AsiaInfo 亚信安全

中国地区 2015 年
第四季度
网络安全威胁报告

2016/01

CHINA RTL

目录

2015 年第 4 季度安全威胁

本季安全警示：

APT 病毒、勒索软件

2015 年第 4 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 **20** 万条。截止 2015.12.31 日中国区传统病毒码 **12.242.60** 包含病毒特征数约 **427** 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 **8,740** 万次。

- 本季度亚信安全在中国地区拦截的恶意 URL 地址共计 **23,295,678** 次。

本季度热点话题为 APT 病毒家族。APT 病毒擅长隐匿跟踪，长期潜伏在用户网络中，持续窃取信息，却又很难被用户发现，一份关于 APT 攻击的报告显示，在所有数据泄漏事件当中，黑客平均潜伏的天数长达 205 天。根据长期跟踪研究，我们发现黑客团体有着组织性犯罪的显著特征，精心选择隐匿行踪的技巧，而且擅长通过有组织的行动将攻击分散开来，以躲避杀毒软件查杀。他们通常通过“鱼叉式”攻击，“零时差”漏洞，浏览器和应用程序漏洞植入系统。其盗取的核心机密数据能够在地下黑市为其换得高额回报，巨大的诱惑让他们长期潜伏下来，并且持续渗透。

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。

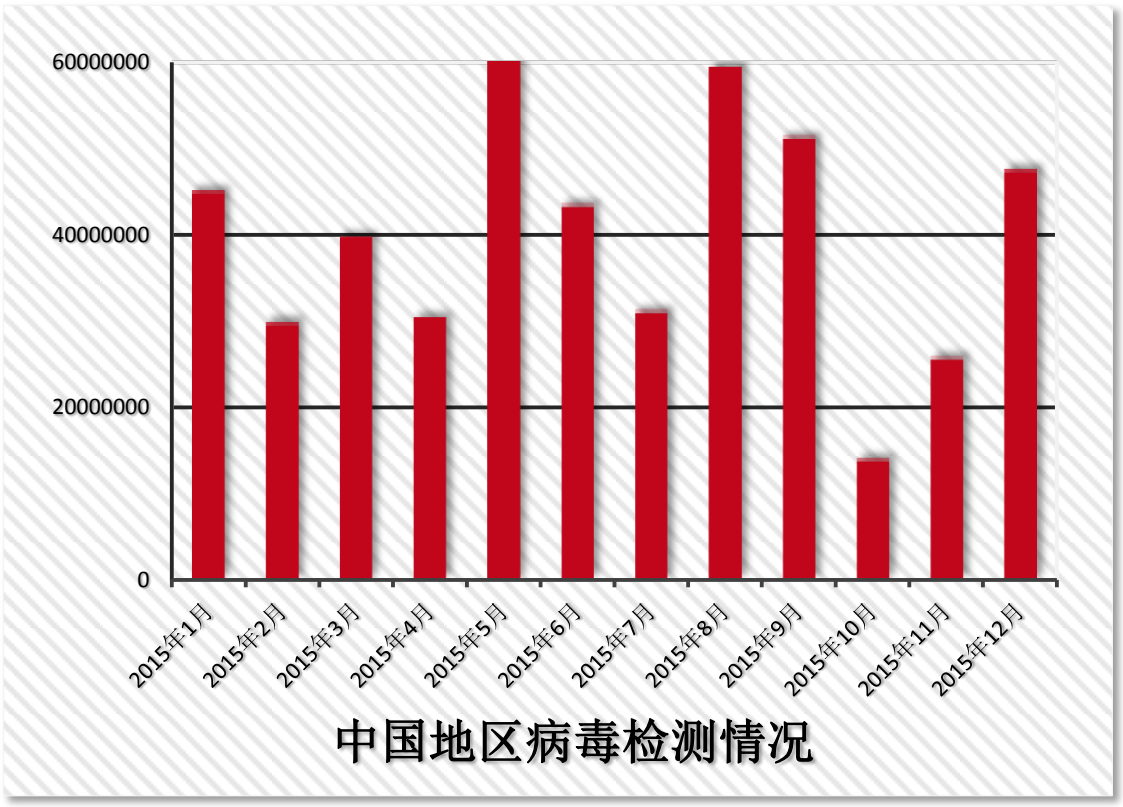
APT 攻击方法在不断更新升级，亚信安全的研究人员发现，当前地下市场上最精密的恶意软件之一就是 Stegoloader，它可以将 C&C 通信隐藏在图片当中。同时采取多种方法躲避杀毒软件的追杀，大多数的系统管理员都会被这样的技巧所骗，因为他们习惯上只会在安全网关上拦截可以执行文件并进行分析，不会拦截图片文件。但这些图片一旦进入目标网络之后，恶意软件就会帮助黑客发挥“横向移动”的能力。

能够骗过管理员和用户的另外一个伎俩就是 Office 文档，而这也是宏病毒藏身的地方。其已经成为 APT 攻击的惯用工具。例如：2014 年出现的数据窃取软件 ZeuS，它通过启用宏的 Microsoft Word 文件来进行散播。在同年 11 月还发现了 DRIDEX（一个针对网络银行用户的数据窃取软件）采用相同的感染策略。紧随其后的是 ROVNIX、VAWTRAK、BARTALEX 这些后门恶意软件，黑客还加上自己的防御手段，他们或是对启用宏的文件加上密码保护来防止防毒软件的查杀，或是开辟新方法来通过宏恶意软件感染用户。

随着度 APT 深入分析，我们研究发现其攻击共有六个阶段，这包括：情报收集、单点突破、命令与控制（C&C 通信）、横向移动、资产/资料发掘、资料窃取。在黑客团体常常分工明确，每一阶段由一组专门的黑客负责。另外，需要注意的不仅是在“单点突破”这个阶段的恶意代码，黑客在第四阶段的“横向移动”对于最后资料窃取阶段的布局也至关重要。不断地在不同终端之间移动，可以让黑客完整扫描整个网络，并且找到最珍贵的数据。

本季度 APT 家族中的佼佼者为证券幽灵病毒，该病毒是一个针对国内银行、证券等金融类机构的 APT 病毒家族，该病毒主体是一个 DLL 文件。其功能非常复杂，配置灵活，路径隐蔽，文件信息往往伪造微软、Adobe 等著名厂商的文件，具有迷惑性。病毒有字符串加密和对抗杀毒软件的功能，而且配置文件和更新文件都是通过远程服务器上的图片来下发，这些特点都使得对该病毒家族的查杀变得更加困难。病毒可以搜集受害者机器上特定后缀的文件并发送出去，还可以接受远端的控制指令，是一个功能齐全的后门。

发现 APT 攻击者在企业内部的藏身之处有一定的难度，但不是说企业就束手无策。相反，企业必须不断提升自己的安全防护，并随时掌握整个企业网络的情况。亚信安全服务器深度安全防护系统（Deep Security）产品可提供 360 度全方位掌握来侦测 APT，防范黑客窃取企业敏感信息。

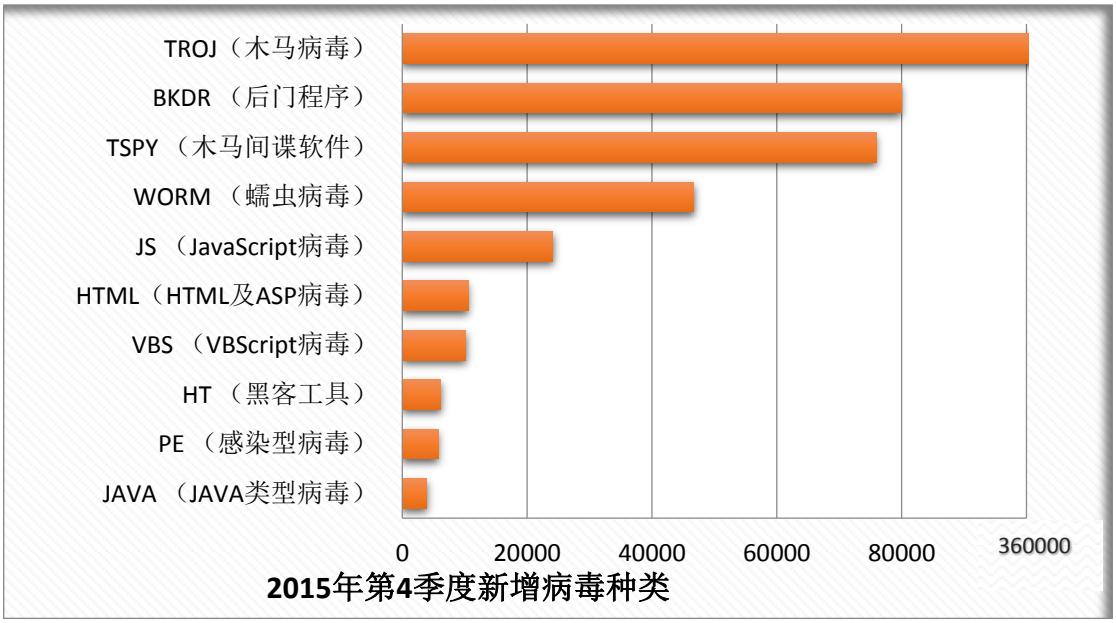


2015 年第 4 季度中国地区病毒检测数量图

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 4 季度病毒威胁情况

2015 年第 4 季度新增病毒类型分析



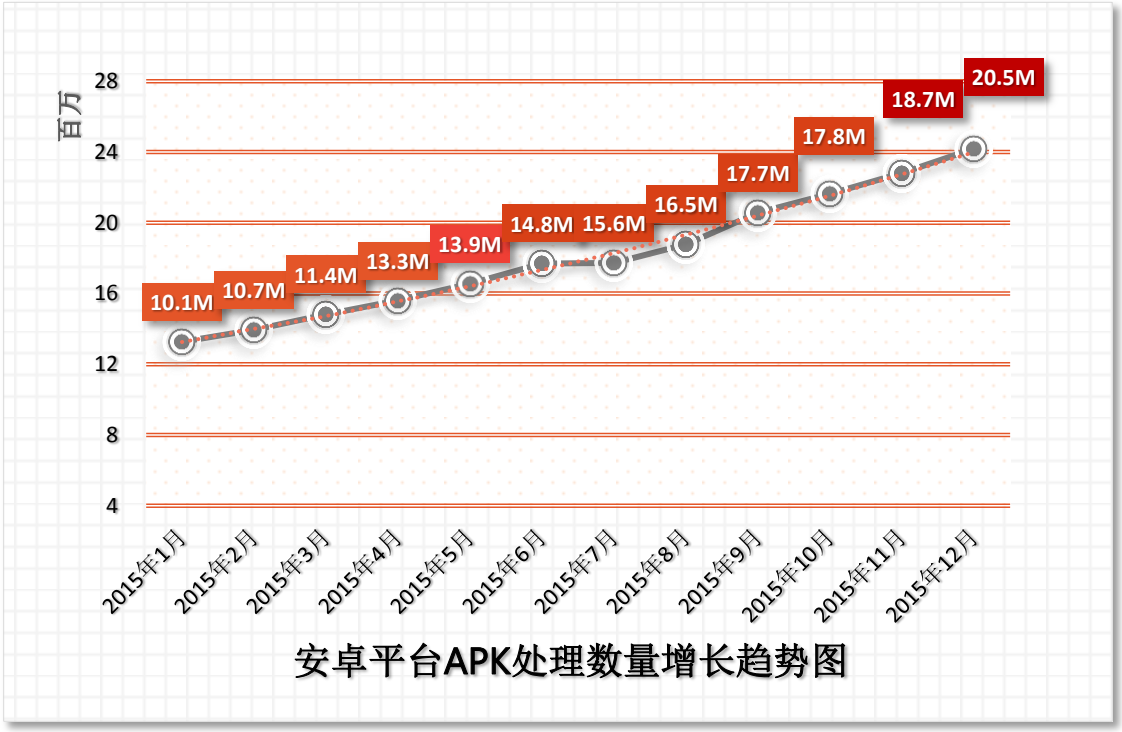
2015 年第 4 季度新增病毒类型分布图

在 2015 年第 4 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 **363,634** 个，和第三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。

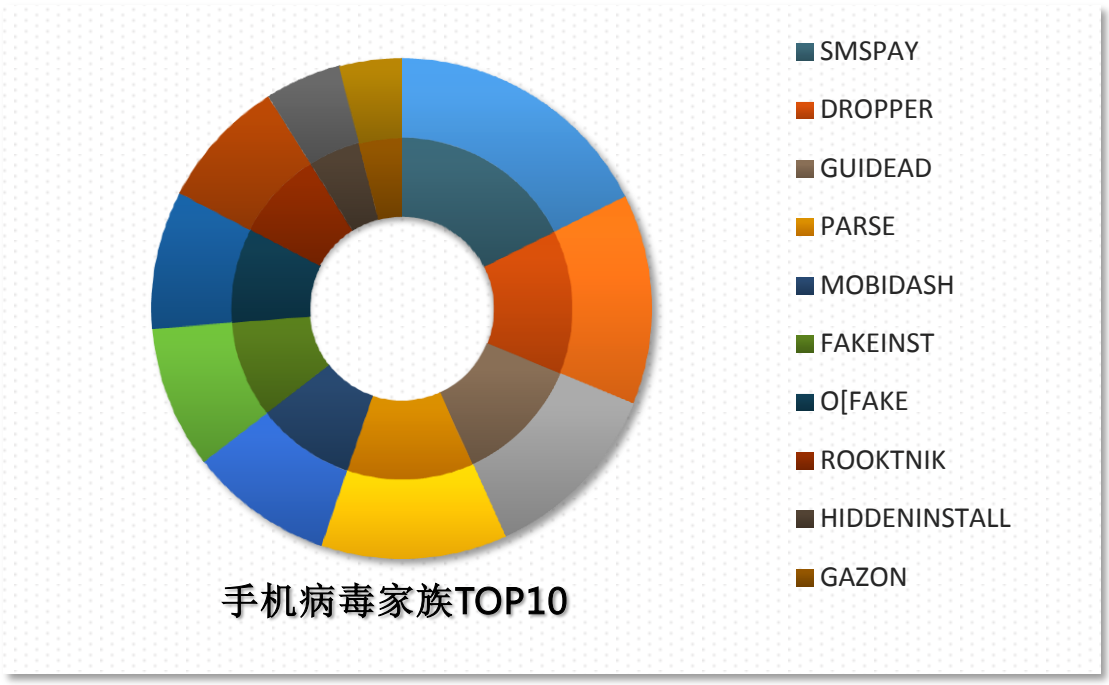
其中 JS(JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒与网页挂马有关，网页挂马是攻击者常用攻击类型。一些正常网站由于自身存在的缺陷漏洞，导致被入侵者挂马，之后浏览被挂马网页的访问者就会在毫不知情的情况下自动下载恶意文件到本地。

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 4 季度安卓平台 APK 处理数量走势图

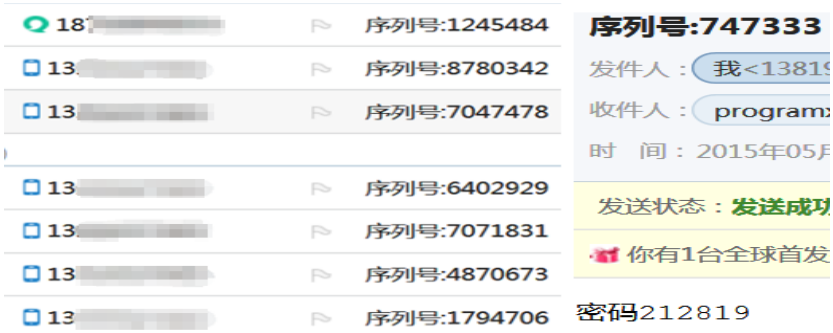
2015 年第 4 季度中，亚信安全对 APK 文件的处理数量依旧呈上升趋势。截止到本季度的 12 月底，处理数量累计达到 2,176 万个。从最近历史处理数据走势图看，安卓病毒单月增长率一直保持上升趋势。



2015 年第 4 季度手机病毒家族 TOP10 分布图

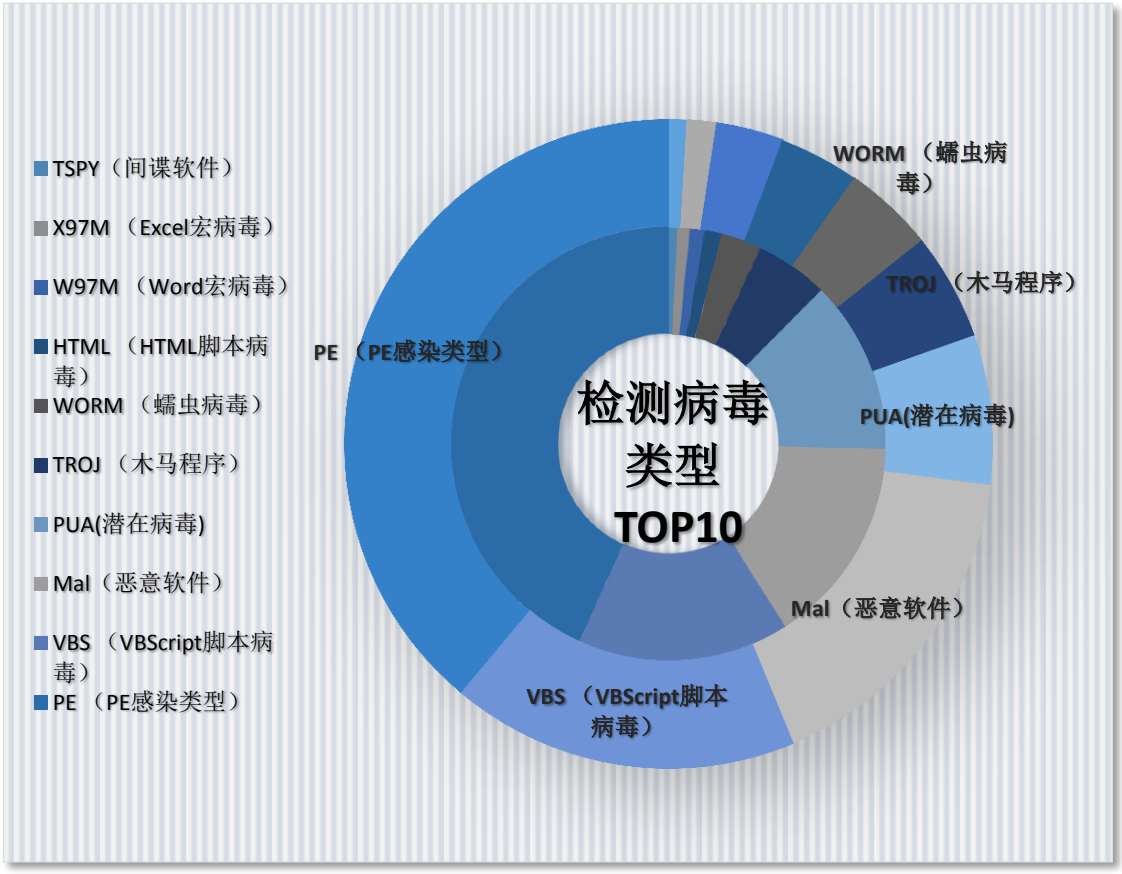
在 2015 年第 4 季度感染安卓平台的手机病毒家族中，SMSPAY 家族数量最多，占到总数的 17.62%；DROPPER 家族位列第二，占 13.62%；GUIDEAD 家族居第三位，占总数的 12.00%。与上季度相比，SMSPAY 家族涨势凶猛，而上季度排名第一的 GUIDEAD 家族则有减弱趋势。

在 2015 年第 4 季度中，亚信安全注意到中国市场正在流行手机勒索软件病毒，本季度新增 20 多种手机勒索软件病毒，其中有代表性的为 ANDROIDOS_JIANMO.HAT 和 ANDROIDOS_GREYWOLF.HBT 病毒，感染 ANDROIDOS_JIANMO.HAT 病毒的手机将被锁屏，被锁屏的手机将无法进行任何操作，病毒作者会通过 QQ 与受害者联系，索要 5-10 美元，而另外的 ANDROIDOS_GREYWOLF.HBT 病毒通过伪装成正常的 APP，诱骗用户安装并运行病毒，其会生成任意序列号及解锁密码发送给病毒制作者，受害者一般会通过支付宝，微信支付，银行转账等方式付款给病毒制作者。



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 4 季度各类型病毒检测情况分析



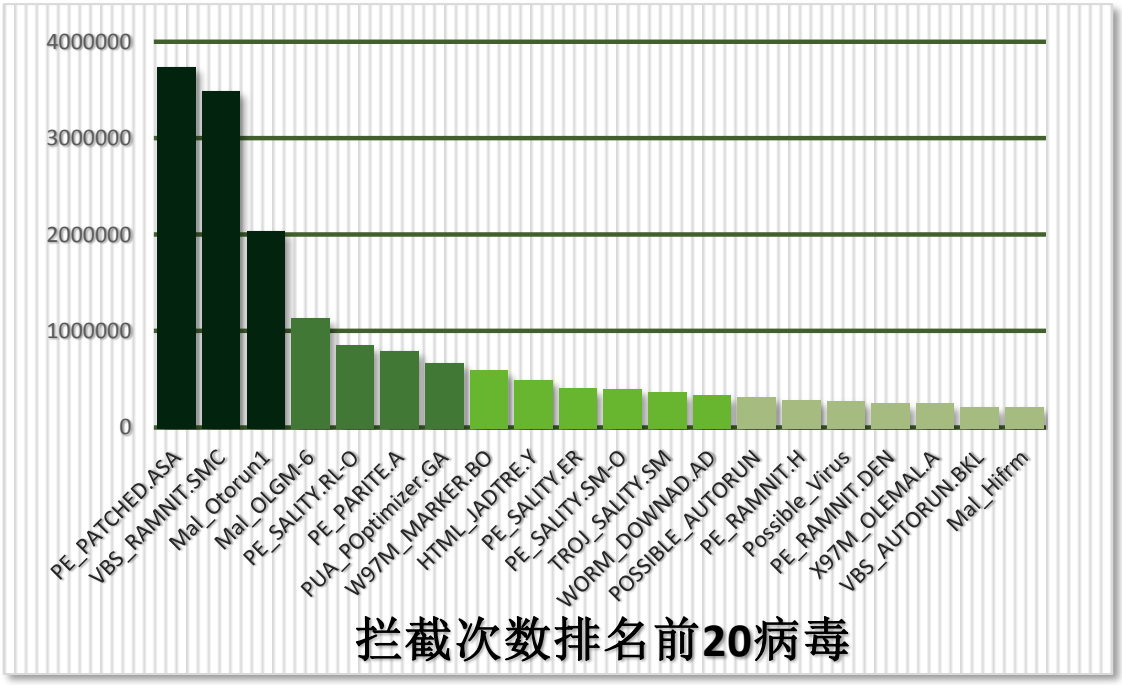
2015 年第 4 季度病毒检测类型分布图

2015 年第 4 季度检测到的病毒种类中，PE 类型病毒感染数量在所有类型中所占比重最大，占到总检测数量的 36.81%。在本季度中，PE_PATCHED 检测数量排名第一，此外 PE_PARITE、PE_SALITY、PE_RAMNIT 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 4.30%，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。

2015 年第 4 季度病毒拦截情况分析



2015 年第 4 季度病毒拦截情况图

在 2015 年第 4 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 374 万多次，拦截次数位居榜首。

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值得关注的病毒检测名为 **PE_PARITE.A**，其属于感染型病毒，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：

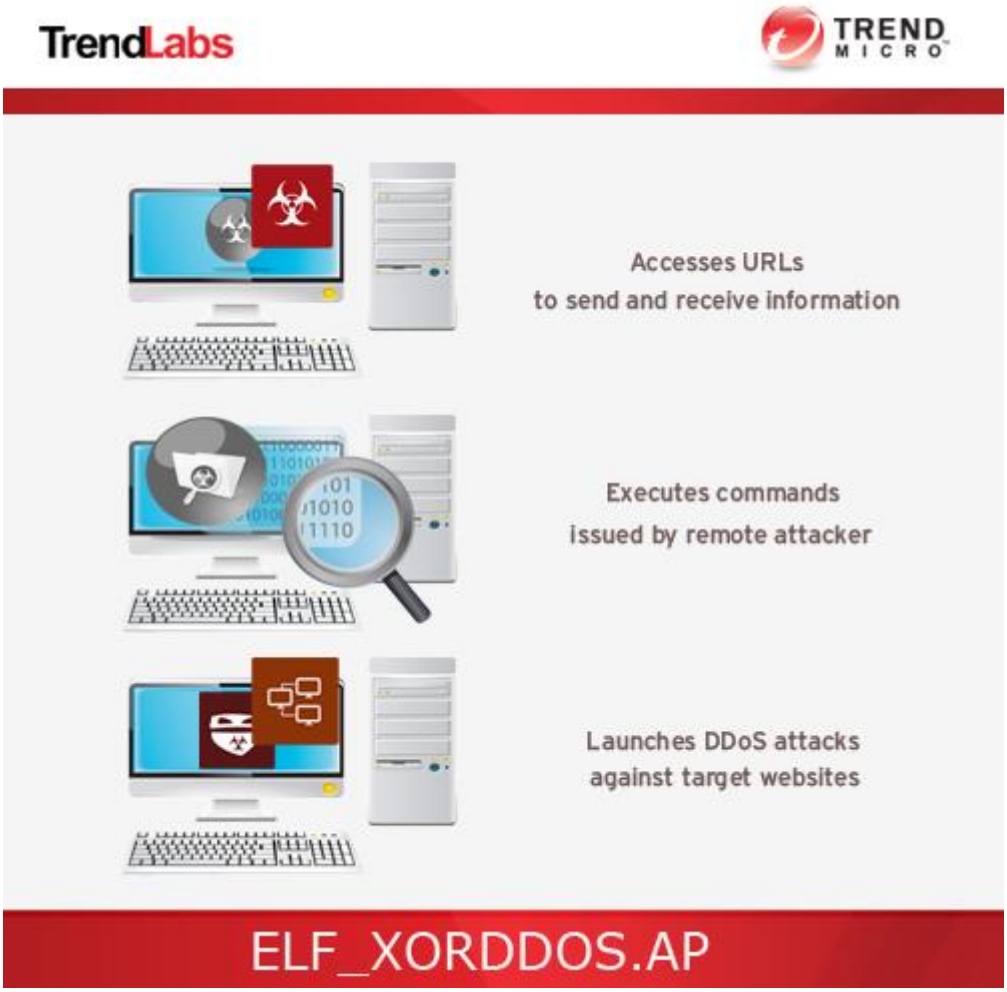
- ✓ 该病毒通过已被感染过的文件以及共享文件夹传播。由于该病毒能够通过共享文件夹传播并感染，所以防护该病毒的一个重要环节即对共享文件夹进行控制。
- ✓ 介于该病毒首先会感染 explorer.exe 这个特性，我们可以使用亚信安全防毒产品中的“爆发阻止”功能，阻止对 explorer.exe 的修改。

相关信息链接：

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

2015 年第 4 季度热门新型病毒分析

本季度热门病毒 ELF_XORDDOS.AP 是针对游戏及教育相关网站发起 DDoS 攻击的热门病毒。



ELF_XORDDOS.AP 恶意行为示意图

病毒的详细信息如下：

病毒检测名：ELF_XORDDOS.AP
文件类型：ELF
常驻内存： 是
抵达细节：该木马由其他恶意软件生成或者从远程站点下载到本地计算机上。

安装：
该木马生成如下文件：

/var/run/udev.pid
/lib/libgcc4.so

生成以下文件达到自启动目的：
/etc/cron.hourly/udev.sh

其它细节：

该木马将会接受远程恶意用户指令执行如下命令：
Start Denial of Service
Stop Denial of Service
Update malware
Download and execute file
Terminate Process
Request MD5 Hash of running malware

该木马链接如下网址接收信息：
gh.{BLOCKED}a1.org:2833
www.{BLOCKED}ngfacai.com:2833
{BLOCKED}.{BLOCKED}.31.154:2833
{BLOCKED}.{BLOCKED}.9.229
{BLOCKED}.{BLOCKED}.9.228

该木马链接如下网址下载其配置文件：
http://info1.{BLOCKED}c.com/b/u.php?id=01

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

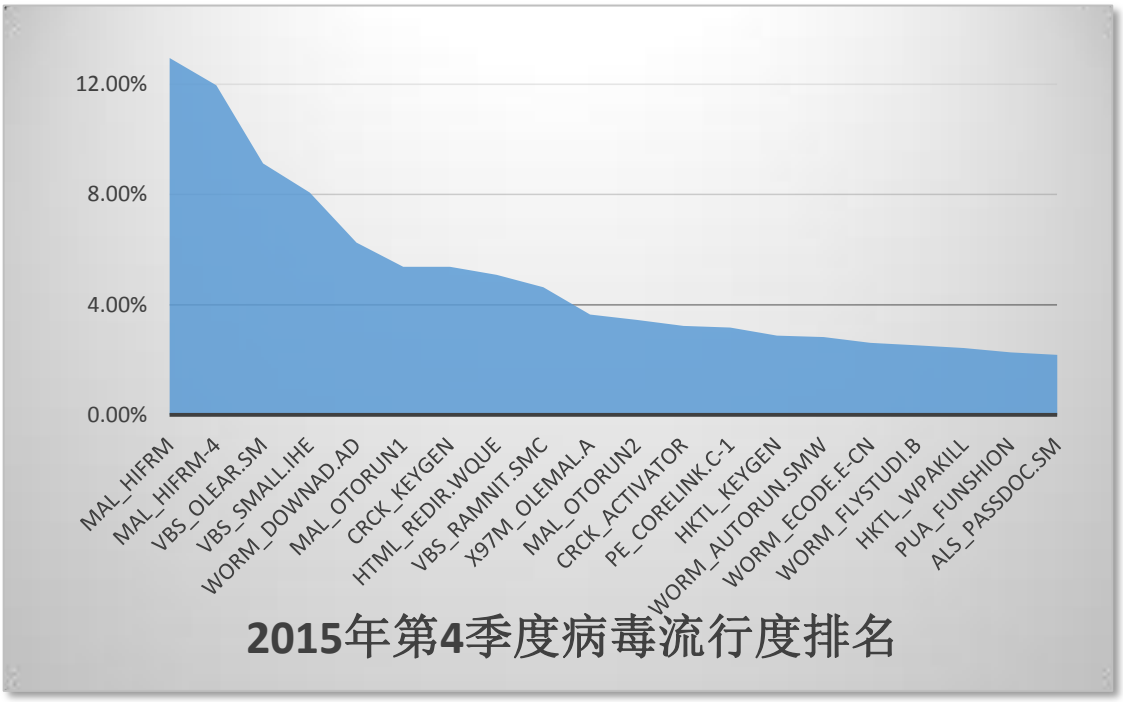
64 位 Windows 操作系统请使用：

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

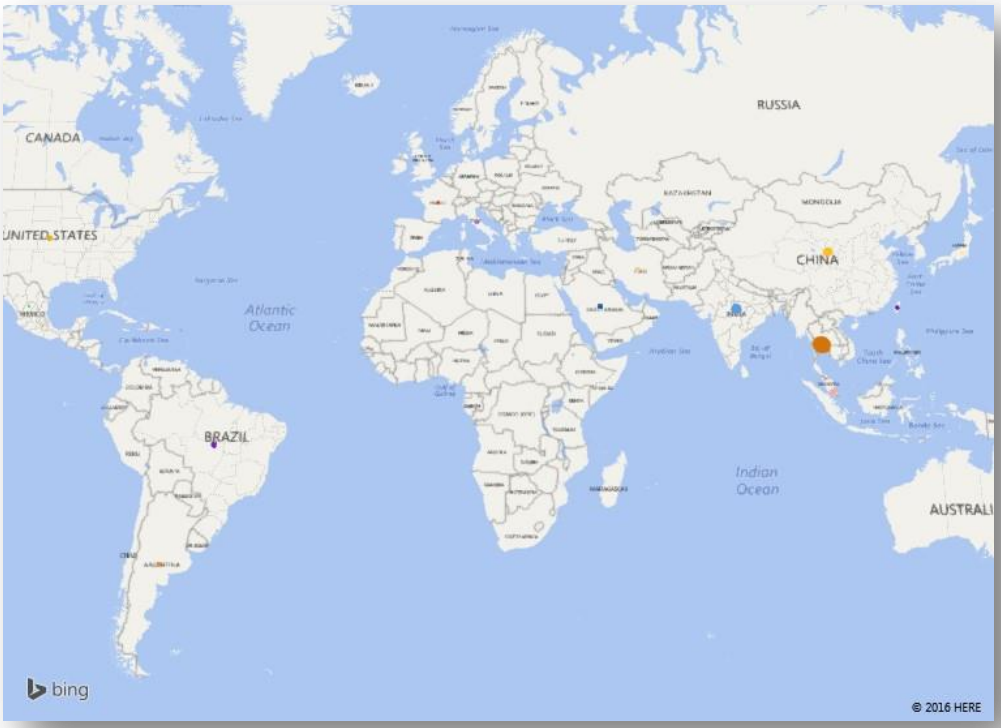
相关信息链接：

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ELF_XORDDOS.AP

2015 年第 4 季度流行病毒分析



2015 年第 4 季度流行病毒排名情况图



2015 年第 4 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， WORM_DOWNAD 在中国的感染与第三季度相比有所改善。截止 2015 年第 4 季度，约有 6.25%的用户遭受到此病毒的攻击。

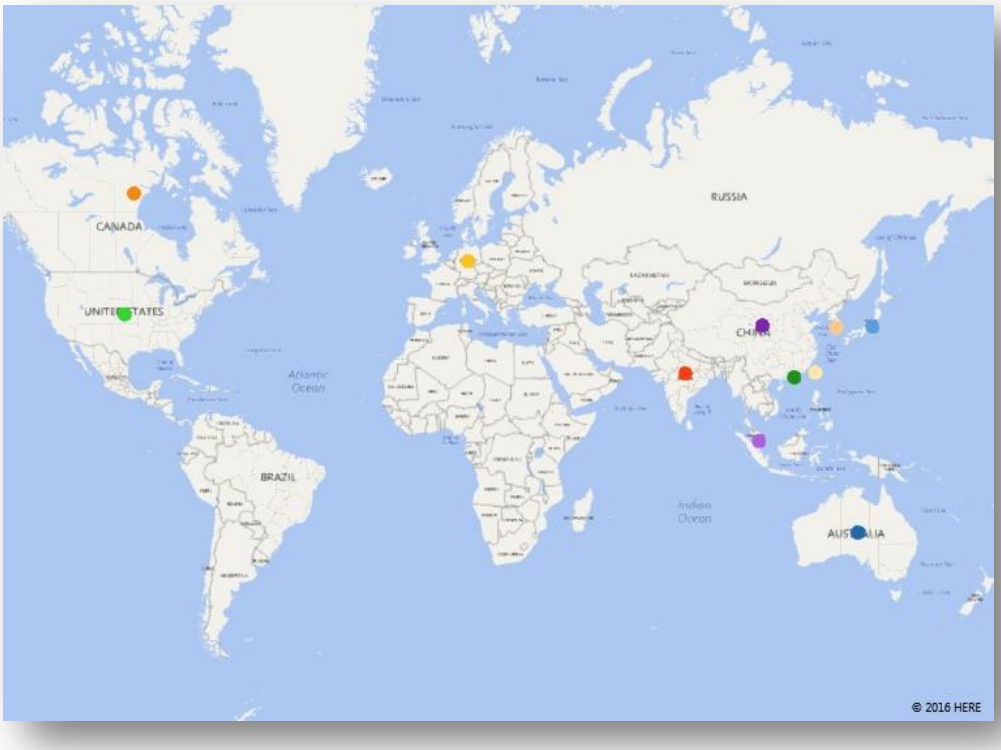
WORM_DOWNAD 病毒的持续流行与用户所处环境和使用习惯有一定联系，虽然目前的防毒产品均可以检测并处理该病毒，但该病毒依然屡见不鲜。

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 4 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 4 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

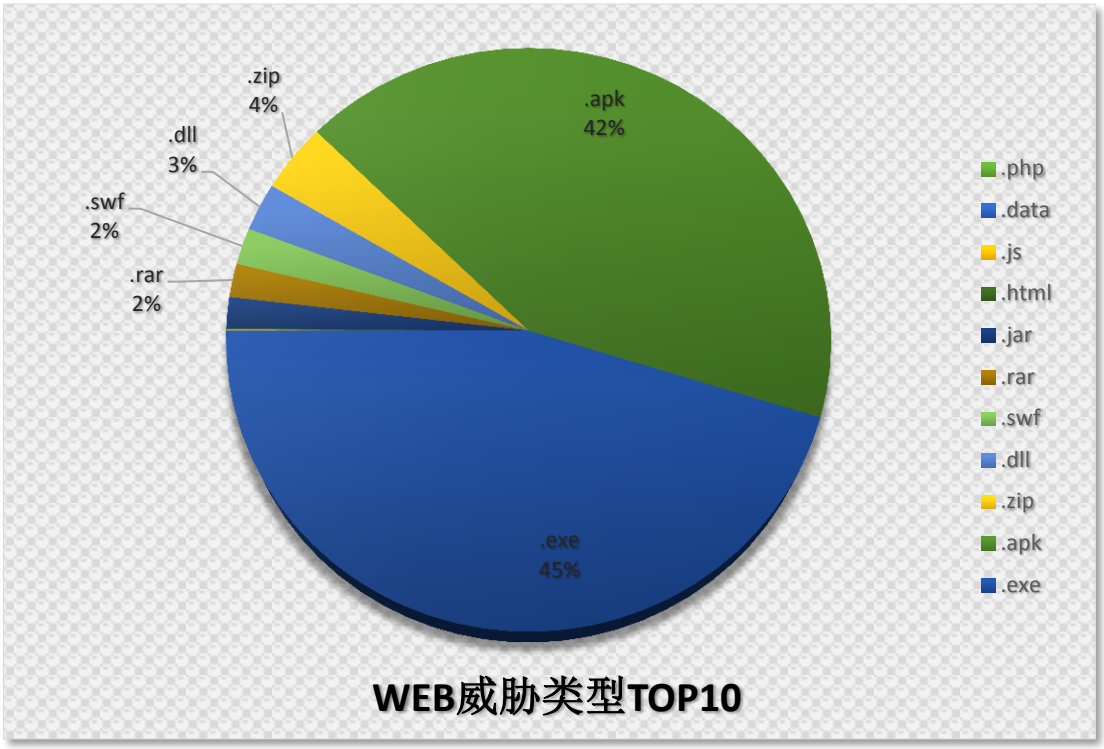
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2015 年第 4 季度 WEB 安全威胁情况

2015 年第 4 季度 WEB 威胁文件类型分析

在 2015 年第 4 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 45%，所占比例比上一季度 42.5%的占比有所上升。.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。

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.ZIP 类型的文件位居第三位。



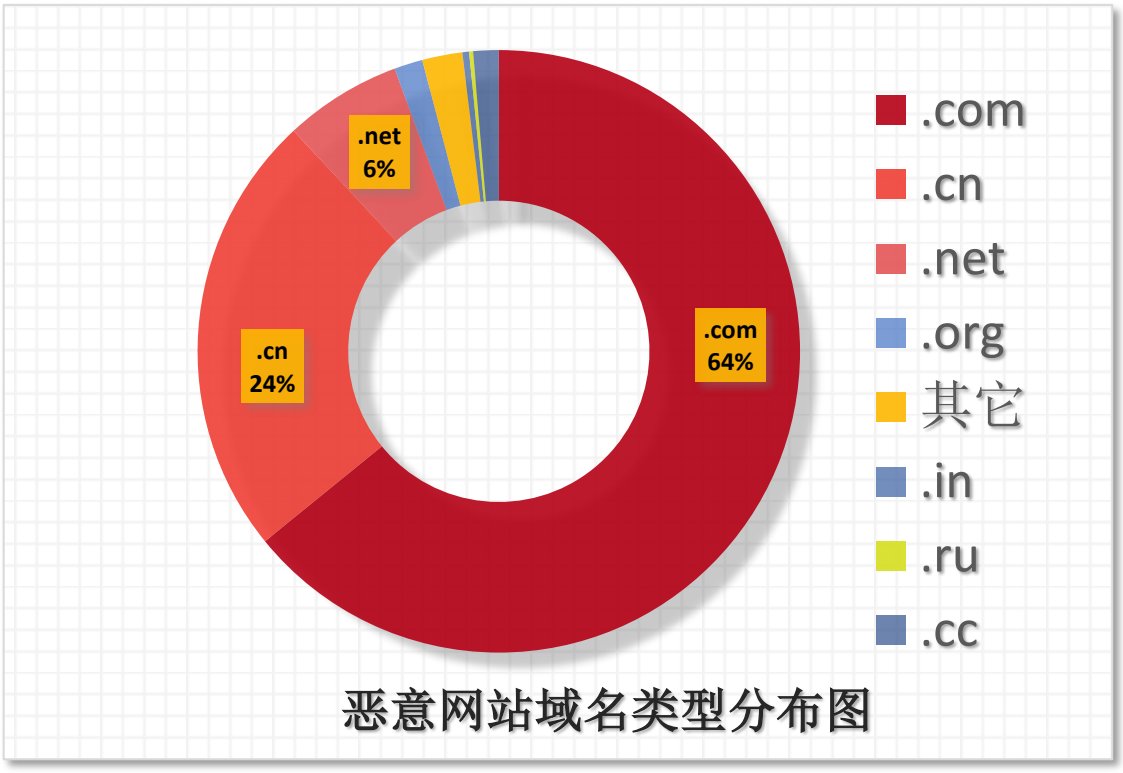
2015 年第 4 季度中国地区 WEB 威胁文件类型分布图

2015 年第 4 季度 TOP 10 恶意 URL

TOP10 恶意 URL		
恶意 URL	描述	点击量
http://down***d.2345.cn/2345zhushou/2345zhushou_v2.7.5194_silent.exe	网站直接或间接帮助传播恶意软件或恶意代码	1,829,001
http://downl***.2345.cn/2345pcsafe/2345PCSafe_shouye.exe	网站直接或间接帮助传播恶意软件或恶意代码	1,266,650
http://download.***5.cn/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	993,138
http://220.***.141.104/msvquery	网站直接或间接帮助传播恶意软件或恶意代码	925,201
http://106.***.167.7/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	830,363
http://106.120.***.15/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	830,287
http://106.120.***.175/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	828,824
http://106.***.167.9/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	826,376
http://106.120.***.29/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	825,142
http://106.120.***.177/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	824,695

2015 年第 4 季度中国地区 WRS 拦截恶意 URL 排名 TOP10

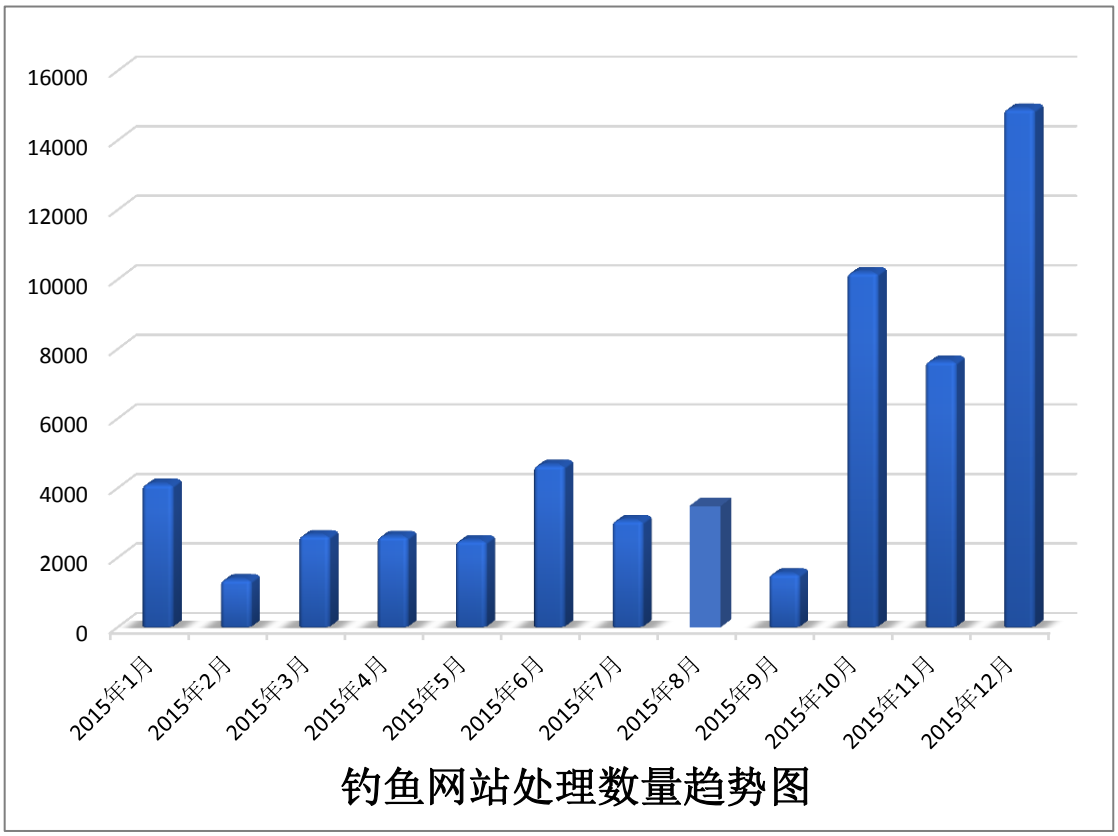
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。



2015 年第 4 季度恶意网站域名类型分布图

2015 年第 4 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 94.00 %。其中.COM 域名的恶意网页数量最多。

2015 年第 4 季度 WEB 威胁钓鱼网站仿冒对象分析



2015 年第 4 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 1 月至 2015 年 12 月的一年中，处理钓鱼网站共计 **58,660** 个。

2015 年第 4 季度中钓鱼网站数量成大幅增长趋势。由于第 4 季度钓鱼网站数量猛增，今年以来发现钓鱼网站数量比去年有所增长。

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 4 季度中使用.COM、.CC 和.AU 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 4 季度漏洞攻击威胁情况

TOP10 漏洞	
漏洞名称	检测数量
CVE-2008-4250	328267
CVE-2010-0806	134
CVE-2010-2568	82
CVE-2010-3340	78
CVE-2010-3343	78
CVE-2010-3962	78
CVE-2010-3333	51
MS08-067	44
CVE-2010-3342	39
CVE-2010-3345	39

2015 第 4 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*
CVE-2010-3340	*http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3340*
CVE-2010-3343	*http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3343*
CVE-2010-3962	*http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3962*
CVE-2010-3333	*http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333*
MS08-067	*http://technet.microsoft.com/zh-CN/security/bulletin/ms08-067*
CVE-2010-3342	*http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3342*
CVE-2010-3345	*http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3345*

漏洞介绍链接

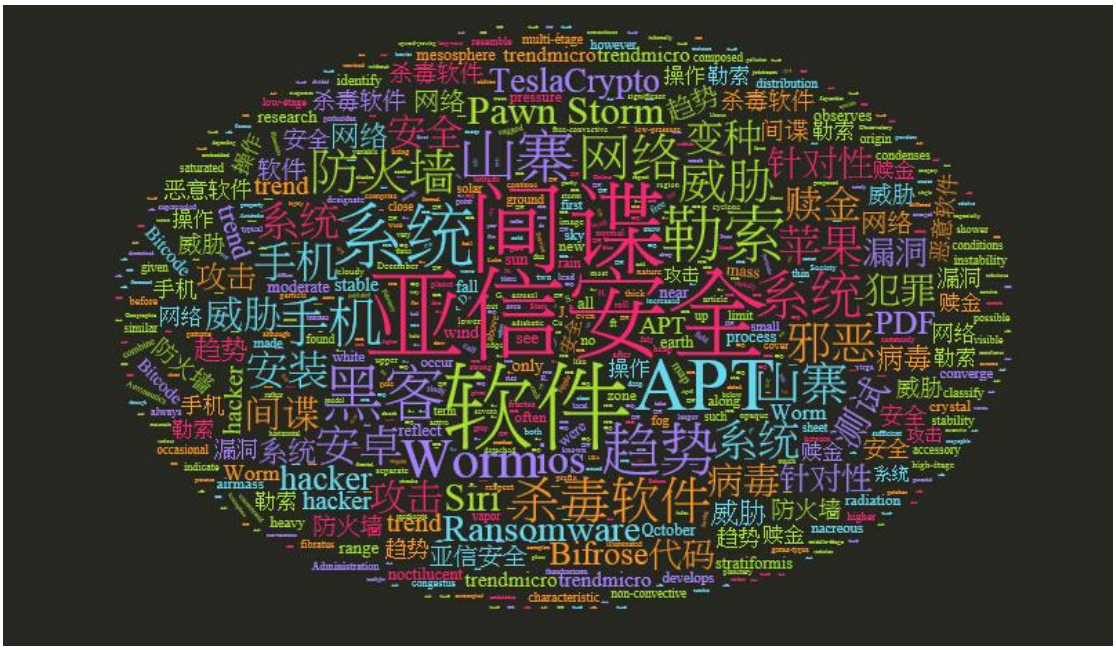
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

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 4 季度最新安全威胁信息

2015 年第 4 季度安全威胁信息摘要



2015 年第 4 季度国内外安全威胁信息关键词

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。

❖ 都是山寨惹的祸 最邪恶安卓恶意程序肆虐网络

最近，幽灵推、a.expense.GhostPush.a 等号称史上“最邪恶”的安卓恶意软件刷爆了朋友圈，这些恶意软件除了具备推送恶意广告、强行安装推广软件等恶意行为之外，还具备一个共同特征，那就是他们往往借助“山寨应用”进行传播。面对如此高风险的病毒，趋势科技建议用户养成良好的应用下载习惯，并使用趋势科技移动安全个人版等具备山寨软件鉴别功能的安全软件进行防范。

http://www.trendmicro.com.cn/cn/about-us/newsroom/releases/articles/20151103091301.html

❖ Pawn Storm 网络间谍行动再度现身

我们最新发现 Pawn Storm 网络间谍行动利用最新的 Adobe Flash 漏洞对全球展开攻击，此漏洞目前确认影响 Adobe Flash Player 19.0.0.185 及 19.0.0.207 这两个版本，多个国家的外交部成为此番攻击的目标。Pawn Storm 是一项兼具深度与广度的持续性网络间谍行动，自 2007 年开始即专门针对一些知名机构和人士，政府机关或是媒体名人等都在攻击目标之列。近年来各国外交部则成为 Pawn Storm 锁定的攻击目标。

http://blog.sina.com.cn/s/blog_5e96245b0102vws9.html

❖ 苹果漏洞：Siri 会泄露你的个人资料！

如果我告诉你，只要 30 秒，就可以让任何人从你朋友的苹果设备上开启 Siri 功能，然后拿到你的姓名、电子邮件地址、电话号码甚至是你的照片，你会担心吗？

苹果智能设备上的 Siri 可能被滥用的情况是会让任何人使用语音识别来取得设备上的数据，即便你已经设定密码。

http://blog.sina.com.cn/s/blog_5e96245b0102w11m.html

❖ 见识新勒索软件家族的新招数

Crytowall 4.0 提高了隐形能力：新的 Cryptowall 让加密勒索软件 Ransomware 变种通讯能力加强，并且更新程序代码让它能够攻击更多漏洞。也有报告指出此次更新还包括通讯协议修改，提高了它的隐形能力。

Power Worm 支付赎金仍无法解决问题：

Ransomware 的新变种被发现加密过程有缺陷，原因是开发者的程序撰写错误。该缺陷基本上会“扔掉”网络犯罪分子应该掌握好让用户可以支付赎金来交换的加密密钥。也就

是说，文件被加密后将无法恢复。支付赎金已经无法解决问题，备份是唯一的解决方案。

可脱机执行的勒索软件：早在去年就发现其攻击俄罗斯用户，这种勒索软件 Ransomware 能够脱机执行而无需连到 C&C 服务器。它会储存加密用 RSA 公钥到被加密文件的元数据内。所以当用户决定付钱，需要至少发送一个加密过的文件到攻击者的电子邮件，让攻击者可以制造基于储存在所发送文件内公钥的解密程序。

Chimera 威胁不付赎金就在网络上散布：全新的勒索软件 Ransomware，Chimera 不只是将用户的文件作为人质，还威胁如果不付赎金就会在网络上散布。然而，分析恶意软件后发现该恶意软件不能窃取任何东西或发送任何加密文件到云端，说明这很有可能只是种恐吓的手法。

http://blog.sina.com.cn/s/blog_5e96245b0102w1nn.html

❖ 【针对性攻击】分工之细，你能否招架的住？

我们最近发现了一起由资金雄厚的黑客组织所发动的网络间谍攻击行动，主要锁定目标群体为亚洲一些重要产业当中与政府有密切关系的民间企业，包括：民营化政府机构及政府承包商，此外还有消费性电子、计算机、医疗、金融等产业。

该组织财力雄厚，足以买下某个热门恶意软件工具的源代码，同时拥有充足的人力根据这份程序代码开发出自己的改良版本，下面就给大家简单介绍一下。

BIFROSE (亦称为 Bifrost) 恶意软件过去在地下市场上的售价高达 10,000 美元。在一起“针对政府机构的攻击”和”Here You Have Mail”(您有来信) 垃圾邮件行动当中我们曾相逢过，尽管 BIFROSE 的网络封包和行为已经广为业界所知，但该组织仍有办法在其攻击行动当中充分运用这个恶意软件。

http://blog.sina.com.cn/s/blog_5e96245b0102w31x.html

❖ 无意间把你的个人资料当圣诞礼物,送给了网络犯罪份子吗?

Merry christmas~又是一年圣诞节！今年的苹果红又甜，三亚的冬天不下雪……各类社交应用又到了恋爱秀优越，单身晒狗粮，土豪秀礼物的红火时刻。但是各类网络犯罪份子也在暗处伺机而动，虽然晒晒更健康，但大家也要注意防范，别一不小心把自己的个人资料当成圣诞礼物，送给了网络犯罪份子。

http://blog.sina.com.cn/s/blog_5e96245b0102w2w9.html

❖ 英国新闻网站“独立报”被黑客攻击,导致 TeslaCrypto 勒索事件

英国著名独立报的网站已被挂马，这可能使数以百万计的读者在受勒索的风险。

我们已经通知了独立报这一安全事件，并与他们一起工作以消除此风险。

http://blog.trendmicro.com/trendlabs-security-intelligence/blog-of-news-site-the-independent-hacked-leads-to-teslacrypto-ransomware/

❖ 攻击者团队合作并购买 Bifrose 代码

最近,我们发现了一个由有组织的集团发起的新的网络间谍攻击，目标为亚洲的政府和重点行业。这些目标包括私有化政府机构和政府承包商,以及消费电子、计算机、医疗和金融行业。

http://blog.trendmicro.com/trendlabs-security-intelligence/new-targeted-attack-group-buys-bifrose-code-works-in-teams/

❖ Moplus SDK 记录和虫洞漏洞

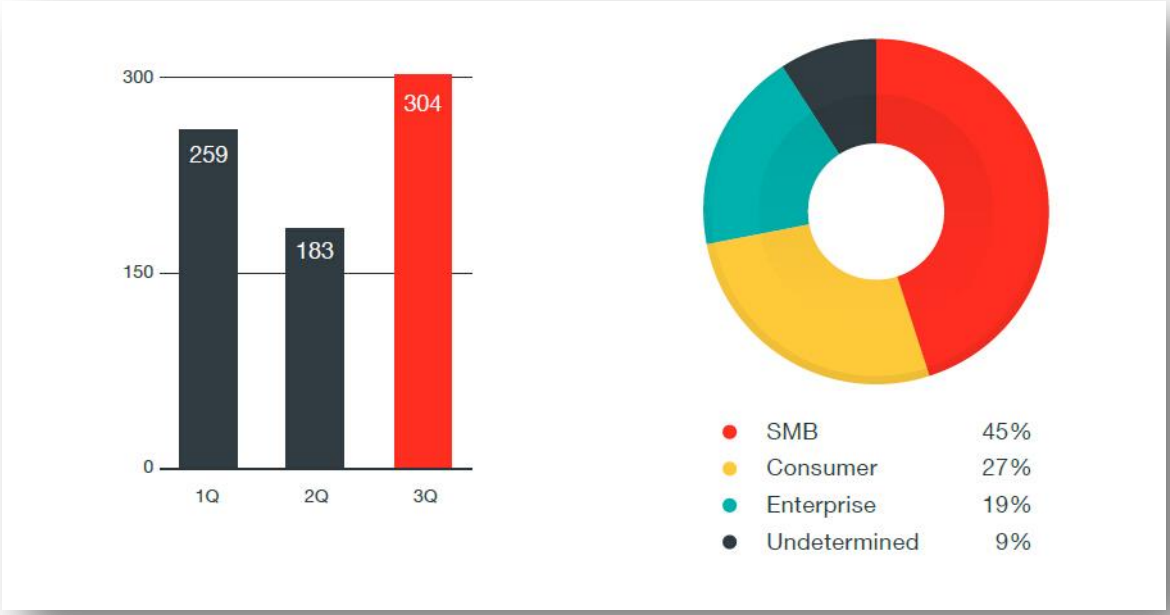
一种被称为虫洞，影响软件开发工具包(SDK)的漏洞 Moplus，正通过百度兴风作浪，一旦成功利用该漏洞将产生严重的影响。该漏洞被中国的一个漏洞报告平台 WooYun.og 发现。

http://blog.trendmicro.com/trendlabs-security-intelligence/setting-the-record-straight-on-moplus-sdk-and-the-wormhole-vulnerability/

全球区最新安全威胁概要

以下是来自 2015 年第 3 季度全球区安全报告的数据。

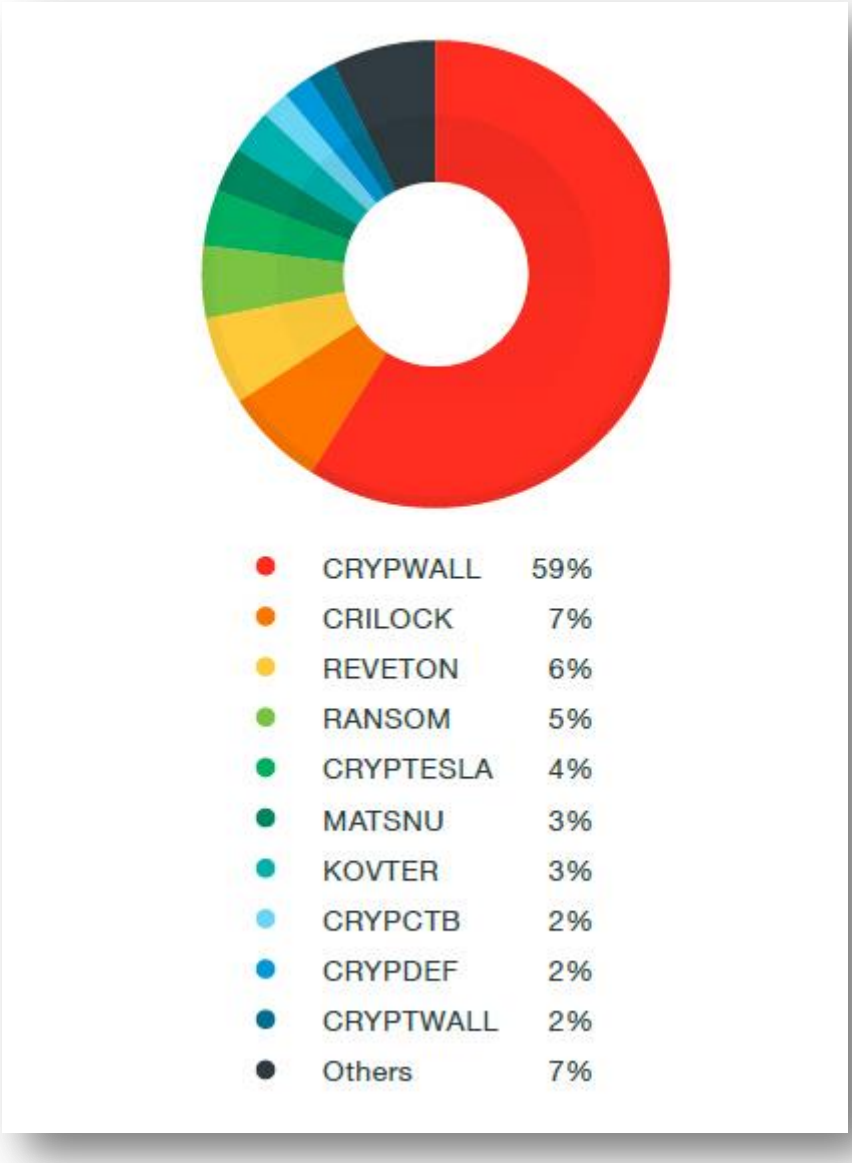
下图是 2015 年第 1 季度到 2015 年第 3 季度期间的 PoS 恶意软件威胁检测表，第三季度总量比第二季度增加 66%,究其原因可能是因为攻击者使用了霰弹枪方法，发现中小企业是最易牟取利益的受害群体。



PoS 恶意软件检测数据和分布图

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。

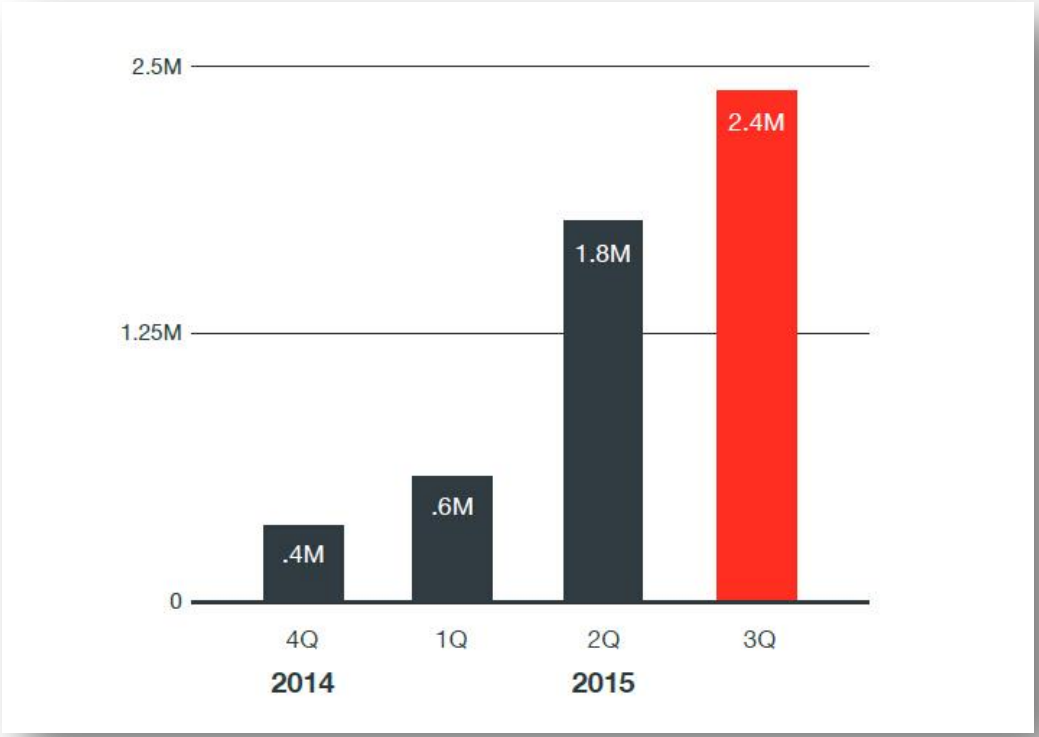
2015 年第 3 季度勒索软件家族数量排名显示，与上季度相比，CRYPWALL 勒索软件家族在本季度快速增长，占据了总数过半。



勒索软件家族数量排名表

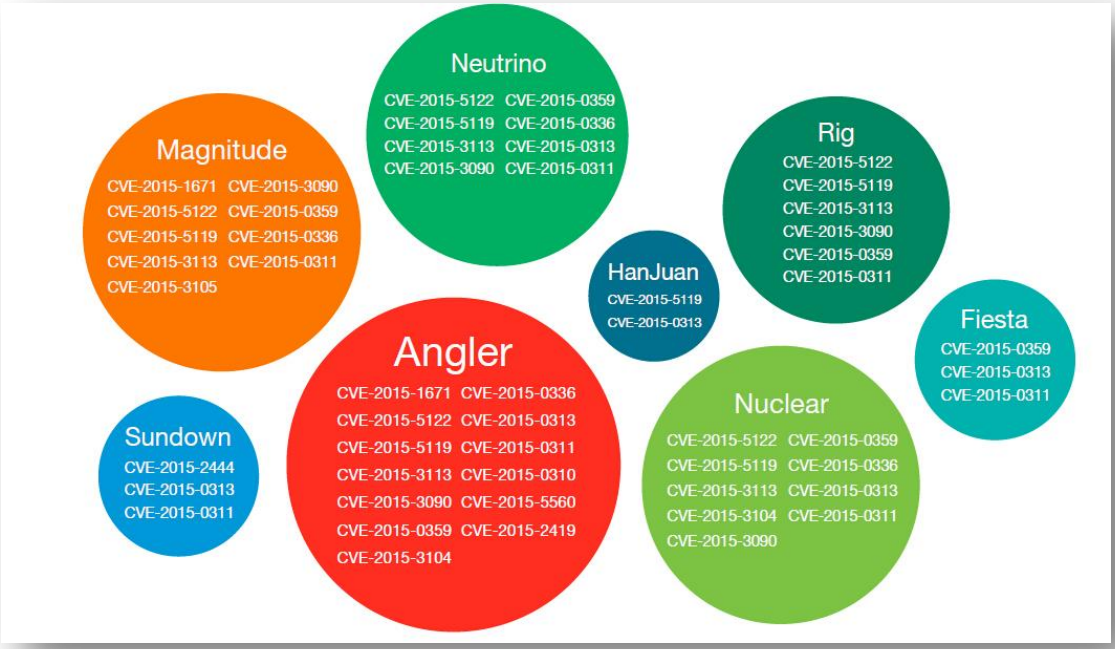
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

从下图可以看到，今年2 季度到3 季度，访问Angler 漏洞利用工具包托管URL 的访问量增加30%，其仍然是最为活跃的漏洞利用工具包。



Angler **漏洞利用工具包托管 URL 数量**

Angler 漏洞利用工具的开发者非常活跃，不断推出新版本，其将会集成更多的 Adobe Flash 漏洞到漏洞利用工具包中。



2015 年 1-3 季度漏洞利用工具包示意图

需要查看更完整的 2015 年第 3 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。

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