# 中国地区 2013 年

# 第三季度

# 网络安全威胁报告

2013/11

CHINA RTL

# 目录

# 2013 年第 3 季度安全威胁

## 本季安全警示：

## APT，漏洞攻击，PE 类型病毒感染

### 2013 年第 3 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 60 万条。截止 2013.9.30 日中国区传统病毒码 **10.308.60** 包含病毒特征数约 **430** 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 **5240** 万次。

- 本季度趋势科技在中国地区拦截的恶意 URL 地址 **204,250,860** 次。

2013 年第 3 季度，趋势科技病毒实验室检测发现有一种窃取信息的病毒同时在国内多家金融行业用户网络中潜伏，该恶意程序以证券/基金行业为目标，极度顽强和具有隐蔽性，在目标环境中已经潜伏了一段时间。我们有理由相信这是由一组专业的黑客，针对证券行业发起的一系列 APT 行为。

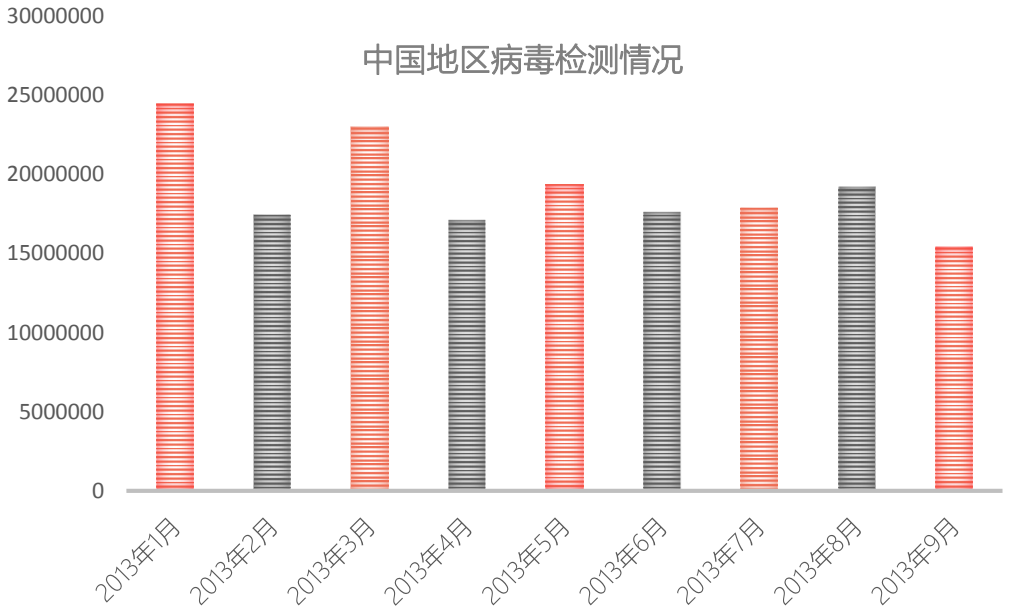
第 3 季度，木马病毒、后门以及间谍软件仍然占据新增病毒数量的前三位。大部分木马有盗号或是窃取系统重要信息的特性。 与其他类型的电脑病毒相比木马更容易编写且更容易使病毒制造者获益。在经济利益的驱使下，更多病毒制作者开始制造木马病毒。后门病毒则会给受感染电脑带来极大的安全隐患，而间谍软件更专注于窃取用户重要信息。另外，新增病毒中黑客工具数量大幅上升。黑客工具的泛滥，给互联网安全带来极大的隐患。

本季度 PE 病毒感染情况持续严重：

- **PE_PATCHED.ASA** 仍占据病毒检测数量排名首位，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，该文件被修改预示着有其他会修改系统文件的恶意行为可能将会发生。

- **PE_SALITY.RL**，**PE_PARITE.A** 在本季度仍在流行中，PE_SALITY.RL 除了常规的 PE 病毒感染方式还会通过微软的快捷方式漏洞传播(**MS10-046**), PE_PARITE.A 除了通过感染文件，网络共享，还能够通过电子邮件传播。

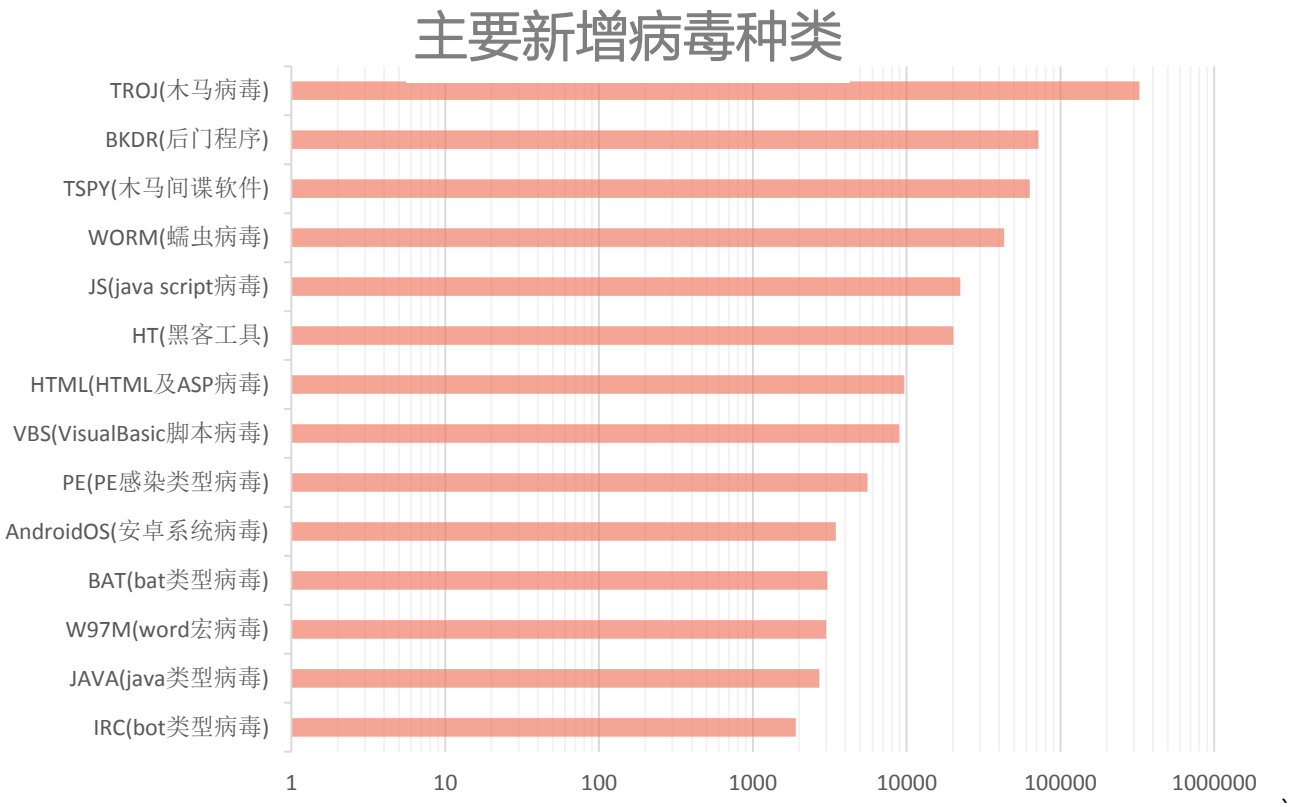
- **另外又有两种 PE（PE_WAPOMI.SM ， PE_RAMNIT.DEN**）病毒进入了感染数量前 20 名的排行中。




在 2013 年第 3 季度趋势科技拦截新的恶意网站中钓鱼网站约有 **3400** 个(以域名计数)。各种钓鱼网站仿冒目标中，网上在线支付以及金融证券仍然是钓鱼网页制造者主要的仿冒对象。目前，很多钓鱼网站通过屏蔽 IP，等各种技术手段阻止安全厂商对其访问和扫描，以躲避侦测。

**2013 年第 3 季度病毒威胁情况**

**2013 年第 3 季度新增病毒类型分析**




2013 第 3 季度中国地区新增病毒类型

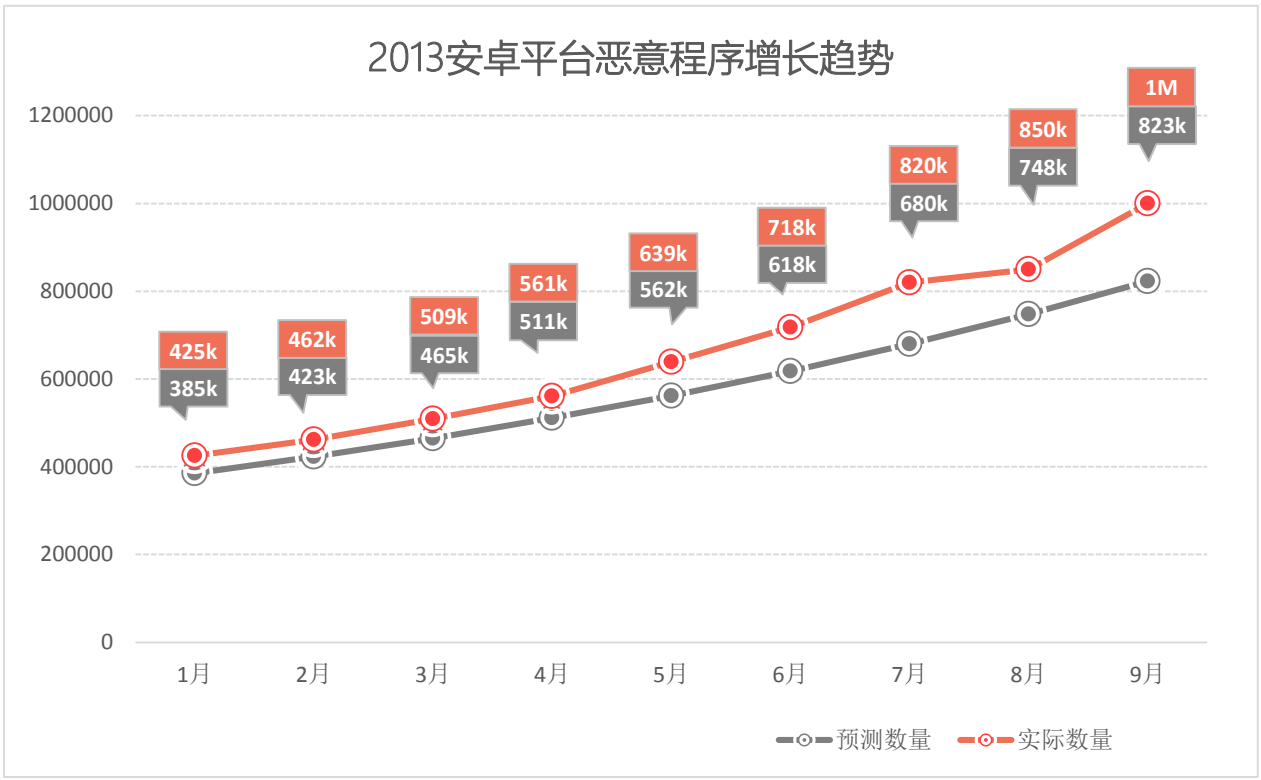
新增的病毒类型最多的仍然为木马（TROJ），本季度新增木马病毒特征 **325690** 个，比上季度稍微有所增加。木马可使病毒制造者更直接的获利，在经济利益的驱使下大量的木马被制造并通过各方式被传入互联网中。木马也是我国目前存在数量最多的病毒类型。

本季度新增的病毒类型中，处于上升趋势的病毒类型为 **JS(java script 病毒) ，HTML(HTML 及 ASP 病毒) ，VBS(VisualBasic 脚本病毒) ，JAVA(java 类型病毒) ，HT(黑客工具)。**其中趋势科技定义以 HT_开头的检测类型为黑客工具，值得注意的是第 3 季度新增黑客工具的数量几乎达到上季度的一倍。地下黑市的活跃使更多的黑客工具流传到市面上，被黑客准“黑客”们大量使用，也使得网络安全问题日趋严重。一些可以从 internet 访问到的机器，越发容易受到攻击，一旦不能及时安装漏洞补丁或是存在某种弱点（例如：开启了远程桌面，或帐号密码较弱等）即有极大的可能被攻击。公司的 WEB 服务器，甚至从互联网上能够访问到的 OA 系统都经常成为攻击，入侵的目标。黑客工具更使得网络攻击变的越来越简单。

JS (java script 病毒)，HTML(HTML 及 ASP 病毒)常常和网页挂马相关。恶意代码的制造者将代码植入网中，这些脚本内容往往不容易被网站管理者以及浏览网页的用户发觉，正常的网站服务器成了扩散病毒，恶意代码的平台。另外，还有部分 JS、HTML 病毒可能是 Webshell，通过向网站中放入 webshell，黑客甚至可以

控制网站服务器的机器。这样一来，网站用户的数据可能会被盗窃，服务器也可能成为这些恶意行为者的肉鸡，被用来进行网络攻击或其他一些非法的网络行为。

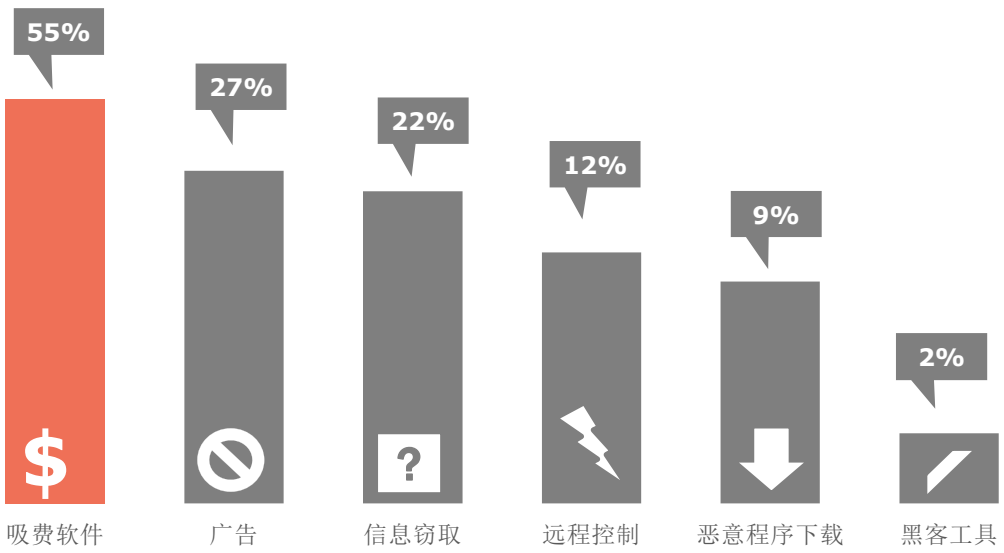
新的安卓系统病毒 (AndroidOS)数量，在 2013 年第 3 季度持续上升。在距离今年结束还差 3 个月的时候，针对安卓系统的恶意程序数量达到 1 亿。安卓系统的恶意程序增长速度比我们之前预计的要快了许多。




第 3 季度，感染安卓平台的恶意程序中，数量最多的为吸费软件。占到所有新增病毒的 55%，广告软件占 27% 上升到第 2 名的位置，而第三名则为窃取数据信息类型的恶意程序。

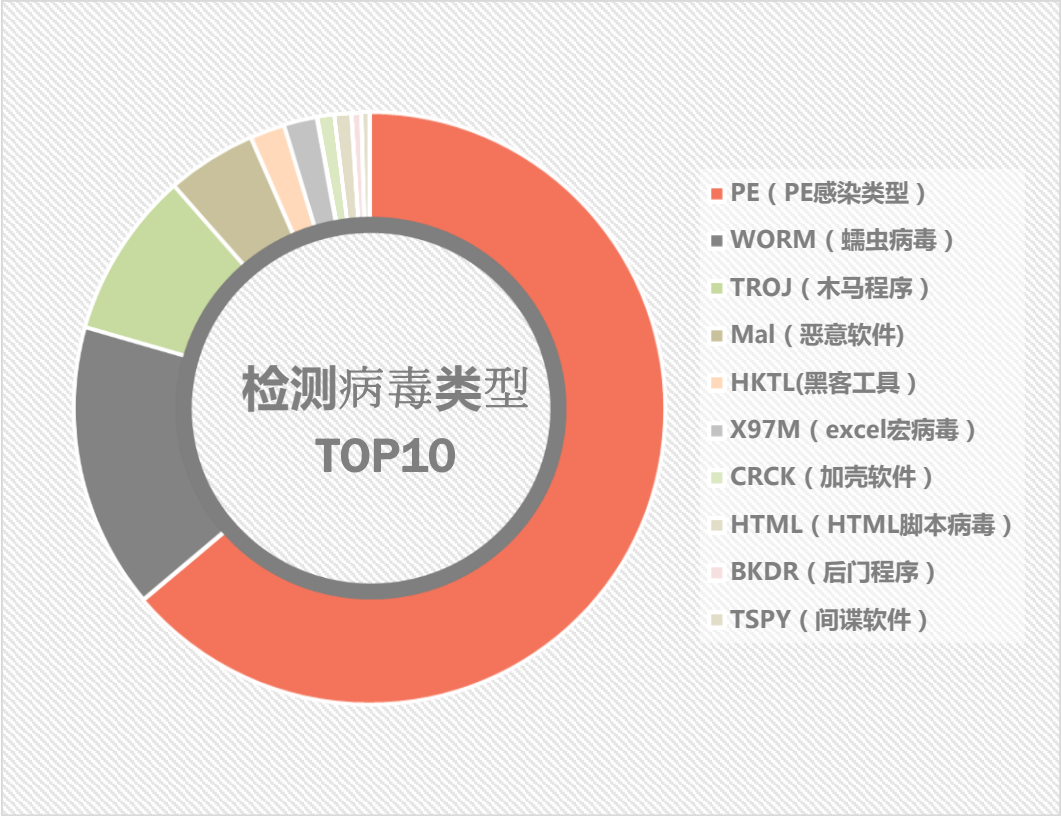
需要注意的是吸费软件也具有一定窃取帐号信息，以及监控短信的功能。这种恶意程序危害极大，会给感染该类病毒的用户带来经济损失和麻烦。

据统计，这些安卓系统的恶意程序超过半数是从网站下载而来。还需要提醒手机用户在下载安装程序，特别是安装程序时要注意过程中的每一个提示以减少因为疏忽而误装恶意程序造成的损失 。




**2013 第 3 季度安卓平台病毒类型排名**

**2013 年第 3 季度各类型病毒检测情况分析**




2013 第 3 季度中国地区各类型病毒检测数量比例图

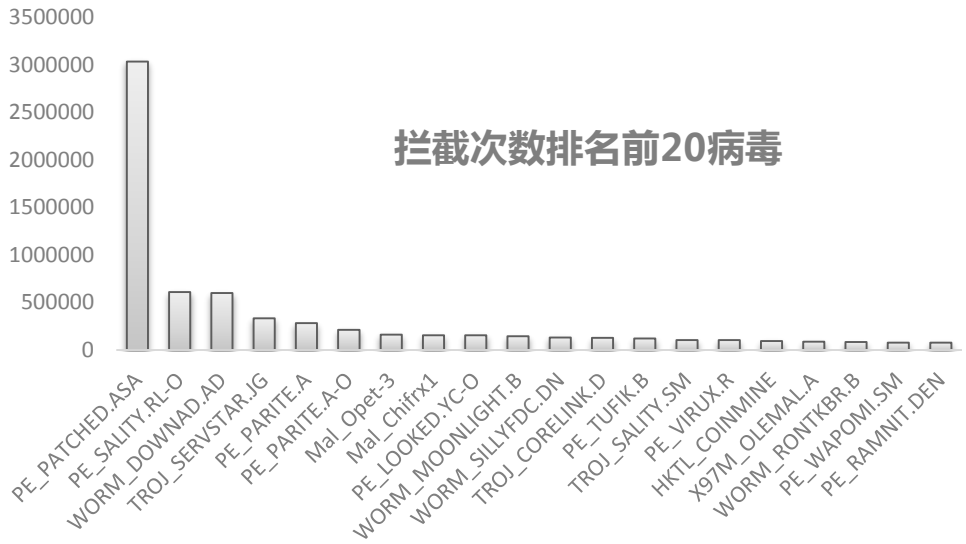
受 PE_PATCHED.ASA 大量被检测的影响，2013 年第 3 季度检测到的病毒种类中 PE 类型病毒感染数量仍保持超过 50% 的百分比，大约占到总检测数量的 62%。PE 病毒为感染型病毒，该类病毒的特征是将恶意代码插入正常的可执行文件中。第 3 季度，检测数量最多的 PE 病毒仍然是 PE_PATCHED.ASA。该病毒为被修改的 sfc_os.dll，sfc_os.dll 是用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能。

另外，在第 3 季度趋势科技监测到一种比较特别的感染型病毒出现，该病毒为 PE_EXPIRO 家族的某个变种。此感染型病毒的感染代码中包含窃取信息的例程，这一行为在感染型病毒中并不常见。PE_EXPIRO 家族最早在 2010 年被发现用来对某公司或组织的 web 站点进行入侵。如有客户检测到该类病毒，则需要密切关注并尽快处理。

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。第 3 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，会感染一些蠕虫病毒。随着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。PE 病毒自身也可能带有木马病毒的特征。

**2013 年第 3 季度病毒拦截情况分析**




**2013 第 3 季度中国区拦截次数排名前 20 病毒**

上图显示了 2013 年第 3 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。

2013 年第 3 季度被趋势科技拦截次数最多仍然的为 PE_PATCHED.ASA。该病毒被拦截次数约为 303 万次。远远超过其他病毒。

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（可以使用以下三种方法中的任意一种进行清理）：

- 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，需要的用户可以到以下地址下载反病毒工具包进行处理：
  http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/Release.zip

对于排名前 3 名的 PE_PATCHED, PE_SALITY 以及 WORM_DOWNAD，一直是中国地区用户感染较多的病毒。

解决方案以及病毒的相关信息已经多次介绍过。如有无法解决的状况请联系趋势科技技术支持部门。

本季度又有两种之前没有进入排名的 PE 类型病感染数量到达前 20 名的位置，需要关注:

这两种感染型病毒都有通过移动存储设备感染的特征，需要注意对移动存储设备自动播放功能的控制。

**PE_WAPOMI.SM /PE_WAPOMI.SM-O**

这是一种感染类型病毒，在感染其他可执行文件的同时还会释放出恶意程序，和 autorun.inf. 释放的恶意程序将会被保存在被感染电脑中。并通过 autorun.inf 自启动.PE_WAPOMI.SM-O 为母体文件，被他感染的可执行程序被趋势科技检测为 PE_WAPOMI.SM

***感染途径:***

该病毒一般通过其他恶意程序释放，或在访问恶意网站时下载而来。也可能通过移动存储设备传播

***修改系统内容:***

PE_WAPOMI.SM-O 会删除以下系统文件：

%Windows%\SoftwareDistribution\DataStore\Logs\edbtmp.log

(注意: *%Windows%* 是 windows 目录, 通常为 C:\Windows 或 C:\WINNT.)

该病毒会释放以下文件:

%System%\{random characters}.sys -被检测为 RTKT_WAPOMI.A, 一个用来隐藏此感染型病毒的进程,文件,以及注册表信息的 rootkit.

%System Root%\Users\Infotmp.txt

%System Root%\Documents and Settings\Infotmp.txt

%Temp%\rcae685c.txt

会删除以下注册表键值:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network

会感染系统中的.exe 文件,被感染的可执行文件(PE_WAPOMI.SM)运行后会释放

%System Root%\{random}.exe 此文件也就是该感染型病毒的母体文件(PE_WAPOMI.SM-O)

但是他会避开感染包含有以下字符串的文件夹中文件:

- Thunder Network
- Thunder
- WinRAR
- WindowsUpdate
- Windows NT
- Windows Media Player
- Outlook Express
- NetMeeting
- MSN Gaming Zone
- Movie Maker
- Microsoft Frontpage
- Messenger
- Internet Explorer
- InstallShield Installation Information
- ComPlus Applications
- Common Files
- RECYCLER
- System Volume Information
- Documents and Settings
- WinNT
- Windows

***解决方法:***

1. 关闭系统还原
2. 升级防毒产品到最新病毒码并进行全盘扫描
3. 没有安装防毒产品或者是防毒产品已经被破坏的用户请到以下站点下载 ATTK 进行扫描：

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

*防护方法：*

1. 保证防毒软件的病毒码及时的更新
2. 关闭移动存储设备的自动播放功能,

**小贴士： 在移动存储设备根目录创建名为 autorun.inf 的文件夹,并设置不可访问权限.有助于预防自动播放类型病毒.**

**PE_RAMNIT.DEN-O / PE_RAMNIT.DEN**

PE_RAMNIT.DEN 为感染型病毒,他会创建一个隐藏的 iexplorer.exe 进程,用来连接远端的恶意站点下载其他恶意程序

被感染的 DLL 和 EXE 文件 - PE_RAMNIT.DEN

被感染的 HTML 文件 - HTML_RAMNIT.AJ

*感染途径：*

该木马程序可能由其他恶意程序释放，或下载而来。

它会释放自身的复制到所有移动存储设备中，病毒释放一个 autorun.inf 文件以达到自启动的目的

*修改系统内容：*

释放以下文件：

%User Profile%\{random filename}.log

%Program Files%\Internet Explorer\dmlconf.dat

复制自身到以下目录：

%User Startup%\{random filename}.exe

%Program Files%\{random folder name}\{random filename}.exe

创建以下目录：

%Program Files%\{random folder name}

创建以下注册表键值，以达到自启动的目的：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Userinit = "%System%\userinit.exe,,%Program Files%\{random folder name}\{random file name}.exe"

修改以下注册表键值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List

%Program Files%\Internet Explorer\IEXPLORE.EXE = %Program Files%\Internet Explorer\IEXPLORE.EXE:*:Enabled:internet Explorer

***文件感染：***

它会感染以下类型文件：

DLL

EXE

HTML

***解决方法：***

1. 升级防毒产品到最新病毒码并进行全盘扫描
2. 没有安装防毒产品或者是防毒产品已经被破坏的用户请到以下站点下载 ATTK 进行扫描：

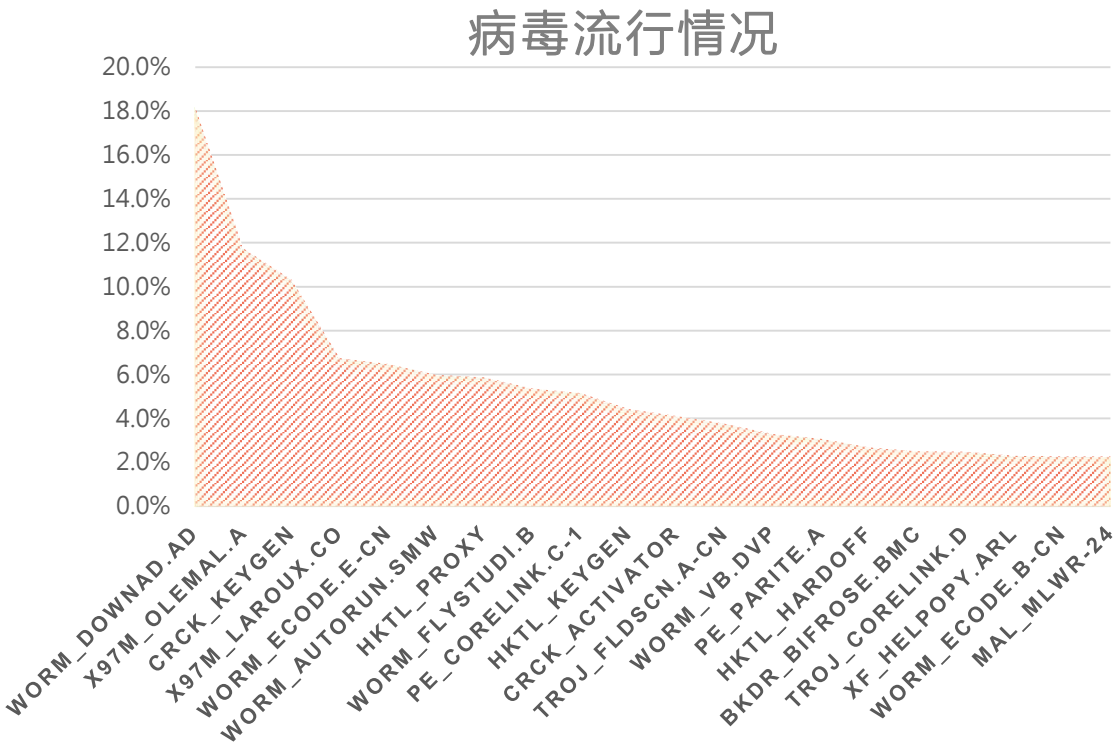
32 位 windows 操作系统请使用：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage.exe

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

***防护方法：***

1. 保证防毒软件的病毒码及时的更新
2. 关闭移动存储设备的自动播放功能,

**2013 年第 3 季度流行病毒分析**




**2013 第 3 季度中国地区病毒流行度排名**

2013 年第 3 季度 Worm_downad 全球分布图

虽然解决方案已知但 WORM_DOWNAD 在中国的感染情况并没有得到很大改善。截止 2013 年第 3 季度，仍约有 18% 的用户遭受到此病毒的攻击。从 WORM_DOWNAD 的全球分布图来看,中国仍然属于感染较严重地区.

目前的防病毒产品都能够检测并处理这些病毒，网络内一直有这种病毒存在，说明环境存在某些安全缺陷，使得病毒能够进入并且持续存活，针对这种情况需要及时处理和分析。

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。

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。

**X97M_OLEMAL.A** 这只从中国地区源起的病毒 EXCEL 病毒目前已经传染至全球各地，并且在美国地区感染趋于严重。

2013 年第 3 季度全球 X97M_OLEMAL.A 病毒感染情况

从我们获得信息来看的该病毒主要感染途径如下：

- 从网站下载而来
- 使用文件传输工具获得
- 通过邮件传送

***病毒防护方法：***

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：***

目前趋势科技最新中国区病毒码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/supportcustmizedpackage.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

另外可以使用 ChinaRTL 的 AVBtool 可以查杀此病毒：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/Release.zip
（解压缩密码：novirus）
使用前请看 readme:
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/readme.txt

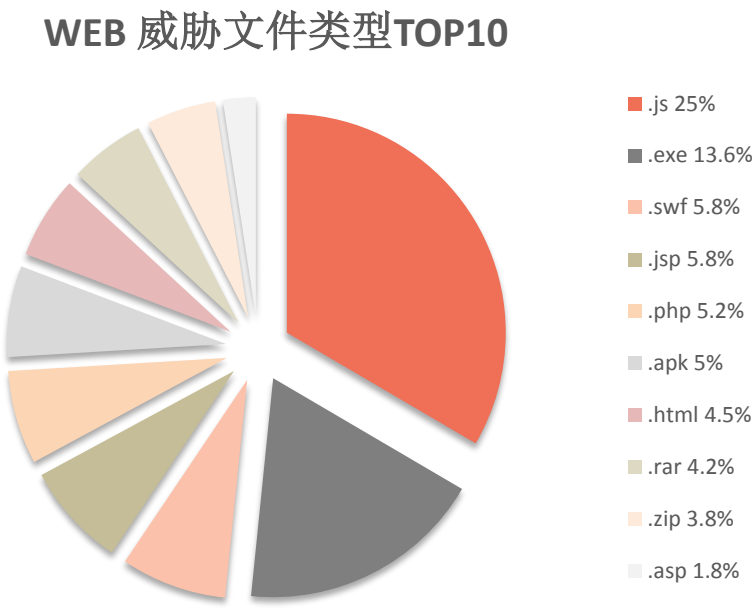
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

**2013 年第 3 季度 web 安全威胁情况**

**2013 年第 3 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 25%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来执行其他恶意行为。

.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。



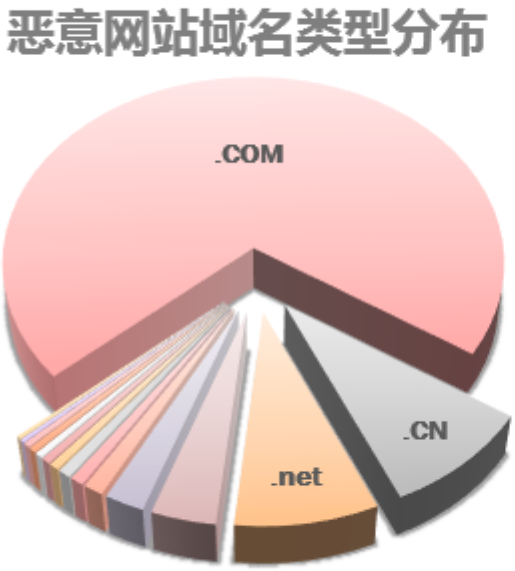

2013 第 3 季度中国地区 web 威胁文件类型

**2013 年第 3 季度 top10 恶意 URL**

| TOP10恶意URL | | |
|---|---|---|
| **恶意URL** | **描述** | **点击量** |
| hxxp://dd.*********.com/p.html | 该网站的地址在垃圾邮件中被发现 | 2759392 |
| hxxp://swf.yk******w.com/crossdomain.xml | 网站直接或间接帮助传播恶意软件或恶意代码 | 2430456 |
| hxxp://cdn.g*******.com/imupdate/patch24/1.2.20.9P/VersionModule.dll | 网站直接或间接帮助传播恶意软件或恶意代码 | 2115706 |
| hxxp://disp.y******6.com/dm.php?uid=16&tid=1&ref=1 | 该网站的地址在垃圾邮件中被发现 | 1707054 |
| hxxp://cdn.ga******w.com/imupdate/patch26/1.2.25.2P/bbtalk/lib/UILib.dll | 网站直接或间接帮助传播恶意软件或恶意代码 | 877927 |
| hxxp://br.p******.net/banner/xml/1.0.0.84/ads_archive.zip | 网站直接或间接帮助传播恶意软件或恶意代码 | 693947 |
| hxxp://treezip.******.net/iteminfo_xml/3/2841074.zip | 网站直接或间接帮助传播恶意软件或恶意代码 | 653590 |
| denis.******.******.com | 网站直接或间接帮助传播恶意软件或恶意代码 | 646088 |
| hxxp://wpad.pnp.gw/wpad.dat | 该网站的地址在垃圾邮件中被发现 | 635115 |
| hxxp://cdn.gar******.com/imupdate/patch26/1.2.25.2P/bbtalk/plugins/D3DHook/OverlayHookD3D8.dll | 网站直接或间接帮助传播恶意软件或恶意代码 | 536421 |

**2013 第 3 季度中国地区已被 wrs 阻止的恶意 url 排名**

**2013 年第 3 季度 web 威胁域名分布**

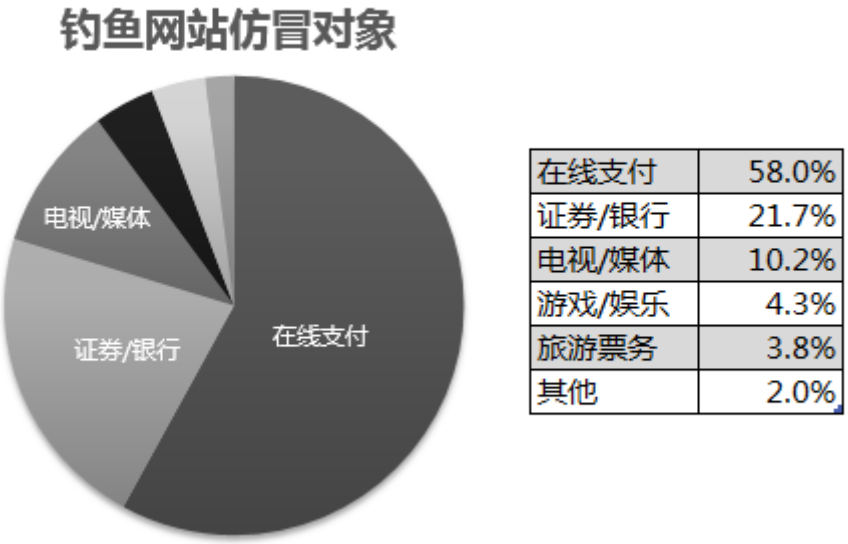



| | |
|---|---|
| .com | 59.5% |
| .cn | 7.7% |
| .net | 7.1% |
| .ru | 3.2% |
| .org | 2.0% |
| .de | 1.0% |
| .info | 0.7% |
| .cc | 0.7% |
| .us | 0.5% |
| .uk | 0.4% |
| .ua | 0.4% |
| .kr | 0.4% |
| .in | 0.4% |
| .hk | 0.2% |
| .nl | 0.2% |

2013 第 3 季度中国地区恶意域名类型分布

第 3 季度，恶意软件域名在各顶级域的分布情况如上图，其中使用.com，.net，.cn 的域名的站点占了 74.3%。其中.com 域名下的恶意页数量最多。

**2013 年第 3 季度 Web 威胁钓鱼网站仿冒对象分析**




| | |
|---|---|
| 在线支付 | 58.0% |
| 证券/银行 | 21.7% |
| 电视/媒体 | 10.2% |
| 游戏/娱乐 | 4.3% |
| 旅游票务 | 3.8% |
| 其他 | 2.0% |

2013 第 3 季度中国地区钓鱼网站仿冒对象

从第 2013 年第 3 季度趋势科技捕获到的钓鱼网站数据来看，网上支付类网站，以及金融证券机构这些能够直接为钓鱼网站制造者带来经济利益的网站仍然是钓鱼者最喜欢仿冒的对象。银行网上支付的钓鱼网站也制作的非常逼真使人防不胜防。

提醒用户在网络上面进行任何交易时请小心谨慎。特别是通过淘宝网站购物时尽量不要点击聊天窗口中的 URL 进入支付页面。

钓鱼网站为了躲避安全产品及机构的检测，采取了屏蔽 IP 等各种手段阻止某些地址访问，使得检测钓鱼网站更加困难，也说明钓鱼网站也趋于使用鱼叉式攻击的方法而越加具有针对性。

**对于无法辨别恶意与否的网站可以到趋势科技网站安全查询页面查询：**
http://global.sitesafety.trendmicro.com/index.php

**2013 年第 3 季度漏洞攻击威胁情况**

| 漏洞名称 | 检测数量 |
|---|---|
| CVE-2010-0870 | 854492 |
| CVE-2008-2894 | 746870 |
| CVE-2008-4250 | 457650 |
| CVE-2009-1140 | 457632 |
| MS09-019 | 457632 |
| CVE-2010-3970 | 20494 |
| CVE-2007-6250 | 4708 |
| CVE-2011-0026 | 3410 |
| CVE-2011-0027 | 3410 |
| CVE-2010-3145 | 3300 |

2013 第 3 季度中国地区漏洞攻击检测情况

| | |
|---|---|
| CVE-2010-0870 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-0870 |
| CVE-2008-2894 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2008-2894 |
| CVE-2008-4250 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2008-4250 |
| CVE-2009-1140 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2009-1140 |
| MS09-019 | http://technet.microsoft.com/zh-CN/security/bulletin/ms09-019 |
| CVE-2010-3970 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3970 |
| CVE-2007-6250 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2007-6250 |
| CVE-2011-0026 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0026 |
| CVE-2011-0027 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2011-0027 |
| CVE-2010-3145 | http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3145 |

漏洞介绍链接

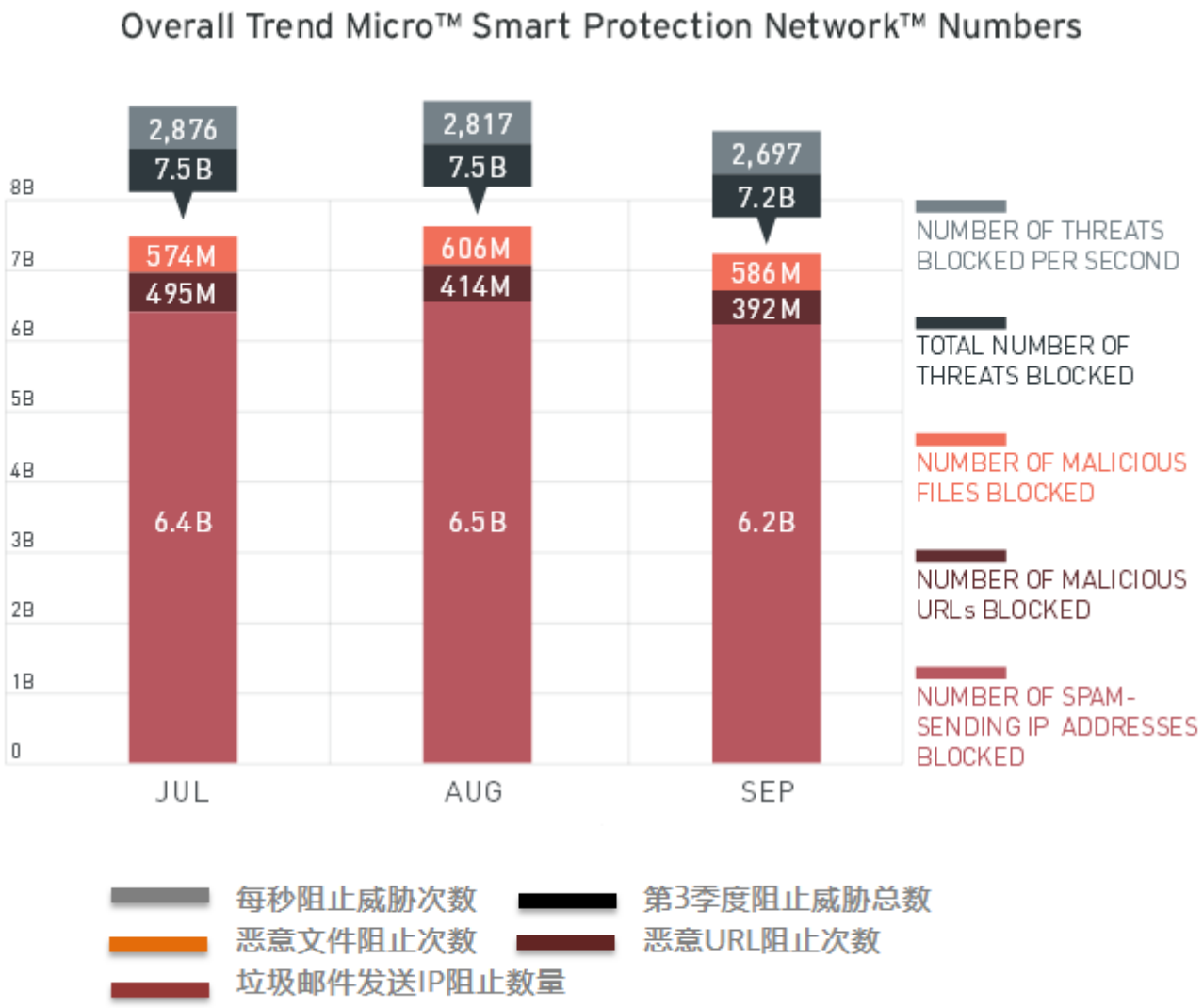
**小贴士：**

**确认补丁成功安装的小方法，开始-运行　输入 cmd 进入 dos 界面　输入 systeminfo 即可检查当前已成功安装的补丁版本**

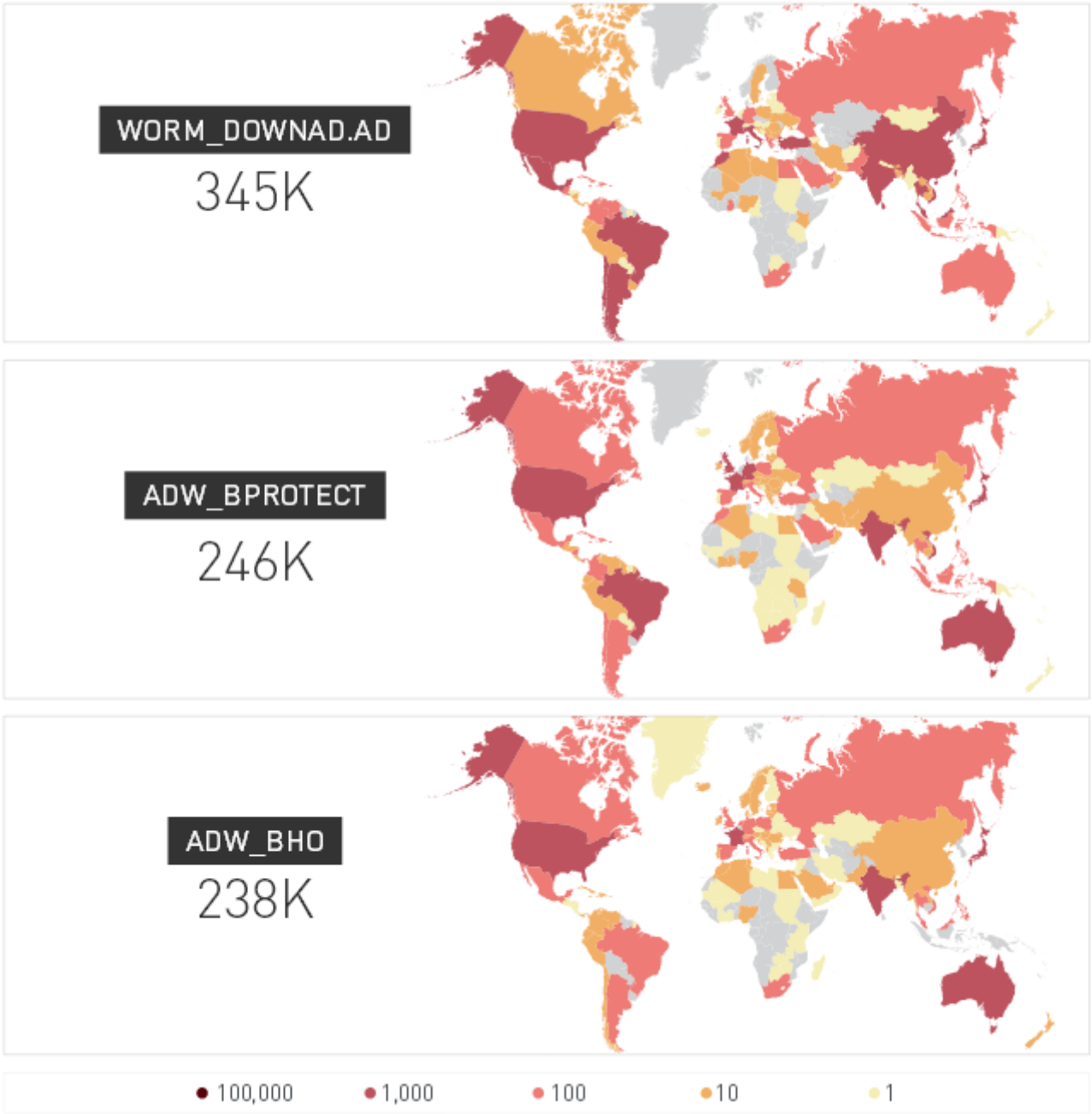
**2013 年第 3 季度最新安全威胁信息**

**2013 年第 3 季度趋势科技全球区安全威胁概要**

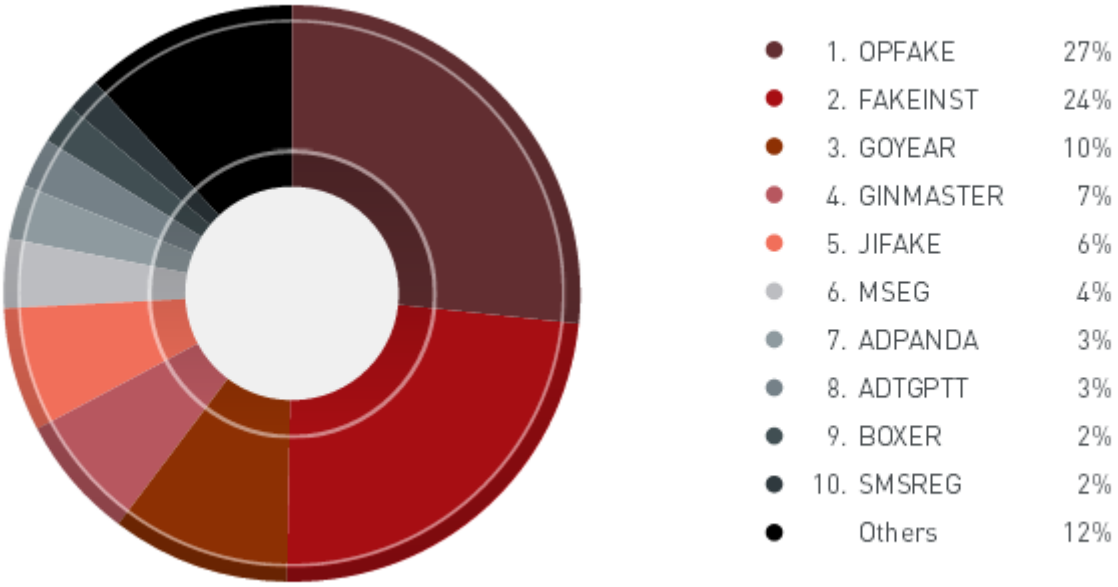
**全球 SPN 智能防护网拦截威胁数量**



## 全球 TOP3 病毒

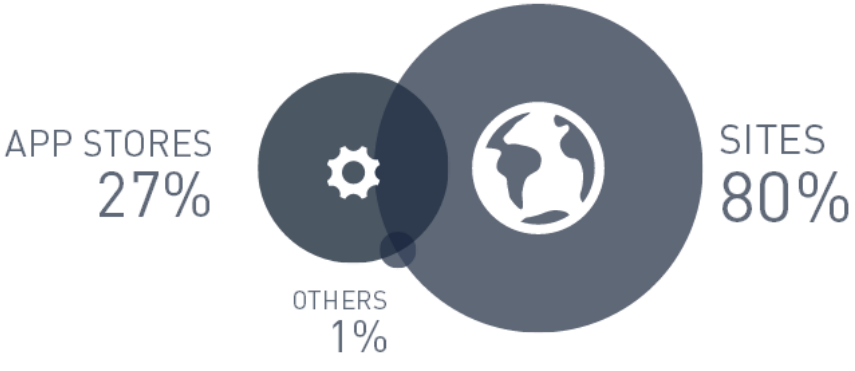

WORM_DOWNAD.AD
345K
ADW_BPROTECT
246K
ADW_BHO
238K
100,000
1,000
100
10
1

## 全球安卓系统病毒家族排名




## 全球手机病毒感染渠道

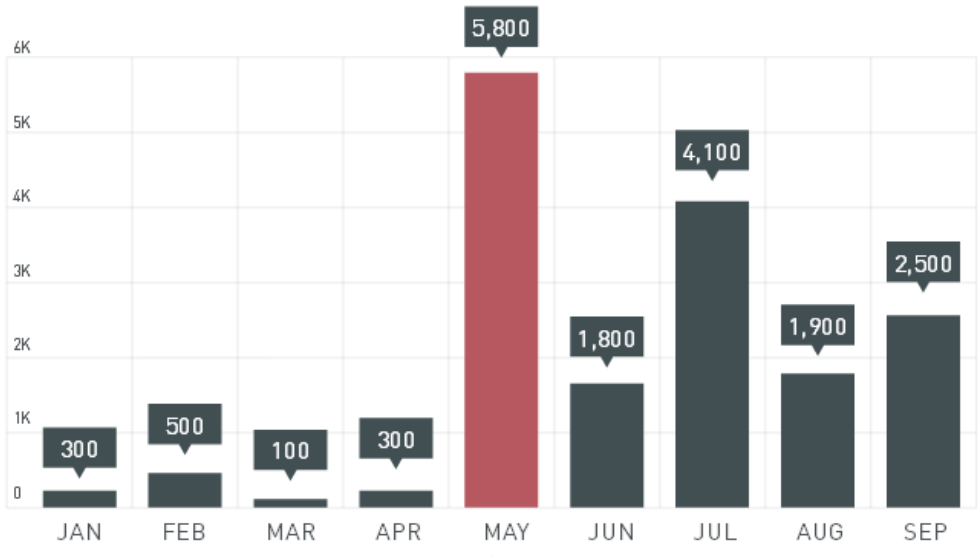
**27% 来自应用商店，80%来自网站**



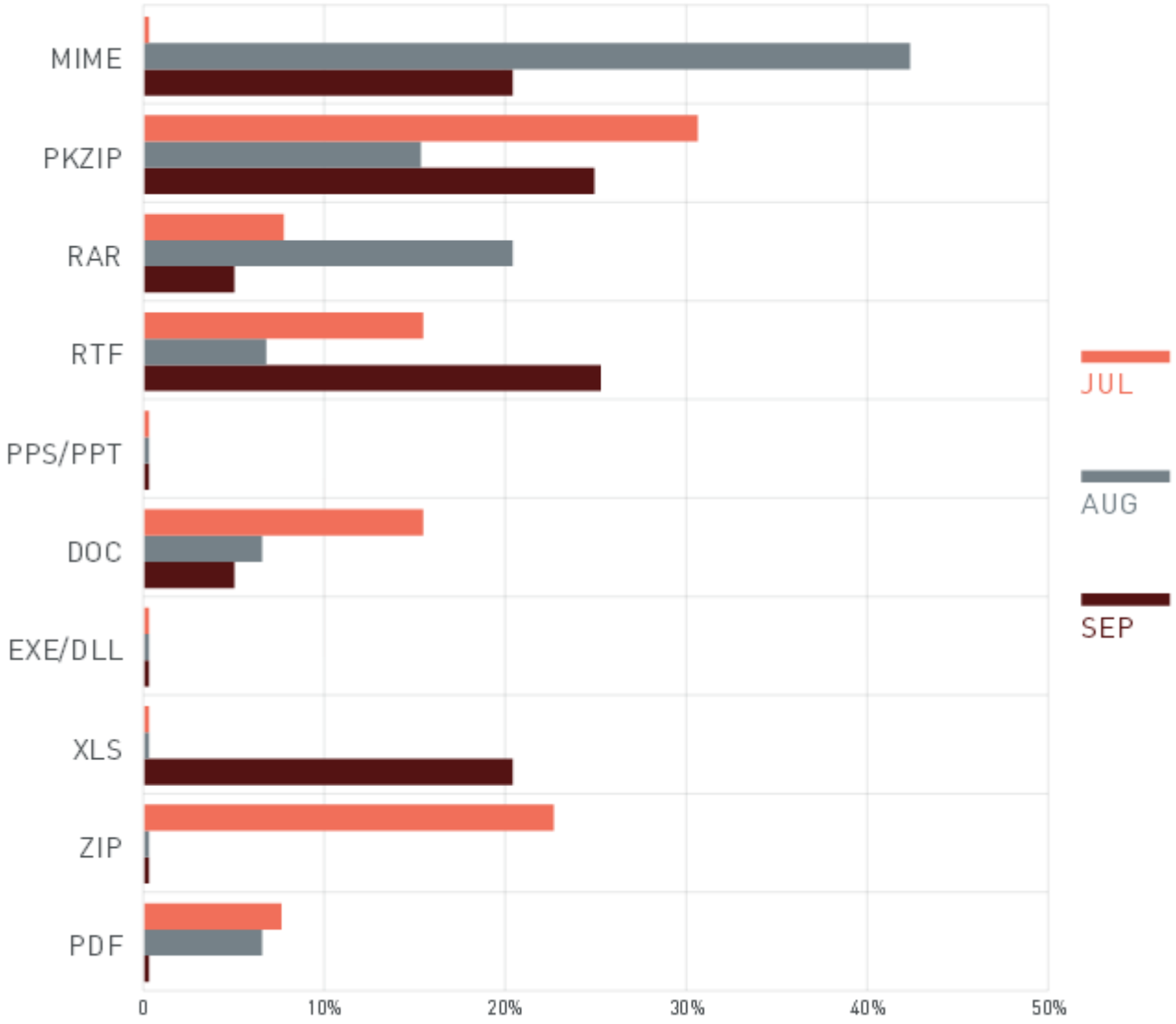
## 吸费软件可以做什么

**96%** 的吸费软件能够访问 SD 卡的数据 （能删除数据）
**92%** 的吸费软件能够读取手机短信 （监控短信息）
**86%** 的吸费软件可以利用你的手机发送预定义的短信内容（发送默认信息）
**48%** 的吸费软件能够访问你的联系人列表 （查看联系人）
**14%** 的吸费软件能够追踪你的位置 （追踪方位）

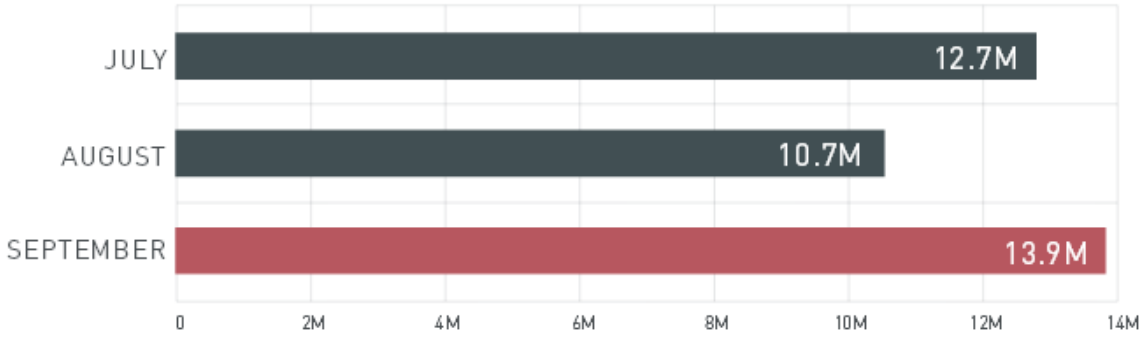

## 苹果新产品发布，导致相关钓鱼网站激增



**在针对性攻击中，鱼叉式钓鱼邮件利用的文件类型排名**



**全球第三季度僵尸网络连接数量**




需要查看更完整的第 3 季度全球安全报告请访问：
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-trendlabs-3q-2013-security-roundup.pdf

**2013 年第 3 季度国际安全威胁信息摘要**

❖ **隐私 VS 安全：云服务提供商如何取得平衡？**

之前针对 2013 年的安全预测中，我们认为，合法的云服务将可能会被犯罪分子滥用。不幸的是，这个预测目前已经被证实。在当前这种网络安全威胁严重的状况下，云安全 VS 客户隐私要如何权衡。
http://blog.trendmicro.com/trendlabs-security-intelligence/2013/07/05/

❖ **一个安卓手机漏洞被利用，该漏洞可能影响 99%的安卓手机用户**
**----趋势科技保障手机安全**

7 月初，安全研究人员宣布了一个新的漏洞被利用，该漏洞可能在用户未知的状况下，允许对安装的应用程序进行修改。几乎所有的安卓手机都受此漏洞影响，因为该漏洞存在于安卓系统 1.6 版本，而只有三星 Galaxy S4 已经修补了此漏洞。

http://blog.trendmicro.com/trendlabs-security-intelligence/2013/07/10/

❖ **详细说明，关于 EXPIRO 文件感染**

之前我们报道过一个比较特别的攻击，该攻击涉及到漏洞工具以及文件感染。引起我们注意到这次特别的攻击的原因是：在该攻击中被感染的文件会带有信息盗窃的代码，这在文件感染中不太常见。这种感染型病毒为 PE_EXPIRO 家族，在 2010 年首次被发现。它们可能被利用来攻击某特定组织或公司的网站。

http://blog.trendmicro.com/trendlabs-security-intelligence/2013/07/19/

❖ **关于 JAVA 本地层的漏洞利用**

最近，安全研究人员披露了两个 JAVA 本地层漏洞（CVE-2013-2465 和 CVE-2013-2471）。这使得我们寻找 java 本地层漏洞利用方法的时间更加紧迫，因为这种漏洞攻击已经变的越来越普遍。在今年的 Pwn2Own 大赛上，Joshua Drake 演示了 CVE-2013-1491 漏洞的利用，这个漏洞可以在 windows 8 系统中的 java 7 中被执行。CVE-2013-1493 变成了黑客工具中，漏洞攻击模块使用的热门的漏洞之一。

http://blog.trendmicro.com/trendlabs-security-intelligence/java-native-layer-exploits-going-up/

❖ **新的 IE 零日漏洞被利用**

距离 9 月补丁更新日仅一个礼拜时间，微软又发布了新的“Fix it”工具
http://blogs.technet.com/b/srd/archive/2013/09/17/cve-2013-3893-fix-it-workaround-available.aspx，
来解决一个新的 IE 零日漏洞（CVE-2013-3893）的问题，据报告这个零日漏洞已经在一些针对性攻击中被利用。
http://blog.trendmicro.com/trendlabs-security-intelligence/new-ie-zero-day-is-actively-exploited-in-targeted-attacks/

*更多趋势科技全球区的网络安全信息请访问：*

http://blog.trendmicro.com/trendlabs-security-intelligence

## 2013 年第 3 季度国内安全威胁信息摘要

### ❖ 7 月趋势科技 CHINA RTL 发布关于金融行业的 APT 攻击证券幽灵病毒警报

请注意“证券幽灵”恶意程序。最近，趋势科技在中国地区，发现了数起感染“证券幽灵”恶意程序的事件。该恶意程序以证券行业为目标，极度顽强和具有隐蔽性，在目标环境中已经潜伏了一段时间。我们相信这由一组专业的黑客，针对证券行业发起的一系列 APT 行为。

**相关检测：BKDR_CORUM 家族、TSPY_GOSME 家族、TROJ_JNCTN 家族及 China Pattern 通用检测 TROJ_GENERIC.APC**

http://cn.trendmicro.com/cn/about/news/pr/article/20130729063643.html

### ❖ “好声音”栏目组提醒你领大奖？ 小心是网络钓鱼陷阱

和夏季炽热的温度一块到来的，是大家对选秀节目高涨的热情。随着“中国好声音”、“超级男声”等选秀节目的热播，在电视或是电脑前守候就成了很多观众的一个习惯。同时，很多不法分子也蠢蠢欲动，并建立以中奖信息、选手隐私揭秘等为幌子的钓鱼网站来吸引用户登录，继而获利。趋势科技提醒观众在为选秀歌手呐喊助威的同时，也别忘了防范网络安全威胁。

http://cn.trendmicro.com/cn/about/news/pr/article/20130829062402.html

## 关于趋势科技

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的1,500余名趋势科技安全专家可为各国家和地区的企业级个人用户提供7×24的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问: www.trendmicro.com.cn。

TREND MICRO 趋势科技 [ 全程护航 迈向云端 ]

## 关于中国区网络安全监测实验室

趋势科技“中国区网络安全监测实验室”是国际杀毒厂商中第一家针对“中国特色病毒”提供解决方案的监测机构。通过 MOC 监控中心和 SPN 数据分析中国区用户的网络安全状况，主动收集中

国地区的病毒样本，对病毒样本进行快速分析，发布专门针对中国地区的病毒码(China Pattern)和解决方案，大幅提高对中国区病毒的查杀率。为中国地区用户提供更广泛、及时、有效的反病毒支持。趋势科技“中国区网络安全监测实验室”利用趋势科技的全球资源优势以及自身的高技术人员资源，真正帮助中国区用户解决病毒危机，营造安全的网络环境。倾力服务中国用户。

ChinaRTL
中国区网络安全监测实验室