中国地区 2014 年
第四季度
网络安全威胁报告

2015/1

CHINA RTL

目录

2014 年第 4 季度安全威胁

本季安全警示：

信息泄露，移动设备安全

2014 年第 4 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 **52** 万条。截止 2014.12.31 日中国区传统病毒码 **11.378.60** 包含病毒特征数约 **366** 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 **12,978** 万次。
- 本季度趋势科技在中国地区拦截的恶意 URL 地址共计 **25,569,465** 次。

近年来国内外有关**信息泄露**的事件频频发生，此类事件影响范围往往规模巨大，泄密信息与受害者的个人日常生活密切相关，包括个人的基本信息、健康信息甚至是财富情况等等。这类信息一旦泄露，对受害者来说影响深远。在 2014 年第 4 季度发生的几起信息泄露事件引起了媒体不小的关注。2014 年 12 月份，国内某知名漏洞报告平台曝出中国铁路客户服务中心 12306 网站用户数据遭到泄露，大量用户账号、密码、邮箱等信息以明文方式在网络上公开传播。而 12 月份正值购买春运火车票的高峰期，消息一经发布便引起了极大关注。铁路公安机关之后迅速抓获了犯罪嫌疑人，并证实此次事件中爆出的数据都是由嫌犯通过“撞库”的方式获取。所谓“撞库”，就是指黑客利用已经获得的用户名和密码信息（通常从非法渠道获取）建立起数据库，然后开始对其它网站进行大批量的尝试性登陆，以此种方式即可建立起对其它网站的用户数据库。因此，如果用户在不同网站使用同样的用户名和密码的话，就极有可能受到“撞库”攻击的影响而造成账户泄漏。

在 12306 事件之前，本季度还发生过其它信息泄露事件，如 2014 年 11 月份爆出的 130 万考研考生信息泄露。此外在全球范围内，也有媒体报导涉及政府机构网站、知名社交网站，及零售业、金融行业、娱乐行业等等信息泄露事件。种种事件都提醒用户对账户信息安全需引起重视，我们建议用户养成以下习惯以保障账户安全：

- ✓ 重要网站（特别是涉及资金账户的网站）的密码必须独立且具有一定强度
- ✓ 尽量不要在公共场合使用没有加密的无线网络
- ✓ 及时打上系统及程序的漏洞补丁
- ✓ 安装安全软件，确保安全软件保持最新的病毒码

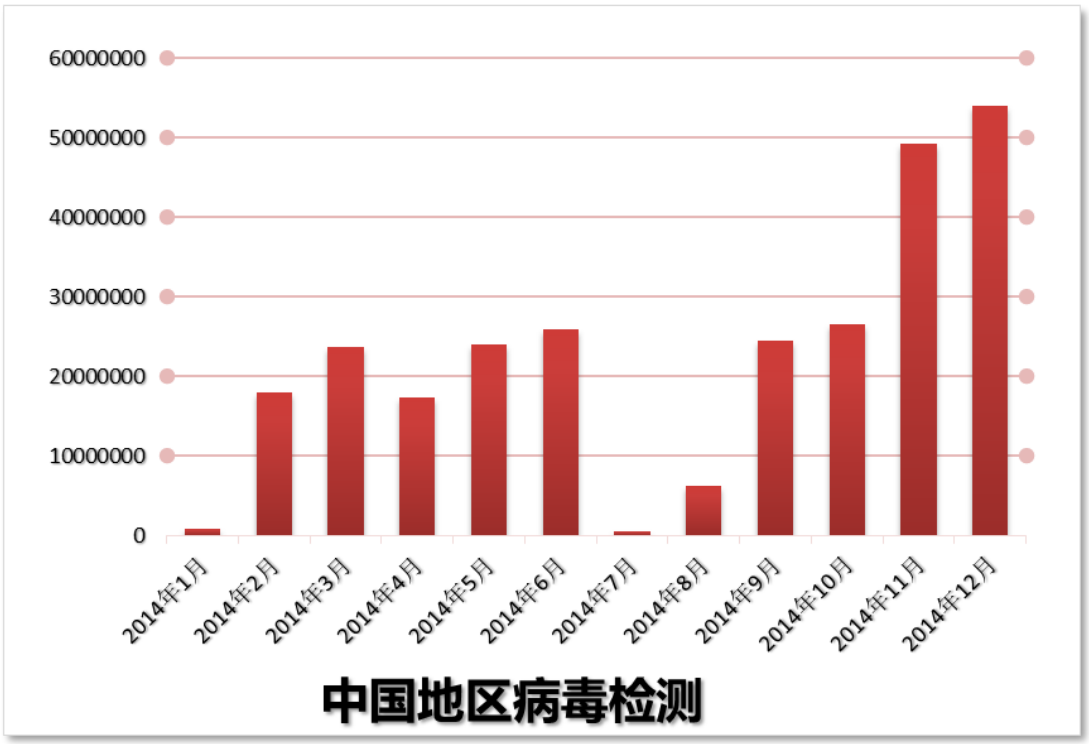
如今，智能手机的飞速发展给现代生活带来在过去无法想象的便利，随之而来的，公众对于个人电脑上信息安全的关注度逐渐转移到**移动设备安全**上。在 2014 年第 4 季度爆出的

一个名为 WireLurker 家族的病毒，因其可以感染苹果 iOS 设备而受到广泛关注。据悉，自 2014 年 4 月起，已有数十万的用户发现从第三方应用商店下载了被感染的应用后不幸受到感染，此次感染范围集中在中国地区。该病毒具有监控设备、自动下载其它应用的行为。趋势科技已将该家族病毒检测为 OSX_WIRELURK.A。我们建议，对于使用苹果设备用户应注意以下事项：

- ✓ 不要越狱 iOS 设备。
- ✓ 确保 Mac 和 iOS 保持最新的更新状态。
- ✓ 不要安装任何盗版软件或不受信任来源的软件。只安装从官方应用商店下载的软件。
- ✓ 确保 iOS 设备连接的是受到信任的计算机。
- ✓ 删除 iOS 设备上任何可疑的配置文件。
- ✓ 仔细检查任何 iOS 应用提出的权限请求：访问摄像头、通讯录、麦克风、位置信息和其他敏感数据。

对于企业用户来说，需注意以下事项：

- ✓ 妥善保管私钥。
- ✓ 确保仅有需求的员工才能够访问私钥。
- ✓ 拒绝已经离职的员工或团队成员提出的访问私钥请求。
- ✓ 重视企业授权应用的安装请求。仅允许来自可靠来源的应用安装到设备上。
- ✓ 如果察觉到私钥有被泄露的可能，尽快撤销证书。

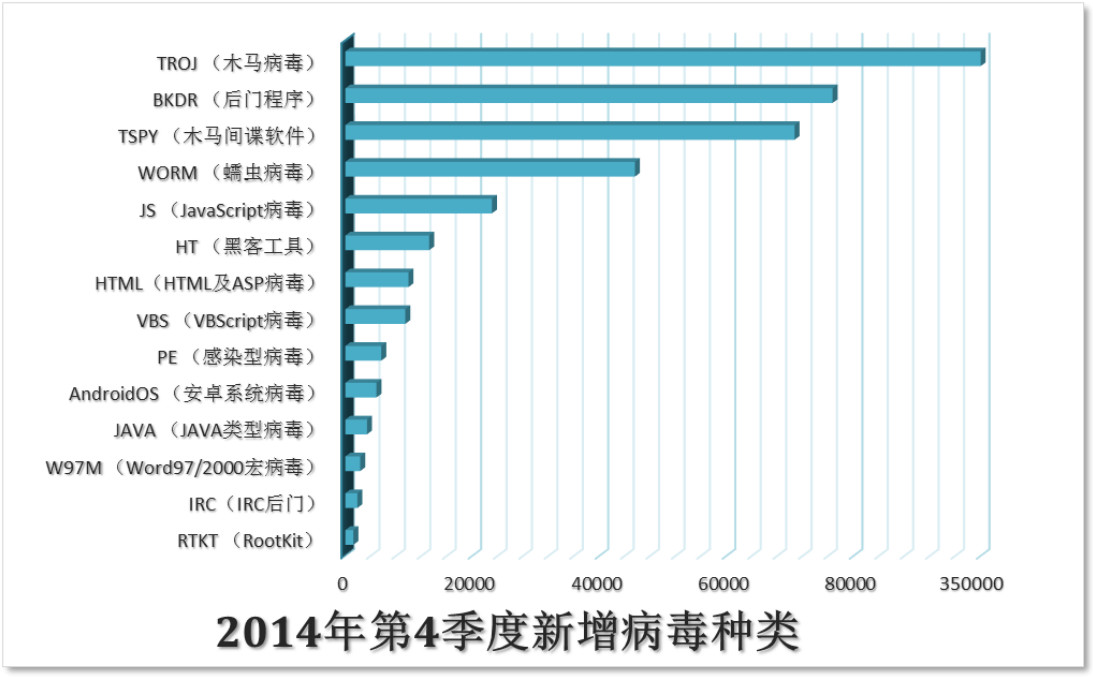


2014 年第 4 季度中国地区病毒检测数量图

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。

2014 年第 4 季度病毒威胁情况

2014 年第 4 季度新增病毒类型分析



2014 年第 4 季新增病毒类型分布图

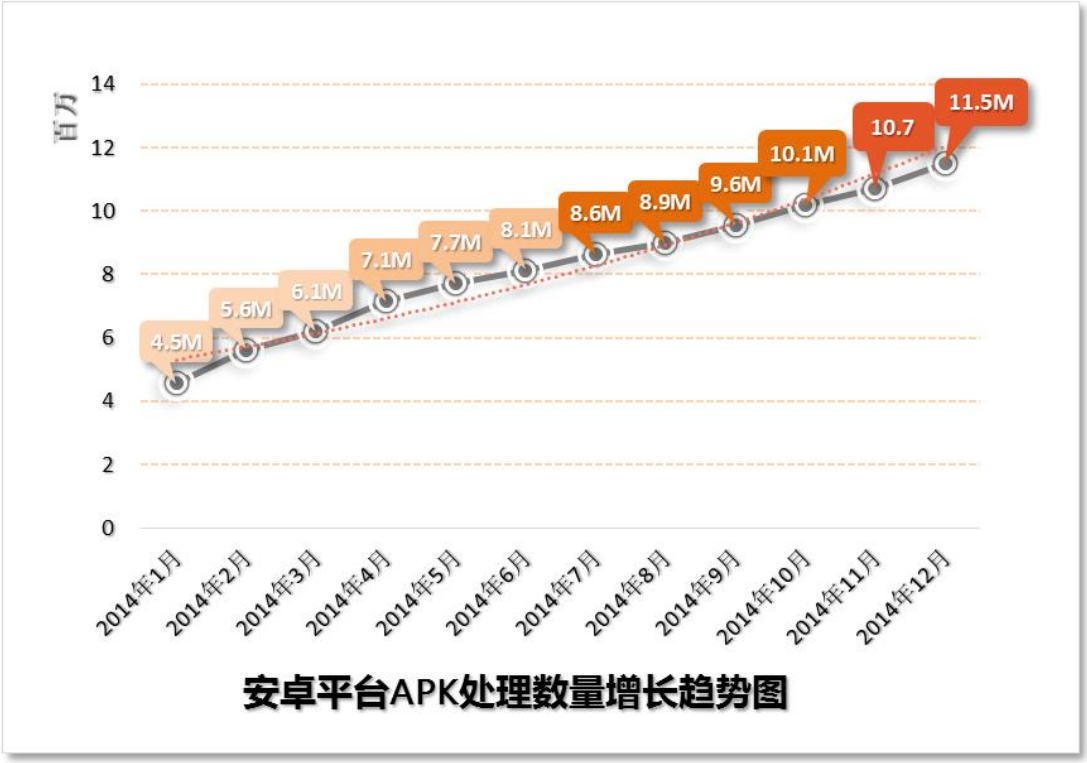
在 2014 年第 4 季度新增病毒种类中，以 **TROJ（木马病毒）**类型增幅最大。据统计，本季度新增木马病毒特征共计 **348,928** 个，与上一季度相比略有减少。木马病毒通常以窃取攻击目标的账户密码为目的，从而获得经济利益。在中国地区，此类型病毒一直高居榜首。

与上一季度相似，在木马病毒类型之后，增加数量较多的病毒类型依次为 **BKDR （后门程序），TSPY（木马间谍软件），WORM（蠕虫病毒），JS（JavaScript 病毒）和 HT（黑客工具）。**本季度新增病毒种类排名无明显变化。

JS (JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒通常和网页挂马相关。普通用户一旦访问被上传了恶意代码的网站，就会自动下载病毒到本机，对网站浏览者来说造成极大威胁。

在本季度中，以 HT_开头的定义为“黑客工具”的检测类型排名依旧靠前。现在黑客工具的获取途径十分简单，从网络黑市上就能购买。对于企业来说，及时为系统和程序打上漏洞补丁、采用强密码账户，都是有效防止外部攻击的方法。

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。

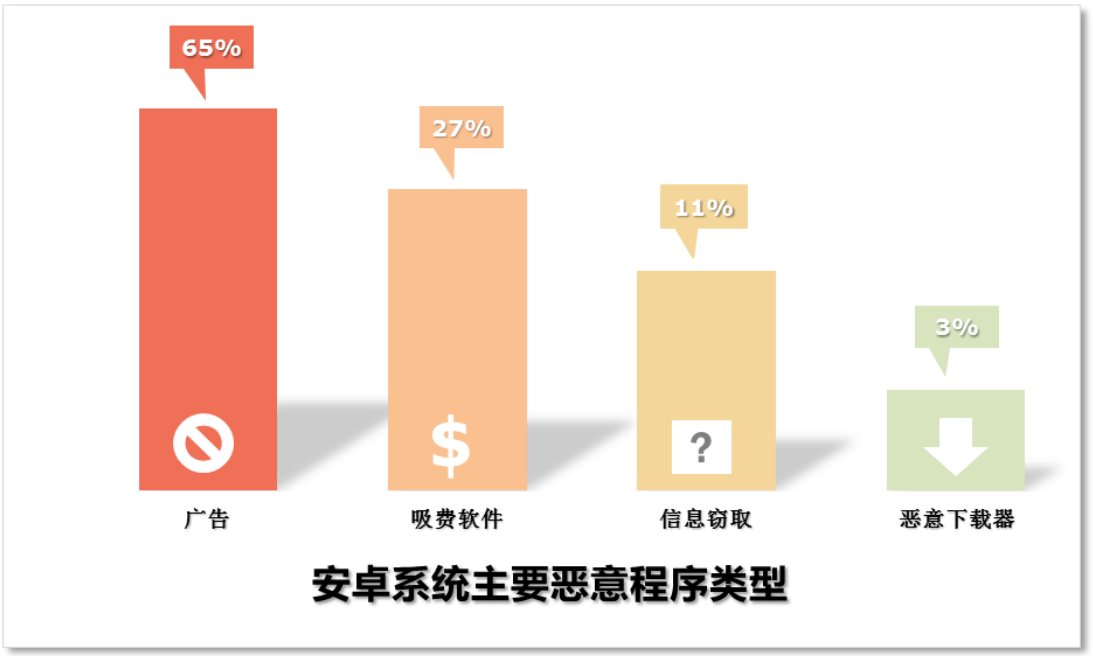


2014 年第 4 季度安卓平台 APK 处理数量走势图

截止到 2014 年 12 月 31 日，趋势科技发布中国区移动客户端病毒码版本是 1.805.00，大小 36,695,532 字节。

趋势科技对 APK 文件的处理数量在 2014 年第 4 季度依旧呈上升趋势。截止到本季度 12 月底，处理数量累计达到 1,150 万个。从 2014 年初至今，安卓病毒单月增长率一直保持上升趋势。

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。



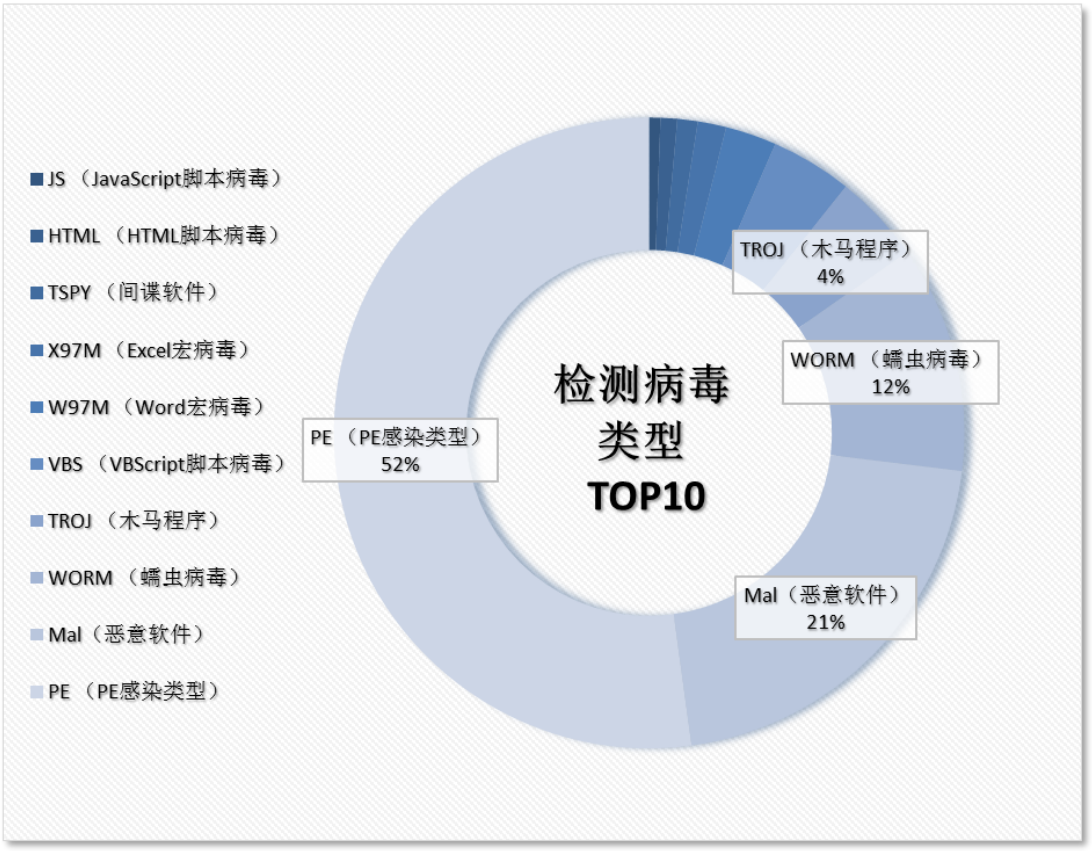
2014 年第 4 季度安卓平台恶意程序类型分布图

在 2014 年第 4 季度感染安卓平台的恶意程序中，数量最多的是“广告”类型，占到总数的 65%；“吸费软件”位列第二，占 27% ；而居第三位的则是“窃取数据信息”类型的恶意程序。另外，请注意上图的数据中一个恶意程序会同时具有上文描述的多种恶意行为。

在 2014 年第 4 季度中，我们监控到一个可以破解 RFID 支付卡的安卓平台恶意程序，趋势科技将其检测为 ANDROIDOS_STIP.A。RFID 卡支付的方式越来越流行，越来越多的设备也加入了对 NFC 的支持。银行、商业和一些其他的公共服务也开始向他们的客户提供带有预存费用的 RFID 卡。因此，黑客将攻击目标转向 RFID 支付卡也是大势所趋。我们还监测到针对另外一种 MIFARE 卡（MIFARE DESFire 卡和 MIFARE Ultralight 卡）的攻击。至少有三种已知的卡片存在漏洞，包括带有银行账户的社会保障卡，用于交通和购物的支付卡，以及就餐卡。这种存在漏洞的社保卡至少有 700 万的用户数量。以上这些 MIFARE 格式都已经不再开发，并被新型的、更安全的模型取代。然而，许多卡片发行者会因为预算的考虑选择旧的方案，这等于将用户的安全置于危险的境地。我们建议用户提高安全意识，保护 RFID 卡的安全。经常查看卡片中的余额。如果可能的话，还应该关注自己使用的卡片是否存在安全漏洞并将这些情况反馈给卡片的发行者。针对 RFID/NFC 的攻击已经受到了广泛关注，终端用户以及企业用户可以参阅我们之前发布的相关安全提示，保障信息的安全。

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。

2014 年第 4 季度各类型病毒检测情况分析



2014 年第 4 季度病毒检测类型分布图

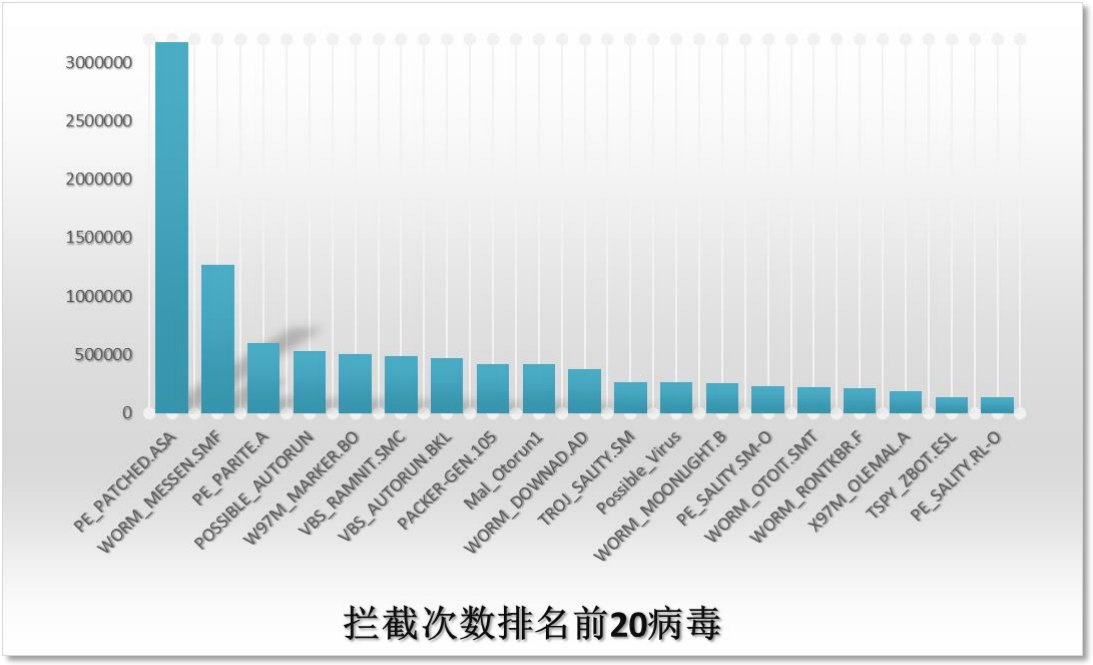
2014 年第 4 季度检测到的病毒种类中，PE 类型病毒感染数量在所有类型中所占比重最大，占到总检测数量的 52%。在本季度中，PE_PATCHED.ASA 检测数量依然排名第一，另外还有数个 PE 家族病毒检测数量排名靠前。PE_PATCHED.ASA 病毒文件是一个被修改过的系统文件 sfc_os.dll，这个文件用以保护系统文件的执行模块，该文件一旦被修改，系统将失去文件保护的功能。

本季度蠕虫病毒占检测类型总数的 12%，比上一季度略有上升。蠕虫病毒的传播途径有以下几种：主动通过网络、电子邮件以及可移动存储设备。它们抵达目标主机后就会进行复制自身的操作，占用大量系统资源。

WORM_DOWNAD.AD 病毒长期以来属于检测数较高的蠕虫病毒，它可以利用多种传播途径在网络间传播并大量占用网络资源。此外，在 2014 年第 4 季度中，WORM_MESSEN 家族病毒监控到的数量也大幅上升。

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。

2014 年第 4 季度病毒拦截情况分析



2014 年第 4 季度病毒拦截情况图

在 2014 年第 4 季度拦截次数排名前 20 位的病毒检测名中，PE 病毒感染量依然较多，PE_PATCHED.ASA、PARITE 家族、SALITY 家族包括在前 20 位中。由于 PE 病毒有大量感染可执行文件的行为，感染速度迅速，导致其检测数量明显高于其它类型的病毒。

本季度由趋势科技产品拦截到的次数最多的病毒是 **PE_PATCHED.ASA**。该病毒被检测到的拦截次数约为 317 万多次，大大高于其它病毒。

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。

对该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，然后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

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。

本季度监控到检测名为 **WORM_MESSEN.SMF** 的病毒检测数量较大。关于该病毒的详细信息介绍如下：

病毒类型：

蠕虫

文件类型：

.EXE

安装：

它会创建以下文件夹：

%User Temp%\jtxbmt

%User Temp%\jtxbmt\vpdrmdsdqkqgvmdr

(注意: %User Temp% 是当前用户的 Temp 文件夹。通常位于 C:\Documents and Settings\{user name}\Local Settings\Temp (Windows 2000、XP 和 Server 2003)。)

恶意行为：

它会添加下列注册表项：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system

EnableLUA = "0"

清除方法：

- ✓ 将趋势产品更新到最新病毒码执行全盘扫描，将所有检测为 WORM_MESSEN.SMF 的文件删除。

详细处理方法请查看以下链接：

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/WORM_MESSEN.SMF

2014 年第 4 季度热门新型病毒分析

REGIN 家族病毒是一个十分复杂的病毒，并且针对特定用户进行针对性攻击。REGIN 家族使用了一系列高级逃避检测技术，利用多个模块来窃取信息并防止被检测到。另外，它还利用多种感染链来增加安装到目标机器的成功率。

TROJ_REGIN.A 恶意行为示意图

病毒的详细信息如下：

病毒检测名：
TROJ_REGIN.A

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。

病毒安装：

病毒最初侵入系统时会伪装成下列名字的 sys 文件，位于“System32”目录下：

abiosdsk.sys
adpu160.sys
atdisk.sys
cdaudio.sys
floppy.sys
ndisips.sys
parclass.sys
pciclass.sys
pcidump.sys
pciport.sys
rasprt.sys
rdpmdd.sys
Ser8UART.sys
serial.sys
usbclass.sys

和通常情况不同，这个病毒不会将文件保存到安装目录下。另外它会将组件保存到 NTFS 扩展属性下来躲避检测：

%Windows%
%Windows%\fonts
%Windows%\cursors
%Windows%\system32
%Windows%\system32\drivers
(注意: %Windows%是 Windows 目录，通常为 C:\Window.)

它还会保存在注册表键值中使自身难以被普通检测手段发现:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RestoreList
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{39399744-44FC-AD65-474B-E4DDF-8C7FB97}
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{3F90B1B4-58E2-251E-6FFE-4D38C5631A04}
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA5A}
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{9B9A8ADB-

8864-4BC4-8AD5-B17DFDBB9F58}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RestoreList\VideoBase

生成以下文件对被感染的机器进行标记：

%System%\nsreg1.dat
%System%\bssec3.dat
%System%\msrdc64.dat
(注意：%System%是 Windows 系统目录，在各版本 Windows 中，通常是 C:\Windows\System32)

病毒行为：

这个病毒会将恶意行为加密为 VFS（Virtual File Systems）进行存储。可能会存储在以下文件或目录下：

%System%\config\SystemAudit.Evt
%System%\config\SecurityAudit.Evt
%System%\config\SystemLog.evt
%System%\config\ApplicationLog.evt
%Windows%\ime\imesc5\dicts\pintlgbs.imd
%Windows%\ime\imesc5\dicts\pintlgbp.imd

集成多种功能和窃取信息

该病毒集合了以下功能:

Rootkit
网络端口拦截
网络监听
凭据窃取
C&C 通讯
加密功能
收集系统信息
界面控制（截屏，击键记录，点击功能）
文件系统控制（写入，读取，创建，删除）
进程和模块控制
IIS Web 服务器日志窃取
GSM 活动日志

它会连接以下 C&C 服务器接收和发送信息：

{BLOCKED}.{BLOCKED}.114.73
{BLOCKED}.{BLOCKED}.144.113
{BLOCKED}.{BLOCKED}.89.80
{BLOCKED}.{BLOCKED}.237.145

解决方法：

1. 使用趋势科技防病毒客户端的客户，升级到最新病毒码，能清除目前我们发现的该恶意软件。

2. 非趋势科技防病毒客户端的用户，可以使用趋势科技提供的 ATTK 扫描病毒并收集信息。

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

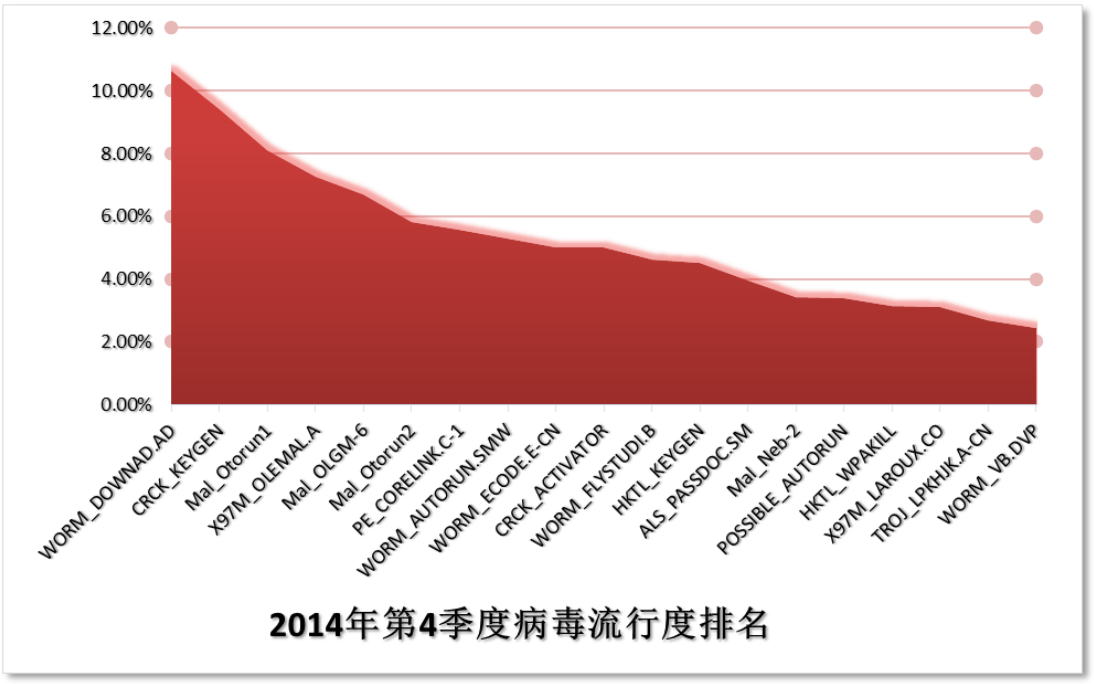
64 位 Windows 操作系统请使用：

http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage_64.exe

相关链接信息：

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_REGIN.A

2014 年第 4 季度流行病毒分析



2014 年第 4 季度流行病毒排名情况图

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。

2014 年第 4 季度 WORM_DOWNAD 病毒全球分布图

WORM_DOWNAD 病毒依然是中国区最为活跃的病毒。目前针对该病毒已有一套完整的解决方案，但 WORM_DOWNAD 在中国的感染情况并没有得到很大改善。截止 2014 年第 4 季度，约有 11.87% 的用户遭受到此病毒的攻击。

WORM_DOWNAD 病毒的持续流行与用户所处环境和使用习惯有一定联系，虽然目前的防毒产品均可以检测并处理该病毒，但该病毒依然屡见不鲜。

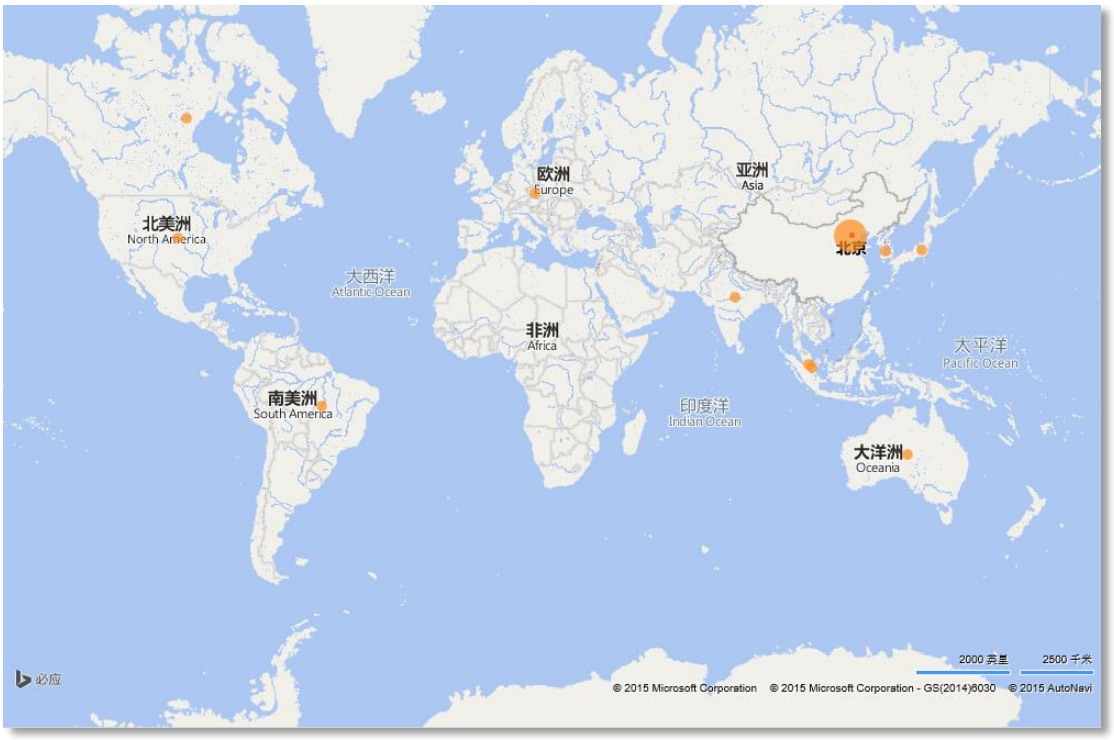
在这里仍然需要提醒用户，WORM_DOWNAD 持续流行的原因有几点：

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。

截止 2014 年第 4 季度为止，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。

X97M_OLEMAL.A 病毒由中国地区源起，是针对 EXCEL 文件进行感染的病毒。该病毒扩散至全球其它地区，虽从近期的感染数查看有略微减少的趋势，但依旧是中国地区比较活跃的病毒。



2014 年第 4 季度 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：

1. 从网站下载而来。
2. 使用文件传输工具获得。
3. 通过邮件传送。

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：

- ✓ 及时更新反病毒产品病毒库，并进行全盘扫描。
- ✓ 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

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。

✓ 另外可以使用 ChinaRTL 的 AVBtool 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 文档进行操作:
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/readme.txt

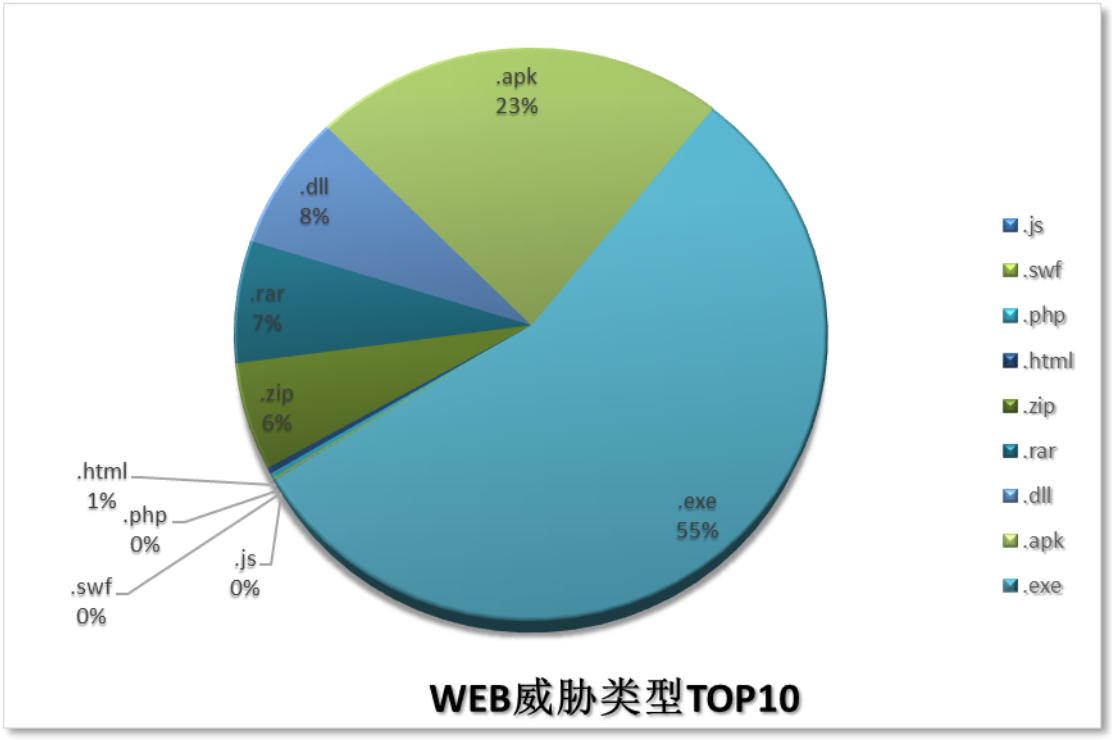
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2014 年第 4 季度 WEB 安全威胁情况

2014 年第 4 季度 WEB 威胁文件类型分析

在 2014 年第 4 季度的数据中，通过 WEB 传播的恶意程序中，.EXE 类型的可执行文件占总数的 55%，所占比例比上一季度有所上升。.EXE 文件类型是通过 WEB 传播的主要文件类型之一，针对此类文件，我们建议企业用户在网关处控制特定类型的文件下载。

此外，在本季度得到的数据中，压缩文件格式.RAR 和.ZIP 文件数量比上一季度有所增加，需要提高对这类文件的关注度。压缩文件格式相较.EXE 文件更具隐蔽性，用户可能会对压缩文件格式降低警惕度，从而对恶意文件进行点击运行。需要引起注意的是，.APK 文件格式所占比例持续上升，占到 23%。



2014 年第 4 季度中国地区 WEB 威胁文件类型分布图

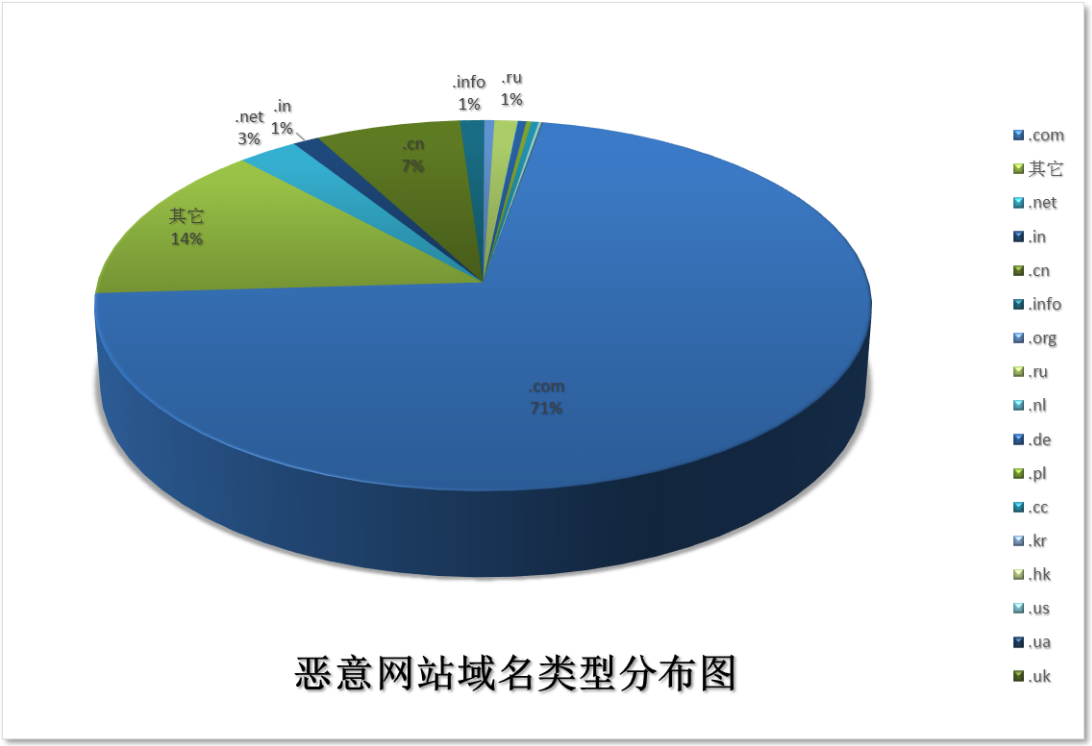
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 4 季度 TOP 10 恶意 URL

TOP10 恶意URL		
恶意URL	描述	点击量
http://traff***verter.biz/	网站直接或间接帮助传播恶意软件或恶意代码	1,394,879
http://220.181.156.43/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	318,404
http://tp.sphwq.net/backmusic.swf	网站直接或间接帮助传播恶意软件或恶意代码	294,750
http://i.fan***rg/images/ico_mall/ico-***lt.png	网站直接或间接帮助传播恶意软件或恶意代码	259,633
http://nei***.funs***on.com/dow***oad/fa***ryland/fi***es/tk/15***/152/C***o.dll	承载恶意负载的域	238,834
http://tk.p***0.com/ca***ck.php?s=6	网站直接或间接帮助传播恶意软件或恶意代码	226,915
http://nei***ng.fun***n.com/air***t/files/Fun***s.dll	网站直接或间接帮助传播恶意软件或恶意代码	211,788
http://tp.sp***.net/dsl***.swf	该网站的地址在垃圾邮件中被发现	186,806
http://v.tt***i.com/1.1***.htm	站点被恶意程序利用，包括用于承载恶意软件升级以及存储被窃取的资料	141,747
http://adv1.do***e.com	网站直接或间接帮助传播恶意软件或恶意代码	134,387

2014 年第 4 季度中国地区 WRS 拦截恶意 URL 排名 TOP10

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。

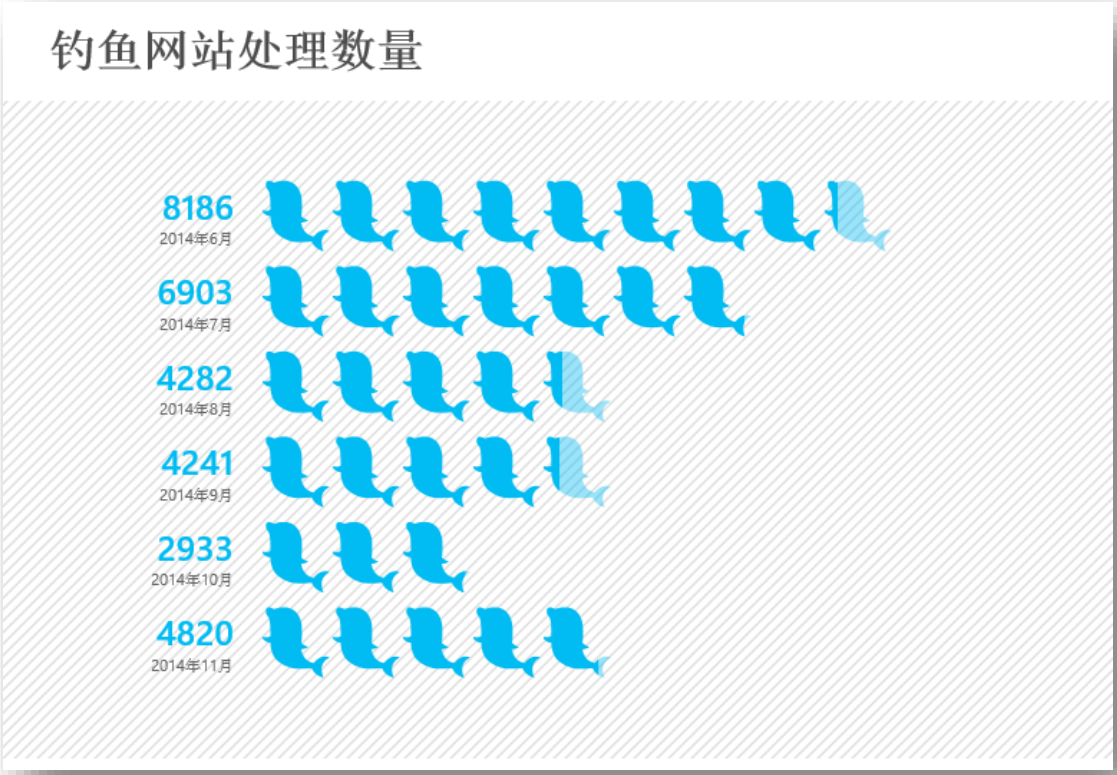


2014 年第 4 季度恶意网站域名类型分布图

2014 年第 4 季度，恶意软件域名在各顶级域的分布情况如上图，使用.COM、.INFO、.NET、的域名的站点占总数 80.93%。其中.COM 域名的恶意网页数量最多。

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。

2014 年第 4 季度 WEB 威胁钓鱼网站仿冒对象分析



2014 年第 4 季度中国地区钓鱼网站数量

从中国反钓鱼联盟得到的数据，2014 年 6 月至 2014 年 11 月共计 6 个月中，处理钓鱼网站共计 **31,365** 个。从示意图中可以得出，后 3 个月的钓鱼网站数量比前 3 个月大幅减少：2014 年中旬每月钓鱼网站数量在 5000 个以上，而在整年下旬，钓鱼网站每月检测数保持在 5000 个以下。

在 2014 年第四季度中，中国地区发现的钓鱼网站以“网络支付”和“金融证券”类型为主要欺诈目标，占到总数的 90%以上。该段时间内，中国地区使用.COM、.TK、.PW 域名的钓鱼网站数量较多，这些类型的钓鱼网站通常占处理总量近 90%以上。其中，.COM 域名下的钓鱼网站占总钓鱼网站数量的比重高居首位。另外，一些非大众化域名下的钓鱼网站数量均有所增加。

本季度联盟接到的钓鱼网站举报中，涉及电子商务网站和银行的钓鱼网站总量占所有举报数量的 90%以上。仿冒电子商务网站的钓鱼网站所占比例虽然比上一季度有所减少，但依然占据总数一半以上。此外，涉及银行页的钓鱼网站所占比例较前一季度增加。

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。

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

趋势科技网站安全查询页面

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。

2014 年第 4 季度漏洞攻击威胁情况

TOP10 漏洞	
漏洞名称	检测数量
CVE-2008-4250	3018476
MS08-067	172,218
CVE-2014-6271	1851
CVE-2012-0507	909
CVE-2010-2568	813
CVE-2010-0806	738
CVE-2013-0422	701
CVE-2010-3340	344
CVE-2010-3343	344
CVE-2010-3962	344

2014 第 4 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= CVE-2008-4250
MS08-067	http://technet.microsoft.com/zh-CN/security/bulletin/ms08-067
CVE-2014-6271	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2014-6271
CVE-2012-0507	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-0507
CVE-2010-2568	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568
CVE-2010-0806	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806
CVE-2013-0422	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-0422
CVE-2010-3340	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3340
CVE-2010-3343	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3343
CVE-2010-3962	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3962

漏洞介绍链接

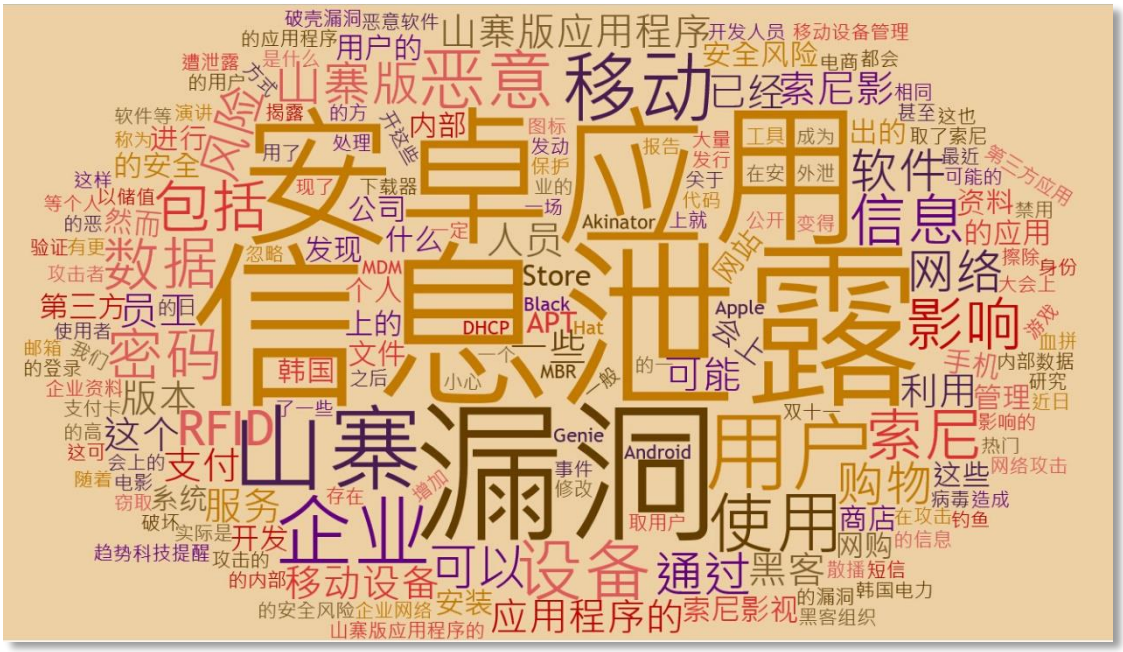
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

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。

2014 年第 4 季度最新安全威胁信息

2014 年第 4 季度安全威胁信息摘要



2014 年第 4 季度国内外安全威胁信息关键词

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。

❖ 索尼影视遭遇重大 APT 网络攻击 大量商业机密遭泄露

近日，索尼影视娱乐公司(Sony Pictures Entertainment)遭到黑客团体发动的 APT 网络攻击，数万名员工的信息以及多部未发行的电影拷贝遭泄露，这个事件再度印证了趋势科技关于 APT 攻击将愈演愈烈的安全预测。

据悉，11 月 24 日，自称为“和平卫士”（Guardians of Peace）的黑客组织声称，已获取了索尼影业的内部数据，包括一些“秘密”数据，包括密码、员工社保号码和一些与名星、经销商签订的合同文本等。并称如果去要求得不到满足的话，将公开这些数据。黑客组织侵入索尼内部数据库后，窃取了索尼至少 100 TB 的内部文件和电影数据，相当于美国国会图书馆十倍的信息存储量。报告显示，在攻击发生之后，索尼影视禁用了整个企业网络，以防范黑客的进一步破坏行动。然而，对企业网络的禁用不仅严重地影响企业的日常营运，也让调查任何攻击变得更加困难。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20141209133205.html

❖ 假冒热门购物网站 APP 盛行

随着双十一的日益临近，“网购达人”们已经进入血拼购物准备模式。然而，钓鱼网站、恶意软件等花样迭出的网购陷阱却让人防不胜防。最近，市场上就有山寨 APP 伪造成为支付宝、天猫等购物 APP，伺机安装到用户手机中，以窃取用户的通讯记录、短信、照片等个人信息，推送垃圾信息，甚至恶意吸费。趋势科技提醒，一定要通过正规渠道下载网购 APP，并安装安全可靠的移动安全软件。

每到购物旺季，购物类移动 APP 的下载量、使用量都会剧增，这也成为不发分子散播山寨 APP 的高峰期。近期，趋势科技拦截到多个实际是木马的山寨电商软件，为了增强可信性，该 APP 会伪装成某电商服务，并使用和官方 APP 极其相似的图标，以试图蒙混过关。在安装之后，有的 APP 还会隐藏图标，使用户难以察觉。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20141111095802.html

❖ 12306 密码外泄 赶快去修改密码吧!!

据某漏洞报告平台称，大量 12306 用户数据在互联网疯传，包括帐号、明文密码、身份证邮箱等！趋势科技提醒大家：邮箱服务和 12306 网站服务一定不要使用相同的登录密码，如二者密码相同，请尽快修改；受信息泄漏影响的用户要小心处理可能的诈骗电话和短信。

http://image.51itapp.com/invitation/qushi/kehu/20141231/data/tips.pdf

❖ 企业不可忽略的问题——员工移动设备管理

企业经常会面临员工把手机、平板电脑等个人移动设备带入工作场所的情况，这样不但给网络管理人员带来麻烦，更会增加企业资料外泄的风险。一般企业会选择使用移动设备管理（MDM-Mobile device management）来防护和监控个人设备里的企业资料和应用程序，但这样的方式也可能存在安全“软肋”。

今年 Black Hat 大会上的一场演讲强调了一些和 MDM 相关的安全风险，会上的展示揭露出了这些安全工具的漏洞，其中包括“忽略身份验证”和“发送未经加密的登录验证码（token）”。研究人员甚至发现了能在攻击者的设备上冒充来电发动攻击的案例。

其实早在去年的 Black Hat 欧洲大会上就已经有过一场关于 MDM 攻击的演讲，并揭露了攻击者通过手机钓鱼软件等方式取得敏感资料的方法。这也正是为什么所有公司在设置保护其设备的工具和界面时都要非常小心谨慎。

http://blog.sina.com.cn/s/blog_5e96245b0102v544.html

❖ 山寨游戏现身 Apple App Store

趋势科技在 Apple App Store 上发现另一个热门应用程序 – Akinator the Genie 的恶搞版本。山寨版本称为“Akinator Genie”，开发人员名称是 Jennifer Mendeison，这人已经因为山寨应用程序而知名。使用者可以在 App Store 下载这个山寨版应用程序。

此应用程序的直接影响无疑是造成金钱上的损失，这可以从使用者所给出的压倒性负面评价看出。山寨版应用程序要价美金$1.99，跟原始版本价钱一样。付费给山寨版应用程序的用户最后只能失望地看见钱丢到水里。

然而，山寨版应用程序的存在对于移动环境具有更大的影响。一方面，开发人员需要担心于保护自己的程序代码，要强化应用程序以避免被重新包装。

http://blog.sina.com.cn/s/blog_5e96245b0102v7w8.html

❖ 恶意 Android 应用程序攻击 RFID 支付卡

趋势科技最近侦测 ANDROIDOS_STIP.A 的高风险 Android 应用程序。这个应用程序通过论坛和博客散播，可以用来攻击用户的 RFID（Radio Frequency IDentification ——感应式电子芯片）公交卡加以储值。

如今通过 RFID 卡来进行支付变得越来越受欢迎，也有更多移动设备加入 NFC(Near Field Communication，近距离无线通信）支持。银行、商家或公共服务都会发行 RFID 卡给他们的客户，并且可以储值。

http://blog.sina.com.cn/s/blog_5e96245b0102vbph.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。

❖ 破壳漏洞事件影响仍在持续扩大，DHCP 会被用于进行漏洞攻击

破壳漏洞（Shellshock）可以通过多种攻击面被恶意利用，包括 Web 应用程序、DHCP、SIP 和 SMTP。随着提出的概念得到了多项证实并公开发布（包括 Metasploit 代码），这个漏洞正在被过度利用。

http://blog.trendmicro.com/trendlabs-security-intelligence/bash-bug-saga-continues-shellshock-exploit-via-dhcp/

❖ App“组件”偷偷下载 App

在第三方 app 商店中出现了一些以游戏为名义实际是下载器的应用，它们会以缺少核心组件为理由骗取用户点击下载其它文件。

我们接触第三方应用程序商店时会探讨其安全隐患。以前的研究已经表明，第三方应用商店往往是恶意软件的温床：特别是流行应用程序的恶意版本。除了恶意的应用程序，我们发现“app 下载器”显著增加，移动用户将面临安全风险。

http://blog.trendmicro.com/trendlabs-security-intelligence/app-component-downloads-apps-onto-devices/

❖ MBR 擦除程序攻击韩国电力系统

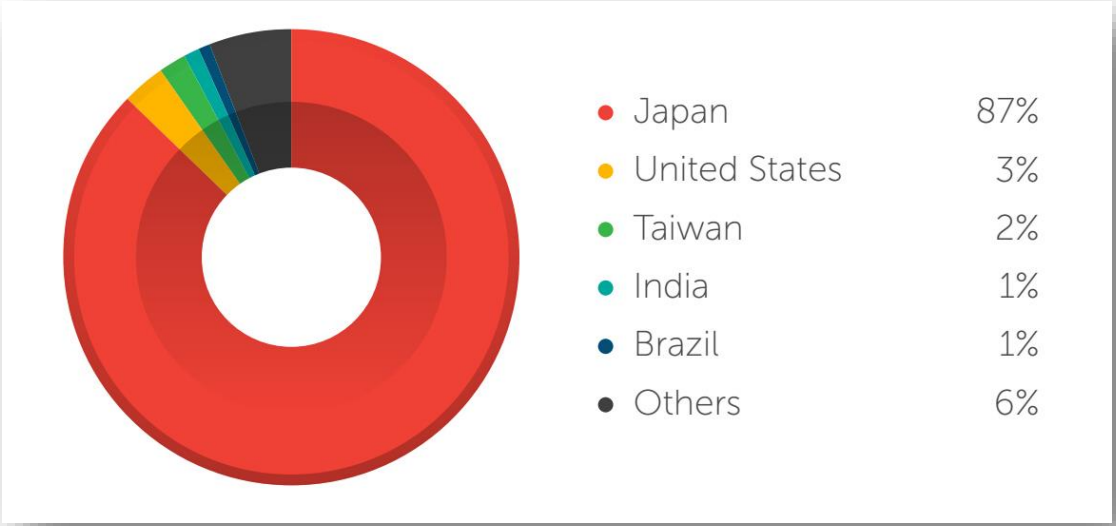
近日，一家韩国电力公司受到破坏性病毒攻击，病毒的目的是擦除受影响的系统引导区信息（MBR）。目前认为该病毒是利用韩文字处理器（HWP）的漏洞抵达系统的，在韩国 HWP 是一个常用的应用程序。该攻击利用了各种社会工程学手段来引诱潜在受害者打开这些文件。

http://blog.trendmicro.com/trendlabs-security-intelligence/mbr-wiper-attacks-strike-korean-power-plant/

趋势科技全球区最新安全威胁概要

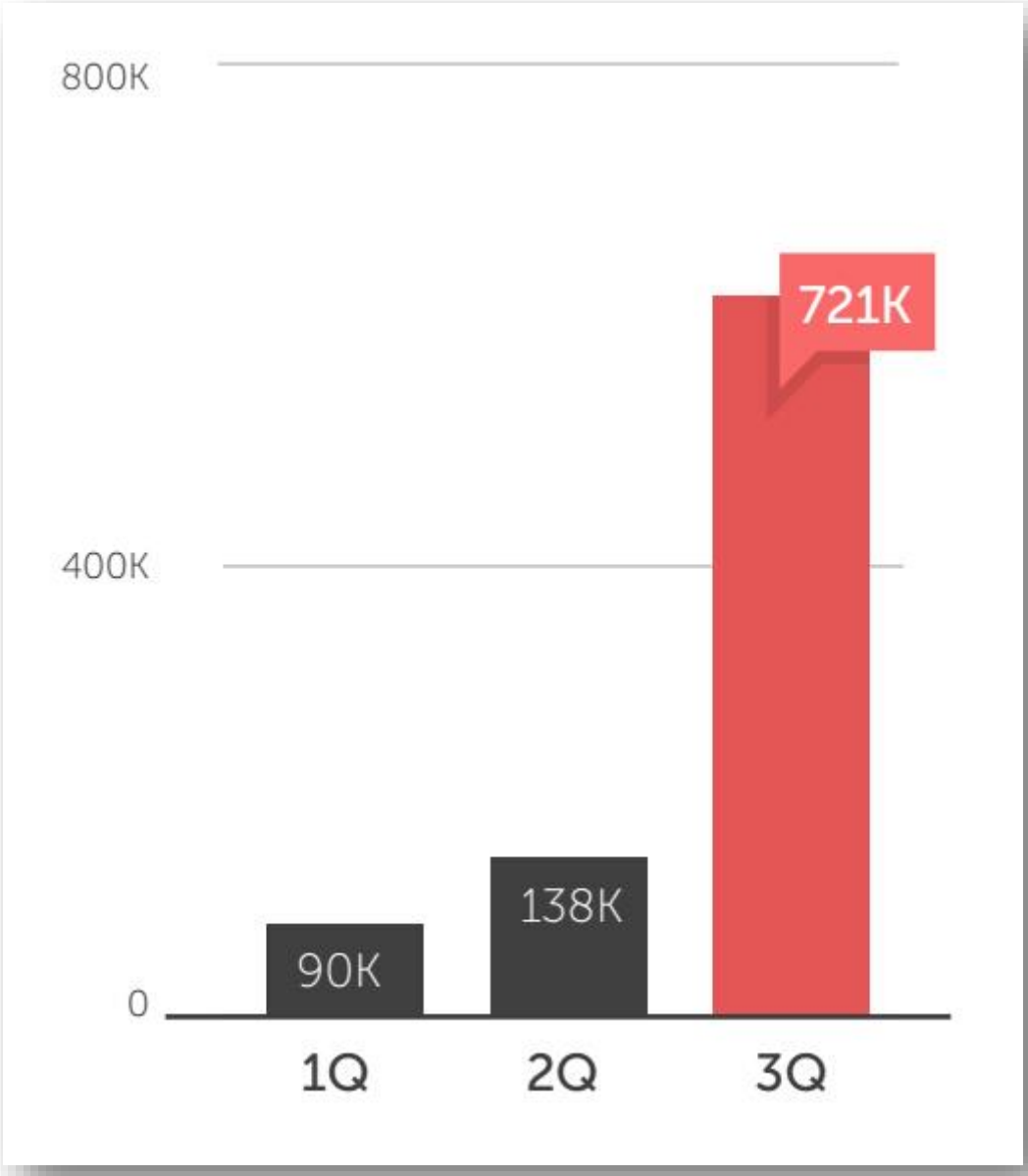
以下是来自 2014 年第 3 季度趋势科技全球区安全报告的数据。

2014 年第 3 季度中，漏洞利用工具滥用情况严重，其中以名为 FlashPack 和 Nuclear 的漏洞利用工具最为显著。在监控的 17 天中（8 月 1 日-17 日），60,000 多名用户受到 FlashPack 的攻击——特别是日本地区的用户。



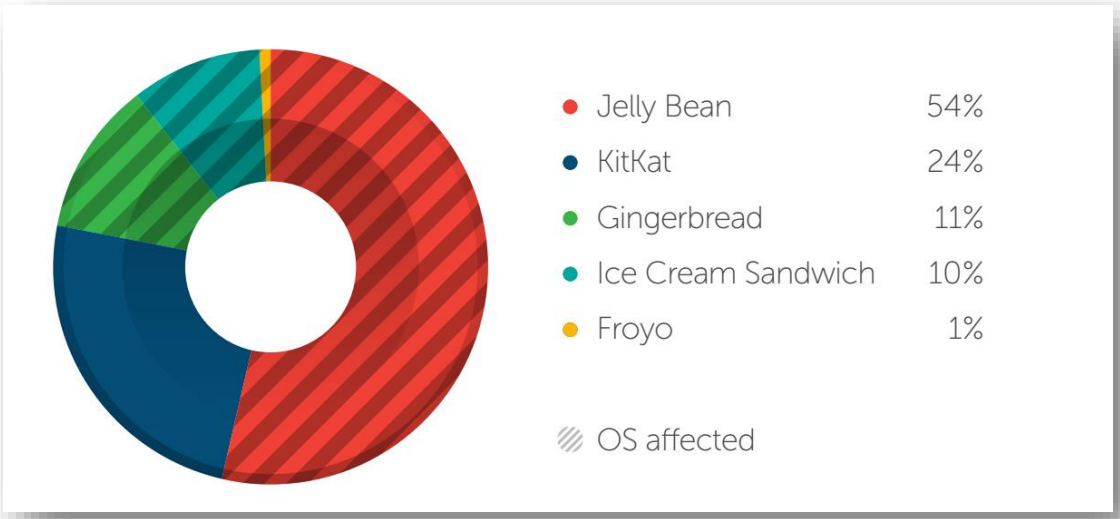
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 3 季度中，全球范围内钓鱼网站 URL 监测数与前 2 个季度相比大幅增加。钓鱼网站的攻击目标通常是一些知名企业，如苹果公司、PayPal、eBay、谷歌、Twitter 等等。



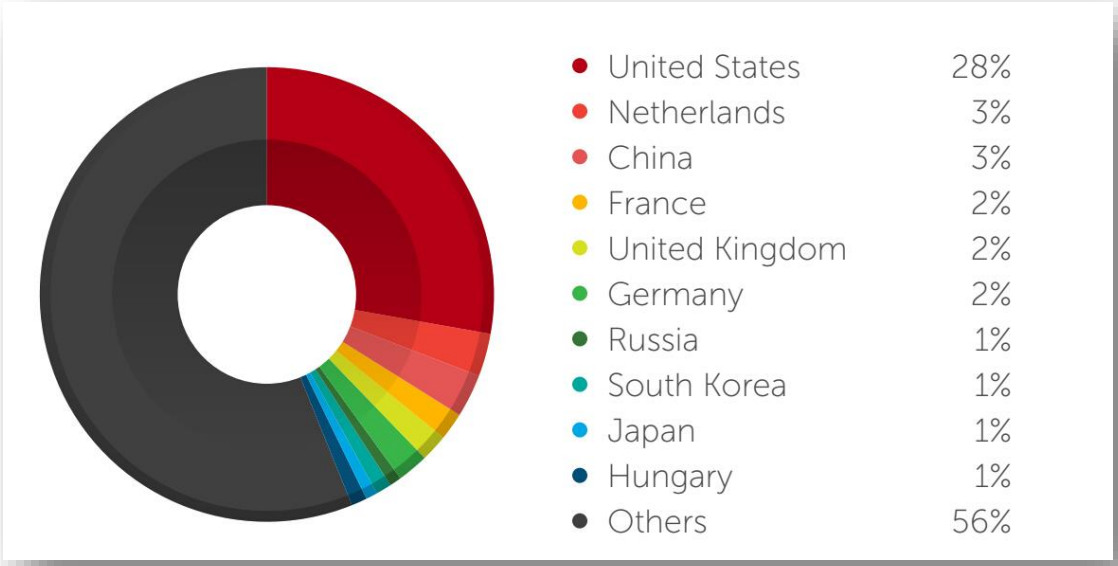
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 3 季度中，超过 75%的安卓用户受到 FakeID 和安卓浏览器缺陷的威胁。只有 KitKat 版本的安卓系统受影响最小。



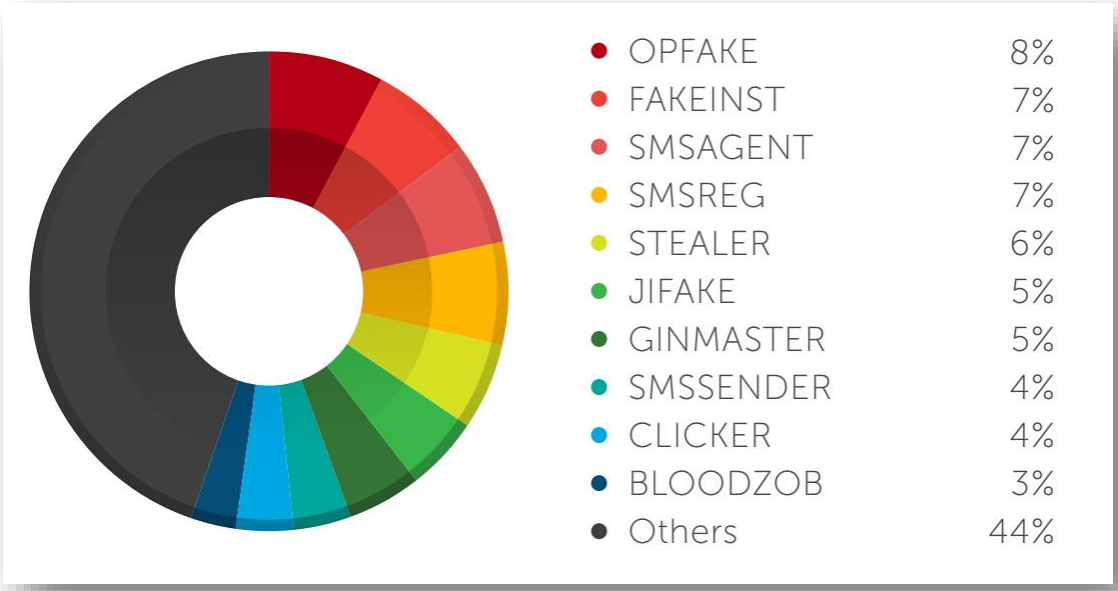
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

下图列出了2014 年第3 季度恶意URL 来源排名前10 的国家。美国居首位，比上一季度增加3%。



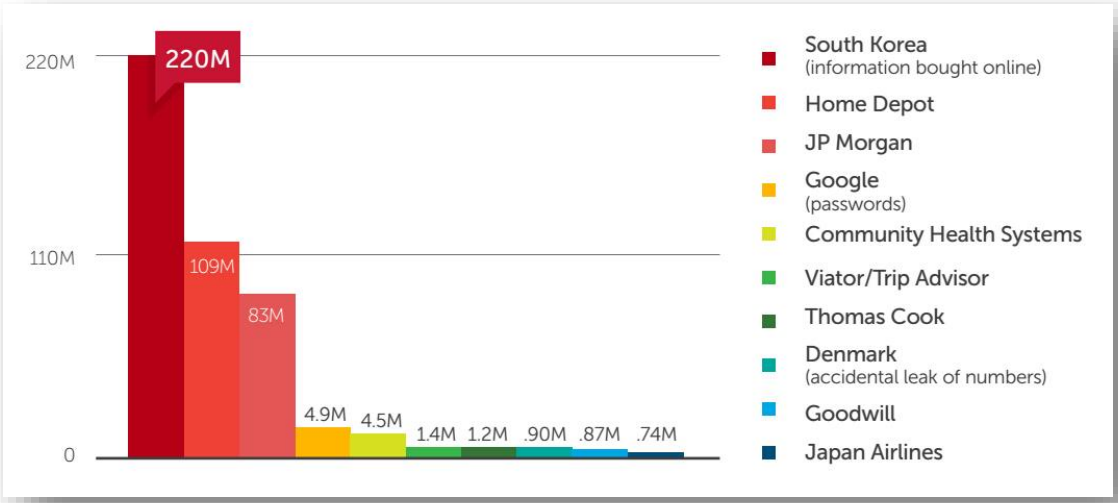
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

下图列出了2014 年第3 季度排行前十的安卓恶意程序家族的分布比例情况。OPFAKE 继上季度之后仍排在第一位。但所占比例较2 季度时的14%已有所减少。



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。

在第 3 季度中，全球范围内信息泄漏事件报告数量如下图所示。



需要查看更完整的 2014 年第 3 季度全球安全报告请访问：

http://www.trendmicro.com/vinfo/us/security/roundup/

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。

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。

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。

TREND MICRO 趋势科技 [全程护航 迈向云端]

ChinaRTL

中国区网络安全监测实验

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。