中国地区 2015 年
第二季度
网络安全威胁报告

2015/7

CHINA RTL

目录

2015 年第 2 季度安全威胁

本季安全警示：

宏病毒、勒索软件

2015 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 **22** 万条。截止 2014.6.30 日中国区传统病毒码 **11.760.60** 包含病毒特征数约 **423** 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 **57,682** 万次。
- 本季度趋势科技在中国地区拦截的恶意 URL 地址共计 **22,102,736** 次。

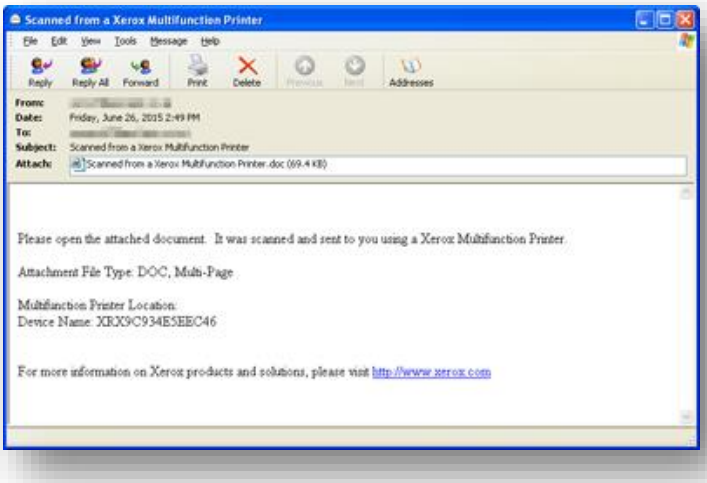
宏病毒虽然是一种古老的病毒类型，但它们依然是黑客手中的攻击“利器”。自 2014 年年末以来，趋势科技在监控数据中发现了一波宏病毒复苏潮。宏病毒数量增多的原因一是携带有恶意宏病毒附件的垃圾邮件数量急剧增加，二是出现了大量宏病毒新变种。普通用户往往安全意识淡薄，这使得黑客利用宏病毒攻击极容易得手，因此成为了他们喜爱使用的一种攻击手段。大部分用户并不了解什么是宏病毒，也不明白它们会有哪些危害。黑客恰恰利用了这一点从而诱骗用户去打开一些看上去非常正常的邮件附件。一旦用户点击这些恶意附件，病毒便开始悄悄运行了。宏病毒受到黑客青睐的另一个原因是它们可以规避传统病毒查杀模式。沙盒检测技术对宏病毒的检测也起不到很好的效果，因为运行宏病毒需要人工干涉；利用混淆技术也可以使宏病毒轻松躲避传统检测。不过，针对邮件的过滤扫描是一种有效的方式，因为它们可以过滤出附件中的可执行文件。

从统计数据看，中国地区是感染宏病毒的重灾区。2015 年以来，中国地区检测到宏病毒数量占到全球总数的 20%以上。虽然微软已将 Office 软件的宏安全性设置在默认关闭状态，但一些旧版本的 Office 软件用户依然面临风险。Word 文档和 Excel 表格是宏病毒两大载体，占到感染总数的 90%以上。

从下文中的示例图可以看到，如今的宏病毒攻击中社会工程学发挥了很大的作用。病毒文件会告知用户为了能完整查看附件内容需要启用宏，用户启用宏后并不会察觉到恶意文件已经在后台悄悄运行了。

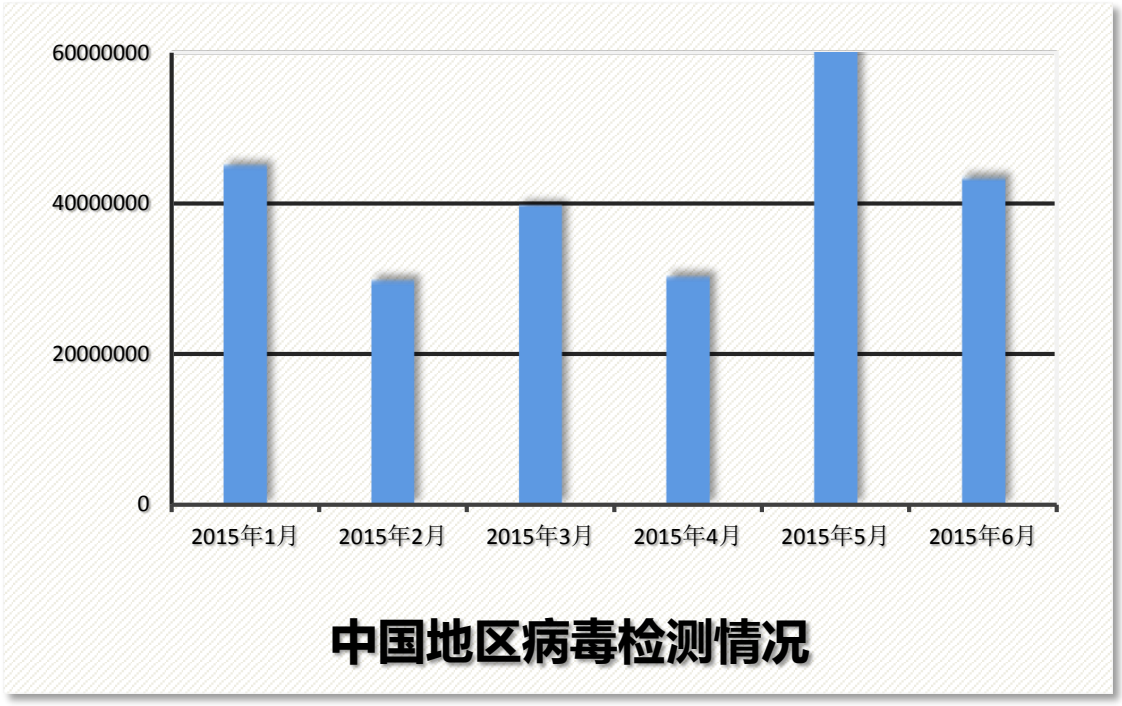
宏病毒如何运行示意图

下图是一封利用社会工程学传播宏病毒的垃圾邮件，该攻击手法十分典型，这个附件的趋势检测名为 W2KM_DLOADR.XTUJ。值得注意的是，DLOADR 家族在所有宏病毒家族中数量排名第一，这种下载器会自动下载其它恶意程序到受感染的计算机上。



携带宏病毒文件的垃圾邮件样本

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。

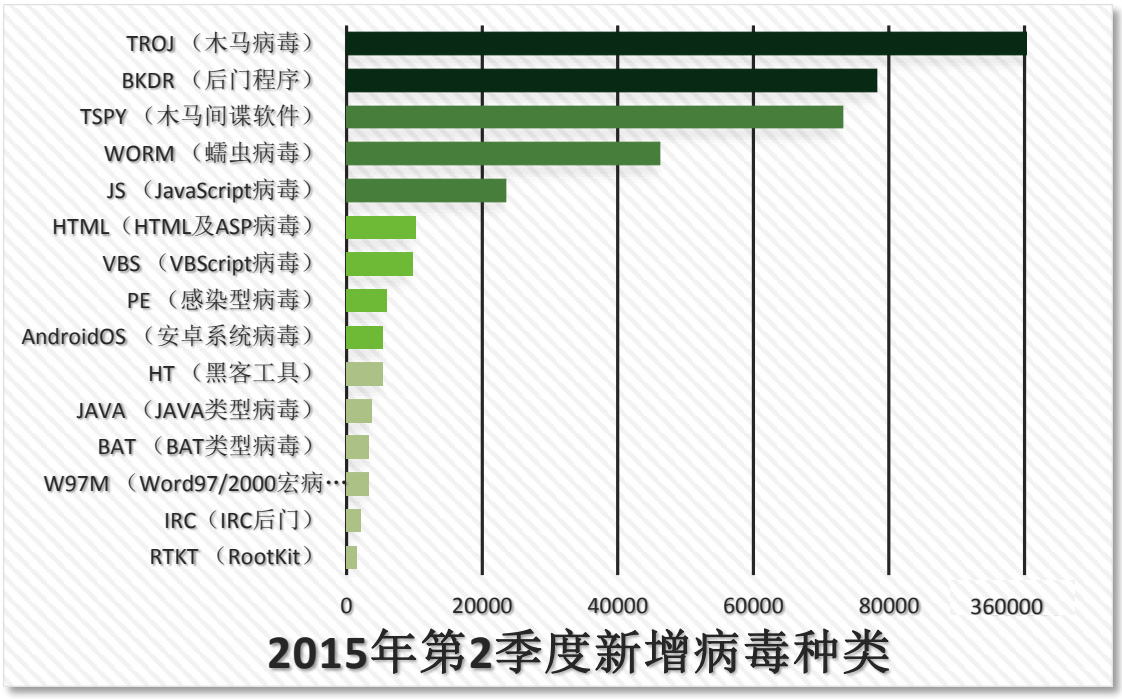


2015 年第 2 季度中国地区病毒检测数量图

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 2 季度病毒威胁情况

2015 年第 2 季度新增病毒类型分析



2015 年第 2 季度新增病毒类型分布图

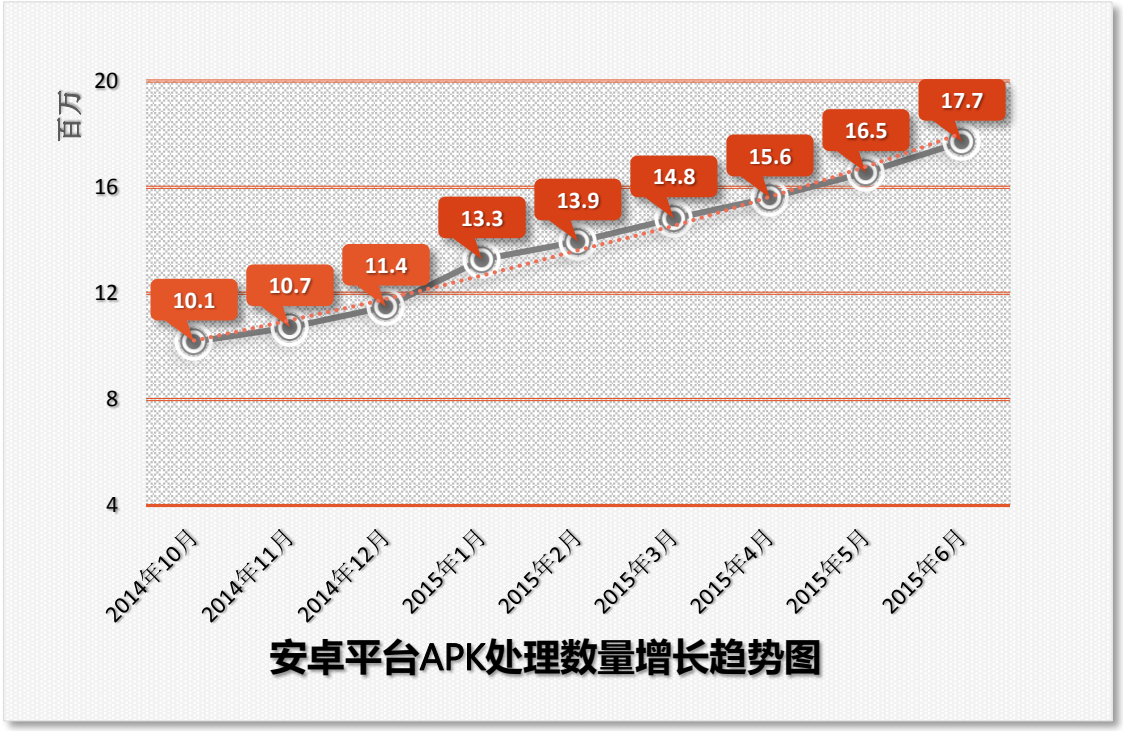
在 2015 年第 2 季度新增病毒种类中，依然以 **TROJ（木马病毒）**类型增幅最大。本季度新增木马病毒特征共计 **357,065** 个，与上一季度新增数量相比略有增加。在中国地区，捕获的木马类型的病毒数目一直大大超过其它类型病毒，木马病毒通常以窃取攻击目标的账户密码为目的，从而获得经济利益。

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。

JS (JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒与网页挂马有关，这类病毒具有一定威胁性。当网站被入侵者挂马后，浏览网页的访问者就会在毫不知情的情况下，自动下载恶意文件到本机。

检测名以 HT_打头的病毒类型“黑客工具”的检测类型连续上榜。网络黑市上大量工具公开售卖，获取途径越发简单，造成当前这类病毒检测数量居高不下。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。

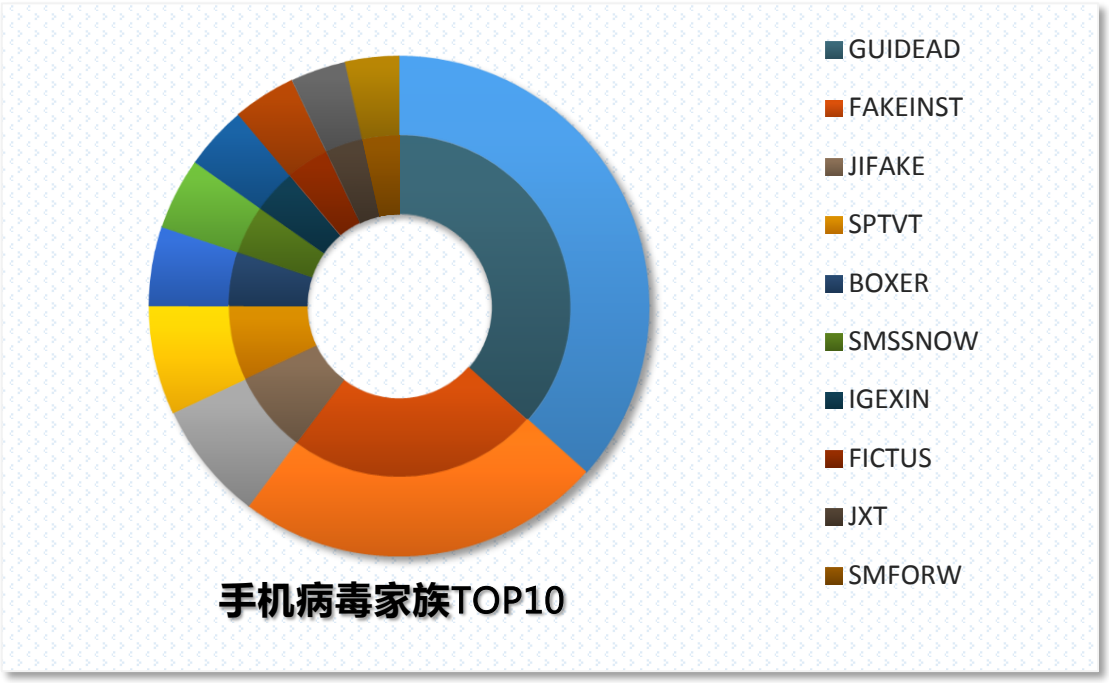


2015 年第 2 季度安卓平台 APK 处理数量走势图

截止到 2015 年 6 月 30 日，趋势科技发布中国区移动客户端病毒码版本是 1.907.00，大小 6,471,696 字节。

2015 年第 2 季度中，趋势科技对 APK 文件的处理数量依旧呈上升趋势。截止到本季度的 6 月底，处理数量累计达到 1,770 万个。从最近历史处理数据走势图看，安卓病毒单月增长率一直保持上升趋势。

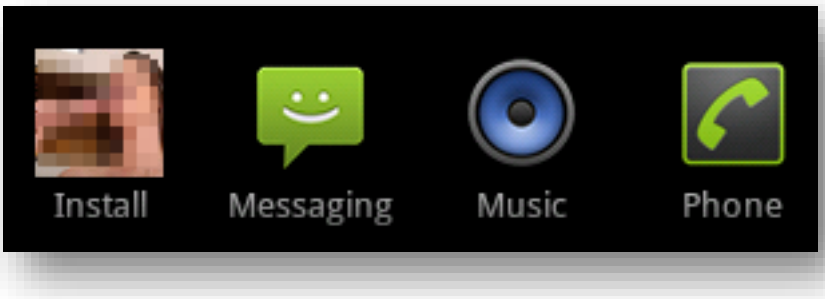
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。



2015 年第 2 季度手机病毒家族 TOP10 分布图

在 2015 年第 2 季度感染安卓平台的手机病毒家族中，GUIDEAD 家族数量最多，占到总数的 36.56%；FAKEINST 家族位列第二，占 23.72%；JIFAKE 家族居第三位，占总数的 7.73%。排列前三的家族占总数的一半以上。

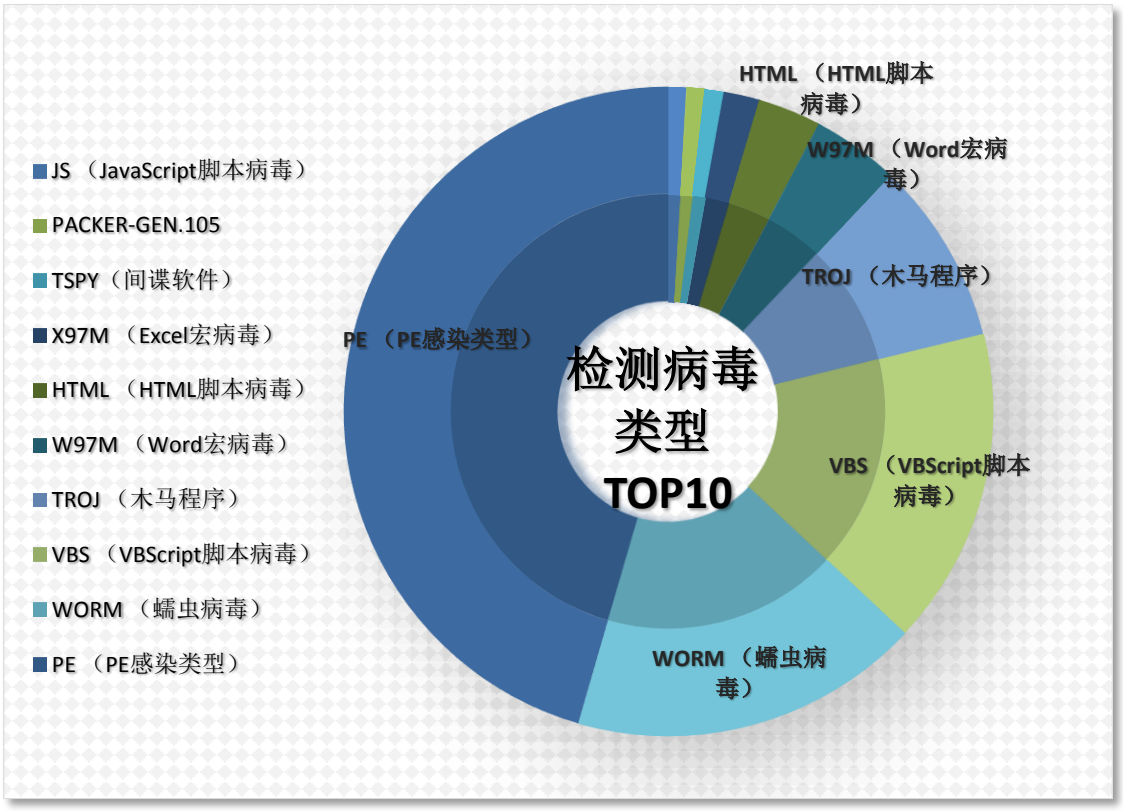
在 2015 年第 2 季度中，趋势科技发现了使用隐写技术的移动设备恶意软件。能够使用各种方法逃避检测的恶意软件一直以来被认为是最危险的安全威胁。在当今最受关注的目标攻击和零日漏洞利用中都经常使用各种方法来逃避检测。能否成功保持隐藏有时候决定了攻击是否能成功，所以隐藏往往成为攻击者追求的首要目标。此次发现的使用隐写技术的手机病毒在程序图标中隐藏了配置文件。我们发现不止一种安卓病毒（如 ANDROIDOS_SMSREG.A）将配置文件隐藏在程序图标中。



携带病毒配置文件的安卓图标。 由于图片包含色情内容，我们进行了模糊处理。

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 2 季度各类型病毒检测情况分析



2015 年第 2 季度病毒检测类型分布图

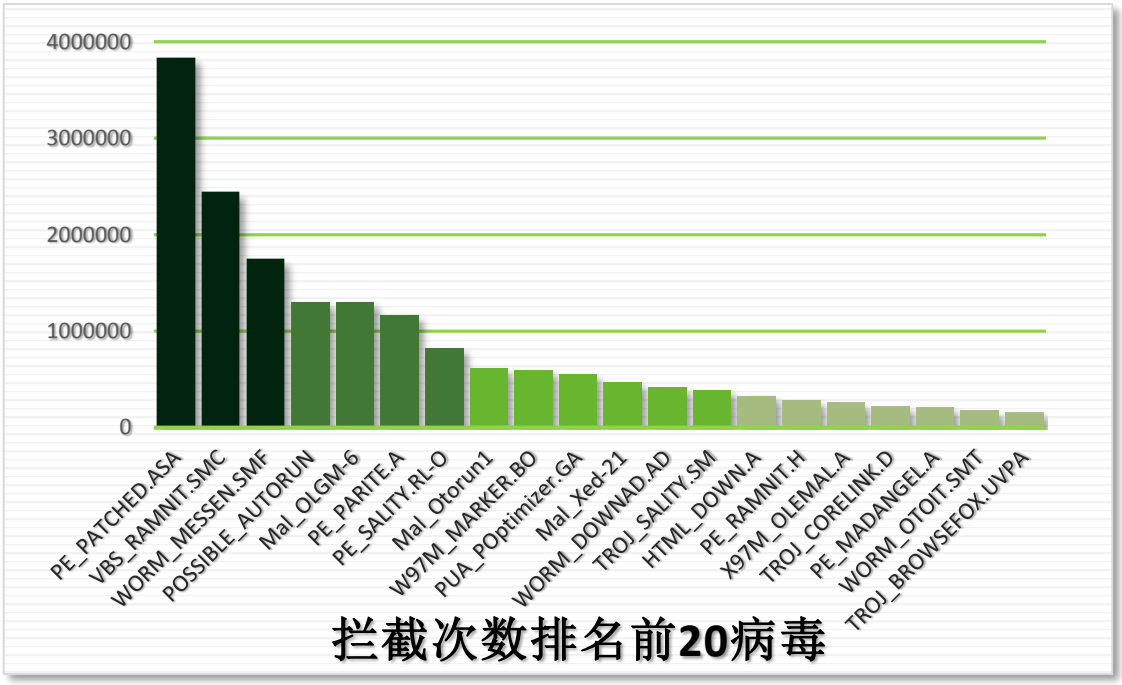
2015 年第 2 季度检测到的病毒种类中，PE 类型病毒感染数量在所有类型中所占比重最大，占到总检测数量的 45.52%。在本季度中，PE_PATCHED.ASA 检测数量依然排名第一，此外 PE_SALITY、PE_PARITE、PE_SAMNIT 家族检测数量排名靠前。PE_PATCHED.ASA 病毒文件是一个被修改过的系统文件 sfc_os.dll，这个文件用以保护系统文件的执行模块，该文件一旦被修改，系统将失去文件保护的功能。

本季度蠕虫病毒占检测类型总数的 17.48%，本季度该类型病毒占比较上一季度有所下降。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 家族本季度继续保持上升趋势。

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 2 季度病毒拦截情况分析



2015 年第 2 季度病毒拦截情况图

在 2015 年第 2 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 382 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 **VBS_RAMNIT.SMC** 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：
VBScript 脚本病毒

文件类型：
.VBS

安装：
当用户访问某些被病毒挂马的网站时会自动执行。
该病毒也可通过以下途径抵达目标及其：
它可能被 PE_RAMNIT.H-O 修改

恶意行为：
它会释放以下文件：

%User Temp%\svchost.exe – 该恶意文件的趋势检测名为 PE_RAMNIT.H-O

(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)。)

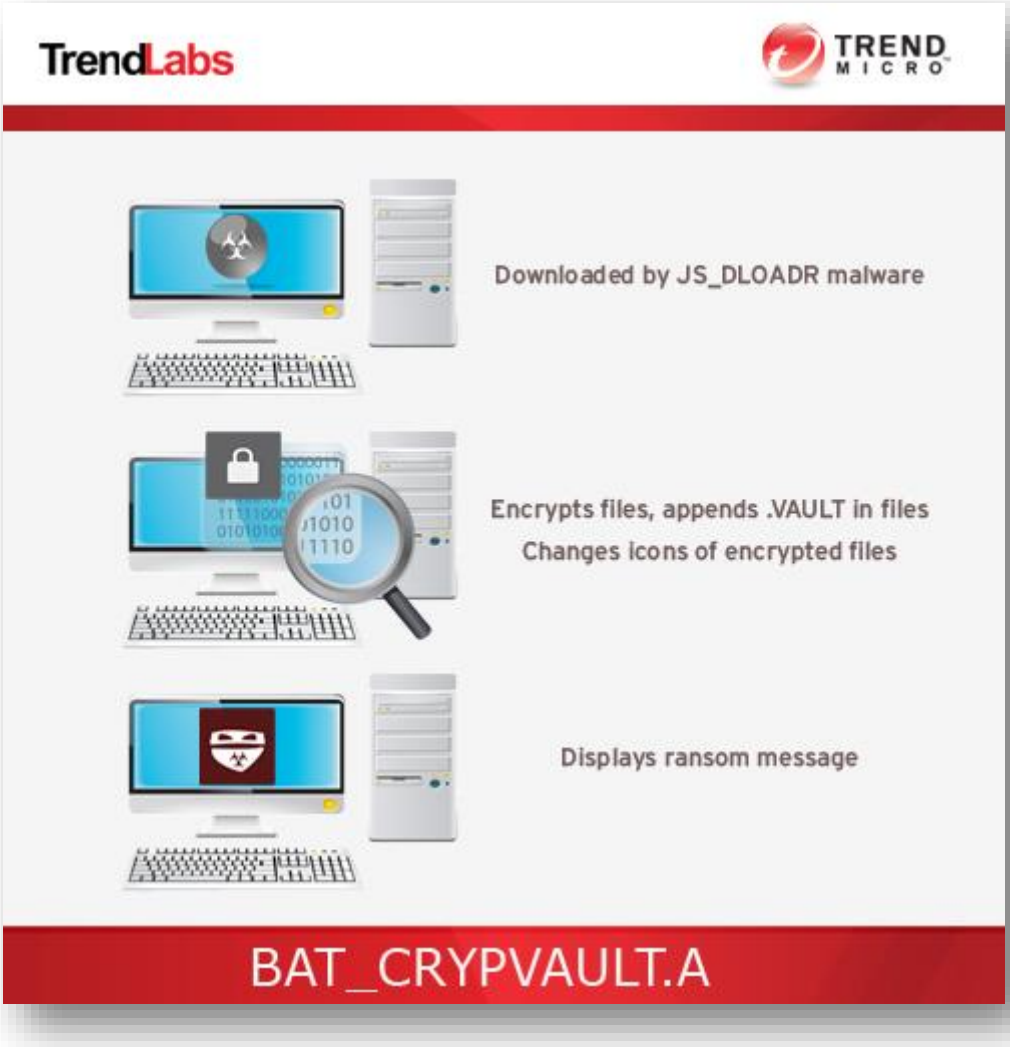
清除方法：

- ✓ 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 VBS_RAMNIT.SMC 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/VBS_RAMNIT.SMC

2015 年第 2 季度热门新型病毒分析

本季度热门病毒 BAT_CRYPVAULT.A 是由其它恶意软件（JS_DLOADR）下载到计算机上并进行加密、勒索行为的勒索软件。当它执行完成恶意行为后就会将自身删除。



BAT_CRYPVAULT.A 恶意行为示意图

病毒的详细信息如下：

病毒检测名：
BAT_CRYPVAULT.A

恶意行为：

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。

连接 URL/ IP 地址，窃取信息，加密文件，显示勒索消息/消息框，显示勒索图形/图像。

抵达细节：
该木马由其它恶意软件下载到计算机上。

下载：
该木马释放以下文件：
%User Temp%\VAULT.txt
%User Temp%\VAULT.hta
%appdata%\VAULT.hta
%User Temp%\a.qq
%User Temp%\gk.vlt
%User Temp%\pk.vlt
%User Temp%\vaultkey.vlt
%User Temp%\cryptlist.lst
%User Temp%\conf.list
%User Temp%\confclean.list
%User Temp%\cryptlist.cmd
%User Temp%\up.vbs
%User Temp%\ultra.js

（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。）

在注册表中植入以下简直实现自启动：
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
TNotification = "notepad %User Temp%\VAULT.txt"

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
VAULT Notification = "mshta %appdata%\VAULT.hta"

感染文件：
该病毒不会感染名字中包含以下字符串的文件：
windows
temp
recycle
program

appdata
avatar
roaming
msoffice
temporary
sample
themes
uploads
csize
resource
internet
com_
intel
common
resources
texture
profiles
library
clipart
manual
games
framework64
setupcache
autograph
maps
amd64
cache
support
guide
abbyy
application
thumbnails
avatars
template
adobe

下载行为：

该病毒连接以下 URL 下载自身组件：

http://{BLOCKED}lpknfp.onion.city

并将下载文件保存在以下路径：

%User Temp%\enigma.exe

其它细节：

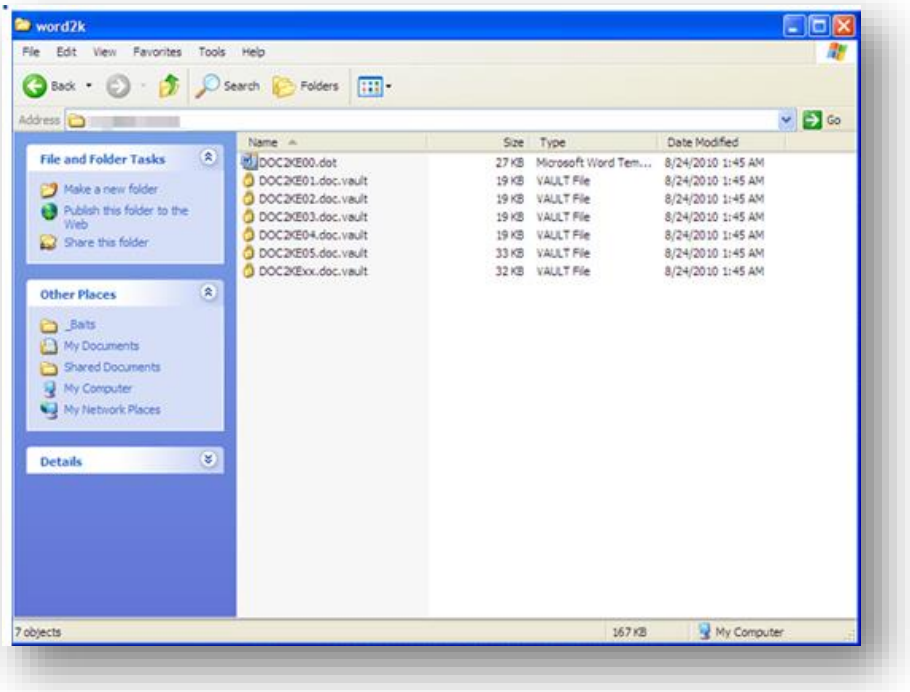
该木马会加密以下扩展名的文件：

*.xls
*.doc
*.pdf
*.rtf
*.psd
*.dwg
*.cdr
*.cd
*.mbd
*.1cd
*.dbf
*.sqlite
*.jpg
*.zip
*.7z

并将加密文档重命名成以下形式：

{文件名及扩展名 }.vault

被加密后的文件如下图所示：



加密文件图标被替换，并加上 VAULT 后缀名

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。

运行后病毒会将自身删除。

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

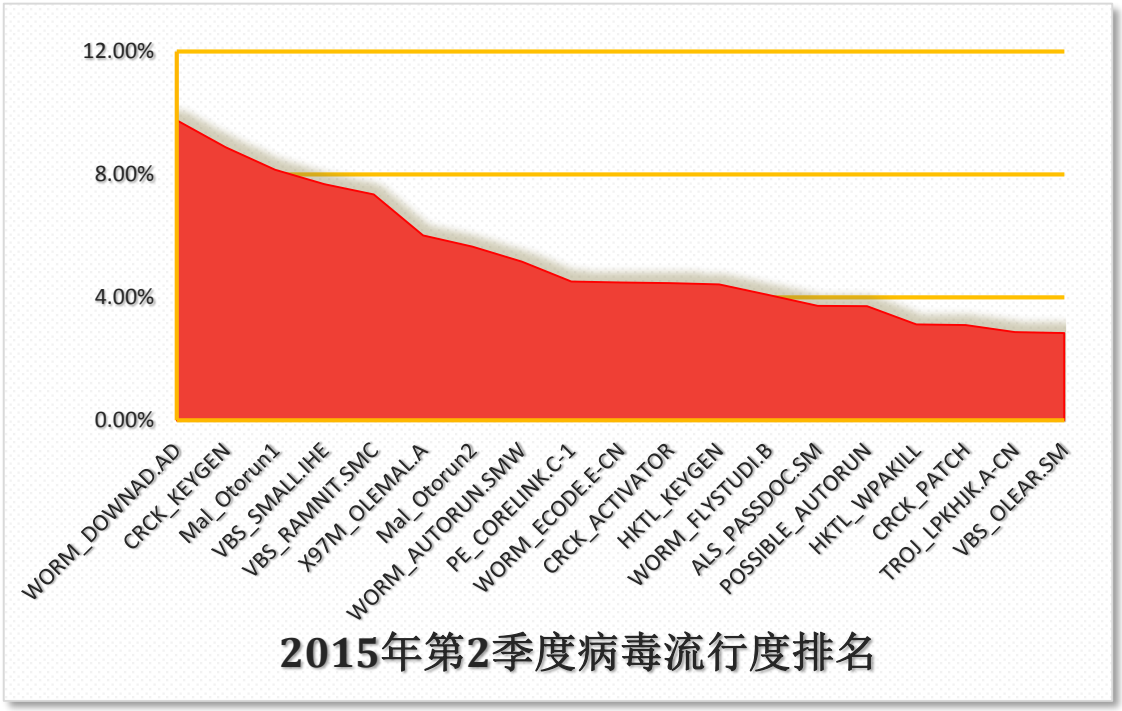
64 位 Windows 操作系统请使用：

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

相关链接信息：

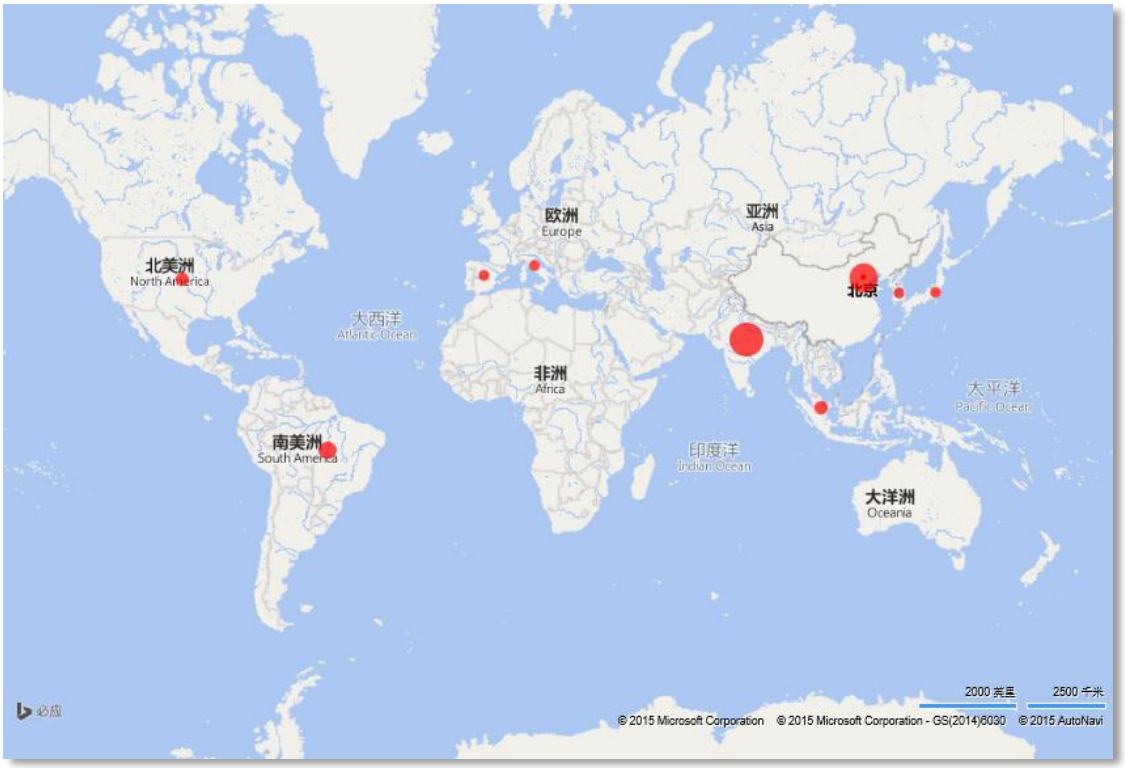
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BAT_CRYPVAULT.A

2015 年第 2 季度流行病毒分析



2015 年第 2 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 2 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 2 季度，约有 9.77% 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。

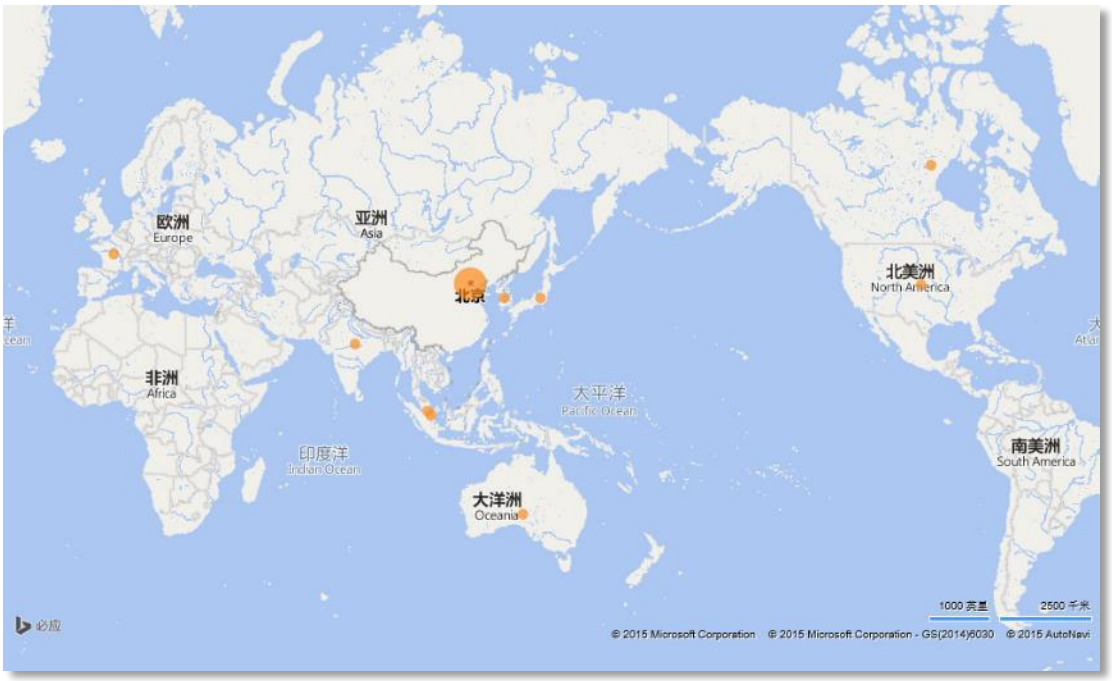
在这里仍然需要提醒用户，WORM_DOWNAD 持续流行的原因有几点：

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 2 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 2 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

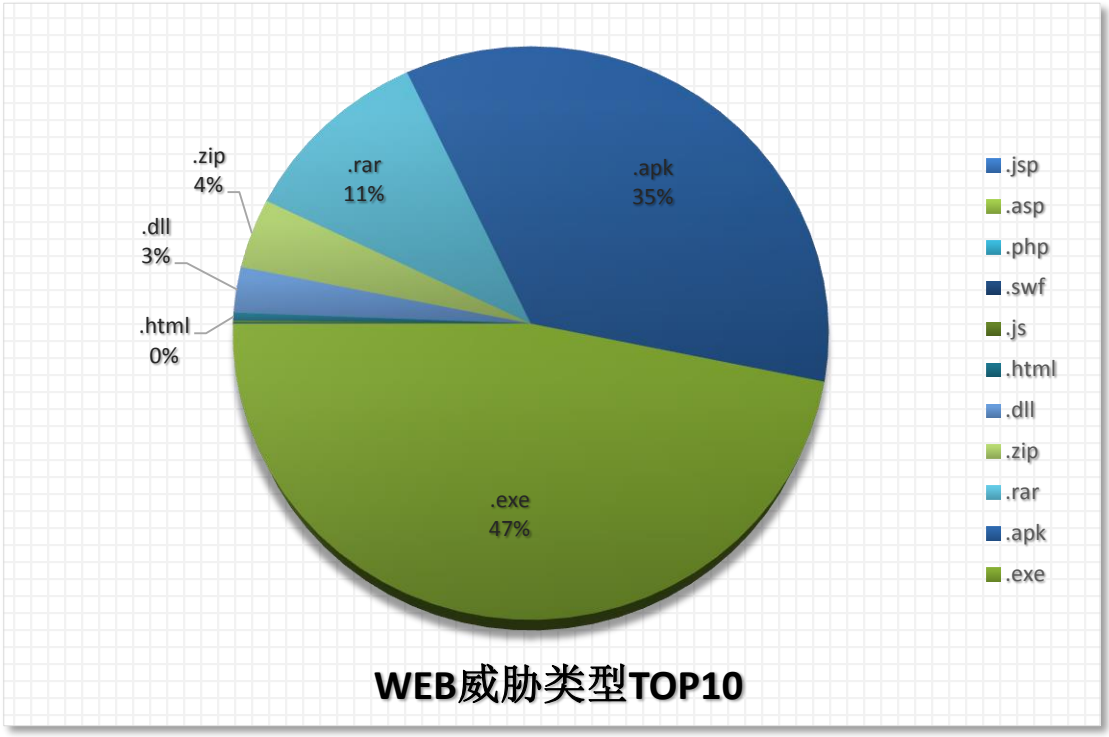
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2015 年第 2 季度 WEB 安全威胁情况

2015 年第 2 季度 WEB 威胁文件类型分析

在 2015 年第 2 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 47%，所占比例比上一季度 41%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。

通过本季度的统计数据可知，.APK 和压缩文件格式.RAR 及.ZIP 所占比例较多。.APK 文件，所占比例达到 35%，在本季度中位列第二位，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 2 季度中国地区 WEB 威胁文件类型分布图

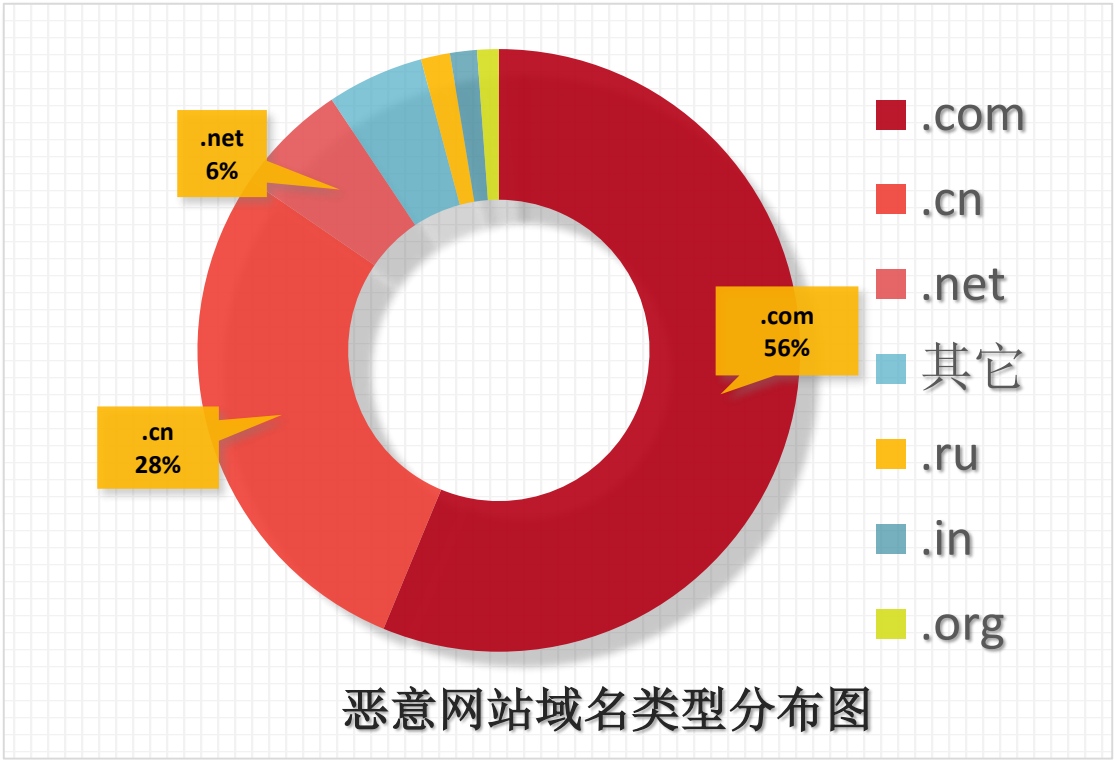
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2015 年第 2 季度 TOP 10 恶意 URL

TOP10 恶意URL		
恶意URL	描述	点击量
http://download.23***n/234***afe	网站直接或间接帮助传播恶意软件或恶意代码	3,617,097
http://trafficcon***ter.biz/	此链接为恶意程序的命令与控制(C&C)服务器。	2,225,722
http://imdd***03.com:6688/511135395.html	此链接为恶意程序的命令与控制(C&C)服务器。	1,876,852
http://traffic***r.biz/4vir	网站直接或间接帮助传播恶意软件或恶意代码	1,514,162
http://220.1***1.104/msvquery	网站直接或间接帮助传播恶意软件或恶意代码	1,303,938
http://downlo***n/234***e/	网站直接或间接帮助传播恶意软件或恶意代码	1,067,200
http://106.12***7/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	1,028,365
http://106.1***7/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	1,027,696
http://106.1***5/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	1,026,993
http://106.12***.9/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	1,026,242

2015 年第 2 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 2 季度恶意网站域名类型分布图

2015 年第 2 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、.NET 的域名的站点占总数 90.64%。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 2 季度 WEB 威胁钓鱼网站仿冒对象分析

2015 年第 2 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 12 月至 2015 年 5 月共计 6 个月中，处理钓鱼网站共计 **17,130** 个。

从数量上看，今年以来发现钓鱼网站数量整体呈下降的趋势。2 月份以后，每月发现的钓鱼网站数均在 3000 个以下，与去年同时期数据相比下降明显。

在所有钓鱼网站中，“支付交易类”和“金融证券类”钓鱼网站所占比例最多，占总数的 95%以上。其中更以电子商务网站和银行为仿冒对象的钓鱼网站占到绝大部分。

钓鱼网站域名在第 2 季度中主要分布于.COM、.CN 和.CC 域名，通常占总数的 75%以上。其中又以.COM 域名的数量最多，所占比例均在总数的一半以上。此外，一些非大众化域名下的钓鱼网站数量均有所增加。

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。

2015 年第 2 季度漏洞攻击威胁情况

TOP10 漏洞	
漏洞名称	**检测数量**
CVE-2008-4250	92459
CVE-2010-0806	75
CVE-2010-2568	30
MS08-067	14
CVE-2014-4113	4
CVE-2014-4148	4
CVE-2010-3333	1
CVE-2012-0158	1
CVE-2012-0507	1
CVE-2013-0422	1

2015 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= CVE-2008-4250
CVE-2010-0806	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806
CVE-2010-2568	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568
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-2010-3333	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3333
CVE-2012-0158	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-0158
CVE-2012-0507	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-0507
CVE-2013-0422	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-0422

漏洞介绍链接

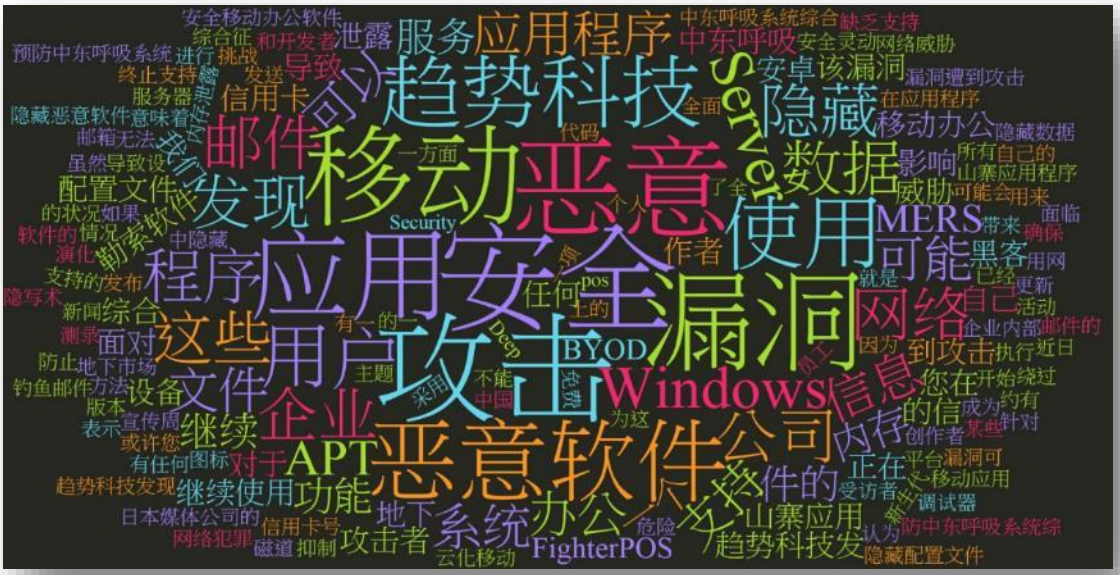
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

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 2 季度最新安全威胁信息

2015 年第 2 季度安全威胁信息摘要



2015 年第 2 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。

❖ 网络威胁不断演化 抑制 APT 攻击防范数据“吸血鬼”

近日，趋势科技在第二届“国家网络安全宣传周”活动中，正确引导青少年安全用网、健康用网的同时，结合宣传周的主题日，对金融、电信、政务等行业面对的网络威胁演化进行了全面展示。针对用户当前无法有效发现与阻拦 APT（高级持续性威胁）攻击的状况，趋势科技提出“知己知彼，百战不殆”的观点，详细揭秘 APT 攻击过程，并建议企业和政府用户采用定制化的解决方案建立 APT 攻击“抑制点”，确保数据安全。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20150608091837.html

❖ “云化移动、安全灵动” 趋势科技发布安全移动办公软件打消 BYOD 顾虑

随着 BYOD 的普及，越来越多的全球范围内的企业级用户都开始着重发展基于云计算的移动应用战略，“云办公”和“移动办公”正在取代传统的 PC 应用。没错，BYOD（自带设备帮办公）已经开始改变企业内部的生产方式和流程，但不可否认的是，安全风险正在成为令人心烦的“绊脚石”。为了帮助企业用户将移动设备全面融入现代商业活动，确保员工安全、便捷、高效、合规且跨平台地访问企业数据和应用程序，趋势科技近日在以“云化移动、安全灵动”为主题的发布会上，正式推出了全新的安全移动办公软件 （Safe Mobile Workforce ,SMW）。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20150612092212.html

❖ 面对即将终止支持的服务器你还能做些什么？

截止到 7 月 14 日终止支持日期，Windows Server 2003 只剩下两次定期性更新，以后将不再有任何安全更新，这就意味着，若您在 7 月 15 日起依然使用 Windows Server 2003 的话，当此服务器发现任何新漏洞，您将立即面临危险！

根据最近的一项调查显示，82%的受访者其企业内部仍有一些 Windows Server 2003 存在，而这些受访者当中的 25%表示，将在缺乏支持和维护的情况下继续使用 Windows Server 2003。

使用缺乏支持的操作系统，在营运上被视为一项漏洞，因为这基本上是个危险又不智的举动。或许您是因为无法在短期之内完成移转，而不得不继续使用 Windows Server 2003；也或许您在业务上的需求而被迫在 7 月 14 日之后仍需要继续使用 Windows Server 2003。

出于以上情况，您可以考虑采用趋势科技 Deep Security 这类产品来防止未修补的漏洞遭到攻击，尽管 Deep Security 不能帮您修正漏洞，但却能防止漏洞遭到攻击，这样就能保障您在转移新平台之前的系统安全了。

http://blog.sina.com.cn/s/blog_5e96245b0102vmab.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。

❖ 隐写术：看黑客如何秘密隐藏恶意软件

在当今最受关注的 APT 攻击和零时差漏洞利用中经常使用某些方法来逃避检测，而黑客用来在隐秘通道内隐藏数据的一切可能方法，就是我们所认为的“隐写术”。ZeusVM 在 JPG 图片里隐藏恶意软件的配置文件；VAWTRAK 用收藏夹图标来隐藏配置文件；FakeReg 在应用程序图标中隐藏配置文件；VBKlip 在 HTTP 协议中隐藏数据。

http://blog.sina.com.cn/s/blog_5e96245b0102vmlh.html

❖ POS 恶意软件，可回传信用卡号及个人资料

FighterPOS 的功能和其他 PoS 恶意软件家族相似，可以收集信用卡磁道 1，磁道 2 和 CVV 码，还包含内存撷取功能，此外，攻击者可以通过键盘测录功能测录到受感染终端上的按键记录。

趋势科技发现巴西有 100 多家受害组织受到 FighterPOS 的影响，已经窃取超过 22,000 笔不重复的信用卡号码，其创作者似乎在支付诈骗和恶意软件制造上有很长的历史，我们认为这个恶意软件创作者是独立行动，没有任何同伙协助。FighterPOS 目前售价是 18 比特币（约为 5,250 美元）虽然不便宜但精心设计的控制面板和多种功能的支持，足以诱惑到攻击者。

http://blog.sina.com.cn/s/blog_5e96245b0102vk1j.html

❖ 90 后走入地下市场成为勒索软件的幕后人

一群新生代网络犯罪集团正在中国崛起，就是这些胆大包天的 90 后相互搜寻并分享程序代码，然后制作出属于自己的恶意软件，使得中国地下市场一下子充斥着各种移动勒索软件。

我们在监控 Android 勒索软件 ANDROIDOS_JIANMO.HAT 的时候发现这群网络犯罪新生代,此恶意软件大约有一千多个变种，其中约有 250 个含有恶意软件作者的相关数据及联络信息，这些人的年龄从 16 至 21 岁不等。

http://blog.sina.com.cn/s/blog_5e96245b0102vmns.html

❖ 趋势科技发现一个安卓漏洞可导致设备内存泄露

趋势科技早安卓调试器 Debuggerd 中发现了一个漏洞，该漏洞可能会导致设别内存泄露。该漏洞会影响从安卓的 Ice Cream Sandwich 到 Lollipop 之间的所有版本。一个特殊构造的 ELF 格式文件可以令调试器奔溃并泄露内存信息。这些信息可以用于辅助进行拒绝服务攻击，并绕过 ASLR 执行硬编码。对于该漏洞自身而言是不能执行代码的。

http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-android-vulnerability-that-can-lead-to-exposure-of-device-memory-content/

❖ MERS 新闻被用来面对某些日本媒体公司的针对性攻击中

有黑客使用与中东呼吸综合征（MERS）爆发有关的新闻作为钓鱼邮件的内容发送给知名日本媒体公司的员工邮箱中。这些钓鱼邮件使用雅虎免费邮箱发送邮件，轻松绕过了反垃圾邮件过滤系统，攻击者引用了网络上公开的信息，诱骗用户点击打开邮件。在这些邮件的标题中，用日语写着“转发：预防中东呼吸系统综合症（MERS）”，附件文件则名为 “预防中东呼吸系统综合征（MERS）.7z”。

http://blog.trendmicro.com/trendlabs-security-intelligence/mers-news-used-in-targeted-attack-against-japanese-media-company/

❖ 移动证书和开发者账户：谁在伪造它？

公司如果继续忽视自己在应用程序商店里的状况就可能失去所有的客户。一方面恶意移动应用对移动安全带来严峻挑战，（70％进入排行榜的免费应用都会有假冒或者恶意版本），另一方面公司和开发者也面临山寨应用这一挑战。

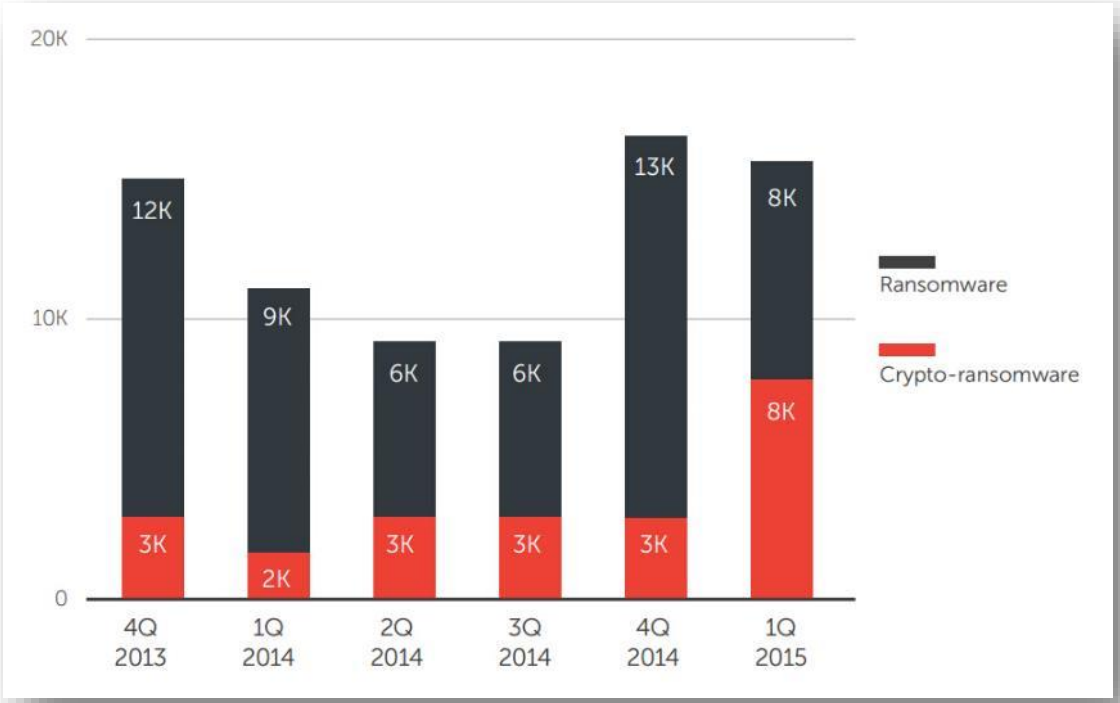
对于一个公司，山寨应用程序可能意味着会给自己的信誉和收入带来损失。对于用户来说，负面影响也是相同的，虽然它们来自个人层面：如果用户错误地下载了山寨应用程序，可能会最终导致信息被盗、名誉受损，进而对公司品牌和服务表示不满。

http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-certificates-and-developer-accounts-who-is-faking-it/

趋势科技全球区最新安全威胁概要

以下是来自 2015 年第 1 季度趋势科技全球区安全报告的数据。

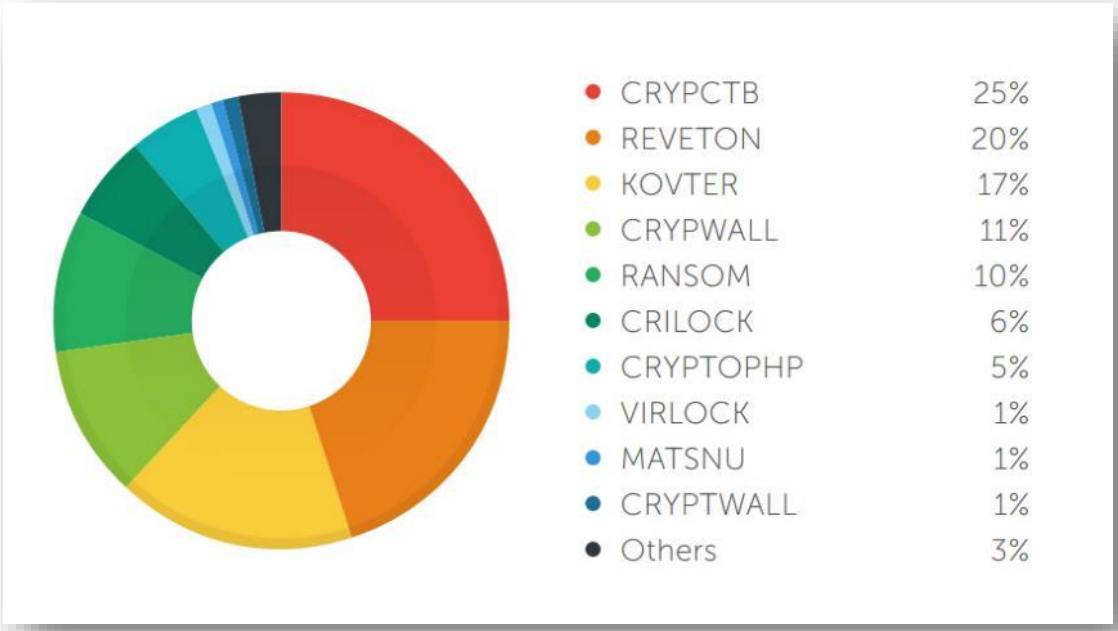
2013 年末，因为黑洞漏洞利用工具的作者 Paunch 被逮捕，从 2014 年年初开始的前 3 季度勒索软件数量大幅下降。（黑洞漏洞利用工具包因散播勒索软件出名。）



勒索软件感染数量图

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。

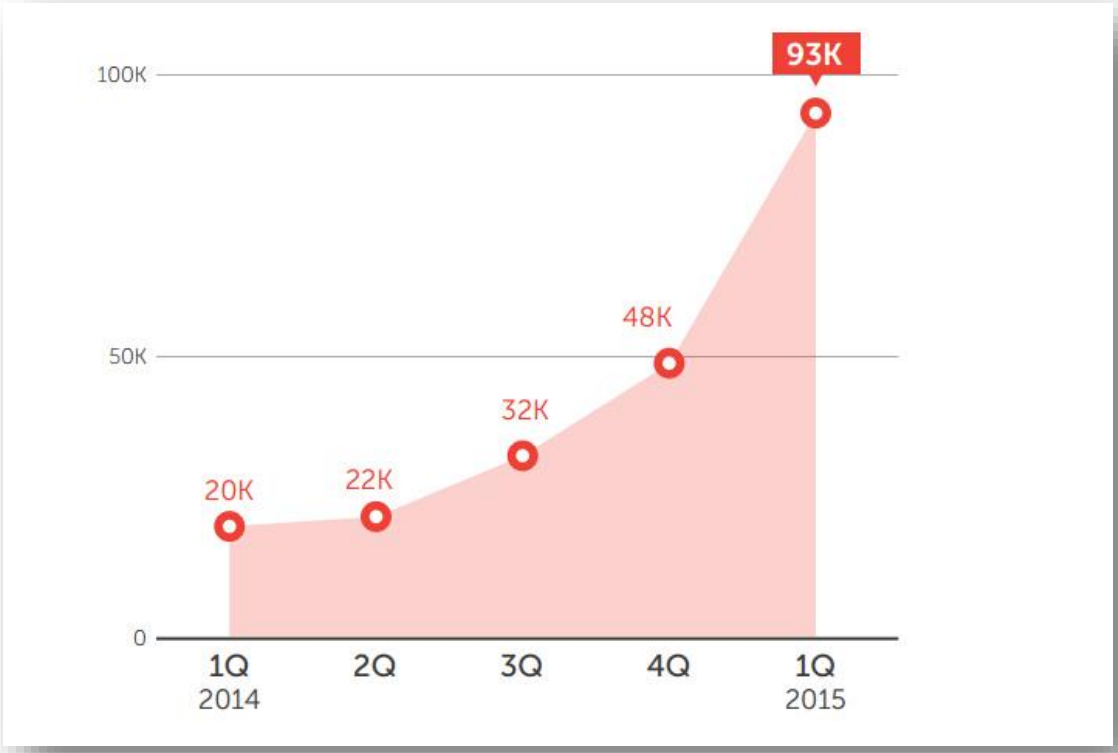
CRYPCTB 勒索软件家族在饼图中占据了25%数量，该趋势检测名对应的是CTB-Locker 勒索软件病毒变种,该家族在今年的前2 个月中泛滥成灾。



勒索软件家族数量排行表

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。

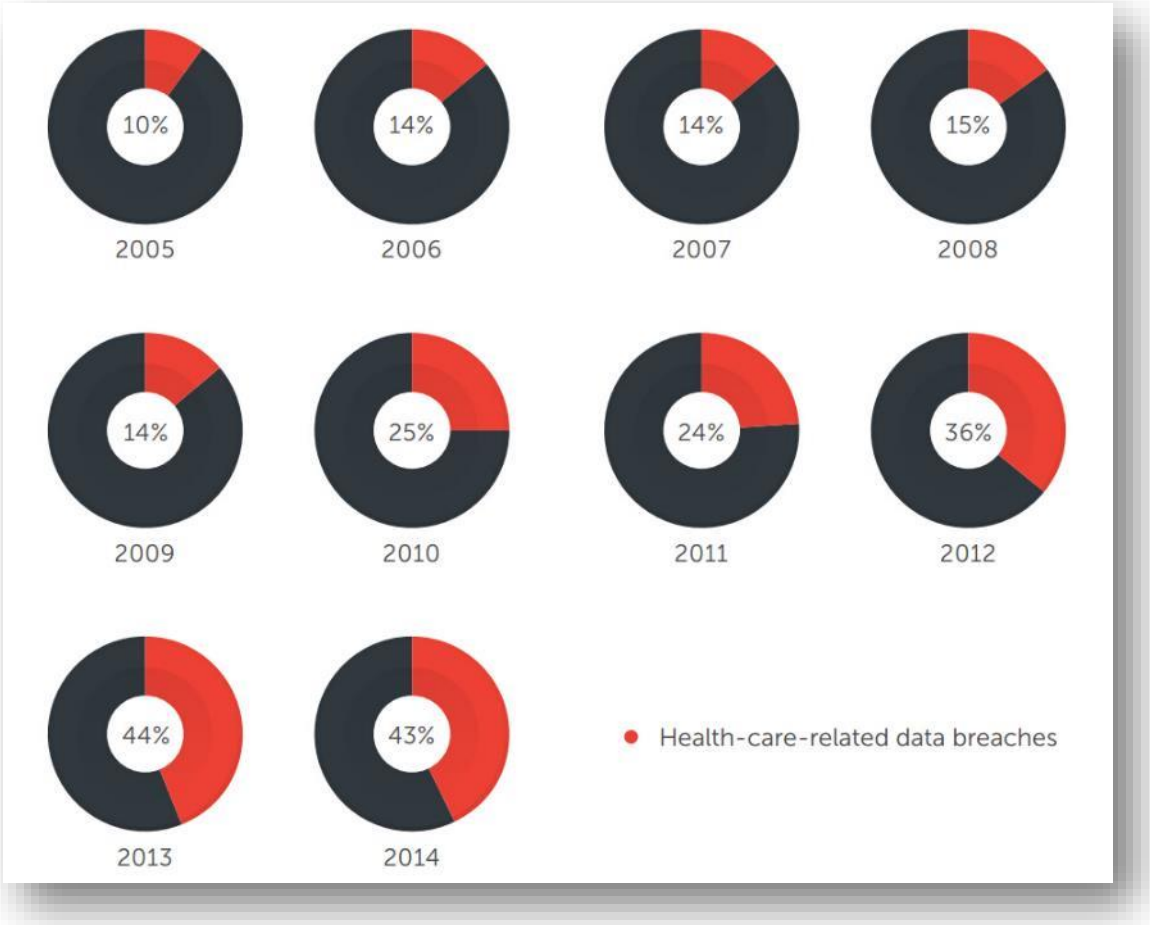
从 2014 年第 1 季度起宏病毒感染数量不断增加。这一现象可能和新变种的出现以及携带恶意宏附件的垃圾邮件数量的大幅增加有关。



2015 年第 1 季度宏病毒感染数量图

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。

医疗服务行业受信息泄露危害的人数从 2005 年到 2014 年增长了近 4 倍。2012 年到 2014 年期间，医疗服务行业的受害者超过了商务、军事和政府行业。下图显示了从 2005 年到 2014 年信息泄露事件和医疗服务行业相关的事件数量。

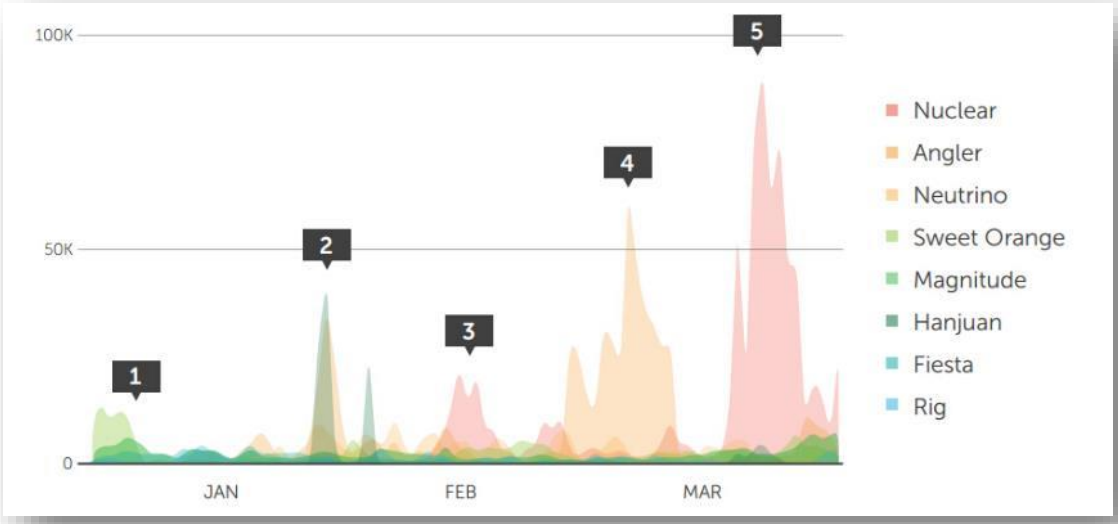


2005 年到 2014 年期间医疗服务行业信息泄露时间所占比例逐渐扩大

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。

（注：下图中峰值处的序号对应以下信息。）

AOL 将恶意广告从其平台上清理的行动，使 SweetOrange 漏洞利用工具的活动量大幅减少（1）。Angler 漏洞利用工具（2 和 4）和 Hanjuan 漏洞利用工具（2）被用来散播病毒 BEDEP（一个利用零日漏洞的病毒），这一系列活动发生在一月下旬至二月上旬期间，这促使与它们的服务器被访问次数增加。Nuclear 漏洞利用工具（3 和 5）通过色情网站散播恶意广告。



2015 年第 1 季度知名漏洞利用工具活动情况示意图

需要查看更完整的 2015 年第 1 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。