AsiaInfo 亚信安全

中国地区 2016 年
第一季度
网络安全威胁报告

2016/04

CHINA RTL

目录

2016 年第 1 季度安全威胁

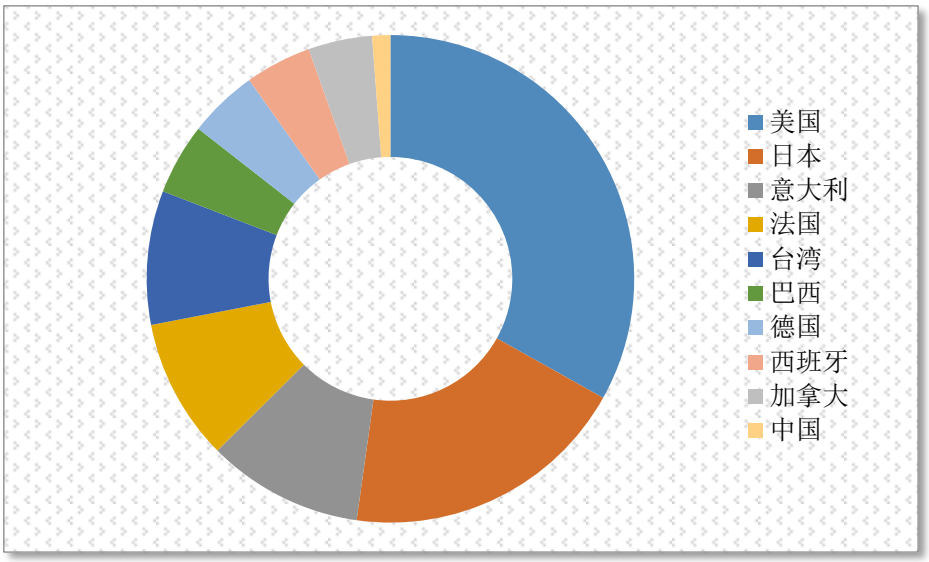
本季安全警示：

勒索软件

2016 年第 1 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 **21** 万条。截止 2016.3.31 日中国区传统病毒码 **12.436.60** 包含病毒特征数约 **434** 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 **17,030** 万次。
- 本季度亚信安全在中国地区拦截的恶意 URL 地址共计 **306,742** 次。

本季度热点话题为勒索软件病毒。本季度勒索软件病毒在全球爆发，其已经成为威胁企业安全的头号病毒。给企业带来巨大灾难的同时，却给攻击者带来巨大的收益，因其使用比特币进行交易，很难追踪。FBI 建议感染勒索软件的用户通过支付赎金进行解密，目前来看，即使支付赎金也不一定能保证可以完全恢复被加密的文件。下图是勒索软件全球感染情况

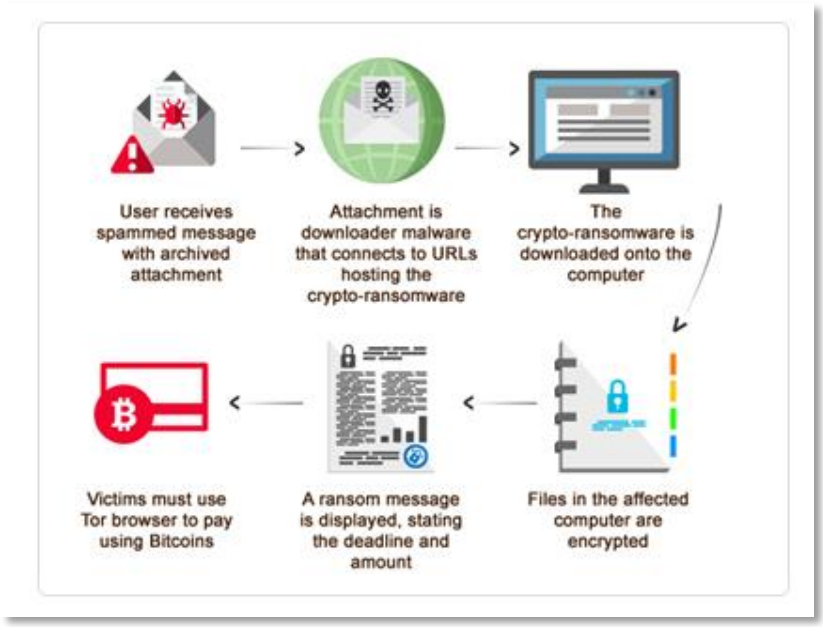


勒索软件全球感染分布图

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。

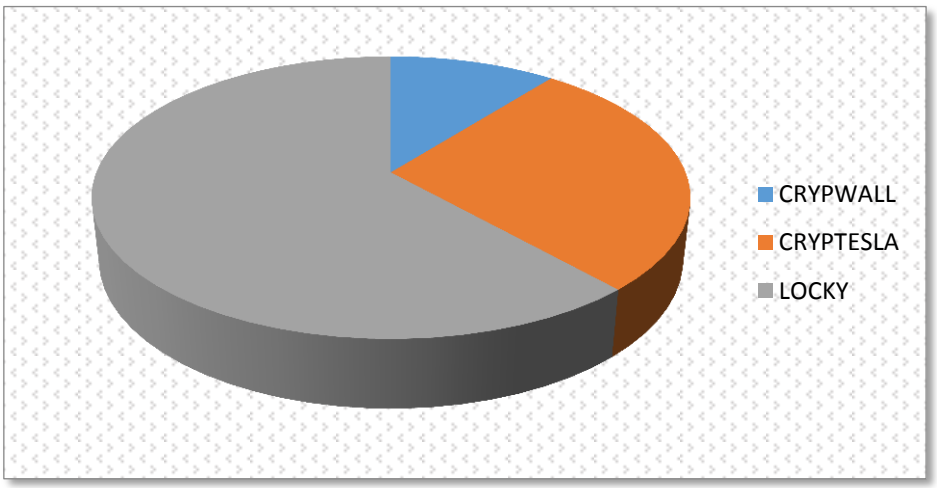
随着勒索软件白热化升级，亚信安全深入研究发现其不仅从代码结构方面有变化，而且感染方式更加多元化，勒索软件使用的语种更加丰富，本地化趋势明显。 本季度我们发现的勒索软件可以支持多数主流系统，不仅是 PC，还包括移动设备。如：Windows，OS X，Linux，IOS，android。

其传播方式从最初的鱼叉式钓鱼邮件，到目前的漏洞利用传播，软件捆绑安装等，增加了用户预防感染勒索软件的难度。



勒索软件感染过程示范图

本季度感染数量最多勒索软件变种是 LOCKY，位居其后的是 CRYPTESLA 和 CRYPWALL。



勒索软件感染数量图

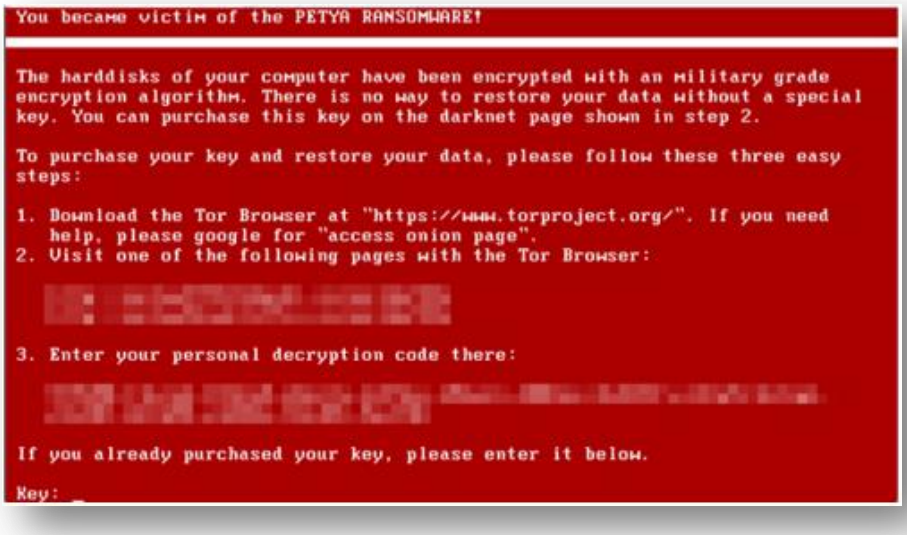
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

LOCKY 通过带有 JS（JavaScript）压缩包附件的邮件进行传播，病毒附件一旦被运行，用户计算机上的文档文件会被加密导致无法打开，同时会加密网络中可访问的网络共享文件。亚信安全提醒用户，切勿打开来历不明的电子邮件，运行其附件。如下是勒索邮件示例

勒索邮件示例图

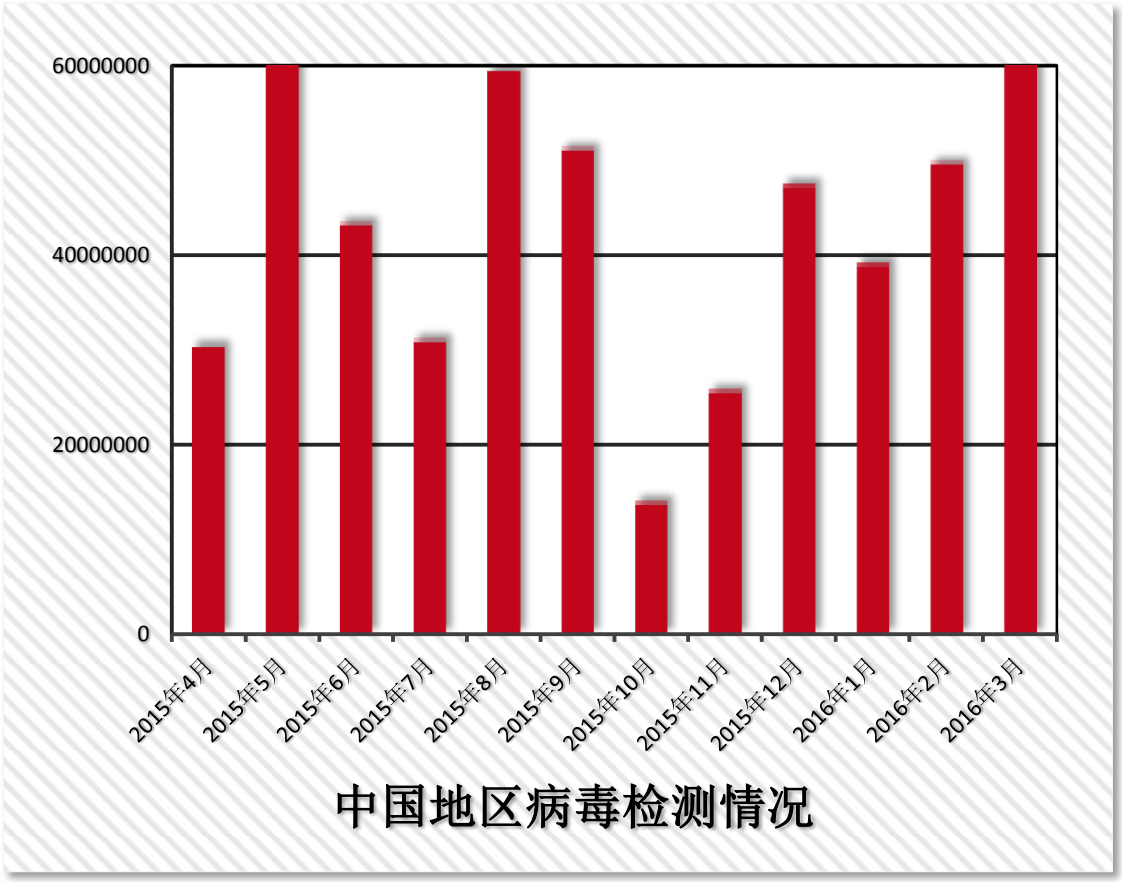
PETYA 是新型勒索软件，其不仅可以覆盖受影响系统的主引导记录（MBR），锁定用户，而且其可以通过合法的云存储服务感染用户（例如，通过 Dropbox）。Petya 一旦感染系统，已修改的 MBR 会阻止 Windows 的正常加载，而是显示一个 ASCII 骷髅图像和提示：支付一定数量的比特币，否则将失去文件和计算机的访问权限。

接下来会显示支付赎金解密文件的指导说明：



通过查看其专业设计的 Tor 网站发现，目前赎金价格为 0.99 比特币（BTC）或 US$431 如果错过了屏幕显示的截止日期，赎金价格将会翻倍。

PETYA 网站

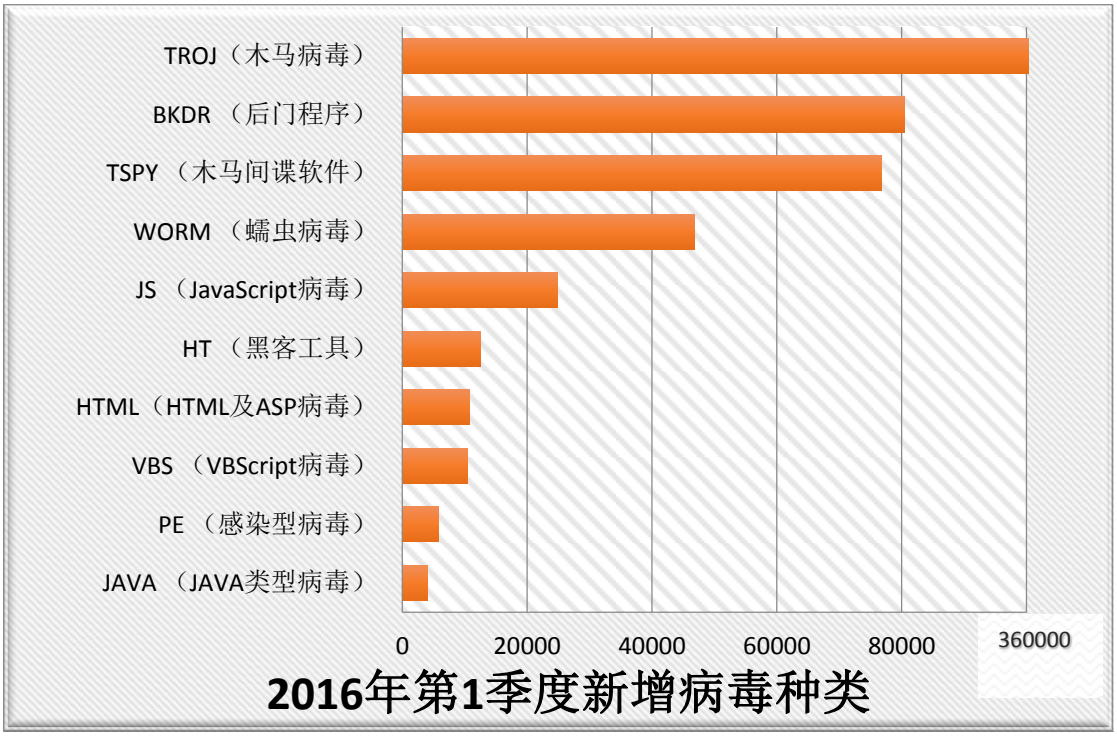


2016 年第 1 季度中国地区病毒检测数量图

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。

2016 年第 1 季度病毒威胁情况

2016 年第 1 季度新增病毒类型分析



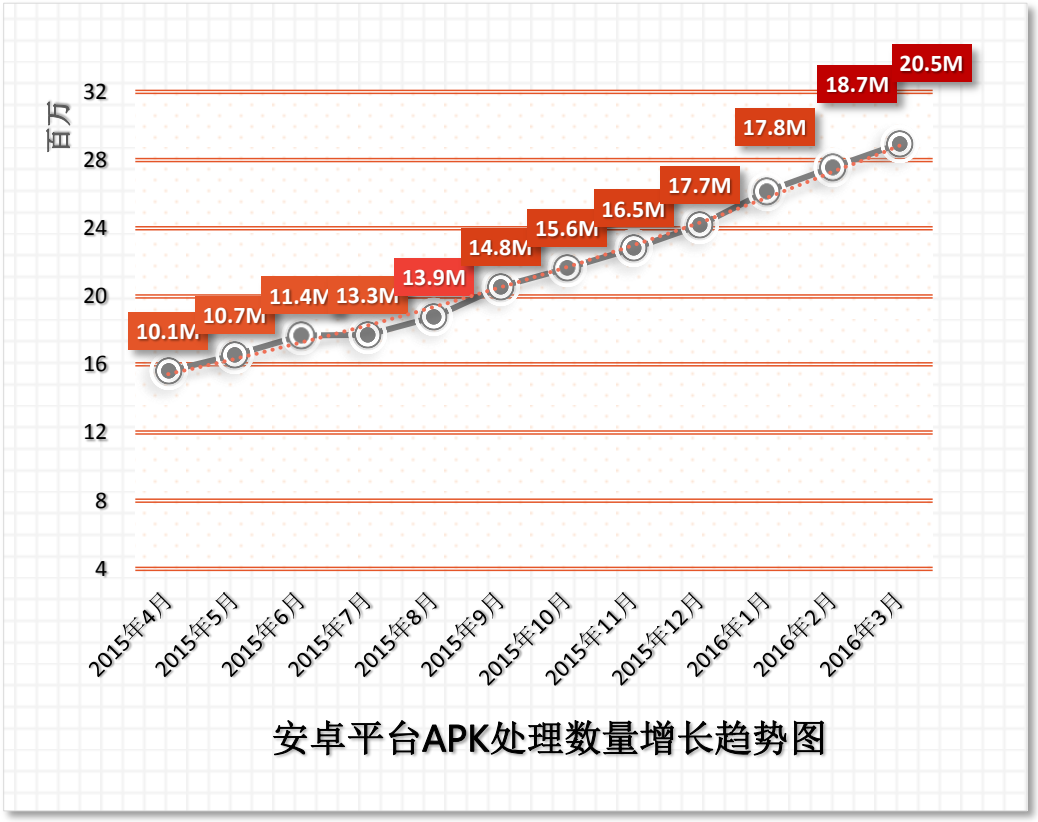
2016 年第 1 季度新增病毒类型分布图

在 2016 年第 1 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 365,209 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 TROJ(木马病毒)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。

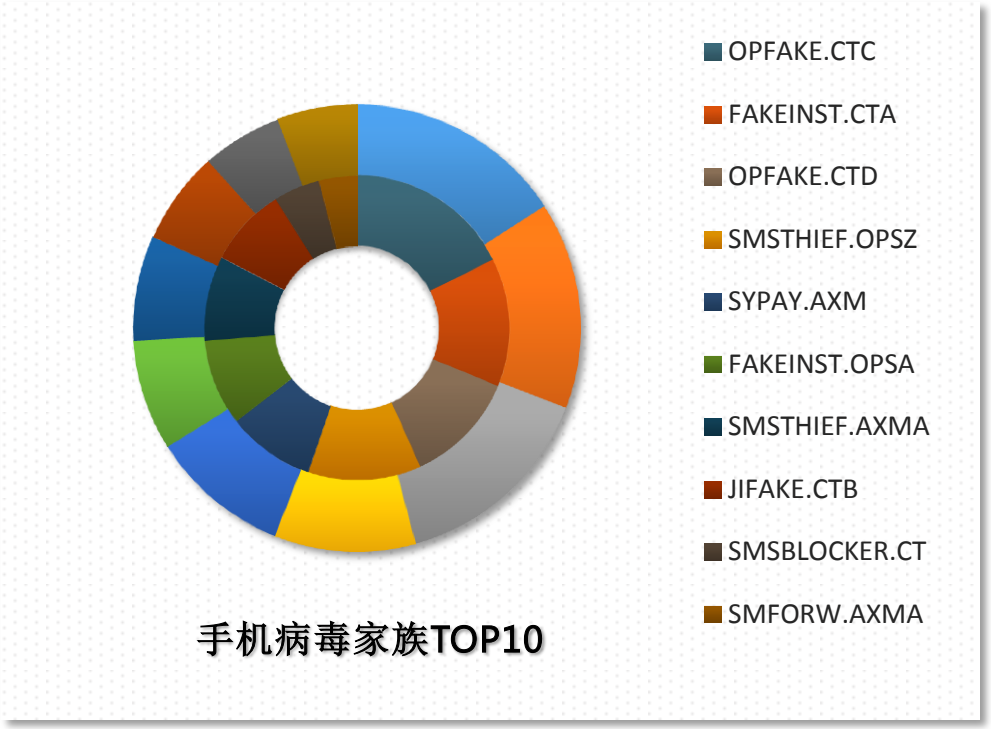
其中 JS(JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒与网页挂马有关，网页挂马是攻击者常用攻击类型。一些正常网站由于自身存在的缺陷漏洞，导致被入侵者挂马，之后浏览被挂马网页的访问者就会在毫不知情的情况下自动下载恶意文件到本地。

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。



2016 年第 1 季度安卓平台 APK 处理数量走势图

2016 年第 1 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 3 月底，处理数量累计达到 2,895 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。



2016 年第 1 季度手机病毒家族 TOP10 分布图

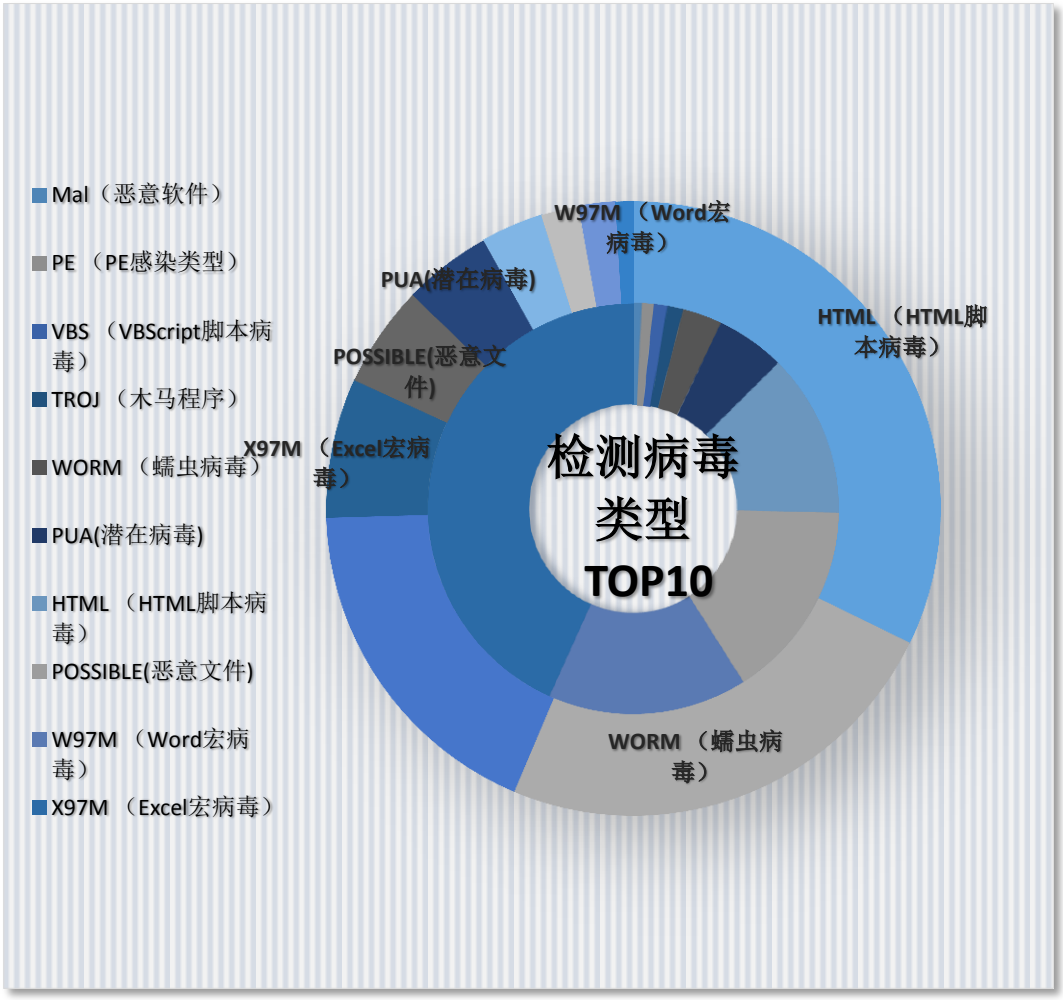
在 2016 年第 1 季度感染安卓平台的手机病毒家族中，OPFAKE 家族数量最多，占到总数的 30.76%；FAKEINST 家族位列第二位，占总数的 23.05%；SMSTHIEF 家族居第三位，占总数的 17.79%。与上季度相比，SMSTHIEF 家族涨势凶猛，而上季度排名第一的 SMSPAY 家族则有减弱趋势。

在 2016 年第 1 季度中，手机病毒持续增长趋势，随着手机 APP 广泛使用，针对手机 APP 的病毒也接踵而来，日前亚信安全发现了一款盗取苹果手机 Instagram 账号和密码的病毒 IOS_INSTASTEALER.A。

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。

亚信安全同时也监测到了针对安卓手机信息应用程序的病毒 ANDROIDOS_MSGCRACK.A，该病毒利用安卓 cve-2015-3840 漏洞对信息应用程序发起拒绝服务（DoS），如下是该病毒的恶意行为示意图：

2016 年第 1 季度各类型病毒检测情况分析



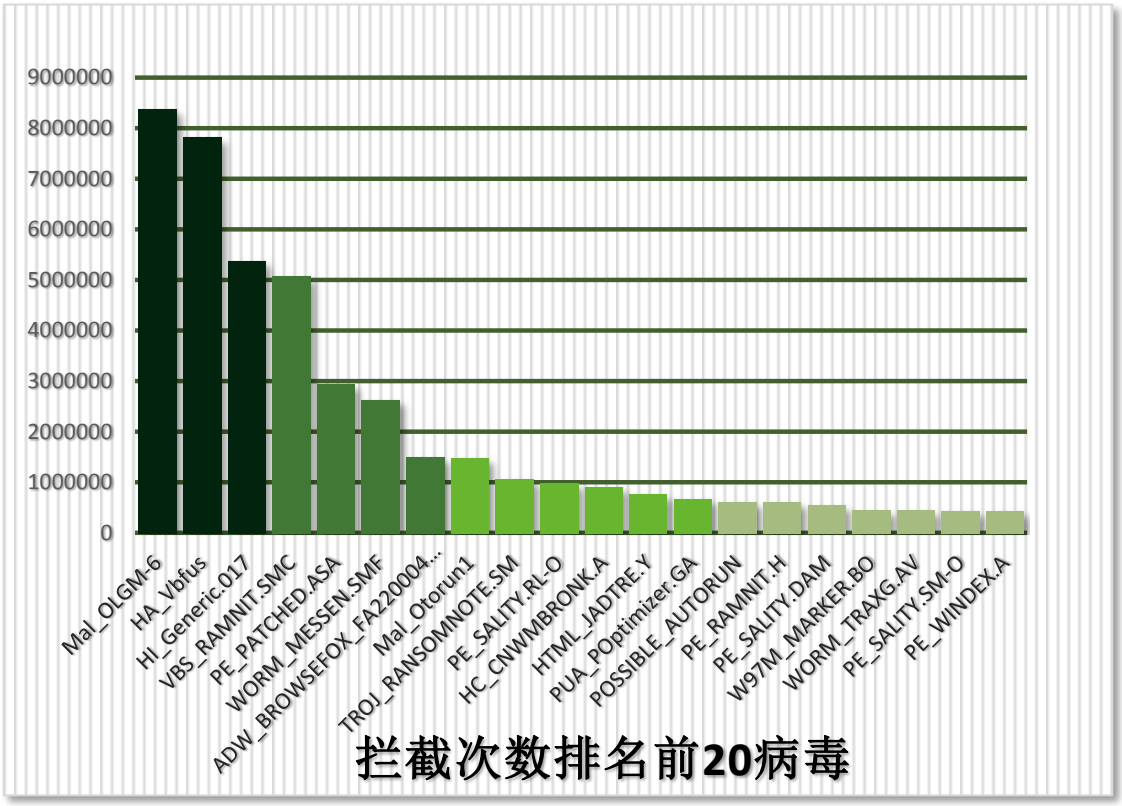
2016 年第 1 季度病毒检测类型分布图

2016 年第 1 季度检测到的病毒种类中，MAL 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 32%以上。在本季度中，Mal_OLGM-6 检测数量排名第一，此外 VBS_RAMNIT.SMC、PE_PATCHED.ASA、WORM_MESSEN.SMF 家族检测数量排名靠前。Mal_OLGM-6 病毒是盗号木马，其主要是盗取网络游戏的用户名及密码。

本季度蠕虫病毒占检测类型总数的 5.40%，本季度该类型病毒占比较上一季度有所上升。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。

2016 年第 1 季度病毒拦截情况分析



2016 年第 1 季度病毒拦截情况图

在 2016 年第 1 季度拦截次数排名前 20 位的病毒检测名中，Mal 及 PE 的感染类型病毒检测数量远高于其它检测名。

Mal_OLGM-6 在本季度被检测到的拦截次数约为 873 万多次，拦截次数位居榜首。该病毒为盗号木马，其主要是盗取网络游戏的用户名及密码。

对该病毒目前的解决方法如下（可以使用以下二种方法中的任意一种进行清理）：

- ✓ 使用 OSCE 对系统进行全盘扫描
- ✓ 使用 ATTK 工具清除该病毒

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_SALITY.RL-O，**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：

- 该病毒通常会先感染 winlogon.exe 文件从而得以驻留内存。一旦成功，它将会感染受感染电脑，包括可移动存储中的所有.EXE 和.SCR 文件。
- **PE_SALITY.RL-O** 会向 Windows\drivers 目录释放随机命名的.sys 文件，并且调用执行它。
- 其通过建立如下注册表键值达到自启动目的
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
  winlogon.exe = "%Windows%\winlogon.exe"
- 其会结束与安全相关软件的进程文件

传播途径及防护方法：

- ✓ 该病毒通过移动存储进行传播。其会在可访问的磁盘目录下生产 AUTORUN.INF 文件，内容如下

```
Note: The order of autorun.inf strings may vary and may contain a
combination of uppercase and lowercase letters.
;{garbage characters}
[AutoRun]
;{garbage characters}
shell\explore\command = {random}.{exe/pif}
;{garbage characters}
open = {random file name}.exe
;{garbage characters}
shell\open\command = {random}.{exe/pif}
shell\open\default = 1
;{garbage characters}
shell\autoplay\command = {random}.{exe/pif}
;{garbage characters}
```

- ✓ 介于该病毒首先会感染 **winlogon.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 **winlogon.exe** 的修改。

相关信息链接：

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/pe_sality.rl-o

2016 年第 1 季度热门新型病毒分析

本季度热门病毒 RANSOM_LOCKY.PUY 利用 Adobe Flash Player CVE-2016-1019 漏洞传播的勒索软件病毒。该病毒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，其会链接特定网站进行信息收发。

病毒的详细信息如下：

病毒检测名：RANSOM_LOCKY.PUY
文件类型：EXE
常驻内存： 是
病毒行为：连接 URL 下载文件，加密系统中的文件

抵达细节：

该病毒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

- ✓ 其可能由 TROJ_LOCKY.DLDRA 病毒生成
- ✓ 也可能从 http://our.{BLOCKED}hasanjay.com.np/bg.gif 下载到达本机

安装：

该病毒生成如下文件：

- ✓ %Desktop%_HELP_instructions.txt
- ✓ %Desktop%_HELP_instructions.bmp
- ✓ {folders containing encrypted files}_HELP_instructions.txt

其也会生成自身拷贝文件：

- ✓ %User Temp%\svchost.exe

自启动：

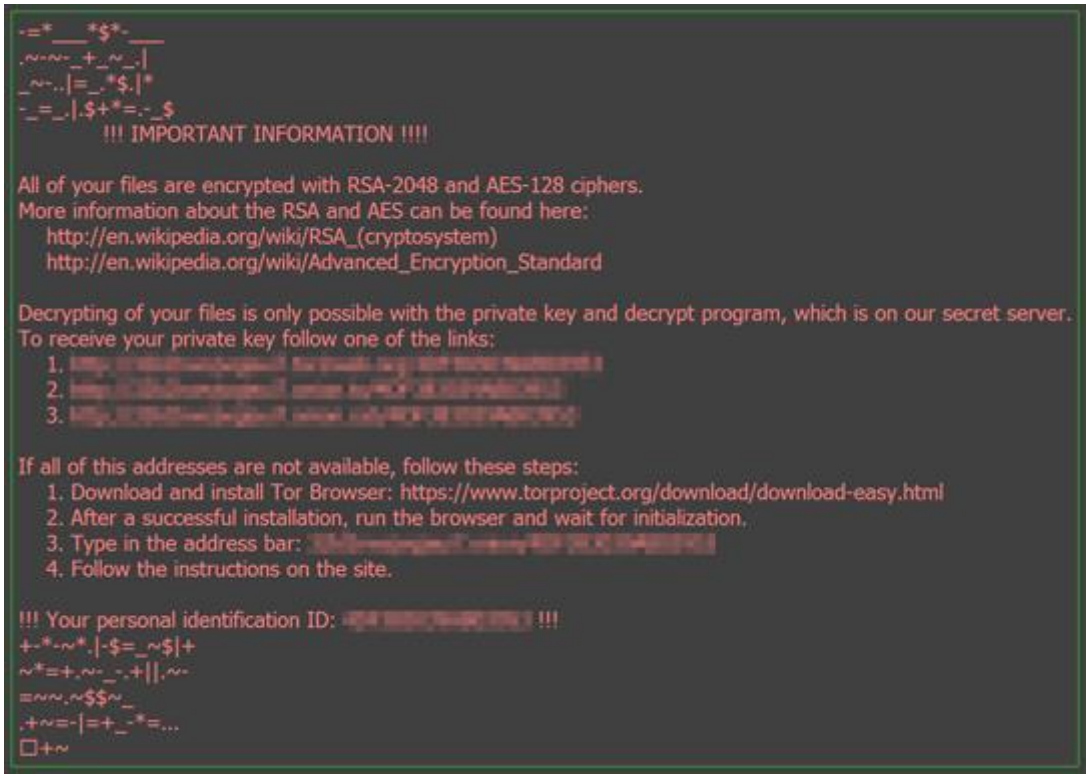
该病毒通过添加如下注册表项目达到自启动目的：

```
HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
Locky = "%User Temp%\svchost.exe"
```

系统修改：

该病毒修改系统中如下文件：

- ✓ 加密硬盘及可移动硬盘中的文件
- ✓ 被加密的文件将会被改名，其命名规则 {unique ID per victim}{identifier}.locky
- ✓ 将下图设置为桌面墙纸



其它细节：

该病毒链接如下网址发送接收信息

- ✓ http://{BLOCKED}.{BLOCKED}.181.164/submit.php
- ✓ http://88.198.119.177/submit.php

该病毒加密如下扩展名文件：

.n64 .flv .asf .swf .vmx .bz2 .7z .bmp .jpg .bat .asp .m4u .3g2 .mpeg .wav .gpg .tbk .rar .png .tif .sh .csm3u .mkv .vob .mp3 .aes .bak .zip .gif .tiff .class .brd .mid .3gp .mpg .qcow2 .ARC .tar .djv .raw .NEF .jar .schwma .mp4 .wmv .vdi .PAQ .tgz .djvu .cgm .psd .java .dchavi .mov .fla .vmdk .tar .gz .svg .jpeg .cmd .rb .dip .pl .vbs .vb.js.h.asm.pas.cpp .c .php .ldf .mdf .ibd .MYI .MYD .frm .odb .dbf .db .mdb .sql .SQLITEDB .SQLITE3 .lay .ms11 .sldm .sldx .ppsm .ppsx .sxm .otg .odg .uop .potx .potm .pptx .pptm .std .sxd .pot .pps .sti .sxi .otp .odp .wb2 .123 .wks .wk1 .xltx .xltm .xlsx .xlsm .xlsb .slk .xlw .xlt .xlm .xlc .dif .stc .sxc .ots .ods .hwp .602 .dotm .dotx .docm .docx .DOT .3dm .max .3ds .xml .txt .CSV

解决方法：

1. 亚信安全防防毒墙网络版(Officescan) 11.0 SP1 的行为监控功能有效拦截勒索软件
2. 亚信安全的 DDEI、DE、IMSA、IMSS 可有效拦截勒索软件
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

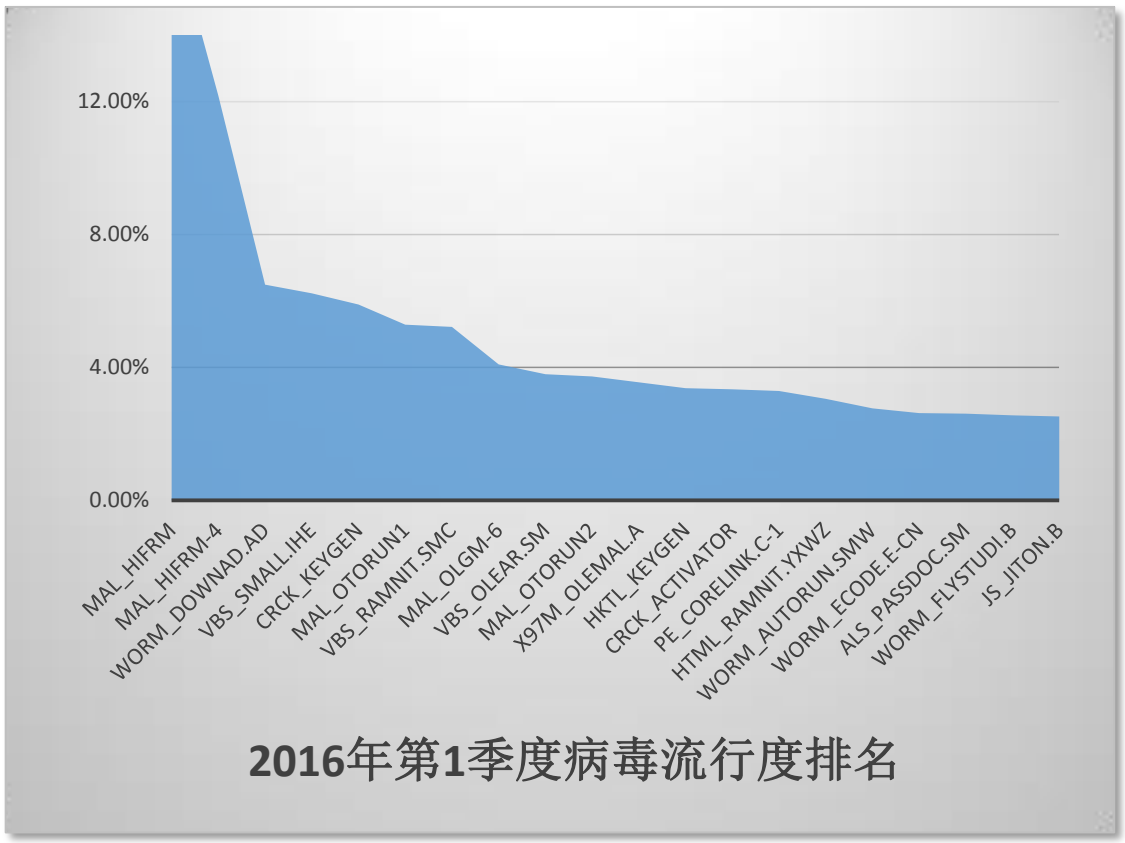
64 位 Windows 操作系统请使用：

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/ransom_locky.puy

2016 年第 1 季度流行病毒分析



2016 年第 1 季度流行病毒排名情况图

2016 年第 1 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 在中国的感染上季度相比有所改善。截止 2016 年第 1 季度，约有 6.49%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 2016 年第 1 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。

2016 年第 1 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

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。

（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

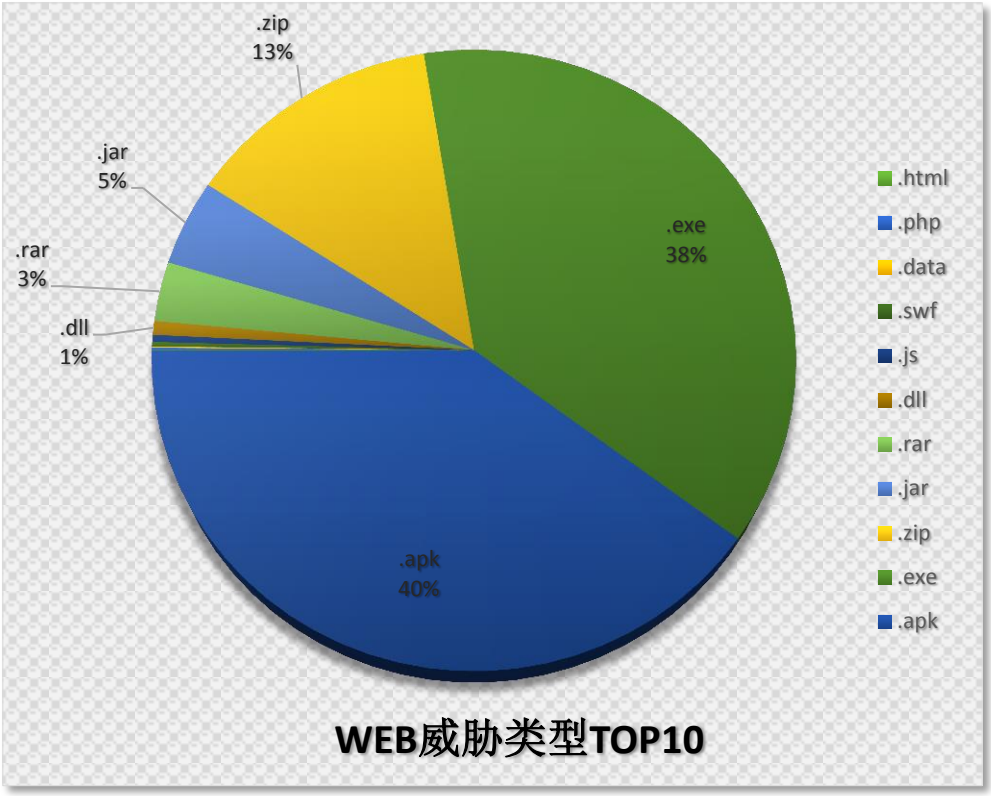
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2016 年第 1 季度 WEB 安全威胁情况

2016 年第 1 季度 WEB 威胁文件类型分析

在 2016 年第 1 季度的数据中，通过 WEB 传播的恶意程序中，.APK 类型的可执行文件占总数的 40%，所占比例比上一季度 42.5%的占比有所下降。.APK 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，.EXE 文件所占比例居高不下，此外.ZIP 类型的文件位居第三位。

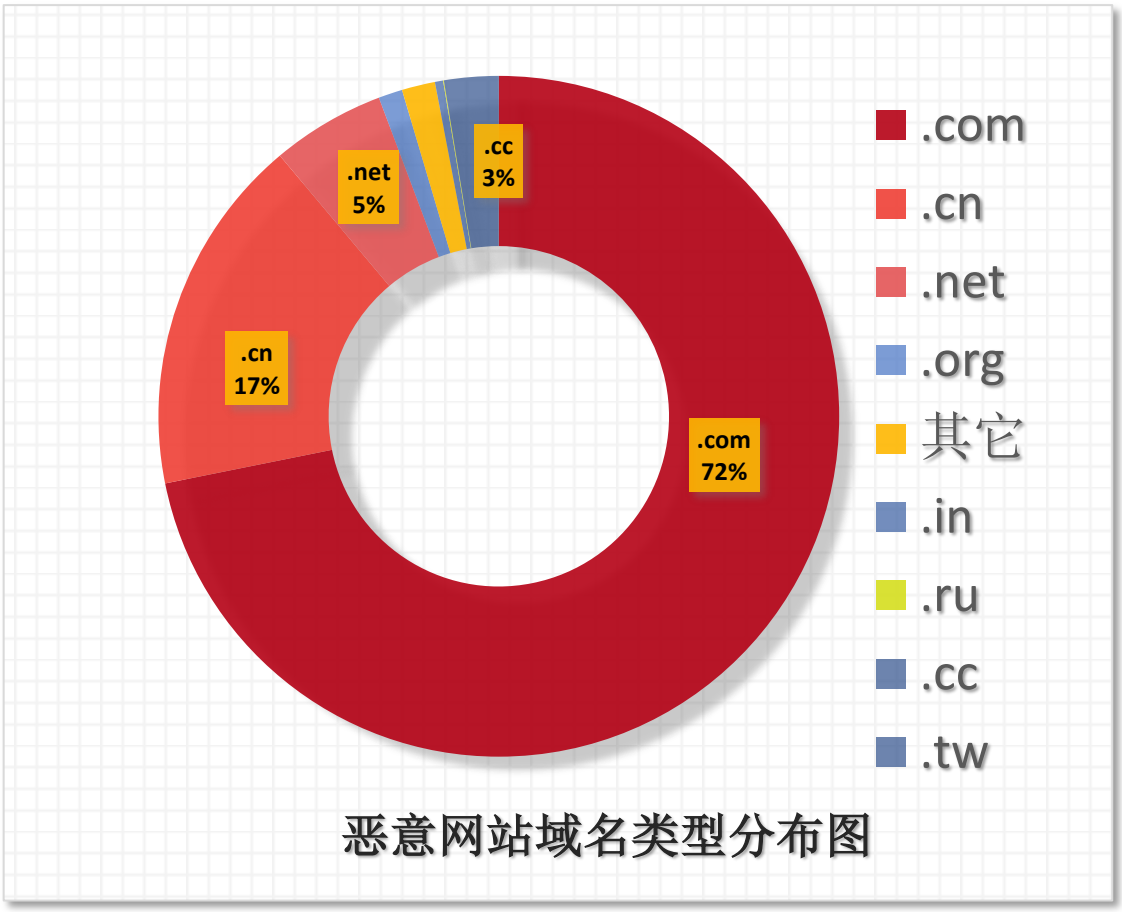


2016 年第 1 季度中国地区 WEB 威胁文件类型分布图

2016 年第 1 季度 TOP 10 恶意 URL

TOP10 恶意 URL		
恶意 URL	描述	点击量
http://dl.gj.gti**.com/invc/xfspeed/c2	网站直接或间接帮助传播恶意软件或恶意代码	1384197
http://sso.an***.com/domain/control.coolkey.org	网站直接或间接帮助传播恶意软件或恶意代码	611520
http://wpsconfig.ks**s.ks-cdn.com/ks3_1526865442eb6575808ff1579ff7edad/Dandelion_stp.gz.exe	网站直接或间接帮助传播恶意软件或恶意代码	514327
http://220.181.***.104/msvquery	网站直接或间接帮助传播恶意软件或恶意代码	438242
http://download.***5.cn/2345safe/2345safe_v2.7.exe	网站直接或间接帮助传播恶意软件或恶意代码	367846
http://masterconn.**.com/	网站直接或间接帮助传播恶意软件或恶意代码	323115
http://101.226.**.201/msvquery	网站直接或间接帮助传播恶意软件或恶意代码	309121
http://download.2***.cn/2345zhushou/2345zhushou_v3.1.5565_silent.exe	网站直接或间接帮助传播恶意软件或恶意代码	290269
http://passport.**.tv/pages/user/proxy.action	网站直接或间接帮助传播恶意软件或恶意代码	280785
http://106.***.162.174/cloudquery.php	网站直接或间接帮助传播恶意软件或恶意代码	269161

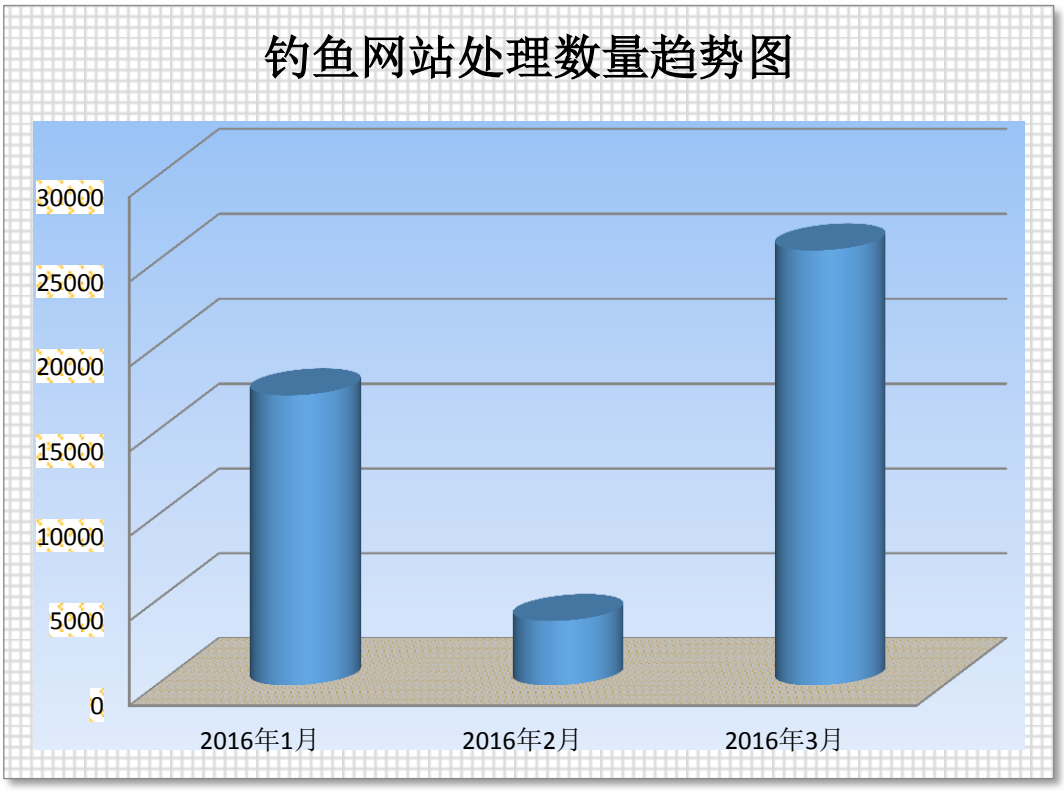
2016 年第 1 季度中国地区 WRS 拦截恶意 URL 排名 TOP10



2016 年第 1 季度恶意网站域名类型分布图

2016 年第 1 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。

2016 年第 1 季度 WEB 威胁钓鱼网站仿冒对象分析



2016 年第 1 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：2016 年 1 月至 2016 年 3 月处理钓鱼网站共计 **46,562** 个。

2016 年 2 月钓鱼网站数量大幅减小，推测是因为春节的原因。3 月钓鱼网站又大幅增加，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。

第一季度的钓鱼网站域名中，主要的域名来自于.COM、.CC、和.TK 域名，其占到本季度钓鱼网站数量 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

2016 年第 1 季度漏洞攻击威胁情况

TOP10 漏洞	
漏洞名称	**检测数量**
CVE-2008-4250	298641
MS08-067	561
CVE-2010-0806	206
CVE-2012-0507	6
CVE-2013-0422	5
CVE-2014-4113	5
CVE-2014-4148	5
CVE-2014-6271	3
CVE-2010-2568	2
CVE-2010-3340	2

2016 第 1 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-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***
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-2014-6271	*http://cve.mitre.org/cgi-bin/cvename.cgi?name= **CVE-2014-6271***
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***

漏洞介绍链接

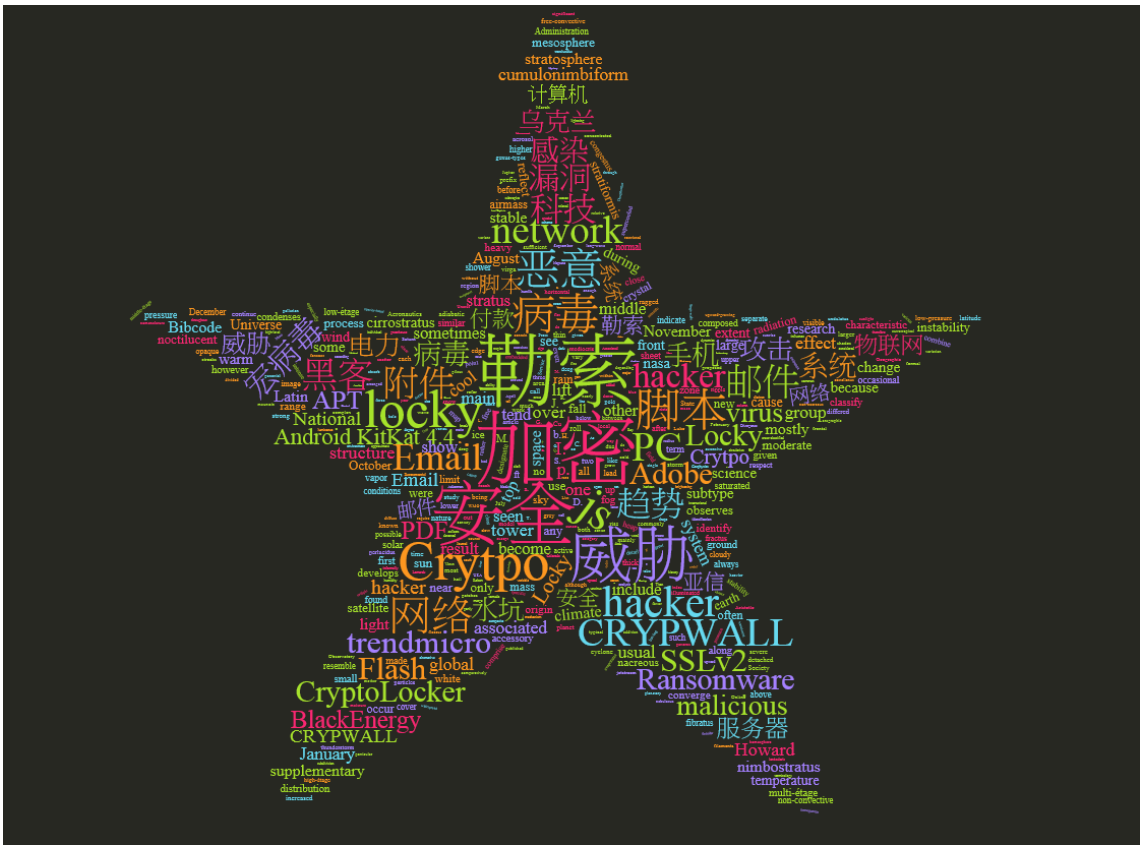
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

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。

2016 年第 1 季度最新安全威胁信息

2016 年第 1 季度安全威胁信息摘要



2016 年第 1 季度国内外安全威胁信息关键词

❖ 危机！SSLv2 漏洞致使三分之一 HTTPS 服务器沦陷

近期，一种存在于 SSLv2 协议中的安全漏洞被发现，它能够对 HTTPS 及 SSL/TLS 服务产生巨大威胁，让黑客通过联网通信侵入目标服务器盗取关键信息。这种攻击行为被称为 DROWN，即“利用过时和脆弱加密算法来对 RSA 算法进行破解”。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402905709&idx=1&sn=ae2b86a5f80820a2e9aae9b32e878939&scene=4#wechat_redirect

❖ Locky 加密勒索软件：堵漏洞 别做梦，一个疏忽让你系统崩盘！

新型的 Word 勒索软件是一种传播方式较为罕见的 Locky 加密勒索软件，它通过宏病毒的方式渗入系统。一些不明真相的用户往往会按照系统提示开启宏来浏览文件，随后 Locky 加密勒索软件就会完成暗中加载，从而感染用户的所有文档。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402814983&idx=1&sn=82bf99058a919f1574b1b244ac9368f5&scene=4#wechat_redirect

❖ 加密勒索软件——让医疗机构谈其如谈虎！

近日，关于加密勒索软件攻击医院的事件日益剧增，网络黑客除了勒索普通用户外，还将罪恶之手伸向急需救助且毫无反抗能力的病人，其行为可谓是灭绝人性。美国一家医疗中心由于受到加密勒索软件的攻击，致使这家医疗中心的网络系统瘫痪了一周，院中 430 个床位病人的所有联网的检查结果、病例查询、药剂使用都无从查找，最后不得不将病人转院治疗从而避开这次浩劫。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402795173&idx=1&sn=34fd49450c614adda290965fecdc7fa1&scene=4#wechat_redirect

❖ 骇人奇事！播放车载光碟可能被人劫持整车

随着科技的不断发展，智能联网汽车已进入日益壮大的物联网世界中，为汽车用户提供着更好的服务。而与此同时，一项研究报告指出这种新兴的科技也将带来风险，美国的一位研究人员在某款智能型汽车系统中就发现了漏洞，这个漏洞只要在车载多媒体设备上播放音乐，就会被黑客程序轻易侵入并且控制整车。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402777227&idx=1&sn=946b737dd252d9b640e538a7ac05fd50&scene=4#wechat_redirect

❖ 中了勒索软件怎么办？只能付款了事么？ 建议牢记四步骤和“三要三不要”

中了勒索软件（Ransomware）该怎么办？「建议受害人付款了事」在网络安全高峰会上 FBI 如是表示，此语一被爆出即惹来了很大争议。

勒索软件藏在邮件、藏在载点、藏在广告里…只要你上网，就有可能是它的觊觎目标。前一阵子有位公司的会计人员，误点免费中奖 iPhone 6S 的钓鱼邮件，导致服务器上的数据被勒索软件 CryptoLocker 加密，结果当事人与主管都调离现职。根据亚信安全研究院的调查"勒索软件攻击"被公认为今年全球最惊世骇俗的安全攻击事件之一；另一项 2015 年度亚信安全网络安全票选活动，第一名也由 CryptoLocker (加密勒索软件)夺魁，得票数占 42.11%。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402705740&idx=1&sn=e2b6bc5aac1aa7823bd02c7718917108&scene=4#wechat_redirect

❖ 警惕！当你要解锁手机时，有人已经清空了你的银行账户

想象一下，你的银行通知你安装更新应用程序，照做之后又发来管理员权限指令，于是你按下同意键……全部完成后你试了一下应用程序，没有一点问题，甚至运作更加流畅了。

可是，第二天你的手机竟然翻脸不认人，它无论怎样都识别不了你自己设置的密码！当你百感交集地还在解锁手机，甚至怀疑自己是否输错密码的时候，已经有人清空了你的银行账户！！！

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402622410&idx=2&sn=eb0c192cabaf2a3c37e8d627f89e9307&scene=4#wechat_redirect

❖ 鳄鱼还是木头？亚信安全提醒：APT 攻击防范要当心"水坑"

水坑攻击是 APT 攻击的一种常用手段，黑客通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站弱点，入侵这些防御措施相对薄弱的服务器并植入恶意程序，当用户访问了这些网站，就会遭受感染。就像是鳄鱼捕食的惯用伎俩一样，捕食者埋伏在水里，等待角马喝水时发动攻击。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402415882&idx=1&sn=a2f37aaf361d33baa45611d13866e208&scene=4#wechat_redirect

❖ 乌克兰电力设施瘫痪，不止威胁能源产业！

导致近日两起乌克兰电力设施中断的攻击者,可能也曾试图对乌克兰矿业公司及大型铁路公司进行类似攻击。这证明造成乌克兰停电事件有关的恶意程序 BlackEnergy，不只是能源产业的问题，甚至延伸成为各产业的威胁。虽然上述攻击的动机一直是被重度炒作的话题，但其主要目的可能是出自于政治动机，为了瘫痪乌克兰公共和关键基础设施。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402299373&idx=1&sn=82913939d198a04bd2d32b208e278de6

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。

&scene=4#wechat_redirect pto-ransomware/

❖ 想防堵这个漏洞？服务器、手机和物联网设备一个都不能少！

众所周知，Linux 核心是所有 Linux 操作系统的共同组件，不仅应用于服务器平台，就连 Android 手机、平板电脑和各式各样的物联网设备都是使用 Linux 系统。近日，Perception Point 研究团队揭露了 Linux 的核心漏洞 (CVE-2016-0728)，影响波及多个层面。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402047724&idx=1&sn=00e6c9ef97bbe52c172d3e5c2baf57cb&scene=4#wechat_redirect

❖ Uber 未经同意追踪乘客位置被罚，谈谈移动应用程序隐私！

经过 14 个月对 2014 年资料外流（包括超过 5 万名现任和前任司机的姓名和驾照号码）事件的调查，Uber（优步）最近要在纽约缴出 2 万美元的罚款。这款应用背后市值数十亿美元的新创公司也因为被发现该应用可以在未经同意下追踪乘客位置而饱受批评。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402269285&idx=1&sn=7bb557bb6733f1dd25fcd87e578beb2c&scene=4#wechat_redirect

❖ Linux 核心漏洞导致全球数千万 Linux PC 和服务器皆受到影响！

最近，Linux 核心出现了一个过去从未被发现的漏洞，导致全球数千万 Linux PC 和服务器皆受到影响。研究人员表示，此漏洞可让黑客将本机使用者的权限提升至最高的系统管理员 (root) 等级，就连 Android KitKat 4.4 或更新版本的设备也受影响。

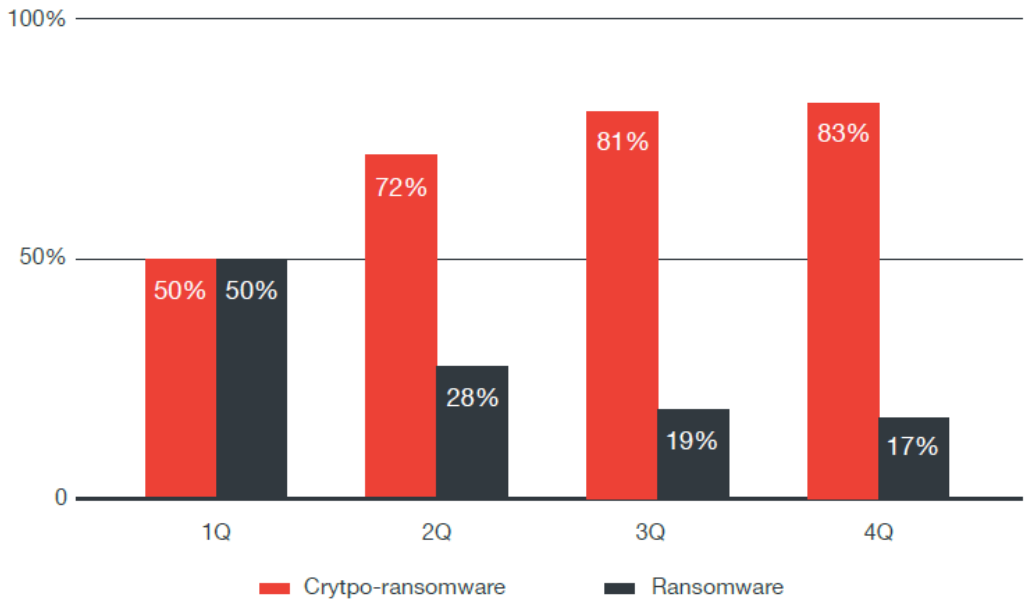
此漏洞最远可追溯至 2012 年，受影响的 Linux 核心版本包括 3.8 或更新版本，而且是出现在应用程序用来储存加密密钥、认证码及其他敏感安全数据的钥匙圈 (keyring) 当中。黑客一旦攻击成功，就能在 Linux 核心上执行程序代码以取得系统快取中的安全数据。截至漏洞揭露日期为止，安全小组仍在研究可能影响的设备范围。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=402285877&idx=2&sn=2ab2ecfd9860ce8c4c6c1b2ff29b27ed&scene=4#wechat_redirect

全球区最新安全威胁概要

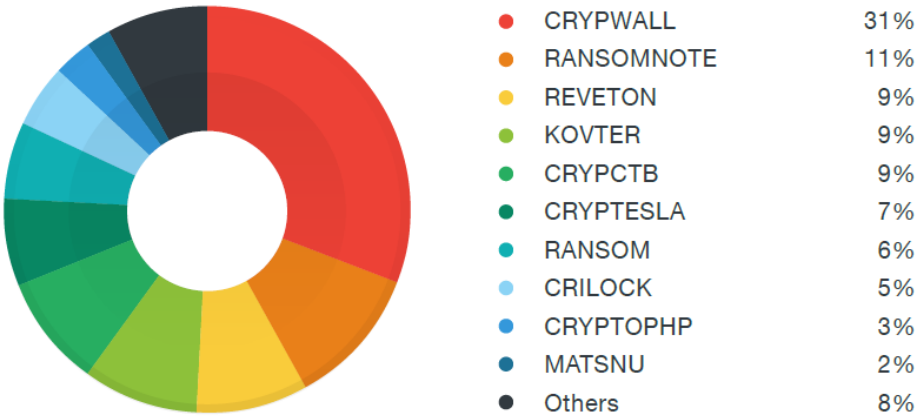
以下是来自 2015 年第 4 季度全球区安全报告的数据。

2015 年勒索软件不仅在代码和结构方面发生变化，而且其攻击目标也发生着变化，其中 crypto 勒索软件涨势迅猛，下图是勒索软件与 Crytpo 勒索软件数量增长对比图



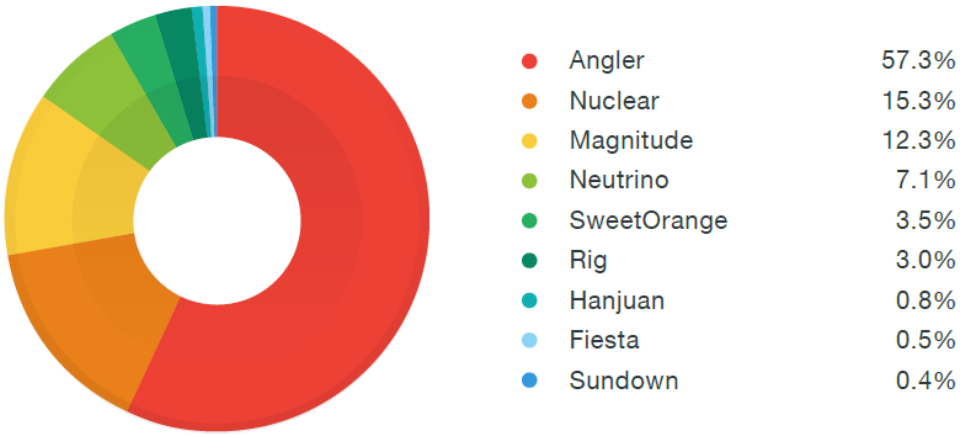
Crytpo 勒索软件与勒索软件数量增长对比图

2015 年度勒索软件家族数量排名显示，CRYPWALL 勒索软件家族长期稳居榜首。



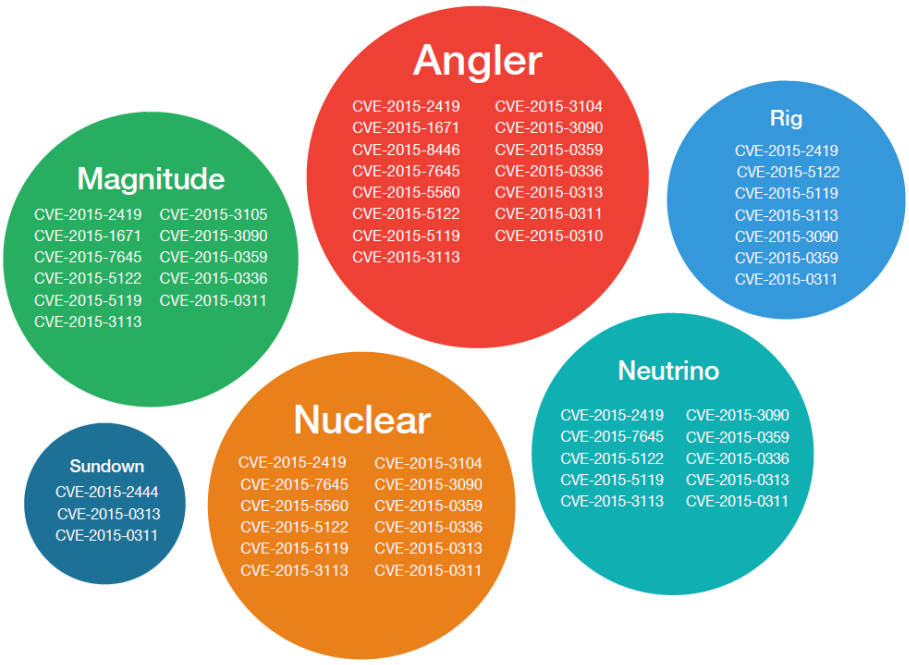
勒索软件家族数量排名表

Angler 钓鱼攻击工具包因其易于整合，其成为 2015 年最常用的漏洞利用工具包。据统计 2015 年共有 1,600,000 个 URL 利用该工具包，远远超过其他漏洞利用工具。



漏洞利用工具包排名表

Angler 钓鱼攻击工具包内容丰富，其会加入零日漏洞。



2015 年漏洞工具包示意图

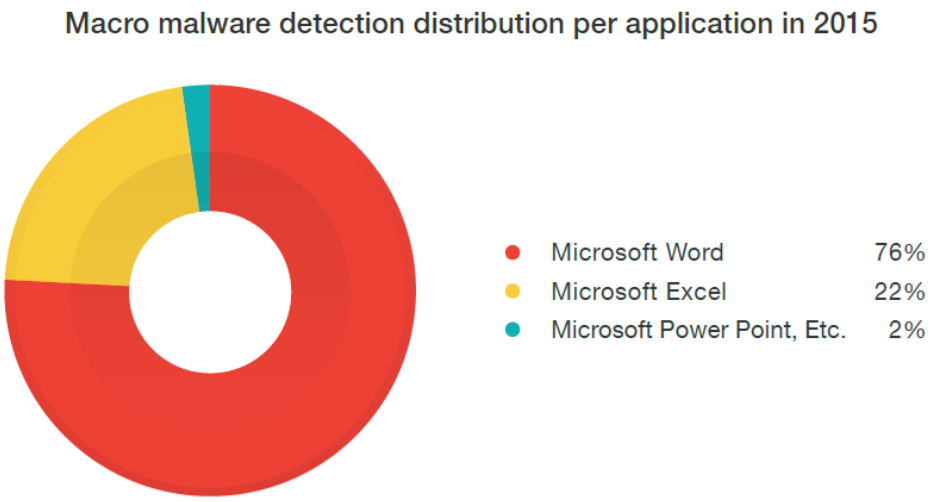
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC),本报告中所有数据仅针对中国地区。

2015 年病毒家族排行中，SALITY 家族居首位。宏病分布排行中，word 家族居首位， 灰色软件排行中，OPENCANDY 居首位

Top malware families of 2015

Family	Count
SALITY	325K
DOWNAD	298K
GAMARUE	207K

2015 病毒家族排行表



2015 宏病毒应用分布排行

Top adware families for 2015

Family	Count
OPENCANDY	1.9M
MYPCBACKUP	504K
DEALPLY	407K

2015 灰色软件家族排行

需要查看更完整的 2015 年第 4 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。