中国地区 2011 年
第三季度
网络安全威胁报告

2011/10

目录

2011 年第 3 季度安全威胁

本季安全警示：

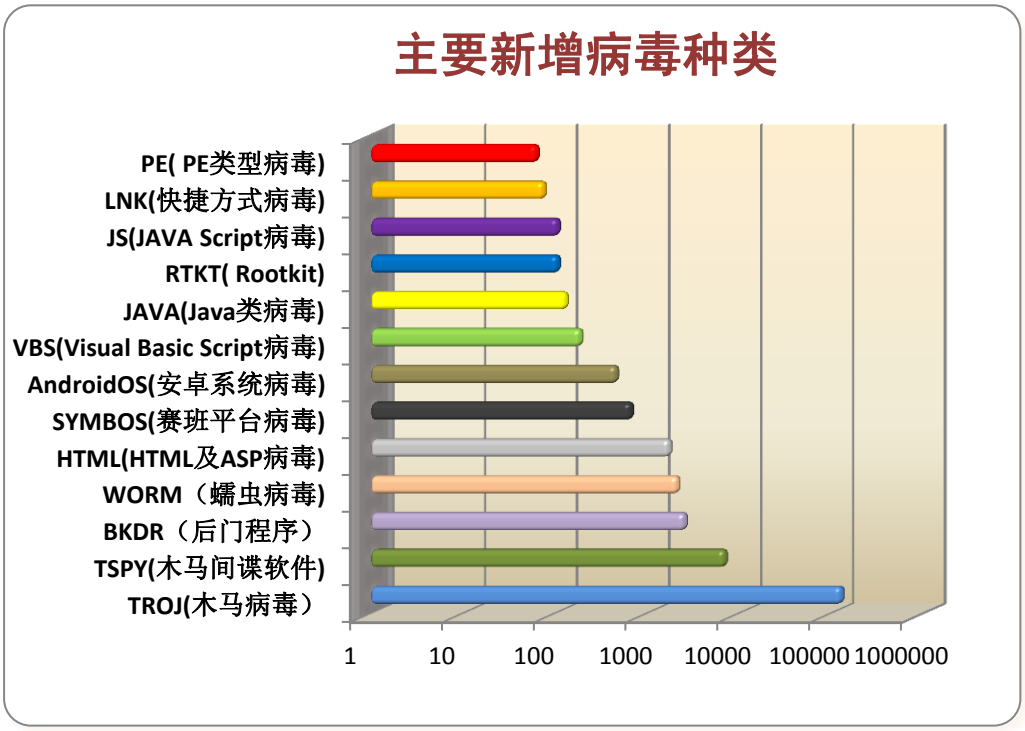
PE 病毒,漏洞, MBR 感染型病毒

2011 年第 3 季度流行病毒概况

- 本季度趋势科技在中国地区发现新的未知病毒约 **15** 万种。截止 2011.9.30 日中国区传统病毒码 8.462.60 可检测病毒数约 350 万种。

  新增的病毒类型最多的仍然为木马（TROJ），木马大部分有盗号的特性。木马的比其他类型的电脑病毒更容易编写且更容易使病毒制造者获益。在经济利益的促使下，更多病毒制作者开始制造木马病毒。

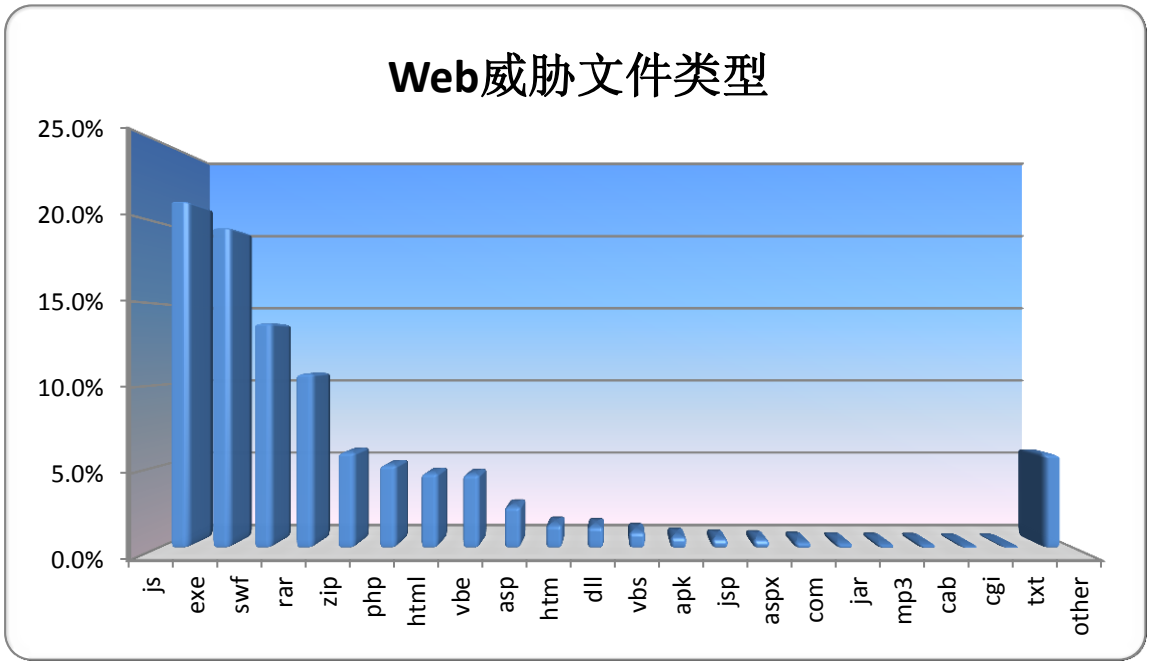
  我们看到本季度新增病毒种类中 RTKT 也进入了前十名中。RTKT 为 rootkit,其主要功能为：隐藏其他程序进程的软件. 可能是一个或一个以上的软件组合。我们怀疑此类病毒的增加，可能与 TDL3/TDL4 的流行有关。



2011 第 3 季度中国地区新增病毒类型

- 本季度趋势科技在中国地区拦截到新的恶意 URL 地址以及相关恶意文件约 **10.2** 万个。比上季度有所减少（上季度为 14.1 万）。

  其中通过 Web 传播的恶意程序中，约有 **21.4%**为 JS（脚本类型文件）。向网站页面代码中插入包含有恶意代码的脚本仍然是黑客或恶意网络行为者的主要手段。这些脚本将导致被感染的用户连接到其它恶意网站并下载其他恶意程序，或者 IE 浏览器主页被修改等。一般情况下这些脚本利用各种漏洞（IE 漏洞，或其他应用程序漏洞，系统漏洞）以及使用者不良的上网习惯而得以流行。



2011 第 3 季度中国地区 web 威胁文件类型

通过对拦截的 Web 威胁进行分析，我们发现。约有 78.5%的威胁来自于 General exploit (针对漏洞的通用检测)。

其中包括利用 Adobe 软件的漏洞（例如：一些.SWF 类型的 web 威胁文件)。利用跨站脚本漏洞攻击，对正常网站注入恶意 JS 脚本，或插入恶意 php，html 代码。

另外一些带有病毒文件的链接也会被加载到某些网站中，一旦访问了这些网站即会重定向到病毒链接下载并执行病毒。

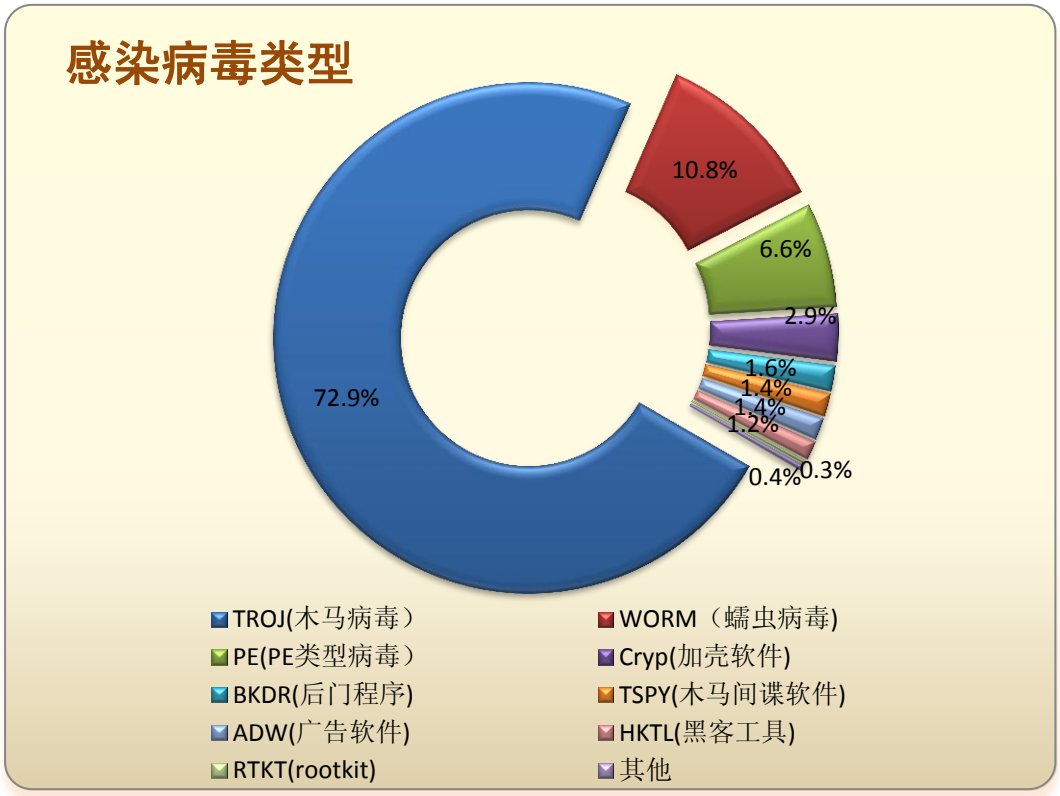
通过 Web 传播的病毒	
病毒名称	百分比
General Exploit	78.5%
Mal_Hifrm	0.7%
TROJ_SPNR.03CG11	0.6%
TROJ_SPNR.03CL11	0.5%
JS_REDIR.SME	0.5%
TROJ_SMALL.SMOK	0.4%
HTML_REDIR.AA	0.4%
TROJ_SPNR.03G611	0.4%
TROJ_GEN.USE0OFF	0.4%
TSPY_KYMBER.SMDV	0.4%
Mal_Opet-3	0.3%
TROJ_DROPPER.ESZ	0.3%
TROJ_PACKED.DVN	0.3%
HTML_JADTRE.Y	0.3%
TROJ_GEN.USE01GF	0.3%
TROJ_LAMEWAR.VTG	0.2%
HTML_DOWN.A	0.2%
TROJ_NOPCK.SMUD9	0.2%
WORM_RIPLIP.SMI	0.2%
OTHER	14.9%

2011 第 3 季度中国地区前 20 名通过 web 感染的病毒

以下网站中也发现有漏洞或恶意代码，这些可能和政府网站被挂马有关：

hxxp://a.dnpk.net:82/dt.asp?www.rzjs.gov.cn
hxxp://a.dnpk.net:82/hx.asp?jcx.pljc.gov.cn
hxxp://bm.wuyishan.gov.cn:80/count/count.js
hxxp://a.dnpk.net:82/sg.asp?www.hx.gov.cn
hxxp://a.dnpk.net:82/dt.asp?www.funing.gov.cn
hxxp://a.dnpk.net:82/dt.asp?www.hnhhsw.gov.cn
hxxp://immigration.gov.ph:80/administrator/components/com_media/old/atualizar.exe
hxxp://www.hdcentenario.gov.co:80/~lazzoz/paypal/us/webscr.php?cmd=_login-run

- 本季度趋势科技在中国地区客户终端检测并清除恶意程序约 **4021** 万次。



2011 第 2 季度中国地区各类型病毒感染数量比例图

本季度木马病毒数量及所占比例大幅上升，蠕虫病毒以及 PE 感染类型病毒比例也稍有下降所占比例分别为 10.8%与 6.6%。

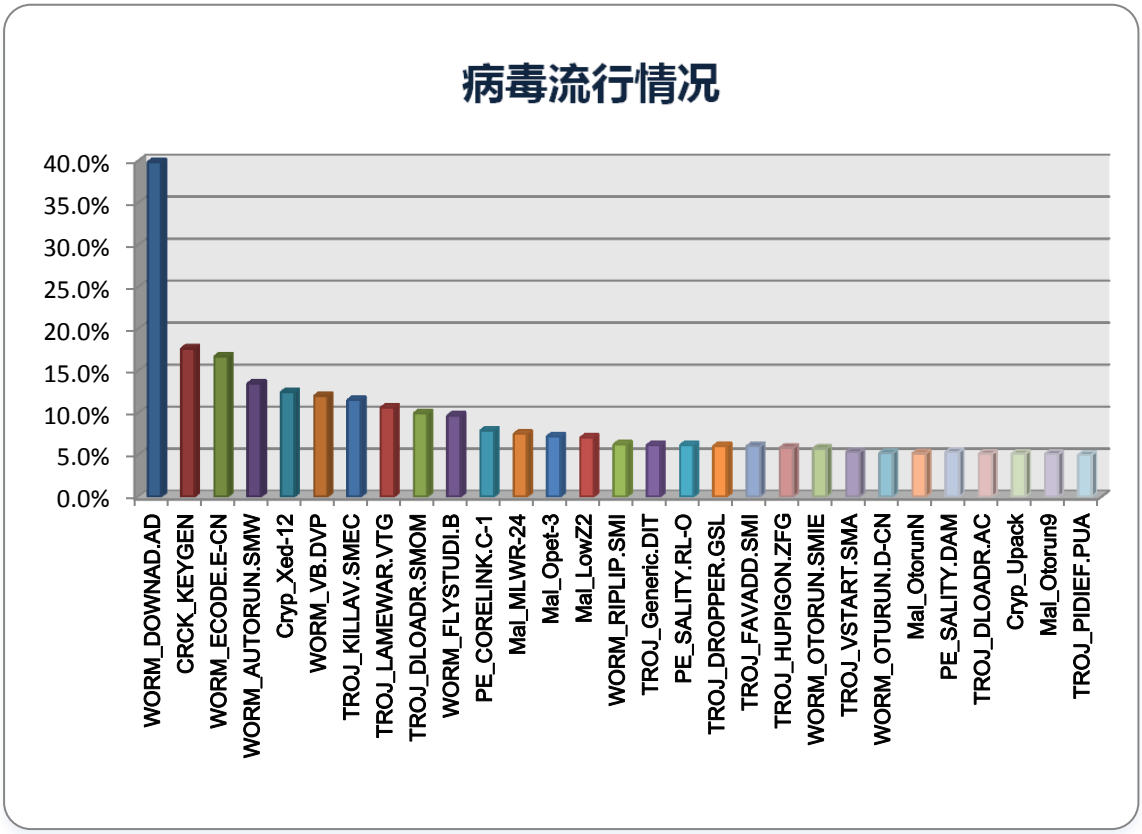
蠕虫病毒最主要的特性是能够主动地通过网络，电子邮件，以及可移动存储设备将自身传播到其它计算机中。与一般病毒不同，蠕虫不需要将其自身附着到宿主程序，即可进行自身的复制

目前比较流行的 PE 病毒，会感染一些蠕虫或者木马病毒。随着木马病毒以及蠕虫病毒在网络内的传播导致网络环境中越来越多的电脑被 PE 病毒感染。

RTKT 类型病毒是近几个季度以来首次进入病毒感染类型排名中。可见近期该类型病毒急速增加。rootkit 真正目的是在于隐藏其他进程，注册表以及程序。使用了 rootkit 技术的病毒往往非常难以清理。

我们有理由怀疑 RTKT 类型病毒的增加与 TDL3/TDL4 的流行有关，而这类病毒也有可能导致了最近一段时间 MBR 感染类型病毒的增加。

2011 年第 3 季度流行病毒分析



2011 第 3 季度中国地区病毒流行度排名

- 本季度最流行病毒依旧是 WORM_DOWNAD.AD,该病毒目前仍然在很多企业用户网络内流行。
  相对于上一个季度 WORM_DOWNAD.AD 病毒的流行程度不但没有降低，反而有了小小的上升。这是出乎我们意料之外的。

  在这里仍然需要提醒用户，该病毒持续流行的原因有几点：

  1. 用户内网中电脑系统补丁安装率较低
  2. 网络中存在弱密码的或空密码的电脑管理员账号
  3. 网络内存在有未安装防毒软件，或防毒软件已损坏的感染源电脑
  4. 没有针对 U 盘等移动存储设备的安全管理策略

由于目前尚未发现关于该病毒的新变种，使用之前发布的专杀工具以及解决方案即可处理此病毒

- 本季度流行病毒中 PE_SALITY 家族病毒排名上升，趋势科技病毒实验室也接到多起关于该病毒的案件。

这只病毒的感染方式从 2003 年出现以来并没有什么很大的改变。这是一个混合型病毒。具有多种病毒的行为特征。会终止安全相关软件和服务，感染 EXE 和 SCR 文件，下载其他病毒文件进入系统。它创建自身拷贝到可移动设备或者网络共享中，以达到传播的目的。

感染了该病毒的主要特征为：

AMSINT 服务被安装.
打开注册表编辑器（开始-运行 输入 regedit），检查是否有以下内容:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\amsint32
ImagePath='\??\%System%\drivers\{随机文件名}.sys'

系统无法进入安全模式.
病毒会修改以下注册表键值来禁用安全模式：
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Safeboot

共享文件夹及其子文件夹下存在 LNK 和 TMP 文件
最新的 PE_SALITY 变种会利用最新的 Windows 快捷方式漏洞。

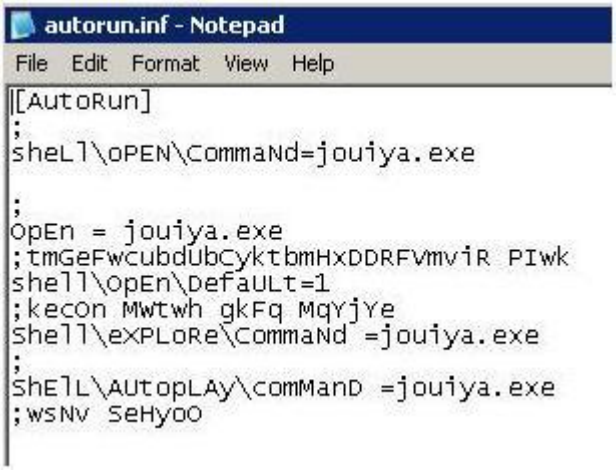
另外一种可能感染此病毒的特征为在网络共享中存在恶意的 LNK 和 TMP 文件:

存在恶意的 AUTORUN.INF

PE_SALITY 将创建一个病毒母体文件的拷贝和自动执行该母体文件的 AUTORUN.INF 至所有驱动器.

当你进入被感染驱动器后，就会自动执行病毒。

这个恶意的 AUTORUN.INF 包含以下内容:



禁用 Windows 安全程序和防火墙

该恶意软件也禁用安全相关的程序，以及 Windows Security 和防火墙. 除此之外，它也创建以下注册表键值来禁用 Windows Security 和防火墙。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center
AntiVirusDisableNotify=1
AntiVirusOverride=1
FirewallDisableNotify=1
FirewallOverride=1
UacDisableNotify=1
UpdatesDisableNotify=1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
EnableLUA=0

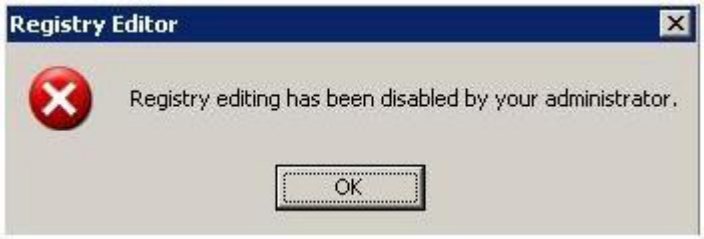
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
EnableFirewall=0
DoNotAllowExceptions=0
DisableNotifications=1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
{病毒路径以及文件名称}='{病毒路径以及文件名称}:*:Enabled:ipsec'

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
GlobalUserOffline = dword:00000000

禁用任务管理器和注册表编辑器

和其他的病毒相似，PE_SALITY 也会禁用任务管理器和注册表编辑器。当用户打算打开以上应用程序，将会出现以下错误信息：



该病毒的主要传播途径以及预防措施：

1.Windows 快捷方式缺陷

微软已经发布了一个补丁来解决这个问题。
http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx
因此我们建议保持最新补丁级别。
关于此威胁的一个变通方案就是禁用显示图标。

2.可移动存储设备

趋势科技检测 Autorun.inf 为 Mal_Otorun1。以防止执行引用的文件，配置产品，执行在插入新设备后执行扫描。

3.被感染的文件

被感染的文件已经被趋势科技检测为 PE_SALITY.RL.
请更新最新的病毒码，以保证被感染文件能够及时被检测以及清除:
http://www.trendmicro.com/download/pattern.asp

4.网络(驱动器,共享,P2P,IM)

使用 TDA/NVW 并且下载最新病毒码文件。
当一台计算机有威胁,将它从网络隔离。
确保用户和程序使用最低权限来完成任务。

5.从 Internet 下载

阻止相关恶意 URL。
使用防火墙来监视源于 Internet 的入站连接。

避免访问不受信任的站点。

6. 电子邮件

避免打开不知情的附件。

.配置你的电子邮件服务器阻止或清除类似 vbs,bat,exe,pif,scr 格式的文件。

另外，趋势科技病毒实验室提供以下专杀工具以清理该病毒：

http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-PE_SALITY.zip

2011 年第 3 季度最新安全威胁信息

2011 年 8 月，中国地区发现新的蠕虫病毒

趋势科技在中国地区发现一种新的蠕虫病毒 WORM_MORTO.SMA,该病毒利用远程桌面协议（RDP）传播
被该病毒感染的电脑会用一种非常特别的方式进行拒绝服务攻击(DOS)。
并且被感染电脑将被恶意控制，成为肉鸡。
当该病毒被加载后，他会将其自身的恶意代码加密保存于注册表 HKEY_LOCAL_MACHINE\SYSTEM\WPA 中。并删除其母体文件。使得其很难被发现

http://about-threats.trendmicro.com/Malware.aspx?language=cn&name=WORM_MORTO.SMA

2011 年 9 月， 恶意软件 SpyEye 可盗取短信验证码

有银行客户在使用互联网银行服务时，发现有恶意软件盗取他们的个人资料，并尝试进行转账。据了解，目前并没有任何人因此蒙受财务损失。新加坡银行公会昨天发布文告，表示有些网上银行用户的电脑，被一个叫做“SpyEye”的恶意软件(malware)所感染。这相信是银行公会多年来，首次公开提醒银行客户要慎防恶意软件入侵。

用户一旦使用受 SpyEye 感染的电脑来登录银行网站，页面就会出现指示，要用户耐心等候，因为网站需要 1 至 10 分钟来“检查用户的安全设置”。SpyEye 此时就开始暗中操作，盗取用户的网上银行服务资料。

这是 SpyEye 最明显的特征。银行公会表示，银行网站在正常情况下，不会要求用户等上那么久的时间，“这表示恶意软件在盗取用户的资料。”

银行公会是个非盈利组织，代表银行业在新加坡的利益，属下有 117 个本土和海外银行成员。

http://blog.trendmicro.com/soldier-spyeyes-a-jackpot/

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC)