信息安全意识

双十一网购高峰
钓鱼网站趁机作乱

001 No. 2014.11
电子期刊
INFORMATION SECURITY

国信办将出 APP 管理办法：
治病毒、窃取信息乱象

Apple Pay 竞争对手被黑：
移动支付安全遭质疑

黑客利用“沙虫”
漏洞攻击瑞士银行客户

简单几招提升个人电脑安全性

苏州银行
BANK OF SUZHOU

Contents 目 录

业界动态：

国信办将出 APP 管理办法：治病毒、窃取信息乱象 01
黑客利用“沙虫”漏洞攻击瑞士银行客户 02
被忽视的企业数据安全致命威胁：文档分享 03

信息安全在身边：

Apple Pay 竞争对手被黑：移动支付安全遭质疑 04
谷歌为 Android Lollipop 增加多项安全特性 05

水滴石穿：

简单几招提升个人电脑安全性 07

警钟长鸣：

双十一网购高峰 钓鱼网站趁机作乱 09

国信办将出 APP 管理办法：治病毒、窃取信息乱象

据悉，国家网信办将出台 APP 应用程序发展管理办法。国家网信办副主任彭波表示，目前在依法治国的进程中，依法治网是最基础的工程，又是最艰巨的任务，需尽快“补课”。

近年来，智能手机产业的发展催生了 APP 应用程序行业的兴起。然而，在提供便捷服务的同时，病毒、窃取用户信息等问题也时有发生，APP 安全问题日益凸显，行业乱象备受关注。

日前，中央网信办主任鲁炜在推进网络空间法治化座谈会上透露，我国将加强互联网立法，依靠严密的法律网来打造规范的互联网。根据国务院授权，国家网信办负责网上内容管理和网上执法。

中国政法大学传播法中心研究员、副教授朱巍对新京报记者表示，在当前的情况下，国家网信办对 APP 管理进行立法是非常必要、及时的。目前很多 APP 客户端存在抓取用户个人信息和通讯录的行为，这实际上侵犯了用户的个人信息权，非该 APP 使用者的个人信息也会被暴露。

朱巍认为，一些手机 APP 类似自媒体，进入门槛低、影响大，缺乏规制，“比如其内容只为吸引眼球，没有维权途径；一些 APP 只重视用户的增加，忽视对内容的监管。”

此外，北京网信办主任佟力强透露，北京正在研究制定《北京市 APP 应用程序公众信息服务发展管理暂行办法》、《北京市即时通信工具公众信息服务发展管理暂时规定实施细则》、《北京市互联网新技术新业务审批暂行办法》等系列法规，还将成立首都互联网协会法律专家委员会，推动各网站人民调解委员会的建立。

焦点 1 APP 管理“九龙治水”比较混乱

据中国政法大学传播法中心研究员、副教授朱巍介绍，目前，在 APP 的管理上没有特别的办法，很多情况下，并没有区分 APP 与电脑程序的治理。

在主管单位方面，我国互联网管理一度处于“九龙治水”的局面，其体现在 APP 管理上，也存在多头管理的现象。举例说，比如一款消费类的 APP，就涉及多个管理部门，包括工商、消协等部门，而一款影视传播的视频 APP，则涉及文化部门或广电部门的管理。

朱巍表示，我国在 APP 管理上，很大程度是依据其用途而分别管理，处于一种相对混乱的状态。

焦点 2 专家建议提高 APP 门槛

朱巍认为，手机 APP 和普通电脑软件不一样，嵌入到手机中，涉及公民的基本隐私，有途径接触到个人的通讯录、图片等。一些 APP 没有处于使用状态，却在后台自动开启运行，一方面占流量，另一方面监控其他软件。

他表示，APP 门槛过低，“一些 APP 从业者缺乏版权意识，很多同款 APP 滥竽充数，窃取用户信息，也有一些 APP 有‘钓鱼’功能，侵犯个人信息隐私。一些运营商还会将窃取到的用户信息出售盈利。”

朱巍认为，有必要提高 APP 的入门门槛，尤其是特殊的 APP 领域，如新闻客户端或网络交易的应用程序，“这样做并不是限制 APP 发展，而是为了营造健康有序、优胜劣汰的市场环境。”

黑客利用“沙虫”漏洞攻击瑞士银行客户

丹麦的安全咨询公司 CSIS 最近警告，“沙虫”漏洞正在被利用来攻击瑞士银行的客户。

CSIS 发现， “沙虫”漏洞被用来传播最新版本的 Dyre 银行木马。 黑客们利用钓鱼邮件， 发送给用户关于未付款发票的邮件， 而附件则是利用“沙虫”漏洞精心构造的 PPT。

“沙虫”漏洞在本月早些时候爆出被利用来攻击欧盟和北约的政府机构。 利用 Windows OLE 包管理软件的漏洞来进行攻击。 而微软则在本月 14 日发布了针对这个漏洞（CVE-2014-4114）的补丁。 而这些最近发布的补丁， 在很多系统中还没有打上，这就给了网络犯罪集团很多的机会。

CSIS 发现，利用“沙虫”漏洞的钓鱼攻击， 犯罪分子诱使用户点开附件的 PPT。 从而把一个名为 Dyreza 的木马， 这个木马会把自己伪装成“Google Update Service”从而在每次开机时启动。 对于 Windows 7 系统， 它把自己注入到 explorer.exe 进程中， 并钩住浏览器，而对于其他的 Windows 系统，这一木马则注入 svchost.exe 进程。

CSIS 还发现， 这一木马的命令与控制服务器的所在地是在法国。 这说明这次攻击瑞士银行的黑客也许并不是来自俄罗斯或者乌克兰。

被忽视的企业数据安全致命威胁：文档分享

近年来随着智能手机和平板电脑取代 PC 成为互联网的主力终端，PC 恶意软件的风头似乎也被移动恶意软件和物联网漏洞抢走了。但值得注意的是 2014 下半年随着全球 PC 市场的触底反弹，近几个月来微软 Office 恶意软件又像万圣节的僵尸一样纷纷复活了，纷纷利用 Office 文档发起攻击。

例如，上个世纪 90 年代流行 Office 宏病毒（VBA 病毒）不但复活，而且还会利用 Office 产品漏洞植入后门或下载木马；最近的重大案例是安全牛前不久报道的“沙虫”高危漏洞，俄罗斯沙虫团队通过在钓鱼邮件附件中的 PPT 文件中植入利用“沙虫”漏洞的恶意代码实施攻击。

Office 恶意软件的“复兴”，让人们对时下缺乏安全管控的企业移动办公、文件分享和团队协作应用不免担心起来，因为企业员工的不安全文档分享行为不但会成为恶意软件和针对性攻击的突破口，还会直接危及企业的数据安全。

今天随着移动应用的普及，原有的企业安全边界消失，虽然有 MDM 等移动管理方案，但员工大量通过移动应用、云存储和社交媒体等个人渠道的文件分享让很多企业的数据端点管理面临失控。

最 近 Intralinks Holdings 和市场调查公司 Ponemon 联合对美国和欧洲 1000 名企业 IT 专业人士进行了一次调查，发现文件分享已经成为企业安全面临的最大安全威胁，企业的高级管理者们现阶段能难实施有效的政策来防范不安全的文件分享行为导致的数据泄漏。

该调查表明在企业 CSO 们的注意力被高级持续攻击、下一代防火墙、基于情景感知的安全等新潮安全技术吸引的时候，很少人注意到，古老的 Office 文档分享行为已经成为企业数据安全面临的最为严重和致命的威胁。

Apple Pay 竞争对手被黑：移动支付安全遭质疑

北京时间 10 月 30 日早间消息，移动支付系统 CurrentC 周三表示，该服务遭到了黑客攻击，一些用户的电子邮件地址可能已经泄露。CurrentC 是 Apple Pay 和谷歌钱包服务的竞争对手。

CurrentC 的开发商 MCX 周三发送电子邮件称，过去 36 小时内，其信息安全系统被未获得授权的第三方侵入。该公司的调查表明，除用户的电子邮件地址之外，没有其他信息出现泄露。

美国科技博客 AppleInsider 的多名读者提供了 MCX 周三发送的这封电子邮件的拷贝，这些读者参与了 CurrentC 的试点项目。目前，CurrentC 正在测试之中，并计划于 2015 年正式推出服务。

CurrentC 近期正遭遇一些争议，参与这一项目的零售商被禁止使用其他移动支付系统，例如 Apple Pay 和谷歌钱包。因此上周，Rite Aid 和 CVS 均关闭了基于近场通信 (NFC) 技术的支付系统，不支持近期启动的 Apple Pay。

CurrentC 的主要合作伙伴包括沃尔玛 (和百思买。商户选择 CurrentC 主要是由于，MCX 的系统利用了用户的银行帐号信息，而不是信用卡。如果 CurrentC 能吸引消费者的使用，那么零售商将不再需要支付信用卡刷卡交易费。

相反地，Apple Pay 用户需要扫描当前的借记卡或贷记卡，随后方便地使用信用卡信息来交易。此外，Apple Pay 也支持非接触式支付技术。此前，谷歌钱包等服务已使用了这样的技术。

周三早些时候，MCX 试图在一篇博客文章中为 CurrentC 辩护。该公司表示，敏感的用户信息被保存在云计算平台中，而非用户的智能手机。然而考虑到此次的信息安全事故以及近期其他用户信息的泄露，MCX 坚持相信云计算平台的安全性或许会遭到消费者的质疑 .

另一方面，Apple Pay 采用了匿名的方式，不会与零售商分享用户信息。通过 NFC 技术，iPhone 用户可以拿出手机，并通过 Touch ID 进行交易验证。在后端，安全的 NFC 模块监控附近的终端，从安全模块发送令牌化的支付数据，同时不需要更多的用户操作。

谷歌为 Android Lollipop 增加多项安全特性

谷歌针对旗下最新的 Android 5.0 Lollipop 操作系统增加了几项关于安全性的新改进，包括默认启用系统数据加密、全新的锁屏界面等，在安全性和方便性上都要比以往更全面。下面让我们一来看看 Android Lollipop 究竟增加了哪些新的安全特性。

谷歌公司曾经表示丢失和被盗的 Android 设备数量非常庞大，成为了影响智能手机用户的一个巨大安全问题，因此谷歌在 Android 5.0 Lollipop 中加入了全新的智能锁功能能，用户可以通过蓝牙、NFC 配对设备等进行解锁，甚至就连人脸笑容识别也加入了进来。另外，谷歌还允许系统在锁屏界面下自定义显示通知内容。

另外，未来所有运行 Android Lollipop 系统的设备都将默认启用设备数据加密功能，只要设备从第一次启动开始就会开始对数据提供保障。而这个特性将最大程度的保护用户数据安全，并且谷歌在博客上表示过去的三年始终都在致力于如何对 Android 设备数据进行更好的加密。

最后，谷歌还在 Android Lollipop 中增强了 Security Enhanced Linux 的沙盒功能，可以让新平台更容易的进行监视，时刻预防可能出现的恶意攻击。Android Lollipop 系统可以在 SELinux 执行模式中运行所有应用程序，而这也使 Lollipop 操作系统对于企业用户来说具备的更大的吸引力。

水滴石穿

水不断下滴，可以洞穿石头。
我们要从身边一点一滴做起，
用恒心和努力来构筑起安全意识的屏障

简单几招提升个人电脑安全性

首先，对于想彻底删除的文件，仅对其使用“删除”指令是不够的，即使选择“清空回收站”，文件还是能被恢复。因此，如果您确定此文件再也不需要，那最好还是干脆对它进行“粉碎”处理吧——简单说就是通过粉碎软件一次性把文件的代码全部清理，相当于对这部分区域进行了一次格式化处理，这样就再也无法恢复了。

其次，对于临时不想删除，却又不便让别人看到的文件，您可以对它进行加密处理，但密码要尽量设置地复杂一些（字母和数字交替排列）即可。

第三，最好养成定期清理系统的习惯。在使用电脑过程中，会不断的产生大量的垃圾文件，其中部分文件中保存着我们打开文件、浏览网页等记录。这些记录也有可能暴露您的隐私。对于浏览网页产生的记录，您可以选择“工具”——“IE 选项”，在 " 常规 " 选项卡中的 "Internet 临时文件 " 选项中单击 " 删除文件 " 按钮，即可删除浏览器缓存里保存的记录。

安全警钟长鸣

用鲜活真实的信息安全案例，提示我们每个人，
提高信息安全意识，避免发生同样的错误。

双十一网购高峰 钓鱼网站趁机作乱

双十一，一年中最受广大网友期待的电商促销活动刚刚过去。很多人都在双十一期间“血拼”一场。然而，网购高峰也正是钓鱼网站做乱之时，一些不法分子正是利用了这个购物高峰时期大肆行骗，让网民防不胜防。数据显示，和以往相比，利用虚假购物信息进行钓鱼的比例进一步增加，已高达 38.6%。

网购高峰到来之际，安全专家建议网友更应提高警惕。

1. 在购物时尽量选择比较知名的购物或电商平台

2. 在收到类似退货、中奖之类的信息或邮件后，应核对发件人的号码、邮箱地址等

3. 尤其是要告知对方身份证号、手机号码、银行卡号等敏感信息之前，应当尽可能确认对方的身份，在没有确定之前，尽可能不要透漏这些信息。


苏州银行
BANK OF SUZHOU