



iOS 恶意应用分析综述

朱易翔^{1,2}, 张慷³, 王渭清⁴

(1.移动互联网系统与应用安全国家工程实验室, 上海 201315;

2. 中国电信股份有限公司上海研究院, 上海 200122;

3. 中国电信股份有限公司上海分公司, 上海 200120; 4. 中国电信集团公司, 北京 100033)

摘要:介绍了 iOS 的安全架构和应用程序的分发模式, 分析了 iOS 平台上恶意应用程序对用户数据安全和隐私构成的威胁, 讨论了 iOS 上恶意应用少于 Android 系统恶意应用的原因, 总结了已出现的 iOS 恶意应用的攻击方法, 并对未来的缓解和对抗策略进行了展望。

关键词: iOS 安全; 恶意代码; 恶意应用

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017048

Review of iOS malicious application analysis

ZHU Yixiang^{1,2}, ZHANG Kang³, WANG Weiqing⁴

1. National Engineering Laboratory for Mobile Internet System and Application Security, Shanghai 201315, China

2. Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

3. Shanghai Branch of China Telecom Co., Ltd., Shanghai 200120, China

4. China Telecom Corporation, Beijing 100033, China

Abstract: The security architecture and distribution of iOS were introduced. The threats to user's data security and privacy from iOS malicious applications were analyzed. The reasons that the number of iOS malicious applications is less than Android malicious applications were discussed. The attacking methods of emerging iOS malicious applications were summed up. And prospect for future mitigation and confrontation strategies were given.

Key words: iOS security, malicious code, malicious application

1 引言

随着移动互联网的迅速普及, 移动设备的各种安全问题日益突出。移动智能终端恶意软件、用户敏感信息泄露及未授权访问等各种类型的安全威胁给移动互联网用户带来了极大的困扰。手机恶意软件对终端用户的侵扰已泛滥成灾, 这对广大手机网民的财产和隐私信息安全构成危害。中国互联网络信息中心报告显示^[1], 超过半数的手机网民遭遇过恶意扣费、恶意强制联网、窃取隐私

信息、恶意传播和破坏等恶意行为。手机恶意软件及隐私泄露已造成大规模的不良影响, 引起社会广泛关注。

谷歌 Android 和苹果 iOS 是两类主流的移动设备操作系统, 二者占据巨大的市场份额。针对 Android 系统的恶意应用已经出现爆发式增长的问题, 学术界和工业界也推出了各种检测、防护与分析技术和安全产品。与 Android 系统紧迫的安全形势不同, 在很长时间里并未大规模出现针对 iOS 系统的恶意应用。因此很多用户都认为 iOS 系统的安全性优于 Android 系统。

本文将介绍 iOS 系统的安全架构和应用程序的分发模式,分析 iOS 平台上恶意应用程序对用户数据安全和隐私构成的威胁,讨论 iOS 系统恶意应用少于 Android 系统恶意应用的原因,总结已出现的 iOS 恶意应用的攻击方法,展望未来的缓解和对抗策略。

2 iOS 安全架构背景

2.1 iOS 版本历史与主要安全机制演进

iOS 的最初名称是 iPhone OS,由第一代 iPhone 设备于 2007 年 6 月搭载发布。随后苹果公司对 iPhone OS 不断升级。2010 年 6 月,随着 iPhone 4 的发行,苹果公司正式将移动设备上的操作系统简称为 iOS 并发布了 iOS 4.0。此后,随着硬件型号的不断升级、新功能特性的引入以及安全漏洞补丁的发布,iOS 系统也一直在频繁升级,目前最新的正式发行版是 iOS 10.2。

iPhone OS 的最初版本(1.x 系列)并未将安全机制作为重点,没有引入任何漏洞攻击缓解方案,而且所有进程以 root 身份运行。但是,随着 iPhone OS 2.0 的发布,苹果引入了 App Store(应用商店)的应用程序发布形式,即第三方应用程序的发布、下载只能通过苹果官方的应用商店。为了支持该特性,苹果公司在 iPhone OS 2.0 中加入了强制代码签名机制。通过强化内核中内存访问和管理机制,iPhone OS 2.0 不允许应用程序分配或使用同时可执行和可写的内存页面,并加强对可执行页面的安全检查,确保所有可执行页面被可信证书签名保护。

此后,硬件的升级为引入更多安全机制创造了条件。iOS 4.3 中引入地址空间布局随机化(address space layout randomization, ASLR),该策略已被其他各主流操作系统广泛应用。这种机制确保程序运行时的内存布局(代码位置、栈位置以及堆数据)对远程攻击者的不可预测性,从而显著增加了漏洞利用的难度。iOS 6 中引入了内核地址空间布局随机化(kernel address space layout randomization, KASLR),从而确保内核执行空间的随机性。iOS 7 中开始启用 touch ID,允许用户在 64 bit 的设备上通过指纹解锁设备。iOS 8 中引入了开发者身份(team ID)验证,确保苹果自身开发的程序与第三方开放

的动态链接库隔离。在 iOS 9 和最新的 iOS 10 中,苹果已经采用基于 TrustZone 的内核完整性保护机制,确保内核可执行页面不可被永久篡改。iOS 主要安全机制发展过程^[2]如图 1 所示。

此外,iOS 继承了 UNIX 操作系统的权限管理和用户隔离机制,并且定制了严格的沙盒(sandbox)规则,基于硬件实现数据加密。苹果基于硬件保护机制确保机器启动过程的完整性,而且将操作系统的内核文件加密保存。在版本控制上,iOS 采用更为严格的机制:设备不能降级安装低版本的 iOS 操作系统。该策略使得 iOS 设备一旦升级后就只能停留在当前或最新版本,有效避免了操作系统版本碎片化问题,减少了已公开漏洞的影响范围。

2.2 iOS 应用程序分发机制

苹果公司于 2008 年 7 月推出应用程序分发和下载平台应用商店。终端用户可以通过应用商店搜索、发现、下载和购买各种应用程序。第三方开发者可以通过参加苹果开发者计划向应用商店提交应用程序并在应用商店上发布。根据苹果公司公布的数据,应用商店上已有 140 万个以上的应用程序,总下载量达千亿次^[3]。

由于 iOS 设备上严格的代码签名机制,第三方开发者必须通过参加苹果开发者计划获得苹果公司签名的开发证书后,才能在物理机上运行、调试自己开发的应用程序。目前苹果公司推出 3 种开发者账号:个人账号、企业账号和教育账号。个人账户开发者证书一年内最多只能在 100 台物理机上有效,而企业账号证书则没有这个限制。教育账号是苹果公司为了鼓励和吸引高校更多地参与到苹果开发者的计划中而特意推出的一项计划,高校计划具有在真机上开发、调试等权限,但不能将 App 发布到苹果应用商店。

第三方应用程序在应用商店上架前,必须经过苹果公司的审计。在审计过程中,苹果公司要进行内容审核、功能稳定性审核以及检查应用程序是否含有恶意功能。对于已上架的应用程序,苹果公司可以随时将其下架。

应用商店上的第三方应用由苹果公司签名,并且通过未公开的数字版权管理(digital right management, DRM)技术加密程序的可执行代码。此外,从应用商店上下载的应用

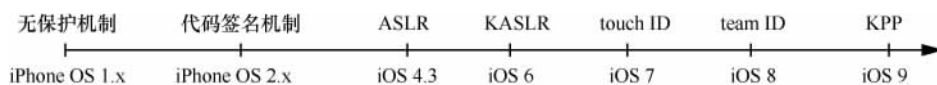


图 1 iOS 主要安全机制发展过程



用程序,如果未经过购买者账户(Apple ID)的授权,依然不能直接在物理机上运行。换言之,苹果公司基于代码签名机制和 DRM 保护机制,严格保护应用商店上应用程序的安全。

2.3 iOS 越狱

由于 iOS 原生系统的封闭性和苹果对 iOS 系统的强控制力,iOS 系统的安全性远强于其他系统。iOS 系统采用了诸多严格的安全机制,如可信启动链、代码签名、沙盒执行环境、权限隔离和数据加密,这使得针对 iOS 系统的安全威胁总数远低于针对 Android 系统的安全威胁总数。这也是“iOS 平台相对安全”惯性思维的由来。

然而 iOS 系统的封闭性也是被很多用户一直诟病的地方。iOS 设备的拥有者仅具有设备的使用权和有限的管理权。例如,iOS 用户只能从指定渠道下载 App,无法获得设备的 root 权限,无法更改系统的关键配置文件。这些特性使 iOS 设备更加安全,但也限制了第三方 App 的功能,影响了用户的体验效果。

从安全研究角度而言,iOS 系统中加密的固件包和严格的沙盒访问控制使得第三方安全人员很难对 iOS 设备的内核和应用程序进行分析。对于应用商店上的第三方 App,苹果公司采用了一套复杂的 DRM 机制来加密这些程序的代码段,只有当这些程序运行时才由内核解密这些代码。这直接导致第三方安全人员无法对 iOS 平台上的可执行程序进行静态分析。

自 iOS 系统发布起,很多安全人员一直致力于研究如何通过利用 iOS 设备硬件和软件中的漏洞,突破 iOS 系统

中的诸多限制,获得对 iOS 设备的完全控制权,这就是越狱。越狱后,用户可以获得对文件系统的完全访问,自主控制应用程序的安装和卸载,从第三方 App 发布平台获取 App,根据自己需求定制化系统配置。

通常而言,越狱的目的是为了突破 iOS 系统的限制,并不是完全破坏 iOS 系统所有的安全策略。越狱工具对 iOS 设备的改变很大,其中最为关键的两点是禁用 iOS 代码签名检查和开放 root 权限。为了维持越狱设备的安全性,越狱工具通常不会破坏其他安全策略,如沙盒、ASLR、数据执行保护(data execution protection,DEP)等。但是,由于越狱后用户可以在设备上安装运行任意代码,这给安全带来了许多隐患。

3 iOS 恶意应用案例

iOS 系统大规模普及后,很长时间内并未出现过大规模流行的恶意应用程序。对历史上出现的典型 iOS 恶意应用和攻击进行回顾分析,见表 1,分类介绍并总结 iOS 恶意应用的发展趋势。

3.1 针对越狱手机的恶意应用

由于越狱后的手机不再具备强制代码签名等安全机制,越狱后的设备成为大部分针对 iOS 恶意应用的首选目标。

(1) iKee^[4]蠕虫

最早出现的针对越狱设备的蠕虫类型。很多用户在越狱的 iOS 设备上安装 open SSH,但未能及时修改 open SSH 的 root 账号和密码。iKee 蠕虫通过扫描 open SSH 端

表 1 典型的 iOS 恶意应用和攻击

恶意应用	出现时间	传播途径	恶意功能	受染机器类型
iKee	2009 年 11 月	open SSH	修改壁纸、锁机以及将 iOS 设备加入 botnet(僵尸网络)中	越狱设备
AppBuyer	2014 年 9 月	第三方 Cydia 源	窃取 Apple ID 和密码、盗用用户身份下载应用程序	越狱设备
WireLurker	2014 年 11 月	已感染的个人电脑	收集用户隐私信息、安装新的应用程序	越狱设备、未越狱设备
SpyPhone	2010 年 8 月	应用商店	收集多种个人隐私数据,包括电话号码、通讯录、照片、地理位置等	未越狱设备
Mactans	2013 年 8 月	充电器	模拟用户点击、安装并隐藏应用程序、监视用户输入等	未越狱设备
Jekyll	2013 年 8 月	应用商店	发送短信、邮件、后台录像、拨打任意电话等	未越狱设备
XcodeGhost	2015 年 9 月	应用商店	收集用户隐私并具备伪造弹窗等功能	未越狱设备
YiSpecter	2015 年 10 月	网络流量劫持、网页欺诈等	收集设备 UUID 等用户隐私、安装企业证书签名的应用、替换其他应用	越狱设备、未越狱设备
Pegasus/Trident	2016 年 8 月	短信发送网址链接的精准 APT 攻击	完全控制 iOS 设备	越狱设备、未越狱设备

口、尝试使用 root 账号和默认密码登录就感染了大量越狱设备。设备一旦感染 iKee 蠕虫,就会被加入某些僵尸网络中,并进一步扫描周围的 IP 地址进一步传播 iKee 蠕虫。

(2) AppBuyer^[5]

随着越狱设备的增多,在越狱应用商店 Cydia 中也不断出现针对越狱 iOS 设备的恶意应用。AppBuyer 是一款非常典型的恶意应用。首先,AppBuyer 通过劫持越狱设备网络通信的关键系统函数,获取用户的 Apple ID 和密码,上传至攻击者控制的远程服务器。其次,AppBuyer 可以远程下载并升级可执行代码等功能。此外,AppBuyer 会模拟用户在苹果公司应用市场上购买应用程序的协议,以用户的身份在应用商店上下载应用。与 AppBuyer 类似的恶意应用还有 AdThief/Spad、Unflod 等。AppBuyer 等恶意应用通常都是通过第三方 Cydia 软件仓库源分发恶意应用,欺骗用户主动下载安装,因此在传播范围上存在很大局限。

(3) WireLurker

在 2014 年 USENIX Security 年会上,研究人员预测通过个人电脑可以大规模感染 iOS 设备^[6]。2014 年 11 月,多个安全公司发现了真实案例。WireLurker^[7]通过在 Mac OS 上的木马应用程序,监视 USB 端口,一旦有 iOS 设备接入,就进一步攻击接入的 iOS 设备。WireLurker 不仅可以攻击越狱的 iOS 设备,还能感染未越狱的 iOS 设备。WireLurker 收集大量用户隐私数据,并且采用代码混淆、加密等对抗性技术手段防止被分析。

3.2 针对非越狱手机的恶意应用

(1) SpyPhone^[8]

早期的 iOS 版本(4.x 版本)中的沙盒规则过于宽松,这导致沙盒内的应用程序可以直接访问电话号码、通讯录、Safari 搜索历史、电子邮件账户、键盘缓存、照片、GPS 以及 Wi-Fi 接入点。Nicolas Seriot 在 Blackhat DC 2010 会议上展示了名为 SpyPhone 的普通应用程序获取用户敏感隐私数据,突出了 iOS 沙盒规则问题的严重性。在 SpyPhone 之前,一家游戏公司 Storm8 在其旗下的多款 iOS 产品中收集用户电话号码。

(2) Mactans^[9]

在 iOS 7 之前,个人电脑可以直接对接入的 iOS 设备进行应用程序的安装或卸载、文件的备份或还原等操作。由于 iOS 设备完全信任个人电脑,引发了很多安全隐患。研究人员设计了一个针对 iOS 设备的特殊充电器,在 USB

接口上对 iOS 设备攻击,实现隐私窃取、模拟用户点击、安装隐藏应用程序、监视用户点击等功能。

(3) Jekyll^[10]

尽管苹果公司会在第三方应用程序上架前进行安全检查,研究人员证实这种检查根本无法杜绝恶意的应用程序。名为 Jekyll 的恶意应用在自身代码中设置基于漏洞触发的后门,在不引入任何新的执行代码的情况下,在程序运行时重新组合已有功能片段实现各种恶意攻击。

(4) XcodeGhost^[11]

2015 年 9 月爆发的 XcodeGhost 事件是迄今为止感染规模最大的 iOS 恶意应用。XCode 是由苹果公司发布的运行在操作系统 Mac OS X 上的集成开发工具,是开发 OS X 和 iOS 应用程序的最主流工具。由于 XCode 安装包太大,从苹果官方下载 XCode 经常失败,因此很多开发者更倾向于从第三方站点下载 XCode。攻击者根据这种现象,通过对 XCode 安装包进行篡改,加入恶意模块,并通过各种社交媒体等渠道进行传播,诱使大量开发者使用被污染过的版本建立开发环境。经污染过的 XCode 编译 iOS 应用程序时,会植入额外的恶意逻辑,其中包括向攻击者注册的域名回传若干加密信息,并包含伪造弹窗和远程控制等功能。在 XcodeGhost 事件中,许多流行 iOS 应用被感染,其中包括微信、网易云音乐、12306、滴滴出行等,据不完全统计,在本次感染事件中中招的 iOS 用户数高达 1 亿户。

(5) YiSpecter^[12]

一款在中国被广泛发现的 iOS 恶意应用。通过 ISP 流量、Windows SNS 蠕虫、离线应用安装等传播途径,YiSpecter 可以在 iOS 设备上安装企业证书签名的恶意应用,从而收集设备 UUID、MAC 地址等用户隐私信息,并利用系统私有 API 特性替换已安装的应用等,在合法应用内展示广告、改变 Safari 默认搜索引擎、向远程服务器上传用户信息。

(6) Pegasus/Trident^[13]

阿联酋的人权活动人士曼苏尔于 2016 年 8 月 10 日与 11 日收到两条声称含有囚犯在阿联酋监狱中遭到折磨的“秘密”短信,曼苏尔觉得此事蹊跷,于是把线索提供给了公民实验室,公民实验室依据链接顺藤摸瓜,发现这是 NSO Group 针对曼苏尔实施的 APT(advanced persistent threat,高级持续性威胁)攻击。该恶意代码使用的就是被称为 iOS PEGASUS(又称 Trident 三叉戟)的一组 0day 漏洞,包括 CVE-2016-4657(Safari 的 Webkit 内核上的内存破坏漏洞)



和 CVE-2016-4655 (内核信息泄露漏洞), 可用于绕过 KASLR 和 CVE-2016-4656(内核 UAF 漏), 控制内核并执行任意代码。为了修复该漏洞, 苹果公司专门发布了一个 iOS 9.3.5 版本。该恶意代码可以直接从沙盒内对内核进行攻击(无需沙盒逃逸), 并且同时影响 iOS (9.3.4) 和 OS X (10.11.6)。

4 iOS 安全生态分析

综上, iOS 系统的恶意应用已经从针对越狱环境发展到越狱环境和非越狱环境兼顾的形态, 从仅能小范围感染发展到可以大规模传播, 并且展现出丰富的攻击途径, 既包括官方的应用商店和越狱应用市场的第三方软件安装源, 也包括恶意的物理外设(例如充电器), 甚至涉及 ISP 层面流量劫持等。

同时, APT 攻击是当前网络空间安全面临的最严峻挑战之一, 随着移动互联网的飞速发展, 智能移动设备已成为 APT 的重点攻击目标。iOS 系统是除 Android 系统外移动智能设备上使用最多的操作系统, 毫无疑问也是 APT 攻击的重点关注对象, iOS 恶意应用也成为 APT 攻击中重要的工具。iOS 恶意应用所用到的攻击技术, 曾经以应用层漏洞利用为主流, 随着苹果公司对 iOS 系统安全机制的不断完善和对攻击途径的不断封堵, 当前直接攻击系统接口和内核的漏洞利用也成为了重要的技术途径, 包括苹果公司、APT 攻击者等黑色产业、越狱研究团队、移动安全研究团队在内的整个生态圈, 都应对相关领域的漏洞发掘技术、漏洞利用技术、安全防范机制基于更多的持续关注。

5 结束语

面对各种层面针对 iOS 的高级攻击和威胁, 业界尚鲜有针对苹果 iOS 的安全审计、检测和分析平台, 与如火如荼的 Android 安全分析市场形成了鲜明对比。已有的针对 iOS 的安全分析工具仍停留在简单的辅助人工分析阶段。国内业界公司尚未在 iOS 平台二进制分析系统上取得重大进展。学术界提出的各种原型系统很难对当前主流 iOS 系统上的应用程序实施有效分析。如何加强对苹果应用商店上应用程序的安全审计并推动第三方独立检测平台落地将成为下一阶段的热点。

参考文献:

[1] 国家计算机病毒应急处理中心. 第十四次全国信息网络安

全状况暨计算机和移动终端病毒疫情调查报告[R]. 2015.

National Computer Virus Emergency Response Center. 14th analysis of national security situation of information network and investigation report on computer and mobile terminal virus[R]. 2015.

- [2] iOS 9.3 or later. iOS security-white paper[S/OL]. (2016-05-01) [2016-10-10]. https://www.Apple.com/business/docs/iOS_Security_Guide.pdf.
- [3] Apple's app store has passed 100 billion app downloads[EB/OL]. (2016-06-08) [2016-10-10]. <http://www.theverge.com/2015/6/8/8739611/Apple-wwdc-2015-stats-update>.
- [4] CHARLIE M, DION B, DINO D, et al. iOS hacker's handbook[M]. New York: Wiley, 2012.
- [5] AppBuyer: new iOS malware steals apple ID and password to buy apps [EB/OL]. (2014-09-12) [2016-10-10]. <http://researchcenter.paloaltonetworks.com/2014/09/APPbuyer-new-ios-malware-steals-Apple-id-password-buy-APPs/>.
- [6] WANG T, JANG Y, CHEN Y, et al. On the feasibility of large-scale infections of iOS devices [C]//The 23rd USENIX Security Symposium (Security), August 20-22, 2014, San Diego, CA, USA. New Jersey: IEEE Press, 2014: 79-95.
- [7] Wirelurker: a new era in iOS and os x malware[EB/OL]. (2014-11-05) [2016-10-10]. <https://www.paloaltonetworks.com/resources/research/unit42-wirelurker-a-new-era-in-ios-and-os-x-malware.html>.
- [8] NICOLAS S. iPhone privacy[S/OL]. (2012-04-07) [2016-10-10]. <http://renewnews.com/files/iPhonePrivacydoc.pdf>.
- [9] LAU B, JANG Y, SONG C, et al. Mactans: injecting malware into iOS devices via malicious chargers[C]// Black Hat USA, July 27-Aug 1, 2013, Las Vegas, NV, USA. New Jersey: IEEE Press, 2013.
- [10] WANG T, LU K, LU L, et al. Jekyll on iOS: when benign apps become evil [C]// Usenix Conference on Security, August 12-13, 2013, Washington D C, USA. New Jersey: IEEE Press, 2013: 559-572.
- [11] 安天实验室. Xcode 非官方版本恶意代码污染事件 (XcodeGhost) 的分析与综述[R/OL]. (2015-09-20) [2016-10-10]. <http://www.antiy.com/response/xcode/xcodeghost.pdf>.
Antian Laboratory. Analysis and review of Xcode unofficial version of the malicious code pollution incident (XcodeGhost) [R/OL]. (2015-09-20) [2016-10-10]. <http://www.antiy.com/response/xcode/xcodeghost.pdf>.
- [12] YiSpecter: first iOS malware that attacks non-jailbroken apple iOS devices by abusing private APIs [EB/OL]. (2015-10-04) [2016-10-10]. <http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices->

by-abusing-private-apis/.

[13] Pegasus- 针对 iOS 设备的 APT 攻击分析[EB/OL]. (2016-08-26) [2016-10-10]. <http://blog.pangu.io/pegasus-apt/>.

Pegasus-analysis of APT attacks on iOS devices [EB/OL]. (2016-08-26) [2016-10-10]. <http://blog.pangu.io/pegasus-apt/>.

[作者简介]



朱易翔(1979-),男,中国电信股份有限公司上海研究院互联网安全部副主任,负责移动互联网系统与应用安全国家工程实验室技术研发工作,主要研究方向为安全体系与架构、安全攻防与漏洞发掘、移动应用安全检测等。



张慷(1969-),男,中国电信股份有限公司上海分公司信息网络部经理、高级工程师,主要研究方向为信息安全管理、云安全。



王渭清(1980-),男,中国电信集团公司工程师,主要研究方向为信息安全管理、大数据安全。