AhnLab

安全月刊

Vol. 28

2014 年 Mac OS X 安全威胁分析

2014年 Mac OS X 安全威胁分析

Mac OS X 系统是否依然安全？

iPhone 的普及程度，相信比 Mac 计算机为高。iPhone 用户未必会用 MacBook。不过，随着全新 Mac OS 版本发布，iPhone 与 Mac 计算机之间的关系，越来越紧密。你用 iPhone，更加要用 Mac 计算机。这就是苹果计算机在 WWDC 2014 开发者大会带给大家的信息。另外，去年苹果公司发布了新一代 Mac OS X 操作系统 Yosemite。新的 OS 进一步强化了与 iOS 设备的互动。[1]

另外，iPhone 6 和 iPhone 6 Plus 上市后人气剖高，再加上 Macbook 用户层的扩大，针对 OS X 系统的恶意软件也呈现增加趋势。苹果 OS X 去年面临的恶意软件攻击数量增加，杀毒软件公司卡巴斯基在2014年度安全报告中提到自己的软件拦截了370万次恶意软件攻击 。[2]

但是，目前 Mac 相关的防病毒软件使用率很低，且普及速度也很慢。这就很容易受到外部的针对性攻击。如果一旦发生攻击事件，其危险性和损害比预想的还要严重。即使现在看起来威胁还不严重，但是为了防止大型事故的发生，有必要预先了解一下有关 Mac 恶意软件，然后采取预防措施。本刊将着重介绍2014年主要出现的 Mac 恶意软件。

2014年 Mac 安全威胁

2014年主要的安全主题是：▲智能手机面临的安全威胁；▲威胁网上银行的域欺骗(pharming)恶意代码；▲攻击路径的多样化；▲黑客攻击POS(Point-Of-Sales)系统；▲开放源码出现严重漏洞。可以看出，去年网络安全威胁已扩大到多样的平台，如“智能手机”、“POS机”和“Mac”等。而且威胁网上银行的攻击手法越来越高级和多样，如利用域欺骗和攻击内存窃取金融交易信息。另外，开放源码软件中也发现了严重的漏洞(HeartBleed 和 ShellShock 等)，震惊了全世界。

2014年发现的 Mac 恶意软件与 Windows 恶意软件相比，尽管在技术上存在差异，但是其形式没有很大差异。对于 Mac 平台上的防病毒措施，苹果公司已经在 Mac 系统中引入了安全功能 GateKeeper，同微软公司一样加强了安全。目前已发现的 Mac 恶意软件主要是通过“未知下载”、“程序漏洞”、“网络钓鱼”和“苹果商店”等感染。这也跟 Windows 系统发生的安全事件很相似。

跨平台恶意软件-Flashback、Icefog

2012年发现的 Flashback 恶意软件是一种专门感染 Mac OS X 的后门程序，感染数量超过60万，甚至打入苹果的总部。此程序用 java 编写，伪装成 flash 播放器更新程序，从主控机下载恶意代码并且传播，据称不需要密码即可感染。[3] 随后，苹果公司意识到问题的严重性，遂将 Java 移除了默认安装选项。根据 Intego 的统计，直到2014年初仍旧有很多 Mac 电脑被 flashback 病毒感染。

“Icefog”是一个专注APT的组织，2011年开始活跃起来，主要活跃在日本和韩国。已知的目标包括政府机构，军队，海上组织，电信部门，制造业和高科技公司和大众媒体。Icefog 的名字来源于恶意软件的C&C服务器中的字符。Icefog 组织常用的手段是利用社会工程学技巧来欺骗受害者，比如“网络钓鱼”，在攻击者使用特制的具有诱惑性的文件发给受害者。主要利用 Java 的漏洞，还有 HWP 和微软 office 等漏洞。

---

[1] http://www.cnbeta.com/articles/297871.htm

[2] http://www.199it.com/archives/313082.html

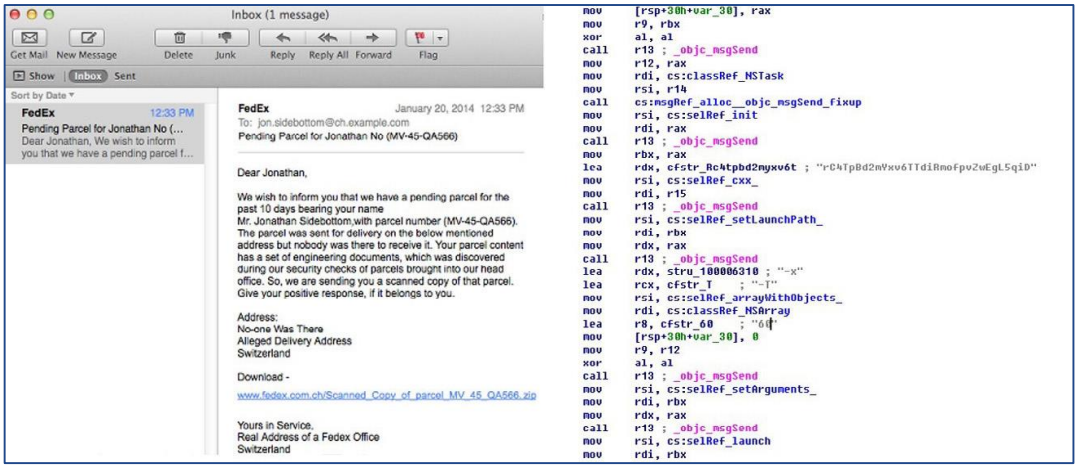
[3] 百度百科http://baike.baidu.com/link?url=LYzFtkOknucQrG7OgZf_9Sb7TZNPdap-Q80IGrcN1LNjQG6WVbUmqkS7o4MmfRE5-L1FZz5beKo4bDshDP4nG9LEJNAlWxek8WaNGjmXNbm

【图 1】Flashback 恶意软件

上述两种恶意软件都利用了 java 的漏洞。尤其，icefog 恶意软件不仅利用 java 漏洞，还有利用多样程序的漏洞来感染 Windows 和 OS X 平台。这就是所谓的跨平台(Cross Platform)攻击，通过一个漏洞来攻击多样的平台，不管用户使用何种平台，照样感染恶意软件的一种攻击形式。在2014年，这种跨平台攻击的恶意软件以多样的形式出现。

Laoshu 恶意软件

2014年发现的 Laoshu 恶意软件通过钓鱼邮件发布。邮件伪装成有名的货运公司并包含下载链接，诱使用户点击该链接下载文件。伪装成PDF图标的 Laoshu 恶意软件被分为 RAT(Remote Access Trojan)恶意软件。与其他 RAT 类恶意软件不同之处在于它集中于窃取用户电脑信息、互联网连接信息和数据。主要窃取扩展名为 DOC、DOCX、XLS、XLSX、PPT、PPTX 和 ZIP 等文件信息，并每一秒将屏幕截屏后将图片传送到外部。



【图 2】 发布的电子邮件全文(左侧)/传送截屏图片的代码(右侧)

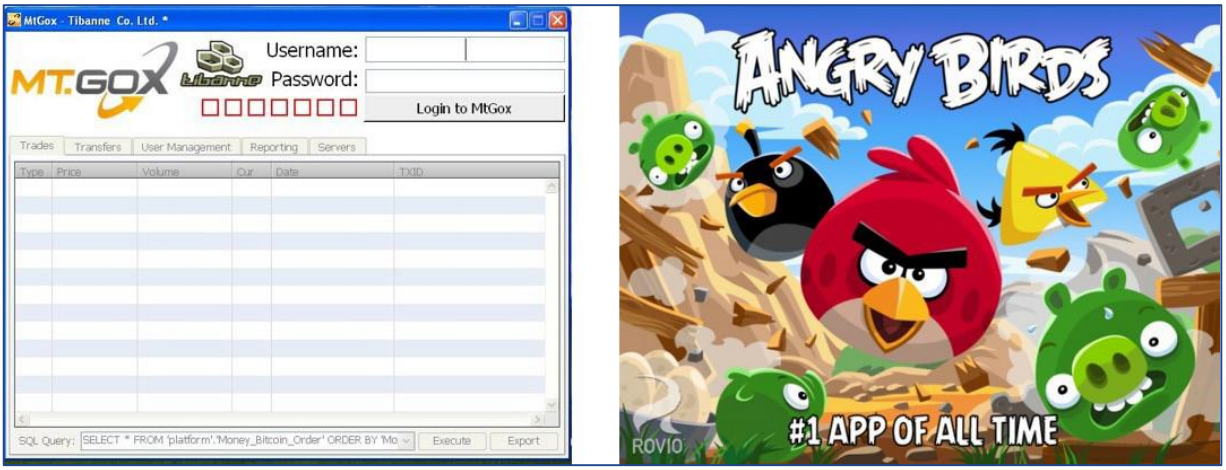
这些 RAT 类的恶意软件主要以APT形式针对特定企业和机关发布，但是从2014年开始攻击对象范围扩大到不特定的一般用户。2014年发现的威胁网上银行的恶意软件中包含 CyberGate RAT 和 Gh0st RAT，这就属于不特定对象攻击的例子。Laoshu 恶意软件是一种典型的针对一般用户的RAT类恶意软件。可以看出， Mac 感染恶意软件呈现出与 Windows 相同的趋势。

盗取比特币-CoinThief 木马

2014年2月，在 Mac OS X 平台上发现一种新型的木马程序，能够监视用户的网页浏览，并通过伪装成一款比特币交易程序，实现盗取用户的比特币。这种木马被称为 CoinThief 或者 CoinStealer。

比特币(Bitcoin)是基于P2P(peer-to-peer)网络发行和进行交易的“电子货币”，并非一种真实存在的货币，它其实是一种虚

拟货币。由于比特币的价值上升，为了盗取比特币攻击者将木马程序安装到用户 Mac 系统。2014年8月，在 Linux 也发现了相同形式的木马，其名称为 Ssabobot、Bossabot。2014年初，日本比特币交易平台 Mt.Gox（当时全球最大的比特币交易平台）遭受黑客攻击，损失额超过5亿美元，最终导致该公司破产。

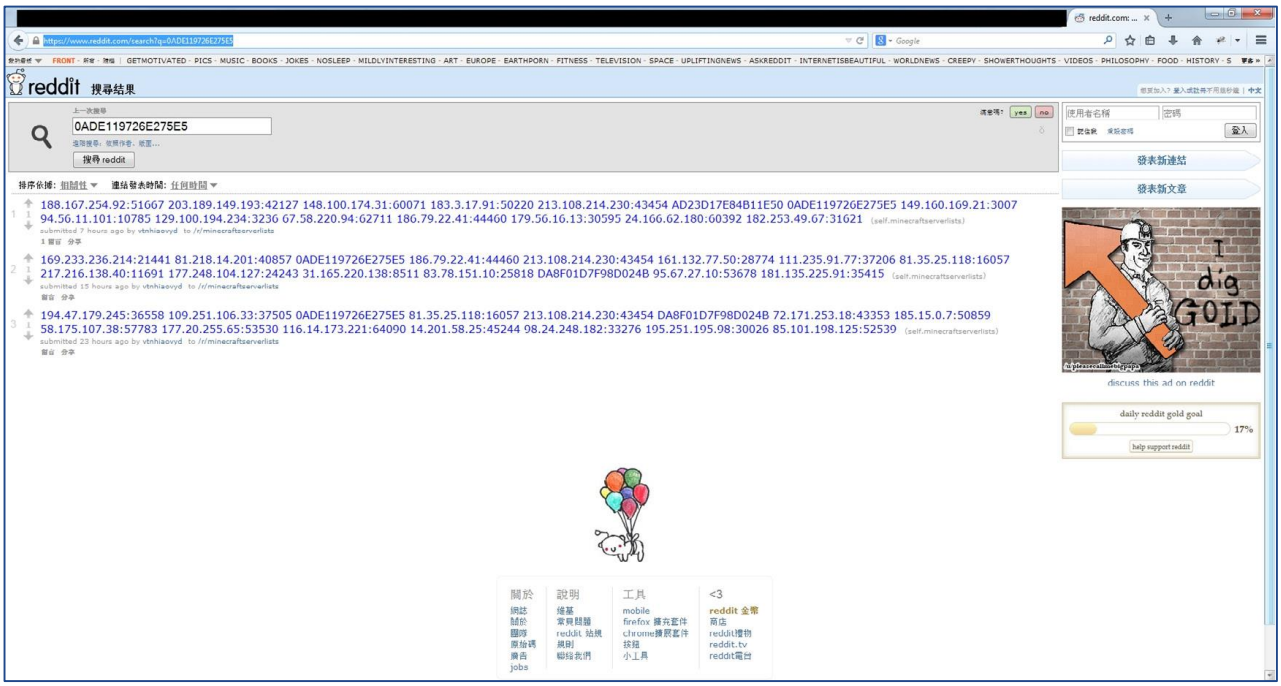


【图 3】 伪装成 Mt.Gox 的Windows 恶意软件(左侧)/Angry Birds(右侧)

2015年1月，全球最大和最可靠的比特币交易平台之一 Bitstamp 停止交易，原因是遭到黑客袭击，导致19000枚比特币被盗(价值约500万美元的虚拟货币)。这次攻击是继日本比特币交易平台 Mt.Gox 事件之后对比特币用户的另一次重大打击。即使比特币交易平台已成为黑客攻击的目标，在这种安全威胁中比特币的价值并没有降低，仍然有很多人在使用。因此，预计2015攻击比特币交易平台的恶意软件有增无减。

僵尸网络 – iWorm

iWorm，又被成为 Luaddit，是一种复制的后门软件，能在被感染的 Mac 电脑上执行多种命令，从而实现窃取用户数据、远程遥控系统等目的。2014年被俄罗斯信息安全研究公司 Dr. Web 发现，并在病毒库中将这一恶意软件标记为“Mac.BackDoor.iWorm”。



【图 4】 iWorm

iWorm 看起来与木马病毒很相似，但是它的特别之处在于能偶调用 Reddit 的搜索服务器获得僵尸网络的服务器列表。已确认的 IP 地址也奖金1万7千以上。这充分说明了不仅在 windows 系统，而且在 Mac 系统也可以大规模被僵尸软件感染。尽

管 Mac 系统已有被 Flashback 感染的大规模的事件，但是这各 iWorm 恶意软件再一次显示了 Mac 系统已不是躲避恶意软件的安全地带。该软件在苹果公司的 XProtect 以 iWorm 标记，AhnLab 则以 Luaddit 的名称诊断。

“模块化”及“开源代码” – Ventir

2014年10月发现的 Ventir 已被确认为加载多样功能的模块化的恶意软件。通常恶意软件针对一种功能和目的而制作，比如“盗取信息”和“远程控制”等。但是 Ventir 恶意软件，Dropper 文件中包含了键盘记录、后门程序和事件监控等功能。图 5 表示一个 Dropper 文件中执行各功能的文件的位置。

Name	Address
start	0000000100000770
_main	00000001000007B0
_updated	0000000100002100
_updated_len	000000010000A290
_update	000000010000A2A0
_update_len	0000000100019B44
_reweb	0000000100019B60
_reweb_len	000000010001E2D8
_keylog	000000010001E2E0
_keylog_len	0000000100026F4C
_kext_tar	0000000100026F60
_kext_tar_len	0000000100053560

Name	Start	End
HEADER	0000000100000000	0000000100000770
__text	0000000100000770	000000010000199D
__stubs	000000010000199E	0000000100001A1C
__stub_helper	0000000100001A1C	0000000100001B00
__cstring	0000000100001B00	0000000100001F5E
__unwind_info	0000000100001F5E	0000000100001FAE
__eh_frame	0000000100001FB0	0000000100002000
__program_vars	0000000100002000	0000000100002028
__nl_symbol_ptr	0000000100002028	0000000100002038
__got	0000000100002038	0000000100002040
__la_symbol_ptr	0000000100002040	00000001000020E8
__data	0000000100002100	0000000100053564
__common	0000000100053568	0000000100053588
__LINKEDIT_hidden	0000000100054000	000000010005479C
ABS	00000001000547A0	00000001000547A8
UNDEF	00000001000547B0	0000000100054868

【图 5】各模块中文件的位置

Ventir 恶意软件代表特征是模块中使用了开源代码。这种开源代码使用户可以自由使用，并且通过 Github 网站共享也很方便。前面已谈到的 Gh0st RAT 工具也可以看成这种开源代码的一种。随着利用这种开源代码的恶意软件的增加，针对 Mac OS X 的恶意软件的制作也变得容易。因此，该恶意软件除了它本身导致的损失，还影响到多样恶意软件的增加。

新的威胁的序幕–Wirelurker

去年11月发现的 Wirelurker 是与以往不同的新的形式的恶意软件。它只针对于 Mac OS X 和 iOS 制作，感染过程如图 6。即主要通过“麦芽地”等第三方苹果应用平台对 Mac 设备及 iOS 设备进行感染。
Wirelurker 主要影响的是中国用户，来源于一个名为“麦芽地”的第三方软件商店。该病毒特征是，利用正常软件的重装、通过 iOS 设备连接PC时被感染、还可以感染没有越狱的 iOS 设备。 Wirelurker 打破了“Mac OS X 安全神话”。虽然由该恶意软件发生的损失并不是很大，但是显示了比以往更精巧的技术，因此对于整个安全行业影响深远。

结束语

通常 Mac 用户认为 OS X 不会像 Windows 经常受到恶意软件攻击。因为确实 Mac 恶意软件远远不及 Windows 恶意软件之多，并且影响程度目前还不是很大。但是，在2014年发现的 Mac 相关的恶意软件说明了 Mac 也无法从恶意软件攻击中获得自由。
上面所提到的跨平台攻击形式 Mac 恶意软件并不是2014年新出现的，而是从过去到现在不断出现的恶意软件。新出现的恶意软件有上述的 Wirelurker，技术水准越来越高且针对于 Mac 系统。这些病毒的出现已证实了Mac 系统已不再安全，也存在被恶意软件攻击的可能性。

为了预防这些恶意软件，必须遵守下面的三个守则：
1. 仅下载和安装经过验证的软件
2. 开启时确认注册的程序
3. 安装反病毒软件并使用

最后，不管是 Windows 还是 Mac，所有的技术不可能完美无瑕。2015年会有更多的新的技术将来到我们的生活圈，如“金融技术(Fintech)”、“物联网(IoT)”等。但是，如果用户不转换对安全的认识，即使有最好的和最方便的技术也因为安全问题而无法自由地使用。只有基于充分的安全知识，才可以完美地享受新的技术。

http:// cn.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | sales@ahn.com.cn