安全威胁每周警讯

2012/11/25～2012/12/01

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

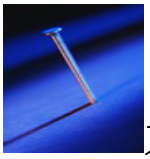
排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	WORM_DOWNAD.AD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
2	X97M_OLEMAL.A	宏病毒	★★	↓	宏病毒,它会将本身的下列副本放置到受影响的系统：%User Profile%\Application Data\Microsoft\Excel\XLSTART\k4.xls
3	WORM_DOWNAD	蠕虫	★★★★	↑	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，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
4	TROJ_DOWNAD.INF	木马	★★★	↓	DOWNAD 关联木马
5	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
6	X97M_LAROUX.BK	宏病毒	★★	↑	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
7	WORM_ECODE.E-N	蠕虫	★★★★	↑	E 语言蠕虫,会在文件夹下建立同名 exe 文件
8	X97M_LAROUX.CO	宏病毒	★★	→	宏病毒，主要通过用户浏览恶意网站感染，该病毒主要感染 Office Excel 文件，并且会在 Excel 中创建一个名为 StartUp 的宏脚本
9	Adware_Adplus 16	灰色软件	★★	→	广告程序,它可能是用户在访问恶意网站时在无意中下载而来。
10	PAK_Generic.001	加壳文件	★★	→	经过加壳技术加密的文件

 系统漏洞信息

MS12-072 ： Windows Shell 中的漏洞可能允许远程执行代码 (2727528)

Windows XP
Windows Vista
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2
Windows 7
Windows 8
Windows Server 2012

描述：http://technet.microsoft.com/zh-cn/security/bulletin/MS12-072



系统安全技巧

当前阵子一百万笔 Apple UDID 被黑客激进份子窃取的消息传出后，用户惊慌失措：什么是 UDID？个人识别身份信息要怎么经由 UDID 泄漏？该如何保护我的个人标识信息？

什么是 UDID?

UDID 本身只是一段冗长的字符串，是所有 iPhone、iPad 和 iPod Touch 的唯一序号，由长长一串数字和字母组成。因此它对黑客来说几乎是无用的，也不会影响到用户的隐私或安全。直到最近，该技术使得开发者可以在未经用户许可下自由收集，使得开发者和合作广告网络可以追踪安装应用程序的群体，并对使用情况加以监控，提供针对性广告或提升用户体验。

个人标识信息要如何跟 UDID 连接?

在收集 UDID 时，很多苹果开发者会将匿名 UDID 字符串代码储存在数据库中，还加上了开发者同样从应用程序中获取的设备所有者的个人标识信息。这也是为何应用程序开发者 - BlueToad 可以建立一个庞大的 UDID 和个人资料（如用户姓名、个人邮件地址和电话号码）数据库，甚至原本被黑客错误地认为是来自「FBI 外泄」的资料。一旦结合这些额外的个人信息，UDID 就可以为网络犯罪份子提供一个宝库，用于进行个人诈欺、网络诈骗等活动，或用来帮忙破解其他更有价值的用户账号。

我该如何在这类型风险下保护自己？

坏消息是，没有办法知道谁访问过你的 UDID，也没有办法防止它落入坏人之手。在这由 iOS 开发者、发行商、广告网络和其他第三方团体所组成的 Apple 复杂生态环境中，你的 UDID 可能已经被分享给太多外部团体了，特别是如果你喜欢玩应用程序的话。这件事本身并没有太大问题，真正的问题是开发者所建立的数据库会将这个产品的唯一标识符和你的个人资料绑定到一起。你可以在出现警告时试着限制授权给开发者的信息，安装应用程序前先读一读那几行小字，仔细检查每个应用程序所要求的权限。但是，在很多状况下，信息已经存在那里了，如果黑客知道要去哪找，最终就是会落入坏人之手。

好消息是，Apple 严格的应用程序商店审核小组已经开始拒绝新的应用程序要求访问 UDID，而且的新 iOS 6 操作系统也会用一套新的 API 来取代 UDID，这也是 Apple 朝向完全不使用这组数字的不久将来所踏出的第一步。

对于那些已经受到影响或是关心 UDID 使用的人，主要问题是 UDID 依然存在，这个庞大数据库的信息还握在第三方开发者手上。就这一点而言，唯一可以让你变换代码并且重新开始的方法只有买支新手机，然后在选择要分享哪些信息给应用程序时更加小心。

@原文出处：UDID Primer: Breaking down Apple’s leaky situation

保护智能手机安全，放心移动生活，Android 用户立即免费下载趋势科技移动安全个人版软件！
http://cn.trendmicro.com/cn/home/home-user/mobile-security-for-android/

趋势科技 PC-cillin 2012 采用最新云端截毒扫描功能，给电脑最放心的防护和安全，即刻免费下载
http://www.trendmicro.com.cn/pccillin/index.html

来源：趋势科技博客

特定用途适用性以及不受侵害的暗示保证。用户对此邮件列表的准确性和使用承担全部风险，因依赖该资料所致的任何损失，趋势科技均不负责。