中国地区 2014 年
第三季度
网络安全威胁报告

2014/11

CHINA RTL

目录

2014 年第 3 季度安全威胁

本季安全警示：
手机病毒，漏洞威胁，木马

2014 年第 3 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 **53** 万条。截止 2014.9.30 日中国区传统病毒码 **11.178.60** 包含病毒特征数约 **434** 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 **6,988** 万次。

- 本季度趋势科技在中国地区拦截的恶意 URL 地址共计 **15,536,971** 次。

在 2014 年第 3 季度中，**手机病毒**的增长数量持续上升。根据统计数据，在不同手机恶意软件类型中，具有高风险的广告软件数量迅速增加。

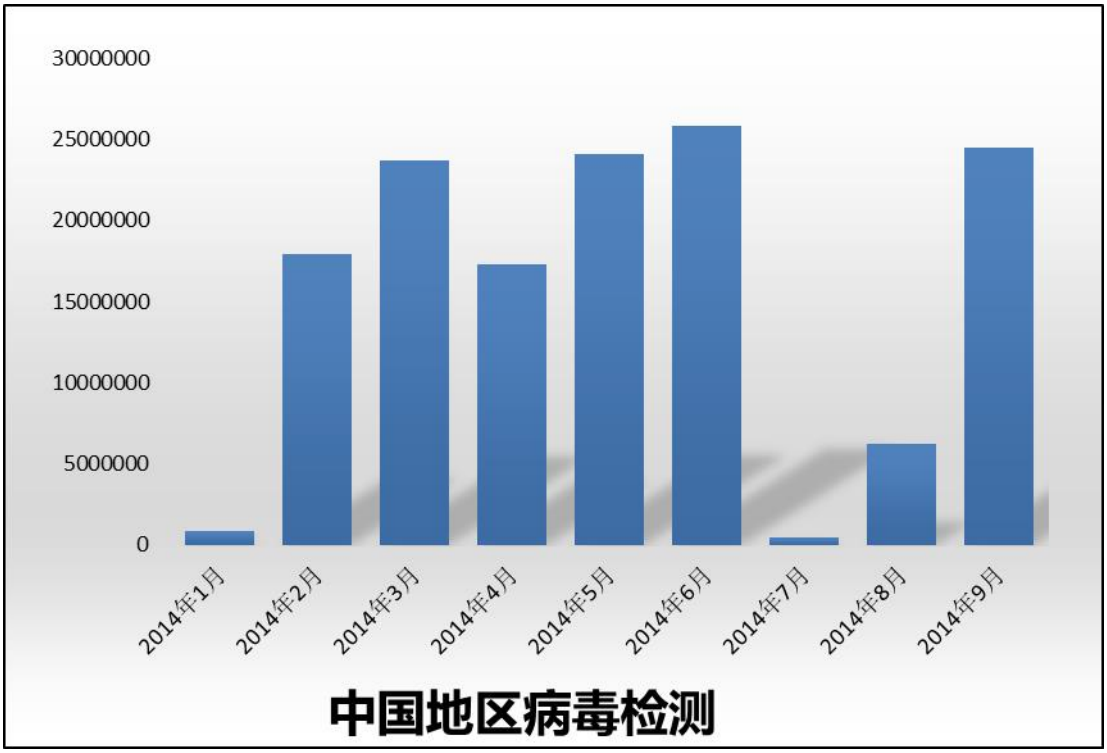
今年 8 月在中国地区爆发的一款名为“XX 神器”的手机病毒引起广泛关注。该病毒针对安卓系统，病毒文件被运行后会遍历受感染手机上的通讯录，并向其通讯录中的联系人群发一条短消息：“XXX（收件人姓名）看这个，http://*** XXshenqi.apk”。收到短消息的人如果下载了链接指向的文件并运行后就会不幸中招。经分析，该病毒的主程序是一个名为 com.android.Trogoogle.V1.0.apk 的文件。运行后，屏幕上显示一个“XX 神器”登录界面，并需要用户输入姓名、手机号等信息，在登录界面之后没有任何其它功能。而主程序则在启动后以服务的形式在后台运行，它没有任何图形界面因此不易被用户发觉。该恶意程序通过手机后台服务监听并拦截短信，并将短信发送给病毒原作者，会造成用户隐私泄露而群发短消息的行为也会使受感染手机产生大笔通信费用。

该病毒在短时间内迅速扩散，造成大量用户的经济损失。但在之后对该手机病毒样本进行的分析报道中可以发现其实它并没有使用复杂技术，在隐藏恶意行为方面也没有作特别的处理，如果仔细观察可以发现漏洞百出。但其相对取巧的传播方式（在消息里嵌入收件人的名字，增加真实度）使接到恶意链接的用户放松警惕，导致大量用户轻易相信了这条短消息并下载了病毒。此次事件也为公众对手机平台安全的关注敲响警钟。

上季度爆出的心脏出血漏洞被定义为迄今为止最严重的漏洞，它带来的震动还未平息，第 3 季度又一严重漏洞——破壳漏洞（ShellShock）再掀波澜。**漏洞威胁**持续成为本季度业界热点。从公开的信息来看，该漏洞存在已久而且影响范围巨大，和心脏出血漏洞相比危险度更为严重。这个存在于 Unix 系统上的漏洞会将全球数以亿计的服务器、设备及用户置于危险之中。破壳漏洞之所以严重，是因为要利用它来发动攻击轻而易举，攻击者不需要太多的专业技术能力。破壳漏洞就像在系统上开了一个后门，让黑客能够从远程执行指令、取得系统控制权、收集和窃取数据、篡改网站等等。绝大多数采用 Linux 操作系统的计算机和

接入网络的设备，如路由器、Wi-Fi 无线路由器等都会受到影响。

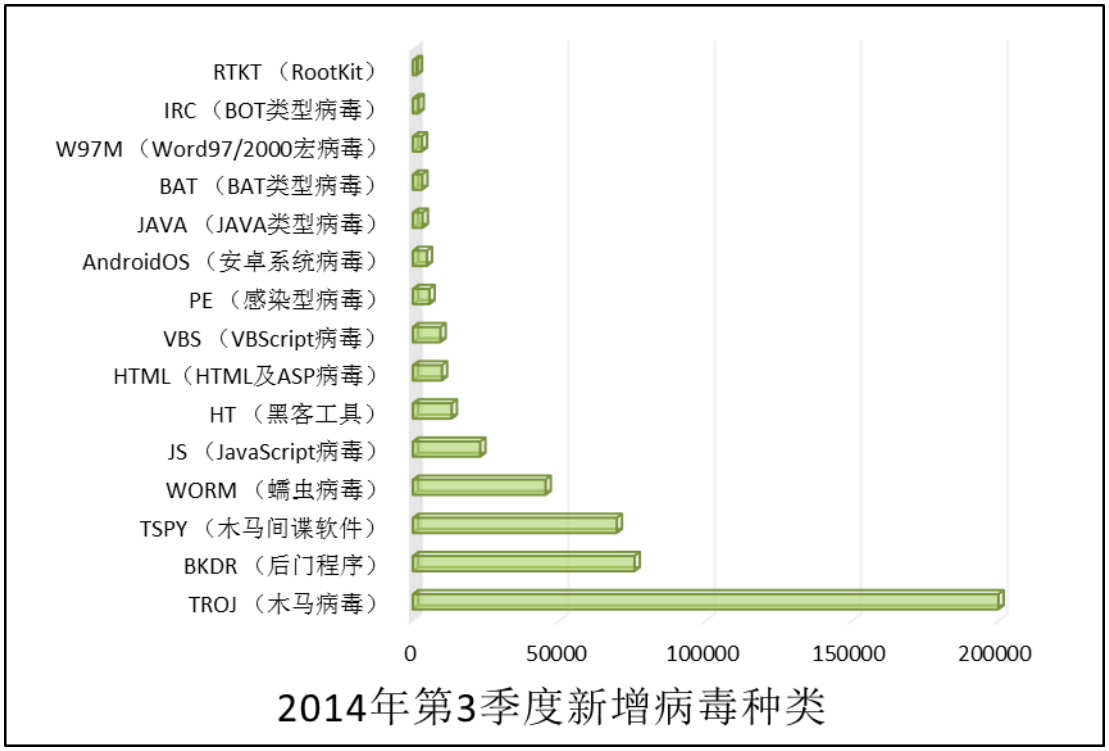
在该漏洞被披露后不久，趋势科技随即发现了利用此漏洞进行的僵尸网络攻击和 IRC 僵尸机器人攻击。攻击范围遍布全球各地区，中国地区同样发现了针对金融机构的破壳漏洞攻击。趋势科技 Deep Discovery 产品侦测到了这一波攻击：攻击者试图确认目标机构下的多个 IP 地址是否有破壳漏洞（即 CVE-2014-06271）。并且使用/bin/uname –a 指令企图收集目标操作系统型号、机器类型和处理器信息等数据。虽然目前这些行为并不会对目标产生直接危害，但这可能是攻击者在策划进行后续攻击的前期准备工作。此次攻击的时间段选择也比较特殊：攻击发生于 10 月国庆长假期间，攻击者选择这段时间在于管理员可能并不在现场。



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 季度病毒威胁情况

2014 年第 3 季度新增病毒类型分析



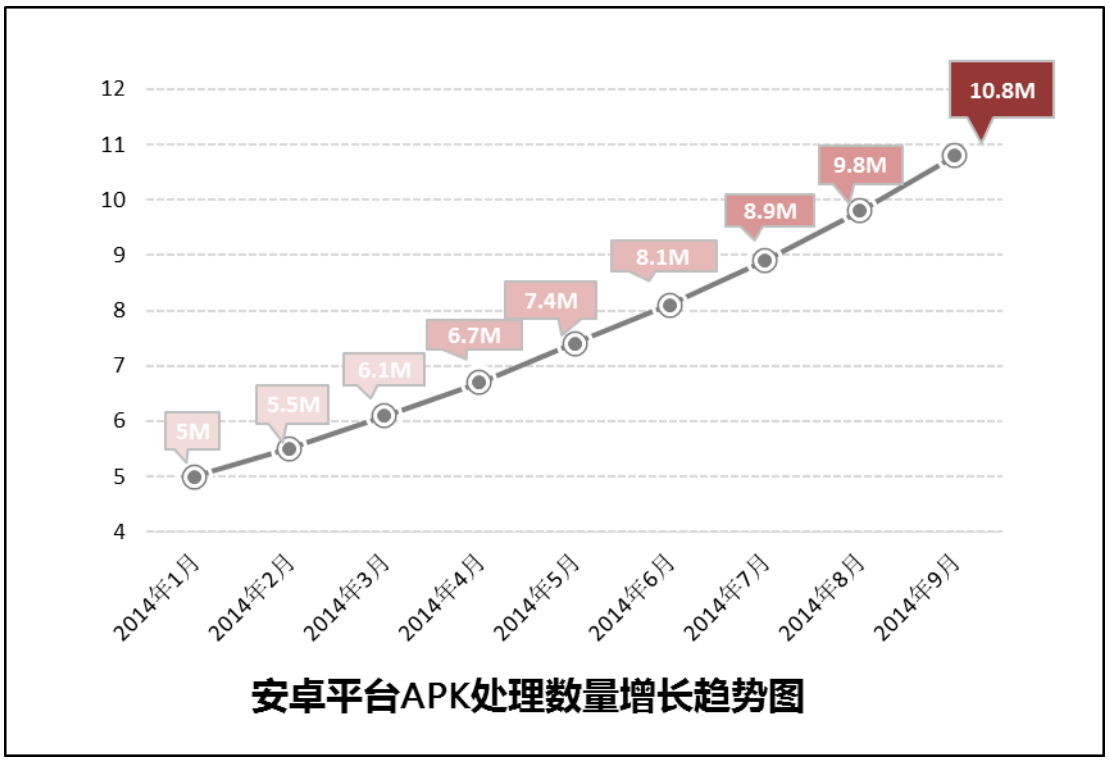
在 2014 年第 3 季度新增病毒种类中，以 **TROJ（木马病毒）**类型增幅最大。据统计，本季度新增木马病毒特征共计 **350,008** 个。木马病毒以获得经济利益为目的，为制作者带来丰厚利益。在中国地区，病毒制作者更倾向于制造此类型病毒，并通过各类方式传入互联网进而传播到受害者的计算机中。

紧随木马病毒类型之后，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），**本季度排名顺序与前季度相比没有出现显著排名变化。

其中 JS (JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒通常和网页挂马相关。在近期媒体报道的多起攻击事件中，网页挂马这种黑客攻击手段经常会被提起。攻击者先将恶意代码通过非正常途径强制上传到被攻击的网站里，然后获得管理员权限操作攻击目标——这是一种攻击者经常会使用的入侵方式。网站管理者以及浏览网页的用户难以察觉到恶意添加的脚本，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。另一方面，网站的 WebShell 也会被攻击者夺得，进而夺取服务器的控制权。攻击者具备管理员权限后，可以任意浏览重要数据、篡改信息。

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。

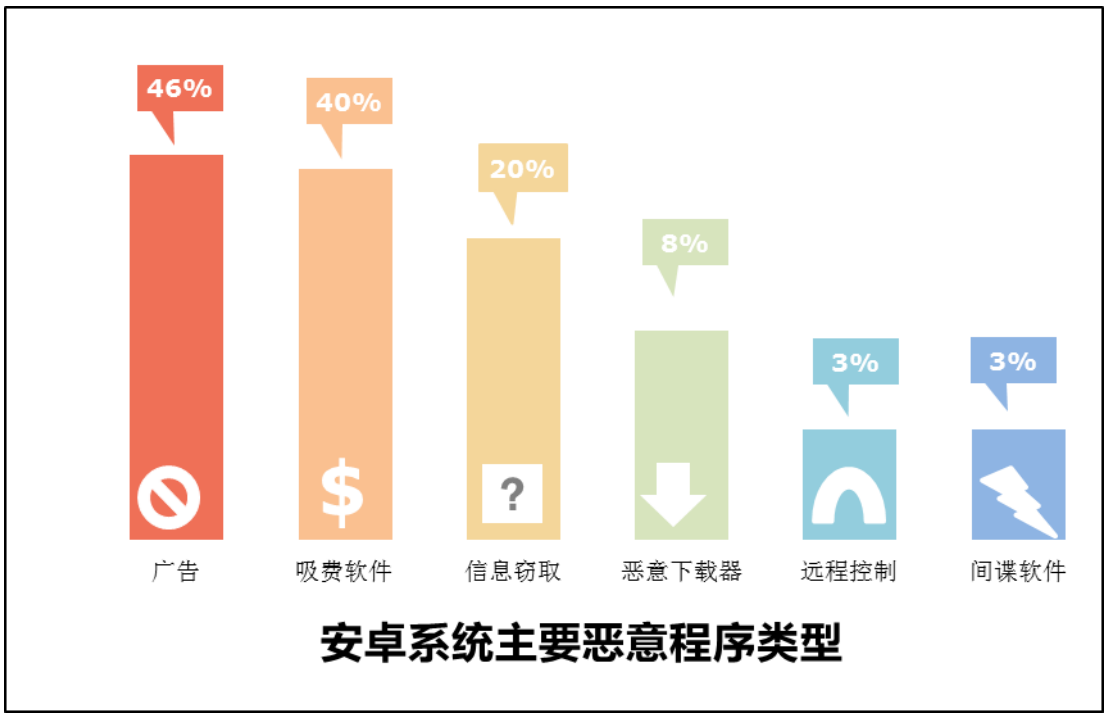
在第 3 季度，以 HT_开头的定义为“黑客工具”的检测类型同样值得我们关注，此类型恶意软件增加数量在过去几个季度中一直排名靠前。分析其中原因，一方面，黑客工具的获取途径简单，从网络黑市上就能轻易购买。另一方面，对攻击目标来说，如果没有及时打上漏洞补丁或存在安全盲点：开启远程桌面或使用弱密码等，就极容易受到来自外部的攻击。如果企业网络安全管理人员没有对安全问题提高关注度的话，内部的 WEB 服务器、甚至从互联网上能够访问到的 OA 系统都会受到威胁。



截止到 2014 年 9 月 30 日，趋势科技发布中国区移动客户端病毒码版本是 1.757.00，大小 23,122,092 字节。

趋势科技对 APK 文件的处理数量在 2014 年第 3 季度依旧呈上升趋势。继上一季度处理 APK 数量突破 800 万个以后。截止到本季度 9 月底，处理数量突破 1000 万个。从 2014 年初至今，安卓病毒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。

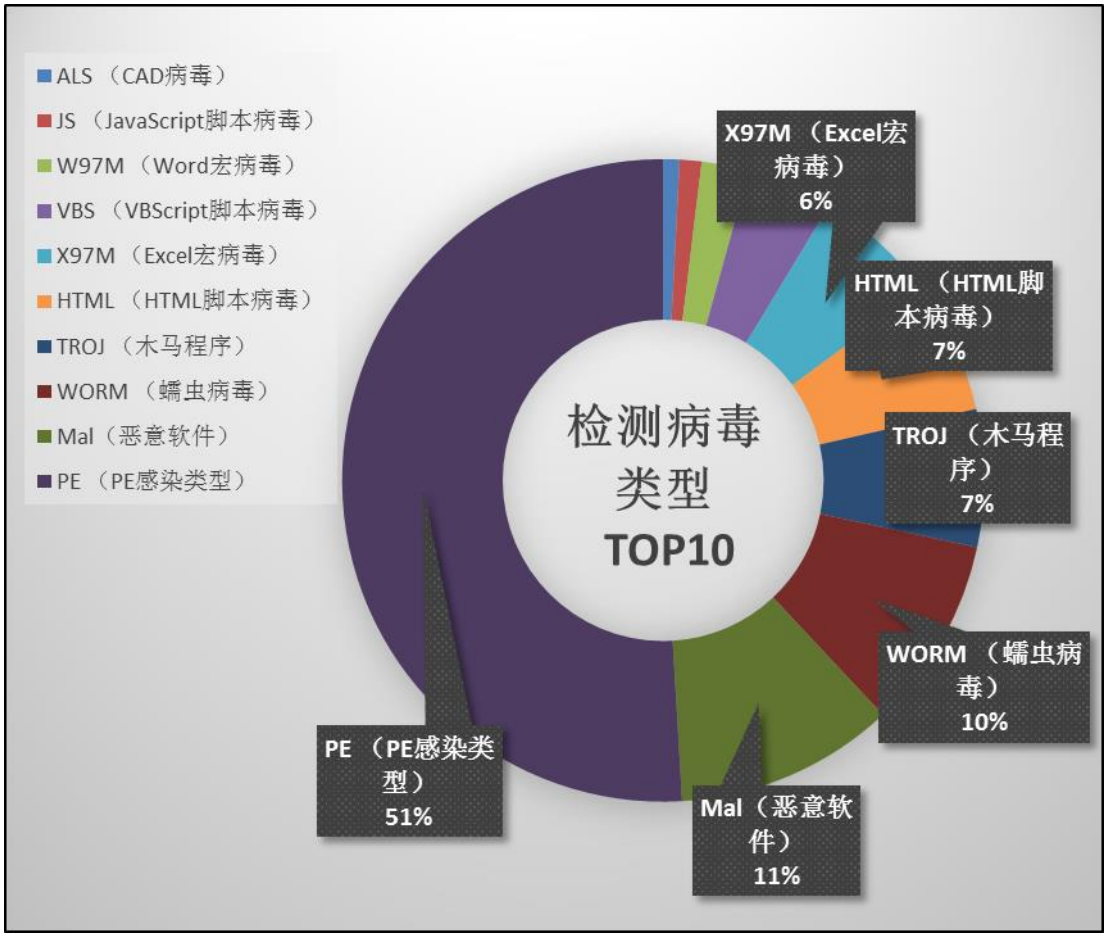


在 2014 年第 3 季度感染安卓平台的恶意程序中，数量最多的是“广告”类型，占到总数的 46%；“吸费软件”位列第二，占 40% ；而居第三位的则是“窃取数据信息”类型的恶意程序。值得注意的是一个恶意程序会同时具有以上描述的多种恶意行为。

安卓平台恶意软件持续增长，iOS 用户可能会庆幸他们的设备不会像安卓用户那样暴露在恶意程序面前，但这并不意味着 iOS 就是坚不可摧的系统。除开恶意程序，其它类型的威胁同样也会侵害到用户。例如本季度 9 月份发生的 **iCloud 好莱坞影星艳照泄露事件**，数位明星的隐私信息遭到泄露，此事件引起不小恐慌。经过调查，苹果公司的官方报告最终将此事件的源头定性为是一起“钓鱼攻击”。研究发现，某些针对移动设备的钓鱼网站可能会利用设备上默认浏览器的特定缺陷来非获取受害者的敏感数据。虽然整个过程并不会感染恶意软件，但同样可以成功攻破用户设备从而给受害者带来了损失。

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 季度各类型病毒检测情况分析



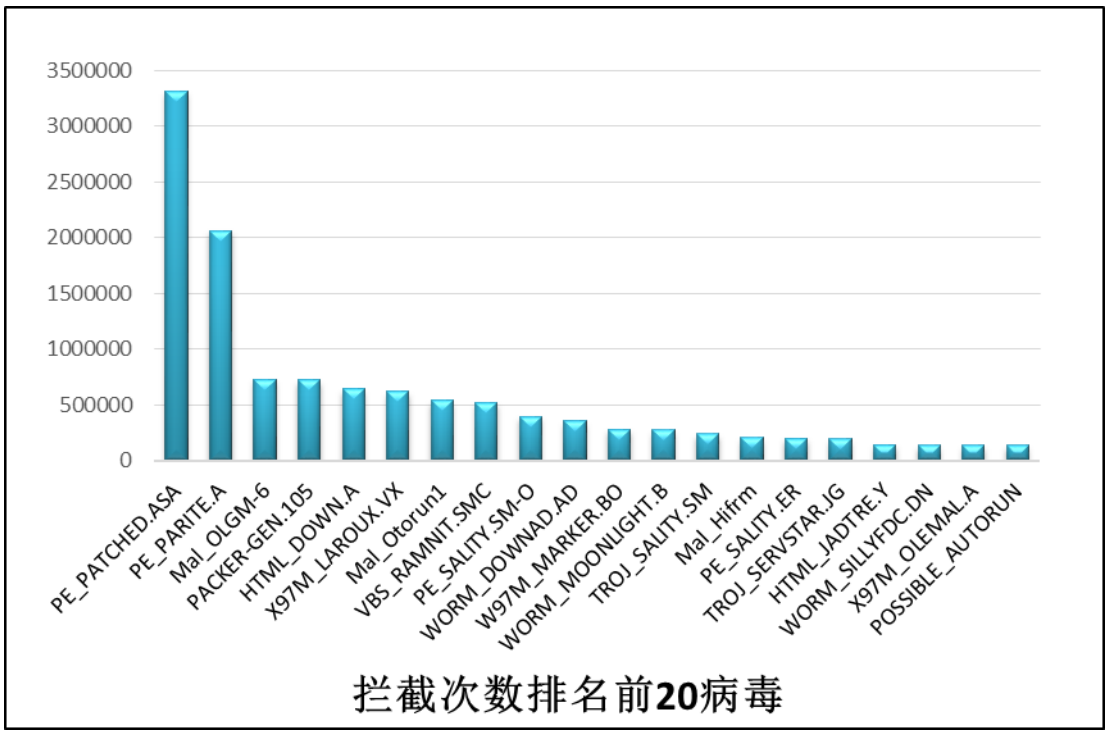
2014 年第 3 季度检测到的病毒种类中，PE 类型病毒感染数量在所有类型中所占比重最大，占到总检测数量的 51%。与前几季度监控的情况相似，PE 病毒 PE_PATCHED.ASA 依然是检测数量最多的病毒。该病毒文件是一个被修改过的系统文件 sfc_os.dll，这个文件用以保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能。

本季度蠕虫病毒占检测类型总数的 10%。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。

在第 3 季度中，WORM_DOWNAD.AD 和 WORM_MOONLIGHT 家族病毒监控到的数量较多。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。另外 WORM_DOWNAD.AD 还可以通过利用微软漏洞进行传播。

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 季度病毒拦截情况分析



在 2014 年第 3 季度拦截次数排名前 20 位的病毒检测名中，PE 病毒的感染数量远高于其它类型病毒。由于 PE 病毒有大量感染可执行文件的行为，刚然速度迅速，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 331 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 **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：

传播渠道：

通过网页传播。当用户访问被病毒植入的网站时，恶意文件会自动执行。

然后，植入文件将被执行。最终已植入文件的恶意行为将在受感染的系统中被执行。

文件类型：

.VBS

恶意行为：

释放以下文件：

%User Temp%\svchost.exe ——恶意文件已经可以检测为 PE_RAMNIT.H-O

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

恶意文件被释放后，它会运行该文件。然后释放的恶意文件将执行自身的恶意行为。

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 的文件和释放的其它恶意文件 PE_RAMNIT.H-O 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

2014 年第 3 季度热门新型病毒分析

2014 年 9 月爆出的 ShellShock 破壳漏洞，继心脏出血漏洞后再次引起业界关注。在该漏洞被揭露后不久，就出现了利用该漏洞进行攻击的病毒案件。目前趋势科技已经可以对该病毒进行检测，检测名为 PERL_SHELLBOT.WZ。

PERL_SHELLBOT.WZ 恶意行为示意图

病毒的详细信息如下：

病毒检测名：
PERL_SHELLBOT.WZ

传播渠道：
由其它恶意软件释放或当用户浏览恶意网站时下载而抵达系统。

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。

病毒行为：

后门行为

1. 该病毒会连接以下 IRC(Internet Relay Chat)服务器：

{BLOCKED}i.bot.nu:5190

2. 加入以下 IRC 频道：

#nrpe

3. 当病毒接收到以下远程恶意控制端用户发送的指令后就会接入 IRC 服务器：

Join – 加入频道

part – 离开频道

rejoin – 离开并重加入频道

op – 授予用户操作状态

deop – 撤消用户操作状态

voice – 授予用户发声状态

devoice – 撤消用户发声状态

nick – 更改昵称

msg – 发送短消息

quit – 断开与 IRC 服务器的连接

raw – 发送原始数据到 IRC 服务器

die – 自行终止

udp1, udp2, udp3 – 执行 UDP 泛洪

tcp – 执行 TCP 泛洪

http – 执行 HTTP 泛洪

ctcpflood – 发送 20 条 IRC 私人消息到目标主机

msgflood – 发送一条长 IRC 消息到目标主机

noticeflood – 发送两条长 IRC 消息通知到目标主机

cback – 执行远程 SHELL (/bin/sh 或 cmd.exe)

download – 从 URL 下载并保存为特定文件

portscan – 扫描一个 IP 地址的以下端口: 1, 7, 9, 14, 20, 21, 22, 23, 25, 53, 80, 88, 110, 112, 113, 137, 143, 145, 222, 333, 405, 443, 444, 445, 512, 587, 616, 666, 993, 995, 1024, 1025, 1080, 1144, 1156, 1222, 1230, 1337, 1348, 1628, 1641, 1720, 1723, 1763, 1983, 1984, 1985, 1987, 1988, 1990, 1994, 2005, 2020, 2121, 2200, 2222, 2223, 2345, 2360, 2500, 2727, 3130, 3128, 3137, 3129, 3303, 3306, 3333, 3389, 4000, 4001, 4471, 4877, 5252, 5522, 5553, 5554, 5642, 5777, 5800, 5801, 5900, 5901, 6062, 6550, 6522, 6600, 6622, 6662, 6665, 6666, 6667, 6969, 7000, 7979, 8008, 8080, 8081, 8082, 8181, 8246, 8443, 8520, 8787, 8855, 8880, 8989, 9855, 9865, 9997, 9999, 10000, 10001, 10010, 10222, 11170, 11306, 11444, 12241, 12312, 14534, 14568, 15951, 17272, 19635, 19906, 19900, 20000, 21412, 21443, 21205, 22022, 30999, 31336, 31337, 32768, 33180, 35651, 36666, 37998, 41114, 41215, 44544, 45055, 45555, 45678, 51114, 51247, 51234, 55066,

55555, 65114, 65156, 65120, 65410, 65500, 65501, 65523, 65533

mail – 发送电子邮件至目标主机

port – 打开一个到指定 IP 地址和端口的连接

dns – 解析一个地址为 IP 地址

注：它会随机选择以下字符作为昵称：

abbore ably abyss acrima aerodream afkdemon ainthere alberto alexia alexndra alias alikki alphaa alterego alvin ambra amed andjela andreas anja anjing anna apeq arntz arskaz as asmodizz asssa athanas aulis aus bar bast bedem beeth bella birillo bizio blackhand blacky blietta blondenor blueangel bluebus bluey bobi bopoh borre boy bram brigitta brio brrrweg brujah caprcorn carloto catgirl cathren cemanmp chainess chaingone chck chriz cigs cintat clarissa clbiz clex cobe cocker coke colin conan condoom coop coopers corvonero countzero cracker cread crnaruka cruizer cubalibre cure custodes dan dangelo danic daniela dario darker darknz davide daw demigd des devastor diabolik dimkam dital djtt dogzzz dolfi dolphin dottmorte dracon dragon drtte dumbblnd dusica ebe edgie eggist einaimou elef elly emmi encer engerim erixon eurotrash fairsight fin fireaway fjortisch floutti fluffer flum forever fqw fra freem freew freud funny furia furunkuli fwsmou gad gamppy gerhard ghostie gili girlie giugno gizmo glidaren gold gomora gracie grave graz grron gsund gufoao hali hallas hammer harri harry hayes hazor herbiez hlios hoffi honeii hongkong hug iasv ibanez ibanz ibar igi illusins imp inkworks iplord ivan ja jaffa jaimeafk james jamezdin janet janne jason javagrl jayc jazz jejborta jester jj jn jockey joe joelbitar johannes johndow johnny joni jonni jornx joshua jossumi judy juge juha juhas julze juutsu kajman kalca kamileon kardinal kasandra katarina kaviee kbee ken keung kewin khan kikeli kikii kilroi kiwi klaara kliimax klimas kode kojv koopal kralj krash krista kronos ktx kungen kuppa kurai lala lamour latina legend lenisaway lily linda lingyee linux lisa lisha litta littleboy liverpoo liyen liz liza lonely lonelygal lonewolf lopez lordie lovebyte lph luarbiasa lucignol lullaby lunatic luny lupo mac macesgl madd mailman malkav malr mamakians mamaw manarimou manarisou maradona marakana marco marillion mark mary master maurino max mcalcota melanie melinda meph mephisto mg mhj mhz mig miina mika mikav mike mikemcgii mikko mikma mimma miss moladmin monikaw monkeyboy monroe monstop mooks mordeshur mpdike mrbate mrbeauty mrblom mrbx mrjee mro mrtabizy mrx mrxx msd mu muimui musashi musc musce musicgal muti myboy mystr mythic mywife nallllle nanask natalie natborta ncubus neutrino niceguy nico niklas nimfa nino nurul obiwanbip ogre olivia omega only orac orace oranzzzzz organza ourlove outworld outzake oxygn paliadog pazarac permaloso perroz pessaar phre phreaky pihkal pinball poesje poison poofie popy powerpc pper primera primetime proxyma pshyche psioncore psiximou psixisou psychosis psyidle pszaah puppetm pzzzz quattro question ra ragio ragnetto raiden raindance raistln ranu raska raul raye reartu red reflect ribica richard rick rigo rikuta rikuxr rita rix rob roku ronaldo ronwrl roticanai rugiada ruthless saalut sammi sand satanins schzsh scorpin sealink sean secret serpentor servant sethi sexbolek sexyman sharmm shearer shekel shio shortys shred sidewalk sil siren skar skill skru sky skygun skylink slaktarn slash slgon smarties smck snake snike snoopgirl sodoma sopocani sorceress spacebbl spacedump spanker spermboy spirtouli srk stazzz steve stinga stj stjf studenica stussy suez suhoj sukun sunsola surfer sutera svearike sweetii sweetlady sweklopi swepilot switch syncphos szern takumura tallaxlc tampone tarabas tatano tato tennis tenx terence terkukur tero thefox thesint timer timewalk tmhd tnxfck to tomihki tommy topo triumph trustme tungau tupac turbozzzz turing tvrdjava tysn unicron uoff uptimer utopia vader vaismi vajje vanda varjo vass vento venusguy vertie viagara vicious vidxxx virex vodafone vone vrgnie vuubeibe wanderer warrr wasabboy weebee wellu wendy whiskey willgood wing winny wknight wlly wolfman wow wp xarasou xtreme xxx xzone yakzr yang yashy yasin yenyen ykbug yogiebear zai zfstr zinj zizu zvezda zwimou zwisou zwsiew zwsiewale

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:

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。

32 位 Windows 操作系统请使用：

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

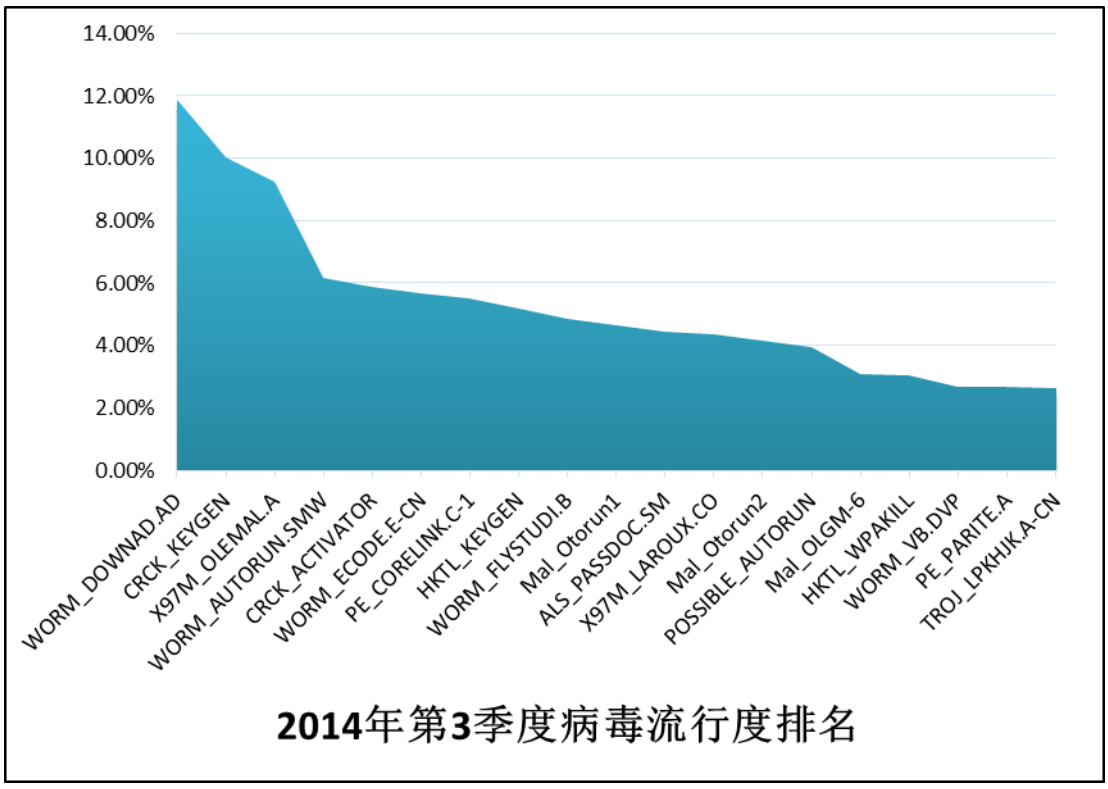
64 位 Windows 操作系统请使用：

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

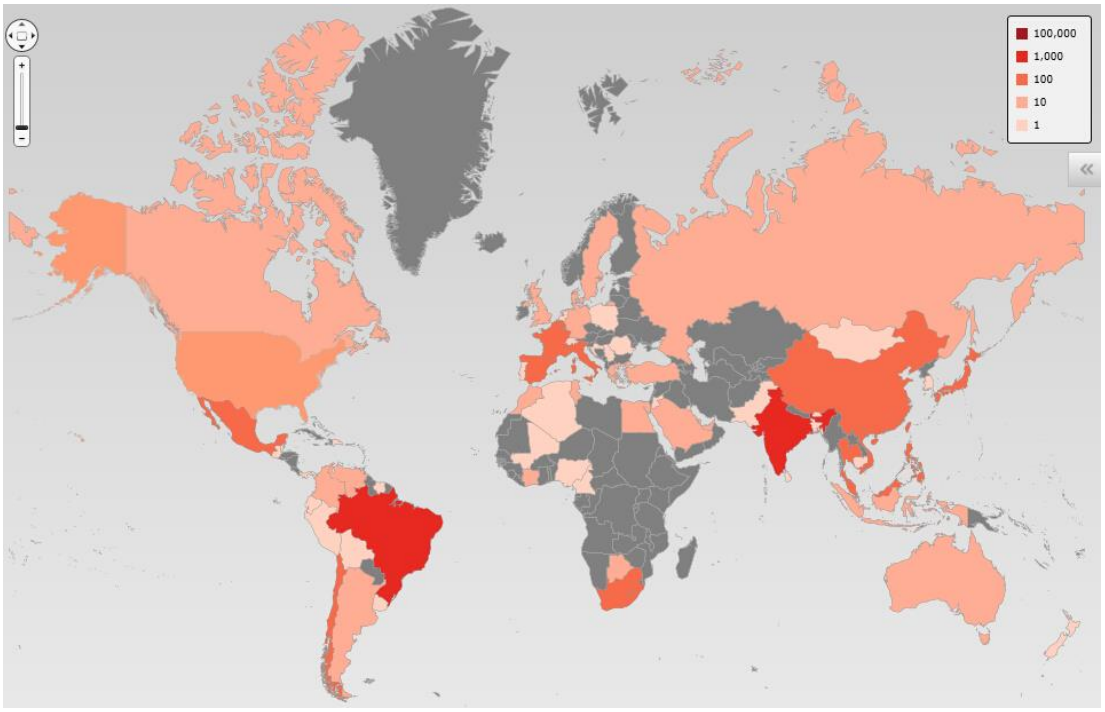
相关链接信息：

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PERL_SHELLBOT.WZ

2014 年第 3 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 3 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 3 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。

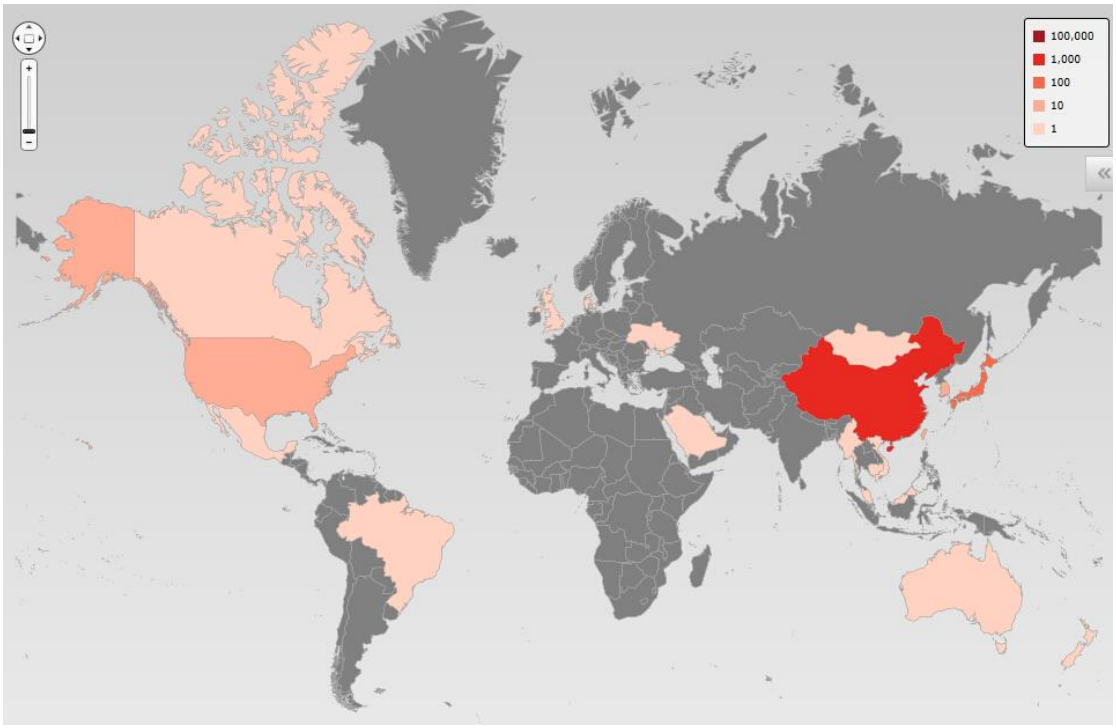
在这里仍然需要提醒用户，WORM_DOWNAD 持续流行的原因有几点：

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 3 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 3 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

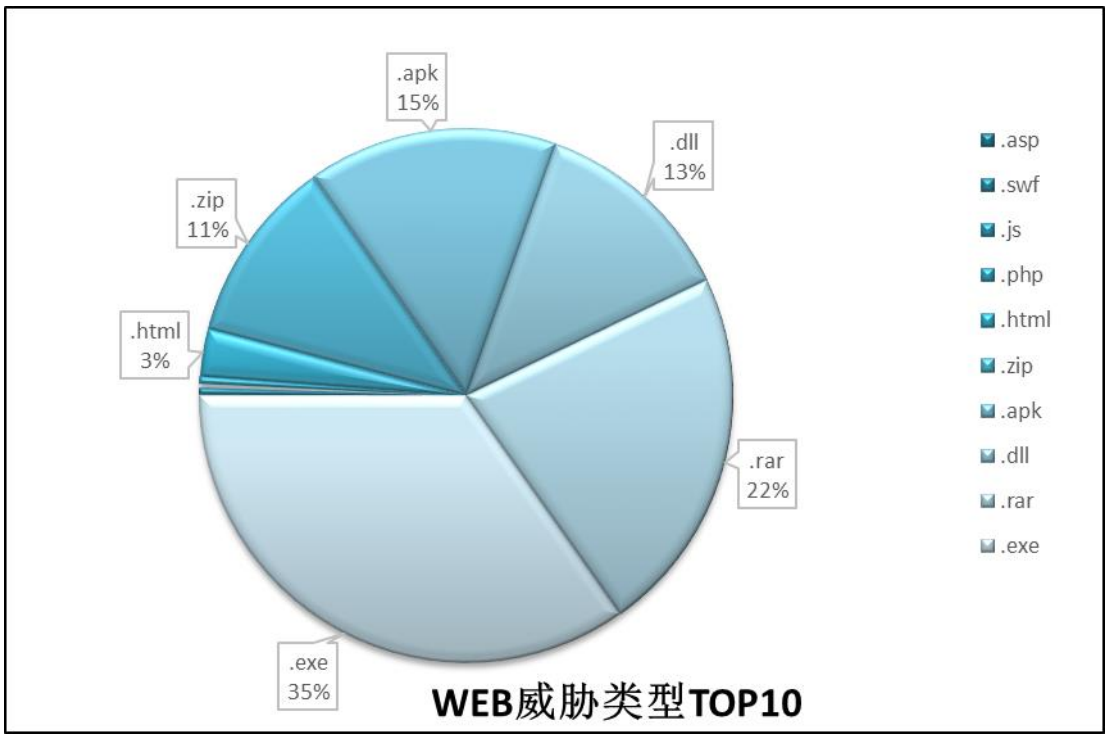
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2014 年第 3 季度 WEB 安全威胁情况

2014 年第 3 季度 WEB 威胁文件类型分析

在 2014 年第 3 季度的数据中，通过 WEB 传播的恶意程序中，约有 35%是.EXE 文件，所占比例延续上一季度保持第一位。.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.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。此外，.APK 文件格式所占比例也大幅上升，占到 15%。



2014 年第 3 季度中国地区 WEB 威胁文件类型分布图

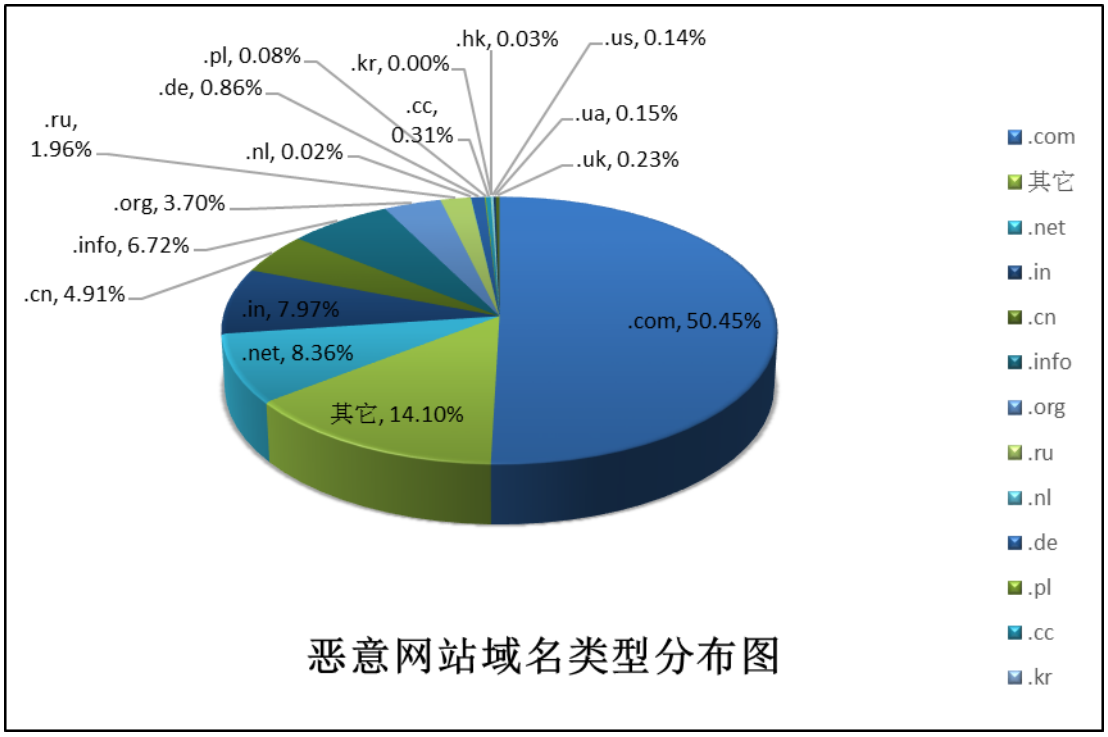
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 3 季度 TOP 10 恶意 URL

TOP10 恶意URL		
恶意URL	描述	点击量
sp-setti***t.com	网站直接或间接帮助传播恶意软件或恶意代码	75,171,534
http://traf***iz/	网站直接或间接帮助传播恶意软件或恶意代码	29,734,913
http://fis***y.com/aa/nn	网站直接或间接帮助传播恶意软件或恶意代码	14,046,256
http://lob***t.com/aa/nn	网站直接或间接帮助传播恶意软件或恶意代码	14,010,130
http://88.***.9/aa/nn	承载恶意负载的域	13,988,163
http://ads.al***l.com/cgi-bin/advert/getkws.cgi?did=11759&version=0&key=azJJ.s8MVPsHc	网站直接或间接帮助传播恶意软件或恶意代码	12,761,446
http://opt***b.info/get/	网站直接或间接帮助传播恶意软件或恶意代码	9,037,892
http://api.luc***p.net/rs	此链接为恶意程序的命令与控制(C&C)服务器。	8,421,085
http://de***er.com/Y2x8MS42fGM4ZWYwNTZiOGM2YWE4MjNhM2I1ZGYxODc5OTdiNzY0fDMxNQ==	网站直接或间接帮助传播恶意软件或恶意代码	8,117,329
http://api.use***nk.com/rs	网站直接或间接帮助传播恶意软件或恶意代码	7,529,791

2014 年第 3 季度中国地区 WRS 拦截恶意 URL 排名 TOP10

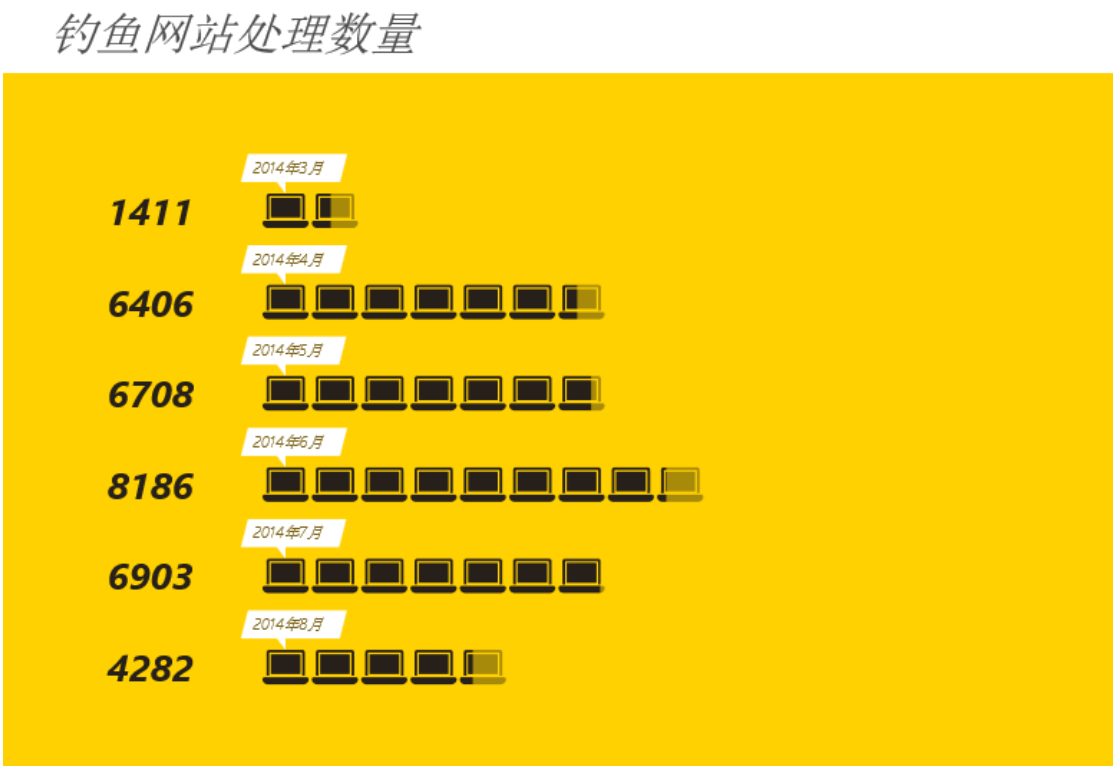
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。



2014 年第 3 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 66.78%。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 3 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

从中国反钓鱼联盟得到的数据，2014 年 3 月至 2014 年 8 月共计 6 个月中，处理钓鱼网站共计 **33,896** 个。从展示图可以看到，2014 年第 3 季度前 2 个月的钓鱼网站发现数量比上一季度略有减少。

据统计，中国地区使用.COM、.TK、.PW 和.NET 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的 50%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。本季度中，.CC、.XYZ 等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、银行和电视媒体的钓鱼网站总量占所有举报数量的 95%以上。其中又以仿冒电子商务网站的钓鱼网站数量最多，占到总数的 8 成以上。网购给生活带来便利的同时，消费者也应该对网络安全加大重视。

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 3 季度漏洞攻击威胁情况

TOP10 漏洞	
漏洞名称	**检测数量**
CVE-2008-4250	3,508,460
MS08-067	64,100
CVE-2010-0806	28,500
CVE-2010-2568	10,500
CVE-2014-0322	2,300
CVE-2012-0002	1,200
CVE-2012-0152	600
CVE-2013-0422	489
CVE-2013-1347	309
CVE-2013-1493	329

2014 第 3 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-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
CVE-2014-0322	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0322
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
CVE-2013-0422	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-0422
CVE-2013-1347	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1347
CVE-2013-1493	http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1493

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。

趋势科技对 Shellshock Bash 漏洞的解决方案说明

2014 年第 3 季度中，美国计算机应急筹备小组（US-CERT）公布了一个名为“Shellshock”的严重 Bash 安全漏洞，并将该漏洞的严重程度被评为 10 级，而且利用难度被评为“低”级，这就是说会有更多的黑客利用它造成更严重的安全危机。影响范围遍及全球大约 5 亿台服务器和其他联网设备，包括手机、路由器、医疗设备等。

为此，趋势科技提供免费解决方案防范 Bash 风险，发布了一套免费的扫描和服务器保护工具，对于 Web 用户，Mac OS X 和 Linux 平台，提供系统安全防护。趋势科技也提醒，漏洞修复工作将会给用户带来很多挑战，因为用户需要为每一个 Linux 版本打补丁。基于这种情况，希望迅速获得解决，存在一些困难。另外，很多路由器、VoIP 和医疗设备都运行着 Linux 系统，而这类产品的漏洞更难以修复。

由于 Shellshock Bash 漏洞的影响范围太广，将会影响以下人群：

- 一般使用者
- IT 系统管理员
- 网站管理员
- 托管服务的客户

Shellshock Bash 漏洞影响哪些系统？

- Linux
- Unix
- Mac OS X

鉴于该问题的紧急性，趋势科技则建议用户尽快采取以下行动：

- ✓ 寻求 Linux 厂商技术支持。
- ✓ 升级 Bash 至最新版本，或改用其他 Linux Shell，然后卸载 Bash。
- ✓ 在有漏洞的系统前部署 IPS 设备，并阻止该漏洞。
- ✓ 如果您使用了托管服务，请尽快联络您的托管服务商。
- ✓ 如果您公司已购买趋势科技的未知威胁发现设备（TDA），请将 Pattern 升级到最新版本，可检查到 Shellshock 漏洞攻击，随后利用防火墙等安全设备，阻挡攻击源。
- ✓ 如果您公司已购买趋势科技的服务器深度安全防护系统（Deep Security），请将 DPI Pattern 升级到 DSRU14-028 或更新版本，可检查和阻挡 Shellshock 漏洞攻击。

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。

- ✓ 如果您公司已购买趋势科技的应用安全网关（Deep Edge），请将 Pattern 升级到最新版本，可检查和阻挡 Shellshock 漏洞攻击。
- ✓ 对于个人消费者，可以通过安装趋势科技 PC-cillin 2014 云安全版为 Mac OSX 进行安全防护。

  试用下载：http://www.trendmicro.com.cn/pccillin/index.html
- ✓ 趋势科技特别发布漏洞进攻+TDA 发现的演示：

  http://v.qq.com/page/n/p/2/n0138uq97p2.html
- ✓ 趋势科技专门准备了 Shellshock Bash 漏洞保护服务站点，供用户实时掌控该风险详情：http://www.trendmicro.com.cn/cn/security/shellshock-bash-bug-exploit/

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 季度最新安全威胁信息

2014 年第 3 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。

❖ 警惕！iPhone 6 即将上市 诈骗邮件已现身网络

随着 iPhone 6 即将上市，各路小道消息已经开始满天飞。就在近几日，一些记者还收到了假的 iPhone 6 将要上市的通知邮件。趋势科技也收到了几封。

iPhone6 马上就要上市了，我们可能会看到更多以 iPhone6 为诱饵的攻击。当产品与热门话题结合时，用户的防御性会变得更加薄弱，更容易成为攻击目标。

趋势科技已经封锁这起攻击所用的垃圾邮件，也封锁了对所有相关恶意网站的存取。我们也建议用户通过 PC-cillin 2014 云安全软件协助过滤，封锁相关的钓鱼邮件及可疑的恶意网址，以保上网安全，避免遭受损失。。

http://blog.sina.com.cn/s/blog_5e96245b0102uzzt.html

❖ 公共无线网有风险，小心黑客“偷袭”!

由于电子前沿基金会发起了开发开源路由器（也叫公共无线路由器）的项目，撒玛利亚人希望安装廉价 Wi-Fi 路由器来创造一个公共的宽带，减少购买数据流量包的套餐。这一项目导致公共无线网络和公共 Wi-Fi 热点的话题又再次引起人们的关注。

提供公共无线网络的好处有两点。第一，可以提供免费的无线网络给有需要的人；第二，当每个人都无需验证身份而登陆公共无线网络之后，基于 IP 地址的监视和追踪行为也不复存在。

http://blog.sina.com.cn/s/blog_5e96245b0102v0jn.html

❖ 勒索软件新变种：不给赎金永久加密被绑文档！

近期，趋势科技在打击网络犯罪方面取得了很大胜利，例如最近中断 GAMEOVER ZeuS 网络僵尸病毒，但类似的网络犯罪活动还是时有发生。近日，趋势科技发现了新的勒索软件，它是通过使用新的加密和回避方法的勒索软件 Ransomware 变种。

不像其它勒索软件 Ransomware 变种，Cryptoblocker 不会产生任何文本文件来指示受害者如何解密档案。它会显示如下对话框，输入交易 ID 到文字框内会产生一个反馈信息：“交易已被发送，很快就会得到验证。

http://blog.sina.com.cn/s/blog_5e96245b0102v1l1.html

❖ Windows 9 开发者预览版可下载？ 小心是钓鱼网站！

近日，趋势科技发现了一个恶意网站发布“今年 9 月将推出 Windows 9 开发者预览版”的诈骗信息，同时网络诈骗分子搭配热门搜索引擎进行关键词操作，诱骗用户下载广告程序。

此外，趋势科技还发现另外一个博客通过一个文件代管服务链接提供 Windows 9 的免费下载。该威胁被侦测为 ADW_INSTALLREX.GA 广告程序。

http://blog.sina.com.cn/s/blog_5e96245b0102v27u.html

❖ Android 再曝重大漏洞！请及时更新你的系统

近期，Bluebox Labs 的安全研究人员发现被称为“FakeID”的漏洞可以让恶意程序冒充合法程序。因为该漏洞导致从版本 2.1 到 4.4 的所有 Android 设备都会受到此漏洞的影响，故广受关注。

为了确保用户安全，趋势科技会继续侦测可能会利用此漏洞所带来的威胁和攻击。建议用户当设备系统程序提示更新时，要及时升级，以减少此类威胁的发生。

http://blog.sina.com.cn/s/blog_5e96245b0102v2rg.html

❖ Google Dorking 攻击：每个网站管理员都应警惕

美国国土安全部发出警告：网站管理员应警惕利用谷歌机器人（Googlebot）获取网站机密信息来进行攻击的行为（Google Dorking）。

谷歌会使用一个访问站点的程序进行搜索：谷歌网络爬虫，即称为谷歌机器人。当谷歌机器人检索网络并发现“秘密”的数据时，就会将它们添加到谷歌的数据库，处理方式和普通信息毫无差别。一旦这些信息可以公开访问到，后果可想而知。

http://blog.trendmicro.com/trendlabs-security-intelligence/google-dorking-waking-up-web-admins-everywhere/

❖ 网络罪犯利用 MH17 坠机新闻散播恶意链接

继失踪的马来西亚航空公司 370 航班的几个月后，又传出涉及马航 777（也称为 MH17）在乌克兰坠机的不幸消息，近 300 名乘客和机组人员遇难再次震惊世界。与过去事件相同，网络罪犯们迅速利用该新闻进行恶意活动。

根据我们的调查，在马来西亚航空公司微博于 7 月 17 日 23:36 发布消息后的短短几个小时。网络上就出现了一些可疑微博消息“马来西亚航空公司从阿姆斯特丹失去 MH17 的联系。最后一个已知的位置是在乌克兰的领空。更多详情后请点击——” 。这些微博后的链接经分析都是恶意的。

http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-hitchhike-on-the-news-of-mh17-crash/

❖ iCloud 泄露事件被黑客用于社会工程学攻击

整个互联网对 iCloud 泄漏事件唏嘘不已——超过一百个名人的私人照片遭到泄露并被公开在网络上。对于此类事件，一些网络罪犯一定会利用它们进行社会工程学攻击。此次事件的目标就是那些正在网上寻找着泄露照片的访问者们。

譬如我们发现的这个威胁：来自于推特，打有泄露名单明星詹妮弗·劳伦斯的标签。表面是一个短链接，如果点击，就会将用户重定向到其它网站上。

http://blog.trendmicro.com/trendlabs-security-intelligence/icloud-hacking-leak-now-being-used-as-social-engineering-lure/

❖ 小心垃圾邮件：已故影星罗宾威廉姆斯去世消息被黑客利用

罗宾·威廉姆斯(Robin Williams)在 8 月 12 日的去世消息震惊全世界，在网络上迅速传开，在成为了网民间热门话题的同时，也引来了垃圾邮件发送者和网络犯罪分子。

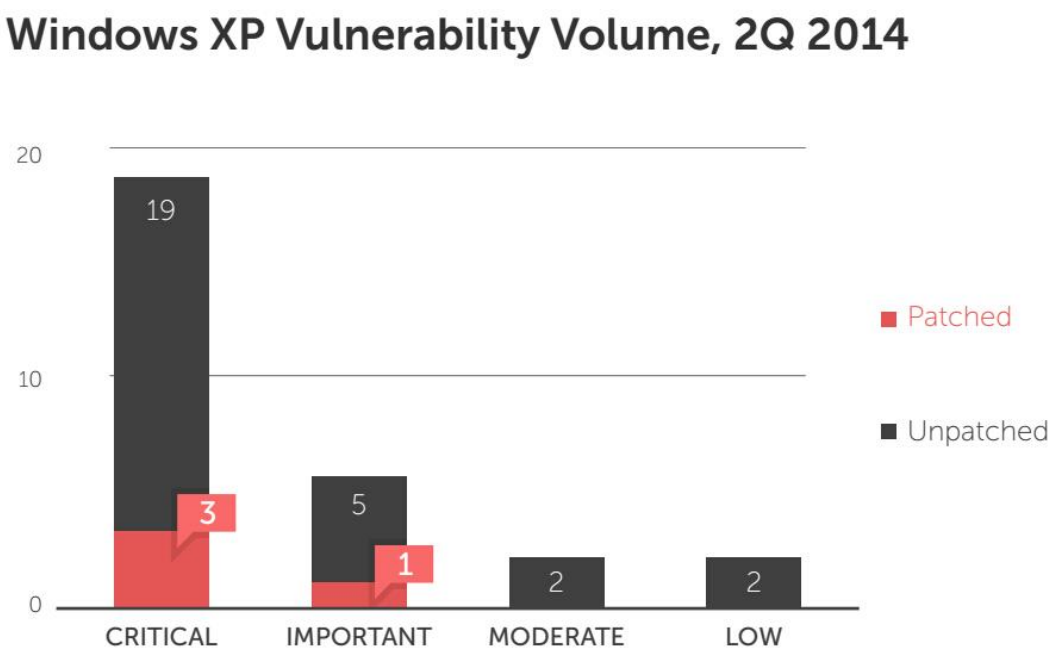
当罗宾·威廉姆斯(Robin Williams)的过世消息一传出，趋势科技就拦截到有垃圾邮件的主题提到他的名字。垃圾邮件内容是用西班牙文，并提示收件者下载关于罗宾·威廉姆斯(Robin Williams)过世“令人震惊”的影片，一旦点开链接就会下载蠕虫 WORM_GAMARUE.WSTQ。

http://blog.sina.com.cn/s/blog_5e96245b0102v12o.html

趋势科技全球区最新安全威胁概要

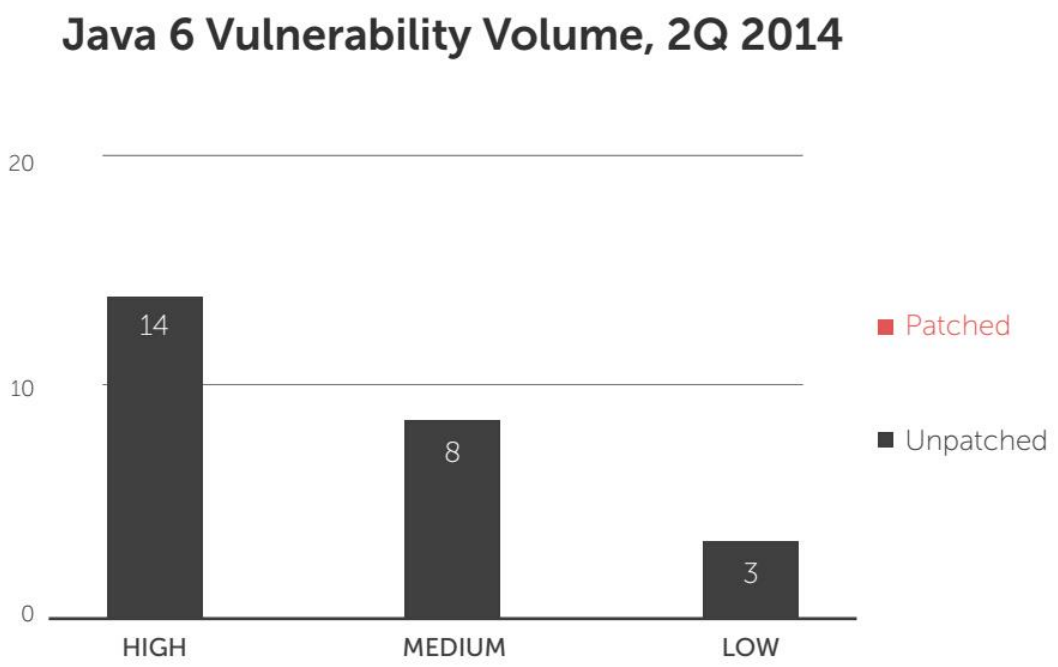
以下是来自 2014 年第 2 季度趋势科技全球区安全报告的数据。

2014 年第 2 季度公布的漏洞涉及互联网浏览和 Web 服务等不同方面：从服务端库到计算机系统再到移动设备应用和浏览器，均发现了危害程度不同的漏洞。以下是 WindowsXP 平台在第 2 季度发现的漏洞数量。



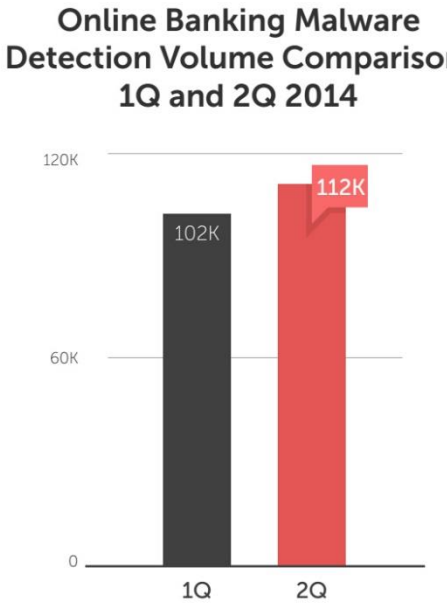
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

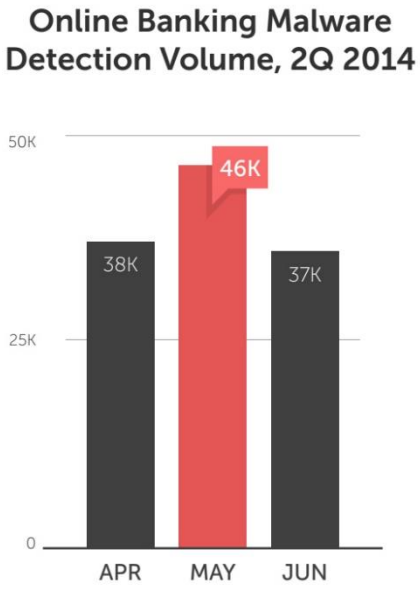
以下是 Java 6 在第 2 季度发现的漏洞数量。



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。

在第2 季度中，针对网银用户的恶意软件检测数比上一季度有所上升。这与在日本发现的VAWTRAK 家族病毒爆发有关。

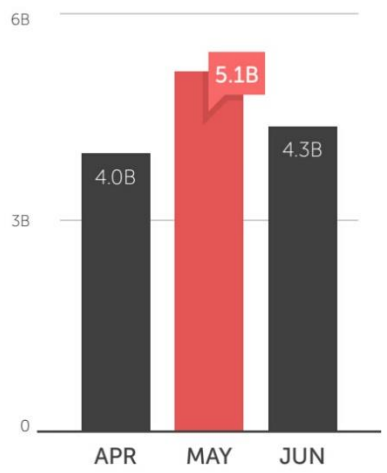




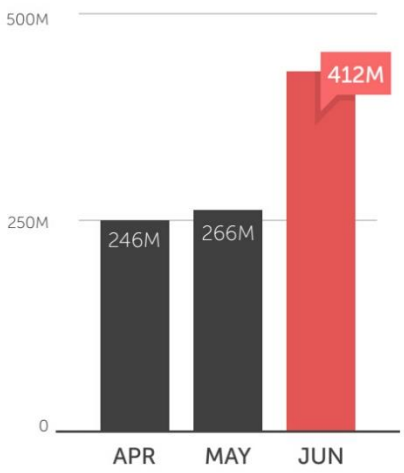
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

第 2 季度我们拦截到的垃圾邮件发送 IP 地址数量和上一季度相比没有明显的上升和下降。而在第 2 季度的 6 月份，拦截恶意网站的数量大幅增加，其中大部分和广告软件有关。

Number of Spam-Sending IP Addresses the Trend Micro Smart Protection Network Blocked Access To, 2Q 2014

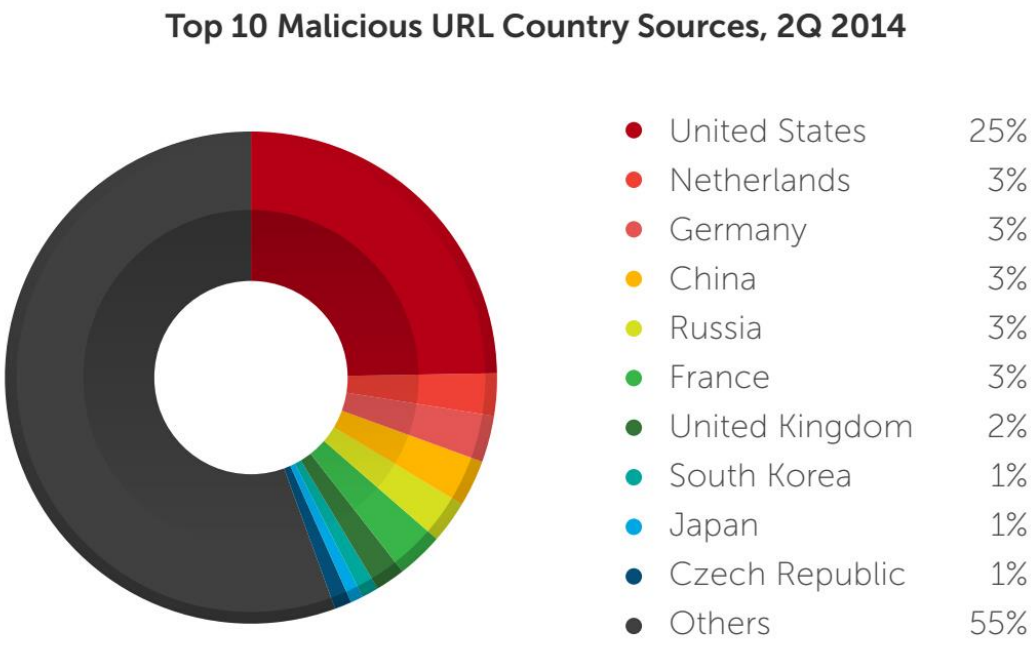


Number of Malicious Sites the Trend Micro Smart Protection Network Blocked Access To, 2Q 2014



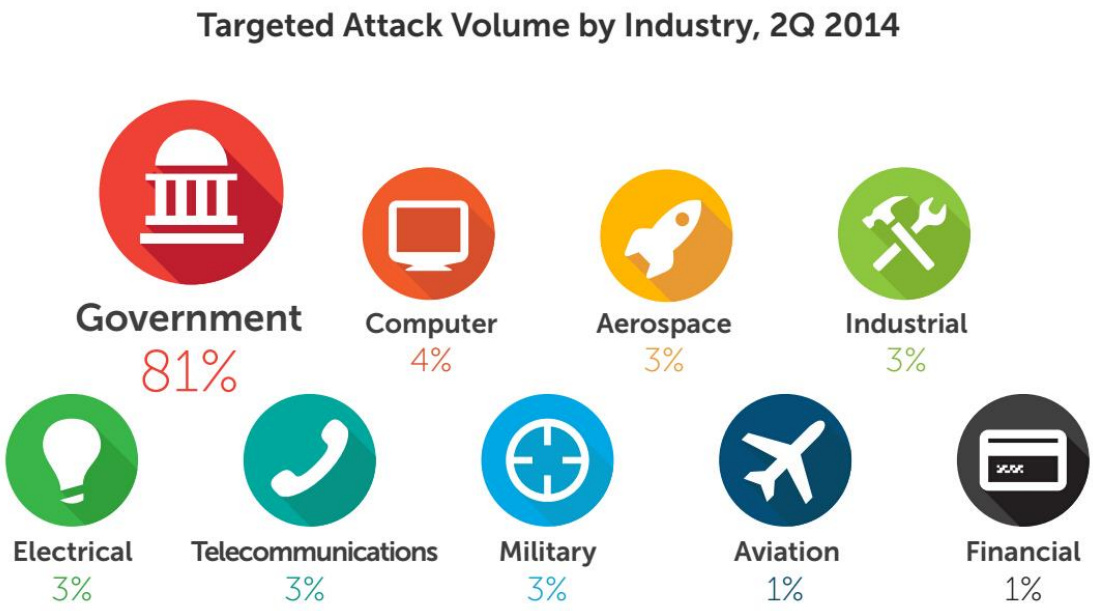
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2014 年第 2 季度统计到的恶意链接来源地，美国占到了四分之一，比上一季度的 22%增加了 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。

在第2 季度中，全球范围内的针对性攻击的目标行业依然以政府机构最多。



需要查看更完整的 2014 年第 2 季度全球安全报告请访问：
http://about-threats.trendmicro.com/us/security-roundup/2014/2Q/turning-the-tables-on-cyber-attacks/

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