AsiaInfo 亚信安全

中国地区 2015 年
第三季度
网络安全威胁报告

2015/10

CHINA RTL

目录

2015 年第 3 季度安全威胁

本季安全警示：

移动设备安全、勒索软件

2015 年第 3 季度安全威胁概况

- 本季度亚信安全中国区病毒码新增特征约 **19** 万条。截止 2015.9.30 日中国区传统病毒码 **11.946.60** 包含病毒特征数约 **405** 万条。

- 本季度亚信安全在中国地区客户终端检测并拦截恶意程序约 **14,183** 万次。

- 本季度亚信安全在中国地区拦截的恶意 URL 地址共计 **27,718,531** 次。

移动设备安全本季度再次成为热点话题。iOS 应用商城因其完整的验证机制一直被认为是值得放心的下载源，然而 2015 年 9 月爆出的 XcodeGhost 事件打破了其壁垒：iOS 应用商城中的数款合法应用被嵌入了恶意代码，且已被大量下载到用户终端上。

在进一步的研究中，其背后原因逐渐浮出水面。Xcode 是苹果公司提供给开发者在不同平台上运行的开发工具，由于其文件大小有几个 G 而中国地区连接苹果服务器的速度又太慢。因此，中国 iOS 应用开发者们多选择从非官方处下载 Xcode——网友将文件转存到当地的文件分享网站上并将下载地址共享在各大论坛上。如下图：

包含有 Xcode 副本下载链接的论坛帖子

本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

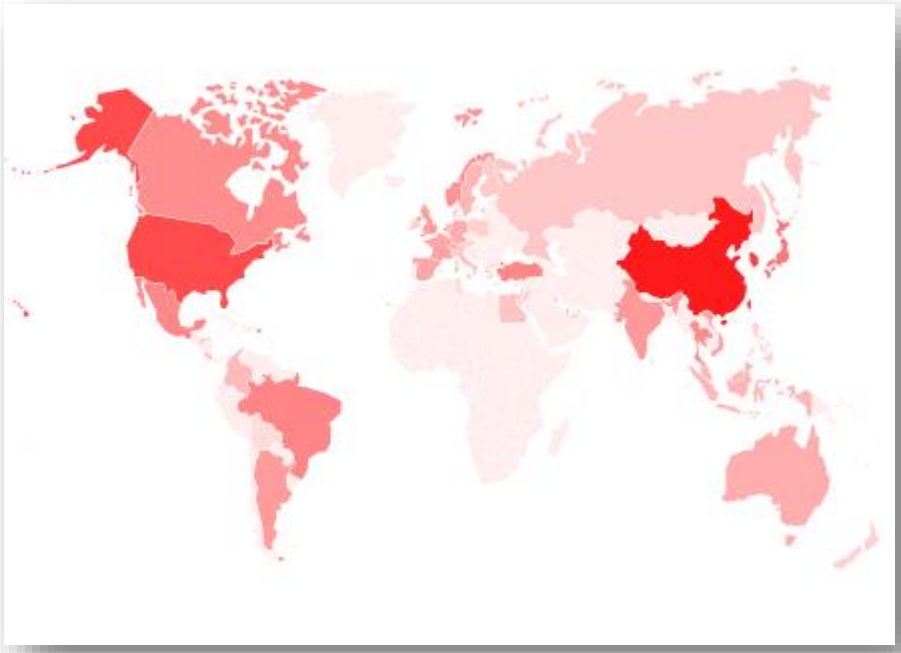
不幸的是，其中某些副本被人为加入了一个新的带有恶意代码的 CoreService 开发框架，以取代原始代码。其结果是，所有在被篡改过的开发环境下生成的应用都会包含恶意代码。

以下列出一些包含 XcodeGhost 代码的应用。由于被篡改版本 Xcode 的广泛使用，其受到影响的应用并不局限于表中列出的这些。

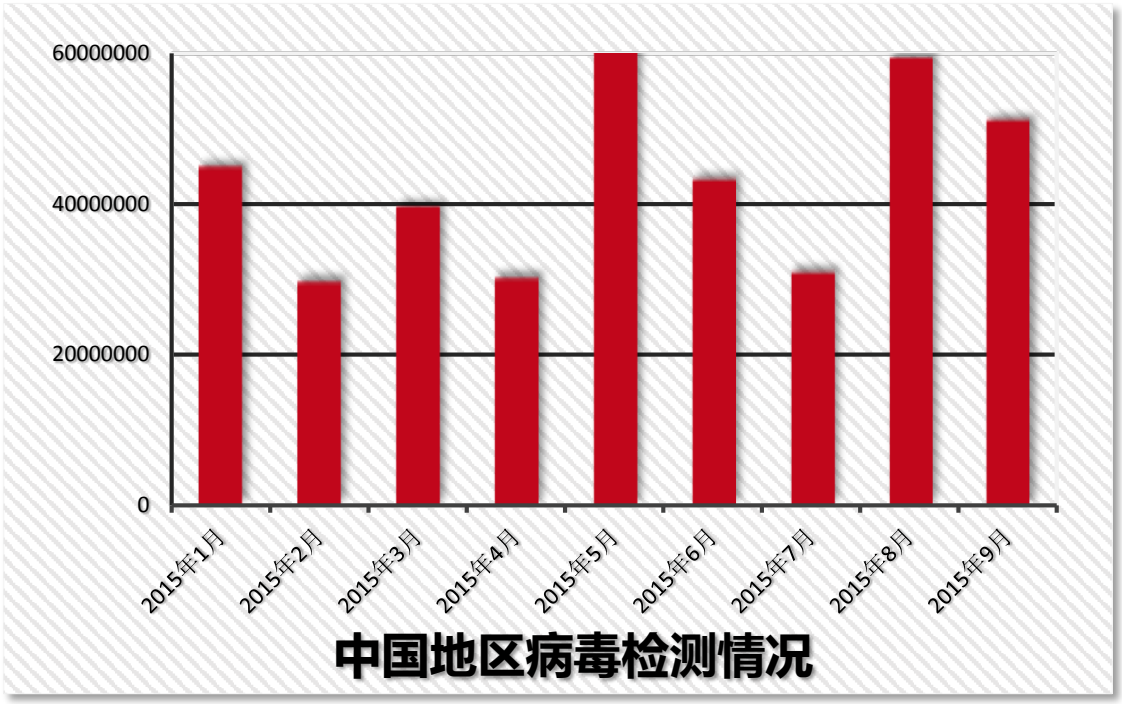
应用标识符	版本	应用名称
com.51zhangdan.cardbox	5.0.1	51 卡保险箱
com.cloud1911.mslict	1.0.44	LifeSmart
cn.com.10jqka.StocksOpenClass	3.10.01	炒股公开课
com.xiaojukeji.didi	3.9.7	嘀嘀打车
com.xiaojukeji.didi	4.0.0	滴滴出行
com.xiaojukeji.dididache	2.9.3	滴滴司机
com.dayup11.LaiDianGuiShuDiFree	3.6.5	电话归属地助手
sniper.ChildSong	1.6	儿歌动画大全
com.rovio.scn.baba	2.1.1	愤怒的小鸟 2
com.appjourney.fuqi	2.0.1	夫妻床头话
com.autonavi.amap	7.3.8	高德地图
com.stockradar.radar1	5.6	股票雷达
cn.com.10jqka.TheStockMarketHotSpots	2.40.01	股市热点
com.jianshu.Hugo	2.9.1	Hugo
com.wdj.eyepetizer	1.8.0	Eyepetizer
com.iflytek.recinbox	1.0.1083	录音宝
com.maramara.app	1.1.0	马拉马拉
com.intsig.camcard.lite	6.5.1	CamCard
com.octInn.br	6.6.0	BirthdayReminder
com.chinaunicom.mobilebusiness	3.2	手机营业厅
cn.12306.rails12306	2.1	铁路 12306
cn.com.10jqka.IHexin	9.53.01	同花顺
cn.com.10jqka.IphoneIJiJin	4.20.01	同花顺爱基金
cn.com.gypsii.GyPSii.ITC	7.7.2	图钉
com.netease.videoHD	10019	网易公开课
com.netease.cloudmusic	2.8.3	网易云音乐
com.tencent.xin	6.2.5	微信
com.tencent.mt2	1.10.5	我叫 MT 2
com.gemd.iting	4.3.8	喜马拉雅 FM
com.xiachufang.recipe	48	下厨房
cn.com.10jqka.ThreeBoard	1.01.01	新三板
com.simiao-internet.yaodongli	1.12.0	药给力
com.gaeagame.cn.fff	1.1.0	自由之战

受感染应用列表

根据亚信安全的监控数据，我们发现中国是此次事件受影响最严重的地区。然而影响并不局限于此，北美地区也遭 XcodeGhost 严重打击。其原因是部分受感染的应用服务在中国以外地区同样也可以使用。目前该恶意代码的检测名为 IOS_XcodeGhost.A。



XcodeGhost 受感染的国家分布图

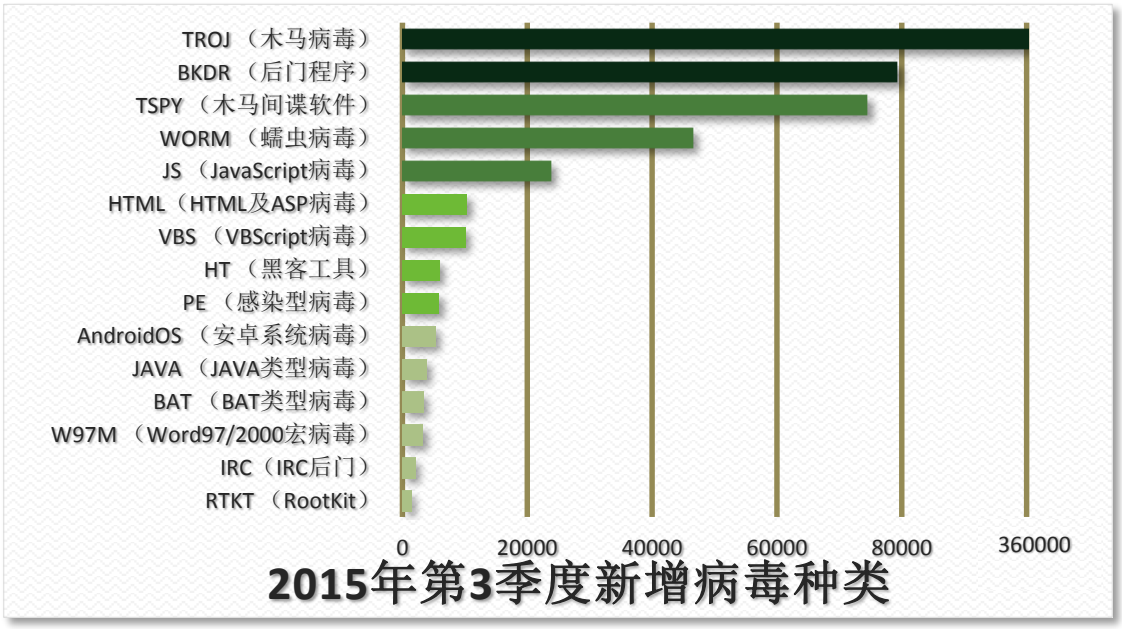


2015 年第 3 季度中国地区病毒检测数量图

本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

2015 年第 3 季度病毒威胁情况

2015 年第 3 季度新增病毒类型分析



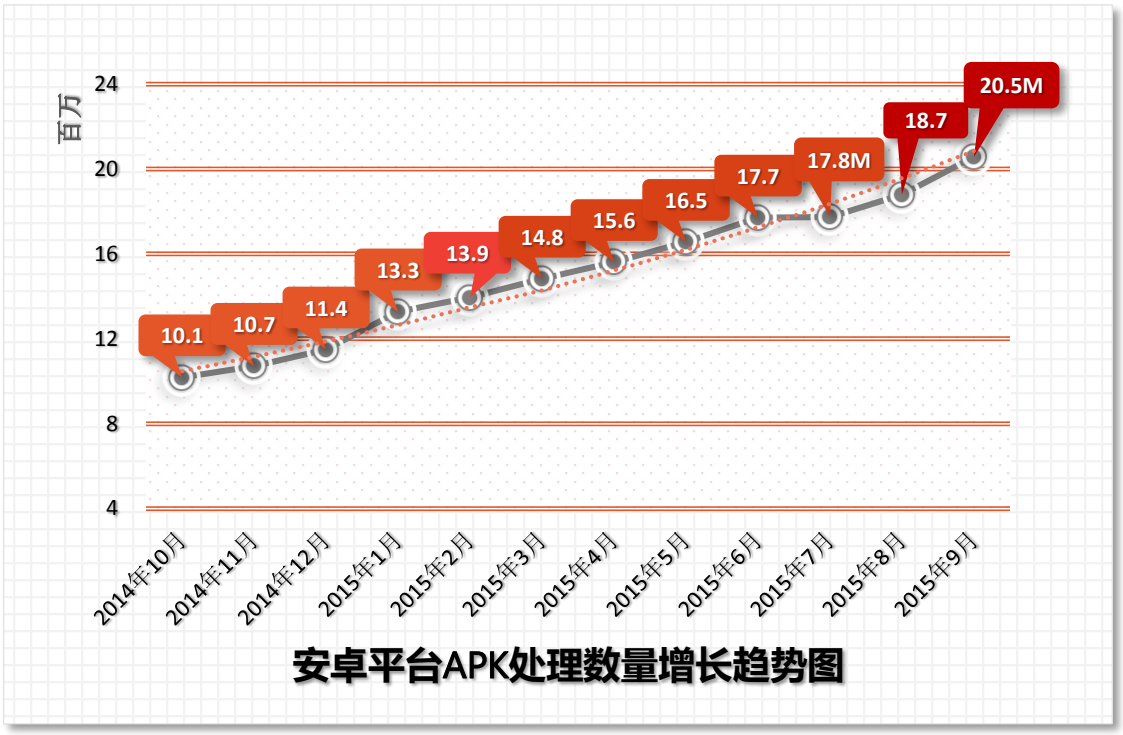
2015 年第 3 季度新增病毒类型分布图

在 2015 年第 3 季度新增病毒种类中，新增数量最大的病毒类型为 **TROJ（木马病毒）**类型。本季度新增木马病毒特征共计 **360,619** 个，和第二季度相比数值略有增加。长期以来，木马一直是中国地区捕获数量最大的病毒类型，其占比远高于其它类型病毒，这是因为此种病毒通常以窃取攻击目标的账户密码等敏感信息为目的，为病毒制造者带来巨大经济回报。

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。

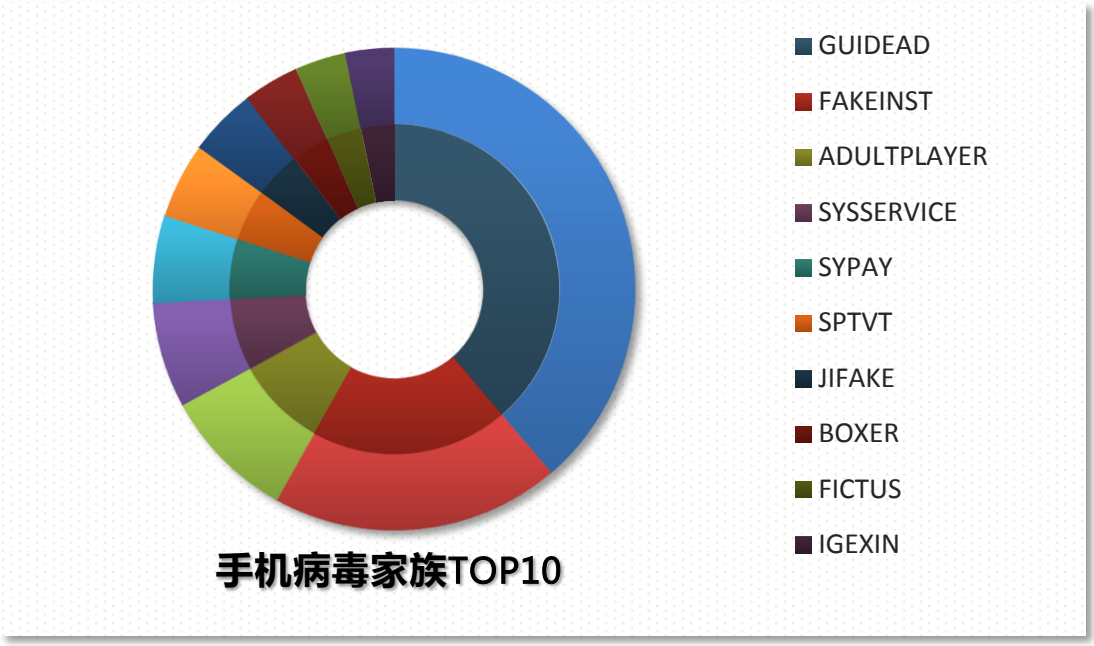
其中 JS(JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒与网页挂马有关，网页挂马是攻击者常用攻击类型。一些正常网站由于自身存在的缺陷漏洞，导致被入侵者挂马，之后浏览被挂马网页的访问者就会在毫不知情的情况下自动下载恶意文件到本地。

以 HT_打头的病毒类型标记为“黑客工具”的检测类型继续上榜。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。



2015 年第 3 季度安卓平台 APK 处理数量走势图

2015 年第 3 季度中，亚信安全对 APK 文件的处理数量依旧呈上升趋势。截止到本季度的 9 月底，处理数量累计达到 2,057 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。



2015 年第 3 季度手机病毒家族 TOP10 分布图

在 2015 年第 3 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 38.76%；FAKEINST 家族位列第二，占 19.35%；ADULTPLAYER 家族居第三位，占总数的 8.92%。排列前三的家族占总数过半。

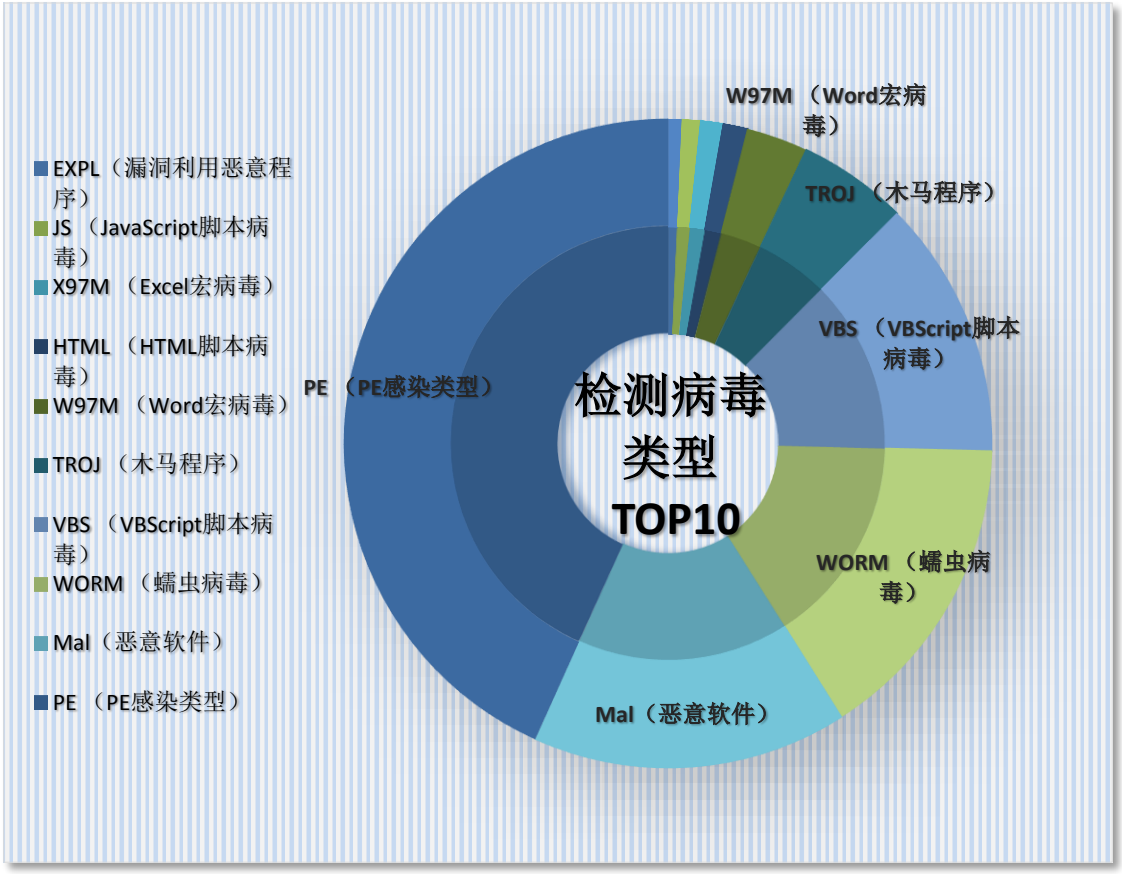
在 2015 年第 3 季度中，亚信安全注意到关于 iOS 设备受到 Hacking Team 间谍软件威胁的消息，其实 Android 设备同样会受到威胁。我们在泄露的内部文件中发现开源间谍软件包 RCSAndroid(Remote Control System Android),这个间谍工具套件向客户出售，用来监控目标。RCSAndroid 可以称为目前最复杂、技术最成熟的安卓恶意软件。泄露的源代码为其他黑客生产更多的监控工具提供了素材。

基于泄露的源码，RCSAndroid 可以实现以下监控功能：

- 通过“screencap”命令抓取屏幕截图
- 监控剪切板内容
- 收集 WIFI 网络密码以及网上账户信息，包括 Skype，Facebook，Twitter，Google，WhatsApp，Mail 和 Linkedin 账户。
- 收集短信、彩信以及 Gmail 信息
- 收集用户地理位置
- 收集设备信息
- 用前置或后置摄像头拍照
- 收集联系人姓名或从 IM 账户解码信息，包括 Facebook Messenger，WhatsApp，Skype，Viber，Line，WeChat，Hangouts，Telegram 和 Blackberry Messenger 通过挂钩系统服务“mediaserver”捕获实时通话内容。

攻击者通过两种方式使目标下载 RCSAndroid：第一个方法是通过短信或邮件向目标发送精心伪造的 URL。该 URL 会触发默认浏览器的 CVE-2012-2825 内存任意地址读取漏洞以及 CVE-2012-2871 堆溢出漏洞，涉及系统包括从 Android 4.0 到 4.3 的版本。这些漏洞利用成功后还可能导致本地提权漏洞的利用。当机器的 root 权限被获得，后门即被安装，RCSAndroid 恶意 APK 也会随之被安装到手机上。第二种方法是用一个可以绕过 Google Play 检测的后门程序，比如 ANDROID_HTBENEWS.A。在这里 ANDROID_HTBNEWS 以及前面提到的恶意 APK 的目的都是来利用安卓设备上的本地提权漏洞。Hacking Team 已经在代码里利用 CVE-2014-3153 和 CVE-2013-6282。这两个漏洞会 root 手机并由此安装后门。

2015 年第 3 季度各类型病毒检测情况分析



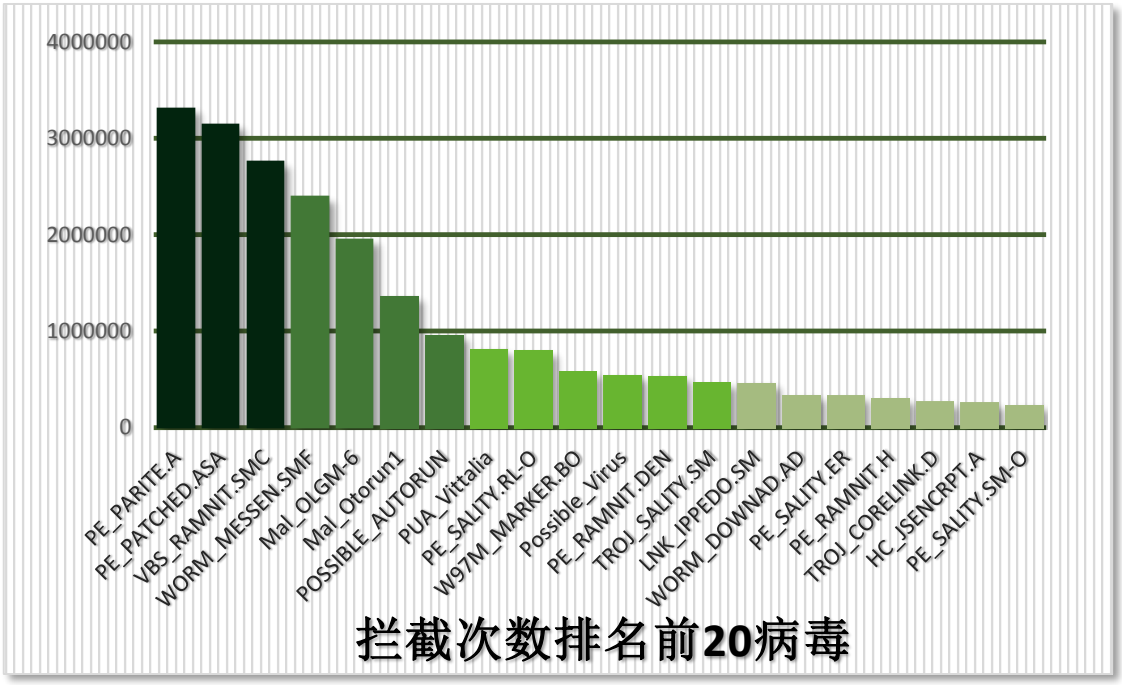
2015 年第 3 季度病毒检测类型分布图

2015 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 43.27%。在本季度中，PE_PARITE 检测数量排名第一，此外 PE_PATCHED、PE_SALITY、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 15.60%，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。WORM_MESSEN 家族蠕虫病毒连续 2 个季度保持上升趋势。

2015 年第 3 季度病毒拦截情况分析



2015 年第 3 季度病毒拦截情况图

在 2015 年第 3 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远高于其它检测名。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。

PE_PATCHED.ASA 在本季度被检测到的拦截次数约为 314 万多次，拦截次数依然高于大部分检测名。

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

值得注意的是，在中国地区本季度监控到检测名为 **PE_PARITE.A** 的病毒检测数量大增，拦截次数排名第一。这种感染型病毒并非新型病毒，但其快速传播的特性值得用户警惕，关于该病毒的详细信息介绍如下：

传播途径：

可能是由远程站点的其他恶意软件/灰色软件/间谍软件下载而来。

通过在受感染计算机上的文件中添加自己的恶意代码来感染文件。

感染文件类型：

.EXE

.SCR

恶意行为：

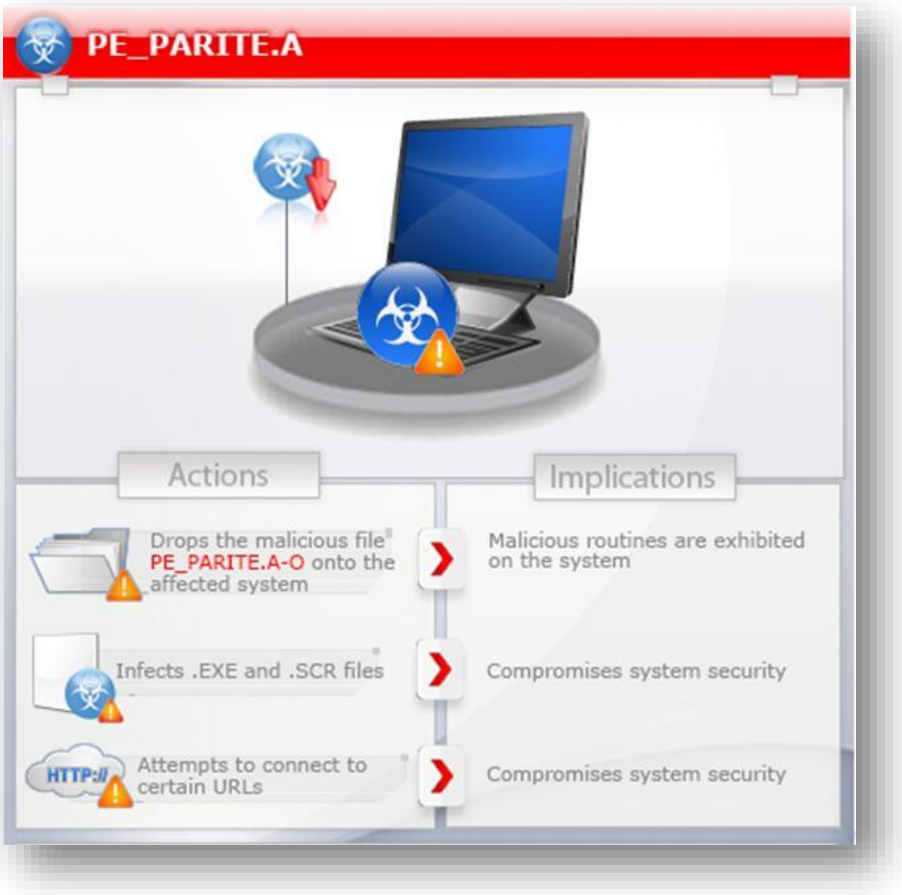
该病毒的母体文件（检测名为 PE_PARITE.A-O）通常会先感染 explorer.exe 从而得以驻留内存。一旦成功，它将会感染受感染电脑上以及可以通过网络共享访问到的目录中的所有.EXE 和.SCR 文件。

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

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

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

该病毒创建名为“RESIDENTED”的互斥量，用以确定自身是否已经运行。



PE_PARITE.A 病毒行为示意图

传播途径及防护方法：

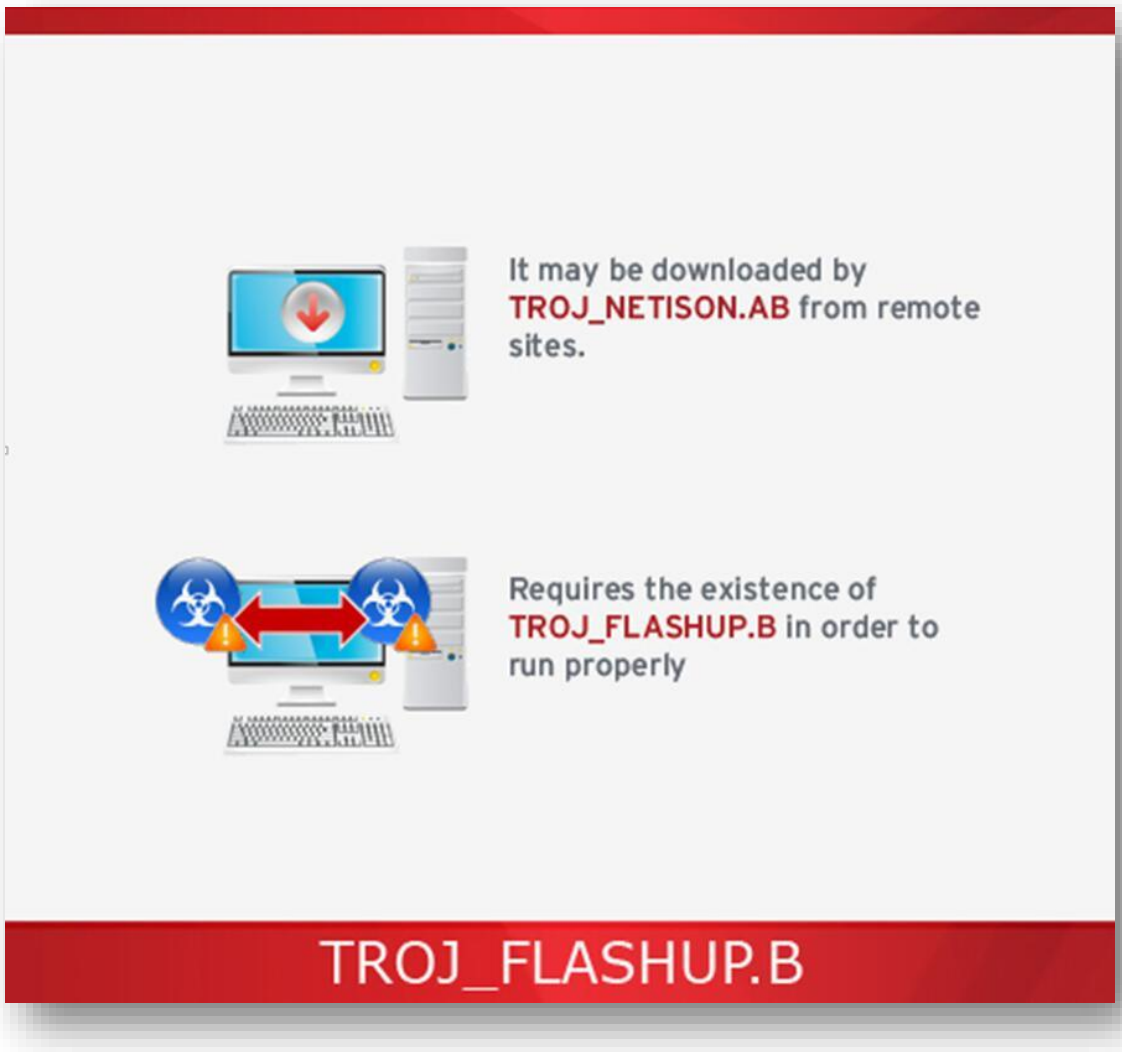
- ✓ 该病毒通过已被感染过的文件以及共享文件夹传播。由于该病毒能够通过共享文件夹传播并感染，所以防护该病毒的一个重要环节即对共享文件夹进行控制。
- ✓ 介于该病毒首先会感染 explorer.exe 这个特性，我们可以使用亚信安全防毒产品中的“爆发阻止”功能，阻止对 explorer.exe 的修改。

相关信息链接：

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

2015 年第 3 季度热门新型病毒分析

本季度热门病毒 TROJ_FLASHUP.B 是一个与零日漏洞 CVE-2015-5119 有关的新型病毒。



TROJ_FLASHUP.B 恶意行为示意图

病毒的详细信息如下：

病毒检测名：
TROJ_FLASHUP.B
抵达细节：
该木马由恶意软件 TROJ_NETISON.AB 从远程站点下载到本地计算机上。

安装：
这个木马的 dll 组件会被注入到以下进程中：
dwm.exe
wuauclt.exe
ctfmon.exe
wscntfy.exe

添加以下互斥量确保只有一个自身副本在运行：
Windows Update Process
Windows Update System Verifier

如果发现受感染的系统内存有以下进程，会终止运行：
Regmon.exe
Filemon.exe
Procmon.exe

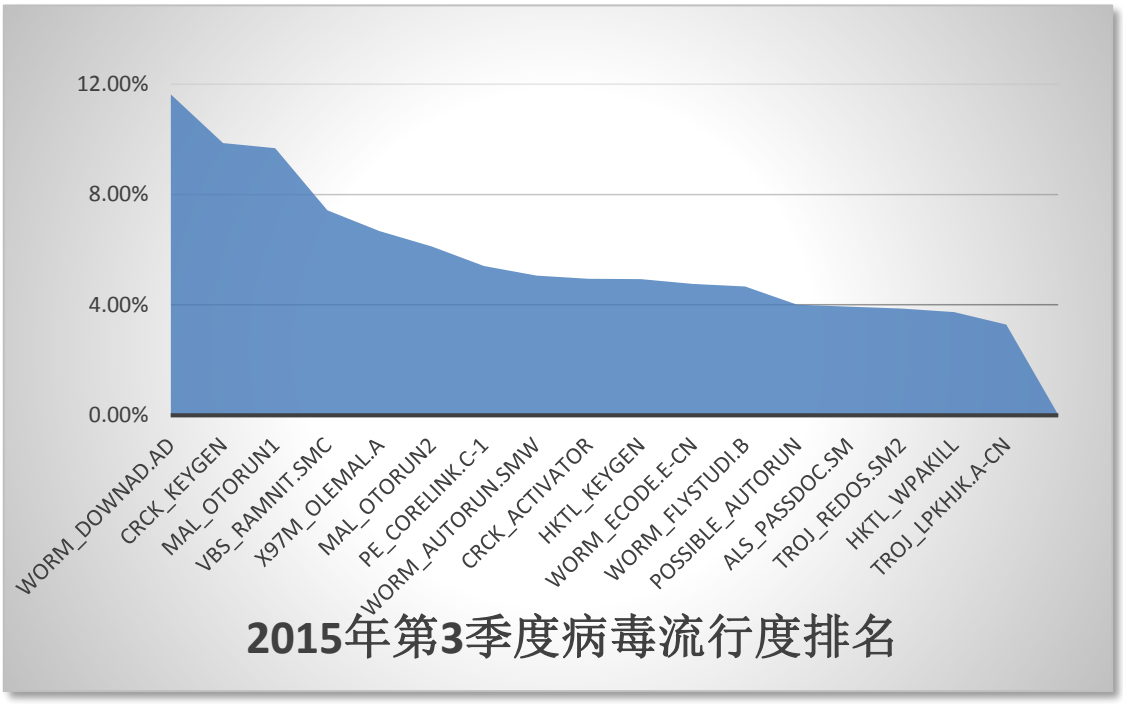
其它细节：
这个木马需要以下这些文件存在才能正确运行：
%System%\kbflashUpd.dll – 病毒检测名 TROJ_FLASHUP.B
%System%\flash32.exe – 病毒检测名 TROJ_FLASHUP.A

解决方法：
1. 使用亚信安全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. 非亚信安全防病毒客户端的用户，可以使用亚信安全提供的 ATTK 扫描病毒并收集信息。

未安装亚信安全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

相关信息链接：
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TROJ_FLASHUP.B

2015 年第 3 季度流行病毒分析



2015 年第 3 季度流行病毒排名情况图

本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

2015 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 2015 年第 3 季度，约有 11.63%的用户遭受到此病毒的攻击。

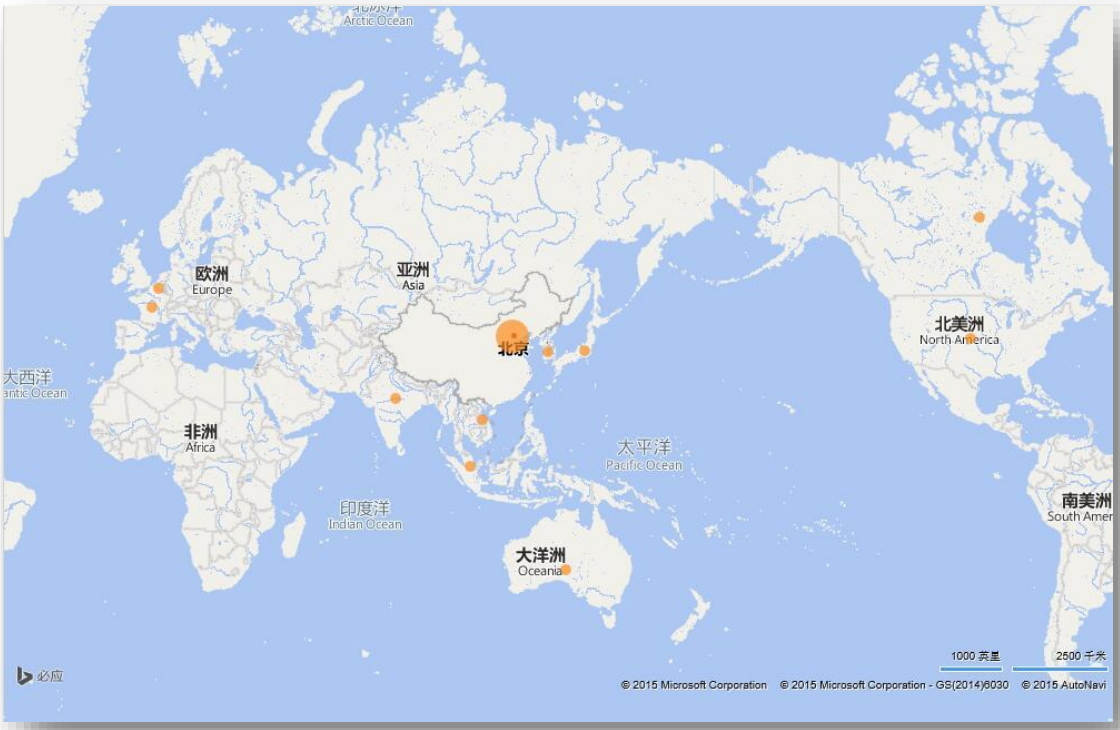
WORM_DOWNAD 病毒的持续流行与用户所处环境和使用习惯有一定联系，虽然目前的防毒产品均可以检测并处理该病毒，但该病毒依然屡见不鲜。

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 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。

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 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。

✓ 未安装亚信安全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

✓ 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

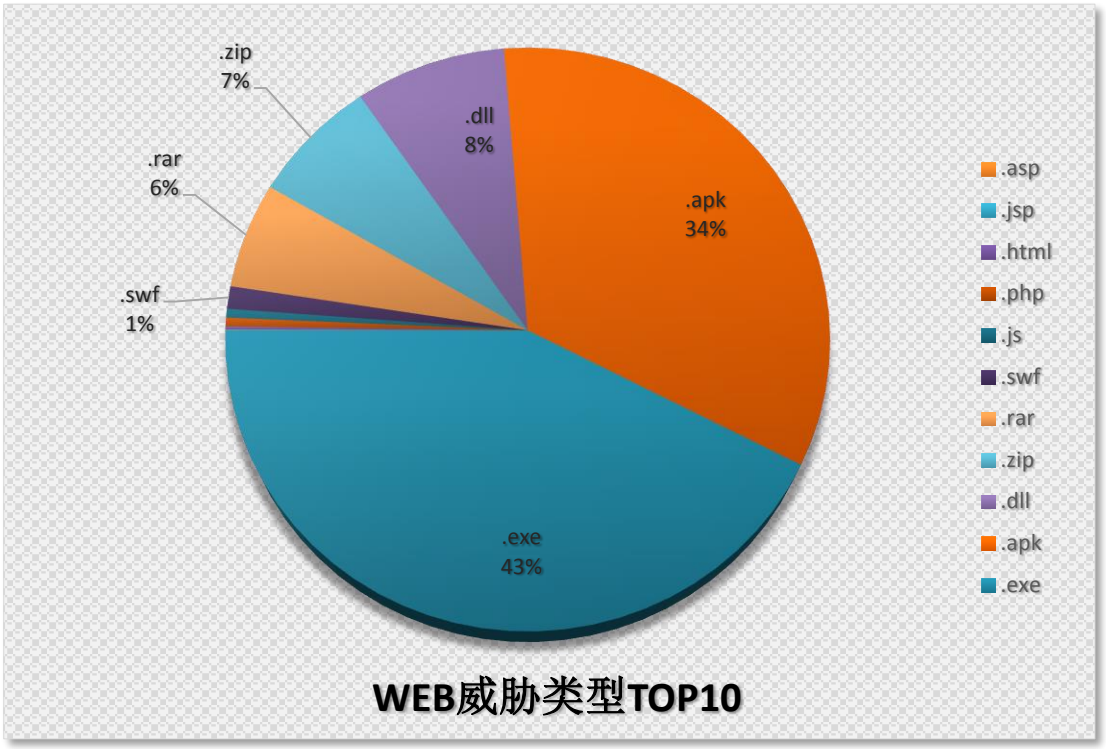
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2015 年第 3 季度 WEB 安全威胁情况

2015 年第 3 季度 WEB 威胁文件类型分析

在 2015 年第 3 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 42.5%，所占比例比上一季度 47.0%的占比有所下降。.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。

本季度通过 WEB 传播的恶意程序中，.APK 文件所占比例居高不下，此外.DLL 类型的文件超过了压缩文件格式.RAR 及.ZIP 所占比例，位居第三位。



2015 年第 3 季度中国地区 WEB 威胁文件类型分布图

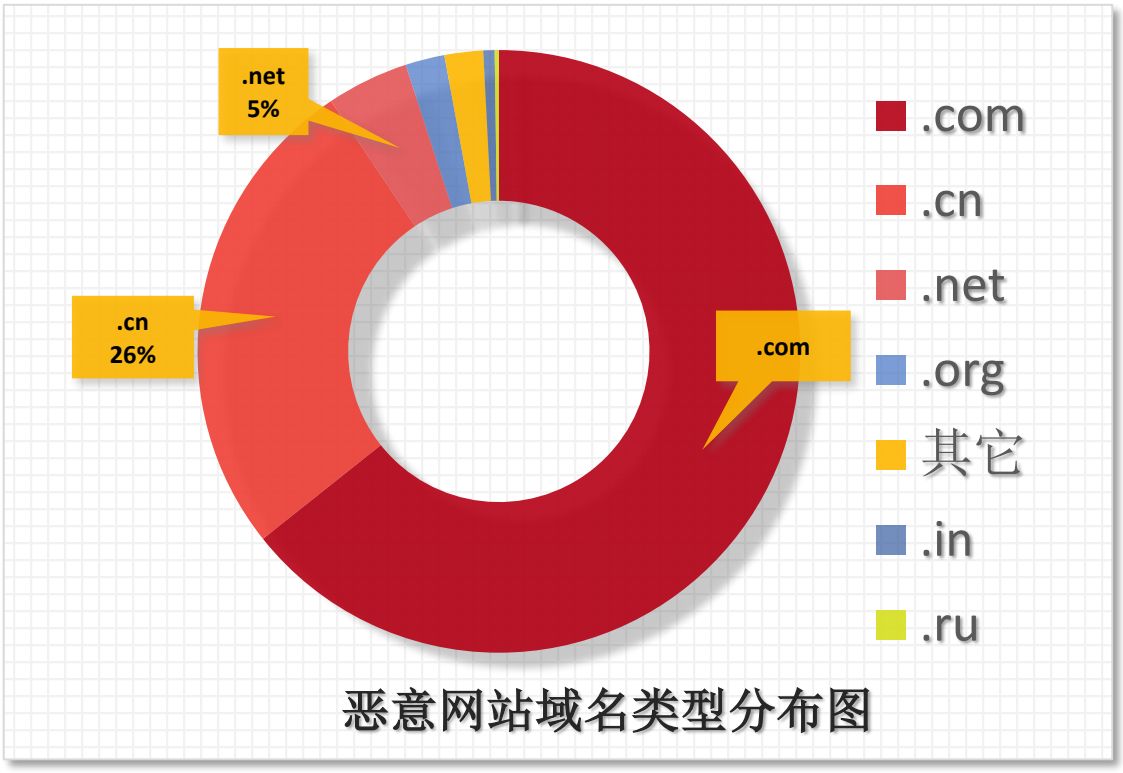
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

2015 年第 3 季度 TOP 10 恶意 URL

TOP10 恶意URL		
恶意URL	描述	点击量
http://download.234***n/2345zhushou	网站直接或间接帮助传播恶意软件或恶意代码	1,829,001
http://download.23***afe/2345PC***uye.exe	网站直接或间接帮助传播恶意软件或恶意代码	1,261,405
http://downl***n/2345pcsafe/2345pcsafe_100011_shouye.exe	网站直接或间接帮助传播恶意软件或恶意代码	989,994
http://trafficc***r.biz/4vir	网站直接或间接帮助传播恶意软件或恶意代码	943,232
http://119.18***35/index.html	网站直接或间接帮助传播恶意软件或恶意代码	931,296
http://119.18***36/index.html	网站直接或间接帮助传播恶意软件或恶意代码	924,419
http://220.18***04/msvquery	网站直接或间接帮助传播恶意软件或恶意代码	824,999
http://106.12***15/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	824,869
http://220.18***04/msvquery	网站直接或间接帮助传播恶意软件或恶意代码	823,498
http://106.12***7.7/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	821329

2015 年第 3 季度中国地区 WRS 拦截恶意 URL 排名 TOP10

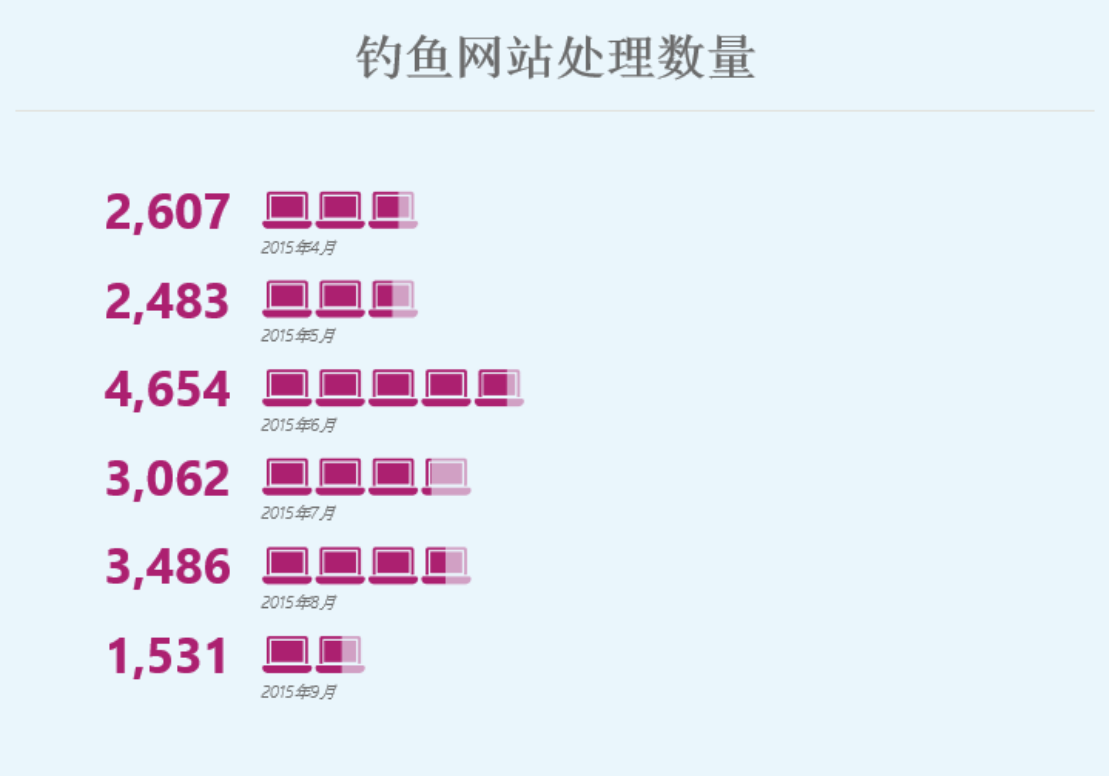
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。



2015 年第 3 季度恶意网站域名类型分布图

2015 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、.CN、.NET 的域名的站点占总数 94.99%。其中.COM 域名的恶意网页数量最多。

2015 年第 3 季度 WEB 威胁钓鱼网站仿冒对象分析



2015 年第 3 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：2015 年 4 月至 2015 年 9 月的 6 个月中，处理钓鱼网站共计 **17,923** 个。

2015 年第 3 季度中 7、8 钓鱼网站数量继第 2 季度依然保持下降趋势。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。

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 99%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 3 季度中使用.COM、.CC 和.TK 域名的钓鱼网站数量占本月处理总量的 80%以上。以.COM 域名下的钓鱼网站占总钓鱼网站数量的比重高居。

对于无法辨别恶意与否的网站可以到亚信安全网站安全查询页面查询：
http://global.sitesafety.trendmicro.com/index.php

亚信安全网站安全查询页面

2015 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	63268
CVE-2010-0806	51
CVE-2010-2568	24
MS08-067	21
CVE-2010-3333	6
CVE-2010-3334	3
CVE-2010-3335	3
CVE-2010-3336	3
CVE-2010-3337	3
CVE-2015-5119	3

2015 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
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-2010-3333	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333
CVE-2010-3334	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-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-2015-5119	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5119

漏洞介绍链接

本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 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 3 季度最新安全威胁信息

2015 年第 3 季度安全威胁信息摘要

2015 年第 3 季度国内外安全威胁信息关键词

❖ 恶意软件“冲击”苹果设备安全防线 果粉稍不留神即遭网络“黑手”

iPhone6s、iPad Pro、iMac 新品接连问世，让不少果粉们“荷包大动”。相对火热的装备升级热潮，另一端苹果设备被感染恶意软件的负面事件也层出不穷。苹果已不再是网络安全威胁的避风港，稍不留神就泄露了个人信息甚至直接造成经济损失。亚信安全提醒果粉在使用 iPhone、Mac 等苹果设备时，也要养成良好的上网安全习惯，并推荐安装亚信安全 PC-cillin2015 等可实现跨平台防护的安全软件。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20151021101159.html

❖ 十一假期或成钓鱼网站“狩猎”季 亚信安全提醒用户访问正规订票网站

消费者在十一黄金周的出游热情不仅让正规商家们翘首以盼，也让网络不法分子们垂涎欲滴。亚信安全发现，不法分子正通过伪造各类网络购票网站、手机票务 APP 等，骗取消费者的个人用户信息、银行账号、支付密码，甚至直接窃取网银资金。亚信安全提醒消费者，十一长假网络订票务必前往正规的网站，登录后留意网站域名是否正常，并安装可信的个人防毒软件帮助实时甄别网络钓鱼威胁。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20150928091215.html

❖ 垃圾邮件两大威胁：宏病毒和勒索软件

在 2014 年，每天有 1963 亿封电子邮件在收发，其中，有 1087 亿封是商业邮件。大量的电子邮件的收发吸引了网络犯罪分子的关注，他们企图利用电子邮件攻击大型企业，这些攻击可能导致数百万美元的损失与数据窃盗。今年上半年主要有宏病毒垃圾邮件和勒索软件两大威胁。

上半年，我们注意到宏病毒垃圾邮件的威胁在显著地增加，这些垃圾邮件夹带着.DOC、.DOCM、.XLS 和.XLSM 等 Microsoft Office 扩展名的附件。

我们也看到一些包含 PDF 附件的电子邮件，这些附件实际上嵌入了可下载恶意宏的.DOC 文件；除了带有附件，有些邮件还包含恶意链接到正常文件托管网站（如 DropBox 等），但所放的却是恶意文件。

http://blog.sina.com.cn/s/blog_5e96245b0102vsw6.html

❖ 安卓用户新危机 间谍软件大起底

有关 Hacking Team 数据外泄入侵事件的各种消息及后续漏洞报导都遗漏了一个对安卓用户很重要的信息——RCSAndroid。对于被忽略的 RCSAndroid 似乎很不满，就让它自己来传达一下吧~

对于安卓用户来说，类似常见、频繁的威胁还有很多，所以是时候给手机装个防护软件来防御威胁了！

亚信安全移动安全防护个人版具有强大的隐私扫描防护功能，可主动侦测通过 APP、网页、短信等传送的恶意程序，防堵恶意软件进行个人资料的搜集，保护你的资料免于外泄。

http://blog.sina.com.cn/s/blog_5e96245b0102vso2.html

❖ 汽车联网安全吗?

五年前，你是否可以想象到你所开的汽车比登陆月球的阿波罗 11 号有更强的运算能力？令人高兴的是，我们现在拥有了最先进车身结构、安全气囊和防锁死系统以防止发生事故的汽车；但同样但令人忧虑的是：我们却不能给它足够的网络安全防护！

在我们的电脑软件和智能手机应用程序上，可以看到各种因商业迫切需求而匆匆上架的商品，但随着产品匆促推出却暴露了软件的潜在缺陷，当然联网汽车也面临同样的状况。跟智能手机应用程序不同的是，这些漏洞可能会危及人身安全。

http://blog.sina.com.cn/s/blog_5e96245b0102vraw.html

❖ Windows Server 2003 终止服务后的一个月，想它想它想它...

距离 2015 年 7 月 14 日,微软终止对 Windows Server 2003 的服务已有一个多月，想必很多企业现在的心态还是希望回到过去有安全性修补程序和漏洞通知的日子。但这时，企业要做的不是没有结果的苦苦等待，而是转移到新的操作系统来防止系统和网络遭受漏洞攻击。

http://blog.sina.com.cn/s/blog_5e96245b0102vq2v.html

❖ Shadow Force 病毒使用 DLL 劫持攻击韩国公司

Shadow Force 是一个新型后门，它会替换特定 Windows 服务调用的 DLL 文件。一旦后门被打开，攻击者可以使用一个或多个工具，以进一步开放权限进行破坏。这种类型的后门攻击之前已被在今年 5 月的博客文章中记录。

http://blog.trendmicro.com/trendlabs-security-intelligence/shadow-force-uses-dll-hijacking-targets-south-korean-company/

❖ 勒索软件 TorrentLocker 和 CryptoWall 改变战术

勒索软件的目标已经从面向消费者转向了小型和中小型企业（SMB）。他们似乎找到了更好的潜在目标，因为中小企业相对于大企业来说不太可能有复杂的安全解决方案，并且这些企业通常也有支付勒索金的能力。

http://blog.trendmicro.com/trendlabs-security-intelligence/businesses-held-for-ransom-torrentlocker-and-cryptowall-change-tactics/

❖ 两个新型 PoS 病毒影响美国中小企业

过去的几个月里 PoS 终端病毒在沉寂了一段时间后开始有所动作。近期我们发现了名为 Katrina 和 CenterPoS 的恶意软件现。

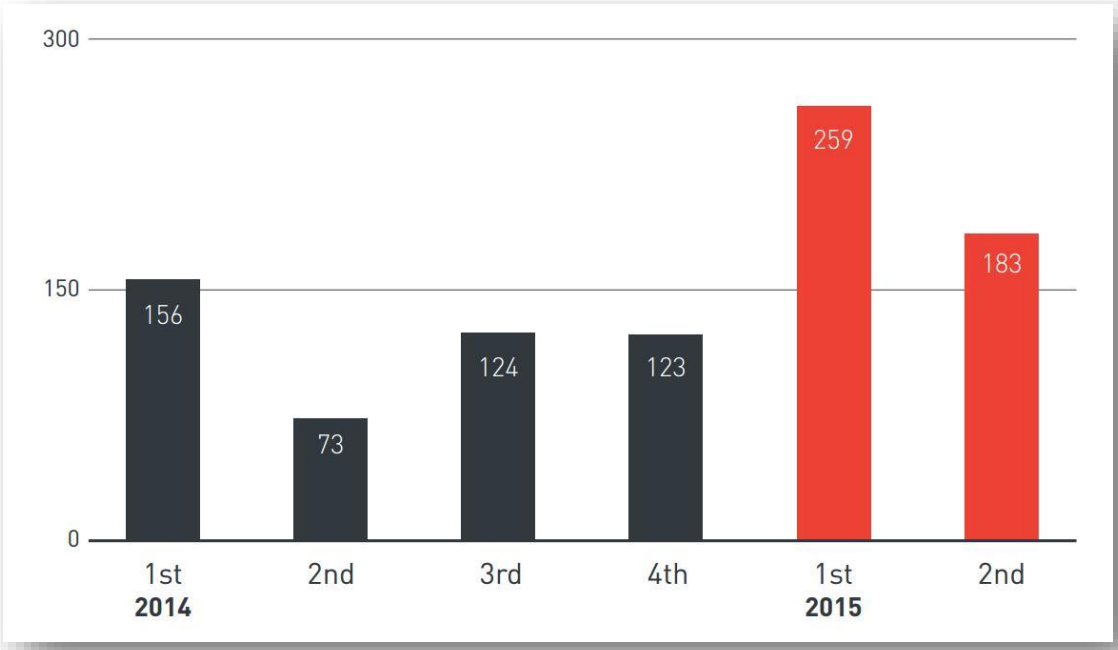
在我们的第二季度安全综述中，我们报告了新的 PoS 终端恶意软件，即四月发现的 FighterPoS，六月发现的 MalumPoS，和之后一个月发现的 GamaPoS。尽管有这些发现，我们注意到 PoS 恶意软件检测可能由于达到其饱和点而略有下降。但随着新一波 PoS 机恶意软件的出现，说明其威胁并没有结束。

http://blog.trendmicro.com/trendlabs-security-intelligence/two-new-pos-malware-affecting-us-smbs/

全球区最新安全威胁概要

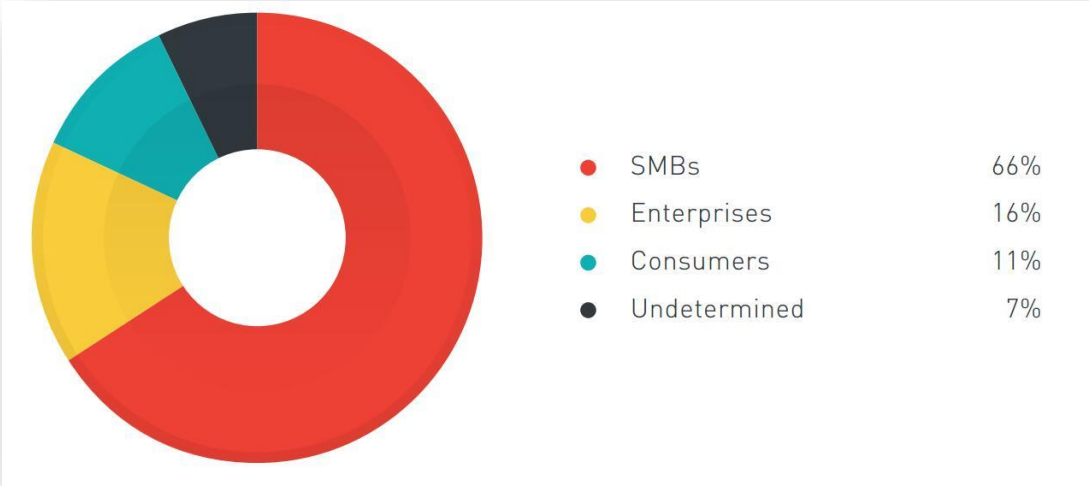
以下是来自 2015 年第 2 季度全球区安全报告的数据。

下图是 2014 年第 1 季度到 2015 年第 2 季度期间的 PoS 恶意软件威胁检测表，检测数下降可能是由于达到了饱和点。今年上半年的出现的一小波高峰可能仅仅是他们作的最后一搏。）



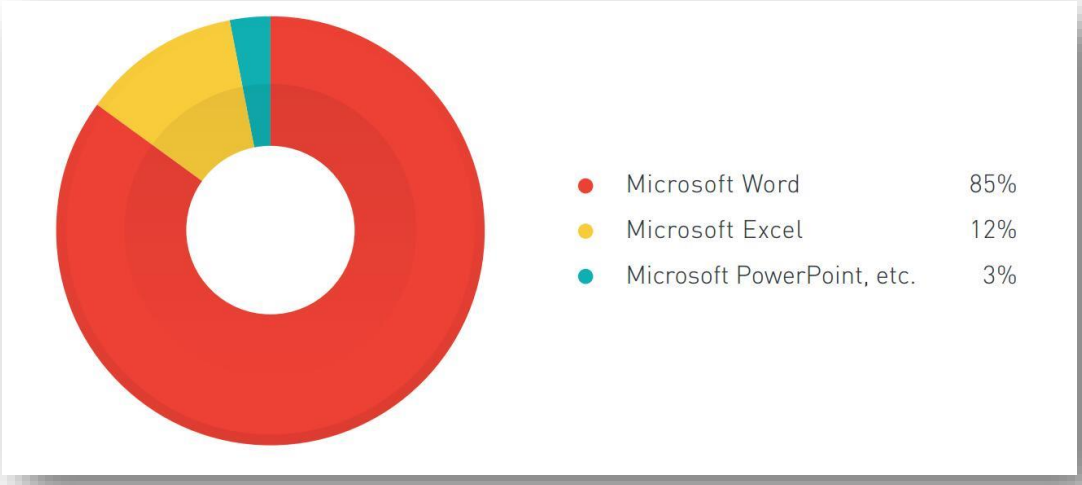
PoS 恶意软件检测数据图

根据 2015 年 6 月份的数据，中小型企业是感染 CryptoWall 的重灾区。



与 CryptoWall 有关的 URL 分布表

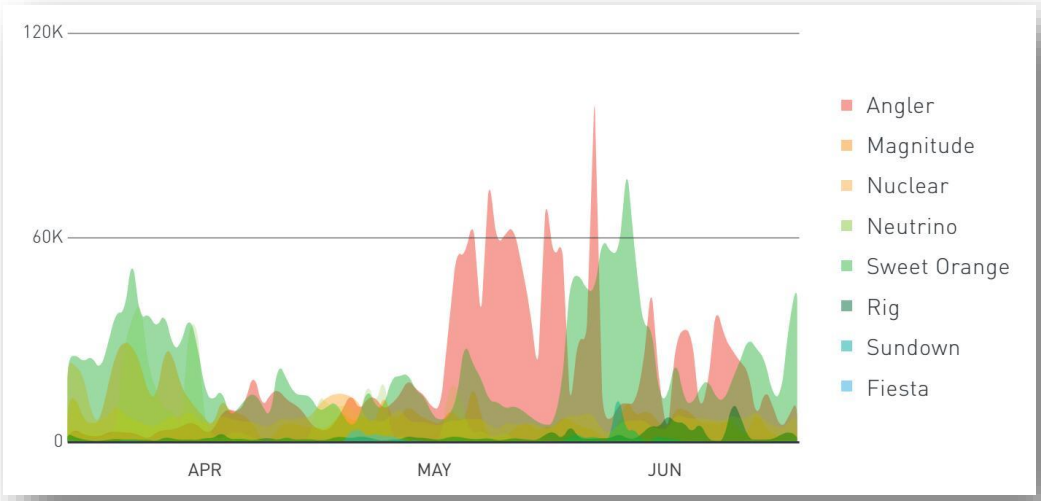
2015 年第 2 季中发现的绝大部分宏病毒基于 Microsoft Word 文档。



宏病毒类型分布图

本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

从下图可以看到，今年5月份到6月初，访问Angler漏洞利用工具包托管URL的访问数大幅激增。在这段时间里检测到了大量与Angler漏洞利用工具有关的成人网站。



漏洞利用工具包托管 URL 分布图

Angler 漏洞利用工具的开发者非常活跃，不断推出新版本，并在漏洞套件里增加了多个漏洞。新增的 11 个漏洞里有 10 个是针对 Adobe Flash 的漏洞，所有加载视频内容的软件都会面临风险。

Angler 和 Magnitude 漏洞利用工具包还集成了一个利用了 Silverlight® 的漏洞（CVE-2015-1671）。

2015 年第 2 季度知名漏洞利用工具新增漏洞示意图

本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 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 2015 年第 2 季度全球安全报告请访问：

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

关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式,助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问: http://www.asiainfo-sec.com。

关于中国区网络安全监测实验室

亚信安全“中国区网络安全监测实验室”是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。亚信安全“中国区网络安全监测实验室”利用亚信安全的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。

AsiaInfo 亚信安全

ChinaRTL

中国区网络安全监测实验室

本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。