2013年8月计算机病毒疫情分析

李冬，杜振华
（国家计算机病毒应急处理中心，天津 300457）

1 计算机病毒总体情况

2013年8月，国家计算机病毒应急处理中心共发现病毒528573个，比上月下降5.2%，新增病毒118275个，比上月上升4.2%，感染计算机31758324台，比上月下降1.0%，主要传播途径仍以“网络钓鱼”和“网页挂马”为主。

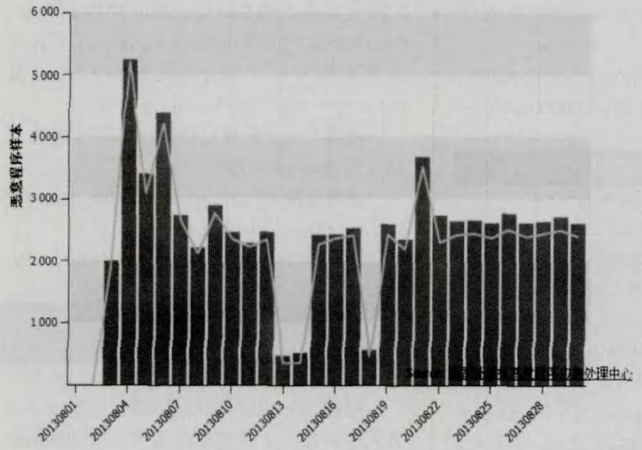

图1 8月份我国新增计算机病毒态势

恶意程序样本数据

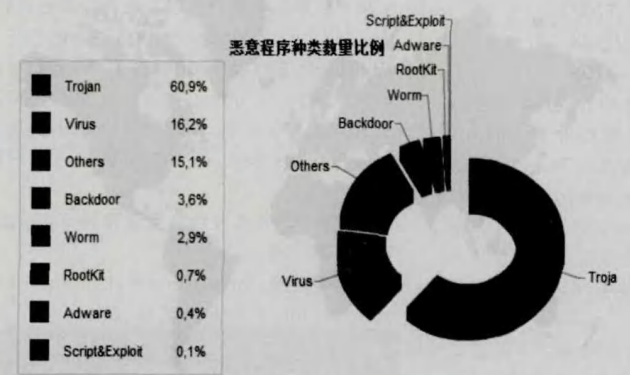

图2 8月份我国新增计算机病毒分类

2 计算机病毒动态

1）8月互联网上出现一种新型蠕虫Worm_TaopuLS.B。该蠕虫通过移动存储介质传播，运行后在受感染操作系统指定目录下新建一个文件夹，并将其自身复制到该文件夹中。同时，该蠕虫将修改受感染操作系统中注册表的相关键值项，迫使系统主动连接恶意攻击者指定的网页。除此之外，该蠕虫能够隐藏受感染操作系统中所有PDF、XLS和PPT等文件，篡改计算机用户系统中的Word文档，向恶意攻击者指定的网站发送大量垃圾数据，导致计算机网络出现拥堵，操作系统运行缓慢。

2）8月互联网上出现一种新型恶意木马程序变种Trojan_Generic.BD。该变种运行后，会将自身复制到受感染操作系统指定目录下，获取其系统权限，接受恶意攻击者远程指令。恶意攻击者会利用计算机用户操作系统对其指定网络地址进行网络攻击，最终导致网络运行速度缓慢甚至瘫痪。另外，该变种会迫使受感染操作系统在后台主动连接恶意攻击者指定的服务器，上传受感染操作系统本机信息，接受恶意攻击者远程指令，最终盗取受感染操作系统中的隐私信息数据、网银账号和密码等敏感信息。

3）8月互联网上出现一种新型恶意后门程序变种Backdoor.Idr.A。该变种伪装成图片图标，诱使计算机用户点击运行。该变种运行后，自身会释放一张图片迷惑计算机用户，同时还将释放一个动态链接库文件，并且对其进行加载和解密。一旦动态链接库文件被解密，受感染操作系统就会主动连接恶意攻击者指定的服务器，接收并执行其发送的远程恶意指令。

4）8月互联网上出现一种新型恶意后门程序变种Trojan_MyDown.CMG。该变种运行后，会尝试终止受感染操作系统中防病毒软件和防火墙的进程，篡改受感染操作系统注册表中的相关键值项，实现随系统开机而自启动，并使操作系统无法正常进入安全模式。另外，受感染操作系统在后台会主动连接恶意攻击者指定的多个服务器，下载其他木马、病毒等恶意程序，盗取受感染操作系统中的隐私信息数据、网银账号和密码等敏感信息。（责编 程斌）