中国地区 2015 年
第一季度
网络安全威胁报告

2015/4

CHINA RTL

目录

2015 年第 1 季度安全威胁 - 1 -

2015 年第 1 季度安全威胁概况 - 1 -
2015 年第 1 季度病毒威胁情况 - 4 -
2015 年第 1 季度新增病毒类型分析 - 4 -
2015 年第 1 季度各类型病毒检测情况分析 - 7 -
2015 年第 1 季度病毒拦截情况分析 - 8 -
2015 年第 1 季度热门新型病毒分析 - 10 -
2015 年第 1 季度流行病毒分析 - 12 -
2015 年第 1 季度 WEB 安全威胁情况 - 16 -
2015 年第 1 季度 WEB 威胁文件类型分析 - 16 -
2015 年第 1 季度 TOP 10 恶意 URL - 17 -
2015 年第 1 季度 WEB 威胁钓鱼网站仿冒对象分析 - 19 -
2015 年第 1 季度漏洞攻击威胁情况 - 21 -

2015 年第 1 季度最新安全威胁信息 - 23 -

2015 年第 1 季度安全威胁信息摘要 - 23 -
趋势科技全球区最新安全威胁概要 - 27 -

2015 年第 1 季度安全威胁

本季安全警示：

勒索软件

2015 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 **36** 万条。截止 2014.3.31 日中国区传统病毒码 **11.570.60** 包含病毒特征数约 **402** 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 **11,482** 万次。
- 本季度趋势科技在中国地区拦截的恶意 URL 地址共计 **19,614,751** 次。

从 2015 年年初至今，趋势科技监控到多个**勒索软件**家族变种，有关勒索软件的犯罪活动依旧活跃。今年一月，澳大利亚及新西兰地区用户最先遭到名为 TorrentLocker 变种攻击。很快我们便发现，TorrentLocker 感染并不仅限于这些地区，之后其它区域也陆续有用户感染这些变种。而后一个“改良版”的 CTB-Locker 变种随之而来，它提供新的“免费解密”服务，且延长了支付解密文件的期限，并且改变勒索通知消息的语言。此外，我们还监控到了勒索软件和信息窃取软件相结合的攻击。2015 年第一季度中发现的这些最新的勒索软件变种使用不同手段来确保他们的受害者支付赎金。下面列举了这些勒索软件变种的不同勒索方式：

1. CryptoFortress：“山寨版”勒索软件加密网络共享文件

上文中提到的 TorrentLocker 变种是最早出现的模仿 CryptoLocker 的山寨版本变种之一。这些山寨版本的勒索信息类似 CryptoLocker 或直接声称受害者的文件“是被 CryptoLocker 加密的”。然而现在 TorrentLocker 也有了模仿它的山寨版本，赎金信息完全相同，只不过显示名为“CryptoFortress”。但在进一步分析后发现 CryptoFortress 仅模仿了 TorrentLocker 的界面，其恶意行为与 TorrentLocker 并不相同。CryptoFortress 使用通配符来搜索进行加密的目标文件，这意味着满足设定条件的搜索结果都会被它一网打尽。它还可以加密网络共享目录下的文件——这一点不同于其它变种，它们只加密网络映射盘上的文件。目前该变种的趋势检测名为 ***TROJ_CRYPFORT.A***。

2. CRYPAURA：恐吓战术

勒索软件变种 CRYPAURA 家族有一个与其它变种迥然不同的怪异差别：它的程序中包含有关键词“埃博拉”。它的通讯功能使用的电子邮件地址通常是以下形式 *id-{id}_help@antivirusebola[.]com*。TROJ_CRYPAURA.F 是 CRYPAURA 家族的最新变种，它将字符串 id-{id}_fud@india[.]com 作为加密文件的后缀。该字符串被用作受害者后续进行

解密操作时进行联系的电子邮件地址。该变种的恶意行为与其它加密勒索软件变种无明显差别。但其进行加密的目标文件类型的数量从 39 种大幅增加至 102 种：其中大部分文件类型是各种应用软件的备份文件，另外一些则是与绘图、三维建模、乐谱和源代码相关联的文件。这些格式似乎是不常见的目标文件，但对于学校或公司来说，一旦失去这些文件损失会非常严重。加密目标文件后，恶意软件会更改受感染系统的壁纸，告知受害人去联系前文所说的电子邮件地址。受害者会收到回复，要求他们支付价值 500 美元的比特币。

3. Teslacrypt：与游戏玩家共升级

变种 Teslacrypt 趋势检测名为 ***TROJ_CRYPTESLA.A***，是有加密与游戏相关数据行为的第一个变种。（当然，它仍然加密受害者的文档、媒体文件和备份文件）。目标受害者和目标文件的转变可能和一直以来勒索软件的主要目标企业用户防御意识逐渐加强有关。网络罪犯认为年轻人通常在计算机上不会有重要到付款来赎回的文档，但是他们可能会愿意支付赎金来恢复他们的游戏数据，尤其是当他们花费时间和金钱来获得东西。目标游戏通常是广受欢迎的单机游戏和网络游戏，比如我的世界、星际争霸 II、刺客信条、使命召唤、魔兽世界和英雄联盟等。安装后，它会尝试删除系统的卷影副本，这样被加密的文档就不能被恢复了。加密文件使用.ECC 后缀名。病毒在加密系统中的文件后会显示一个界面并改变墙纸，用来显示勒索信息，用于指导受害者访问一个 Tor 支付网站来支付价值 500 美元的赎金。和其它加密勒索一样，Teslacrypt 提供免费的解密或“免费增值功能”，以证明他们有能力解密文件。

概括来说，本季度网络罪犯发动的勒索攻击呈以下趋势：

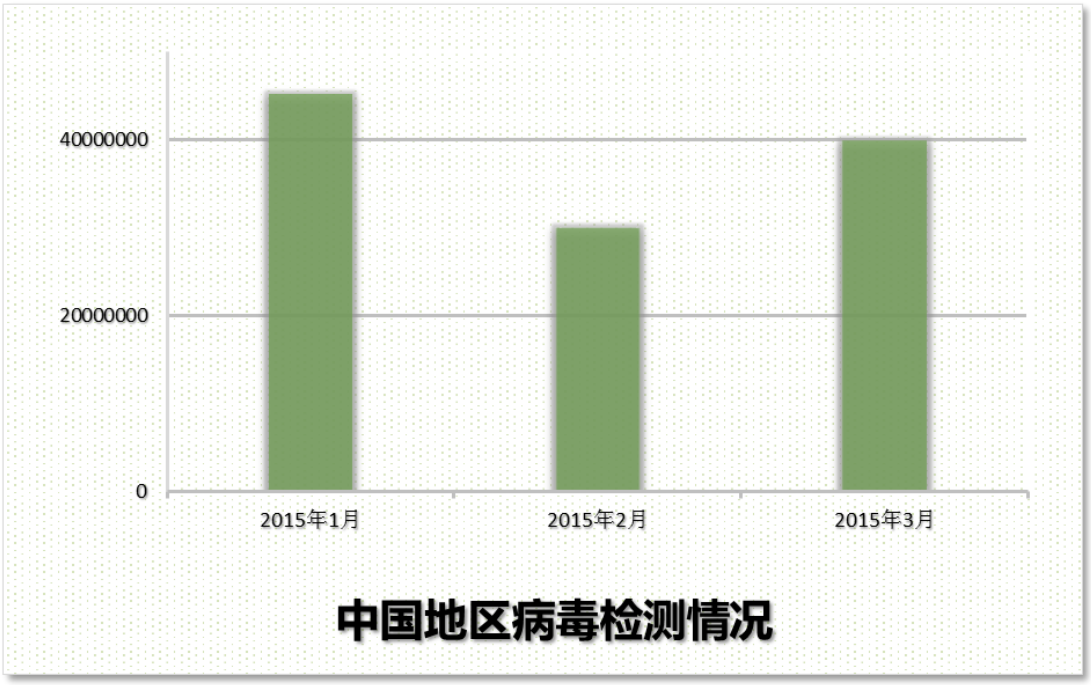
1. 为了网罗更多的受害者，越来越多的文件类型或扩展名被列为加密目标。
2. CryptoLocker 的恶名被加以利用，大多数新的勒索软件变种使用 CryptoLocker 之名来增加恐吓力度。
3. 卷影副本的备份文件也会被病毒删除，使得文件无法恢复。卷影副本是 Windows 一项可以手动或自动进行文件备份的功能。删除卷影副本的备份文件使得受害者只能受网络罪犯的任意摆布。
4. 加密勒索开始提供“免费增值”解密若干加密文件的服务，以此来证明他们可以解密文件。

当然有些东西不会改变，特别是勒索软件的匿名性。比特币始终是首选付款方式，这样网络罪犯能够在不暴露身份的情况下拿到钱财。

以下是一些针对用户的建议提醒：

我们分析勒索软件的变化趋势的原因是希望用户应该时刻提高警惕来保护自己的设备和文件。

安装安全软件及仔细检查电子邮件可以有效防止被感染。比如不要打开来自未知或未经证明的发件人的电子邮件。用户访问之前可以先***检查网站信誉***。当涉及处理未知或未经验证的电子邮件、文件或网站时，宁可谨慎一些也不要轻易打开。受害者想要以支付赎金的方式来找回文件的做法不会有保障，受害者可能会遇到支付赎金后依然不能找回任何文件的情况。用户可以定期备份文档来更好地防止这种情况的发生。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

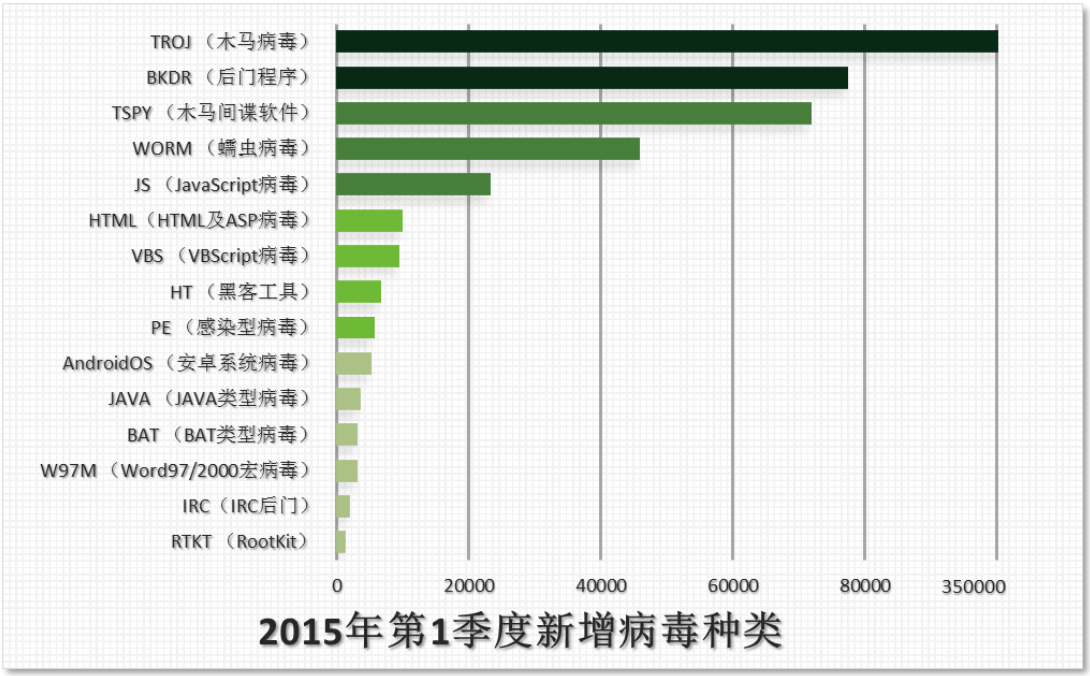


2015 年第 1 季度中国地区病毒检测数量图

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。

2015 年第 1 季度病毒威胁情况

2015 年第 1 季度新增病毒类型分析



2015 年第 1 季度新增病毒类型分布图

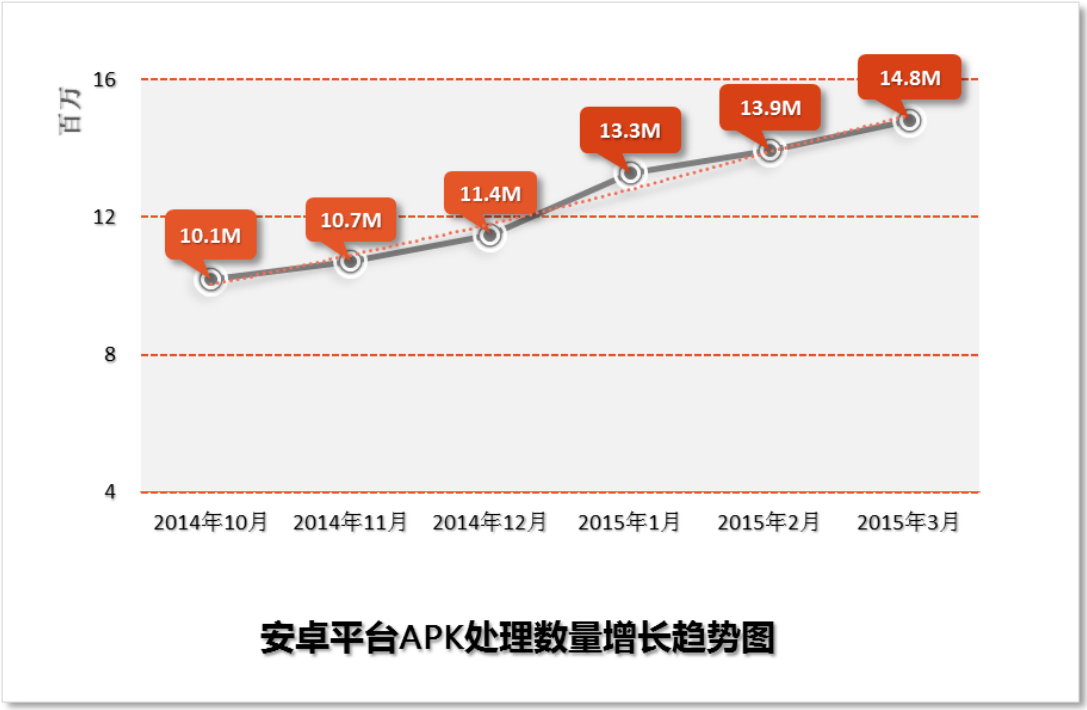
在 2015 年第 1 季度新增病毒种类中，以 **TROJ（木马病毒）**类型增幅最大。据统计，本季度新增木马病毒特征共计 **353,286** 个，比上一季度新增数量有所增加。木马病毒通常以窃取攻击目标的账户密码为目的，从而获得经济利益。在中国地区，此类型病毒一直高居榜首。

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 HTML（HTML 及 ASP 病毒）。**本季度新增病毒种类排名无明显变化。

在新增病毒类型分布图中所显示的病毒类型中，和网页挂马有关的 JS (JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒具有一定威胁性。挂马的网页被添加了恶意代码，浏览者访问这些网页时，恶意文件就会自动下载到本机，执行恶意操作。

此外，检测名以 HT_打头的病毒类型“黑客工具”的检测类型排名依然榜上有名。黑客工具在网络黑市上大量贩卖，黑客获取的途径十分简便，这造成了此类型病毒数量居高不下的原因。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。

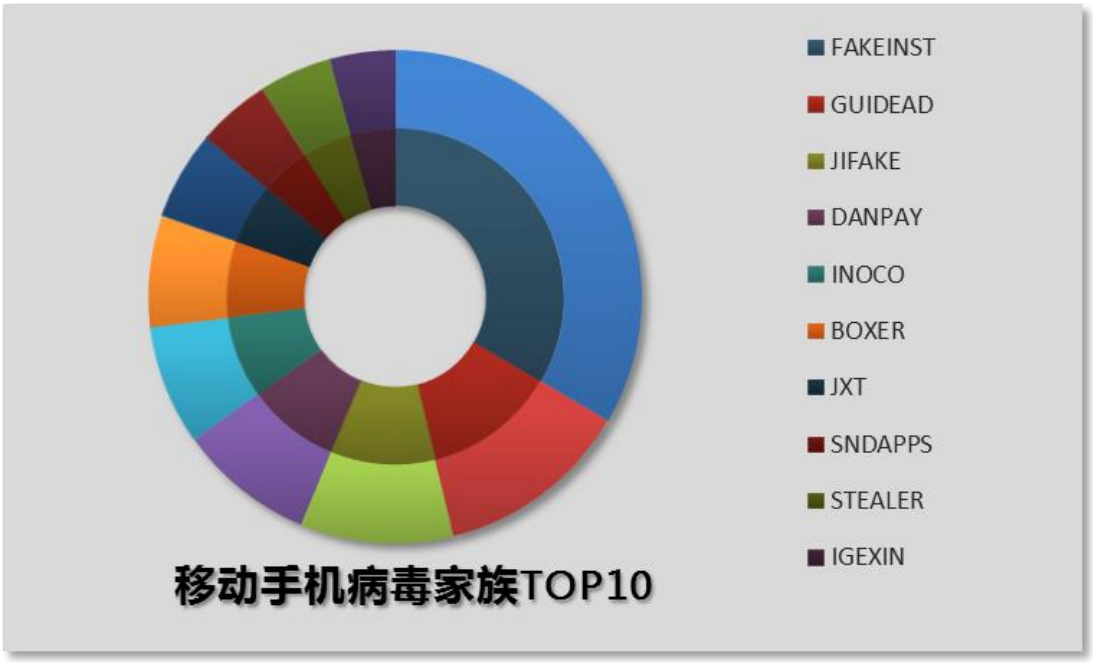


2015 年第 1 季度安卓平台 APK 处理数量走势图

截止到 2015 年 3 月 31 日，趋势科技发布中国区移动客户端病毒码版本是 1.857.00，大小 21,279,494 字节。

趋势科技对 APK 文件的处理数量在 2015 年第 1 季度依旧呈上升趋势。截止到本季度的 3 月底，处理数量累计达到 1,483 万个。从最近 6 个月的处理数据走势图来看，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。



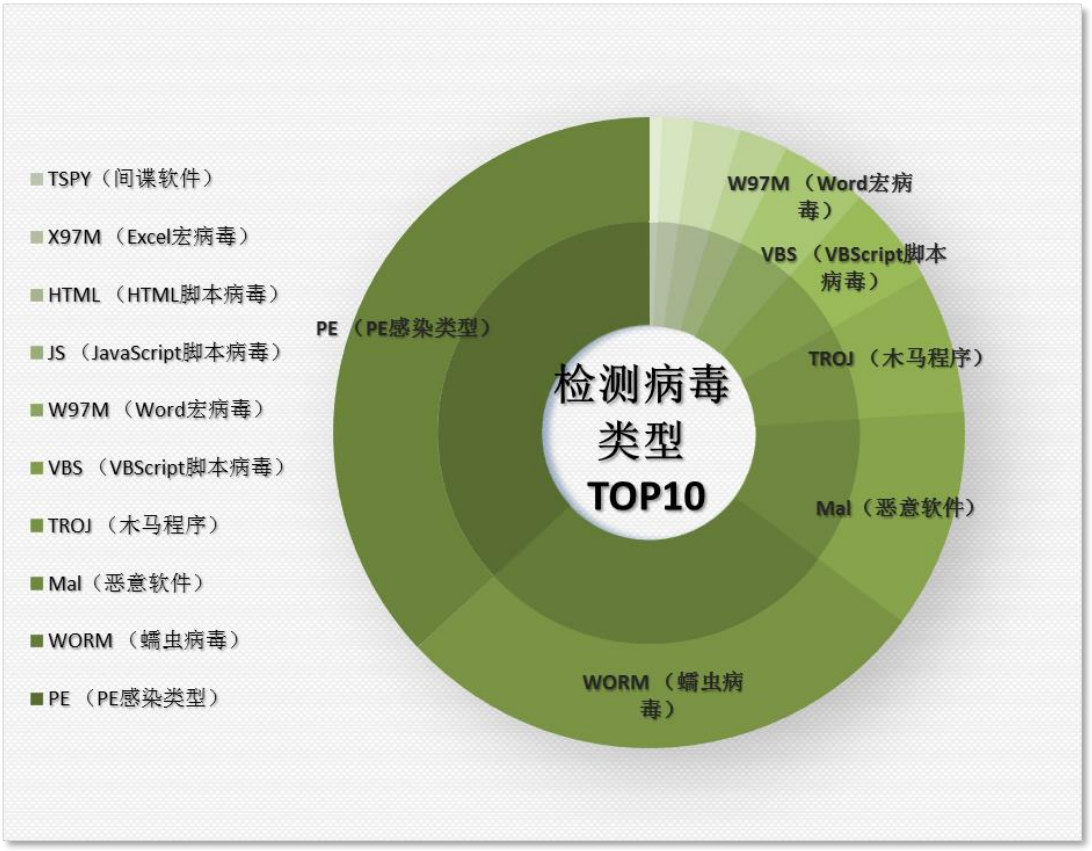
2015 年第 1 季度移动手机病毒家族 TOP10 分布图

在 2015 年第 1 季度感染安卓平台的手机病毒家族中，FAKEINST 家族数量最多，占到总数的 33.42%；GUIDEAD 家族位列第二，占 12.78% ；JIFAKE 家族居第三位，占总数的 10.07%。排列前三的家族总数超过了 50%。

在 2015 年第 1 季度中，趋势科技发现在各大中文应用商店中出现了大量重打包的安卓应用。这些应用号称“免费”，但最终用户还是要掏出钱包付钱。因为安装后用户就会发现，它们不是自带大量广告就是会订购付费服务。(这类程序一般是不会出现在官方 Google Play 商店中的。) 这些程序的出现有两个渠道。第一种渠道是国外的应用经中国的一些公司本地化、 重新打包后发布。但在本地化过程中，一些不良公司会向程序中加入自己的代码来达到推送广告和通过短信收取费用的目的。第二种渠道是正版软件被破解并加入广告和其它代码。在这种情况下重打包文件被加入的代码有可能是恶意的。破解者（个人及公司）将正版程序破解，向其中加入自己的代码，通过主流应用商店传播。通过造假，这些重打包程序还能登上应用商店的下载排行榜前列，拥有百万以上的下载量。这些应用会在运行的时候弹出许多广告，试图关闭它们会导致下载其他程序并带来更多的广告。更有甚者，会伪装成安全软件请求 root 权限，但实际上它们是广告软件，这样的程序更难清除。趋势科技在此提醒中国地区的安卓平台用户，在下载一些热门应用时要注意辨别此类恶意安装包。

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。

2015 年第 1 季度各类型病毒检测情况分析



2015 年第 1 季度病毒检测类型分布图

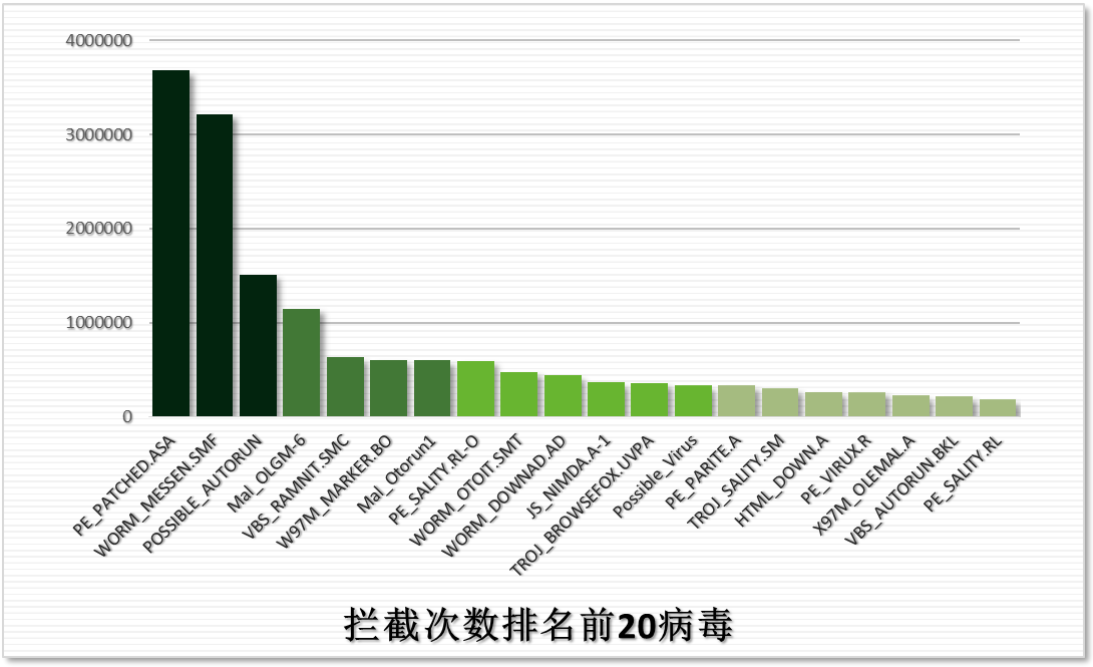
2015 年第 1 季度检测到的病毒种类中，PE 类型病毒感染数量在所有类型中所占比重最大，占到总检测数量的 36.9%。在本季度中，PE_PATCHED.ASA 检测数量依然排名第一，此外 PE_SALITY、PE_PARITE、PE_VIRUX 家族检测数量排名靠前。PE_PATCHED.ASA 病毒文件是一个被修改过的系统文件 sfc_os.dll，这个文件用以保护系统文件的执行模块，该文件一旦被修改，系统将失去文件保护的功能。

本季度蠕虫病毒占检测类型总数的 27.88%，本季度该类型病毒占比比上一季度明显上升。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。蠕虫病毒的一个重要特征是它们往往会在各个目录下复制自身副本，这一特征会占用大量系统资源。

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。上一季度中监控到检测数量较多的 WORM_MESSEN 家族本季度持续上升。

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。

2015 年第 1 季度病毒拦截情况分析



2015 年第 1 季度病毒拦截情况图

在 2015 年第 1 季度拦截次数排名前 20 位的病毒检测名中，PE 感染类型病毒检测数量依然占据总数的绝大部分。由于 PE 病毒有大量感染可执行文件的行为，而且感染速度迅速，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 367 万多次，拦截次数远高于其它病毒检测名。

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

2015 年第 1 季度热门新型病毒分析

本季度热门病毒 JS_DLOADE.XXPU 与 2015 年三月份检测到的 CryptoWall3.0 勒索软件攻击有关联。它利用社会工程学，以垃圾邮件的恶意附件形式传播。一旦解压执行，它会下载 CryptoWall 恶意软件至受感染的系统上并自动执行。

它会自动执行下载的文件。然后，一系列勒索行为就会开始执行。

JS_DLOADE.XXPU 恶意行为示意图

病毒的详细信息如下：

病毒检测名：

JS_DLOADE.XXPU

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：

该木马伪装成一个恶意电子邮件附件，用这种方式抵达目标系统。

病毒下载：

该木马连接以下网站，下载并执行恶意文件：

HTTP：//{BLOCKED} okolrt.com/images/one.jpg

HTTP：//{BLOCKED} okolrt.com/images/two.jpg

HTTP：//{BLOCKED} okolrt.com/images/two.jpg

并用以下名字保存下载文件：

%User TEMP%\542824559.exe

%User TEMP%\589878543.exe

（注：%User TEMP%是用户的临时文件夹，Windows 2000 和 Windows Server2003 和 Windows XP（32 位和 64 位）的环境下它通常在 C:\Documents and Settings\{user name}\Local Settings\Temp 路径下; Windows Vista（32 位和 64 位），Windows7（32 位和 64 位），Windows8（32 位和 64 位），Windows8.1（32 位和 64 位），Windows Server 2008 和 Windows Server2012 的环境下它通常在 C:\Users\{user name}\AppData\Local\Temp 路径下。）

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

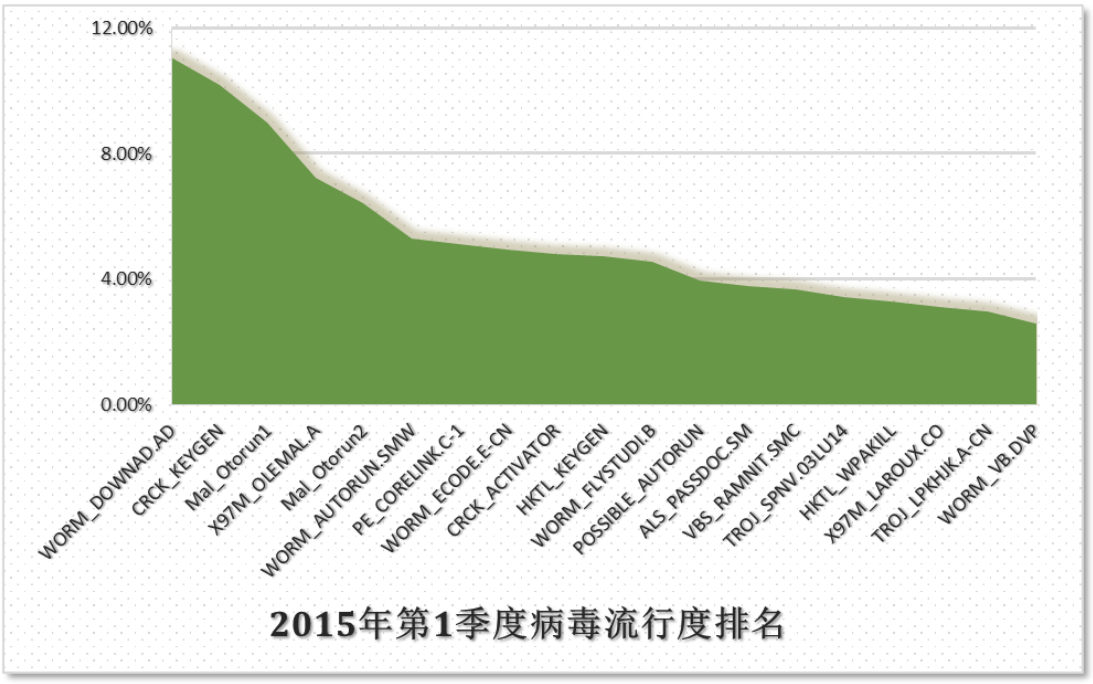
64 位 Windows 操作系统请使用：

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

相关链接信息：

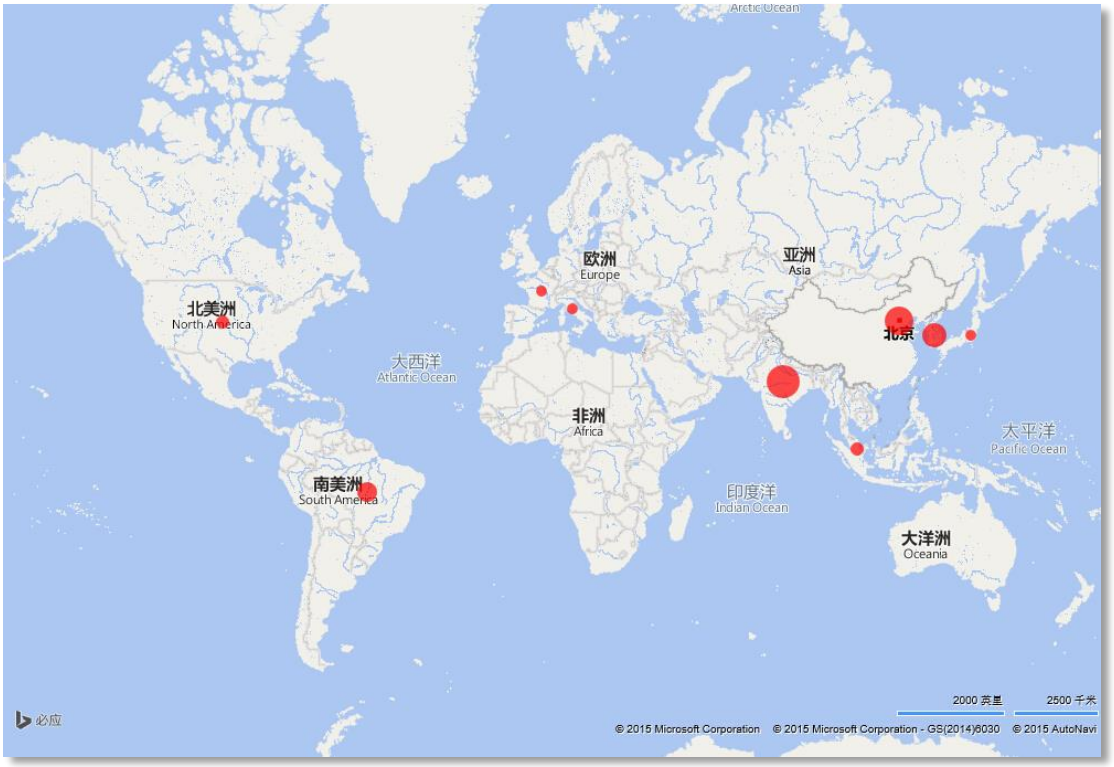
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/JS_DLOADE.XXPU

2015 年第 1 季度流行病毒分析



2015 年第 1 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。



2015 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 2015 年第 1 季度，约有 11.07% 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 2015 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。

2015 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

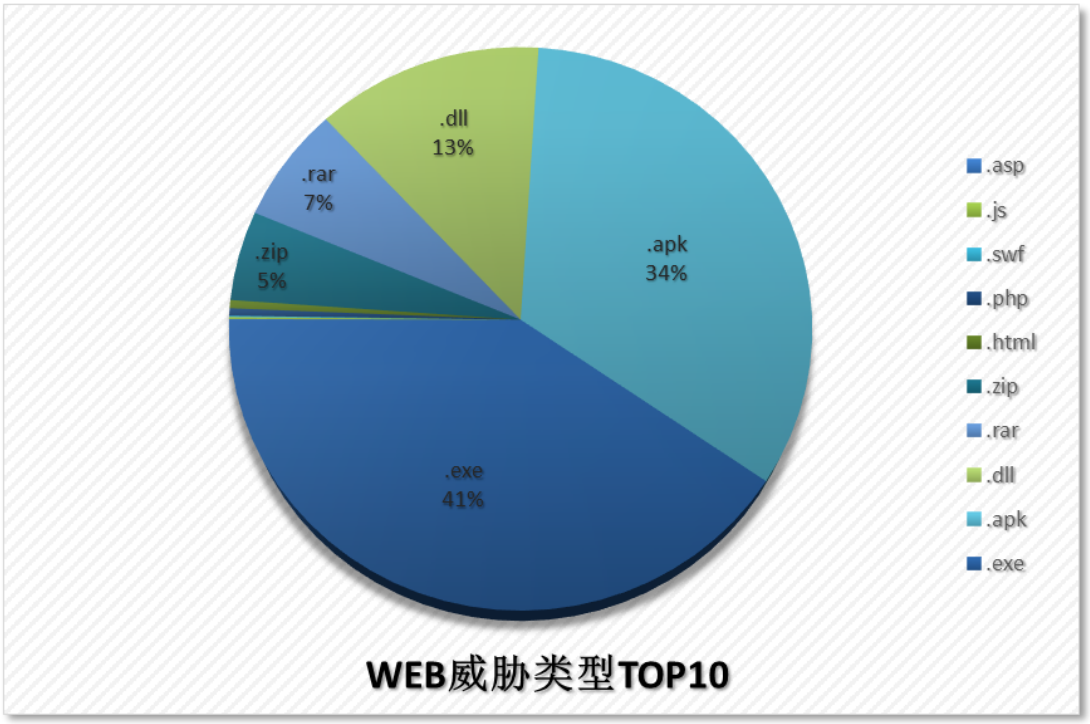
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2015 年第 1 季度 WEB 安全威胁情况

2015 年第 1 季度 WEB 威胁文件类型分析

在 2015 年第 1 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 41%，虽然所占比例比上一季度有所下降，但依然占据第一位。.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.APK 和.DLL 文件数量上升明显。特别是.APK 文件，所占比例达到 34%，在本季度中跃居第二位，仅次于.EXE 格式文件，对于此类格式文件我们应加以关注。



2015 年第 1 季度中国地区 WEB 威胁文件类型分布图

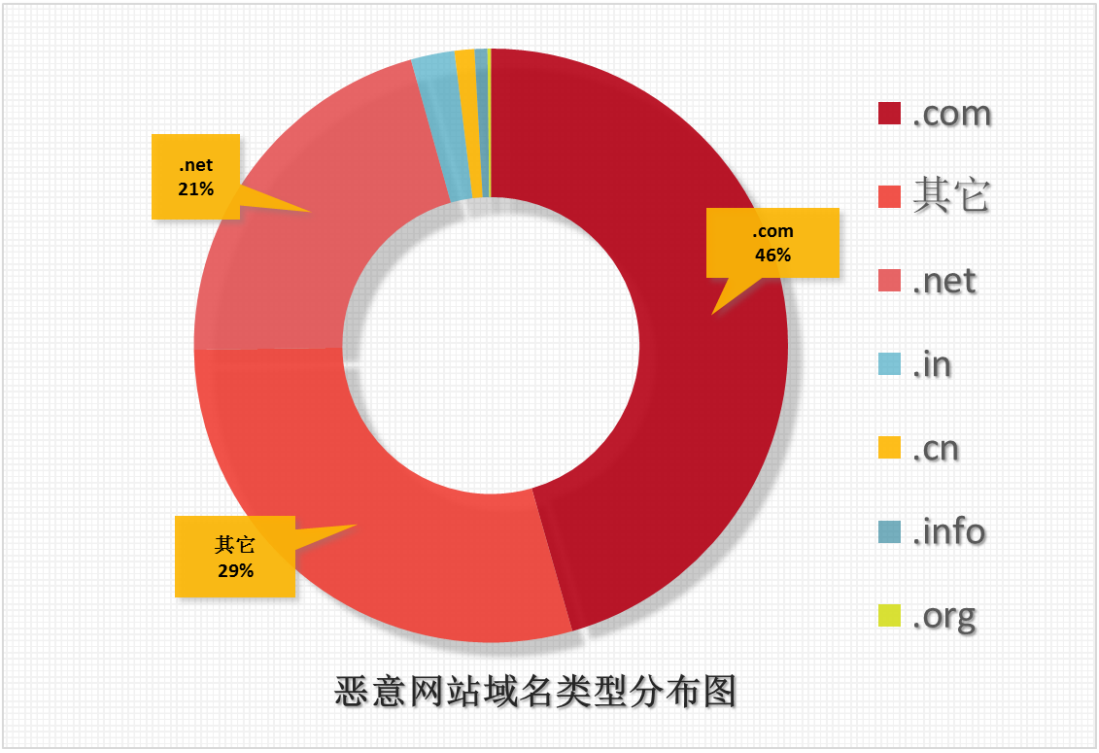
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2015 年第 1 季度 TOP 10 恶意 URL

TOP10 恶意URL		
恶意URL	描述	点击量
http://imdd***3.com:6688/511***395.html	包含恶意软件或钓鱼信息	2,830,130
http://traffi***rter.biz/	包含恶意软件或钓鱼信息	1,760,246
http://trafficcon***r.biz/4vir/anti***ware/loadadv.exe	网站直接或间接帮助传播恶意软件或恶意代码	1,755,824
http://downl***.2***45.cn/23***safe/2345PCSa***ouye.exe	网站直接或间接帮助传播恶意软件或恶意代码	548,630
http://220.18***41.104/msv***ery	网站直接或间接帮助传播恶意软件或恶意代码	466,207
http://download.ppl***om/tipsdone/1.0***.8/tipsdone(1.0.0***?agent=ppap	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	462,457
http://106.120***.174/clo***uery.php	网站直接或间接帮助传播恶意软件或恶意代码	444,263
http://106.120.167.***/clo***uery.php	网站直接或间接帮助传播恶意软件或恶意代码	444,206
http://106.120.167.***/clo***ry.php	网站直接或间接帮助传播恶意软件或恶意代码	443,195
http://106.120.162.***/clo***ery.php	网站直接或间接帮助传播恶意软件或恶意代码	443,165

2015 年第 1 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。

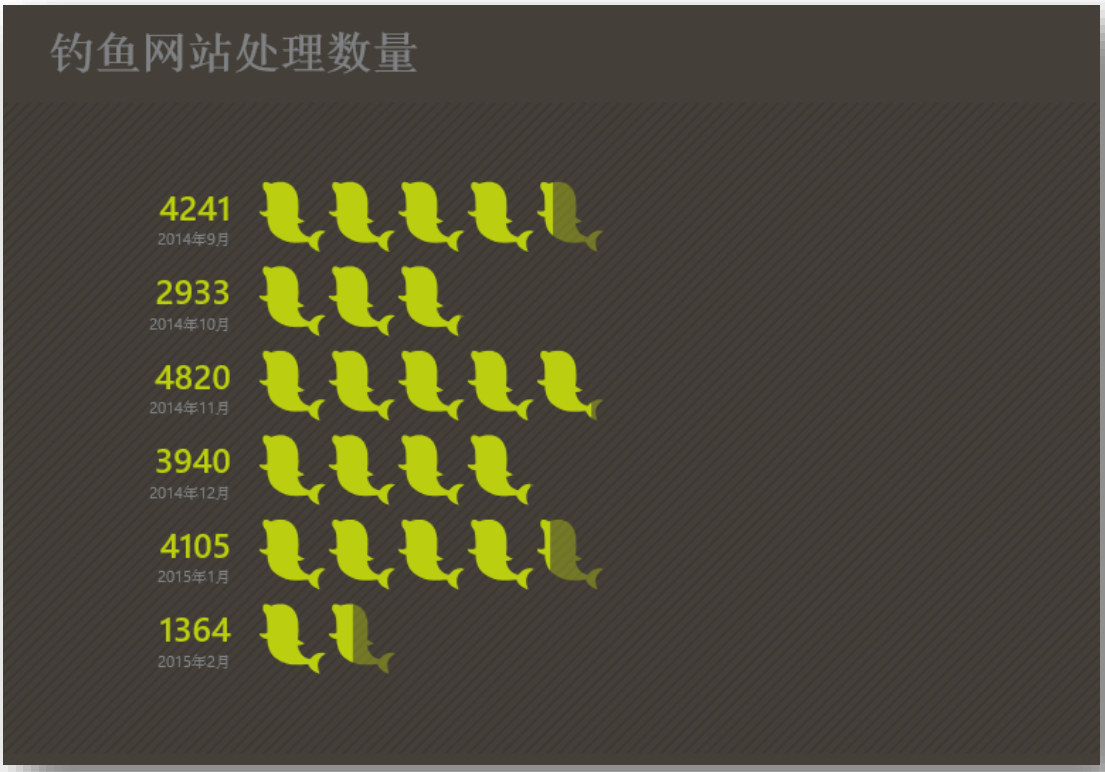


2015 年第 1 季度恶意网站域名类型分布图

2015 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、.CN、.IN、的域名的站点占总数 68.55%。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。

2015 年第 1 季度 WEB 威胁钓鱼网站仿冒对象分析



2015 年第 1 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 9 月至 2015 年 2 月共计 6 个月中，处理钓鱼网站共计 **21,403** 个。

在本季度中，趋势科技发现以信用卡为目标的网络钓鱼诈骗又出现新手段。不法分子通过搜索引擎大肆推广钓鱼网站，并利用钓鱼网站或手机 App 应用来进行诱惑诈骗用户。这些钓鱼网站或 App 应用以修改信用卡密码、清除不良信用记录等方式为诱饵，以此骗取消费者的信用卡信息，进而盗取信用卡内资金。趋势科技发现，很多钓鱼网站或 App 应用并不针对特定的银行，是利用各银行监管的灰色地带，降低被封堵的几率，使用户暴露在更大的风险之中。

一些钓鱼网站打着“提高信用卡额度”的标题实行诈骗，识别难度极高，不法分子不仅精心设计了网站界面，使其看起来与正规网站无异。还会在大量网站中嵌入该钓鱼网站的域名，并通过搜索引擎优化（SEO）技术使其排到搜索结果页面的首页，消费者稍不留神就有可能误入该网站。更令人担心的是，其页面并不包含任何恶意代码或捆绑恶意插件，这使其容易躲过安全防护软件的监测，进而诱使用户提供信用卡卡号、密码、有效期等重要信息。

趋势科技通过进一步研究发现，不法分子在盗取被害者信用卡资金之后，还会通过购买点卡、“兼职返现”等行为，通过互联网将钱“洗白”。而且，这个所谓的兼职返现其实是一

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。

个“套中套”，不法分子会引诱那些喜欢贪小便宜的人购买点卡以获得“返现”。然而，当被害者持续投入之后，最终会发现这笔钱掉进了不法分子的钱包。

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。

2015 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	440439
MS08-067	401
CVE-2014-4113	65
CVE-2014-4148	65
CVE-2010-2568	59
CVE-2010-0806	17
CVE-2012-0507	9
CVE-2015-0313	7
CVE-2012-0002	6
CVE-2012-0152	3

2015 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
MS08-067	http://technet.microsoft.com/zh-CN/security/bulletin/ms08-067
CVE-2014-4113	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2014-4113
CVE-2014-4148	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2014-4148
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-2012-0507	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-0507
CVE-2015-0313	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2015-0313
CVE-2012-0002	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-0002
CVE-2012-0152	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-0152

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。

2015 年第 1 季度最新安全威胁信息

2015 年第 1 季度安全威胁信息摘要

2015 年第 1 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。

❖ 趋势科技发布 Ponemon 全球网络隐私调查：物联网时代网络隐私权受挑战

尽管消费者要求隐私权得到保护，但却不愿改变习惯来保护自己。这是趋势科技最近委托第三方研究机构所做的一项调查所发现的主要结论之一。根据 Ponemon Institute 研究机构一项名为“联网生活的隐私与安全：针对美国、欧洲及日本消费者的调查”(Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers)的全球问卷结果显示，多数的消费者认为物联网(Internet of Things，简称 IoT)给生活带来的便利胜过隐私权的担忧，并有 75%的受访者觉得对自己的个人信息缺乏掌控能力。此外，该研究也调查了消费者对隐私权的看法、他们是否愿意改变习惯，以及他们认为自己的个人信息有多少价值。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20150409115344.html

❖ 新型病毒任性绑架手机 以假关机为掩护疯狂窃取用户隐私

一款名为 PowerOffHijack 的安卓关机劫持软件正在肆虐中国地区。该软件的“创新”之处在于，它会自动劫持关机过程，让用户误以为自己已关闭了手机。而事实上，该软件利用关机行为作为“掩护”，暗中窃取用户的账号、短信等个人信息。移动威胁已经到了无处不在、无孔不入的地步，要避免被此类恶意软件感染，趋势科技建议用户谨慎下载未确定安全性的第三方应用程序，并安装安全可靠的移动安全防护软件。

研究显示，这款软件主要在第三方安卓 App 商店传播，并针对那些已经获得 Root 权限的安卓手机。一旦恶意软件进入到用户的安卓设备上，它就会获取硬件控制权限，并劫持关机过程。当用户试图关机时，恶意软件会通过播放关机动画等方式，让用户确信手机真的已关机。骗过用户之后，该恶意软件就会在后台进行抓图、读取联系人信息等动作，并发送到指定服务器上。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20150319121025.html

❖ 趋势科技揭露全球最新跨国犯罪、预谋性私密视频勒索犯罪手法

趋势科技揭露了亚太区全新跨国私密视频犯罪行为。犯罪集团通过诱拐受害者拍摄私密视频并下载可窃取隐私的 APP，继而威胁受害者将在网络上散布私密视频，以勒索赎金。犯罪集团亦可能借此个人信息，再次窃取受害者财产。趋势科技指出，韩国、日本受害人数持续攀升，临近的中国有可能成为犯罪集团下一波攻击目标，提醒用户提高警觉。

此外，趋势科技观察，网络犯罪平台过去多以电脑为主，现在转变为多平台犯罪，除了电脑以外，手机更为黑客锁定新目标！建议消费者不要轻易下载来源不明的 App，并通过趋势科技移动安全个人版等高信誉的移动安全防护软件，协助侦测手机内的恶意程序、过滤恶意网址，降低个人信息被窃取风险，以免遭受个人隐私及钱财双重损失。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20150326100801.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。

❖ 网购热门商品的陷阱，你躺枪了没？

去年是购买智能手机、平板电脑、玩具、电动游戏和相机的好时机，这些热门商品有着大量的网络点击率，但也有许多网络威胁被制造来针对搜索这些东西的人们。我们列出了最受欢迎的礼物清单，并通过趋势科技 SPN 智能云防护网络来加以分析，希望帮助大家筛选出可能存在的威胁。

http://blog.sina.com.cn/s/blog_5e96245b0102vecf.html

❖ 当你的个人信息流入黑市……

数据货币化不再只限于信用卡诈骗，身份盗窃经过长时间的演变也跟上了科技的脚步。今天的地下经济会买卖你的在线数据——电子邮件、社交媒体、在线游戏和网络银行账号登录证书等等，就跟一般商家买卖货物、商品和服务一样。对于黑客来说，网络账号就像是一口可以深掘的井。而对于受害者来说，影响并不仅仅只是失去金钱或变得不便。丢失个人资料会造成一辈子的影响，因为资料不会过期，可以无限地重复使用和在地下交易。

谁负责保护数据？当然，数据拥有者或是我们信任去拥有我们个人资料的公司应该要保证其安全，他们需要遵循一定的规则和标准。但是我们也有责任去保证自己的数据安全，我们在给出数据时要认真了解对象是谁。毕竟，如果我们没有给出去，它也不会落在别人手里。

http://blog.sina.com.cn/s/blog_5e96245b0102vgno.html

❖ 勒索软件新发展，免费解密你敢信吗？

趋势科技在去年七月发现一个称为 Critroni 或 Curve-TOR-Bitcoin（CTB）Locker 的加密勒索软件。最近我们观察到 CTB 恶意软件的改进，现在提供了“免费解密”服务、延长文件解密期限及提供变更勒索信息语系的选项。这个新变种还要求支付 3 比特币（约 630 美元），而在七月所看到的旧版本只收取 0.02 比特币或 24 美元。

除了这些改进外，我们也看到这些攻击在某些地区激增，主要是欧洲、中东和非洲（EMEA）、中国、拉丁美洲和印度。

http://blog.sina.com.cn/s/blog_5e96245b0102vfea.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。

❖ CryptoWall 3.0 勒索软件与 FAREIT 间谍软件联手

近期，趋势科技首次发现一个包含了间谍软件的勒索软件。最新版本的勒索软件 CryptoWall3.0 中使用了硬编码的 URL。硬编码 URL 采用了高度混淆，使得研究人员无法方便提取出。由于拦截 URL 是一种被动手段，成功拦截前有一段空档期，恶意软件足够使用这段时间与 C&C 服务器通信获取 RSA 公钥来进行文件加密。

http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/

❖ 最新 Flash 漏洞被加入 Nuclear 漏洞利用工具包中

我们通过趋势科技云安全智能防护网络检测到 Nuclear 漏洞利用工具包已更新，新版本包括了近期被修复的 Adobe Flash Player 漏洞 CVE-2015-0336。我们于今年 3 月 18 日首次探测到与此有关的恶意活动迹象。

该漏洞在 Adobe 对 Adobe Flash Player 的三月常规更新中进行了修复，软件版本为 17.0.0.134。然而，我们收到的反馈数据显示许多用户仍在运行较旧的版本 16.0.0.305。 我们建议用户立即将 Flash Player 版本更新到最新，而这起事件很好地提醒我们为什么要这么做。我们曾于三月初指出，Flash 播放器被漏洞利用工具包锁定为目标的频率逐渐增高，而且近期这种趋势没有改变的趋势。

http://blog.trendmicro.com/trendlabs-security-intelligence/freshly-patched-flash-exploit-added-to-nuclear-exploit-kit/

❖ .gov 域名被利用进行钓鱼攻击

品牌拥有者经常使用 SPF 和 DKIM 来保护自己的品牌免于被电子邮件伪造。例如，一个品牌拥有者可以在多个顶级域名（TLD）（如.com，.net，.org 等）下注册相同域名，并公布所有这些域名的 SPF/ DKIM 记录（即使它们并不活动）。虽然这方法普遍有效，但有一个漏洞：.gov 的 TLD 怎么办？

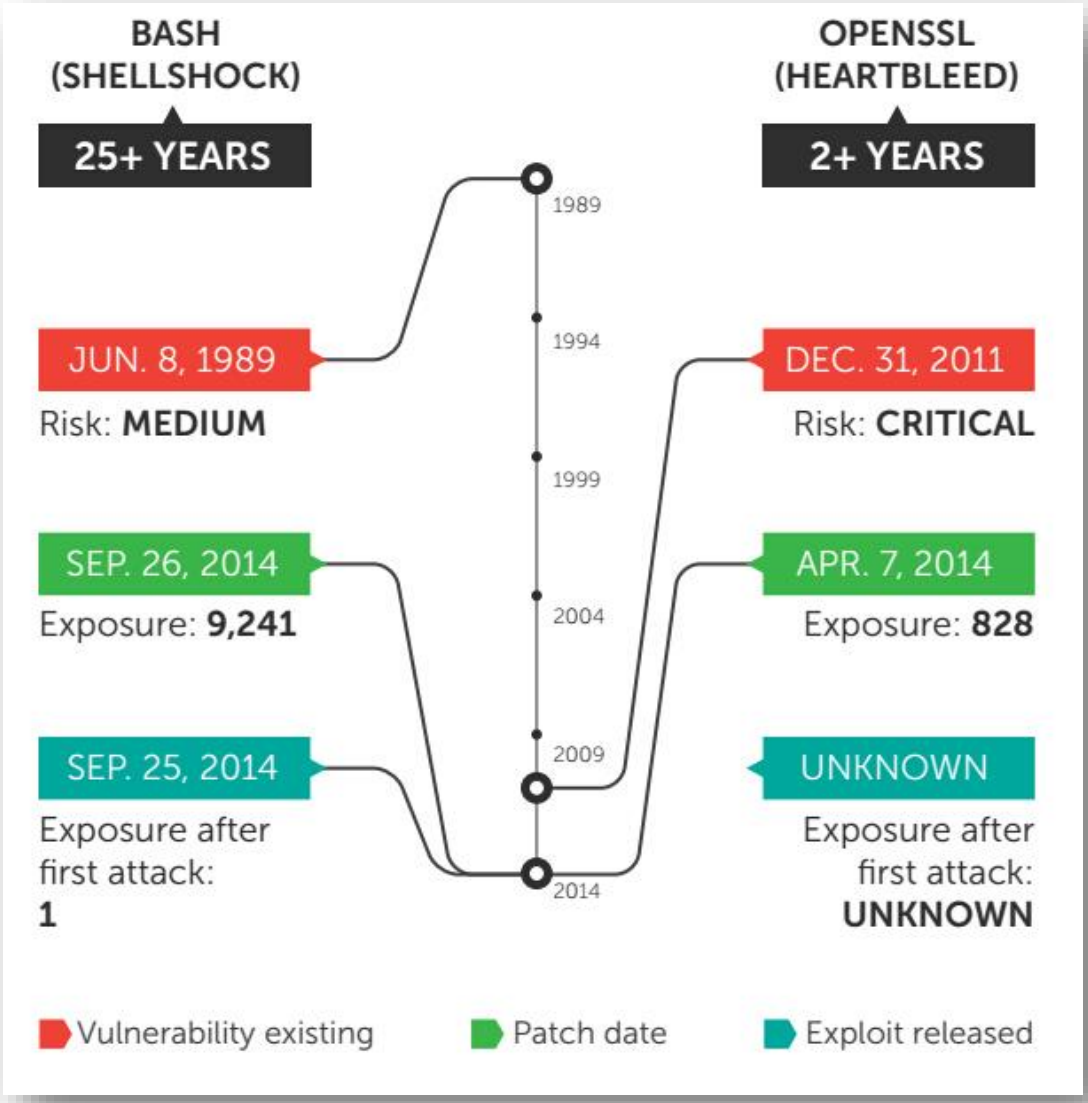
这个漏洞最近在针对美国运通公司的攻击时被利用，这次大规模钓鱼攻击开始于 3 月 4 日。攻击者发出的电子邮件模仿美国运通公司的通知，其中包含一个钓鱼网站链接。我们确定了此次攻击中使用了超过 50 个不同域名的钓鱼网站。这些域名托管在受害域名上，格式为：hxxp://{compromised website}/amerrricaneaxpress/security.html。

http://blog.trendmicro.com/trendlabs-security-intelligence/phishing-and-the-gov-tld/

趋势科技全球区最新安全威胁概要

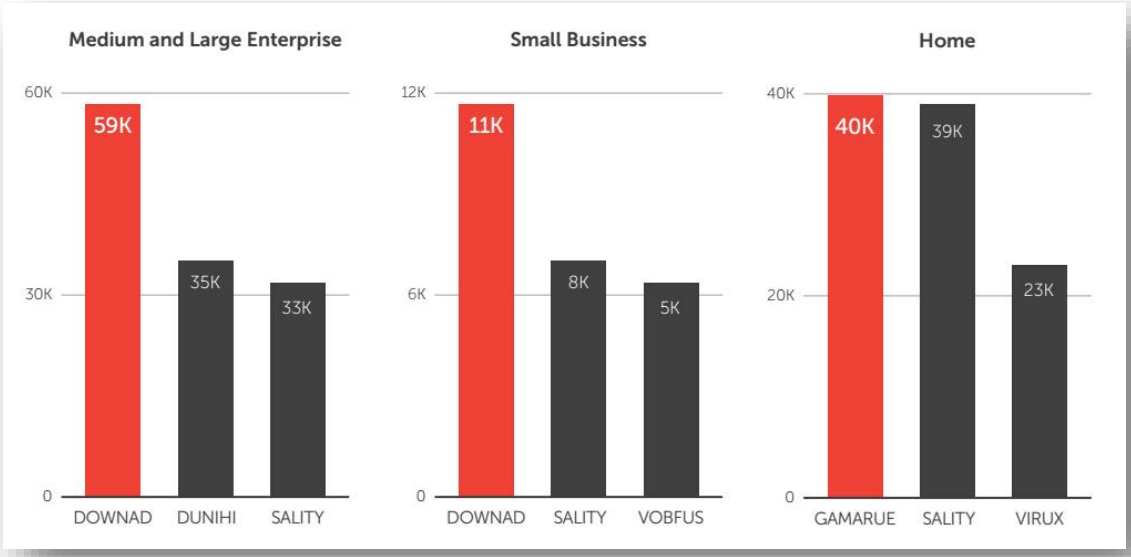
以下是来自 2014 年第 4 季度趋势科技全球区安全报告的数据。

下图列出了 2014 年披露的高危险性漏洞（Shellshock 和 Heartbleed）信息。



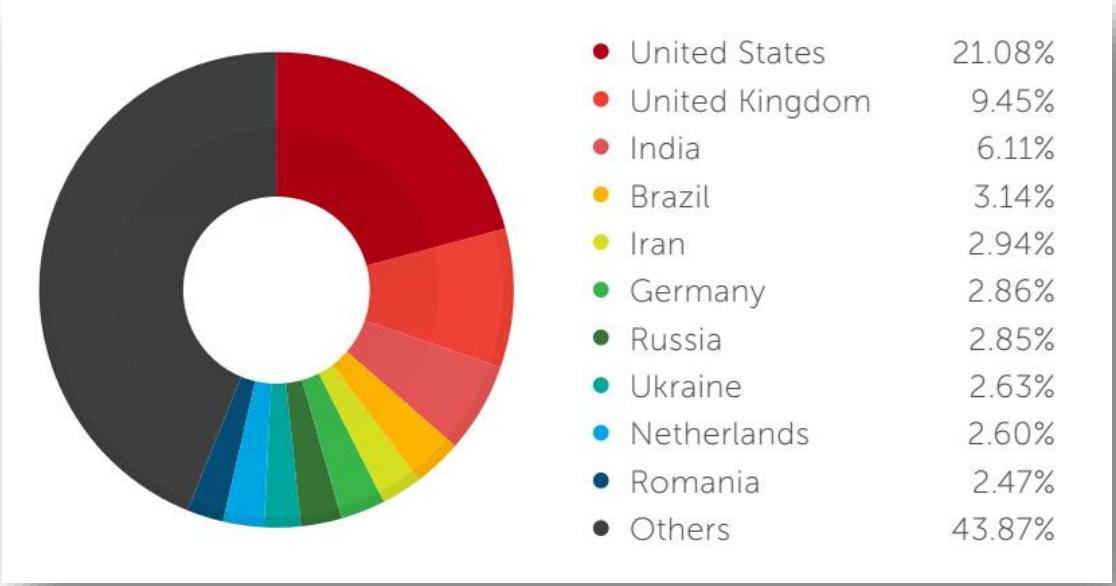
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

下图列出了不同用途的计算机在 2014 年中感染最多的病毒家族。DOWNAD 家族依然是企业感染最多的病毒。这与许多公司还在使用 Windows XP 系统有关。XP 系统容易受到这种病毒的攻击，特别是在微软已停止对 XP 的支持之后。



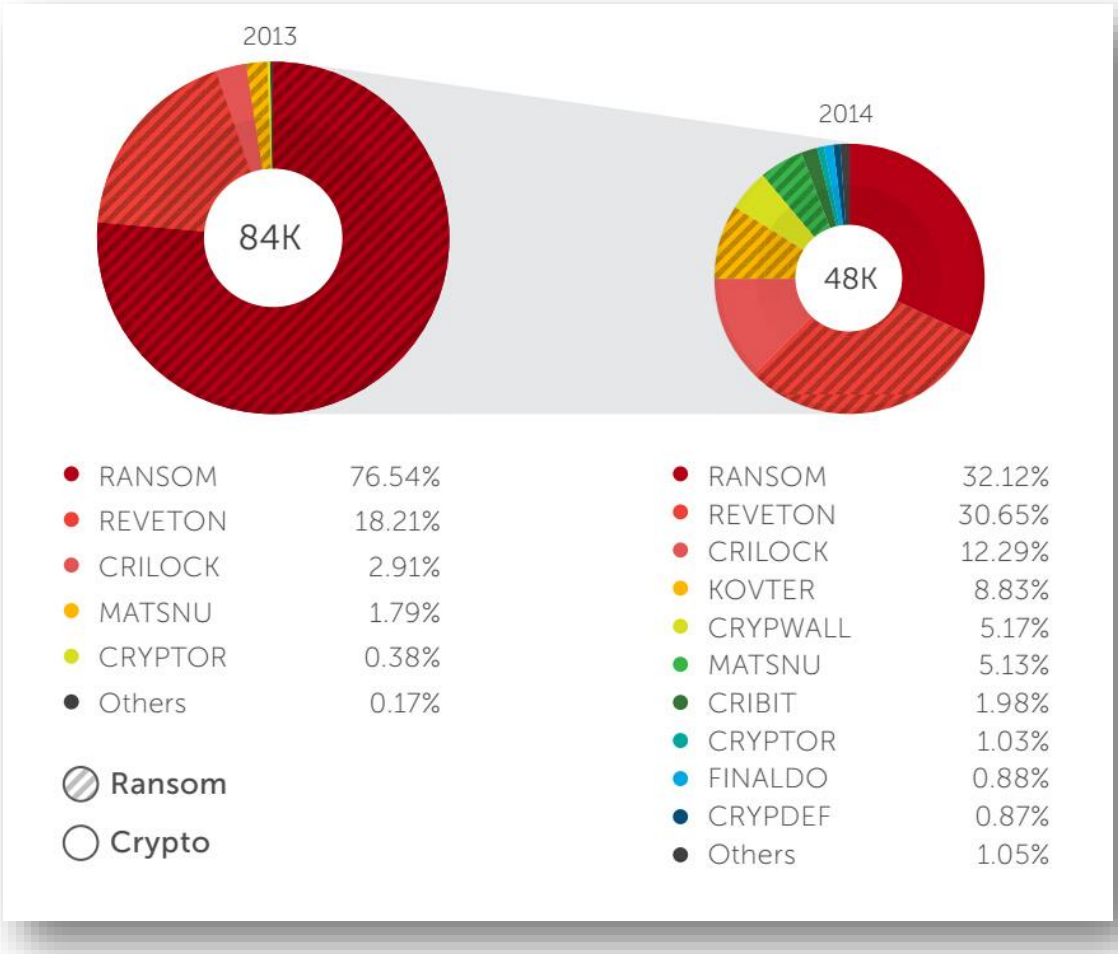
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

下图列出了2014 年中C&C 服务器分布地区情况。在2013 年的统计数据里，与僵尸网络有关的C&C 服务器分布最多的地区位于美国，英国和印度。值得注意的是，这一现象在2014 年并没有好转，原因可能是因为C&C 服务器可以远程操控。



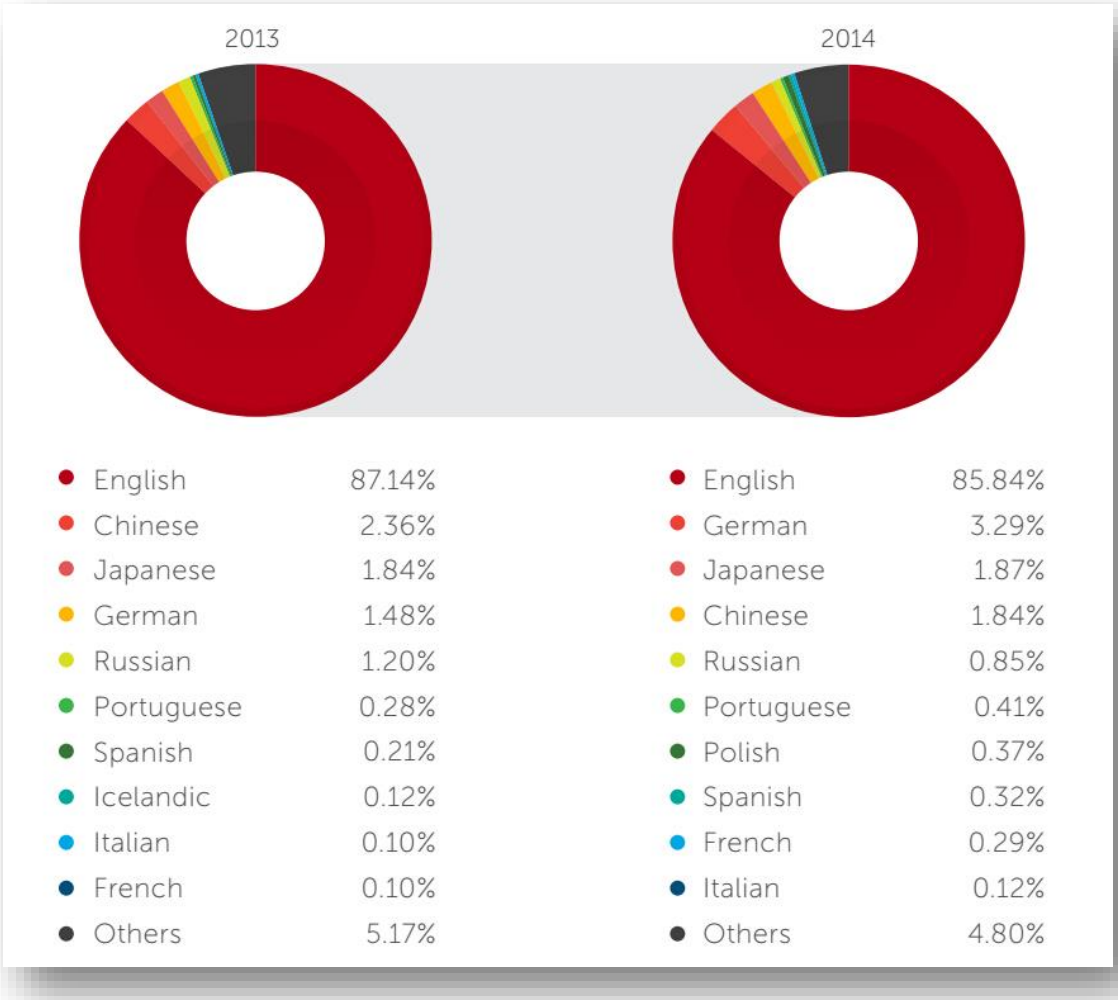
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

下图列出了2013 年和2014 年勒索软件家族数量对比。



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 2013 年与 2014 年在垃圾邮件中使用频率最高的 10 种语言。英语仍然是垃圾邮件发送者的首选语言，虽然所占比重从 2013 年的 87.14%有所下降到 85.84%。这意味着我们略微看到了更多的非英语垃圾邮件，其中使用德语书写的邮件最多，超越了前一年使用中文和日语垃圾邮件数量。



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。

需要查看更完整的 2014 年第 4 季度全球安全报告请访问：

http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/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室

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。