中国地区 2014 年
第二季度
网络安全威胁报告

2014/8

CHINA RTL

云安全3.0 全面防护云平台 请登录趋势科技官方网站www.trendmicro.com.cn或致电800-820-8876

目录

2014 年第 2 季度安全威胁

本季安全警示：
UPATRE 家族病毒，漏洞，木马

2014 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 **57** 万条。截止 2014.6.30 日中国区传统病毒码 **10.886.60** 包含病毒特征数约 **436** 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 **6,719** 万次。

- 本季度趋势科技在中国地区拦截的恶意 URL 地址 **17,178,314** 次。

在 2014 年第 2 季度中，趋势科技病毒实验室监控到多起 **UPATRE** 病毒感染事件，并发现该病毒家族频繁出现变种的现象。早在 2013 年，UPATRE 病毒已成为垃圾邮件附件出现频率最高的病毒文件。该病毒因下载其它恶意软件，包括宙斯病毒（ZeuS）和勒索软件（特别是 CryptoLocker）的行为而臭名昭著。这也可以说明，过去的这段时间勒索软件的大量出现和爆发与 UPATRE 病毒家族关系密切。

随着时间的推移，这个病毒的传播方式也在不断变化：UPATRE 病毒变种除了“以邮件附件进行传播”这一特点外，制作者在垃圾邮件的形式上也做了调整，使得它们变得更具欺骗性。

根据我们对这些垃圾邮件的观察分类，垃圾邮件主要会使用以下 3 种欺骗形式：

1.伪装成网络传真通知邮件，并且在邮件正文里加入一个链接，这些链接会将用户重定向至恶意站点下载 UPATRE 病毒文件。

2. 伪装成某些国外银行发送的通知邮件，这些邮件附有所谓的银行金融活动账单，而账单文件本身就是病毒文件。

3. 利用纳税作为主题的垃圾邮件。

这三种伪装方式其实都是网络罪犯最常用的手段：利用一些引人注意的关键信息千方百计地诱骗访问者点击运行病毒文件，一旦病毒被运行，就会导致计算机受到恶意攻击和信息泄露。

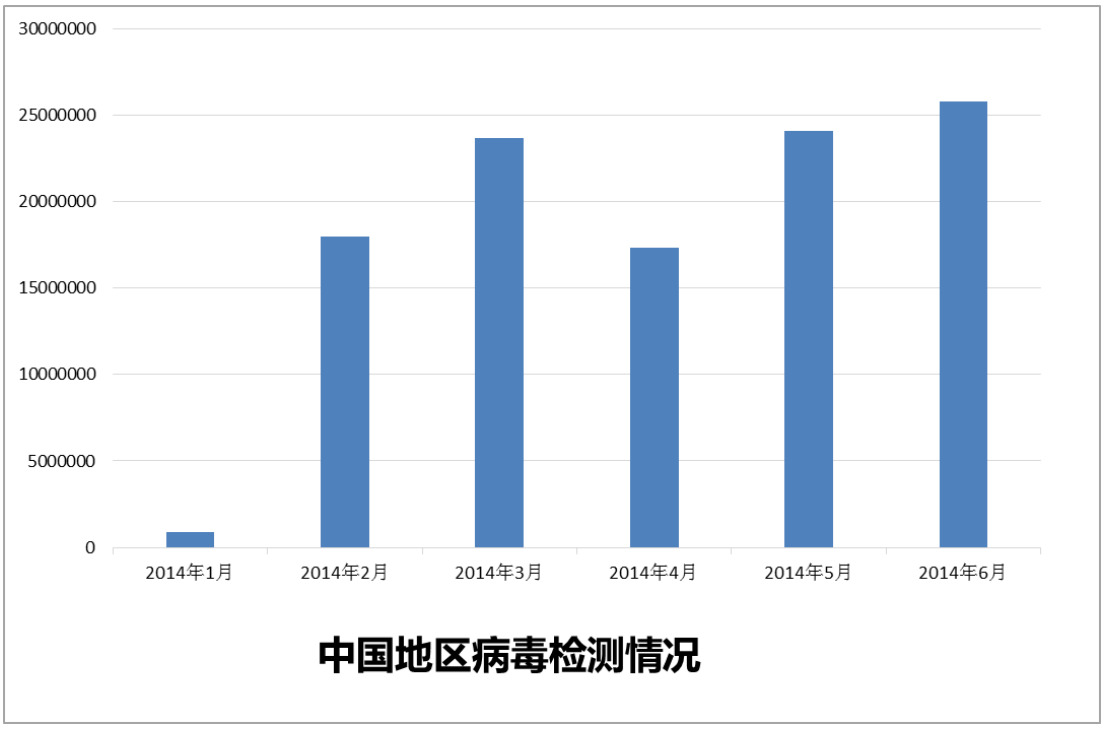
在第 2 季度中，**漏洞威胁**成为业界热点话题。因近期爆出的若干零日漏洞和 Windows XP 停止服务等重大事件，将公众对漏洞危险性的关注提升到一个新的高度。本季度发现的多个零日漏洞，影响范围包括浏览器、浏览器插件和多款软件。在三月份微软公布的安全补丁中包含了一个针对 Microsoft Word 的补丁，这意味着 Office 2010 可能会被黑客利用而沦为他们的攻击目标。上季度二月份曾有一个 Adobe Flash 的漏洞被曝光，此漏洞可以被利用来传播 PlugX 这一远程控制工具，这个工具通常被黑客用于进行针对性攻击。而就在当月

微软发布的安全通报 2934088 也提到了一个可被利用进行针对性攻击的零日漏洞，分别会影响 IE9 和 IE10。微软将这个漏洞的等级定为“严重”，因为它影响了大部分版本的 Windows 系统。Windows8.1 和 Windows XP 因使用 IE11 和 IE8 而未受该漏洞的波及。

微软从 2014 年 4 月 8 日开始正式对 Windows XP 停止服务后，XP 系统将会变得更容易受到攻击。XP 平台不兼容高于 IE8 的版本，这种情况并不能说明系统是安全的，相反这意味着 XP 用户只能使用滞后的老版本浏览器。当然用户可以选择使用 IE 以外的浏览器，但这也不能百分百保证其它浏览器就不存在漏洞。

本季度另一牵动人心的新闻就是 OpenSSL 爆出心脏出血漏洞，从披露的信息看，这个引起轩然大波的 CCS 注入漏洞已经存在了至少 10 年且影响深远，该漏洞可能会被攻击者用以窃取网银、电子商务网站上的重要信息。

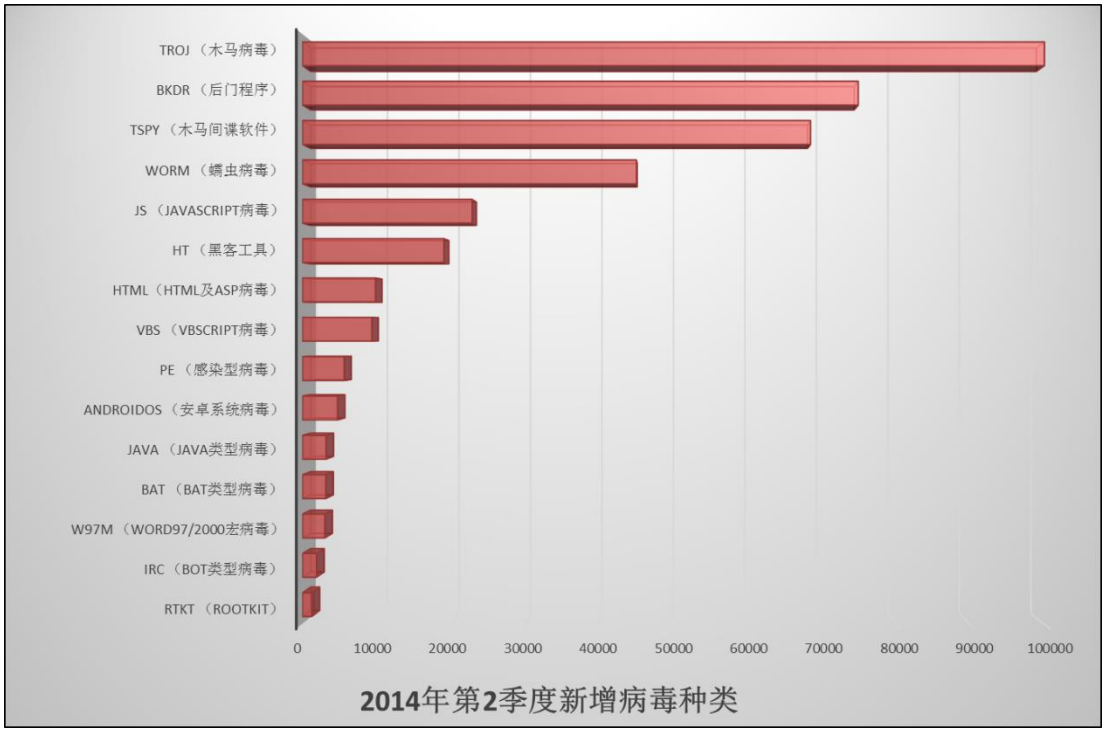
在 2014 年第 2 季度中，木马病毒、后门、间谍软件依然位列新增病毒数量排名的前三位。木马特别是盗号木马可以为编写者带来巨大的经济利益，这一特性使得木马病毒数量居高不下。后门病毒则会使受害者的计算机向攻击者敞开大门，带来极大隐患。位列第三的间谍软件则更侧重于窃取受害者的重要信息。



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 2 季度病毒威胁情况

2014 年第 2 季度新增病毒类型分析



从本季度新增种类分布图中可知，**TROJ（木马病毒）**依然是新增病毒数量类型最多的病毒类型，本季度新增木马病毒特征共计 **344,604** 个。由于木马程序的制作和散播能够得到直接的经济利益，病毒制造者倾向于制作大量木马并通过各类方式传入互联网进而传播到受害者的计算机中。木马依然是我国目前存在数量最多的病毒类型。

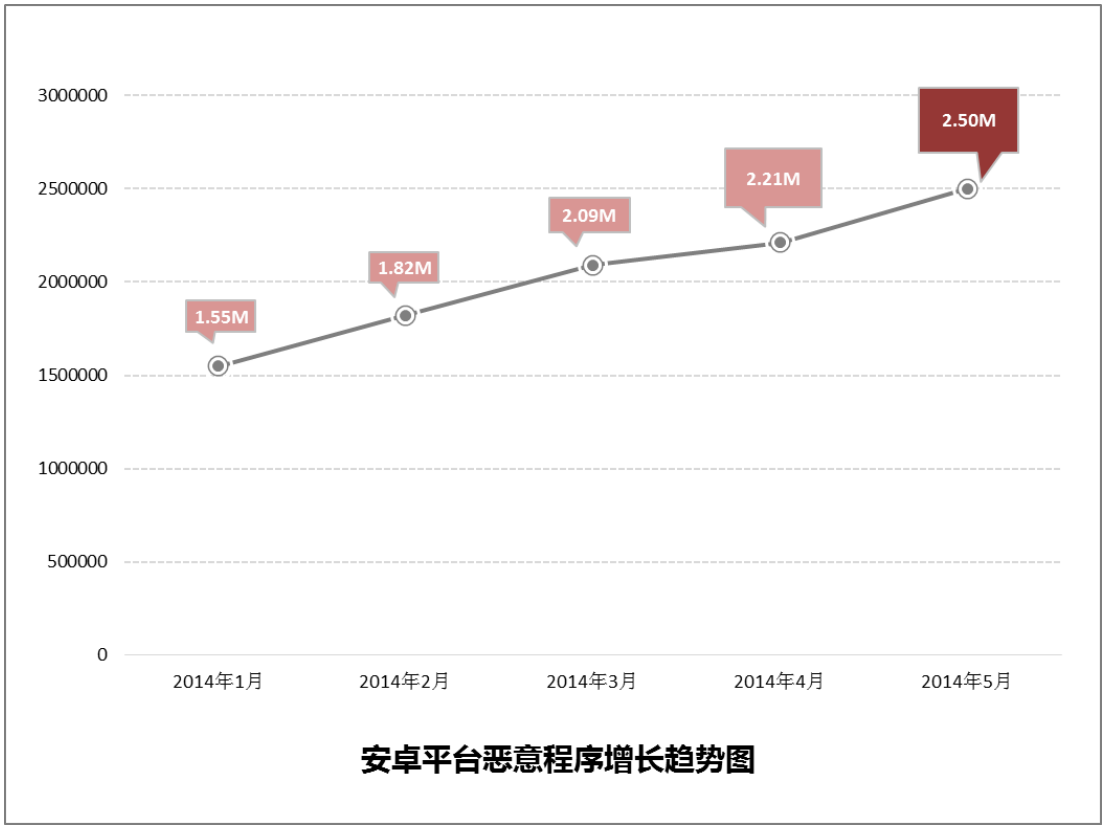
除木马类型以外，本季度新增的病毒类型中，增加数量较多的病毒类型依次为 **BKDR（后门程序），TSPY（木马间谍软件），WORM（蠕虫病毒），JS（JavaScript 病毒）和 HT（黑客工具）。**

在这些新增种类较多的病毒类型中，JS (JavaScript 病毒)、HTML(HTML 及 ASP 病毒)通常和网页挂马相关。所谓网页挂马，即攻击者将恶意代码通过非正常方式植入到被攻击的网站中。这些被恶意添加的脚本往往不容易被网站管理者以及浏览网页的用户发觉，此时正常的网站服务器就会被攻击者利用来进行散播病毒、恶意代码。此外，通过向网页插入恶意代码，网站的 WEBSHELL 也会被攻击者获取，从而能够控制网站服务器。这使攻击者具备了极高的权限，可对网站上的重要数据进行读取或修改，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，进而被用来进行网络攻击或其他一些非法的网络行为。

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。

另一个值得注意的是以 HT_开头的定义为“黑客工具”的检测类型。黑客工具从去年年初开始逐渐受到关注。地下黑市论坛的活跃使黑客工具流传广泛，不需要许多的黑客工具，网络罪犯只需购买黑客工具即能进行攻击，这使得网络安全问题日趋严重。若一台联网机器没有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），就有极大的可能被攻击。若没有完善的防护措施，公司的 WEB 服务器，甚至从互联网上能够访问到的 OA 系统都会成为攻击、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。

新增 AndroidOS(安卓系统病毒)数量在 2014 年第 2 季度中上升幅度依旧明显。上一季度可检测到的安卓病毒数量已超过 200 万个。截止到本季度 5 月底，检测数量已达 250 万个。从走势图中可以看到从 2014 年初至今，安卓病毒增长率一直保持上升趋势。

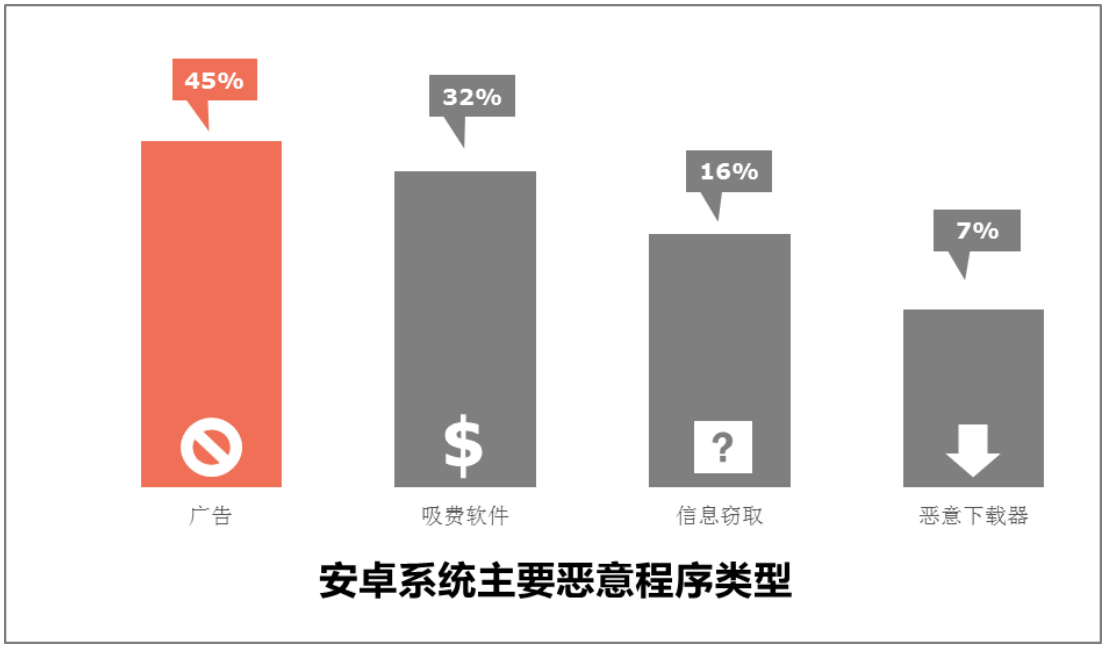


在 2014 年第 2 季度感染安卓平台的恶意程序中，广告分类超越了去年所占比例最多的吸费软件类型，成为占比最多的类型，占到所有新增病毒的 45%。吸费软件则位列第二占 32% ，第三位则依旧为窃取数据信息类型的恶意程序。随着移动运营商政策的调整，吸费软件的获益越来越少，这可能是手机病毒制造者将攻击重点转移至广告的原因。

本季度爆出的 OpenSSL 心脏出血（Heartbleed）漏洞同样影响到安卓系统。安卓 4.1.1 版本受到了心脏出血漏洞的影响。安装了该版本系统的设备，任何使用了 OpenSSL 库的应

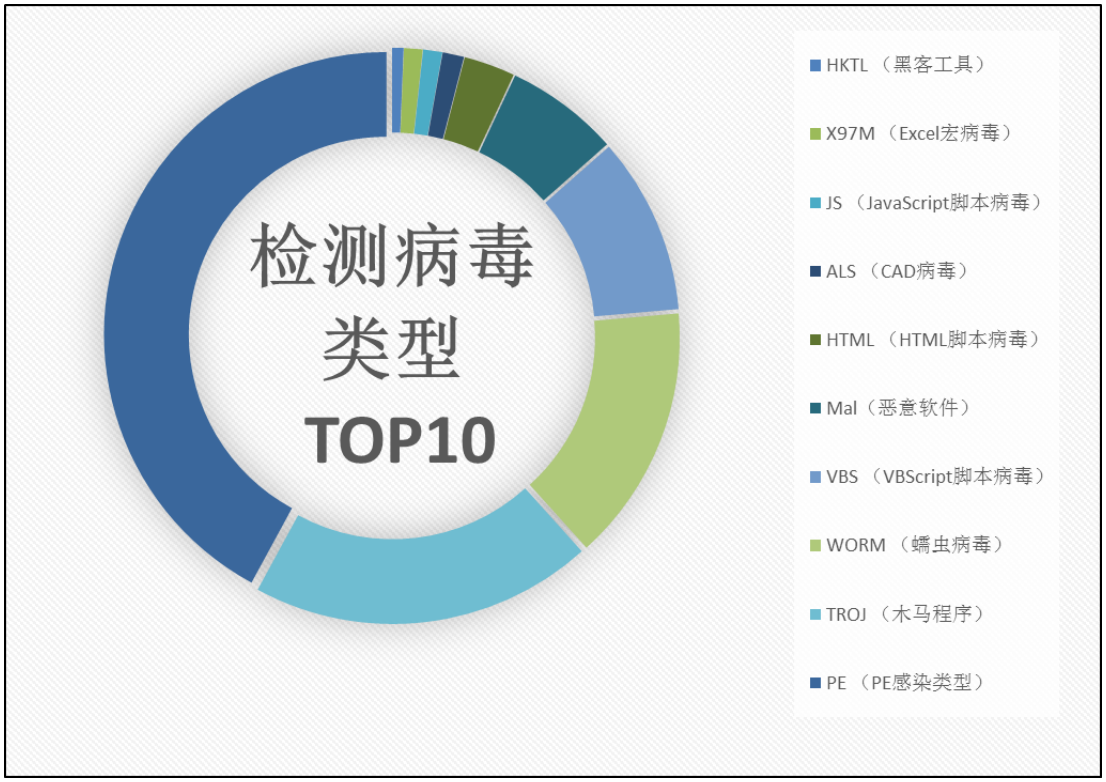
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

用程序都可能受到攻击并致使黑客从设备上获取内存当中的信息。值得注意的是，即使用户使用的安卓系统并非该版本也不代表完全安全，如果在设备上安装了存在该漏洞的应用程序同样会面临风险。



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 2 季度各类型病毒检测情况分析



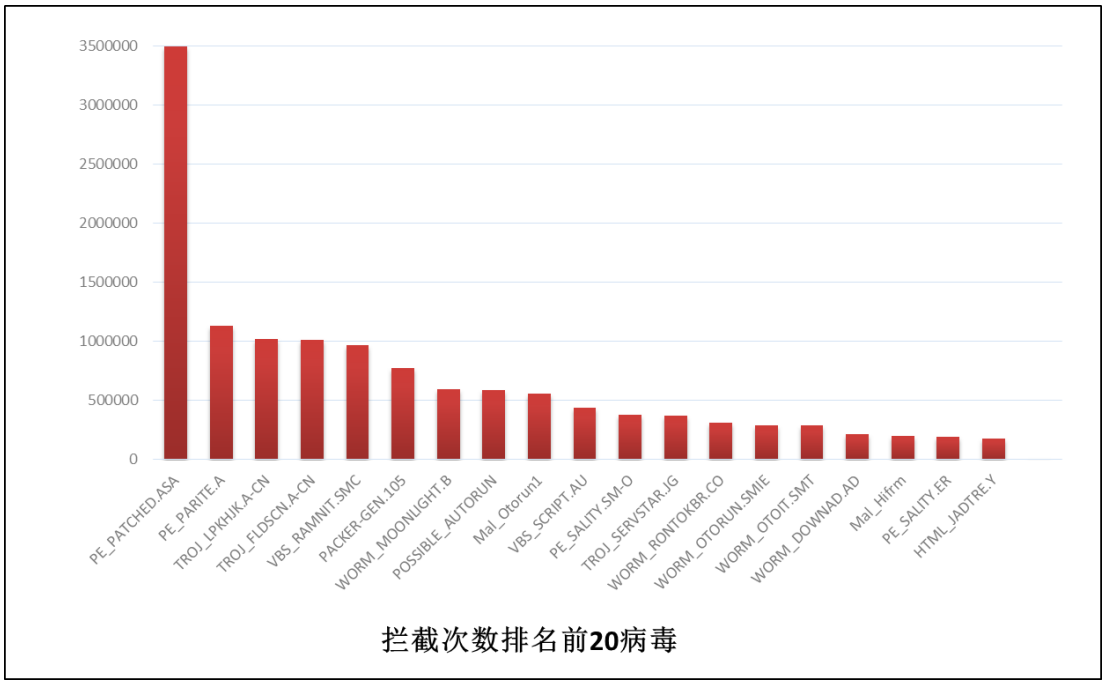
2014 年第 2 季度检测到的病毒种类中，PE 类型病毒感染数量在所有类型中所占比重最大，占到总检测数量的 42.07%。PE 病毒是感染型病毒，会大量感染系统中的可执行文件，在原有的正常文件中插入恶意代码。由于 PE 病毒的此种特性，系统一旦感染 PE 病毒就会出现大片文件连锁感染的情况，因而造成 PE 病毒的检测量很大。在本季度中，检测数量最多的 PE 病毒仍然是 PE_PATCHED.ASA。该病毒是被修改的文件 sfc_os.dll，sfc_os.dll 用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能。

木马类型病毒检测数位居第二，占总检测数的 19.61%。木马病毒通常会由其它恶意文件释放从而抵达受感染的计算机。由于木马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 和木马类型之后检测数量最多的病毒，占总检测数的 14.71%。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 2 季度感染比较多的蠕虫病毒为 WORM_MOONLIGHT 和 WORM_RONTOKBR 家族病毒。这两个家族具有典型的蠕虫病毒特征，它们的多个不同变种可通过垃圾邮件、可移动设备进行传播，释放自身的恶意副本至系统各个关键目录下，同时添加自启动项达到开机运行的目的。

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 2 季度病毒拦截情况分析



拦截次数排名前20病毒

上图显示了 2014 年第 2 季度拦截次数排名前 20 位的病毒。PE 病毒的感染数量大大高于其它病毒类型。木马类型的病毒检测名同样占据排名靠前的数个位置。PE 病毒会导致大量可执行文件被感染，而另一些传播途径多样、变种频繁的病毒也是造成检测次数居高不下的原因。

本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 349 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_MOONLIGHT.B** 检测数量大幅上升。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。

可能从其它恶意站点下载。

文件类型：

.EXE

恶意行为：

释放以下文件：

%User Profile%\O72810Z\service.exe
%System%\msvbvm60.dll
%User Profile%\O72810Z\winlogon.exe
%Windows%\M03731\EmangEloh.exe
%Windows%\M03731\smss.exe
%System%\X57785go\Z051656cie.cmd
%Windows%\sa-430654.exe
%Windows%\Ti237417ta.exe
%Windows%\M03731\Ja346188bLay.com
%System%\051656237417l.exe
%User Startup%\sql.cmd
%User Profile%\O72810Z\TuxO72810Z.exe

创建以下文件夹：

%Windows%\M03731
%User Profile%\Templates\O72810Z
%System%\X57785go

修改\添加注册表实现自启动：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
T1TT4 = "\l.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
T = "\sa-.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
Shell = "explorer.exe, \Tux.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

Userinit = "\userinit.exe , \JabLay.com"

并且修改以下注册表项，导致禁用系统资源管理器、注册表和文件夹选项：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

DisableRegistryTools = "1"

清除方法：

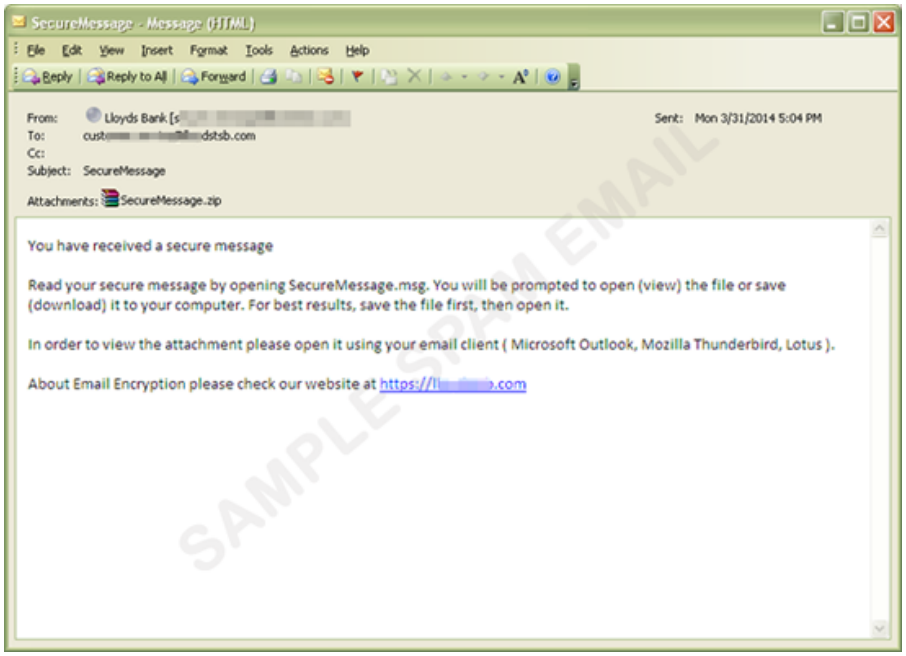
- ✓ 将趋势产品更新到最新病毒码执行全盘扫描，将所有检测为 WORM_MOONLIGHT.B 的文件删除。

详细处理方法请查看以下链接：

http://about-threats.trendmicro.com/malware.aspx?language=cn&name=WORM_MOONLIGHT.B

2014 年第 2 季度热门新型病毒分析

2013 年起，China RTL 监控到检测名为 UPATRE 的病毒家族变种频繁出现，该家族病毒利用社会工程学，通过一封带有加密附件的垃圾邮件诱骗用户点击打开病毒附件来进行传播。



带有恶意附件的垃圾邮件样本

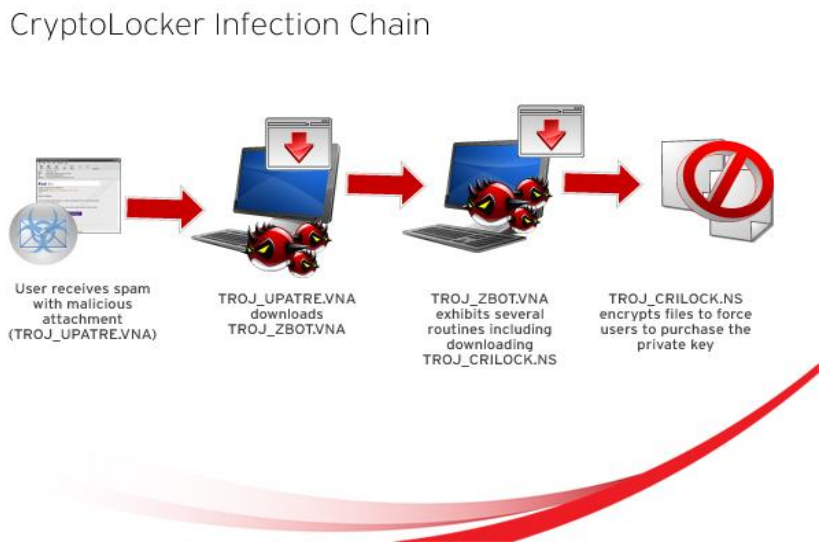
该病毒的详细信息如下：

相关检测名：

TROJ_UPATRE.SM,TROJ_UPATRE.VNA，
TROJ_UPATRE.SMA，TROJ_UPATRE.SMZ8，
TROJ_UPATRE.SMZ9，TROJ_DLOADER.SM3

传播渠道：

通过垃圾邮件伪装成一个附件进行传播。这些垃圾邮件利用社会工程学引诱用户打开并执行恶意程序从而导致被感染。此次发送的垃圾邮件中包含一个加密附件，并在邮件附件中写上密码，从而诱骗用户以为是一封正常邮件。



UPATRE 病毒附在垃圾邮件中下载勒索软件

病毒行为：

1. 创建自身副本并将原文件删除

病毒会在受感染的系统上释放一个自身文件的副本：

%User Temp%\{random name}.exe

运行该副本，并终止、删除原来的可执行文件。

2.下载其它恶意软件

它会连接硬编码 URL，下载恶意文件到系统以下位置：

%User Temp%\{random name}.exe

它通过一个加密的 SSL 连接下载。经分析，大部分 URL 都是恶意网站，在这些网站上发现有恶意文件。

现有 IMSA 的应对措施：

- ✓ 内容过滤策略，过滤关键字
  作用：可以通过关键字过滤部分已知的仿冒邮件攻击。
- ✓ IMSA 病毒检测
  作用：可以过滤已知的病毒附件
- ✓ 附件过滤策略
  作用：可以有效降低客户机受感染的风险
  注意：当遇到针对性高密度攻击的时候，推荐临时采取此方案
- ✓ 开启 ERS 过滤 和 WRS 过滤
  作用：可以过滤掉一批经常用来发送恶意邮件的 IP 地址或有害链接
- ✓ 开启 IMSA 反向 DNS 解析验证
  作用：有效阻止仿冒的发件人
- ✓ 整合 “Deep Discovery Advisor”，对可能存在的未知文件进行分析，对潜在的风

险及时发现并发出警告
作用：可以有效发现潜在的安全风险

建议处理措施：

1. 开启反向 DNS 解析，阻止仿冒邮件。
2. 及时更新病毒库，并且向 RTL 提交未检测到病毒的仿冒邮件样本。
3. 加强员工安全教育，请员工不要随意打开可疑邮件的附件，告知员工管理员不会向员工以附件的方式发送任何程序和脚本，不要打开任何在邮件中的可执行文件。谨慎打开附件中的 WORD 文档。
4. 及时更新产品病毒库。

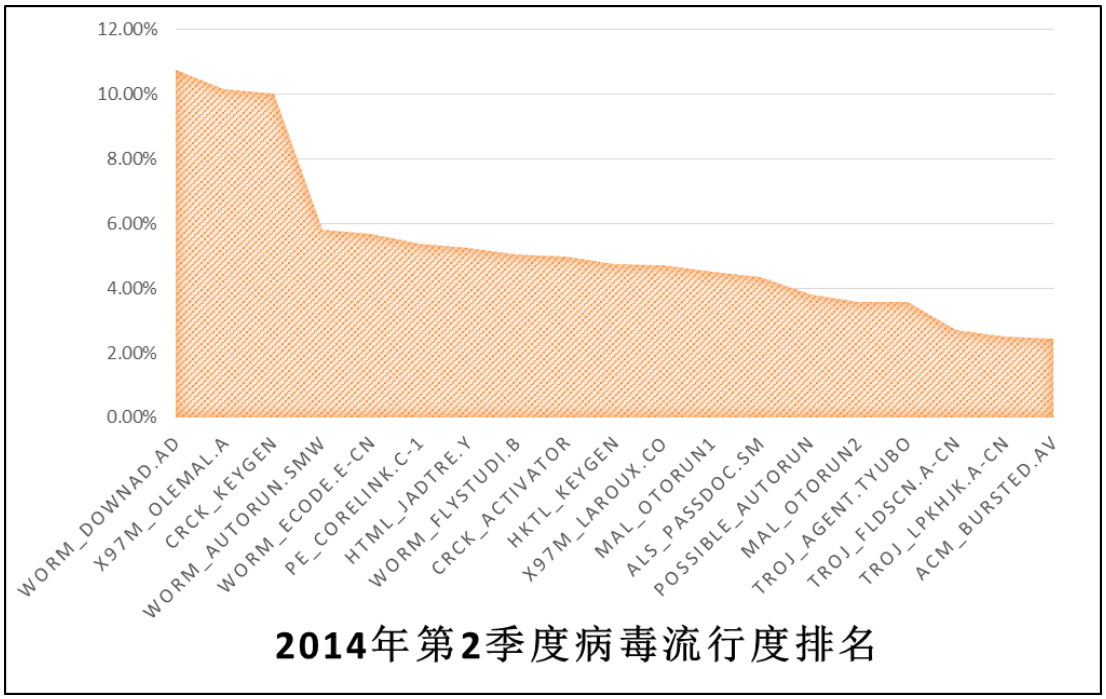
解决方法：

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该恶意软件的所有变种。
2. 使用趋势科技邮件安全产品，升级到最新垃圾邮件特征码可有效拦截带有恶意附件的垃圾邮件。
3. 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，如有需要，请和我们联系。

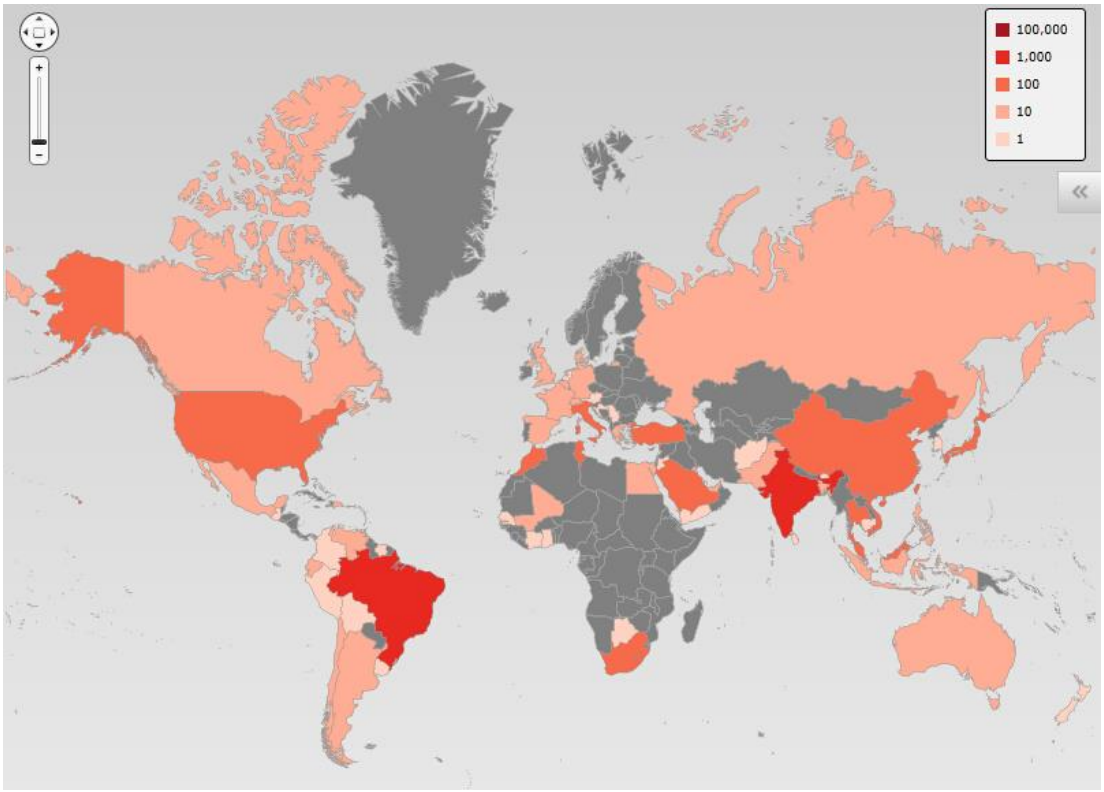
相关链接信息：

http://blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeuszbot-connection/

2014 年第 2 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 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 2014 年第 2 季度，约有 10% 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 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。

2014 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：

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。

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

✓ 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

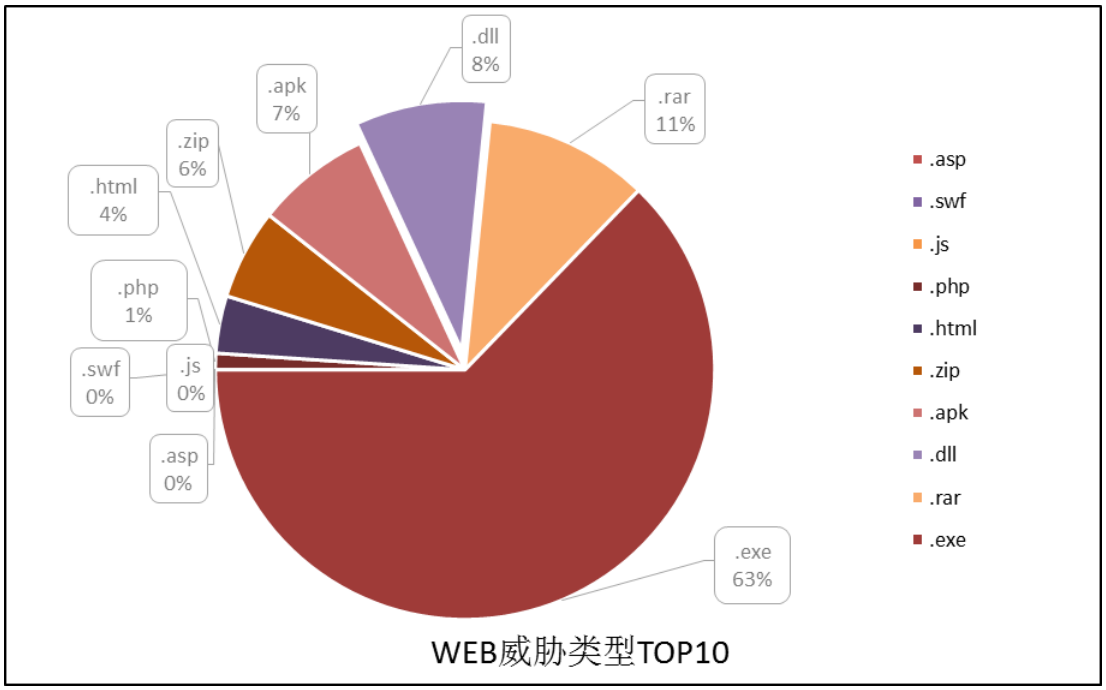
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2014 年第 2 季度 WEB 安全威胁情况

2014 年第 2 季度 WEB 威胁文件类型分析

在 2014 年第 2 季度的数据中，通过 WEB 传播的恶意程序中，约有 63%是.EXE 文件，占到统计总数的一半以上。.EXE 文件类型依然是通过 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某些类型的文件下载。

此外，在本季度得到的数据中，压缩文件格式.RAR 和.ZIP 文件所占比例相对靠前，应值得注意。此类文件相较.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。



2014 年第 2 季度中国地区 WEB 威胁文件类型分布图

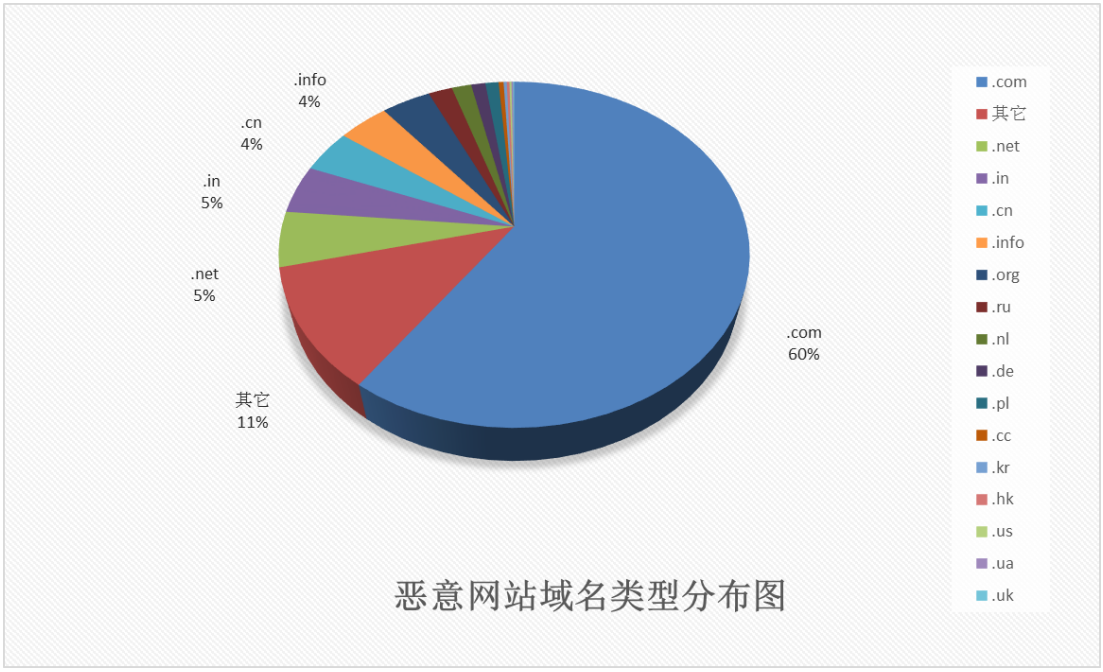
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 2 季度 TOP 10 恶意 URL

TOP10 恶意URL		
恶意URL	描述	点击量
http://wp***1.dat	该网站的地址在垃圾邮件中被发现或网站直接或间接帮助传播恶意软件或恶意代码	3,227,013
http://wpa***ad.dat	该网站的地址在垃圾邮件中被发现或网站直接或间接帮助传播恶意软件或恶意代码	1,309,548
http://n.im**8.net/	该网站的地址在垃圾邮件中被发现或网站直接或间接帮助传播恶意软件或恶意代码	967,062
http://wpa***w/wpad.dat	该网站的地址在垃圾邮件中被发现或网站直接或间接帮助传播恶意软件或恶意代码	617,171
http://treez***841074.zip	间接帮助传播恶意软件或恶意代码	591,412
tlo***do.com	此链接为恶意程序的命令与控制(C&C)服务器。	582,181
http://up.s***.1.0.1130&trigger=sched	该网站的地址在垃圾邮件中被发现	580,183
http://wpa***et/wpad.dat	该网站的地址在垃圾邮件中被发现	532,181
http://wwww.5id***m/	该网站的地址在垃圾邮件中被发现或网站直接或间接帮助传播恶意软件或恶意代码	494,712
http://imd***11135395.html	此链接为恶意程序的命令与控制(C&C)服务器。	398,426

2014 年第 2 季度中国地区被 WRS 拦截的恶意 URL 排名

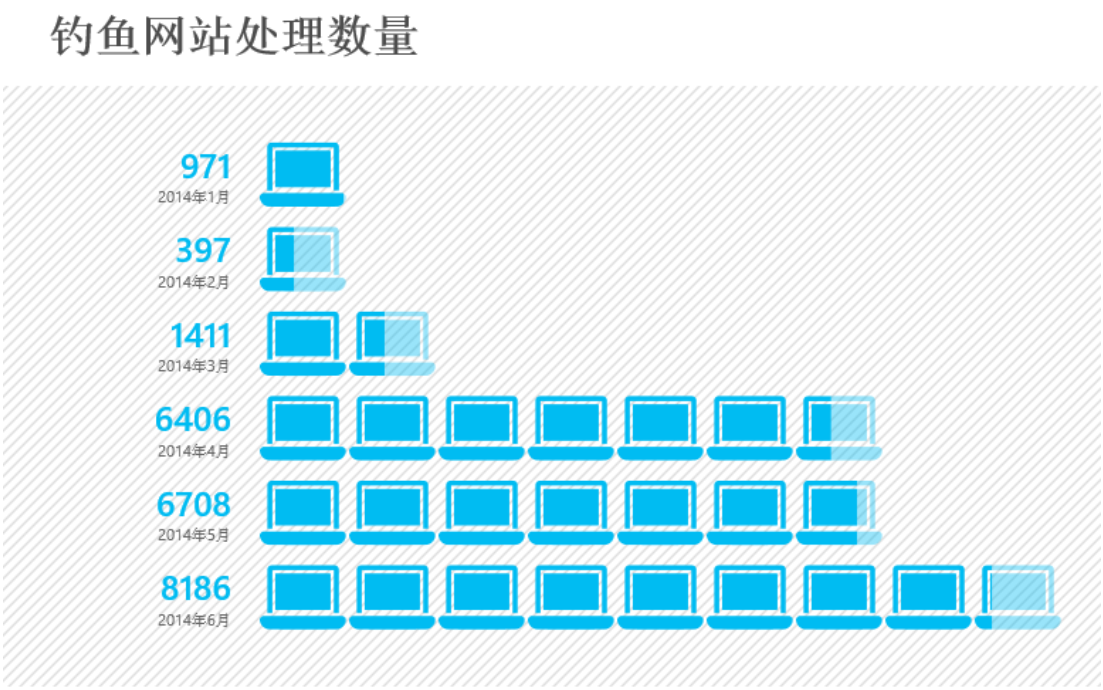
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。



2014 年第 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、.NET、.IN 的域名的站点占总数 76.42%。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 2 季度 WEB 威胁钓鱼网站仿冒对象分析



中国地区钓鱼网站数量

从中国反钓鱼联盟获得的数据，2014 年 1 月至 2014 年 6 月共计 6 个月中，处理钓鱼网站共计 24,079 个。从趋势图可以看到，2014 年第 2 季度钓鱼网站发现数量大大高于第 1 季度。

从过去几个月的监控数据来看，钓鱼网站的仿冒对象涉及媒体传播类、金融证券类、支付交易三大类最多。媒体传播类中多以仿冒各大电视台为对象：央视和地方卫视是本类钓鱼网站中频繁被仿冒的对象；金融证券类多以仿冒各大银行为对象，主要以四大行居多；支付交易多以仿冒淘宝网为对象。本季度 5、6 月份以淘宝网作为仿冒对象的钓鱼网站数量剧增，占总数 8 成以上，需特别引起重视。

对中国地区钓鱼网站历史数据监控可以发现，钓鱼网站的仿冒对象往往会随着媒体热点话题的变化而转移。第 2 季度中恰逢儿童节、父亲节及国定小长假等假期，在对假日期间的钓鱼网站监控后发现针对“旅行社类”、“航空公司类”、“酒店类”等相关行业的网站有明显增多的趋势。

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。

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 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	3,654,451
MS09-019	237,385
CVE-2009-1531	198,158
CVE-2009-1140	39,222
CVE-2010-3333	22,324
CVE-2010-3334	11,158
CVE-2010-3335	11,158
CVE-2010-3336	11,158
CVE-2010-3337	11,158
CVE-2005-0491	5,143

2014 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
MS09-019	http://technet.microsoft.com/zh-CN/security/bulletin/ms09-019
CVE-2009-1531	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2009-1531
CVE-2009-1140	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2009-1140
CVE-2010-3333	http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2010-3333
CVE-2010-3334	http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2010-3334
CVE-2010-3335	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3335
CVE-2010-3336	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3336
CVE-2010-3337	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-3337
CVE-2005-0491	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2005-0491

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。

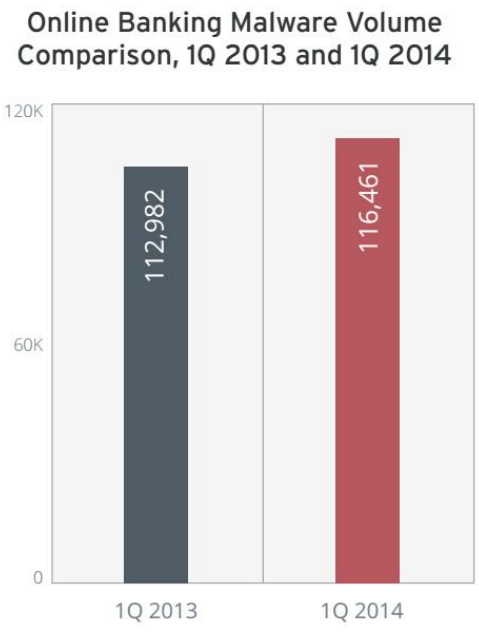
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 2 季度最新安全威胁信息

2014 年第 1 季度趋势科技全球区安全威胁概要

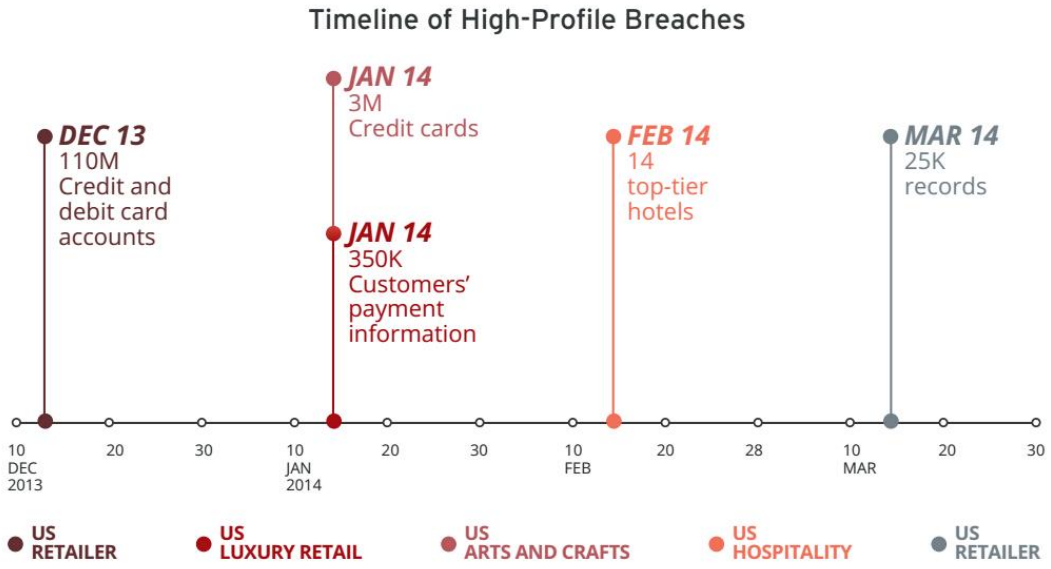
以下是来自 2014 年第 1 季度趋势科技全球区安全报告的数据。

在 2014 年第 1 季度中检测到针对网银的恶意软件检测数量达到接近 116,000 次，较 2013 年第 1 季度的检测数量 113,000 次有缓慢的稳固上升趋势。美国依然是遭受网银相关恶意软件攻击次数最多的地区。



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 1 季度中，多家公司承认遭受 PoS 系统引发的泄露事件，甚至在单起事件中引起 1.1 亿用户的个人信息被盗的情况。

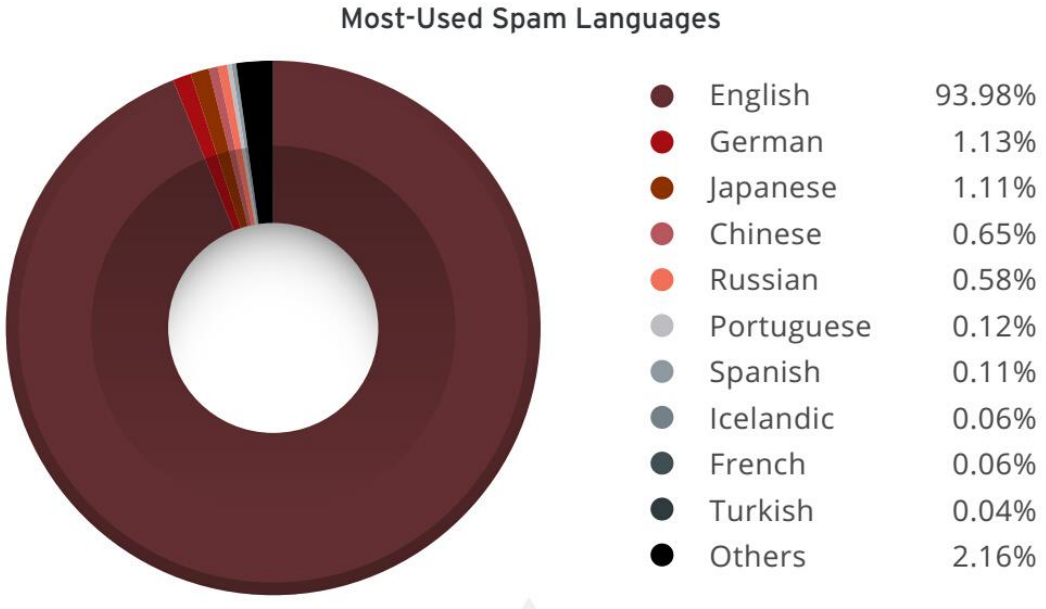


在第 1 季度中，政府机构依然是针对性攻击最大的攻击目标。

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。

网络罪犯利用热门话题、活动、电影、应用和自然灾难等等，诱骗尽可能多的受害者掉入他们预先设置的“陷阱”。从图中可以看到，诸如“Flappy Bird”、“MH370 搜索”也曾是中国地区的热门搜索关键词。

2014 年第 1 季度中，英语依然是垃圾邮件最常使用的语言：



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 1 季度全球安全报告请访问：

http://about-threats.trendmicro.com/us/security-roundup/2014/1Q/cybercrime-hits-the-unexpected/

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 2 季度安全威胁信息摘要

2014 年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。

❖ Gameover ZeuS 病毒被中断

美国联邦调查局（FBI）宣布 Zeus/ZBOT 的 P2P 变种（即 Gameover 病毒）在多国协力合作下已经被中断。趋势科技也参与了此次摧毁 Gameover 病毒的行动。

Gameover 是基于 ZeuS 源代码编写的病毒，这些源代码在 2011 年 5 月时被泄露。基于被泄露代码编写的其它病毒家族（如 Citadel 和 Kins）与它有极大差异。ZeuS 病毒只会连接到它的配置文件中写入的特定 C&C 服务器上。如果服务器无法访问，ZBOT 病毒就无法下载包含目标 URL 的动态配置文件。而 Gameover 病毒则具有 P2P 连接功能。

http://blog.trendmicro.com/trendlabs-security-intelligence/gameover-zeus-with-p2p-functionality-disrupted/

❖ 安卓勒索软件利用 TOR

分析检测名为 AndroidOS_Locker.HBT 的样本，我们发现这个恶意软件会提示用户通知他们的设备已被锁定，需要支付 1000 卢布的赎金来进行解锁。这一行为是典型的勒索软件特征，同时我们发现该恶意软件是通过 TOR 来和它的 C&C 服务器进行通讯的。虽然这不是第一个利用 TOR 的安卓恶意软件，但这是首次发现利用 TOR 的勒索软件。我们预测这可能将会成为移动设备上的勒索软件的一个新趋势。

http://blog.trendmicro.com/trendlabs-security-intelligence/android-ransomware-uses-tor/

❖ VOBFUS 家族病毒新发展，加入多国语言

VOBFUS 家族病毒因其多态能力而受到关注，这一特点使其极易产生新的变种。而我们近期发现它的一个新变种具有之前从未出现过的新能力：这一变种具有了“说”多国语言的能力。利用“本土化”威胁的方式可以被看作是网络罪犯的一种欺骗方式。用母语书写的文件或者通知比看到用英语写的文字更能激起读者的兴趣。用户也往往会产生“本土化”的文件和通知相对安全的错觉。

http://blog.trendmicro.com/trendlabs-security-intelligence/vobfus-evolves-adds-multiple-languages/

❖ 微软 2014 年 5 月推出 8 个安全公告

这个月的微软安全公告共推出 8 个补丁，是今年到目前为止发布数量最多的一次。在这 8 个安全公告中，2 个被评为“严重”等级，其余则为“重要”等级。尽管微软已经发布了额外的适用于 Windows XP 的补丁以解决零日漏洞，在公告中针对 XP 系统补丁的空缺依旧醒目。

http://blog.trendmicro.com/trendlabs-security-intelligence/may-2014-patch-tuesday-rolls-out-8-bulletins/

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。

❖ 网络罪犯在垃圾邮件中利用心脏出血漏洞

4 月初传出心脏出血漏洞（Heartbleed）消息后，互联网上安全专家、知名人士对这个漏洞的更新、细节分析等消息源源不断。网络犯罪分子已经开始利用心脏出血漏洞的相关新闻伺机进行垃圾邮件攻击。

http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-take-advantage-of-heartbleed-with-spam/

❖ Windows XP 正式宣布“退休” 趋势科技协助用户防范未知风险

微软已经正式宣布终止对 Windows XP 操作系统的支持！这意味着新发现的 Windows XP 漏洞微软官方将不再进行追踪、回应和修补。有鉴于 Windows XP 仍是目前普遍被企业与消费者使用的操作系统，终止支持势必带来潜在的信息安全疑虑。全球服务器安全、虚拟化安全及云安全领导厂商趋势科技表示，使用 Windows XP 的风险将会攀升，用户最好尽快升级操作系统，同时趋势科技也将提供必要的工具，来协助用户防范 Windows XP 系统所面临的未知风险，包括虚拟补丁修补/漏洞防护技术、强化终端设备的安全性等，以帮助企业与个人用户实现平稳过渡。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20140507071836.html

❖ 互联网“心脏大出血” 趋势科技紧急提供虚拟补丁解决方案

近日，互联网爆发了被称为“心脏出血”式的严重安全事件。互联网应用最普遍的网络安全协议 OpenSSL 协议的源代码被爆存在高风险漏洞，可以让攻击者获得服务器内存中的数据内容，甚至导致网络账户与密码、网银资金、电子邮件等重要信息的泄漏！全球服务器安全、虚拟化安全及云安全领导厂商趋势科技提醒互联网服务提供商应尽快升级服务器，并通过趋势科技入侵防御系统（IDF）保护服务器信息不被窃取。同时，趋势科技已在第一时间发布了虚拟补丁，帮助用户避免重要数据泄露。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20140507072247.html

❖ 新型 0-day 漏洞影响 IE 浏览器 趋势科技虚拟补丁助用户脱离险境

近日，微软发布了一个安全公告：2963983，其指出当前所有主流版本 Internet Explorer 浏览器（IE6~IE11）均存在 0-day（零日攻击）漏洞，这成为第一个会影响 Windows XP 系统而不会被修补的漏洞，将可能导致内存崩溃，使攻击者能够在当前用户账户下执行恶意代码！截止目前，趋势科技已在漏洞公告两天内 (4/29-4/30)将虚拟补丁自动推送给所有部署

了趋势科技 Deep Security（服务器防护）、OfficeScan IDF（终端防护）或 Deep Edge（网关防护）等解决方案的用户。此外，趋势科技威胁发现设备 TDA 也在已更新的病毒码中会包含了对于此漏洞攻击行为的检测，在攻击还没有造成破坏之前，帮助用户全面、及时的找出安全威胁。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20140507075806.html

- 世界杯相关恶意 App 已超过 375 种！趋势科技建议采取“读、不、安”三大法宝　保护球迷“百毒不侵”!

随着世界杯足球赛赛程推进，世界杯相关恶意程序也大量涌出!根据趋势科技最新统计，目前全球已出现超过 375 种移动恶意 App，正潜伏在未经授权/第三方应用程序下载商店，等待用户安装到移动设备上。趋势科技呼吁球迷可采取“读、不、安”三大防御法宝，让自己“百毒不侵”!。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20140626032800.html

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