安全威胁每周警讯

2011/05/07～2011/05/14

本周威胁指数

***TrendMicro* 中国区网络安全监控中心**

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	↑	DOWNAD 蠕虫关联木马
2	WORM_DOWNAD.AD	蠕虫	★★★★	↓	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
3	TROJ_IFRAME.CP	木马	★★★	↑	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
4	WORM_DOWNAD	蠕虫	★★★★	↓	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
5	TROJ_DLOADER.UVD	木马	★★★	↑	该木马程序是一个恶意软件，但危险低，不具备自动传播到其他系统的能力。它通常是从网上下载，并在用户不知情的情况下自动安装。 通常携带有效载荷木马或其他恶意行为，可从轻度恼人的范围到无可挽回的破坏。他们也可以修改系统设置为自动启动。
6	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
7	TROJ_SPNR.03CG11	木马	★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
8	HTML_IFRAME.AZ	网页病毒	★★	↑	网页病毒,通常在网页在插入一个恶意 iframe,用户在访问该网页时会下载恶意文件或重定向到恶意网站
9	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒
10	WORM_VB.DVP	蠕虫	★★	↑	蠕虫病毒，通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒

系统漏洞信息

MS11-036：Microsoft PowerPoint 中的漏洞可能允许远程执行代码

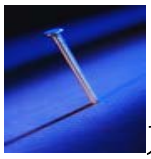
受影响的软件：

Microsoft Office XP Service Pack 3，

Microsoft Office 2003 Service Pack 3

Microsoft Office 2007 Service Pack 2

描述：http://www.microsoft.com/china/technet/security/bulletin/MS11-036.mspx



系统安全技巧

Juniper 网络公司的最近一项调查显示，40%的员工正使用自己的移动设备来处理个人或商业事务，其中 80%的人承认他们未经允许就访问了所在公司的网络。除非企业实施控制，用来防止这些员工所持设备的损失、盗窃或是非法使用，否则任何一件诸如此类的安全事件都可能会使相当多的业务数据承受巨大风险。

保护企业移动设备数据的措施是众所周知的，包括从实施加密到擦除遗失设备上的数据。但是，与员工设备有关的业务数据必须得到相关保障，而不是依赖于 IT 采购和用户，同时还需要尊重用户对个人隐私和选择的期望。

以下介绍五个对员工移动设备和平板电脑上重要数据进行保护的最佳方法。

1. 移动设备锁

设备锁是 IT 业界的第一道防线，防止那些未经授权，对储存在员工移动设备或平板电脑上的业务数据和账户的访问。然而，员工购买的消费电子设备通常不具备足够强大的设备锁。还有，用户可能会重置复杂的密码而不方便个人设备的使用。这种业务需求可以通过一个三步骤方法得以解决。

实施一个程序让用户注册自己的移动设备和平板电脑，并按照最低安全要求检查它们。这样可以防止设备去进行不合标准的商业运用，而允许那些可以支持 IT 范畴内的安全政策。

自动配置已注册的设备以启动内部的 PIN 或密码锁，执行复杂的规则并自动锁定待机的设备。专注于那些可以减少商业风险而不会使之过于严格的规则。

实施无线设备配置监测以保证设置没有被改动。例如，对设备每一次试图访问一个企业账户的行为进行检查，

从而阻止或修复不兼容设备。

如果员工移动设备中包含交互环境搭建（EAS）或多操作系统移动设备管理软件（MDM），那么就可以采取这些措施。目前这些软件已经由诸如 AirWatch、BoxTone、Good Technology、MobileIron、Odyssey Software、Sybase 和 Zenprise 这些公司推出。那些没有 MDM 也不想安装 MDM 的公司可以使用托管 MDM 服务。

2. 移动设备的远程数据擦除

当以前注册过的设备遗失/被盗或者它的主人离开了你的公司，远程数据擦除可以防止将来对存储在设备当中的所有业务数据和账务进行访问。然而，擦除员工的设备资料在没有明确的许可下是不应该的，且在理想情况下，不应对个人数据造成影响或者给用户带来不便。这些业务需求可以解决，方法如下：

作为设备可以注册的条件，员工必须被要求正式同意一些可接受的使用条款。移动设备条款还应该明确，在什么情况下可以调用远程擦除，怎样擦除才不会影响个人设备的使用和数据，以及数据备份/恢复的责任。

考虑使用数据加密工具来区分业务数据、账户和应用程序。例如，使用自加密（self-encrypting）企业信息应用程序能够将电子邮件、通讯录、日历及其他数据保存到一个需要认证的加密沙箱里，这个箱子能够轻易的被移除而不需要擦除整个设备。

实施能够远程擦除员工的设备的流程。为了防止逃避技术，在经过重复登录失败，长时间脱机使用或者移除了 SIM/USIM 卡的情况下，通过自动擦除可以完善无线命令确认机制。确保密切注意留在移动媒体设备（如 Android 设备）上的企业数据。

使用 EAS、任何 MDM，或许多供个人使用的免费或便宜的应用程序（如，苹果的 MobileMe，迈克菲 WaveSecure），可以实现基本的无线远程擦除。然而，更大的 IT 控制和可见性可以按照下面这种 MDM 的用法来实现：例如，报告哪部设备将被擦除，或者自动移除 MDM 之前已安装的企业应用程序和账户。

3. 移动定位和跟踪

在任何移动设备的使用寿命里，关于它的使用情况的大量信息可能会被记录，其中包括地理位置。持续跟踪能（On-going tracking）够帮助 IT 迅速恢复丢失的设备，或产生有关盗窃信息的漫游警报，警告 IT 可能发生的威胁。然而，员工对于隐私权的要求可能会阻碍持续的跟踪。此外，一些用户的设备可能不容易定位（例如，断开或禁用的设备）。最后，如果要追踪涉及到频繁的 SMS 信息，所需的成本可能相当大。

强调商业需求并且考虑到个人和成本的敏感性，决定是否真正需要将持续追踪应用到员工的设备上。如果是这样，你需要在可接受的使用政策中描述定位追踪的业务理念和具体做法，这在注册个人设备为商业使用时需要得到员工的同意。如果定位仅仅只是用来找回遗失的设备，那么你需要将这条陈述写入到可接受的使用政策中，并坚持使用这个有限制的做法。

按需制定的定位服务对每个主要的移动操作系统（例如，苹果的 MobileMe, Lookoutd 的 Find My Phone（安卓），微软的 My Phone，和黑莓的 Wheres My Phone）均可免费使用。但在这里，通过使用移动设备管理器来实施这一做

法能够得到更集中的可视性和控制效果。

4. 移动设备的存储数据加密

在一些情况下，设备锁加上远程擦除就足以减轻用于有限业务的个人设备的风险了。如果移动设备被用于检查无毒的电子邮件且不保存附件，或者只是一台用以进行远程桌面访问的平板电脑，那么它不需要储存那些永久保护的业务数据。然而，在处理敏感信息或者需要更多的功能时，员工还需要对被存储的数据进行加密。不幸的是，一些消费设备并不支持全设备加密。为了解决这一业务需求，可以采取以下步骤：

扩展上述注册流程来检查依托于存储数据加密需求的个人移动设备，在扩展中要使用工作人员已认证的身份来确定移动数据的需求和风险。如果必须加密但设备却不支持，那么需要为员工提供适合设备的指导，条件允许的话，甚至可以提供一个有 IT 安全保障的公司设备。

自动配置已注册的设备，从而在任何可能的地方都能支持全设备加密或者可去掉的媒体加密方式。凡是需要需求和风险允许的地方，都可以配置个人加密应用程序来提供另一层保护，从而使公司的数据和个人的数据分隔开。最后，还可以配置设备的设置和应用程序来最小化存储在设备中的数据量。

使用无线设备配置的监测来确保用户遵守了所有的数据加密政策。此外，要小心关注设备显示出的有被干扰的迹象（即，获得了 Android 设备的 Root 权限，或破解了 iPhone 手机），因为这些可能潜藏着木马，从而访问和传播用其他方式加密的数据并发送给远程攻击者。

为了实现第一步，需要将你的注册过程同公司的目录、现有身份认证登录，以及使用群组隶属关系等整合起来，从而确定业务的需求和风险。第二步，你需要配置安全的移动应用程序，如 Good for Enterprise 和 NitroDesk TouchDown，或者替换门户网站和远程桌面访问，这些措施可以用来减少某些员工的设备存储，他们其实并不需要对业务数据进行离线或分离访问。

5. 移动活动监测和审计

请注意，不断的监测对这些最优做法而言是很重要的，单单配置一个员工设备就希望业务数据可以长期安全是不现实的。即使 IT 可能不会选择或拥有员工移动设备，公司仍然需要监测和审计业务数据和活动，以确保它们在整个生命周期内都一直符合规定。然而，这必须通过无线方式来实现，从而不会对个人使用产生干扰。

从监测未经 IT 允许而用于商业场合的员工设备的工作环境开始，网络访问控制、设备指纹识别工具和无线/有线网络 IPS 等操作，都是帮助 IT 部门发现移动设备或平板电脑的理想工具。这些工具的有些监测机制甚至可以防止未知设备接入企业。

其次，记录包含已注册移动设备的每一个商业系统的交互操作，包括电子邮件/联系方式/日历的同步、网络会议、虚拟专用网（VPN）连接、在线配置更新和 MDM 应用程序安装。这些记录对日常报告和审计来说是很重要的，因此应该在设备被擦除或取消注册后长期保留。理想情况下，设备应该以某种可以防止被诈骗或克隆的方式来进行身份识别，比如说设备可以使用 SCEP 来进行授权。

最后，为每个注册的员工设备定期执行符合规定的检查。至少应该在正常交互操作中进行检查（例如，在每次

进行电子邮件同步时，使用 EAS 来验证设置）。不过，MDM 产品通常提供了更加丰富的移动设备审计和报告功能，比如在某些情况下所进行的预定和按需设备的设置检索以及 IT 指定策略的自动对比等操作。

通过实施这五项基本移动设备数据保护最优措施，许多公司都可以接纳个人移动设备的商业化使用趋势。公司需要把注意力集中在业务数据上，并且制定出所需的最低控制，从而保障这些数据的安全。例如，很少有用户会同意白名单措施，这样会阻止他们安装个人应用程序；然而，许多用户会接受，甚至欢迎——对被盗的个人设备进行擦除的 IT 帮助。为了实现接受度最大化并避开陷阱，你需要确定一个测试组，并按照安全策略和控制对它进行初始设置，还要在公司全范围推广之前进行任何有必要的改进。

来源：51CTO