中国地区 2012 年
第二季度
网络安全威胁报告

2012/07

目录

2012 年第 2 季度安全威胁

本季安全警示：

宏病毒，PE 病毒，漏洞 ，钓鱼

2012 年第 2 季度安全威胁概况

- 本季度趋势科技中国区病毒码新增特征约 59 万条。截止 2012.6.30 日中国区传统病毒码 9.224.60 包含病毒特征数约 400 万条。
- 本季度趋势科技在中国地区客户终端检测并拦截恶意程序约 **8420** 万次。
- 本季度趋势科技在中国地区发现并拦截新的恶意 URL 地址约 **33** 万个。

2012 年第 2 季度中国地区，木马病毒仍然占据新增病毒数量排名首位。木马大部分有盗号的特性，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。在经济利益的驱使下，更多病毒制作者开始制造木马病毒。

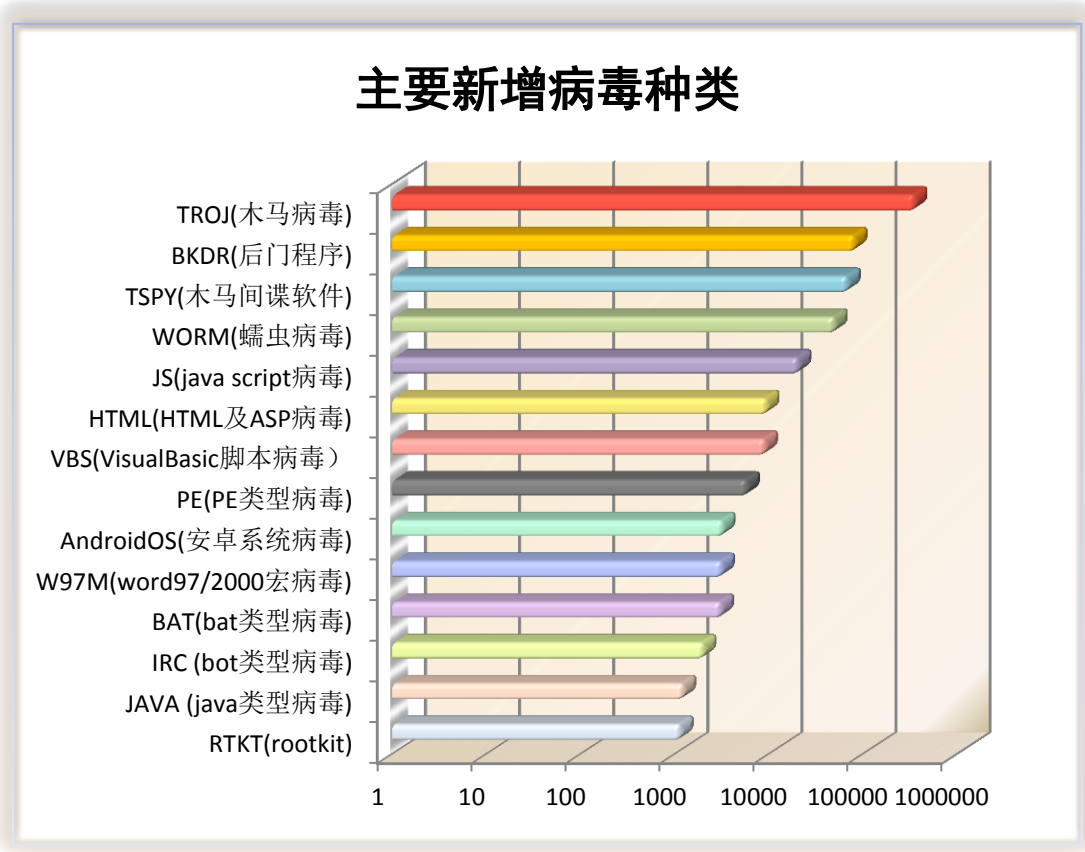
宏病毒在本季度趋于爆发。在上季度我们报告了一种新型的宏病毒，这种宏病毒除了能够通过感染 Excel 文件传播外，还会主动通过 Outlook，将打开的被感染文件通过附件形式发送给其他收件人。这种宏病毒本季度在很多用户环境中都开始被发现。该宏病毒除了能够更广泛的传播外，还可能会导致 Excel 文件的内容泄漏。需要引起高度重视

有 2 种 PE 病毒 PE_PARITE.A，PE_SALITY.RL 在本季度病毒拦截次数排名中仍然保持上升趋势，并在一些企业用户环境中大面积暴发。这两种病毒除了通过感染文件，共享目录，U 盘传播之外还可能通过电子邮件传入。

在 2012 年第 2 季度趋势科技拦截新的恶意网站中钓鱼网站约有 7000 个(以域名计数)。China RTL 接到数起网银诈骗案件，这些案件均与钓鱼网站有关。在网上购物或访问银行网站时须仔细核对网站域名，并且保持警惕，发现有问题立刻断开网络中止付款。

2012 年第 2 季度病毒威胁情况

2012 年第 2 季度新增病毒类型分析



2012 第 2 季度中国地区新增病毒类型

新增的病毒类型最多的仍然为木马（TROJ），本季度新增木马病毒特征 335161 个，大约占新增病毒数量的 57% 。木马可使病毒制造者更直接的获利，在经济利益的驱使下大量的木马被制造并通过各方式被入互联网中。木马也是我国目前存在数量最多的病毒类型。

2012 第 2 季度新增病毒种类中，AndroidOS(安卓系统病毒)排名又有上升，新增的安卓系统病毒特征数量为 3044 个，较之于上季度又增加 10%。安卓作为手机平台的操作系统，由于它的开源特性得到了众多设备厂商以及软件开发者的青睐，也成就了它的迅速崛起。然而，在安卓系统风光的背后，也隐藏了种种无奈-- 基于该平台的病毒伴随而来。虽然在已发布的安卓 4.0 中引入了 ASLR 技术以及对用户凭据安全进行了加固，但是我们认为这些安全加固，对于阻止吸费以及窃取信息类型的病毒的作用并不是特别

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) ,本报告中所有数据仅针对中国地区。

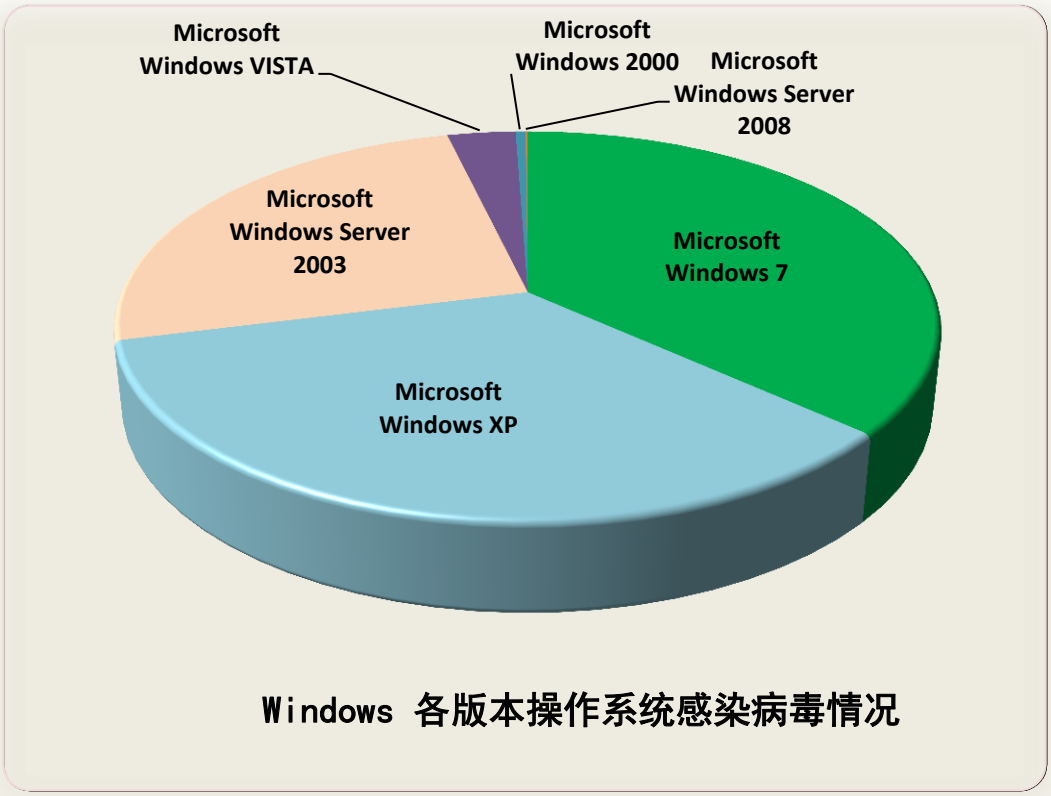
大。而吸费和窃取信息又正是目前手机病毒的主流。所以安卓平台上的病毒数量仍然会持续增长。手机系统的安全正在面临越来越艰巨的挑战。

W97M/X97M(word/Excel 宏病毒)在上一季度业进入了新增病毒数量排名的前几位。宏病毒的传播速度十分快，并且不容易被发现。这是一种比较老的病毒，但是最近这种有了些历史的病毒又被翻新，并且采用了新的技术，使这种病毒可以做更多的事情。Office 文件中往往保存了用户的重要数据和信息，宏病毒的增长也给数据安全带来了很大的挑战。

IRC 病毒(IRCBOT)也值得我们特别的关注。IRC（internet relay chat）是一款功能强大的即时聊天协议，IRCBOT 是一些运行在后台的恶意程序，通过登陆某一个频道，分析接受到的内容并做出相应的动作。

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) ,本报告中所有数据仅针对中国地区。

2012 年第 2 季度 windows 系统感染病毒情况分析



2012 第 2 季度中国地区

Windows 各版本操作系统感染病毒情况

在 2012 年第 2 季度，windows7 平台病毒感染数量已超过 windows xp 越居第一位。感染数量的增长可能和 windows7 系统的使用数量有所增长而 windows xp 用户数在减少也有很大的关系。但是 Windows7 系统不需要装杀毒软件的神话已经不在，Windows7 系统用户也许要密切注意自己的系统安全。

从病毒感染比例上看，安装了 sp1 补丁的 windows7 系统病毒检测比例明显少于未安装补丁的系统。趋势科技中国区病毒实验室提醒大家及时更新操作系统补丁，抵御最新的安全威胁。

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) ,本报告中所有数据仅针对中国地区。

Microsoft Windows 7	病毒检测次数
Windows 7 Home Basic	2956846
Windows 7 Home Premium Service Pack 1	1587802
Windows 7 Home Basic Service Pack 1	1021895
Windows 7 Ultimate	752311
Windows 7 Home Premium	680383
Windows 7 Ultimate Service Pack 1	665697
Windows 7 Ultimate Professional Service Pack 1	574827
Windows 7 Ultimate Server 4.0, Enterprise Edition Service Pack 1	442215
Windows 7 Professional Service Pack 1	254293
Windows 7 Ultimate Professional	221244
Windows NT 6.1.7601	100098
Windows 7 Professional	80196
Windows NT 6.1.7600	41537
Windows 7 Ultimate Home Edition Service Pack 1	40300
Windows 7 Ultimate Home Edition	21950
Windows 7 Enterprise Service Pack 1	21486
Windows 7 Ultimate Server 4.0 Service Pack 1	18931
Windows 7 Starter Service Pack 1	13928
Others	15733

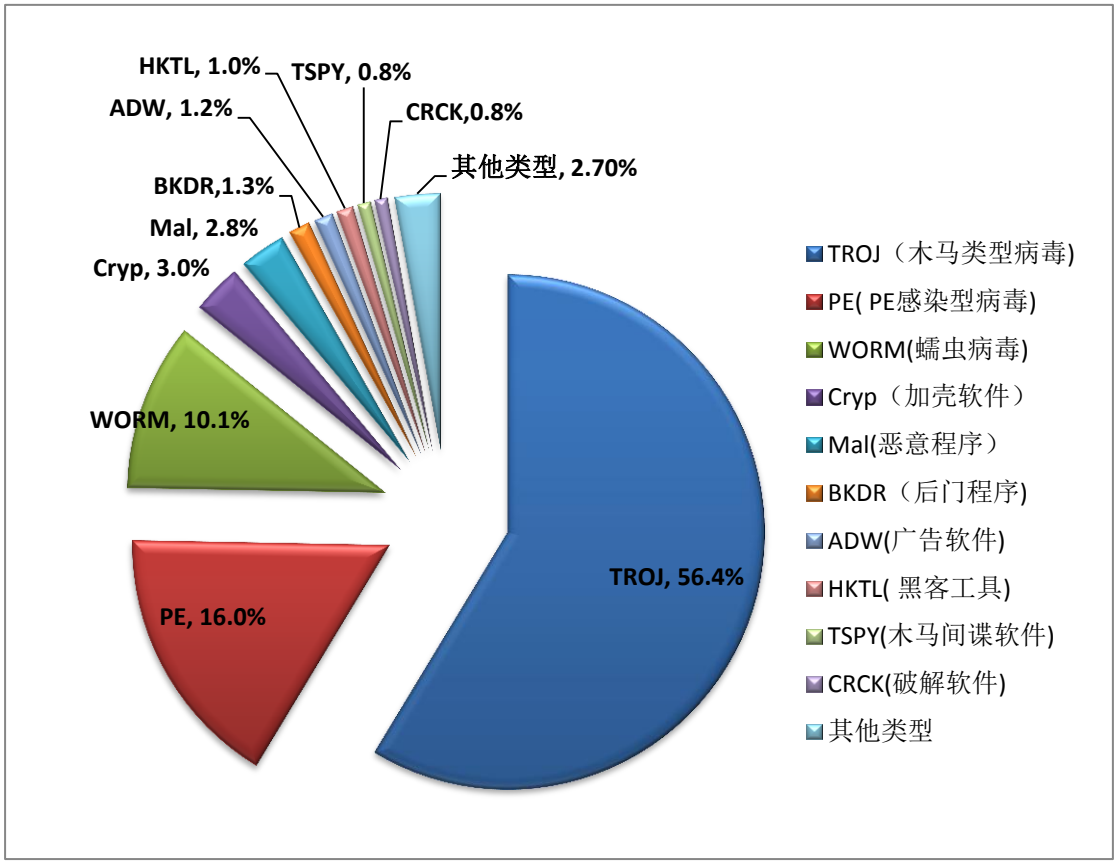
2012 第 2 季度中国地区

各版本 Windows7 操作系统感染病毒情况

另外，对于任何 64 位的 windows 操作系统感染病毒数量均极大的少于 32 位操作系统。这可能是因为目前大部分病毒都不兼容 64 位操作系统。

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) ,本报告中所有数据仅针对中国地区。

2012 年第 2 季度各类型病毒检测情况分析



2012 第 2 季度中国地区各类型病毒检测数量比例图

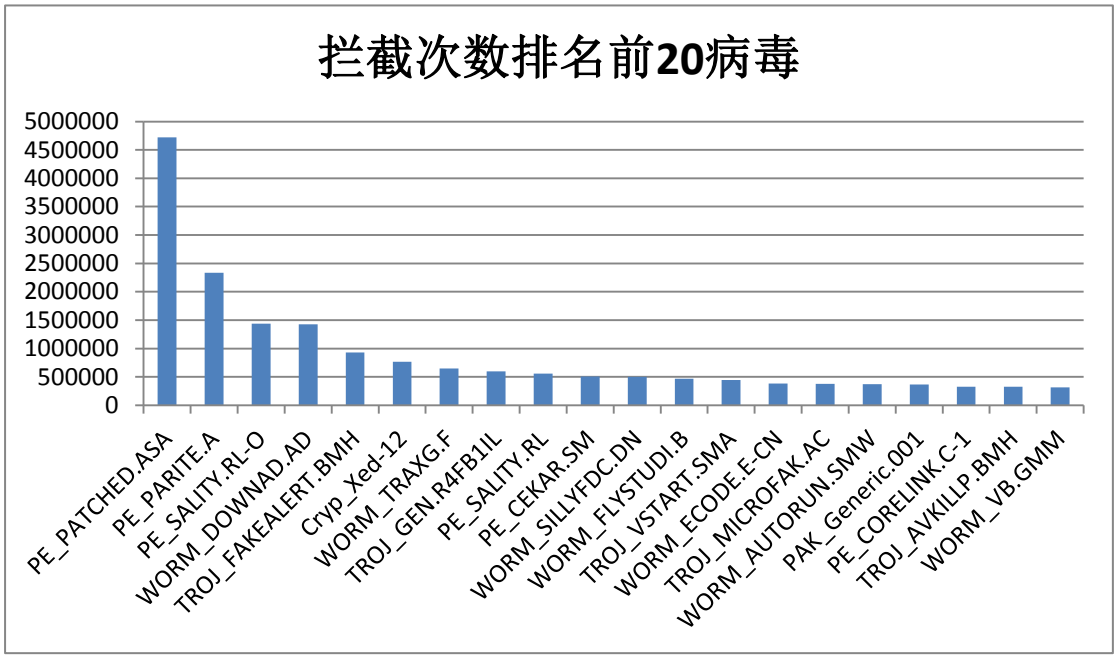
2012 年第 2 季度检测到的病毒种类中 PE 类型病毒感染仍然占有较大的比例。PE 病毒为感染型病毒，该类病毒的特征是将恶意代码插入正常的可执行文件中。

蠕虫病毒基本与上季度持平。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。第 2 季度感染比较多的蠕虫病毒仍然为 WORM_DOWNAD 以及文件夹病毒。另外某些 PE 病毒的母体也以蠕虫病毒的方式传播

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。

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) ,本报告中所有数据仅针对中国地区。

2012 年第 2 季度病毒拦截情况分析



2012 第 2 季度中国区拦截次数排名前 20 病毒

上图显示了 2012 年第 2 季度被拦截次数排名前 20 的病毒。被拦截次数多的病毒可能是感染文件数量较多的 PE 病毒，也可能是会反复感染难以清理的病毒。

2012 年第 2 季度被趋势拦截次数最多仍然的为 **PE_PATCHED.ASA**。该病毒被拦截次数约为 460 万次。远远超过其他病毒。跟上季度相比略有下降。

在上季度我们介绍过这只病毒，该病毒为被修改的 sfc_os.dll，sfc_os.dll 是用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能

由于该文件是系统文件，防毒软件强行查杀可能会导致系统崩溃。

对这只病毒目前的解决方法如下：

- 将被修改的文件复制到其他目录使用杀毒软件清除以后再替换回去。
- 使用干净的相同版本系统中的文件替换。
- China RTL 已针对此病毒制作专杀，如有此病毒问题请与趋势科技技术支持联络

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) ,本报告中所有数据仅针对中国地区。

PE_PARITE.A 和 **PE_SALITY.RL** 是两只比较难清理的 PE 病毒，我们在之前的季报中都有提到过。

PE_PARITE.A

该病毒通过已被感染过的文件以及共享文件夹传播。
由于该病毒能够通过共享文件夹传播并感染，所以防护该病毒的一个重要环节即对共享文件夹进行控制。

关于该病毒的详情以及解决方案请参考以下链接：
http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionId=72241&submit2=%CB%D1%CB%F7

PE_SALITY.RL

该病毒通过 U 盘，共享文件夹，以及系统漏洞传播，也有可能通过电子邮件进入系统
对于可能被感染的恶意软件,参考以下方法,来防止 PE_SALITY 进入你的系统:

a.Windows 快捷方式缺陷

1.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。

2.关于此威胁的变通方案就是禁用显示图标。

b.可移动存储

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。

c.被感染的文件

被感染的文件已经被趋势定义为 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

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) ,本报告中所有数据仅针对中国地区。

d. 网络(驱动器,共享,P2P,IM)

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

e. 从 Internet 下载

1. 阻止相关恶意 URL。
2. 使用防火墙来监视源于 Internet 的入站连接。
3. 避免访问不受信任的站点。

f. 电子邮件

1. 避免打开不知情的附件。

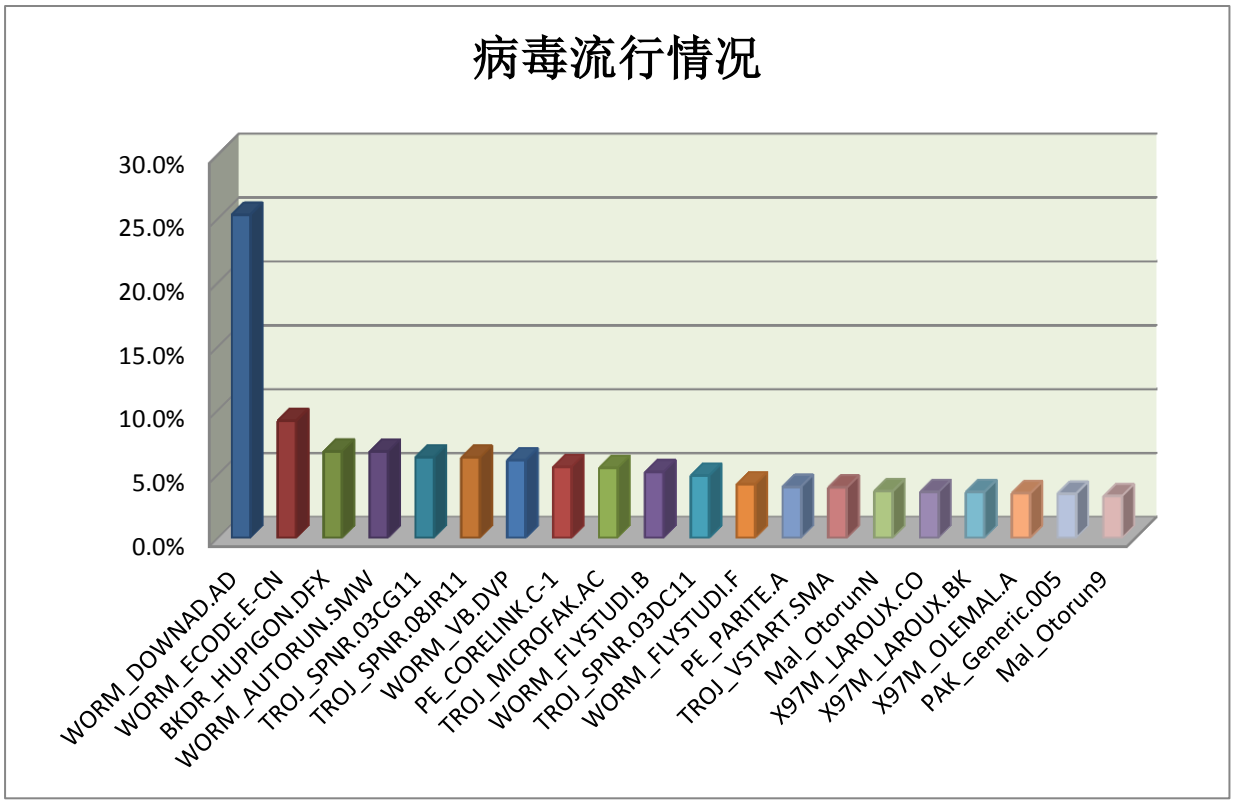
2. 配置你的电子邮件服务器阻止或清除类似 vbs,bat,exe,pif,scr 格式的文件。

关于该病毒的详情以及解决方案请参考以下链接:
http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionID=71063

http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionID=71048

可以看到，拦截次数较多的病毒多为 PE 病毒以及蠕虫病毒，由于这两种类型病毒的传播特性以及难以清除的特性，在感染这两种类型病毒时务必要加以重视，并及时联系趋势科技技术支持部门协助解决。

2012 年第 2 季度流行病毒分析



2012 第 1 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**。

不过相对于去年以及第一季度，该病毒的流行程度仍然处于下降,2011 第 4 季度时有 40%左右的用户正在或曾经遭受过 Worm_Downad 的攻击，第一季度度下降到了 27%左右。而本季度仅有 25%的客户环境中出现过此病毒，从数据显示该病毒已逐步得到控制。

在这里仍然需要提醒用户，Worm_Downad 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。

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) ,本报告中所有数据仅针对中国地区。

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。

流行程度排名第 2 的 **WORM_ECODE.E-CN**，是一种文件夹病毒，该病毒在前几季度一直处于比较靠前的位置。本季度更一跃到了流行程度排名第二。

该病毒要特性为将系统根目录中文件夹属性改为隐藏，并生成与文件夹同名的 exe 文件，欺骗用户运行病毒以达到全盘感染的目的。此病毒主要通过 U 盘传播，在局域网内也可能通过网络的映射磁盘传播。

文件夹病毒的变种极多，伴随有各种附加特性，例如导致任务管理器，注册表，组策略无法打开。被病毒修改的隐藏文件夹属性很难被修复

关于该病毒的详情以及解决方案请参考以下链接：

http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionId=72242&submit2=%CB%D1%CB%F7

X97M_OLEMAL.A 是在上季度末发现的新的 EXCEL 宏病毒，在本季度就进入了前 20 名的病毒流行病毒排名。
这种宏病毒不仅仅能感染 EXCEL 文件并且还会将感染系统中的 EXCEL 文件自动通过 OUTLOOK 发送

关于该病毒的技术细节如下：

感染途径：

该病毒主要通过邮件以及已被感染的 EXCEL 传播

行为特征：

该病毒会将自身复制并释放至以下目录中：

%User Profile%\Application Data\Microsoft\Excel\XLSTART\k4.xls
(%User Profile%为当前用户目录，它通常是 C:\Windows\Profiles\{用户名} 在 Windows 98 或 windows ME 系统中,或者是 C:\WINNT\Profiles\{用户名} 在 Windows NT 系统中，或者是 C:\Documents and Settings\{用户名} 在 Windows 2000, XP, 以及 Server 2003.系统中)

windows7 系统中这个目录通常在：

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) ,本报告中所有数据仅针对中国地区。

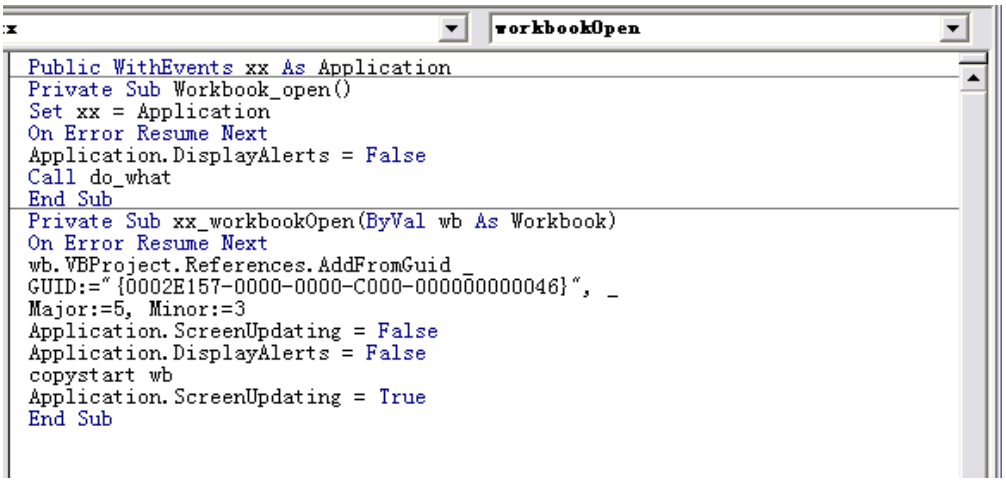
C:\Users\用户名\AppData\Roaming\Microsoft\Excel\XLSTART

这个病毒通常还会添加以下注册表键值：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Office\{Application Version}\Excel\
Security
AccessVBOM = "1"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Office\{Application Version}\Excel\
Security
Level = "1"

感染的文件，会被在 ThisWorkbook 下添加如下脚本。



感染的文件会被添加模块，模块中包含恶意代码。

另外，如果被感染的电脑中存在 E 盘，E 盘根目录中将生成名为 KK 的文件夹，文件夹中存放有以 EXCEL 文档名称命名的恶意 .VBS 脚本。

病毒防护与解决方法：

介于该病毒的传播以及感染方式，建议通过以下方法防护此病毒：

1. 将 EXCEL 宏安全等级调高。在接受到别人发送来的 EXCEL 文件时最好先将宏安全等级调到最高，如果需要使用宏，请在先用防毒软件扫描
2. OUTLOOK 安全等级调高，禁止其他应用程序使用 OUTLOOK 发送邮件

解决方法：

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) ,本报告中所有数据仅针对中国地区。

目前趋势科技最新中国区病毒码 9.244.60 及以上版本病毒码以可检测此文件，感染此病毒机器请对系统进行全盘扫描

未安装趋势科技产品用户可至以下站点下载 ATTK 工具扫描系统:

32 位 windows 操作系统请使用：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage.exe

64 位 windows 操作系统请使用：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage_64.exe

另外针对此宏病毒，趋势科技中国区病毒实验室已制作专杀工具，如有感染此病毒并无法处理的情况，请与趋势科技技术支持部门联络。

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) ,本报告中所有数据仅针对中国地区。

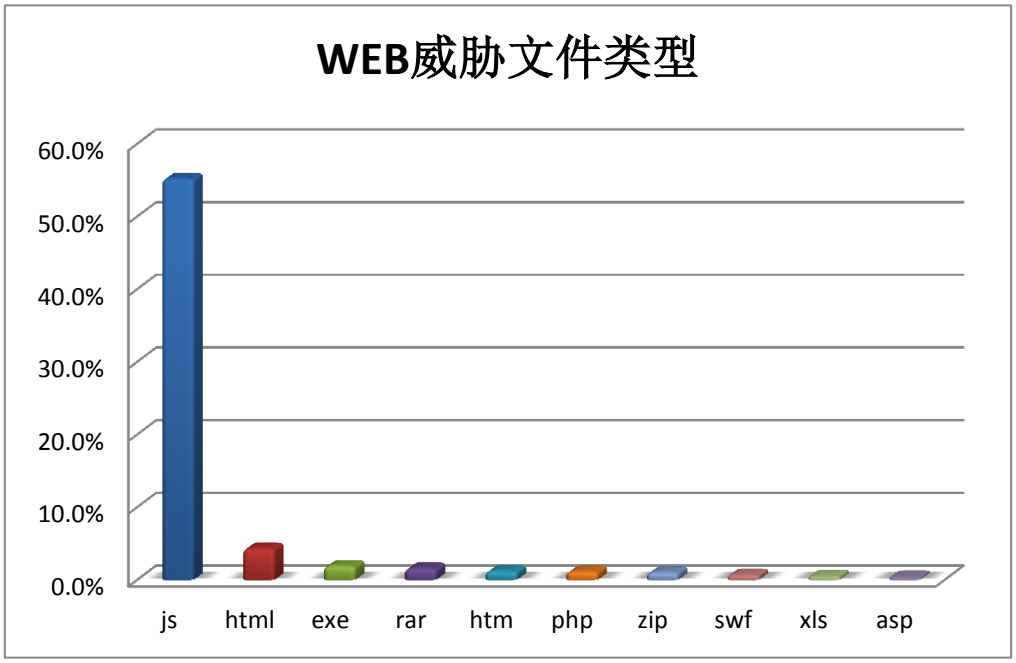
2012 年第 2 季度 web 安全威胁情况

2012 年第 2 季度 Web 威胁文件类型分析

其中通过 Web 传播的恶意程序中，约有 **55.3%**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。

.exe 仍然是占很大比例的 Web 威胁文件类型,企业用户建议在网关处控制某些类型的文件下载。

本季度在 WEB 威胁类型中也看到了.xls 文件者可能与近期宏病毒的爆发有关



2012 第 2 季度中国地区 web 威胁文件类型

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) ,本报告中所有数据仅针对中国地区。

2012 年第 2 季度 Web 威胁病毒类型分析

通过 WEB 感染的病毒排名	
病毒名称	百分比
General Exploit	68.79%
X97M_LAROUX.BK	3.77%
TROJ_SPNR.08JT11	3.68%
HTML_JADTRE.Y	2.79%
TROJ_SPNR.08JR11	1.50%
TROJ_SPNR.03JR11	0.84%
X97M_MICRO.A	0.73%
WORM_RIPLIP.SMI	0.70%
Mal_DLDER	0.65%
TROJ_SPNR.03CL11	0.59%
TROJ_RVERSE.SMI	0.49%
TROJ_SOFTSTOP.B	0.42%
TROJ_SPNR.08JS11	0.40%
TROJ_SPNR.08K111	0.33%
HTML_DOWN.A	0.33%
TROJ_AGENTT.EX	0.28%
X97M_LAROUX.DA	0.27%
BKDR_RIPINIP.SMA	0.26%
其它病毒	13.20%

2012 第 2 季度中国地区 web 威胁病毒排名

通过对拦截的 Web 威胁进行分析，我们发现。约有 68.8%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。

另外一些带有宏病毒的 office 文档被挂在 internet 供公众下载，这些是宏病毒传播的一个主要途径。感染了宏病毒的电脑使用者在不知情的情况下将带有病毒的文档上传至网站，会导致下载阅读文件的用户感染。

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) ,本报告中所有数据仅针对中国地区。

2012 年第 2 季度最新安全威胁信息

2012.6 中国区病毒实验室接到数起网络购物欺诈案件

用户在某购物网站购买吸尘器时，有个卖家给了他一个网址，称可以通过这种方式付款给他网址是：xxx.chinapay.com.xxxxx.in

网站上有一些链接，标价只有 2 块钱。但是实际提交的请求是一个更大的金额。

实现欺诈过程的文件为该钓鱼网站要求下载的一个支付插件。

对于该恶意插件的功能，分析如下：

恶意插件被下载后将自己释放到 c:\windows\safemda.dll ，注册为 BHO 控件，当运行 IE 浏览器时会自动被加载。
病毒运行后，会在后台起一个线程监视浏览的网址。通过截取网页中的敏感字符串来判断交易流程，例如“订单金额”、“请核对签吮信息”、以及一些相关银行的名称。

最后在订单确认环节，通过修改订单金额欺骗用户点击，例如 ，实际订单确认信息为 “订单金额 10000.00 元” 被修改为“订单金额 2.00 元”。

趋势科技提示用户，网络购物须谨慎切勿从卖家从聊天窗口提供的 URL 中进入支付流程。

2012.6《九阴真经》《暗黑 3》遭钓鱼网站围堵 玩家需小心装备不翼而飞

趋势科技近日发布消息，其全球最大的云安全动态威胁信息库（WRS）中发现大量针对热门网络游戏的钓鱼网站。以最新的网络游戏《九阴真经》为例，趋势科技在一天时间内便发现了多达 58 个针对该网游的虚假钓鱼网站。而针对《暗黑破坏神 3》的钓鱼页面成几何倍数增长，进一步证实了近期网络上“D3 出现大量黑号”的流言。使用动态威胁信息库（WRS）联动机制的趋势科技企业和 PC-cillin 2012 云安全版个人用户，皆已自动更新，并可主动拦截此类威胁。

钓鱼犯罪分子与铁杆游戏迷们一样，对热门网游都十分追捧。除了域名近似之外，骗子们做出的钓鱼网站与官网几乎一模一样，都以“领取免费大礼包”为诱饵，再加上钓鱼邮件、社交网络虚假信息发布等辅助攻击手段，骗取网游账号的信息，包括账号、密码、二级口令、角色名称和角色区服。游戏厂商的安全防护设置也常常被黑客破解，例如异地账号锁定等等，玩家如果不能在第一时间找回密码，辛苦打回来的装备和虚拟金币都可能不翼而飞。

相关链接：
http://cn.trendmicro.com/cn/about/news/pr/article/20120619094755.html

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) ,本报告中所有数据仅针对中国地区。

2012.6 黑客攻破中国电信网络 发布 900 个后台密码

6 月 4 日消息，据国外媒体报道，黑客组织 Swagger Security（又名 SwaggSec）近日宣布其攻破了中国电信和华纳兄弟的网络，并在网上发布了相关文档和登录证书。

Swagger Security 周日在代码分享网站 Pastebin 上发布了相关消息，并在海盗湾提供了相关文件的下载。该黑客组织曾于今年年初宣布攻破了富士康公司的网络。

该黑客组织称，中国电信的相关数据中包括了从一个不安全的 SQL 服务器获取的中国电信网络管理员的 900 个用户名和密码，他们还在中国电信的服务器上留下了一条信息告知该公司相关情况。

Swagger Security 表示，他们很幸运，因为我们没有破坏他们的基础设施而让千百万用户无法使用通信服务。

华纳公司的数据则被包含在一个题为“内容安全状态更新”，并被标注为“机密”的报告中，报告的日期为 4 月 27 日。报告对华纳公司旗下网站的安全状态进行了评估，列出了该公司网络中 10 个“中高级”安全漏洞和 10 个中级安全漏洞最多的网站。

若该报告内容属实，其他黑客可以借此对华纳兄弟公司旗下的网站展开攻击。报告同时包含了其他一些文件，部分文件标注的日期为 2007 年。

相关链接：
http://it.sohu.com/20120604/n344731733.shtml

2012.6 Windows 又现高危漏洞 “暴雷”轰然而至

6 月 13 ，微软发布紧急公告，称 Windows 基础组件出现高危漏洞“暴雷”，并推出“暴雷”漏洞临时解决方案。据悉，“暴雷”是基于 Windows 基础组件的远程攻击漏洞，黑客可以通过该漏洞，以恶意网页、文档等形式将任意木马植入用户电脑，窃取重要资料和账号信息。

相关链接：
http://technet.microsoft.com/zh-cn/security/advisory/2719615
http://www.freebuf.com/tools/4172.html

2012.6 Intel CPU 漏洞导致 64 位操作系统、虚拟化软件易受黑客攻击

美国计算机应急预备小组本周发布了一份安全报告，一些 64 位操作系统和虚拟化软件程序在 Intel 处理器上运行时，容易受到本地特权扩大攻击（ local privilege escalation）。该漏

洞可能被利用来获取本地特权扩大或是 guest-to-host 虚拟机逃逸（virtual machine escape）。

这一漏洞（CVE-2012-0217）源于 Intel 处理器在 x86-64 扩展（也就是 Intel 64）中执行 SYSRET 指令集的方式，仅仅影响 Intel 处理器上的 Intel 64 扩展使用，32 位操作系统或虚拟化软件不受影响。

受影响的操作系统包括：64 位 Windows 7、Windows Server 2008 R2、64 位 FreeBSD 和 NetBSD、Xen 虚拟化软件、红帽企业 Linux、SUSE Linux Enterprise Server。

VMware 安全团队表示，VMware 的管理程序不使用 SYSRET 指令集，因此，VMWare 不受此漏洞影响。

Vendor	Status	Date Notified	Date Updated
Citrix	Affected	-	14 Jun 2012
FreeBSD Project	Affected	01 May 2012	12 Jun 2012
Intel Corporation	Affected	01 May 2012	13 Jun 2012
Joyent	Affected	-	14 Jun 2012
Microsoft Corporation	Affected	01 May 2012	08 Jun 2012
NetBSD	Affected	01 May 2012	08 Jun 2012
Oracle Corporation	Affected	01 May 2012	08 Jun 2012
Red Hat, Inc.	Affected	01 May 2012	12 Jun 2012
SUSE Linux	Affected	02 May 2012	12 Jun 2012
Xen	Affected	02 May 2012	12 Jun 2012
AMD	Not Affected	-	13 Jun 2012
Apple Inc.	Not Affected	01 May 2012	08 Jun 2012
VMware	Not Affected	01 May 2012	08 Jun 2012
Debian GNU/Linux	Unknown	02 May 2012	02 May 2012
Fedora Project	Unknown	02 May 2012	02 May 2012

相关链接：

http://news.mydrivers.com/1/231/231509.htm

2012.6 LinkedIn 用户的密码泄露

北京时间 6 月 7 日消息，据国外媒体 ZDNet.com 报道，全球知名社交网站之一的 LinkedIn 被匿名黑客攻击，超过 640 万 LinkedIn 用户的密码信息被张贴在一个俄国黑客网站上。

据介绍，超过 30 万简单密码已被解密，而更多的密码正在解密过程中。事件发生后，芬兰

安全公司 CERT-FI 发表声明称，芬兰信息安全公司 CERT-FI 警告 LinkedIn 称，尽管黑客并未公布相关的用户信息，但他们很可能已获得了这些信息，其中可能还包括 LinkedIn 用户的邮件信息。

LinkedIn 信息安全研究人员佩尔·索谢姆在 Twitter 主页上确认了这一消息，声称 LinedIn 目前正针对这一事件进行调查，而调查结果稍后会向大众进行报告。这一信息发布后，LinkedIn 的股价陡然下跌。

根据《纽约时报》报道，LinkedIn 密码泄露主要是因为该网站移动程序中的日历功能存在漏洞，会议地址、时间、记录等信息会在用户不知情的前提下，被传回 LinkedIn 服务器。

ZDNet.com 报告中指出，LinkedIn 全球用户总数超过 1.5 亿，这意味着约有 4%的用户密码被泄露，建议用户马上修改自己的密码。
相关链接：

http://www.newhua.com/2012/0607/163032.shtml

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) ,本报告中所有数据仅针对中国地区。