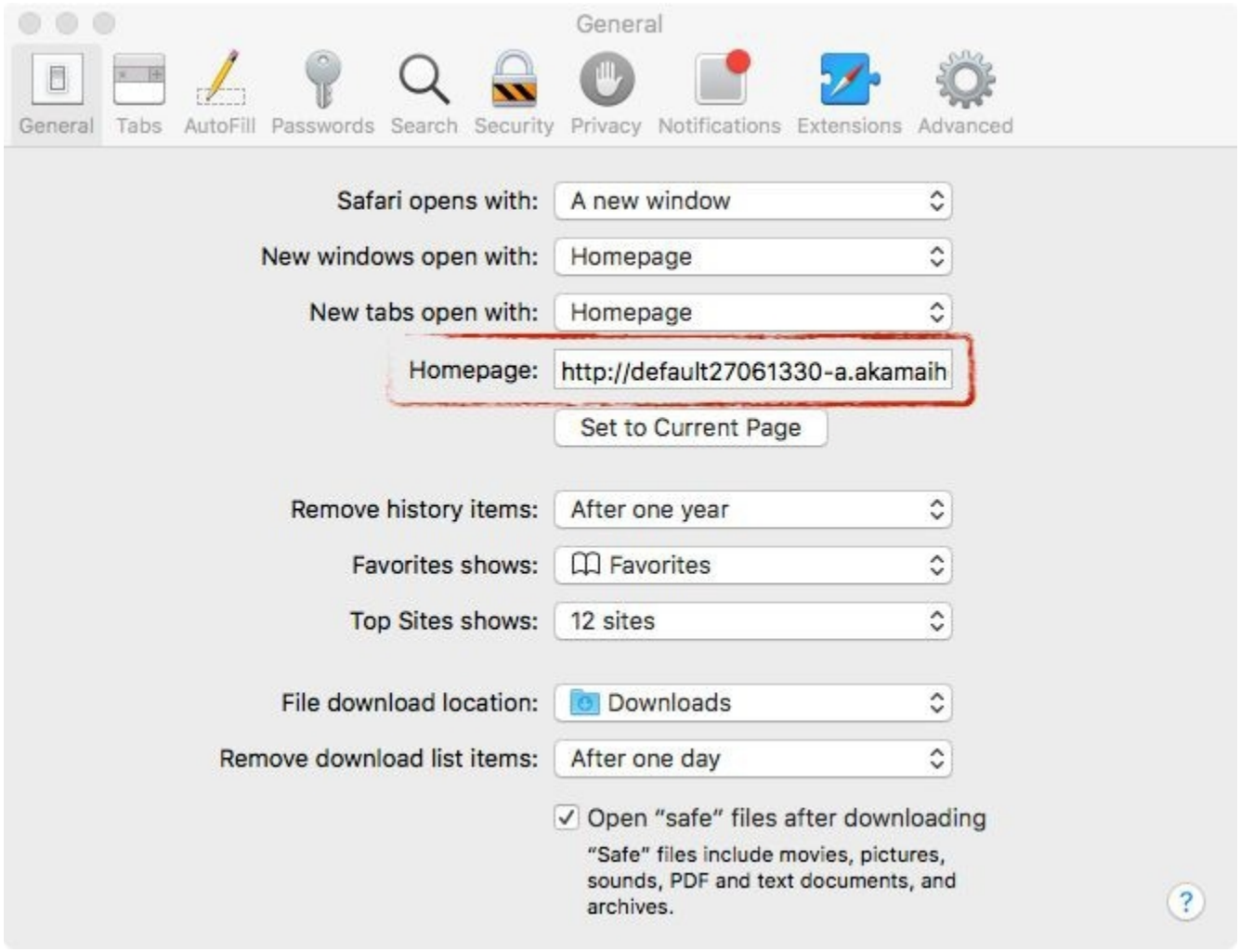
如前所述，普通Mac用户不太可能成为熟练的网络间谍攻击者攻击的目标，他们的攻击时间为0天。相反，它们更有可能成为更简单的广告软件相关攻击的牺牲品。

与其他类型的Mac恶意软件相比，广告软件的数量相当多。广告软件的目标通常是通过广告为其创作者赚钱（因此得名！）或者通过被劫持的搜索结果（由附属链接支持）。

例如，在一篇题为“WTF是Mughthesec！？”的文章中[5] ，我分析了一个这样的广告软件（伪装成Flash安装程序）：



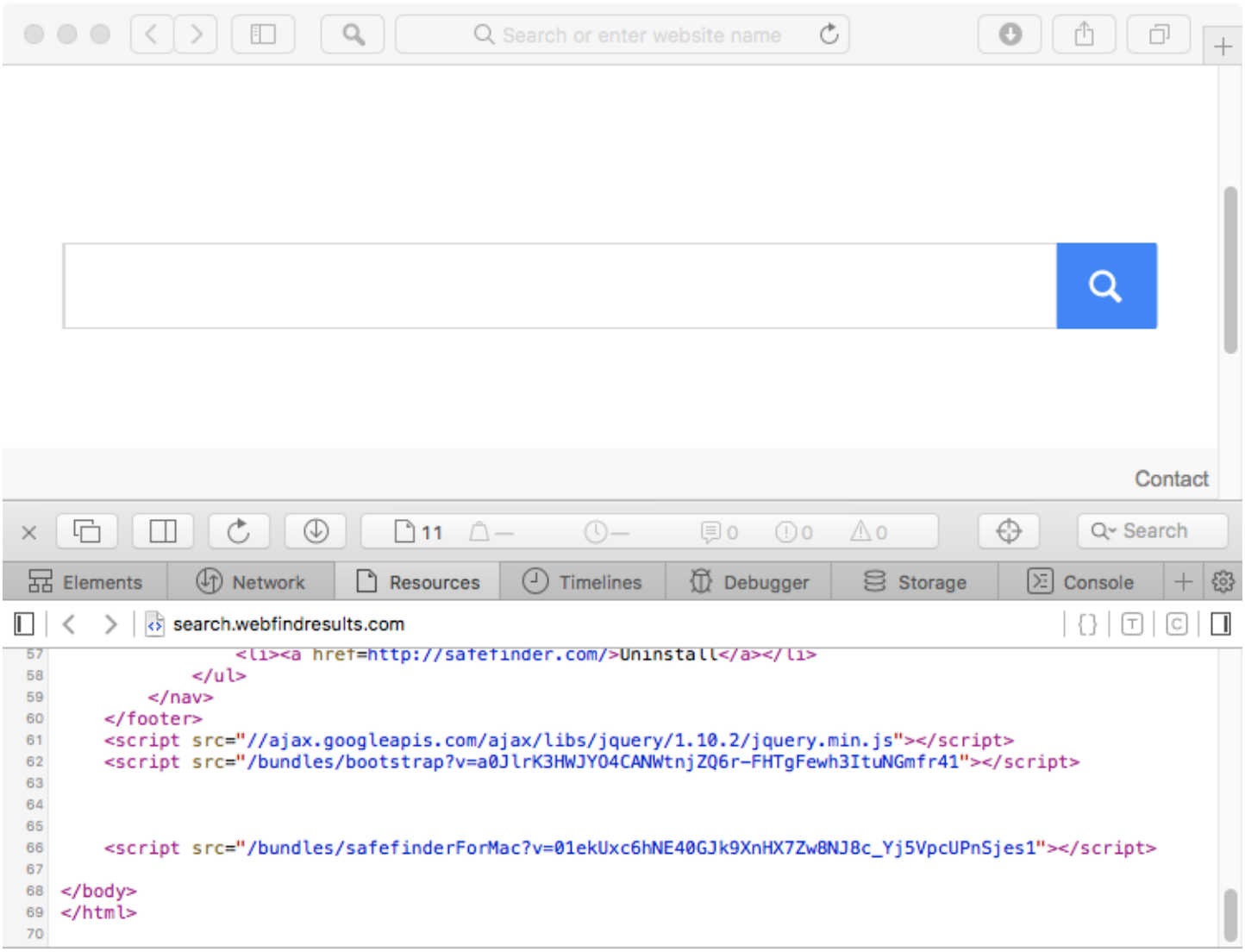
该应用程序将安装各种广告软件，包括名为“Safe Finder”的软件。“Safe Finder”会劫持Safari的主页，将其设置为指向由分支机构驱动的搜索页面。



Safari的主页被劫持

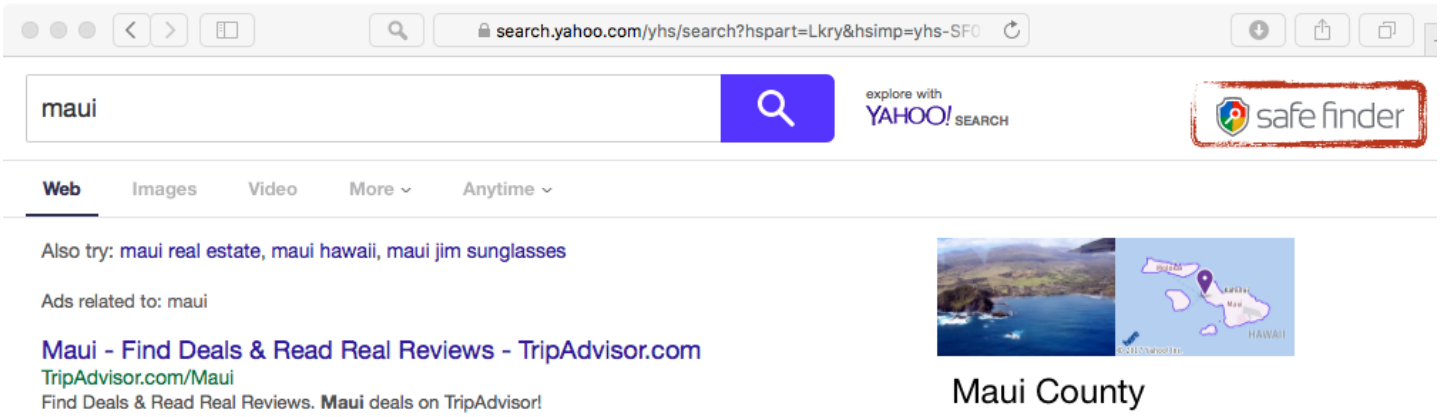
在受感染的系统上，打开Safari确认主页已被劫持
...虽然看起来是无害的：它只是显示了一个相当“干净”的搜索页面。

然而，查看页面源代码可以发现包含了几个“安全查找器”脚本：



用户的“新”主页

通过这个被劫持的主页，用户搜索通过各个分支机构进行，最后由雅虎搜索提供服务。然而，“安全查找器”逻辑（如图标，以及可能的其他脚本）被注入到所有搜索结果中：



劫持（？）搜索结果

操纵搜索结果的能力可能会通过广告视图和附属链接为广告软件作者带来收入。

> 笔记:
>
> 要深入了解该广告软件及其与附属项目的关系，请参阅“How Affiliate Programs Fund Spyware” [6]

加密货币矿工

如前所述，大多数感染Mac电脑的用户都是被出于经济利益动机的恶意软件感染的。20世纪末，试图感染macOS系统并秘密安装加密货币挖掘软件的Mac恶意软件大幅上升。

大多数实现加密货币有效载荷的Mac恶意软件都是以一种相当懒惰（尽管效率很高）的方式实现的。怎样通过打包合法矿工的命令行版本。

例如，OSX。CreativeUpdate [7]（通过流行的Mac应用程序网站MacUpdate[.]秘密发布）com），这是MinerGate合法的加密货币矿商[8]。

具体来说，该恶意软件作为启动代理（MacOS.plist）持久存在，以指示系统持久执行名为mdworker的二进制文件: