AsiaInfo | 亚信安全

# 亚信安全 2016 年
# 第二季度
# 网络安全威胁报告

2016/07

亚信安全网络监测实验室

# 目录

# 2016 年第 2 季度安全威胁

**本季安全警示：**

**SWIFT 银行劫案 、数据泄露**

**2016 年第 2 季度安全威胁概况**

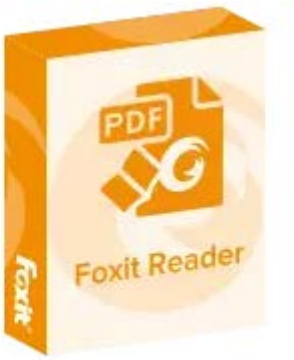
- 本季度亚信安全病毒码新增特征约 **20** 万条。截止 2016.6.30 日病毒码 **12.620.60** 包含病毒特征数约 **437** 万条。
- 本季度亚信安全客户终端检测并拦截恶意程序约 **12,495** 万次。
- 本季度亚信安全拦截的恶意 URL 地址共计 **28,220,020** 次。

本季度热点话题为 SWIFT 银行劫案。本季度陆续报道了孟加拉国、厄瓜多尔、越南、菲律宾等多个国家的银行曝出曾经遭遇黑客攻击并试图窃取金钱事件，这些事件中黑客都瞄准了 SWIFT 银行间转账系统，对相关银行实施攻击和窃取。


SWIFT 全称是 Society for Worldwide Interbank Financial Telecommunication，中文名是“环球同业银行金融电信协会”。是国际银行同业间的国际合作组织，负责运营世界级的金融电文网络，银行和其他金融机构通过它与同业交换电文（Message）来完成金融交易。目前全球大多数国家大多数银行已使用 SWIFT 系统。

上述这些备受瞩目的攻击引发大家的疑问，攻击者如何获得授权做交易或拿到支付指令？使用了哪些工具？哪些安全控制可以检测到这些可疑的活动？

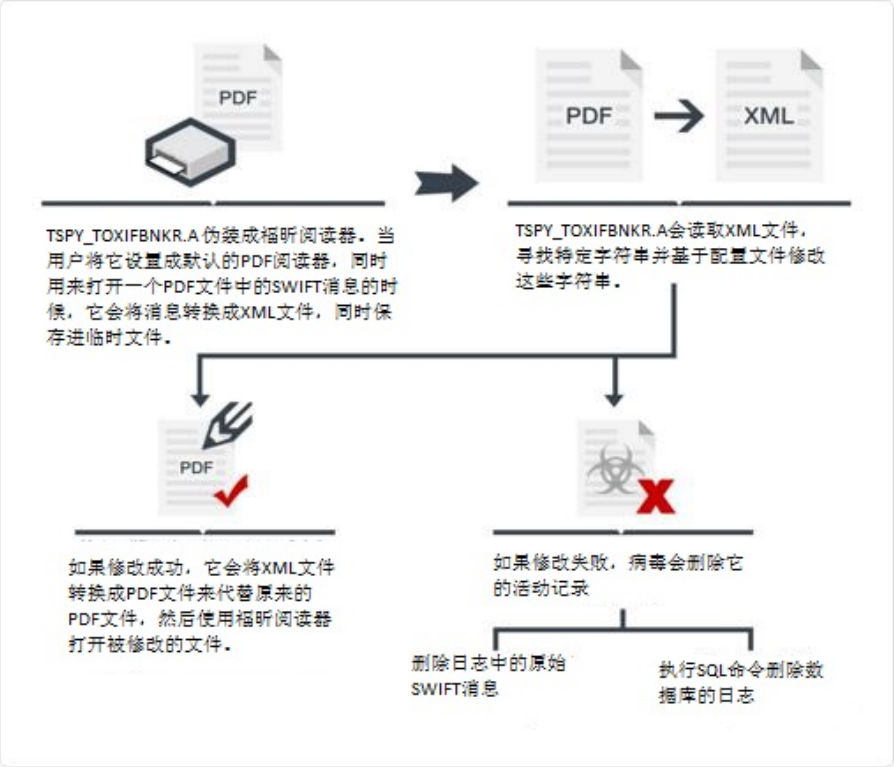
操纵这些计划周密的网络劫案的幕后黑手去年还曾利用针对 SWIFT 网络的工具修改 SWIFT 指令，尝试从越南先锋商业股份银行盗取资金。同时，这些黑客对 SWIFT 体系以及银行如何部署和使用 SWIFT 有着比较深入的了解。他们利用福昕 PDF 阅读器（Foxit Reader）伪造 PDF 文件来发起社会工程学攻击来诱骗越南银行。通过前期侦查，他们了解到这家银行在日常工作中使用了这款 PDF 阅读器。




通过追踪越南银行的攻击事件，亚信安全研究团队发现，在黑客定向式攻击目标中，有75%的银行的 SWIFT 代码被硬编码在恶意软件中。但是这些银行系统不仅仅在亚太地区，还有两个在美国和欧洲，但犯罪分子为何把主要攻击目标设立在亚洲呢？这一切，并非巧合！

首先，在黑客已经熟悉的银行系统中，挑战这些地区的银行网络防御体系的难度相对要小。其次，尽管认识到安全的重要性，许多区域性银行也非常不乐意投入更多预算构建先进的安全解决方案。最后，根据 2015 年的一项研究，缺乏公私合作关系是亚洲银行与欧美银行的一大差距，某些亚洲国家缺乏跨境合作，这可能会是解决网络犯罪的巨大障碍。

亚信安全截获了在此次攻击越南银行的事件中所使用的病毒工具(该工具被命名为 TSPY_TOXIFBNKR.A)。其在系统上执行 SWIFT 的时候有 3 个主要的任务模块的，下面是该病毒感染流程图。




TSPY_TOXIFBNKR.A 病毒感染流程图

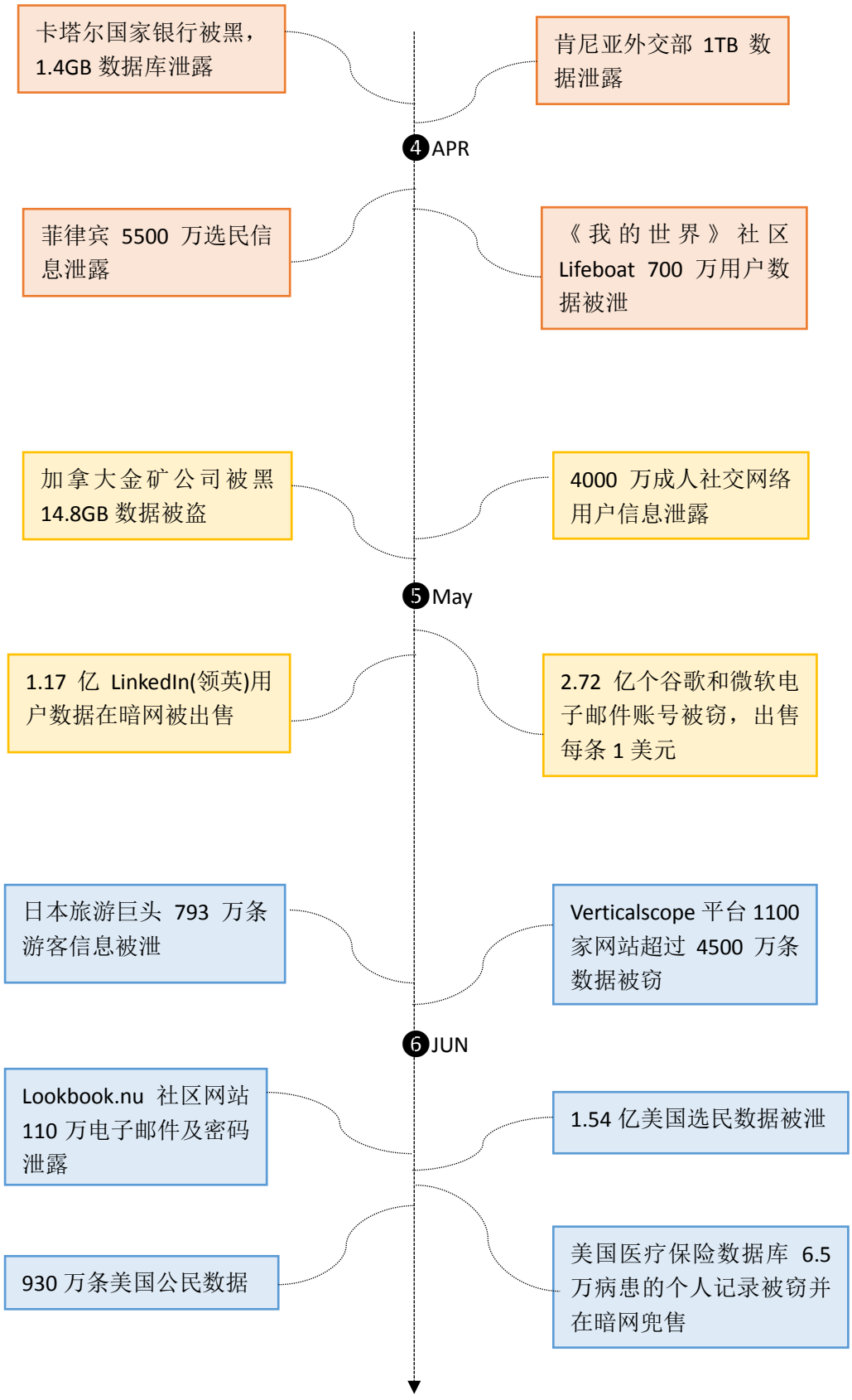
第一、 其通过 pdf 文件中的 SWIFT 消息修改银行交易信息。这个病毒只在恶意的福昕阅读器是默认的 pdf 打开工具的时候才会工作，或者用户手动选择这个程序去打开包含 SWIFT 消息的文件。

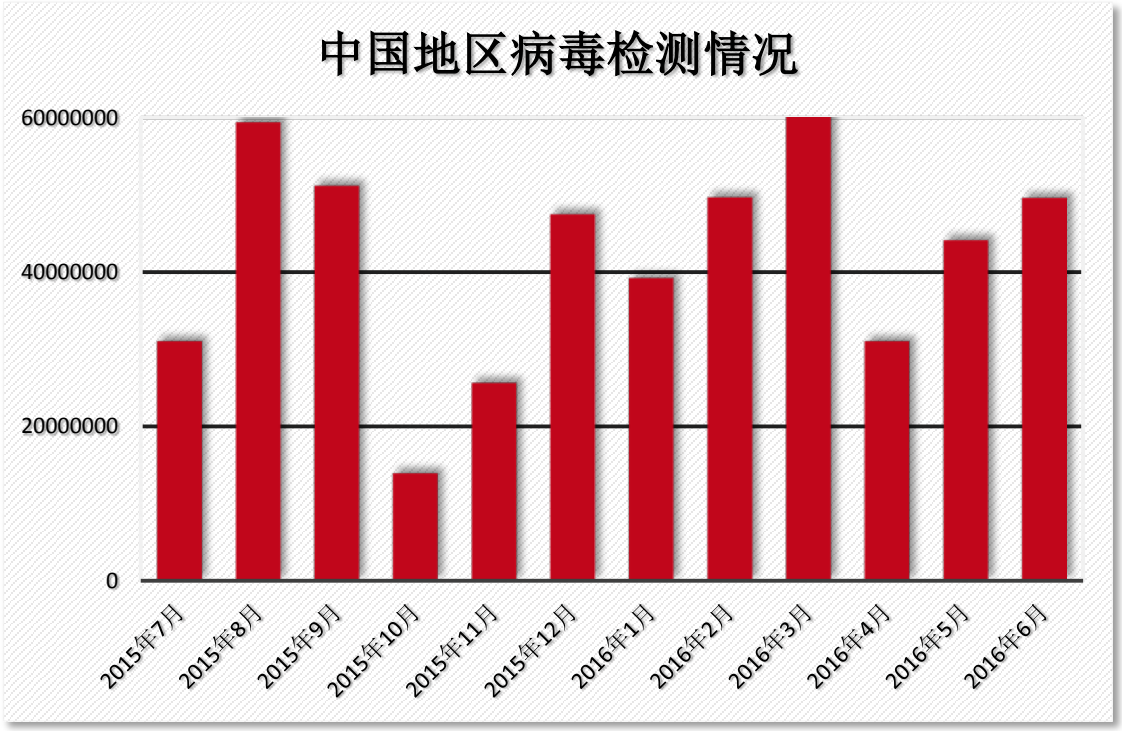
第二、 第二，病毒会删除它自身留下的痕迹，包括修改失败记录，其中之一就是入账出账的银行交易数据日志。

第三、 它会记录活动的细节描述。

我们仍然监控着任何有关于该病毒的更新以及其他的威胁。

本季度另一个热门话题是数据泄露，本季度发生了多起数据泄露事件，给公司乃至个人都带来了巨大损失，如下是本季度典型的数据泄露事件。

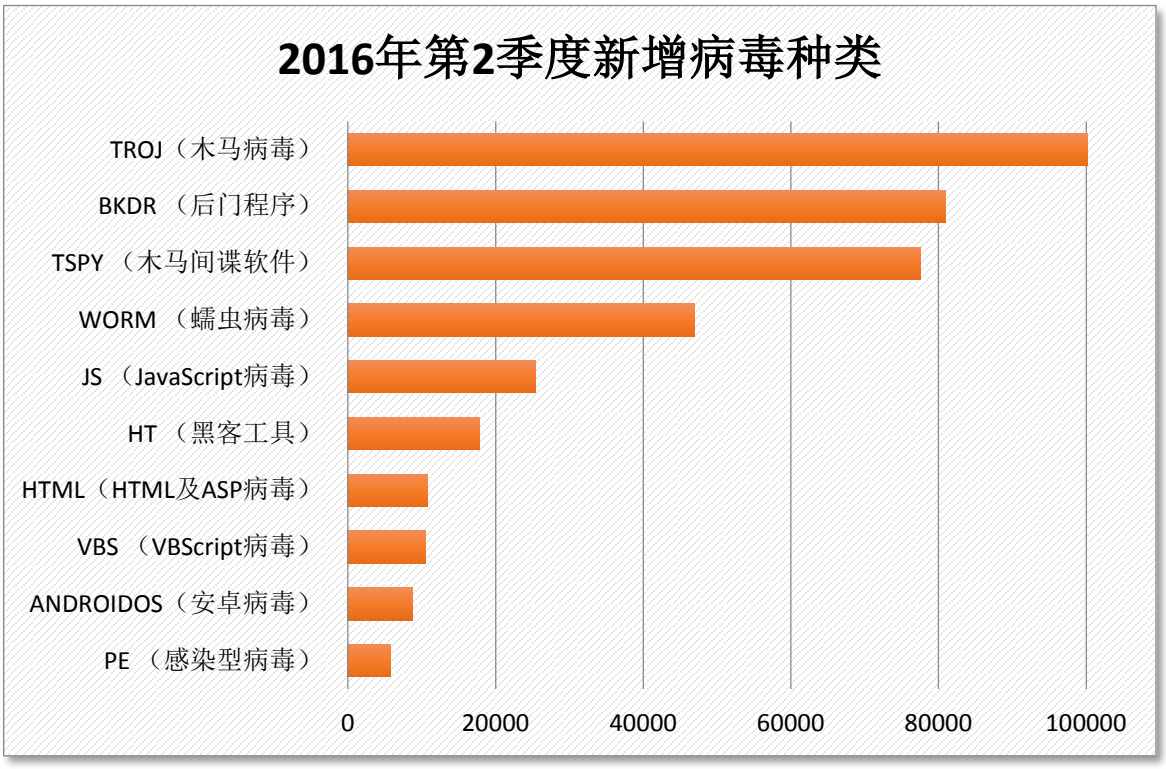

卡塔尔国家银行被黑，1.4GB 数据库泄露
肯尼亚外交部 1TB 数据泄露
4 APR
菲律宾 5500 万选民信息泄露
《我的世界》社区 Lifeboat 700 万用户数据被泄
加拿大金矿公司被黑 14.8GB 数据被盗
4000 万成人社交网络用户信息泄露
5 May
1.17 亿 LinkedIn(领英)用户数据在暗网被出售
2.72 亿个谷歌和微软电子邮件账号被窃，出售每条 1 美元
日本旅游巨头 793 万条游客信息被泄
Verticalscope 平台 1100 家网站超过 4500 万条数据被窃
6 JUN
Lookbook.nu 社区网站 110 万电子邮件及密码泄露
1.54 亿美国选民数据被泄
930 万条美国公民数据
美国医疗保险数据库 6.5 万病患的个人记录被窃并在暗网兜售




**2016 年第 2 季度病毒检测数量图**

**2016 年第 2 季度病毒威胁情况**

**2016 年第 2 季度新增病毒类型分析**



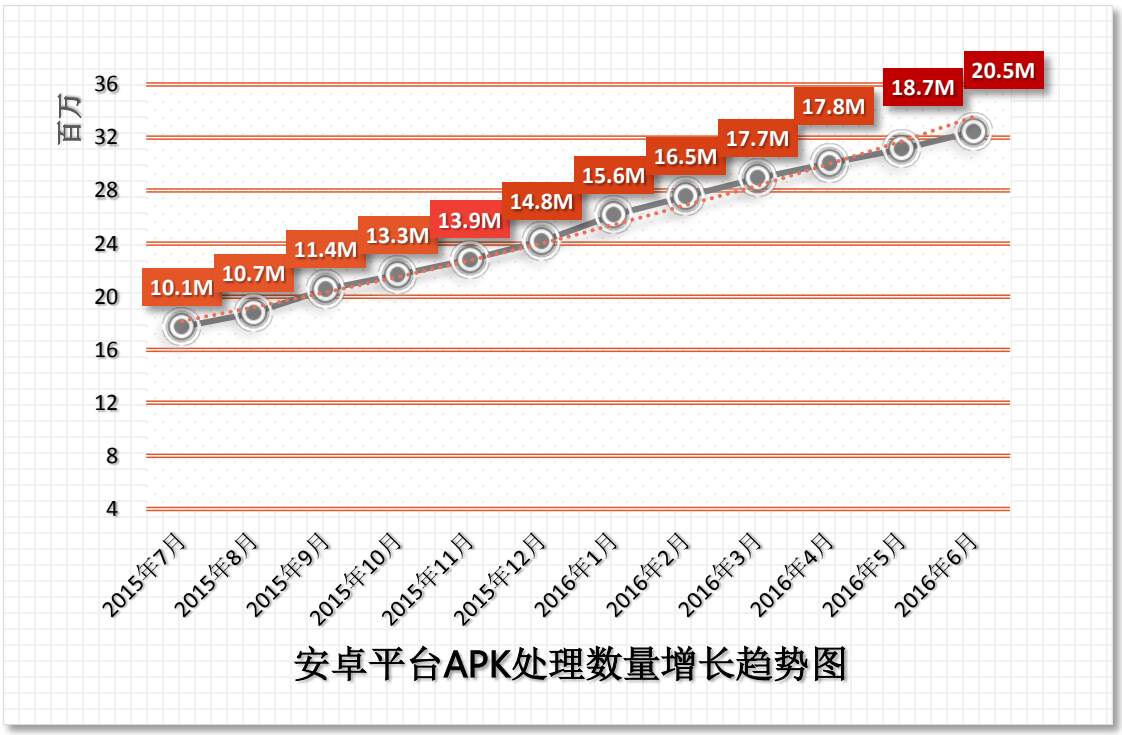

**2016 年第 2 季度新增病毒类型分布图**

在 2016 年第 2 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 366,538 个，和第一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。

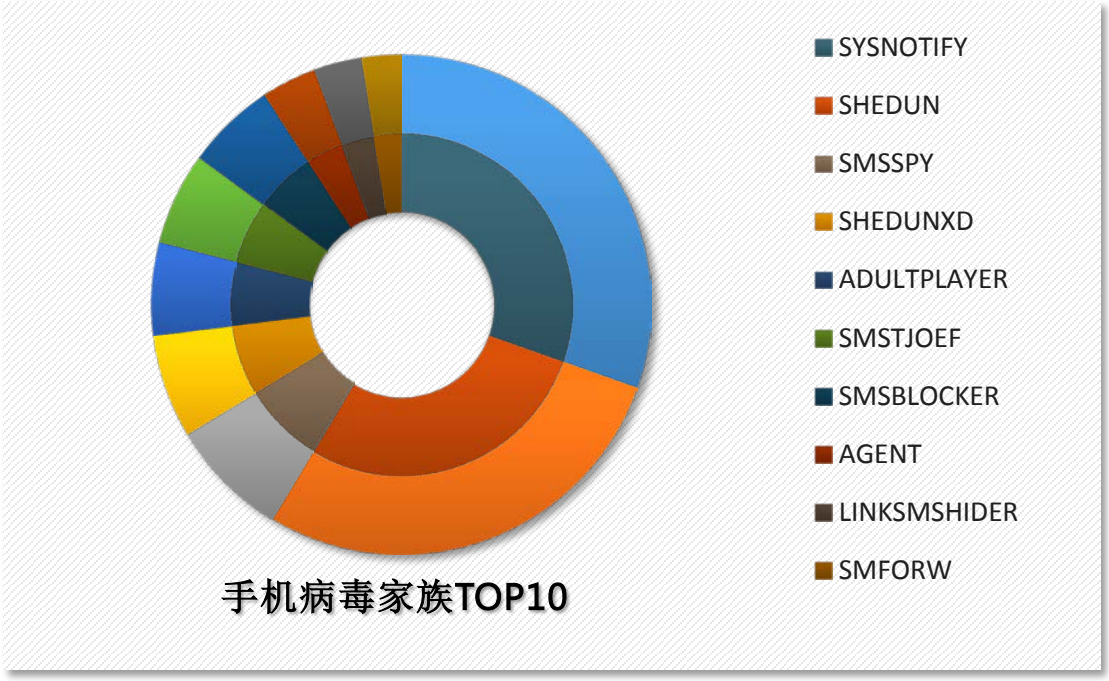
其中 JS(JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒与网页挂马有关，网页挂马是攻击者常用攻击类型。一些正常网站由于自身存在的缺陷漏洞，导致被入侵者挂马，之后浏览被挂马网页的访问者就会在毫不知情的情况下自动下载恶意文件到本地。

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 2 季度安卓平台 APK 处理数量走势图**

2016 年第 2 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 6 月底，处理数量累计达到 3,244 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 2 季度手机病毒家族 TOP10 分布图**

在 2016 年第 2 季度感染安卓平台的手机病毒家族中，SYSNOTIFY 家族数量最多，占到总数的 30.40%；SHEDUN 家族位列第二位，占总数的 28.24%；SMSSPY 家族居第三位，占总数的 7.71%。与上季度相比，SYSNOTIFY 家族涨势凶猛，而上季度排名第一的 OPFAKE 家族则有减弱趋势。

在 2016 年第 2 季度中，手机病毒持续增长趋势，其中手机 APP 病毒大幅增长，日前亚信安全发现了一款能 Root 掉手机的安卓应用程序 Godless，亚信安全将其检测为 ANDROIDOS_GODLESS.HRX，该程序看上去是合法的应用，研究人员发现它潜伏在包括 Google Play 的应用商店中，其攻击目标是运行安卓 5.1 及更早版本的设备，这也意味着其目标将涵盖超过全球 90%的安卓设备。


全球感染情况分布图

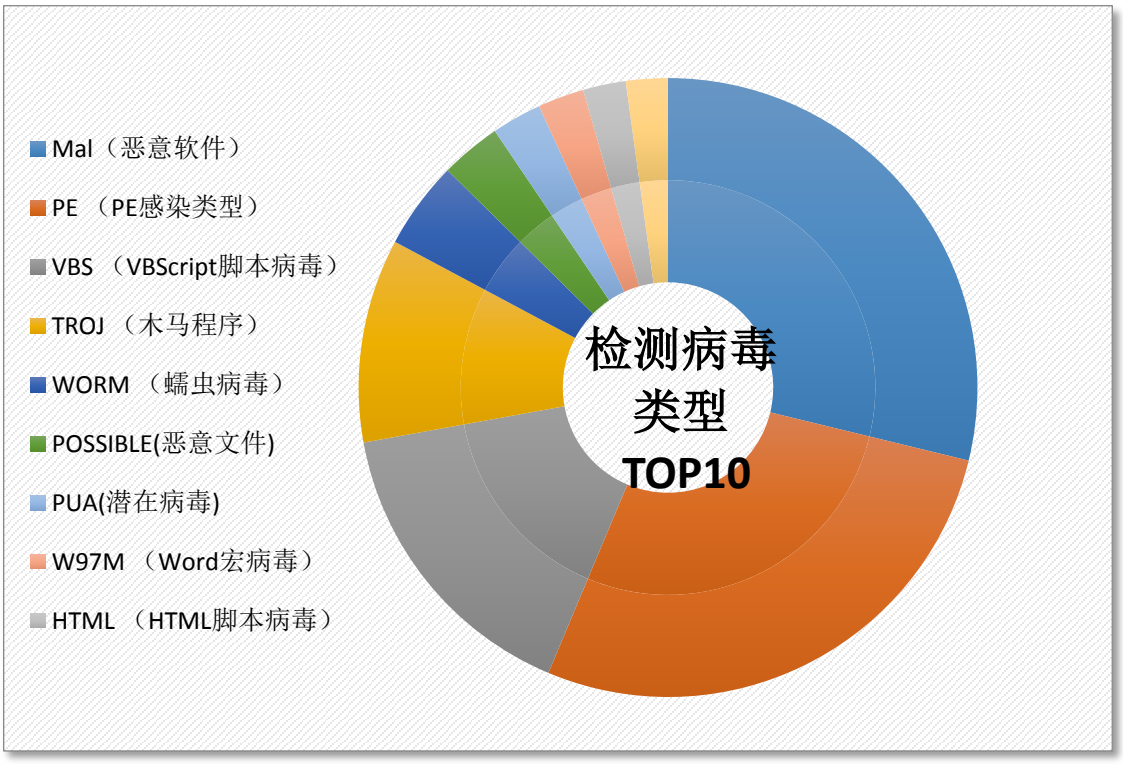
Godless 隐藏在应用中，并使用漏洞利用，尝试将手机操作系统 Root 掉。这基本上等于获取了设备的管理员权限，因此它可以对设备安装未经授权的应用。它还自带多种漏洞利用，以确保它能够成功 Root 掉设备。其甚至可以安装间谍应用。

最新的变种也可以绕过 Google Play 等应用商店的安全检查。在该恶意应用结束 Root 操作之后，其会卸载自身，逃避杀毒软件查杀。

本季度初发现了感染 IOS 恶意软件 AceDeceiver，该病毒在 App store 上以壁纸应用程序进行传播，其能够成功感染非越狱苹果设备。其会盗取受害者 Apple ID 及密码。

AceDeceiver 利用了 Apple DRM 机制上的设计漏洞，即使其已被苹果从 App Store 内移除，也可以借助其他全新攻击途径进行传播。

**2016 年第 2 季度各类型病毒检测情况分析**



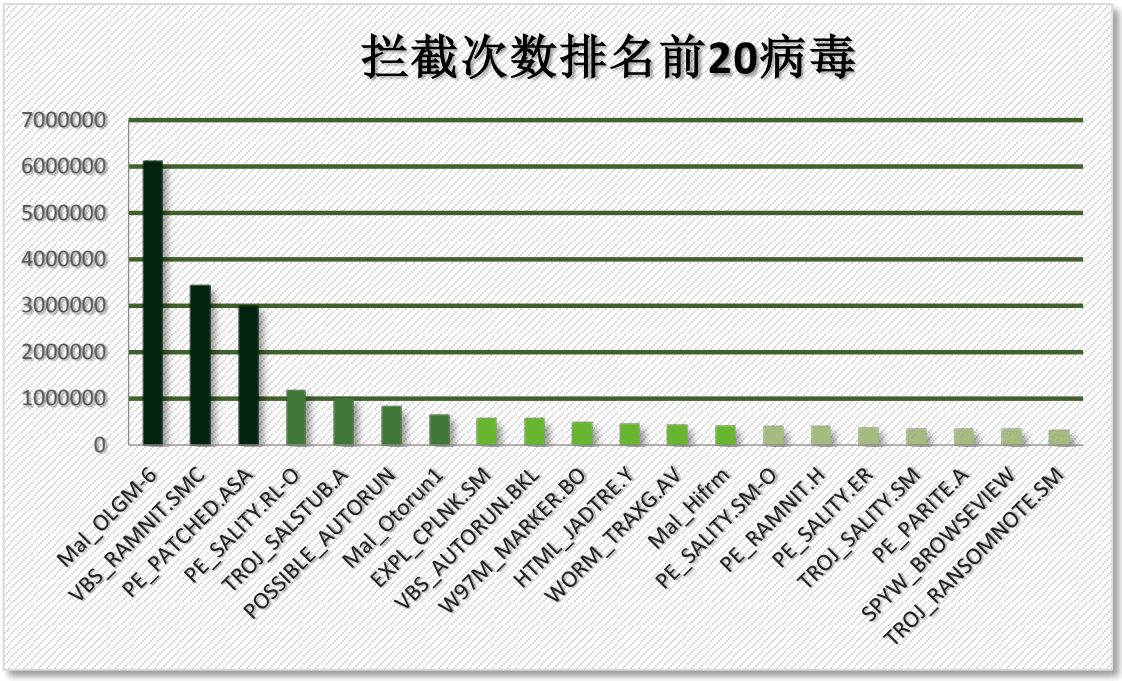

**2016 年第 2 季度病毒检测类型分布图**

2016 年第 2 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 28%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、PE_SALITY.RL-O 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。

本季度木马病毒占检测类型总数的 10.65%，本季度该类型病毒占比较上一季度有所上升。木马病毒通常不会主动传播，其是用户不经意从网络下载或者是其它恶意文件生成感染本机，本季度蠕虫病毒有小幅下降，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。

**2016 年第 2 季度病毒拦截情况分析**




**2016 年第 2 季度病毒拦截情况图**

在 2016 年第 2 季度拦截次数排名前 20 位的病毒检测名中，Mal、VBS 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 612 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，木马文件 TROJ_RANSOMNOTE.SM 勒索病毒，其是 CRYPTESLA 和 CRYPWALL 勒索家族生成文件。对于勒索软件防护方法，请安装 OfficeScan 11.0，并开启勒索软件行为监控功能。

另外一个值得注意的是，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 2 季度热门新型病毒分析**

本季度热门病毒 TSPY_TOXIFBNKR.A，该病毒卷入 2016 年 4、5 月份的全球金融网络传输系统 SWIFT 案件中，其利用 SWIFT 通讯网络偷盗资金。


TSPY_TOXIFBNKR.A 病毒行为流程图

**病毒的详细信息如下：**

**病毒检测名：** TSPY_TOXIFBNKR.A
**文件类型：** EXE
**常驻内存：** 否
**病毒行为：** 修改 SWIFT 报文格式的银行交易

**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

**其它细节：**

该病毒需要如下组件配合才可以运行

- %Temp%\WRTU\ldksetup.tmp <- 恶意行为的日志文件
- %Temp%\WRTU\LMutilps32.dat <- 配置文件
- fpdfsdk.dll <- 提供 PDF 和 XML 相互转换功能

- 修改使用 PDF 的 SWIFT 报文格式的银行交易
  - ✓ 触发条件：打开 PDF 文件时
    - ◆ 读取 PDF 文件，并将 PDF 转换成 XML 保存在临时文件中
    - ◆ 读取并解析 XML 文件，查找下列字符串：
      - ": Statement Line"
      - "Closing Balance (Booked Funds)"
      - "POS_TEMP"
      - "Opening Balance"
      - "Sender"
      - ": Debit"
      - ": Credit"
      - " Debit"
      - " Credit"
      - "POS_PAGE_START"
      - ": Closing Avail Bal (Avail Funds)"
      - "Message Trailer"
      - "Message Text"
      - "Message Header"
      - "Instance Type and Transmission"
      - "pagecount"
      - ": FIN 950"
  - ✓ 基于配置文件修改 XML 文件
  - ✓ 将 XML 文件转换为 PDF 文件，并替换原始的 PDF 文件
  - ✓ 使用福昕阅读器打开修改后的 PDF 文件
- 如果修改失败，病毒会删除自身痕迹
  - ✓ 执行 mspdclr.exe 文件，参数为 PDF 文件
  - ✓ 删除原始的 SWIFT 报文信息（PDF 格式）
  - ✓ 执行 SQL 命令删除数据库日志
- 在%Temp%\WRTU\ldksetup.tmp 文件中记录其活动行文信息

**解决方法：**

1. 亚信安全防防毒墙网络版(Officescan) 可以有效检测并清除该病毒
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.asiainfo-sec.com/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage.exe

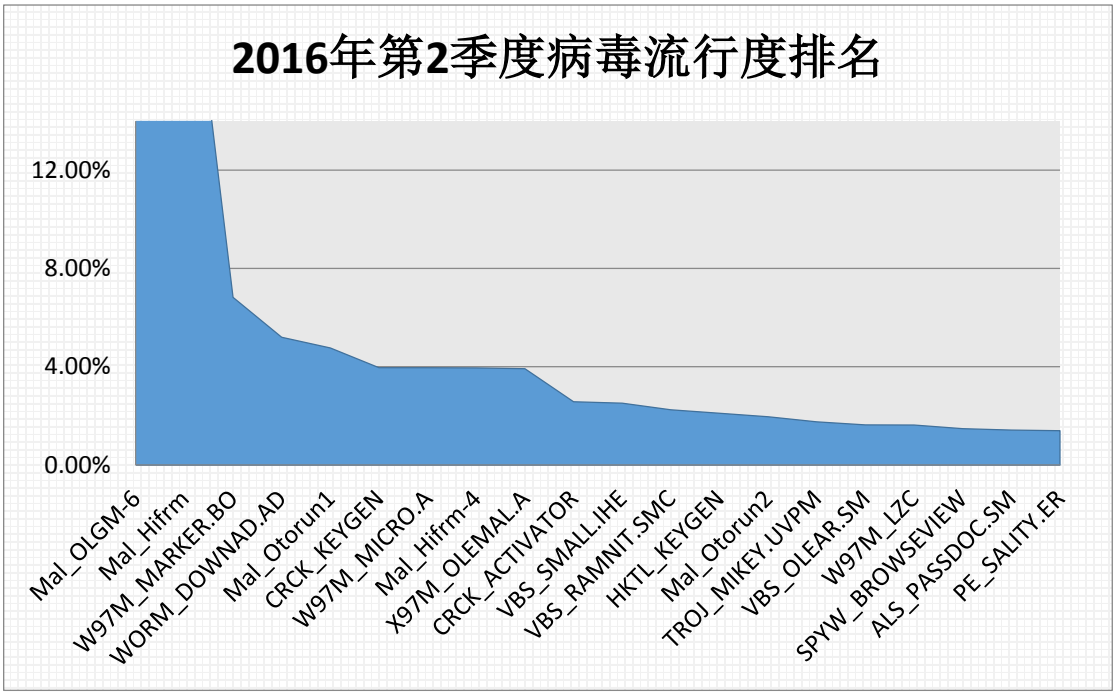
64 位 Windows 操作系统请使用：

http://support.asiainfo-sec.com/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage_64.exe

**相关信息链接：**

http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_toxifbnkr.a

**2016 年第 2 季度流行病毒分析**




**2016 年第 2 季度流行病毒排名情况图**


**2016 年第 2 季度 WORM_DOWNAD 病毒全球分布图**

WORM_DOWNAD 病毒依然是最为活跃的病毒。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 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。

**X97M_OLEMAL.A** 病毒是针对 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，但依旧是比较活跃的病毒。


**2016 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.asiainfo-sec.com/Anti-Virus/Clean-Tool/ATTK_CN/supportcustmizedpackage.exe

64 位 Windows 操作系统请使用：

http://support.asiainfo-sec.com/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.asiainfo-sec.com/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.asiainfo-sec.com/Anti-Virus/Clean-Tool/AvbTool/readme.txt

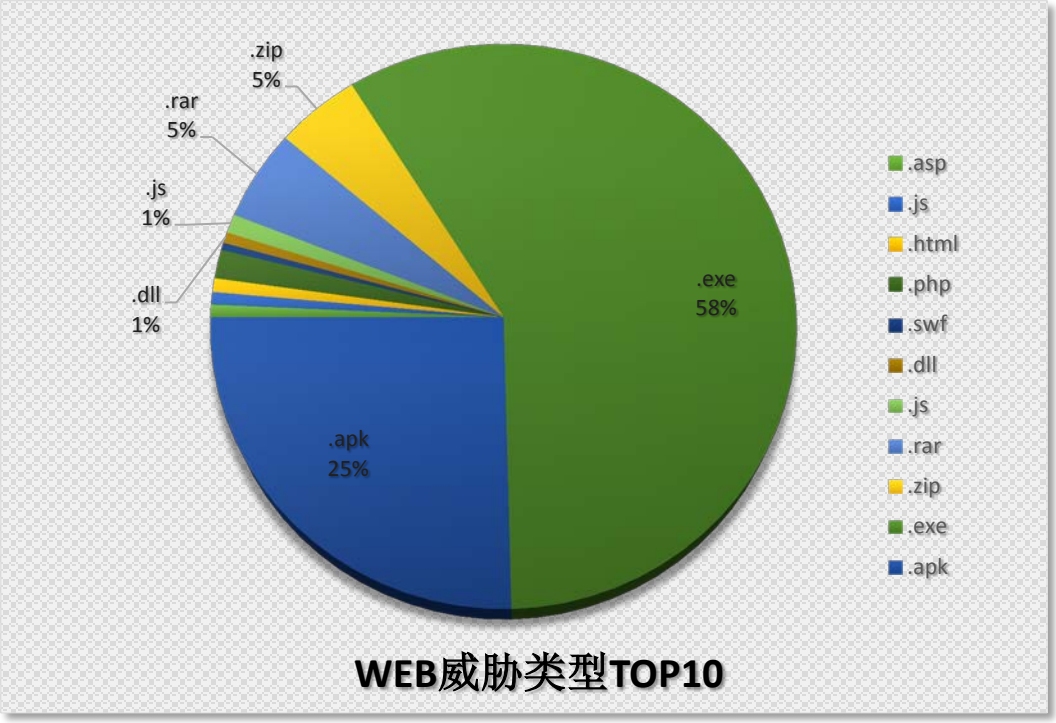
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

## 2016 年第 2 季度 WEB 安全威胁情况

## 2016 年第 2 季度 WEB 威胁文件类型分析

在 2016 年第 2 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 58%，所占比例比上一季度 37.72%的占比有所上升。.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，.APK 文件所占比例居高不下，此外.ZIP、.RAR 类型的文件位居第三位。

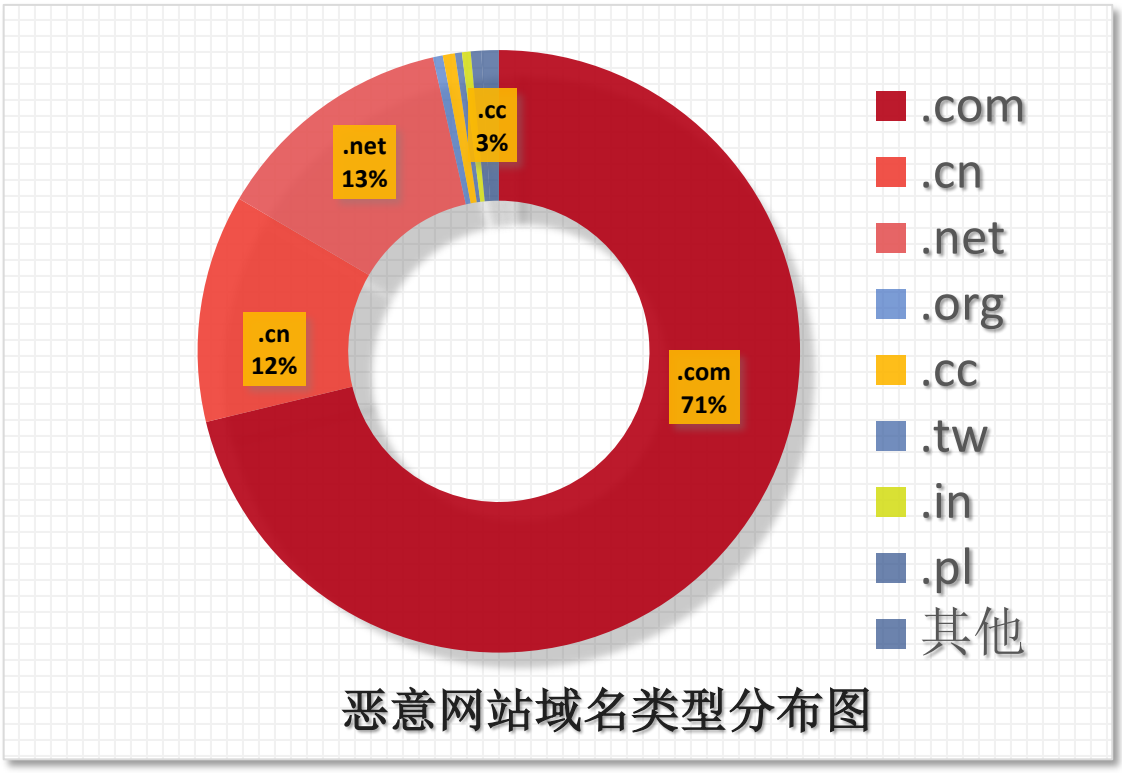



**2016 年第 2 季度 WEB 威胁文件类型分布图**

**2016 年第 2 季度 TOP 10 恶意 URL**

| TOP10 恶意 URL | | |
|---|---|---|
| **恶意 URL** | **描述** | **点击量** |
| http://www.369**.com/az.html | 网站直接或间接帮助传播恶意软件或恶意代码 | 2219387 |
| http://api.mei****ew.com/configCpp.ashx | 网站直接或间接帮助传播恶意软件或恶意代码 | 1700235 |
| http://www.app***.com/apk/avplay1851.apk | 网站直接或间接帮助传播恶意软件或恶意代码 | 1055262 |
| http://bb.a***.com:8080/ssa.ashx | 网站直接或间接帮助传播恶意软件或恶意代码 | 933494 |
| http://180.***.26.124/cgi-bin/micromsg-bin/statusnotify | 网站直接或间接帮助传播恶意软件或恶意代码 | 823841 |
| http://www.****softwares.com/playd0313/show/root.html | 网站直接或间接帮助传播恶意软件或恶意代码 | 703496 |
| http://101.***.211.44/cgi-bin/micromsg-bin/statusnotify | 网站直接或间接帮助传播恶意软件或恶意代码 | 681250 |
| http://download.***.cn/2345zhushou/2345***shou_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 | 674671 |
| http://www.****z.com/apk/avplay1844.apk | 网站直接或间接帮助传播恶意软件或恶意代码 | 584879 |
| http://www.**588.com/apk/avplay1853.ap | 网站直接或间接帮助传播恶意软件或恶意代码 | 533102 |

**2016 年第 2 季度 WRS 拦截恶意 URL 排名 TOP10**




**2016 年第 2 季度恶意网站域名类型分布图**

2016 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、.CN、.NET 的域名的站点占总数 96.00 %。其中.COM 域名的恶意网页数量最多。

**2016 年第 2 季度 WEB 威胁钓鱼网站仿冒对象分析**


**2016 年第 2 季度钓鱼网站数量**

从中国反钓鱼联盟得到的数据：2016 年 4 月至 2016 年 6 月处理钓鱼网站共计 **33,157** 个。

2016 年第二季度，月钓鱼网站数量程递减趋势，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。

第二季度的钓鱼网站域名中，主要的域名来自于.COM、.CN、和.NET 域名，其占到本季度钓鱼网站数量 90%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 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 | 272845 |
| MS08-067 | 334 |
| CVE-2010-0806 | 138 |
| CVE-2014-4113 | 7 |
| CVE-2014-4148 | 7 |
| CVE-2010-2568 | 2 |
| CVE-2012-0158 | 1 |
| CVE-2012-0507 | 1 |
| CVE-2013-0422 | 1 |
| CVE-2013-1493 | 1 |

**2016 第 2 季度漏洞攻击检测情况**

| | |
|---|---|
| ***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-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-2010-2568*** | *http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-2568* |
| ***CVE-2012-0158*** | *http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-0158* |
| ***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-2013-1493*** | *http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-1493* |

**漏洞介绍链接**

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 2 季度最新安全威胁信息

## 2016 年第 2 季度安全威胁信息摘要


**2016 年第 2 季度国内外安全威胁信息关键词**

❖ 坑你没商量，就连警察局也成黑客盘中菜啦！

近期，在美国发生了重大案件：美国亚拉巴马州的某警察局遭到网络袭击，黑客加密锁定了警局犯人的照片与资料，要求警察负责人支付 500 美元以换取文件解密。最终警察局拒绝了勒索要求，同时也放弃了被加密的资料文件。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574620&idx=1&sn=1b8aabe1c2063673a45c32ea9c0dca48&scene=4#wechat_redirect

❖ 亚信安全发现勒索软件新变种，Word 文档成为导火索

小心！如果收到陌生的 Word 文档，千万别急着打开，因为你的重要文件可能因此被非法加密，强行支付大量赎金。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574703&idx=1&sn=0f170af99dfd13229dc2fe0c624878dd&scene=4#wechat_redirect

❖ 苹果 iMessage 漏洞是否给研发者敲响了警钟？

美国约翰·霍普金斯大学电脑系教授马修•格林指出，iMessage 漏洞在去年就已经出现了。经过几个月的研究，格林团队用试验还原了这个即时通讯软件被破解的详细过程。他们发现，只要制作一个伪装成苹果服务器的软件，就有办法拦截该档案发送的信息。其中一项破解案例就是关于 iCloud 服务器上某照片的连接，这里让人很为惊讶的是，获取照片的 64 位密钥居然也一起存储在服务器上。有了这个密钥黑客就能轻松地解开用户在苹果服务器存储的照片，而且在毫不知情的情况下轻易窃取用户的各项资料。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574773&idx=1&sn=891b2a3eed87351b535981796ded2095&scene=4#wechat_redirect

❖ 是什么黑掉了你的销售管理系统？

是谁黑掉了销售终端管理系统（POS）的程序，让它成为信息失窃的背锅侠？当你在 POS 系统刷卡消费时是否觉得一切都安然无恙？其实，在这背后有张无形的黑手伸向了你的磁卡隐私，能让你瞬间遭受损失。

亚信安全研究院根据其特性，将这种恶意程序命名为 FastPOS。在入侵过程中，FastPOS 会立即将窃取到的信用卡资料外传，而并非先将资料存储在本机上的一个档案，过后再传递给黑客。其实这个 FastPOS 程序是专门针对小型网络环境而设计，就像只有一台 DSL 数据机连结 POS 系统的环境。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575126&idx=1&sn=64d0bd2c2549245b06ad7410b5205539&scene=4#wechat_redirect

❖ 勒索软件也分“洗剪吹”和“高逼格”吗？

勒索软件也分“洗剪吹”和“高逼格”吗？所谓勒索软件的“洗剪吹”派，也就是例如 TeslaCrypt 勒索软件之类非主流病毒。而今天，小编先带大家认识一下“高逼格”派系——叱咤网络界的主流病毒 CryptXXX 勒索软件。

从目前网络形势看，CryptXXX 勒索软件已被安全人士重点关注！在勒索软件蔓延过程中，CryptXXX 一直都在进行着更新，它最新的变种体不仅能加密用户档案，而且还会锁住屏幕，让使用者无法进入界面。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575111&idx=1&sn=95c2196f0ed54cbfd935ea919b558bfc&scene=4#wechat_redirect

❖ 防御勒索软件的第一步应该是？

不管你的企业使用何种操作界面，如果让勒索软件（Ransomware）在 IT 系统中扩散，它会强行加密被侵文件，几天内都不能存取资料，甚至永远锁死文档。这种状况对企业有什么影响？会造成业务中断、生产力损失，并且严重损害企业信誉度与盈利。很多用户为了防范勒索病毒，非常重视在电子邮件及网页网关上的攻击拦截。不过，这也仅仅是防御的一部分，其实更为重要的是犯罪分子总想找机会对企业的服务器下手，也就是说，漏洞过多且没有及时更新的服务器系统才是勒索病毒制造者的重点攻击目标。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575083&idx=2&sn=40fb38ea9da9f034e599ef520821f459&scene=4#wechat_redirect

❖ Skimer 让自动提款机成为“洗劫”用户的帮凶！

如今，深入人们生活的 ATM 已经成为了网络犯罪分子首要侵占的目标。犯罪分子通过恶意软件感染自动提款机，即便没有受害用户的银行卡他们仍然可以获取卡内敏感信息并提取机器内现金。这种令人惊骇的事情并非危言耸听，网络黑客的窃取手段已经实实在在地威胁着用户的隐私安全。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575034&idx=2&sn=c3225837669386a4a4fe36125a31211b&scene=4#wechat_redirect

❖ 如何避免勒索病毒冲击？亚信安全为你打造钢铁防线

近两年，勒索软件从一个小骚扰演变成网络的主要威胁，勒索软件黑客为隐藏踪迹而要求受害用户以电子货币方式支付赎金，以换取解密电脑数据所需要的“特殊密钥”。如果黑客没有达成勒索目的，他们则会永久性地强制加密文件，让用户没有任何办法解除病毒，完全损失中毒文件。据统计，网络黑客借助此类病毒软件每年敲诈的金额达到数十亿美元。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575012&idx=1&sn=ea3f5bf9f3555f77bccd7b05f2afc4c6&sc

ene=4#wechat_redirect

❖ 【警示】求职旺季，小心诈骗集团利用招聘骗取钱财！

近日，亚信安全研究院发现，在各大人才招聘中心网站上，诈骗集团以投资公司的名义大量收集刊登的求职简历。他们与求职者联系后随即告知对方有合适的职位，并要求求职者提供部分账户作为“工作所用”。在这期间，诈骗分子会将许多空头账户当作不法所得的输出管道，因为他们不会使用自身的真实账户去执行这种洗钱行为。当你向这些不法公司提交了某些信息账户后，你的账户就会不间断的出现大笔资金的出入，这种异常现象很容易被银行或监管部门所察觉。一旦你的账户被欺诈受害人检举，那些曾被你提供给公司的账户将被设为危险账户，账户里的资金款项将面临全部冻结、不能使用的状况。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575006&idx=1&sn=3acd83134e4b9e09c5b66ef9e0e536a9&scene=4#wechat_redirect

❖ 头痛的可定制化攻击？Lost Door 详解

亚信安全最近发现了一种被称为 Lost Door 的远端存取攻击木马（RAT），它经常出现在社交媒体网站里。不过最令人惊讶的是，这个远端存取木马所发动的网络攻击会通过路由器端口进行病毒转发，它可以借助这个转发功能，让远端系统连到内网里指定的电脑或服务。一旦网络黑客通过远端攻击来掩盖自己在网络内的活动，那么他们就可以避免被侦测，并让网络用户陷入到病毒布局，从而肆意蔓延网络威胁。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574972&idx=1&sn=3173c7909d3efeb6f20efecf827a0891&scene=4#wechat_redirect

❖ 全球 2 亿帐号被卖 1 美元，你的隐私还有保障么？

你是否算过人的一生中有多少个帐号密码？不论储蓄卡、信用卡、社交账号、网络购物账号，凡是最常用的相信你都会牢记于心，当作自己最重要的资源。然而，当你的个人资料得不到安全保障，就像平日里各种广告电话打到你手机，向你推销那些不相干的产品时，此时此刻，你的电话、姓名其实已经成了废料，在别人的眼里，它好似纸屑一般没有任何的价值。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574966&idx=1&sn=a5f2c05297947dfdaf1d54b6f843053e&scene=4#wechat_redirect

❖ 亚信安全拍案说法：银行大劫案其实不用“枪”

最近有很多关于越南、孟加拉、厄瓜多尔银行被抢劫的报道和讨论，这三个案例均涉及全球银行结算（SWIFT）系统。而为了搞清楚黑客入侵银行事件的始末，我们首先需要涨点姿势。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574916&idx=1&sn=0b0d0ef872321bad7073c11e1e4ce759&scene=4#wechat_redirect

❖ 挟持漏洞打“暗战”，深层技术成全犯罪集团的黑暗动机

当你在使用各项网络服务时，有没有想过，如果这些前沿技术被不法之人所利用，那会是种什么状况？在这里面，网络黑客们可没有正义、正向的使用思维。

就像经常出现的攻击软件、网站及网络程序的漏洞，借助云端服务器来散布恶意程序的软件，利用社交网站段落文章和链接引诱用户掉入网络陷阱等，各式各样的网络诈骗攻击、病毒软件侵犯都紧紧包围着我们的互联网生活。可以肯定地说，不管未来出现什么样的技术与服务，总会遭到非法者的滥用。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574899&idx=1&sn=9d890cb90d9a5daec6bcdf5b7b33acc3&scene=4#wechat_redirect

❖ 医院被整蛊，又是服务器惹的祸！

前不久，美国肯塔基州的医院在一个月内居然两次遭到勒索软件的攻击。在这种网络攻击事件中，一个名为“SAMSAM”的新型变种勒索软件浮出水面，它通过捕捉系统漏洞侵入医院局域网络，加密医院重要文档，威胁院方支付赎金来解密。如果未达到勒索目的，此勒索软件将锁死损毁截获的所有文档，让医生无法进行检查结果、病例的查询，并且还会造成院内大面积的停电，使医院的运营处于瘫痪状态。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574714&idx=1&sn=071238ec730888c66317e3f14b679390&scene=4#wechat_redirect

❖ 又是勒索软件！报税季，企业税务看过来

如果说现在的网络黑客足智多谋、神机妙算，那真是对他们太过抬举或夸大。毕竟这些词汇都是用在正面事物，与那些投机倒把的颠覆行为实在是相隔甚远。但是，面对这些黑客的翻新花样，你又不得不佩服他们的“别出心裁”。网络系统中的一点瑕疵都会被他们放大利用，形成各种漏洞攻击。别的不提，单说目前恶意横行的加密勒索软件，就已经让企业用户惊恐不安了！

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650574585&idx=1&sn=cb447a4de5e5308957393428030e0890&scene=4#wechat_redirect

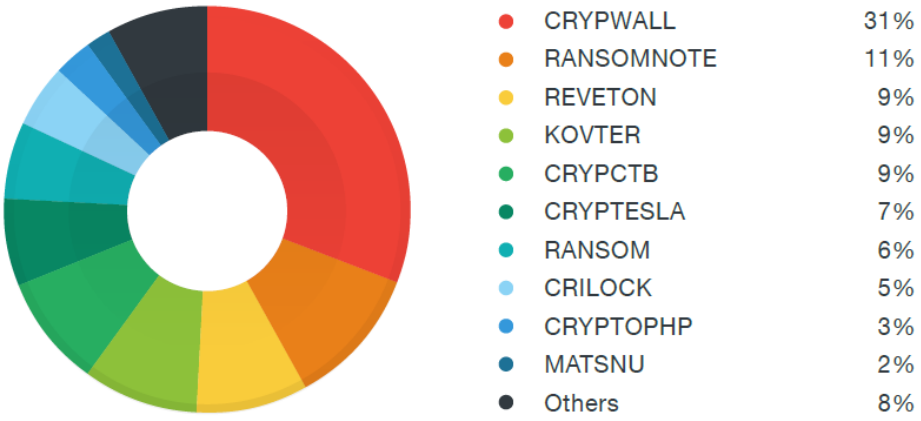
**全球区最新安全威胁概要**

以下是来自 2016 年第 1 季度全球区安全报告的数据。

*2015 年，中国地下网络犯罪仍然在全球保持领先地位，其中，POS 病毒，ATM 病毒以及袖珍分离器盗取信用卡信息占主要地位。*

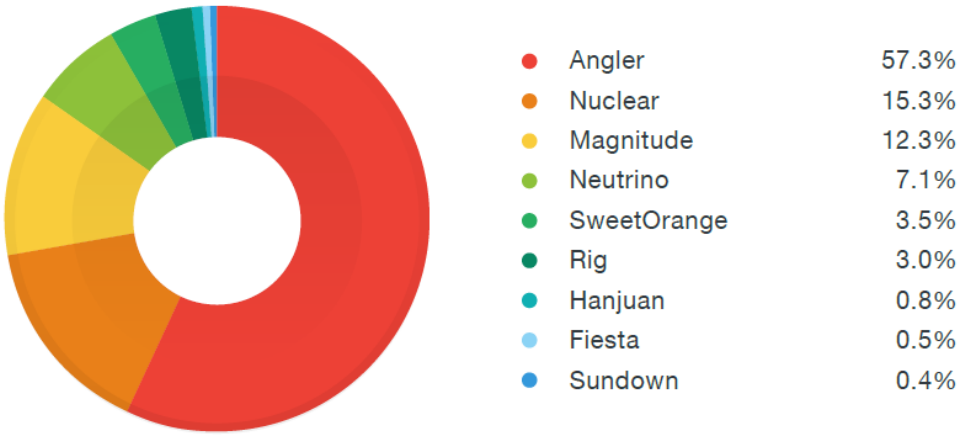

2015 年全球地下网络犯罪分布图

*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。*



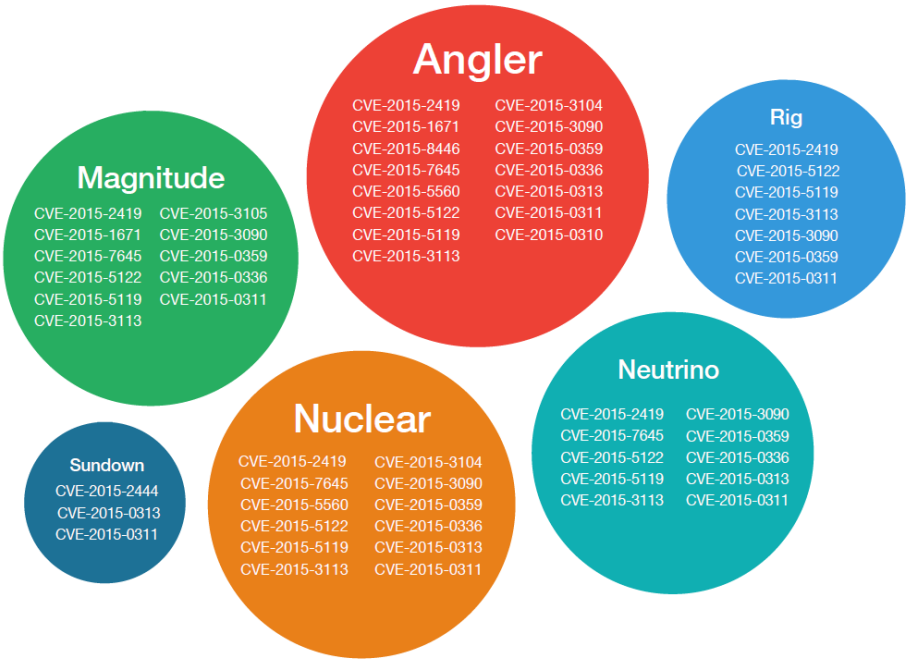

**勒索软件家族数量排名表**

*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。*

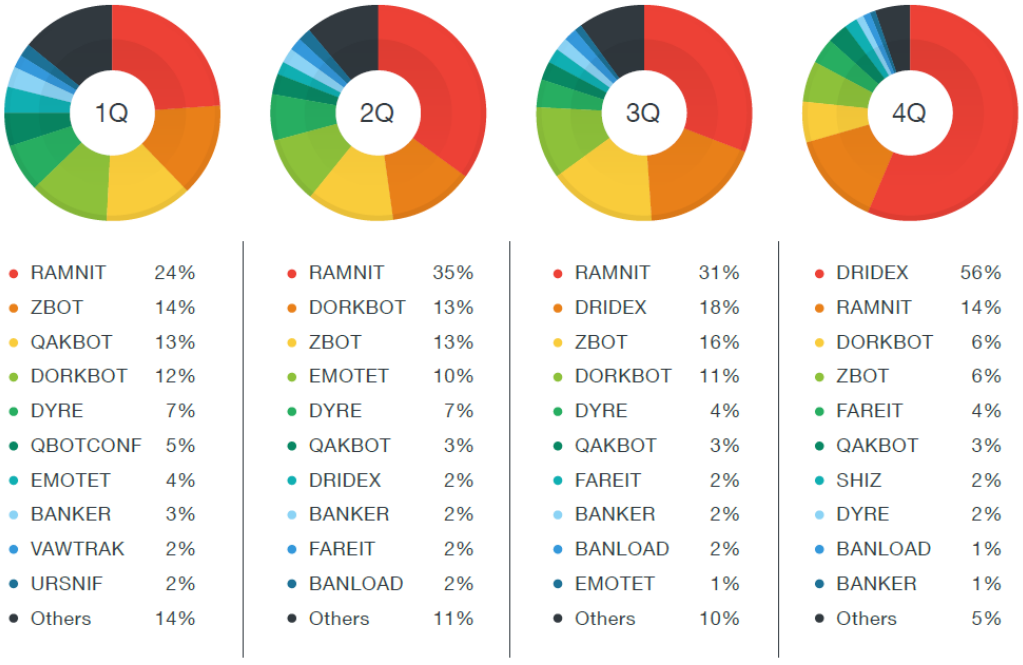



**2015 年漏洞工具包示意图**

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

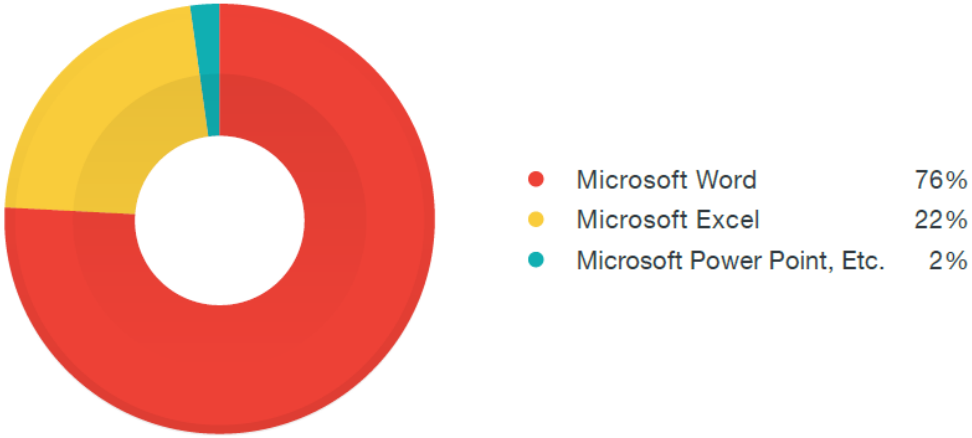
2015 病毒家族排行表

| Family | Count |
|---|---|
| SALITY | 325K |
| DOWNAD | 298K |
| GAMARUE | 207K |




**2015 银行类病毒排行表**

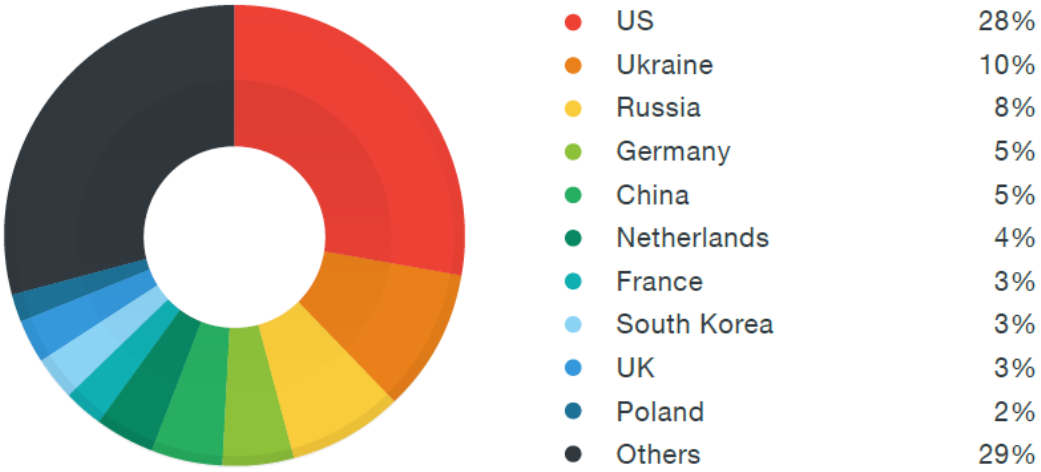
## 2015 宏病毒应用分布排行




## 2015 灰色软件家族排行

| Family | Count |
|---|---|
| OPENCANDY | 1.9M |
| MYPCBACKUP | 504K |
| DEALPLY | 407K |

2015 C&C 服务器数量全球分布图




更多关于亚信安全的威胁信息，请参看如下链接：

http://www.asiainfo-sec.com/report/index.html

## 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

更多安全资讯请您关注亚信安全官方微信：

AsiaInfo | 亚信安全