中国地区 2013 年

第二季度

网络安全威胁报告

2013/8

CHINA RTL

目录

2013 年第 2 季度安全威胁

本季安全警示：

后门/间谍软件，漏洞攻击，APT

2013 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 2013.6.30 日中国区传统病毒码 **10.124.60** 包含病毒特征数约 **450** 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 **5400** 万次。
- 本季度趋势科技在中国地区拦截的恶意 URL 地址 **109,344,203** 次。

2013 年第 2 季度，中国地区病毒检测数量稳中有降，并没有大规模的病毒爆发事件。但传统病毒的检测数量持续降低，并不能够完全代表目前中国地区互联网安全状况。在第 2 季度初始，各种针对中国的 APT 报告频出，各国之间网络攻击事件也时有发生。利用漏洞的攻击数量持续上升，恶意网站以及挂马网站数量也在增加。另外，安卓系统病毒快速增长，移动通讯设备的安全问题同样不容忽视。在一些旧的安全威胁尚未解决的同时，我们还需要面对新型攻击，此时应该意识到当前国内的互联网安全状况表面平静实则汹涌。迫切需要将互联网安全防护意识，关注程度，以及防护措施措施提高到一个新的高度。

第 2 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。

在第 2 季度，并没有新的高危险病毒爆发。值得注意的是 **PE_SALITY** 又有了更新，这只 2010 年就已经出现的病毒不但具有感染.EXE 以及.SCR 的能力。并且会破坏，终止安全软件，能够对感染电脑进行远程控制，破坏性不容小觑。

本季度 PE 病毒感染情况仍然严重：

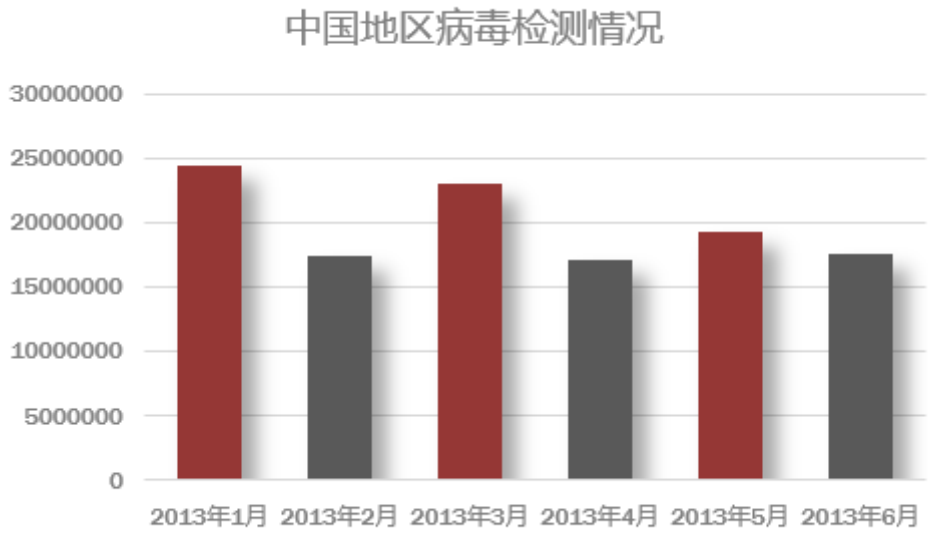
PE_PATCHED.ASA 仍占据病毒检测数量排名首位，该病毒为被修改的 sfc_os.dll，sfc_os.dll 是用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能，该文件被修改预示着有其他会修改系统文件的恶意行为可能将会发生。

PE_SALITY.ER，**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**),快捷方式漏洞也可能通过邮件到达被感染客户端。 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。

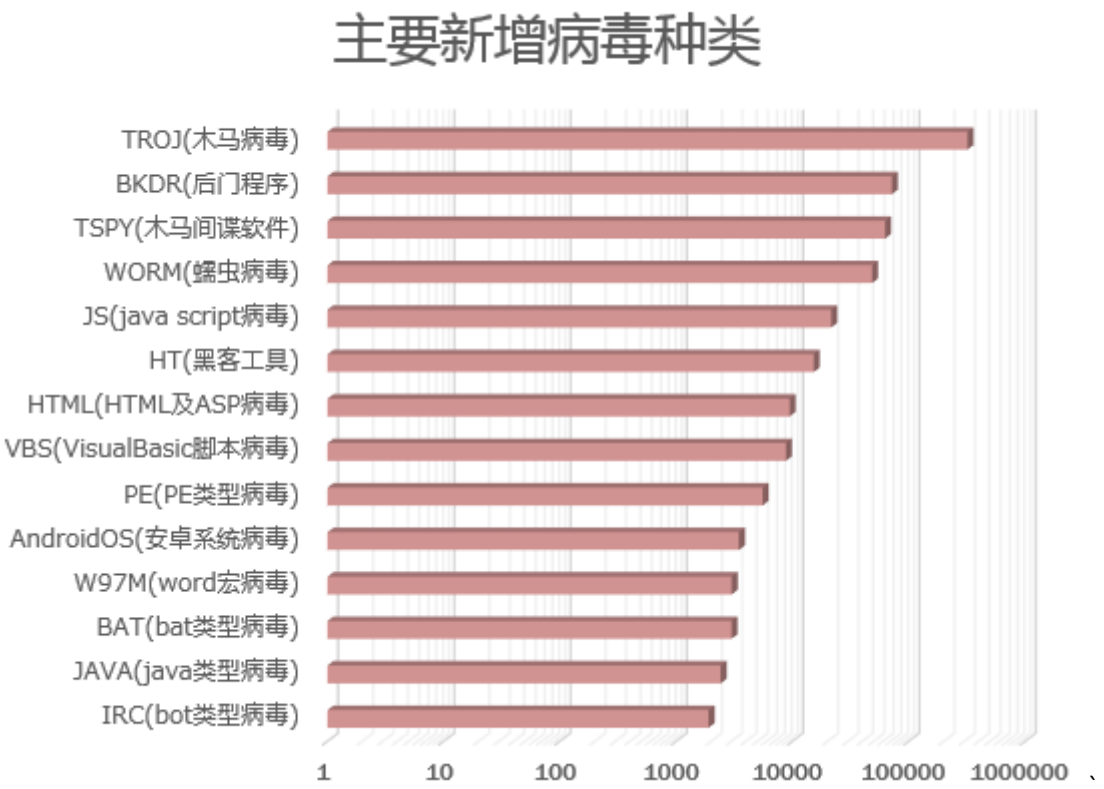
BKDR_BIFROSE，该病毒执行远程恶意用户的命令，有效地攻击受感染的系统。会连接到网站，发送和接收信息。此病毒目前检测数量及流行范围排名均在上升，需要密切关注。

在 2013 年第 2 季度趋势科技拦截新的恶意网站中钓鱼网站约有 **2300** 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 2 季度病毒威胁情况

2013 年第 2 季度新增病毒类型分析



2013 第 2 季度中国地区新增病毒类型

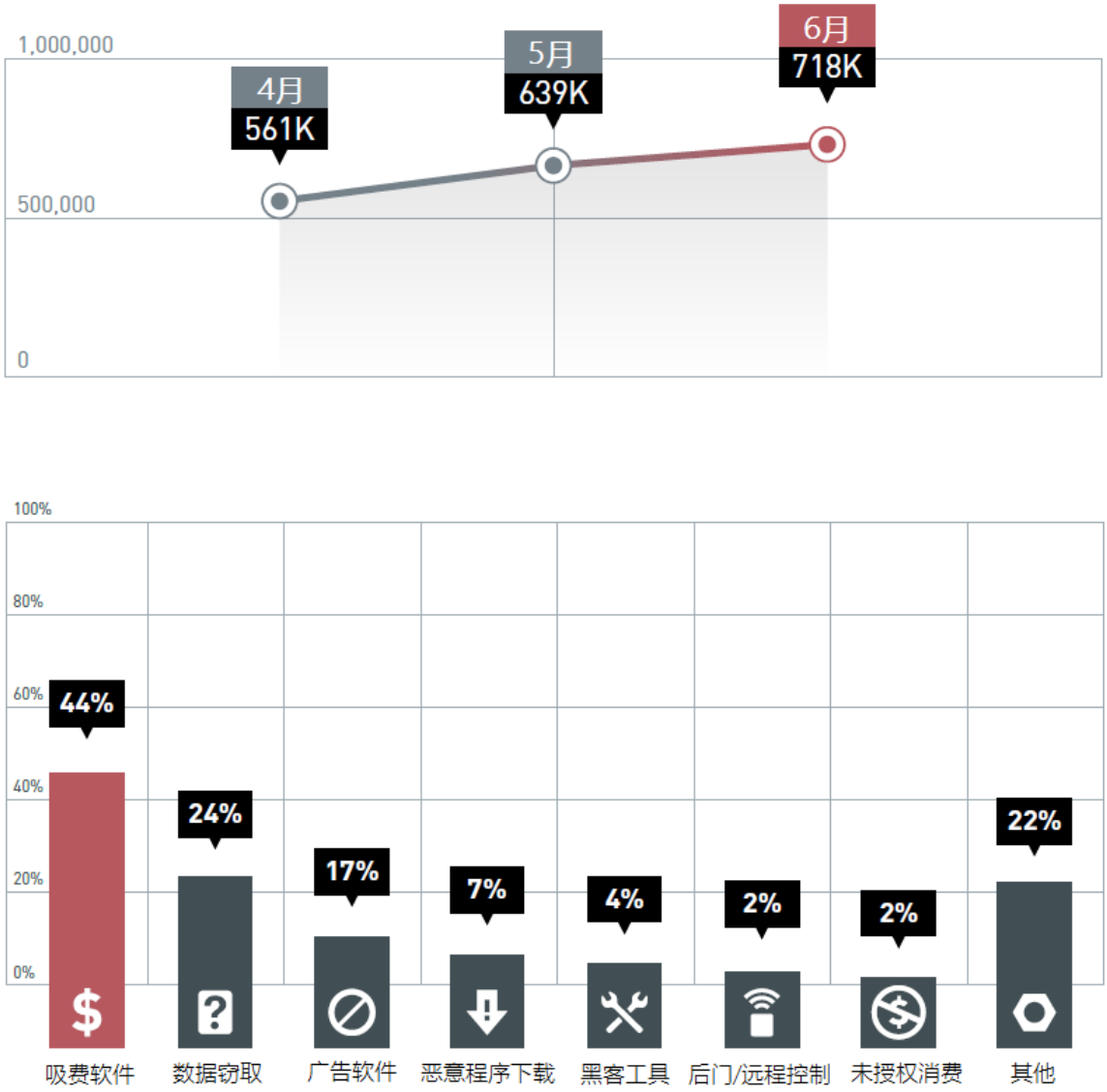
新增的病毒类型最多的仍然为木马（TROJ），本季度新增木马病毒特征 **319734** 个，比上季度略有下降。木马可使病毒制造者更直接的获利，在经济利益的驱使下大量的木马被制造并通过各方式被传入互联网中。木马也是我国目前存在数量最多的病毒类型。

本季度新增的病毒类型中，处于上升趋势的病毒类型为 **WORM(蠕虫病毒)**，**JS(java script 病毒)**，**HT(黑客工具)**，**HTML(HTML 及 ASP 病毒)**，**VBS(VisualBasic 脚本病毒)**，**AndroidOS(安卓系统病毒)**，其中趋势科技定义以 HT_开头的检测类型为黑客工具。目前，有越来越多的数据表明一些网络攻击中使用的黑客工具，源自中国黑客组织。黑客工具在网络攻击和病毒传播中起着重要的作用，对此类检测需要引起重视。

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站中，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，通过向网页插入恶意代码，网络罪犯可以进一步获得网站的 webshell ，甚至使他们能够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 AndroidOS(安卓系统病毒)数量，在 2013 年第二季度持续上升。2013 年 6 月爆出的安卓平台漏洞‘master-key’，使安卓平台的系统安全问题雪上加霜。

第 2 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 44%，信息窃取程序上升到第二名的位置占 24%,第三名为广告软件。



2013 第 2 季度安卓平台病毒类型排名

2013 年第 2 季度各类型病毒检测情况分析

2013 第 2 季度中国地区各类型病毒检测数量比例图

2013 年第 2 季度检测到的病毒种类中 PE 类型病毒感染数量又有上升。大约占到总检测数量的 65%。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 2 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。由于 sfc_os.dll 文件是系统文件，防毒软件强行查杀可能会导致系统崩溃.此外 PE 病毒通常会感染系统中所有的可执行文件。一旦被感染，系统中多数文件都会被检测。

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 1 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。

2013 年第 2 季度病毒拦截情况分析

2013 第 2 季度中国区拦截次数排名前 20 病毒

上图显示了 2013 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。

2013 年第 2 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 370 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种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 4 名的 PE_PARITE,WORM_DOWNAD,以及 PE_SALITY，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。

BKDR_BIFROSE

BKDR_BIFROSE 是一种后门病毒，它具有超过 10 个变种。通常会作为一个客户端连接远程的恶意服务器。恶意程序释放者能够通过远程指令对被感染电脑进行控制以及攻击。

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 ，或者由恶意的钓鱼邮件或垃圾邮件附件夹带。

修改系统内容：

该病毒可能在系统中释放以下文件：

%ProgramFiles%\bifrost\server.exe
%System%\cdndll.exe
%System%\cmdd.exe
%System%\explor.exe
%System%\gdiplus.exe
%System%\jusched.com
%System%\kjset.exe
%System%\lcass.exe
%System%\lmao.exe
%System%\microvido.com
%System%\msn.exe
%System%\new.exe
%System%\photo.exe
%System%\piji.exe
%System%\qsservice.exe
%System%\server.exe
%System%\server_poison.exe
%System%\svchost32.exe
%System%\system.exe
%System%\system12.exe
%System%\system32.exe
%System%\umgr32.exe
%System%\update.exe
%System%\windows_32.exe
%System%\winlive.exe
%System%\winload.exe
%System%\winupd.exe
%System%\xjbl998.exe

%Temp%\20080612\20080612_1.exe
%Temp%\613818.exe
%Temp%\665716.exe
%Temp%\808561.exe
%Temp%\82708.exe
%Temp%\828580.exe
%Temp%\852578.exe
%Temp%\decrypted.exe
%Temp%\exe.exe
%Temp%\exporer32.exe
%Temp%\h.exe
%Temp%\ixp000.tmp\setup.exe
%Temp%\server.exe
%Temp%\temp2.exe
%Temp%\tmp.exe
%Temp%\wh674ew7h47h.exe
%Windir%\53341winrar.exe
%Windir%\logo.exe
%Windir%\msnmgr.exe
%Windir%\nod321.scr
%Windir%\scvhost.exe
%Windir%\server1.exe
%Windir%\sp0olsv.exe
%Windir%\sql.exe
%Windir%\svchost.exe
%Windir%\sys.exe
%Windir%\system32:camview.exe
%Windir%\system32:connect.exe
%Windir%\system32:dang.exe
%Windir%\system32:dllload.exe
%Windir%\system32:explorer.exe
%Windir%\system32:game.exe
%Windir%\system32:iexplorers.exe
%Windir%\system32:msi10.exe
%Windir%\system32:mswinxs29.exe
%Windir%\system32:svchost.exe
%Windir%\system32:system.exe
%Windir%\system32:system32.exe
%Windir%\system32:updatesvp.exe
%Windir%\system32:updatetmsv.exe
%Windir%\system32:winzocks.exe
%Windir%\system32:xjiher.exe
%Windir%\winaudio.exe

c:\99.exe
c:\windows:msfirewall.exe
c:\windows:msnmsgs.exe
c:\windows:split.exe
c:\windows:svchost.exe

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吗及时的更新
2. 使用爆发阻止策略阻止上述提到的恶意程序

TROJ_SERVSTAR.JG

TROJ_SERVSTAR 是一种窃取用户帐号信息的木马程序。它带有键盘记录功能，记录信息包括被感染电脑的用户名，密码，信用卡等信息。它会和远程恶意 URL 连接传送恶意病毒释放者的命令或上传窃取的信息。

通过 8080 端口访问 xi*****.3322.org

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。

修改系统内容：

创建以下注册表键项：
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MSUpdqte
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MSUpdqte\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSUpdqte
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSUpdqte\Security

添加以下注册表键值：
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MSUpdqte

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MSUpdqte\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSUpdqte
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSUpdqte\Security

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MSUpdqte\Security]
Security = 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01 00 00 00 00 00 05 12 00 00 00 00 00 18 00 FF 01 0F 0
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\MSUpdqte]
Type = 0x00000010
Start = 0x00000002
ErrorControl = 0x00000000
ImagePath = "%ProgramFiles%\srchasst\svchost.exe"
DisplayName = "Microsoft Windows Uqdate Service"
ObjectName = "LocalSystem"
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSUpdqte\Security]
Security = 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01 00 00 00 00 00 05 12 00 00 00 00 00 18 00 FF 01 0F 0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSUpdqte]
Type = 0x00000010
Start = 0x00000002
ErrorControl = 0x00000000
ImagePath = "%ProgramFiles%\srchasst\svchost.exe"
DisplayName = "Microsoft Windows Uqdate Service"
ObjectName = "LocalSystem"

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：

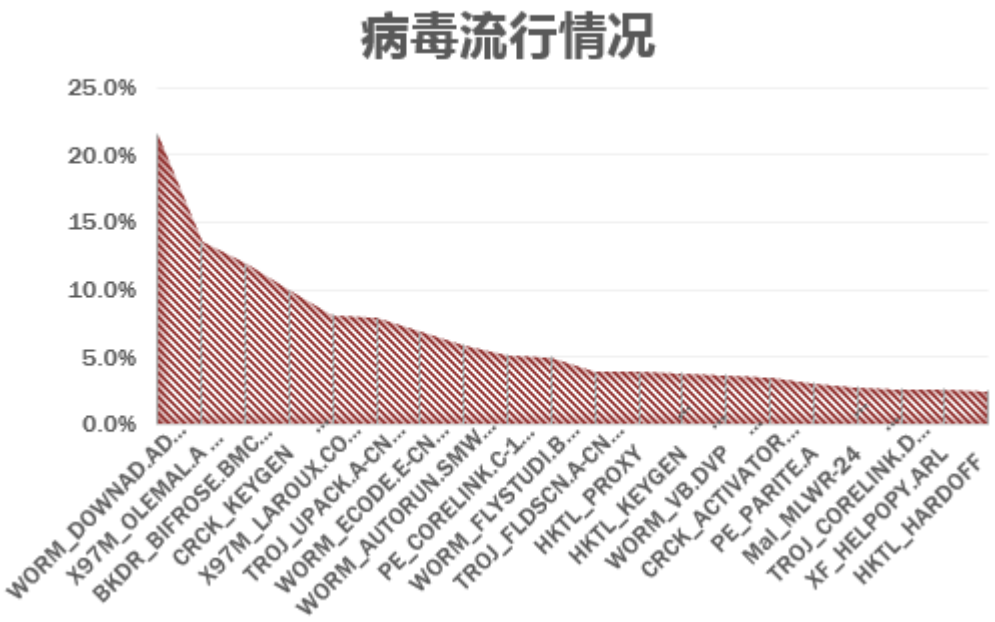
32 位 windows 操作系统请使用：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage.exe

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吗及时的更新
2. 从网关防火墙阻止恶意地址的访问
3. 使用爆发阻止阻止在 %ProgramFiles%\srchasst\创建 svchost.exe 文件

2013 年第 2 季度流行病毒分析



2013 第 2 季度中国地区病毒流行度排名

2013 年第 2 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 2 季度，仍约有 20% 以上的用户遭受到此病毒的攻击。

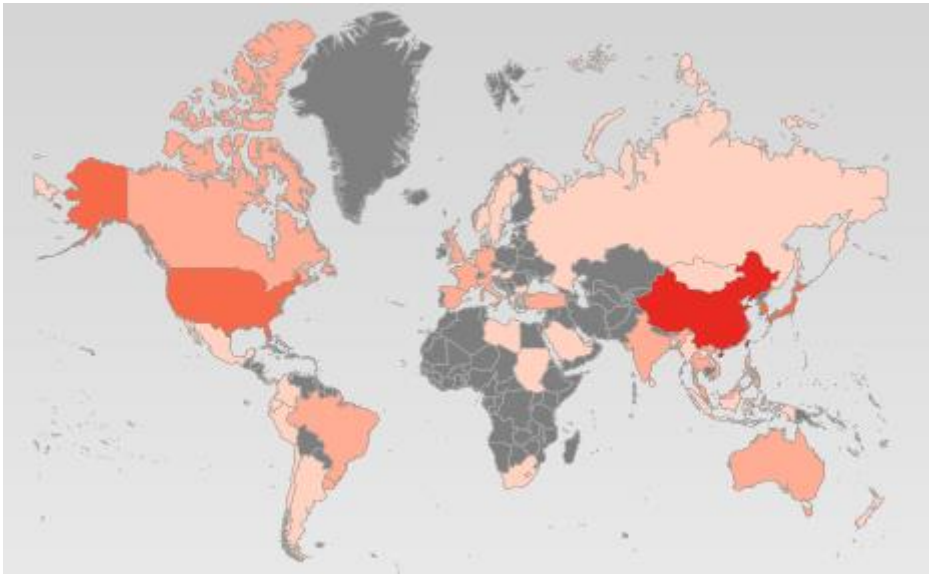
目前的防病毒产品都能够检测并处理这些病毒，网络内一直有这种病毒存在，说明环境存在某些安全缺陷，使得病毒能够进入并且持续存活，针对这种情况需要及时处理和分析。

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 2 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

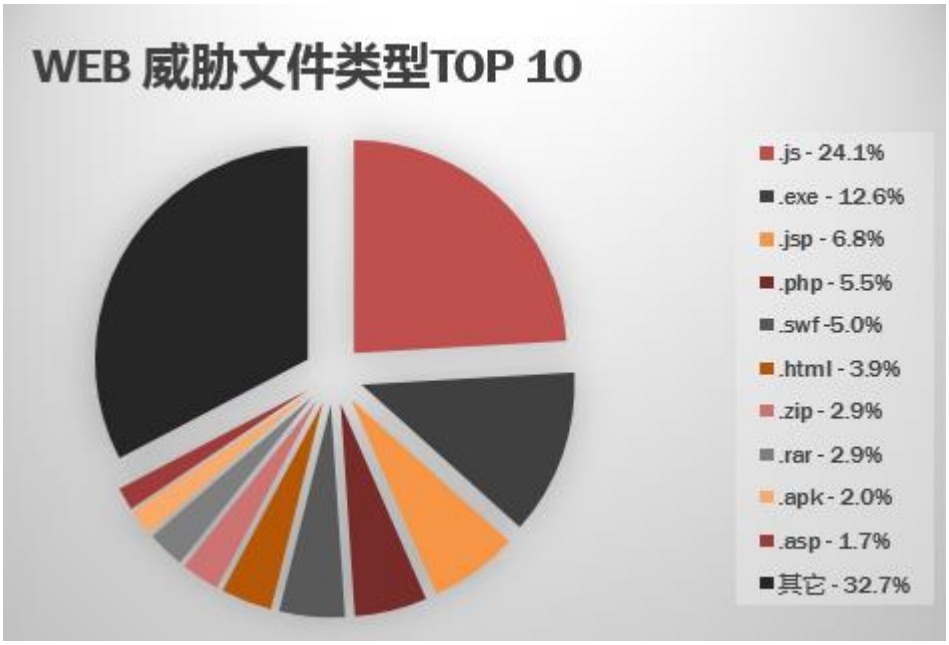
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2013 年第 2 季度 web 安全威胁情况

2013 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 **24.3%**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。



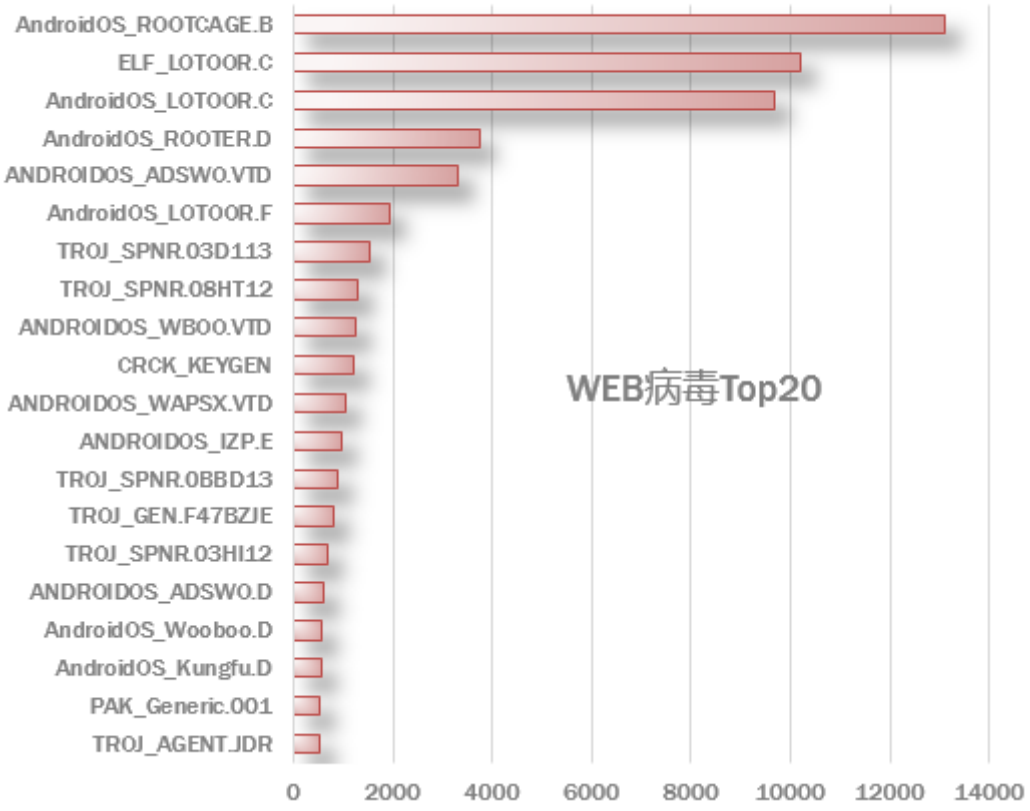
2013 第 2 季度中国地区 web 威胁文件类型

2013 年第 2 季度 top10 恶意 URL

TOP 10 恶意URL		
恶意URL	描述	点击量
hxxp://211.98.**.195/wpad.dat	模仿合法网站收集敏感信息的诈骗站点，例如收集用户名和密码	1749436
hxxp://di**.**186.com/dm.php?uid=16&tid=1&ref=1	该网站的地址在垃圾邮件中被发现	1567167
hxxp://denis.s***lker.h**.com	网站直接或间接帮助传播恶意软件或恶意代码	1045214
hxxp://123.1**.203.**:80/	网站直接或间接帮助传播恶意软件或恶意代码	974992
hxxp://h.98yyw.com/ad/adrd_config2.xml	网站直接或间接帮助传播恶意软件或恶意代码	673530
hxxp://221.130.***.177/04133_shashou5shemian.gmz	模仿合法网站收集敏感信息的诈骗站点，例如收集用户名和密码	671777
hxxp://js.yi***.com/i.js	网站提供恶作剧程序的下载，包括那些扰乱用户的应用程序	545314
hxxp://treezip.***feng.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	544611
hxxp://da*****forum.com/data/image/gate.php	网站直接或间接帮助传播恶意软件或恶意代码	533718

2013 第 2 季度中国地区已被 wrs 阻止的恶意 url 排名

2013 年第 2 季度 Web 威胁病毒类型分析



2013 第 2 季度中国地区 web 病毒 top20

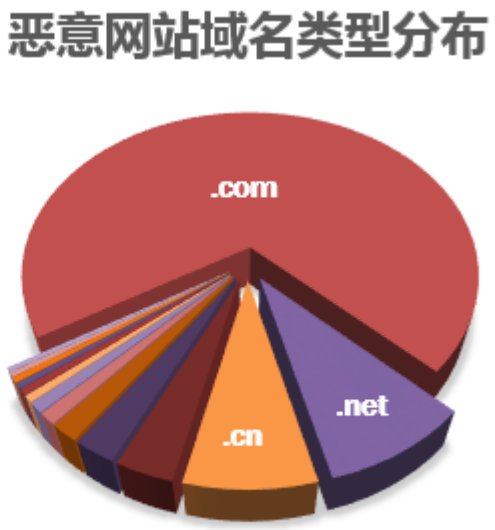
通过对拦截的 Web 威胁进行分析，我们发现。2013 年第 2 季度安卓平台的恶意软件检测数量大幅度提升。检测数量排名前五的病毒均为安卓平台病毒。 使用者需要尽量安装手机安全产品，尽量从可信的安卓市场中下载安装程序。程序安装过程中仔细观察安装画面，发现有不正常的权限请求时及时中止安装过程。

破解软件常常携带有木马被用户下载，在用户安装破解软件时往往在不知不觉中同时将木马安装到电脑上。并且不容易被发现。

间谍软件和后们程序在第 2 季度开始增长，用户需要在访问网站时留意，尽量在正规网站下载程序。接受到未知发件人的邮件时请勿轻易点击邮件中的链接，以防止下载到恶意程序。

2013 年第 2 季度 web 威胁域名分布

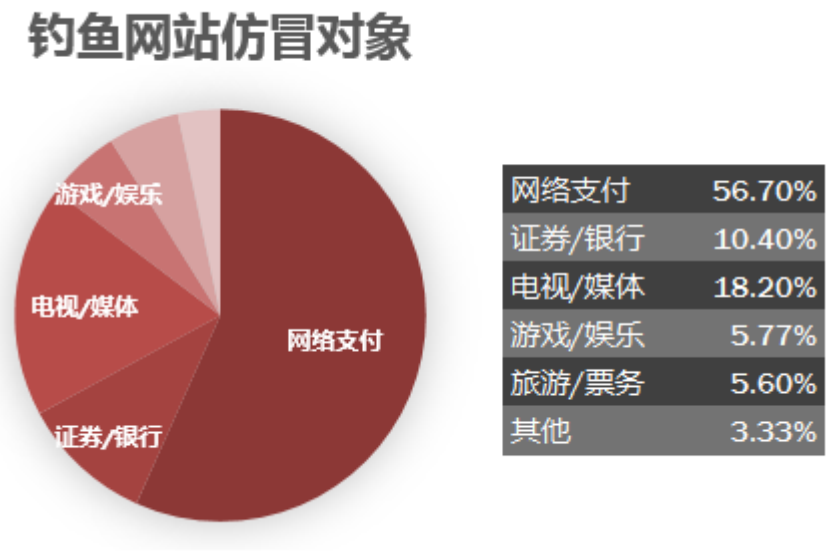
.com	58.8%
.net	7.4%
.cn	6.4%
.ru	2.9%
.org	2.1%
.de	1.4%
.cc	0.9%
.info	0.8%
.uk	0.5%
.us	0.5%
.nl	0.4%
.in	0.4%
.ua	0.3%
.kr	0.3%



2013 第 2 季度中国地区恶意域名类型分布

第 2 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 72.6%。其中.com 域名下的恶意页数量最多。

2013 年第 2 季度 Web 威胁钓鱼网站仿冒对象分析



2013 第 2 季度中国地区钓鱼网站仿冒对象

从第 2013 年第 2 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站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 2 季度漏洞攻击威胁情况

漏洞编号	拦截攻击次数
CVE-2008-4250	1520140
CVE-2009-1140	1520122
MS09-019	1520122
CVE-2010-0870	1128426
CVE-2008-2894	1018990
CVE-2010-3970	15420
CVE-2011-0026	4476
CVE-2011-0027	4476
CVE-2010-3145	4016
CVE-2007-6250	4012

2013 第 2 季度中国地区漏洞攻击检测情况

CVE-2008-4250	http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-4250
CVE-2009-1140	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1140
MS09-019	http://www.microsoft.com/technet/security/Bulletin/MS09-019.mspx
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-2010-3970	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3970
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
CVE-2007-6250	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6250

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 2 季度最新安全威胁信息

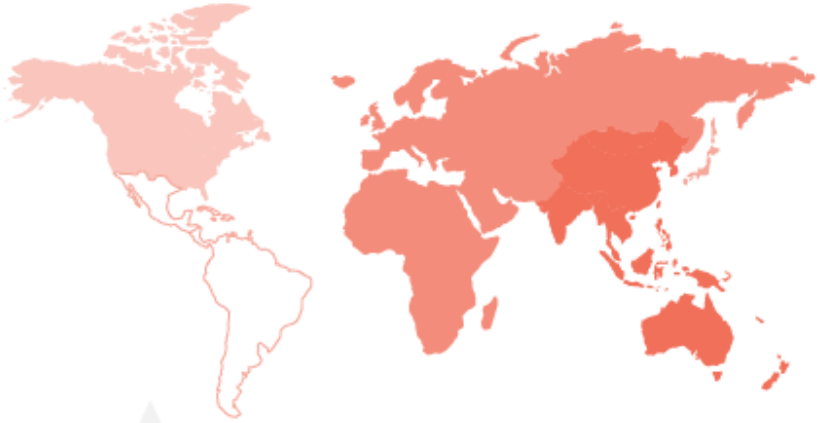
2013 年第 2 季度趋势科技全球区安全威胁概要

全球 TOP3 病毒

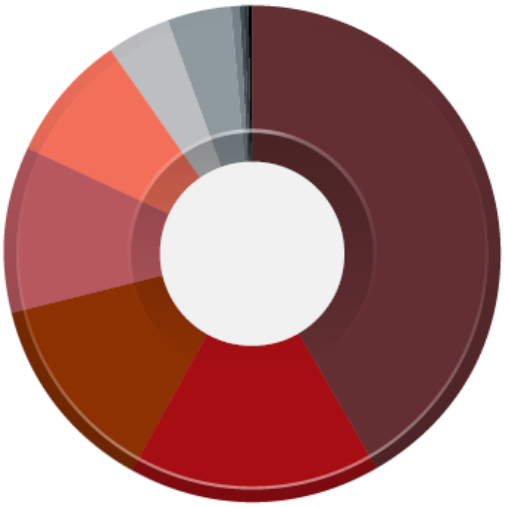
WORM_DOWNAD	509K
APAC	51%
EMEA	19%
LAR	15%
NORTH AMERICA	9%
JAPAN	6%

ADW_BHO	448K
JAPAN	34%
APAC	26%
EMEA	19%
NORTH AMERICA	17%
LAR	4%

ADW_BPROTECT	311K
APAC	28%
EMEA	28%
JAPAN	20%
NORTH AMERICA	15%
LAR	9%

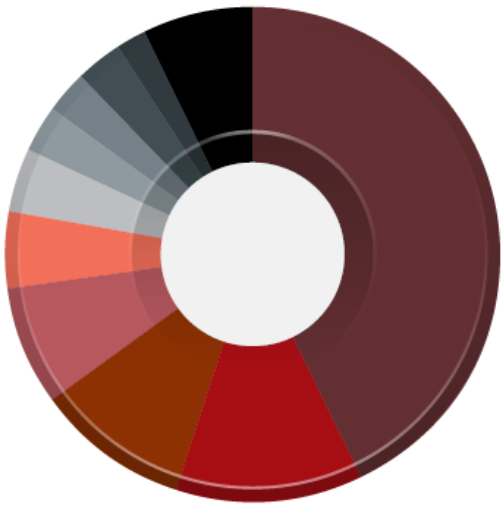


全球安卓系统广告软件家族 TOP10



1	ARPUSH	41.79%
2	ADSWO	16.50%
3	PLANKTON	12.84%
4	LEADBLT	11.02%
5	IZP	8.17%
6	WAPSX	4.25%
7	OQX	4.10%
8	WBOO	0.67%
9	YOUMI	0.27%
10	UAPSH	0.13%
	Others	0.26%

具有针对性攻击的鱼叉式钓鱼中使用到的文件类型排名



1	EXE/DLL	43%
2	PDF	12%
3	DOC	10%
4	JPG	8%
5	TXT/HTML	5%
6	RTF	4%
7	ZIP	3%
8	XLS	3%
9	RAR	3%
10	PPS/PPT	2%
	Others	7%

全球恶意 url 检测数量排名

	国家 COUNTRY	SHARE
1	United States 美国	25.90%
2	Germany 德国	3.24%
3	China 中国	3.16%
4	Netherlands 荷兰	3.13%
5	South Korea 韩国	2.60%
6	France 法国	1.94%
7	Japan 日本	1.93%
8	Russia 俄罗斯	1.64%
9	Canada 加拿大	0.81%
10	United Kingdom 英国	0.77%
	Others 其他	54.88%

全球僵尸网络 C&C 服务器数量排名

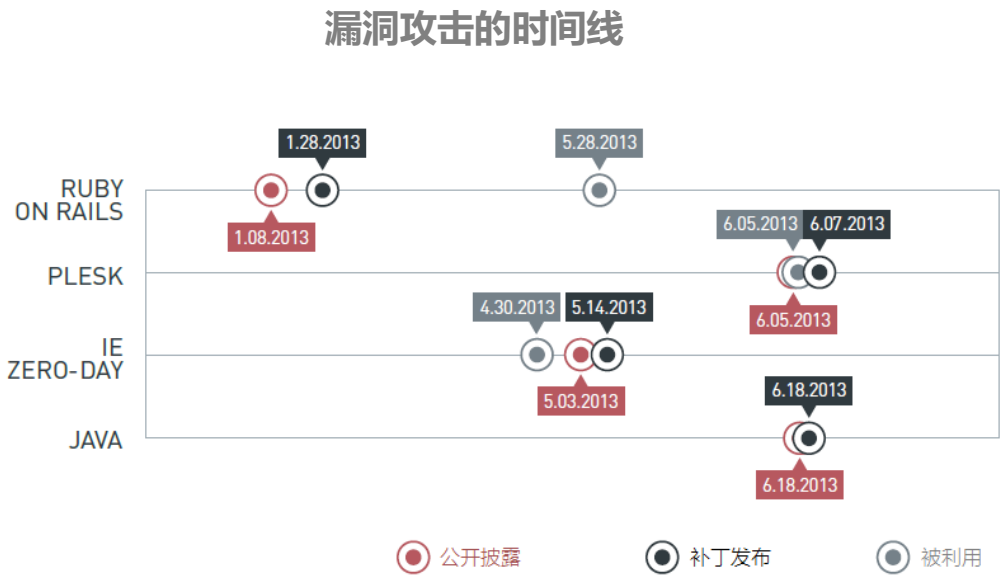
	地区	SHARE
1	United States 美国	24.05%
2	Australia 澳大利亚	5.15%
3	South Korea 韩国	3.38%
4	China 中国	3.02%
5	Germany 德国	2.87%
6	Taiwan 台湾	2.10%
7	France 法国	1.88%
8	United Kingdom 英国	1.72%
9	Brazil 巴西	1.47%
10	Canada 加拿大	1.18%
	Others 其他	53.18%

全球僵尸网络 C&C 连接数量排名

	地区	SHARE
1	Malaysia 马来西亚	28.39%
2	United States 美国	14.14%
3	France 法国	11.63%
4	Germany 德国	5.64%
5	Canada 加拿大	5.29%
6	South Korea 韩国	4.13%
7	United Kingdom 英国	3.84%
8	Thailand 泰国	3.22%
9	Hong Kong 香港	3.07%
10	Italy 意大利	2.53%
	Others 其它	18.12%

介于上季度大量零日漏洞被爆出，Oracle 采取了一系列的措施来改善 JAVA 的安全性。其中包括： 季度更新发布，自动安全检测，以及不允许自签名或未签名的 JAVA APP 在浏览器中使用。

尽管在这个季度，漏洞比上季度有所减少但是仍然有一些漏洞被利用，并且给用户带来了极大的威胁。IE8 的零日漏洞被利用攻击了美国能源部以及劳工部门的计算机系统。Ruby on Rails 的漏洞被利用来制造僵尸网络。Adobe 的 Plesk ColdFusion 平台被利用漏洞攻击。



需要查看更完整的第 2 季度全球安全报告请访问：
http://about-threats.trendmicro.com/us/security-roundup/2013/2Q/mobile-threats-in-full-throttle/#

2013 年第 2 季度国际安全威胁信息摘要

- **僵尸网络死而复生**

  虽然垃圾邮件僵尸网络是以发送不受欢迎的广告邮件着称，尤其是那些卖假药的公司，但他们同时也是散播恶意软件不可或缺的一部分。除了发送自己的恶意软件好提高自己僵尸网络的规模，安装其他的恶意软件也让这些幕后黑手们可以通过按次付费安装模式来赚钱。

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

- **倒数计时：windowsXP 系统支持仅剩一年**

  根据微软的说法，Windows XP 已经正式接近尾声了。还有不到一年，就会在 2014.4.8 结束对这十一岁的操作系统的官方技术支持

  http://blog.trendmicro.com/trendlabs-security-intelligence/on-borrowed-time-windows-xp-support-expires-in-under-a-year/

- **WordPress 暴力攻击影响数千网站**

  许多用 WordPress 架设的博客都遇到大规模的暴力攻击。这些攻击使用暴力破解法来登录 WordPress 控制台，并将恶意代码写入被入侵的博客和网站上。

  http://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-wordpress-attacks-affect-thousands-of-sites/

- **韩国政府的 DNS 服务器遭到攻击**

  6 月 25 日韩国政府的 DNS 服务器遭到 DDOS 攻击

  http://blog.trendmicro.com/trendlabs-security-intelligence/south-korean-government-dns-servers-targeted-by-ddos-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 2 季度国内安全威胁信息摘要

- **趋势科技联手腾讯手机管家 公布安卓手机病毒“权限杀手”疫情**

  近日，国内知名手机安全软件腾讯手机管家与全球云安全领导厂商趋势科技联合公布了一款安卓 ROM 内置手机病毒“权限杀 手”。该病毒拥有系统最高权限，可自动删除手机中 superuser.apk 和 su 文件，禁止其他应用获取 Root 权限，导致用户无法通过 Root 手机删 除该病毒文件。

  http://blog.iqushi.com/index.php/archives/2399

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