中国地区 2014 年
第一季度
网络安全威胁报告

2014/5

CHINA RTL

目录

2014 年第 1 季度安全威胁

本季安全警示：
勒索软件，PE 病毒，木马

2014 年第 1 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 2014.3.31 日中国区传统病毒码 **10.694.60** 包含病毒特征数约 **432** 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 **4248** 万次。

- 本季度趋势科技在中国地区拦截的恶意 URL 地址 **196,739,572** 次。

2014 年第 1 季度，趋势科技病毒实验室监控到勒索软件有不断爆发的趋势。勒索软件通常会通过聊天工具、电子邮件、恶意网站等途径进行传播，或被其它病毒下载、释放。攻击者利用社会工程学，诱骗攻击对象运行这些恶意文件。勒索软件一旦被运行，病毒即会搜索计算机上特定类型的文件（通常是文档文件）并进行加密。由于解密所需的私钥在攻击者手中，第三方没有任何办法获得，攻击者即利用掌握的私钥对受害者进行勒索：必须支付钱款买下解密私钥，如果在限定时间内没有赎回，私钥就会被销毁，那么这些被加密的文档就再也无法恢复。目前已接到多起勒索软件引发的案件，并且利用此种方式进行勒索的病毒出现了较多变种。其中典型且影响较大的如 **TROJ_CRILOCK**、**TROJ_CRIBIT** 等家族，勒索手法基本相似。

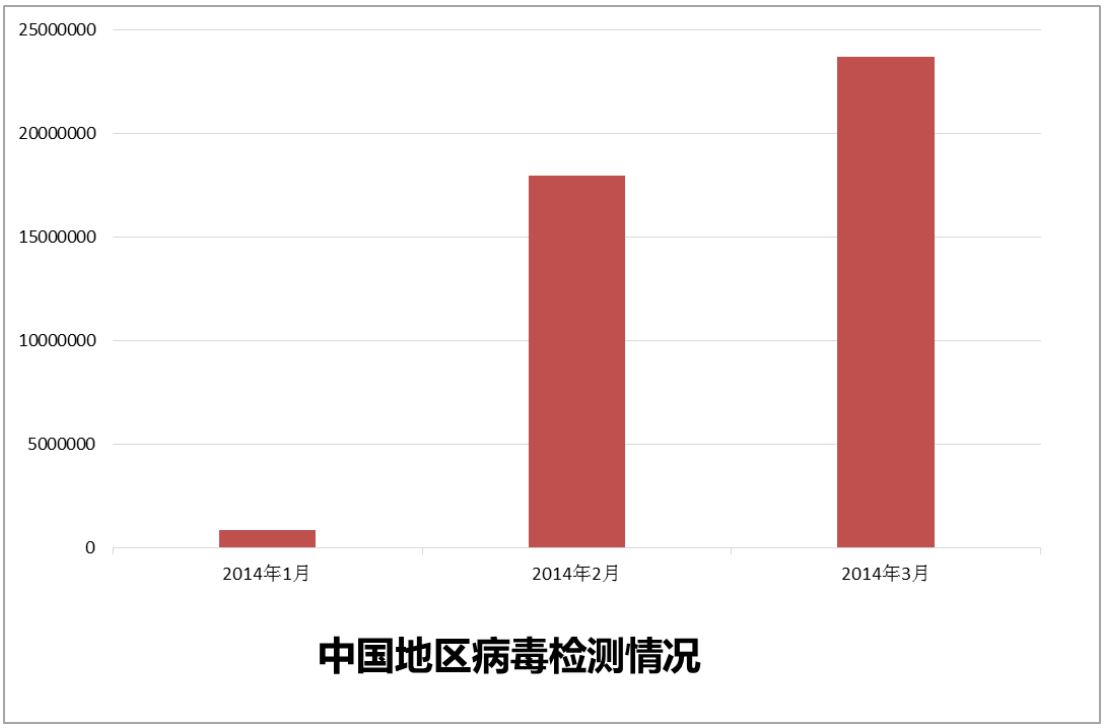
第 1 季度 PE 病毒感染情况依然严峻，其中 **PE_PATCHED.ASA** 和 **PE_VIRUX PE_PARITE**、**PE_SALITY 家族**的感染型病毒检测数量居高不下：

PE_PATCHED.ASA 连续多个季度占据病毒检测数量排名首位。该病毒修改 Windows 系统目录下的正常文件 sfc_os.dll，sfc_os.dll 是用来保护系统文件的执行模块，如果文件被修改系统会失去文件保护的功能，此系统文件被修改可能是攻击者在受感染计算机上执行下一步恶意行为的准备阶段。

PE_VIRUX、PE_PARITE、PE_SALITY 家族在本季度依旧流行，这几种 PE 病毒各有特点，可能是造成它们长期占据病毒检测数排名前几位的原因。PE_VIRUX 病毒变种繁多。PE_SALITY 除常规的 PE 病毒传播方式外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 除了通过感染文件、网络共享到达系统外，还能够通过电子邮件传播。

2014 年第 1 季度，木马病毒、后门、间谍软件分别位列新增病毒数量排名的前三位。

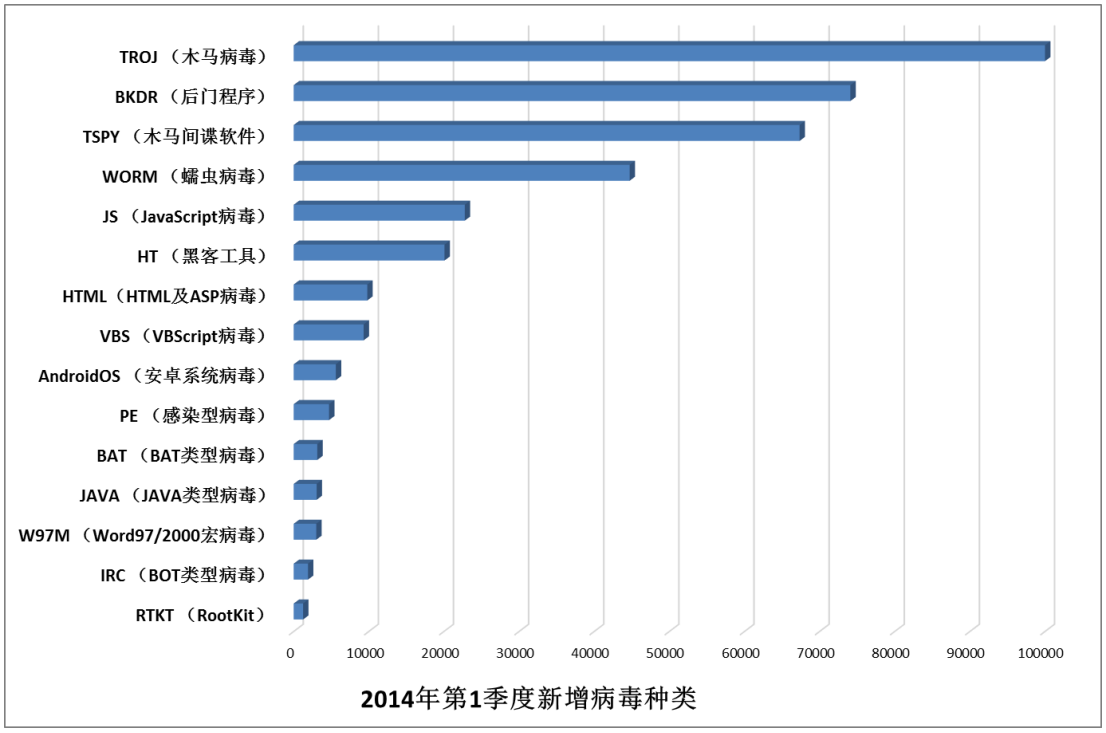
木马通常有盗号和窃取系统重要信息的功能，与其他类型的电脑病毒相比，木马更容易编写且更容易让病毒制造者获益。在经济利益的驱使下，病毒制造者通常更趋向于制作木马。后门病毒则会给受感染电脑带来极大的安全隐患，而间谍软件更专注于窃取用户重要信息。



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 1 季度病毒威胁情况

2014 年第 1 季度新增病毒类型分析



本季度中，**TROJ（木马病毒）**居新增病毒数量类型首位，本季度新增木马病毒特征共计 **340,064** 个。病毒制造者可通过制造木马程序更直接的获利，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。

除木马类型以外，本季度新增的病毒类型中，增加类型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）。**

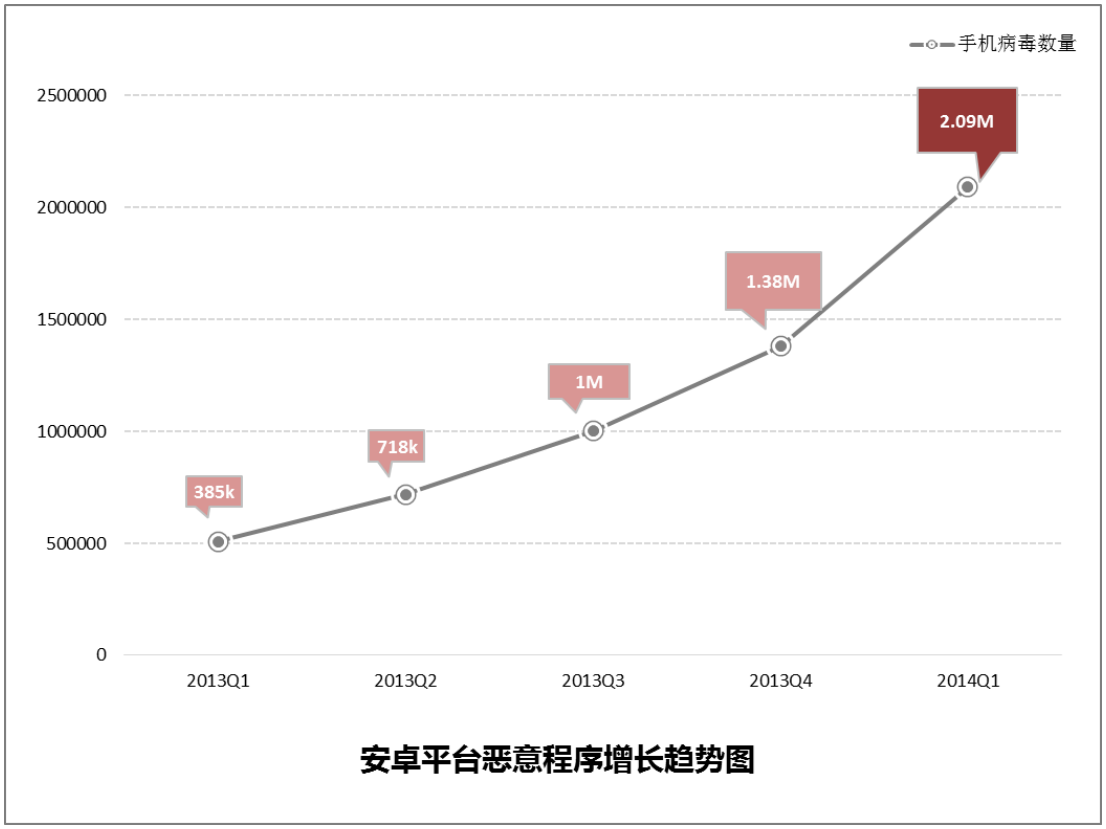
排名靠前的 JS (JavaScript 病毒)，HTML(HTML 及 ASP 病毒)通常和网页挂马相关。恶意代码的制造者将代码植入网站中，这些脚本内容往往不容易被网站管理者以及浏览网页的用户发觉，正常的网站服务器成了扩散病毒、恶意代码的平台。另外，通过向网页插入恶意代码，网络罪犯可以进一步获得网站的 WEBSHELL，甚至能够控制网站服务器的机器。如此，网站用户的数据可能会遭到泄露，服务器也可能成为这些恶意行为者的肉鸡，被用来进行网络攻击或其他一些非法的网络行为。

另一个值得注意的是以 HT_开头的检测类型，此类型是黑客工具。从 2013 年初开始，此类型病毒活跃度居高不下。地下黑市的活跃使更多的黑客工具流传到市面上，被黑客和准

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。

黑客们大量使用，也使得网络安全问题日趋严重。一些可以从因特网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些弱点（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。黑客工具的出现使得网络攻击变得越来越简单。

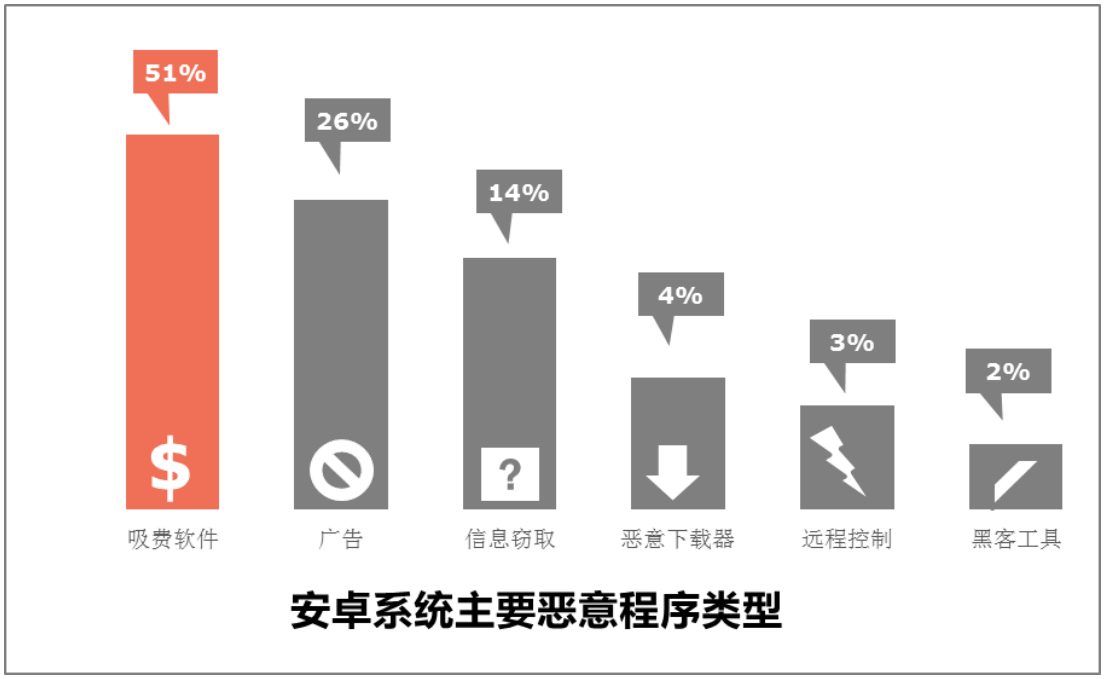
新的 AndroidOS(安卓系统病毒)数量在 2014 年第 1 季度中有明显上升幅度。自 2013 年第 3 季度破一百万后，仅过了 6 个月，病毒数量已直破二百万个。安卓系统的恶意程序增长速度惊人。



在 2014 年第 1 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 51%。广告软件位列第二占 26% ，而第三位则为窃取数据信息类型的恶意程序。

需要注意的是本季度信息窃取类安卓平台恶意程序所占比例有所增加，其中假冒手机银行类的恶意程序有所增加（如 PERKEL 和 FAKEBANK 家族）。用户的手机一旦感染此类恶意程序则可能造成信息泄露和财产损失，用户的个人信息安全受到严峻考验。

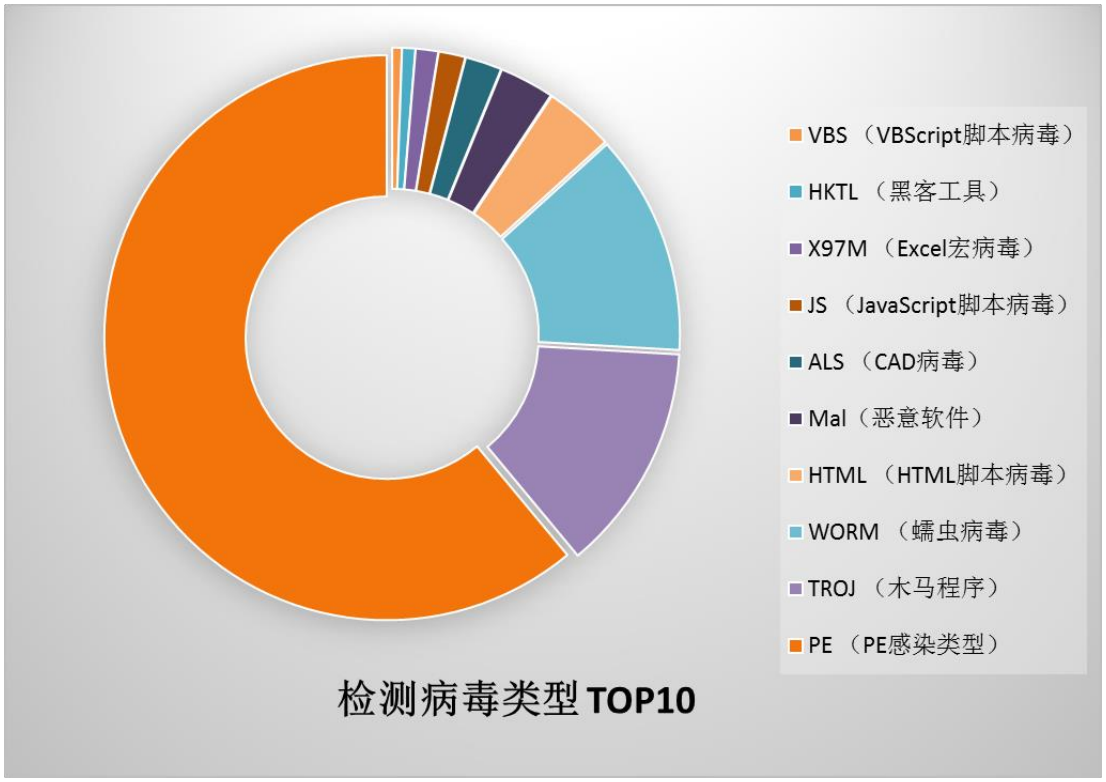
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。



安卓系统主要恶意程序类型

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。

2014 年第 1 季度各类型病毒检测情况分析



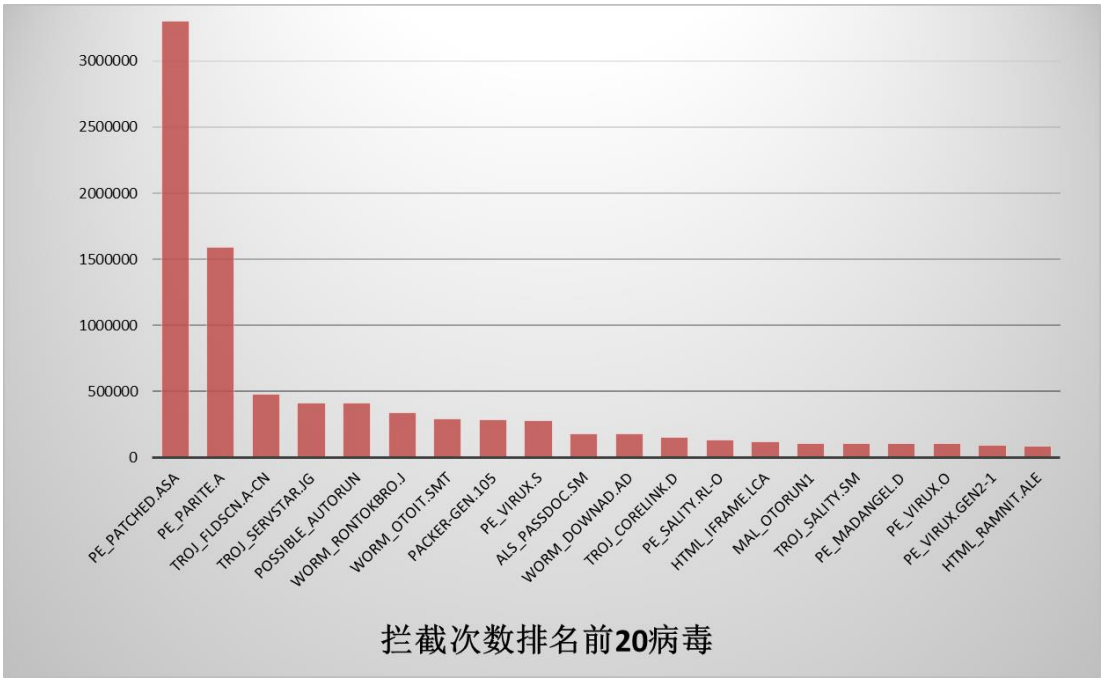
2014 年第 1 季度检测到的病毒种类中以 PE 类型病毒感染数量位列第一，占到总检测数量的 61%。PE 病毒为感染型病毒，会搜索系统中的可执行文件并在每一个符合条件的文件中插入恶意代码。因其特殊的感染原理，系统若感染 PE 病毒，就会出现大片文件被感染的情况。在第 1 季度中，检测数量最多的 PE 病毒仍然是 PE_PATCHED.ASA。该病毒是被修改的 sfc_os.dll，sfc_os.dll 用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能。

木马类型病毒检测数位居第二，占总检测数的 13%。木马病毒的高检测数量与 PE 病毒的爆发有密切关系。通过统计数据可以发现，如本季度拦截次数排名进入前 20 的木马病毒：TROJ_CORELINK.D、TROJ_SALITY.SM，它们分别由 PE_CORELINK 和 PE_SALITY 家族的感染型病毒文件释放从而抵达受感染的计算机。由于木马通常具有窃取用户个人信息、账户密码的行为，造成用户的直接经济损失，因此对此类病毒的防御应予以一定重视。

蠕虫病毒是继 PE 和木马类型后检测数量最多的病毒，蠕虫病毒最主要的特性是能够主动通过网络、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 家族病毒。

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。

2014 年第 1 季度病毒拦截情况分析



上图显示了 2014 年第 1 季度拦截次数排名前 20 位的病毒。与前文提到的病毒检测类型排名一致，拦截次数较多的病毒包括大量感染可执行文件的 PE 病毒，另外还包括部分反复感染难以清理的病毒。

2014 年第 1 季度由趋势科技产品拦截到的，次数最多的病毒仍然为 PE_PATCHED.ASA。该病毒被拦截次数约为 330 多万次，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。

本季度排名位列第二的 PE_PARITE 也是中国地区用户感染较多的病毒。关于该病毒的详细信息介绍如下：

传播途径：

可能是由远程站点的其他恶意软件/灰色软件/间谍软件下载而来。

通过在受感染计算机上的文件中添加自己的恶意代码来感染文件。

感染文件类型：

.EXE

.SCR

恶意行为：

该病毒的母体文件（趋势科技检测名为 PE_PARITE.A-O）通常会先感染 explorer.exe 从而得以驻留内存。一旦成功，它将会感染受感染电脑上以及可以通过网络共享访问到的目录中的所有.EXE 和.SCR 文件。

PE_PARITE.A 会向 Windows 系统下的临时目录释放随机命名的.TMP 文件，并且调用执行它。

它会导出一个名为 INITIATE 的函数，该函数包含恶意行为，一旦被执行，该病毒将会创建以下注册表键值：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Pinf

该病毒创建名为“RESIDENTED”的互斥量，用以确定自身是否已经运行。

PE_PARITE.A 病毒行为示意图

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。

传播途径及防护方法：

- ✓ 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。
- ✓ 介于该病毒首先会感染 explorer.exe 这个特性，我们可以使用趋势防毒产品中的“爆发阻止”功能，阻止对 explorer.exe 的修改。

详细处理方法请查看以下链接：

http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/solutionDetail.asp?solutionId=72241

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 1 季度热门新型病毒分析

2014 年第 1 季度，China RTL 收到多家用户反馈感染勒索软件病毒的案件，感染该病毒后系统中多种文档文件会被加密，需要向攻击者支付一定金额或虚拟货币才能获取密钥将文件解密。

如勒索软件 CRILOCK（趋势检测名 TROJ_CRILOCK）感染客户会警告窗口：

勒索软件弹窗

该病毒的详细信息如下：

病毒检测名：
TROJ_CRILOCK

传播渠道：
此木马病毒可能通过聊天工具、电子邮件、恶意网站传播或由其他病毒释放而来。

病毒行为：
1.释放其自身的副本，复制到以下目录：
%Application Data%\{随机字母的文件名}.exe
(注意: %Application Data% 是当前用户的 Application Data 文件夹,在 Windows 2000, XP，Server 2003 系统中通常为 C:\Documents and Settings\{帐户名称}\Application Data, 在 Windows 7 及以上版本系统中通常为 C:\Users\{user name}\AppData\Roaming.)

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。

2. 会创建互斥量，以避免自己重复运行。

3. 会在注册表中添加自启动项。

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunCryptoLocker = "%Application Data%\{随机文件名}.exe"

4. 会添加以下注册表键值：

HKEY_CURRENT_USER\Software\CryptoLocker

HKEY_CURRENT_USER\Software\CryptoLocker\Files

其中子键 files 下方列出的是已被加密的文件列表。

5. 该病毒会连接以下域名以获取加密的密钥：

gktibioivpqbot.net

mlernipmrlrnjj.com

lnjaadfliwshke.info

kktvnsdykphojs.co.uk

jmyeansxbbiibw.org

qnamcbakhsitnw.ru

ppfuovpjxejnoy.biz

这些地址中任意一个可连接的域名最终指向 IP 地址为 93.189.44.187 的服务器。

6. 在获取加密密钥后以下类型文档将被加密：

*.3FR *.ACCDB *.ARW *.BAY *.CDR *.CER *.CR2 *.CRT *.CRW *.DBF *.DCR *.DER *.DNG *.DOC *.DOCM *.DOCX *.DWG

*.DXF *.DXG*.EPS *.ERF *.INDD *.KDC *.MDB *.MDF *.MEF *.MRW *.NEF *.NRW *.ODB *.ODC *.ODM *.ODP *.ODS *.ODT *.ORF *.P12

*.P7B *.P7C *.PDD *.PEF *.PEM *.PFX *.PPT *.PPTM *.PPTX *.PSD *.PST *.PTX *.R3D *.RAF *.RAW *.RTF *.RW2 *.RWL *.SR2 *.SRF *.SRW *.WB2

*.WPD *.WPS *.X3F *.XLK *.XLS *.XLSB *.XLSM *.XLSX

7. 勒索者接受以下支付方式：

Bitcoin

cashU

MoneyPak

Ukash

防护方法：

1. 从网关处阻止恶意地址的连接。

2. 将防毒软件病毒码更新至最新。

3. **不要随意点开未知发送者的邮件附件。**

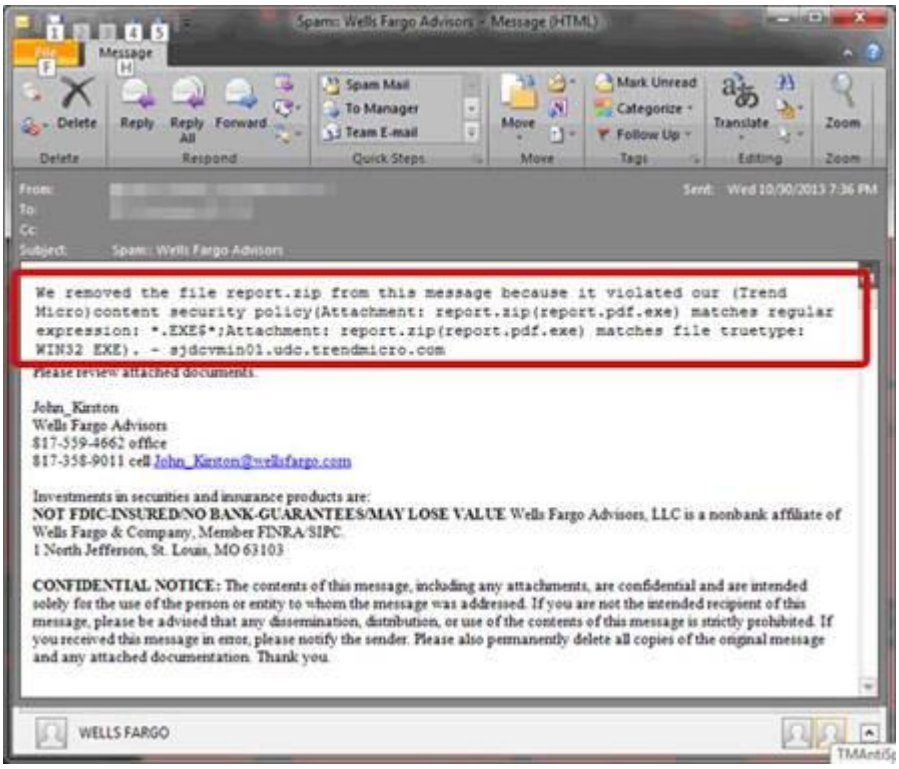
4. 不要随意接收并运行聊天工具中发送的文件（包括看上去是图片文件或 OFFICE 文档的文件）。

5. 不要随意访问未知的国外站点，特别是黄色站点或是视频下载站点。

6. 重要文档请注意备份。

值得特别注意的是，为了增强组织的整体安全策略。使用者所需要的安全防护方案不仅是对可执行文件进行扫描检测，还可在恶意软件到达系统前提供保护。

比如在整个防护方案中加入电子邮件信誉评分服务可以阻止这些包含恶意附件的垃圾邮件，文档真实类型过滤功能可以在检测到电子邮件附件有可疑文件时提醒使用者，如下图：



邮件过滤服务将可疑文件隔离

解决方法：

✓ 及时更新反病毒产品病毒库，并进行全盘扫描。
（被加密的文件尚无法解密）

✓ 未安装趋势防毒软件的用户可至以下站点下载 ATTK 工具进行扫描：

32 位 Windows 操作系统请使用：

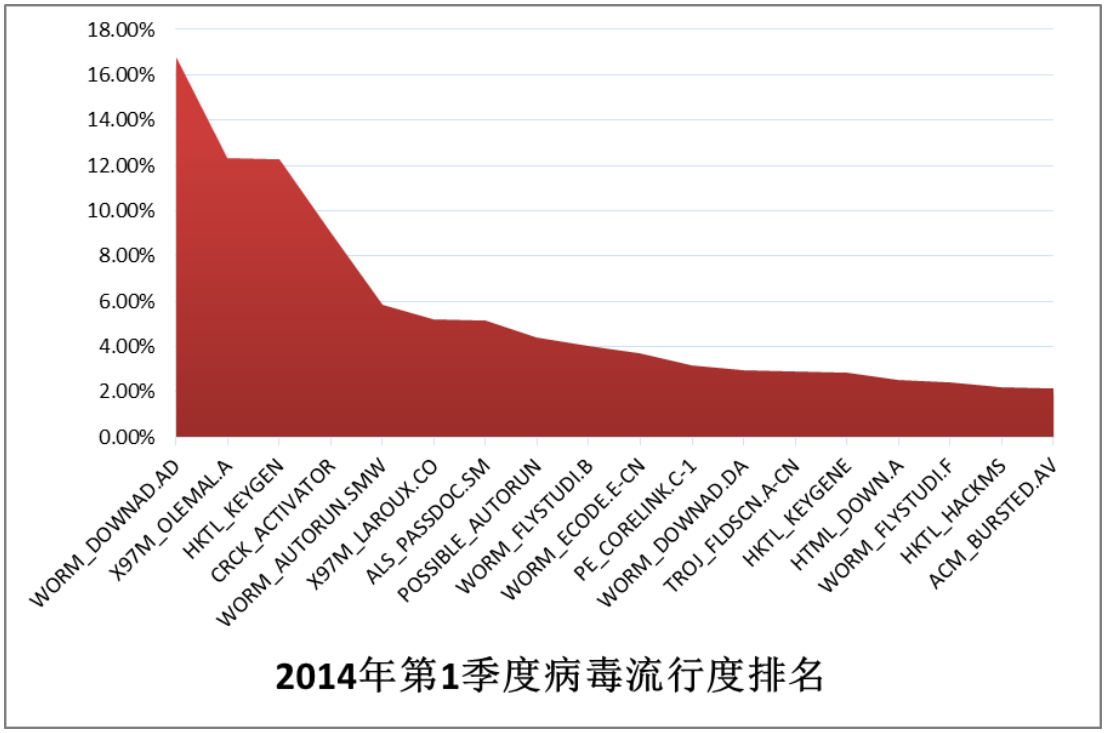
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustmizedpackage.exe

64 位 Windows 操作系统请使用：

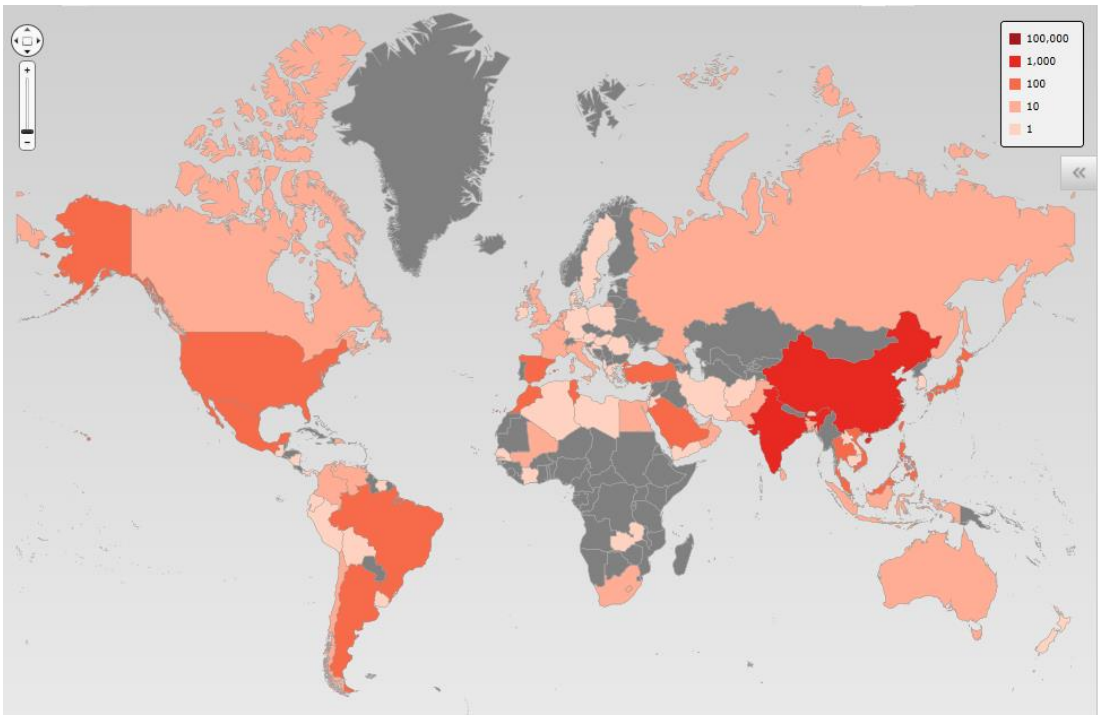
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage_64.exe

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。

2014 年第 1 季度流行病毒分析



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 1 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 1 季度，仍约有 17% 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。

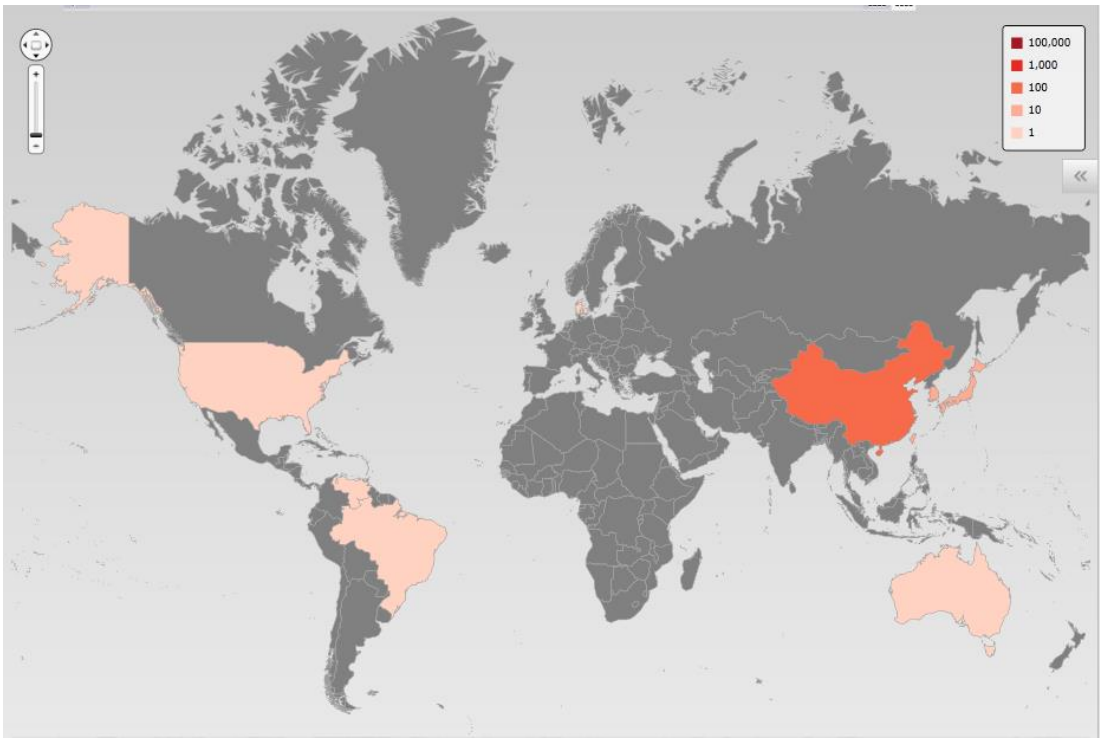
在这里仍然需要提醒用户，WORM_DOWNAD 持续流行的原因有几点：

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 1 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 1 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

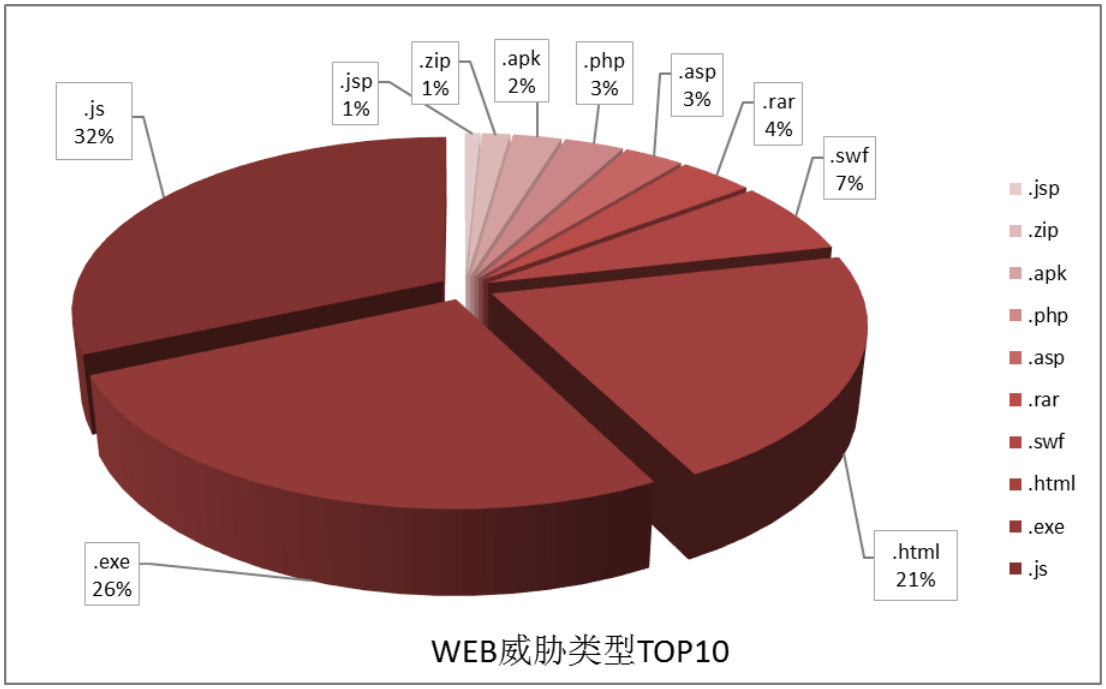
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2014 年第 1 季度 WEB 安全威胁情况

2014 年第 1 季度 WEB 威胁文件类型分析

分析本季度的数据，通过 WEB 传播的恶意程序中，约有 32%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它恶意程序，或者进行修改 IE 浏览器主页等恶意行为。一般情况下这些脚本利用各种漏洞（微软的 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它恶意行为。

.EXE 仍然是占很大比例的 WEB 威胁文件类型,我们建议企业用户在网关处控制某些类型的文件下载。



2014 年第 1 季度中国地区 WEB 威胁文件类型分布图

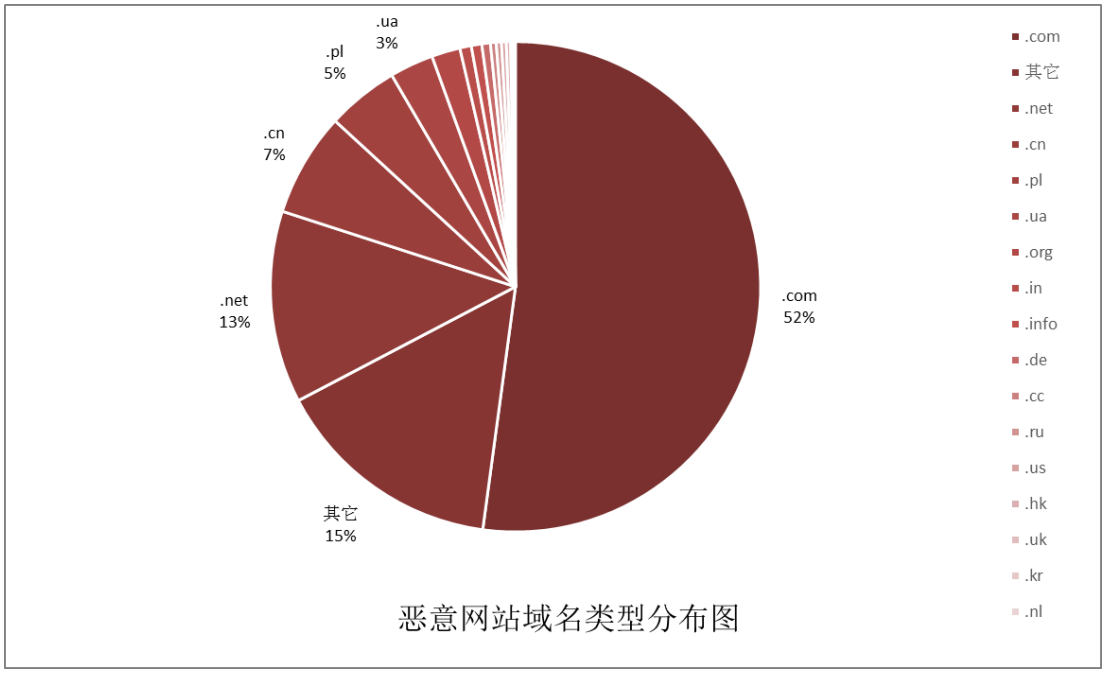
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 1 季度 TOP 10 恶意 URL

TOP10 恶意URL		
恶意URL	描述	点击量
hxxp://traffic***.biz/	网站直接或间接帮助传播恶意软件或恶意代码	35555824
hxxp://fist***.com/aa/nn	网站直接或间接帮助传播恶意软件或恶意代码	25807074
hxxp://88.***.9/aa/nn	发现有恶意行为的域名	25798418
hxxp://lobo***.com/aa/nn	网站直接或间接帮助传播恶意软件或恶意代码	25759593
hxxp://aevo***.cc/client.html	网站直接或间接帮助传播恶意软件或恶意代码	22343618
hxxp://wl-***/windows_live/master.dat	该网站的地址在垃圾邮件中被发现 网站直接或间接帮助传播恶意软件或恶意代码	19628979
hxxp://wl-***/default/master.dat	该网站的地址在垃圾邮件中被发现 网站直接或间接帮助传播恶意软件或恶意代码	19424435
hxxp://cinema-***4MjAwMGM1MGQ3fDMxMA==	网站直接或间接帮助传播恶意软件或恶意代码	19288177
hxxp://optpro***.info/get/	网站直接或间接帮助传播恶意软件或恶意代码	13236772
hxxp://ads.alpha***redirect&label=	网站直接或间接帮助传播恶意软件或恶意代码	12813176

2014 年第 1 季度中国地区被 WRS 拦截的恶意 URL 排名

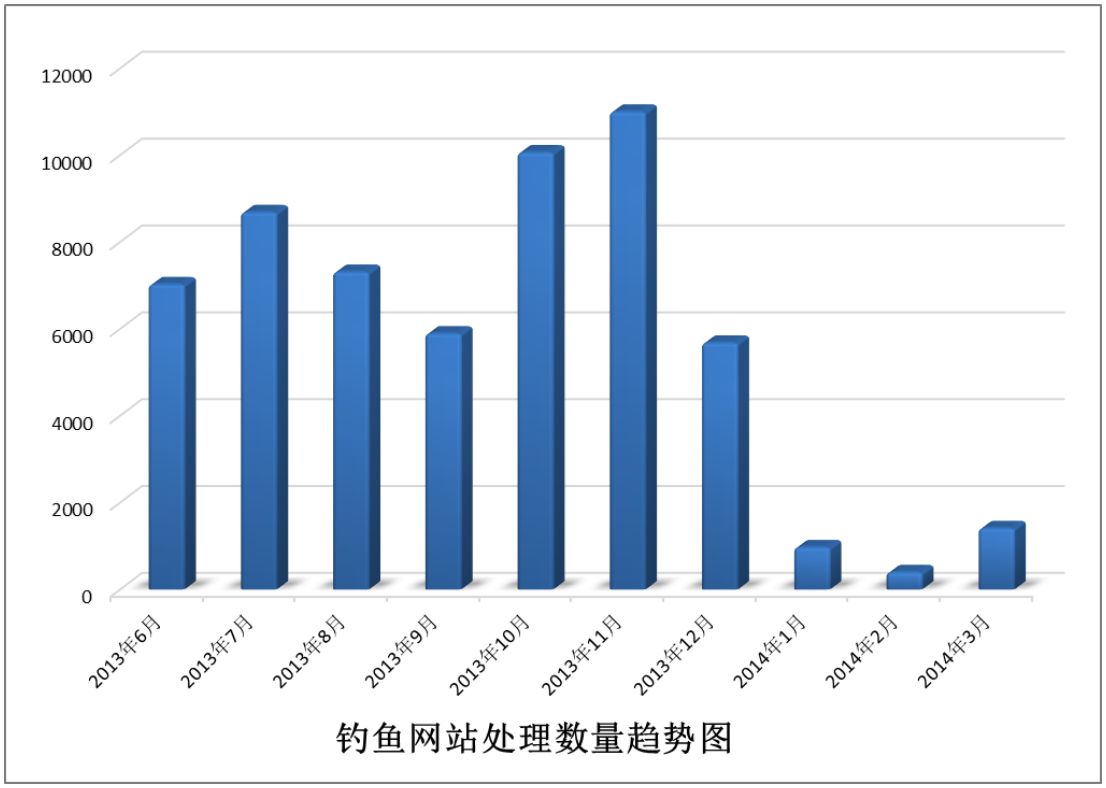
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。



2014 年第 1 季度，恶意软件域名在各顶级域的分布情况如上图，使用.COM、.NET、.CN 的域名的站点占总数 71.65%。其中.COM 域名下的恶意页数量最多。

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 1 季度 WEB 威胁钓鱼网站仿冒对象分析



从中国反钓鱼联盟获得的数据，2013 年 6 月至 2014 年 3 月共计 10 个月中，处理钓鱼网站共计 58,445 个。从趋势图可以看到，2014 年第 1 季度钓鱼网站发现数量较前几个月大幅下降，年初通常是钓鱼网站的低发期，但这并不代表日常访问网页时就可以掉以轻心。

从过去几个月的监控数据查看，钓鱼网站涉及行业中以媒体传播类、金融证券类、支付交易三大类居多。媒体传播类中多以仿冒各大电视台为对象；金融证券类多以仿冒各大银行为对象；支付交易多以仿冒淘宝网为对象。这些对象与我们生活日常息息相关，平日浏览相关网页时需加以重视。在此提醒用户在网络上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，采取了屏蔽特定 IP 等手段阻止某些地址访问，使得检测钓鱼网站更加困难，这也说明钓鱼网站有趋于使用鱼叉式攻击的方法，对攻击目标更具有针对性。

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

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。

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 1 季度漏洞攻击威胁情况

TOP10 漏洞	
漏洞名称	**检测数量**
CVE-2008-4250	180111
MS09-019	58939
CVE-2009-1140	58937
CVE-2007-6250	2344
CVE-2009-2932	2341
CVE-2013-1289	2341
CVE-2013-1295	2341
CVE-2013-1302	2341
CVE-2013-1316	2341
CVE-2013-1317	2341

2014 第 1 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
MS09-019	http://technet.microsoft.com/zh-CN/security/bulletin/ms09-019
CVE-2009-1140	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2009-1140
CVE-2007-6250	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2007-6250
CVE-2009-2932	http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2009-2932
CVE-2013-1289	http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2013-1289
CVE-2013-1295	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1295
CVE-2013-1302	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1302
CVE-2013-1316	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1316
CVE-2013-1317	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1317

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：

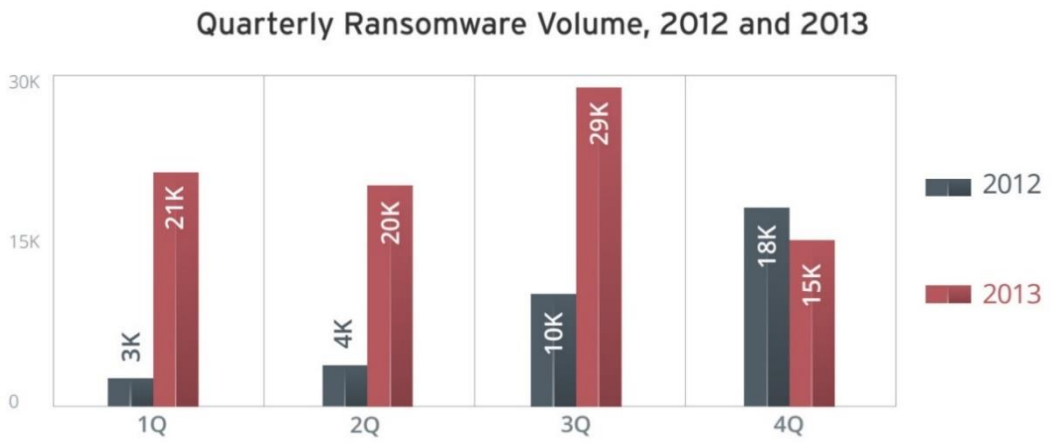
确认补丁成功安装的小方法：开始——运行——输入 cmd 进入 DOS 界面——输入 systeminfo 即可检查当前已成功安装的补丁版本。

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。

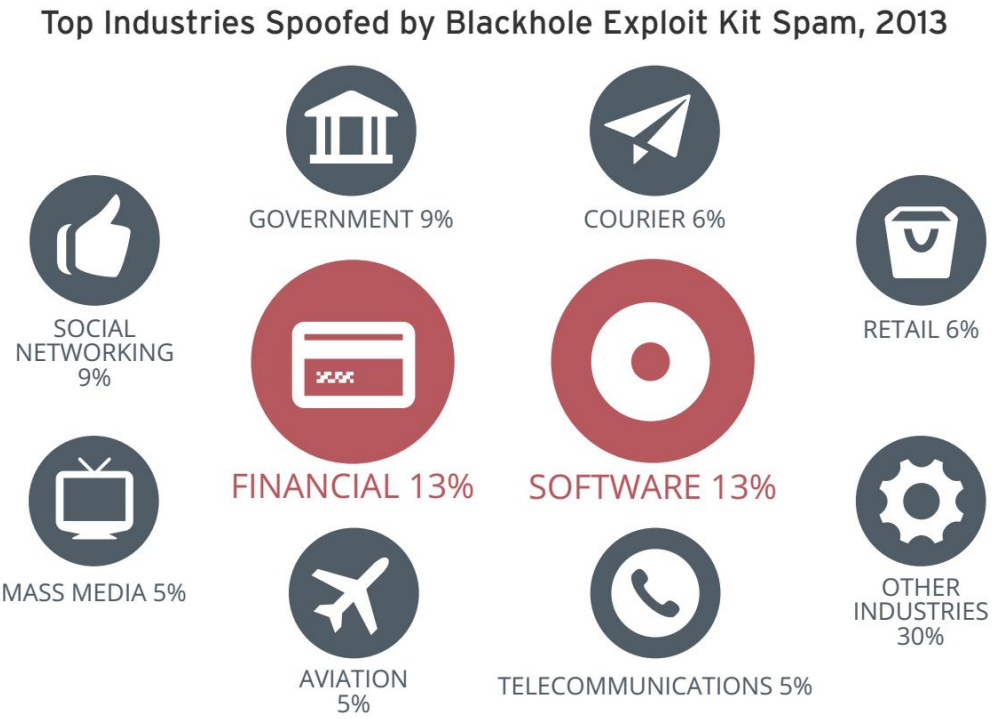
2014 年第 1 季度最新安全威胁信息

2013 年度趋势科技全球区安全威胁概要

以下是来自 2013 年趋势科技全球区安全报告的数据。
2013 年全球检测到勒索软件的数量与 2012 年相比翻了一倍。

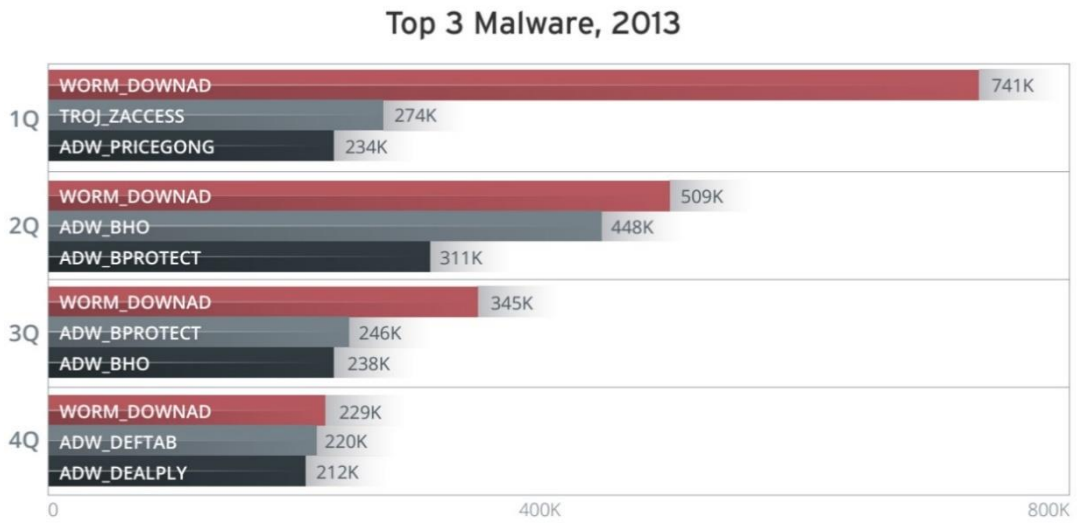


追踪 BlackHole 黑客工具包发出的垃圾邮件的攻击目标，25%是银行一类金融机构和软件行业：

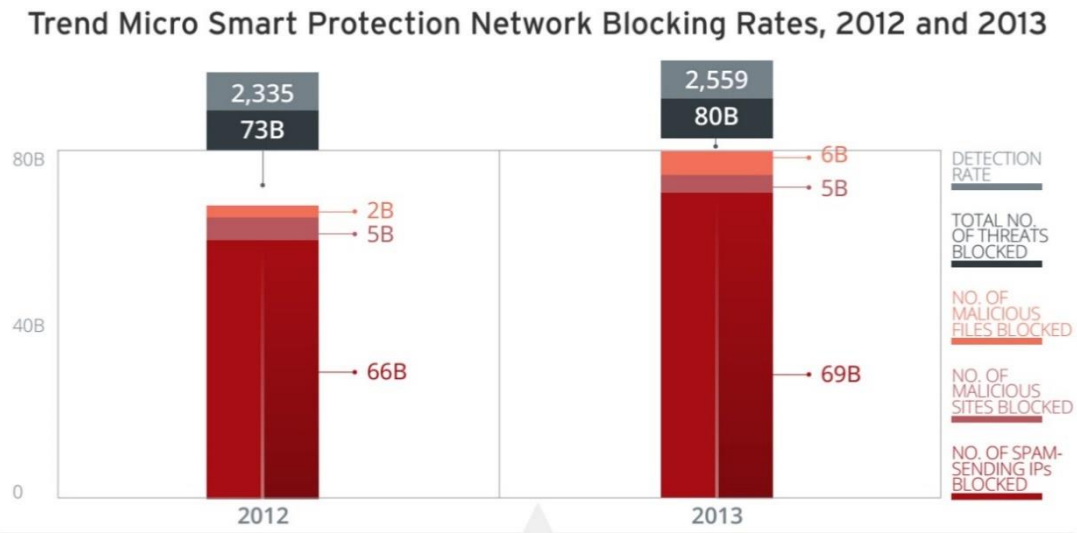


本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

DOWNAD 病毒在全球范围内是检测数量最高的病毒，但从 2013 年第 2 季度起，全球范围内的检测数量有所下降。



2013 年全年趋势科技智能防护网络较 2012 年的检测数量增加 70 亿次，目前平均每秒 SPN 检测威胁达 2,500 次。



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。

2013 年，政府机关是针对性攻击最大的攻击目标，下图列出了 2013 年整年遭到针对性攻击的行业：

针对性攻击发起者在 2013 年全球范围内发起无差别的大范围攻击，亚洲地区，特别是日本和台湾地区受到了相对更为严重的攻击。

需要查看更完整的 2013 年度全球安全报告请访问：
http://about-threats.trendmicro.com/us/security-roundup/2013/annual/cashing-in-on-digital-information/

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 1 季度国际安全威胁信息摘要

❖ 文件感染者与 ZBOT 再次联手

感染型病毒和 ZBOT 通常不会同时出现，但近期的一个案例中这两种病毒进行了“联手”行动，从而形成了一种新型病毒。这种特殊的感染型病毒——PE_PATNOTE.A（MD5：871246d00caffdbed56b1374975c368e）。它会在被感染的系统上的所有可执行文件里添加代码。而在这段代码里同时释放并执行 ZBOT 变种：TSPY_ZBOT.PNR（MD5：5c492c6300fd9def233bfaa56fb6b0f2）。TSPY_ZBOT.PNR 会被释放到以下位置：%USER TEMP%\ notepat.exe。

http://blog.trendmicro.com/trendlabs-security-intelligence/file-infectors-and-zbot-team-up-again/

❖ “WhatsApp 的桌面客户端不存在”被垃圾邮件攻击者利用

Facebook 以 160 亿美元巨额资金收购知名移动即时信息应用 WhatsApp！犯罪者很快利用该重磅新闻进行攻击：消息发出后仅 1 星期，就出现了声称该应用的一个新的桌面版本正在测试的垃圾邮件。

http://blog.trendmicro.com/trendlabs-security-intelligence/whatsapp-desktop-client-doesnt-exist-used-in-spam-attack-anyway/

❖ 网络犯罪地下产业链：俄罗斯，中国和巴西

互联网上存在着聚集网络犯罪分子的场所，不同的产品和服务被集中售卖。不用从零开始编写自己的攻击工具，犯罪分子就可以购买其他人已经制作好的工具，而且价格十分具有竞争力。像任何其他市场一样，供求规律决定着产品的价格和功能。值得注意的是，最近此类商品的价格一直都在下降。

http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminal-underground-economy-series-russia-china-and-brazil/

❖ Flappy Bird 和第三方 APP 商店

之前我们讨论过一些关于 Flappy Bird 的威胁。在挖掘它们的背景的过程中，我们发现了一些第三方的应用程序商店有分发或创建类似危险的移动应用程序的现象。

这些第三方应用商店针对越南手机用户，在流行应用中插入广告甚至恶意代码。这些应用会把用户的隐私置于危险之中，甚至可能造成财产损失——近期被植入木马 Flappy Bird 版本的应用为吸费软件获取利润并且还会连接 C&C 服务器来接收指令。

http://blog.trendmicro.com/trendlabs-security-intelligence/flappy-bird-and-third-party-app-stores/

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。

❖ 利用 Windows Power Shell 感染 WORD 和 EXCEL 文件的新型技术

针对 WORD 和 EXCEL 文件的恶意软件已经存在一段时间，最近我们发现了一个新的病毒家族 CRIGENT（也被称为“Power Worm”），它利用了一些新型技术。趋势检测名为 W97M_CRIGENT.A 和 X97M_CRIGENT.A。

http://blog.trendmicro.com/trendlabs-security-intelligence/WORD-and-EXCEL-files-infected-using-windows-powershell/

2014 年第 1 季度国内安全威胁信息摘要

❖ 情人、元宵双节邂逅送礼难　礼品“低价”网络陷阱危机重重

在农历新年过去之后，恋人们很快就迎来了“不送礼物会死”的情人节，更何况，今年情人节和元宵节同在 2 月 14 日这一天，玫瑰花等礼品的价格飞涨，这让很多恋人为了如何选择礼物而绞尽脑汁。恰恰在此时，有不法分子在网上散布能够“低价”购买情人节礼品的钓鱼网站，这些网站会盗取用户邮箱、银行卡账户等隐私个人信息。为了避免此类威胁，趋势科技提醒用户不要轻信那些低价诱惑，并使用网络安全软件来进行防护。

http://cn.trendmicro.com/cn/about/news/pr/article/20140214080420.html

❖ 趋势科技揭秘移动互联网“地下市场” 犯罪工具“明码标价”

为了帮助更多的普通用户深入了解并有效防范恶意风险，让掌中的智能终端和消费意愿真正“属于自己”，作为全球服务器安全、虚拟化安全及云安全领导厂商，趋势科技近期发布了《中国移动互联网地下黑市调查报告》。

http://cn.trendmicro.com/cn/about/news/pr/article/20140319070615.html

❖ 失联马航客机找到了？！ 趋势科技发现新诈骗主题 小心点击恶意邮件和诈骗视频

失联的马航客机到底在哪儿？何时可找到？当全世界都在为之祈祷的同时，黑客却趁机进行不法行为。全球服务器安全、虚拟化安全及云安全领导厂商趋势科技最近发现网上流传名为“马航 MH370 五分钟影片”的文档，其内藏窃取用户信息的恶意程序。除此之外还发现一种新的恶意邮件，利用“失踪马航客机”为话题，吸引用户点击恶意链接以观看影片并骗取个人信息，甚至要求用户通过社交网络分享给亲友。点击浏览的受害者超过 40%来自亚太地区！趋势科技将密切观察此恶意程序的后续发展，并提醒用户慎防“马航”相关的电子邮件或社交网络分享，谨慎点击以免受害。

http://cn.trendmicro.com/cn/about/news/pr/article/20140324064449.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。

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