Love Security Group 2011年第一季度安全综述

吾爱破解论坛
[LCG]
[LSG]

立足软件安全和病毒分析最前端，丰富的技术版块交相辉映，由无数加密解密及反病毒爱好者共同维护，留给世界一抹值得百年回眸的惊艳，沉淀百年来计算机应用之精华与优雅，信息线条与生活质感淡定交融，任岁月流转，低调而奢华的技术交流与研究却是亘古不变。

1. 微软禁用 Autorun 功能。

Microsoft 宣布推出自动运行功能的更新，帮助在 Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 的受支持版本上将自动播放功能仅限于 CD 和 DVD 媒体。将自动播放功能仅限于 CD 和 DVD 媒体有助于保护客户，防止在插入 USB 闪存驱动器、网络共享或其他在文件系统中包含 Autorun.inf 文件的非 CD 和非 DVD 媒体时因自动运行而导致任意代码执行的攻击媒介。 ——摘自微软安全通报

KB971029的发布有效阻止了病毒通过移动介质的传播，使一种病毒传播方式成为历史。需要注意的是，这并不代表这移动介质的绝对安全。在打开文件之前使用杀毒软件扫描仍然是必要的。

2. Bootkit 的持续流行。

Bootkit 并不是一个新名词，在2005年已经出现，只不过最近颇受关注。从当时的鬼影到现在的 TDSS，已经愈加完善。Bootkit 的防范要重于后期处理。一旦 MBR 被改写，病毒可以先于杀毒软件加载，给查杀带来困难。在 Bootkit 的处理上，可以使用 WinHex 或 Sector Editor 查看 MBR。若发现异常，可以使用 BOOTICE 进行修复。卡巴的专杀工具 TDSSKiller 可以方便地处理。综上所述，Bootkit 的处理十分麻烦，有些品牌电脑的引导扇区还有别的内容，所以自行处理的难度较大，需要对此保持警惕。

3. 支付宝木马。

网银的偷盗价值快被榨干了，人们又转到支付宝上来。对于只有简单安全措施的支付宝账户来说，只要得到支付宝密码，就可以进行各种操作。这种情况下，可以通过保护 IE 进程的办法来防护，一些安全软件已经可以做到这点。所以在将来的一段时间内，只要做好个人电脑和支付宝账户防护措施，支付宝木马是没有立足之地的。

4. WEB 安全趋势。

随着各类防挂马软件的出现，网页挂马成功的几率越来越低。钓鱼网站的风头仍然不减。究其原因，网页挂马可以通过技术手段得以阻止，但对钓鱼网站的识别目前还没有成熟的手段，只能局限于发现后加库，而不能提前处理。对用户而言，钓鱼网站的识别是非常轻松的——注意网站的域名。一些浏览器，如 IE、Chrome 对 URL 的网站域名部分进行了高亮，可以达到有效的提醒作用。

5. 三星笔记本电脑中的“Starlogger”。

众所周知，Starlogger 是一种键盘记录器，被预装在三星的产品中实在匪夷所思。MohammedÂ Hassan 发现后随即将此事公之于众，但在之后的调查中发现这是一次误报。