300多款热门App感染恶意程序 病毒制造者身份已被锁定

还能愉快地让苹果“裸奔”吗

近日，多家安全企业都曝光了一起名为“XcodeGhost”的安全事件，病毒制造者通过感染苹果应用的开发工具Xcode，让AppStore中的正版应用带上了会上传信息的恶意程序。据估算，受到影响的用户数量可能超过了1亿。这一事件的爆发，也打破了原本被认为安全性很高的苹果iOS系统的“金身”。360公司表示，目前已经通过技术手段基本锁定了病毒制造者的身份，并且已经报警。

事件

300多款热门App感染恶意程序

近日，多款知名社交、地图、出行App的iPhone版被爆出有“恶意代码”。此次的“XcodeGhost”事件之所以热度极高，很重要的一个原因是受到影响的用户数量极多。

事件曝光后，多家移动安全企业都公布了各自检测出受波及的App名单，其中360涅槃团队公布的受影响App数量最多。涅槃团队称，通过对14.5万款App的扫描，发现有344款App都感染了恶意程序，其中不乏微信、12306、高德地图、滴滴打车等热门App。据腾讯安全应急响应中心发布的报告，保守估计，受这次事件影响的用户数超过了1亿，这可能是苹果AppStore上线以来涉及用户数最多的一起安全事件。

目前，微信、高德地图、滴滴打车、网易云音乐等一些知名App都对外承认受到了“XcodeGhost”事件的影响。不过，这些公司在声明中也表示，这一事件不会对用户的信息安全造成威胁，并且已经发布了修复恶意程序的新版本应用，用户自行升级就可以解决。例如，微信团队在公开声明中就表示，“该问题仅存在iOS6.2.5版本中，最新版本微信已经解决了此问题，用户可升级微信自行修复，此问题不会给用户造成直接影响。目前，尚未发现用户因此而造成信息或者财产的直接损失，但是微信团队将持续关注和监测此事。”

当然，在为数众多的App中，公开信息的毕竟还是少数。360安全实验室负责人林伟表示，有些小应用的开发团队可能还没有及时对应用进行升级，甚至不排除有的开发者还不知道自己的应用中枪了。“我们也在尽可能发现并且通知用户和开发者。”林伟表示。

木马代码嵌入开发工具源头

在安卓平台上，各种安全问题的爆发对于用户来说已经习以为常了，而苹果的iOS系统一直被认为相当安全，因为苹果对于其中的App有着严格的安全审核机制。不过这一次，对自己手机安全没怎么操过心的苹果用户也有些傻眼了，“从苹果官方下载的App怎么也中毒了？”手机裸奔的感觉让很多iPhone用户感到了惶恐。

“这已经注定成为移动安全史上标示性的事件。”有移动安全方面的人士这样评价，这可以说是迄今为止手机行业最大的一次安全事件，受影响的用户过亿，确实让人感到不寒而栗。

另外，这种直接把木马代码嵌入iOS开发工具源头的攻击方式，在国内尚属首次，而一旦这扇门开了，带来的风险是不言而喻的，类似的攻击方式也会引发更多黑色产业链的效仿。

据盘古越狱团队的创始人韩争光介绍，实际上这种从源头上进行污染的黑客手段，很早之前就有人提出过。UNIX之父KenThompson在一次演讲中就做过类似的假设，斯诺登曝光的材料里也提到过Xcode污染的案例。只不过，本次是这种情况的首次大规模传播。

林伟则表示，苹果是不允许用户使用第三方安全软件的，之前大家可能觉得这没什么，但此次事件之后能看出，安全企业提供的保护方案要比手机厂商自己做的要更专业。他认为，最理想的情况就是苹果向第三方安全软件开发iOS系统，让不越狱的iPhone用户也能接受更加专业可靠的安全保护。

苹果已经向受影响的应用开发者发出了应用下架通知，要求开发者从正规渠道下载Xcode程序，重新编写应用程序再上传。

进展

病毒制造者的身份已被锁定

就在事件爆发后，自称是“XcodeGhost”始作俑者的新浪微博用户@XcodeGhost-Author在网上发了一封道歉信。他称，XcodeGhost源于他自己进行的一项实验，获取的全部数据实际为基本的App信息：应用名、应用版本号、系统版本号、语言、国家名、开发者符号、App安装时间、设备名称、设备类型，除此之外，没有获取任何其他数据。他也承认，出于私心他在代码加入了广告功能，希望将来可以推广自己的应用，但从开始到最终关闭服务器，并未使用过广告功能。而在10天前，他已主动关闭服务器并删除了所有数据，更不会对任何人有任何影响。“XcodeGhost不会影响任何App的使用，更不会获取隐私数据，仅仅是一段已经死亡的代码。”这个给无数人带来大麻烦的人这样说道。

不过，这种轻描淡写遭到了很多安全行业从业者的质疑。林伟就表示，360团队对其行为的追踪发现，在半年之前，就有人开始在大量的iOS开发论坛上散布Xcode的下载链接，甚至还有人入侵了某论坛版主的ID来修改下载链接。而这些下载链接全部指向了同一份网盘文件，如此大规模的举动，做实验的说法根本解释不通。也有网络工程师在微博上算了一笔账，这种对用户信息的收集，仅仅是使用海外服务器的成本每月就要四五十万美元。“这难道仅仅只是个苦×开发者的个人实验吗”？

韩争光也认为，进行这种黑客行为，对制造者的技术水平要求很高，绝非一般人能够所为。而且，从其一系列行为来看，不大可能是一个人做出来的，应该是有一个团队在操盘，背后很可能和黑色产业链有关系。

360公司对记者表示，目前已经通过技术手段基本锁定了病毒制造者的身份，并且已经报了警，正在配合警方进行调查。不过360相关人士表示，在警方结案前，还不能公布关于病毒制造者身份的更多细节。从记者在多个渠道获得的信息来看，病毒制造者并非一个人，其中一名主要成员曾是国内某名校的保送研究生，不过已经退学。

建议

用户应定期修改密码

不管黑客是怎么得手的，对于普通用户来说，最重要也是最关心的事只有一个，那就是自己的手机究竟安不安全？“微信、滴滴打车、12306，这些应用我都装了，还做过支付，会不会有风险？绑定的信用卡会不会被盗刷？”很多用户急切地想知道答案。

从上述“病毒开发者”的回应来看，“XcodeGhost”收集的数据确实不涉及太敏感和关键的信息，目前尚无证据证实“XcodeGhost”有利用收集用户信息违法获利的行为，也没有收到用户损失方面的报告。从这个方面来说，即便安装了受影响的App，iPhone用户也不必过于紧张。

不过，韩争光认为，虽然现在看不到这个恶意程序造成了什么损失，但这个恶意程序是可以带来很多更严重威胁的。就像一个高明的窃贼，撬开了严密的防盗门，进到一个人的家里，只留下了几张“小广告”就走了，但是，他将来是有能力进到家中把财物席卷一空的，“也有可能家中失窃了，但是房主还没有发现。”

韩争光建议，手机中安装了受到影响的App的用户，如果是常用的应用，就暂停使用，等开发者发布新的版本，更新后再使用；如果是不常用的应用，可以直接卸载。他同时还建议，虽然目前还没有看到造成损失的案例，但确实存在泄露个人关键信息的风险，还是建议用户修改一下手机中的重要密码。无论有没有安全事件，定期修改密码都是一个良好的习惯。

开发者应确保开发环境安全

这一次的“XcodeGhost”事件和以往安全事件最大的不同，在于用户开始是无从防范的，苹果应用的开发者成为了病毒传播链条上很关键的一环。虽然病毒制造者污染了Xcode工具，但如果开发者都从正规渠道下载这一工具，也不会造成现在的局面。

有iOS开发者表示，从其他渠道下载Xcode而不是从苹果官方渠道下载，其实是业内很普遍的行为。因为官方下载渠道速度太慢，很多程序员为了节省时间，往往直接使用国内的下载工具下载，这就给了“XcodeGhost”病毒以可乘之机。

猎豹移动表示，这件事给程序员敲响了警钟：要安全，首先得保证自己的开发工具安全。程序员被黑客暗算的事曾经多次发生，无论如何，建议使用正版、未被非法篡改过的开发工具编写程序，避免用户成为受害者；其次，编译环境、发布环境的安全也值得注意，编译服务器和自动发布服务器应保持干净的环境，不要随意安装来源不明的可疑软件。

安全行业业内人士表示，这一次事件给苹果在安全机制方面敲响了警钟，让苹果注意到了自身安全机制方面存在的漏洞。相信苹果会修补这次安全事件造成的影响，在安全审查上变得更加严格。 （京华）