AsiaInfo | 亚信安全

亚信安全 2016 年
第三季度
网络安全威胁报告

2016/10

亚信安全网络监测实验室

目录

2016 年第 3 季度安全威胁

本季安全警示：

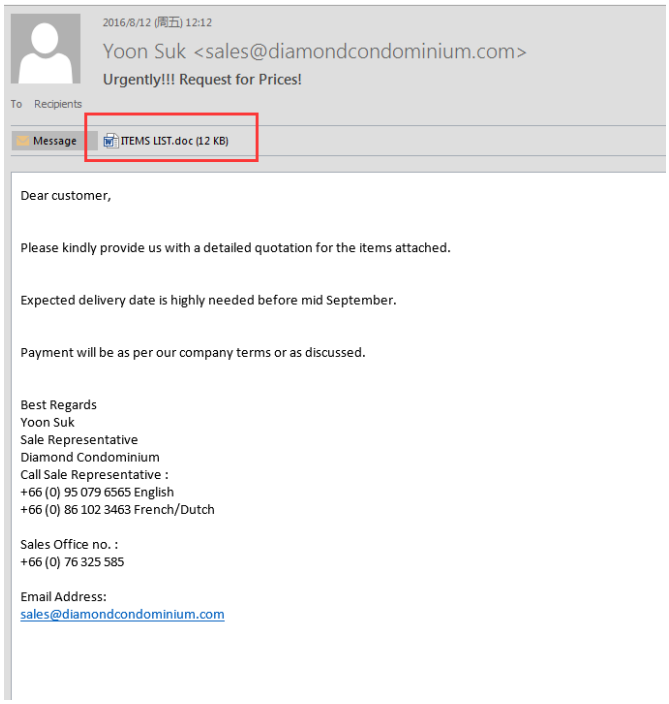
APT、ATM 大盗、物联网安全

2016 年第 3 季度安全威胁概况

- 本季度亚信安全病毒码新增特征约 **19** 万条。截止 2016.9.30 日病毒码 **12.806.60** 包含病毒特征数约 **452** 万条。
- 本季度亚信安全客户终端检测并拦截恶意程序约 **12,128** 万次。
- 本季度亚信安全拦截的恶意 URL 地址共计 **31,410,970** 次。

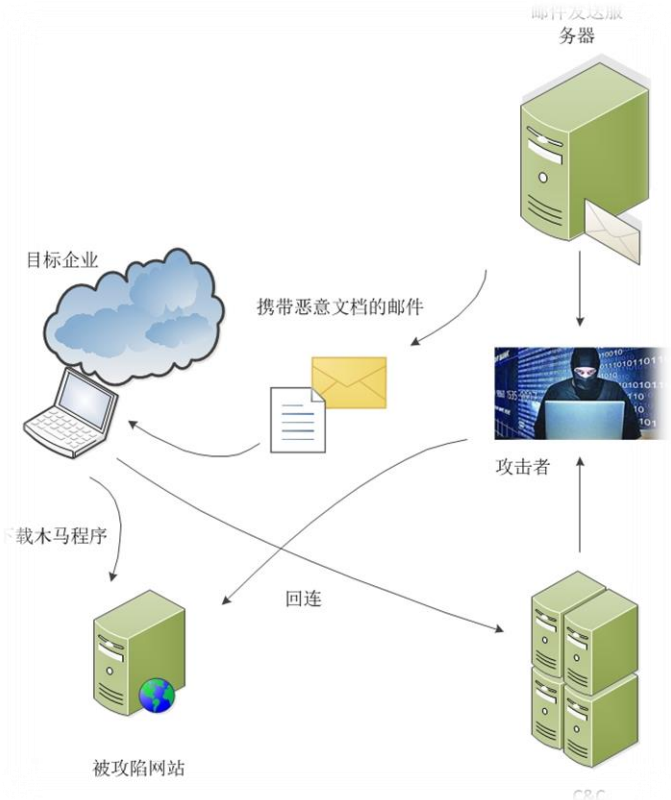
本季度热点话题为 APT，亚信安全跟踪发现 Rotten Tomato APT 组织仍在行动。

该 APT 组织主要利用 office 的 CVE-2012-0158 和 CVE-2014-1761 漏洞，携带 Zbot 攻击载荷，并利用被攻陷的网站作为木马更新的地址。攻击者通常使用邮件的方式，携带含有漏洞攻击的附件，我们监控到的发件者 IP 定位均在美国。该方式通常以电子邮件为诱饵，正文内容通常是清单、通知、快递信息等等，诱使接收者点击。一旦点击之后，精心构造好的恶意文档会利用 Office 套件的漏洞执行指定命令，向系统内植入木马等恶意程序。



携带恶意附件的邮件示例

此次 APT 攻击事件流程：



虽然该 APT 利用的是 office 的已知漏洞，但有些用户软件版本过旧以及补丁不及时，往往给漏洞利用留下通道。加上企业内部人员安全意识参差不齐，防病毒和入侵检测系统部署不到位，一封鱼叉式钓鱼邮件即可轻松直达内网，严重威胁企业信息安全，造成重要信息外泄。未来的企业信息安全要着眼于构建多层防护体制，同时也要加强员工信息安全培训，养成良好的安全意识，不随意打开陌生来源的邮件附件，定期更新系统和应用软件补丁，定期升级安全软件特征库。

本季度另一话题则是 ATM 大盗，似乎黑客们永远对银行充满了兴趣，也许这是给他们带来巨大经济利益的便捷途径，本季度黑客将目标瞄准 ATM。

7 月份台湾发生 ATM 机自动吐钱事件，总计 41 台 ATM 机被盗，被盗金额达 8327 余万元。无独有偶，一个月后，泰国 ATM 机被盗，总计 21 台 ATM 机受影响，损失达 1200 万泰铢。这两起事件均是由于 ATM 机被植入恶意程序。入侵者仿冒更新软件程序，开启 ATM 远程控制服务(Telnet Service)，上传 ATM 操控程序后，导致 ATM 机吐钞。

针对 ATM 机防护建议：

- 及时升级 ATM 系统版本
- 及时更新系统补丁程序
- 及时更新防病毒软件病毒码版本

本季度最后一个热门话题为物联网安全，随着智能设备的发展，物联网（IoT）安全备受关注，早在几年前人们对于物联网的迅猛发展就已有预测，如今市面上出现了大量基于物联网而开发的连接设备：家庭安全摄像头、婴儿监视器、胰岛素泵、心脏起搏器、健身追踪器、智能手表等。每一种连接设备的出现，都为人们的生活增添了些许的智能。

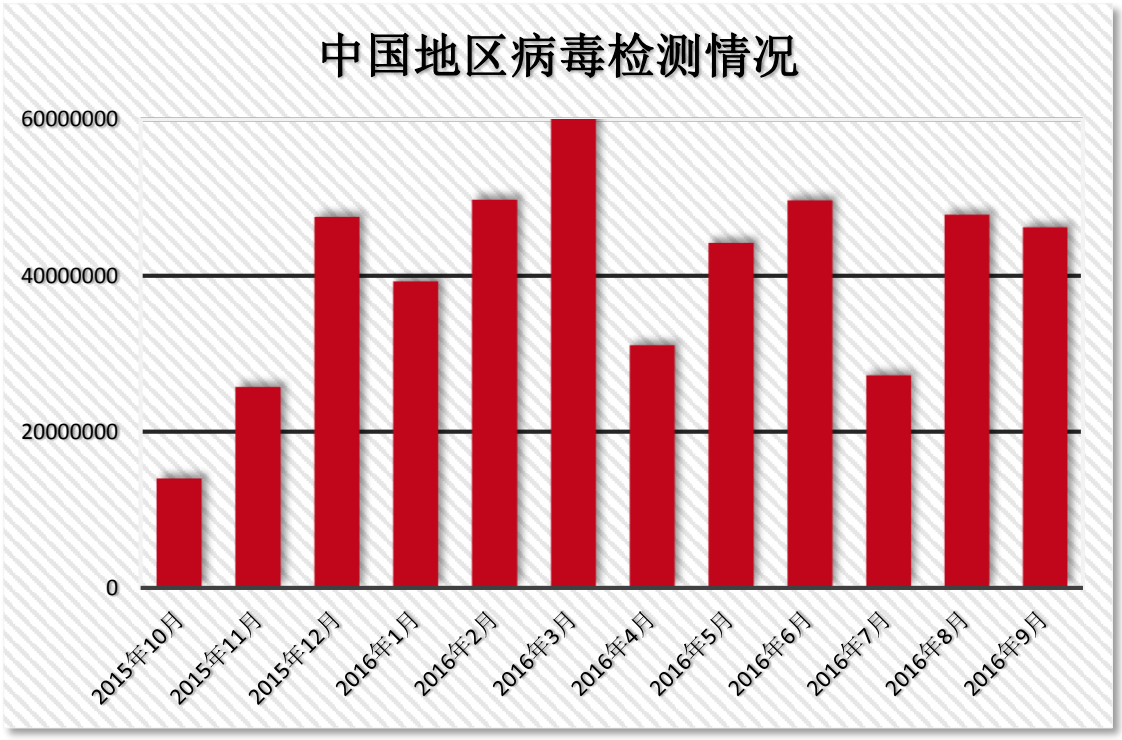
物联网在给人们生活带来便捷的同时也增添了很多安全隐患，如下是本季度发生的重要物联网安全事件。

胰岛素泵漏洞可导致患者低血糖

汽车遥控钥匙漏洞影响一亿辆大众汽车

黑客侵入闭路电视摄像头攻击珠宝店

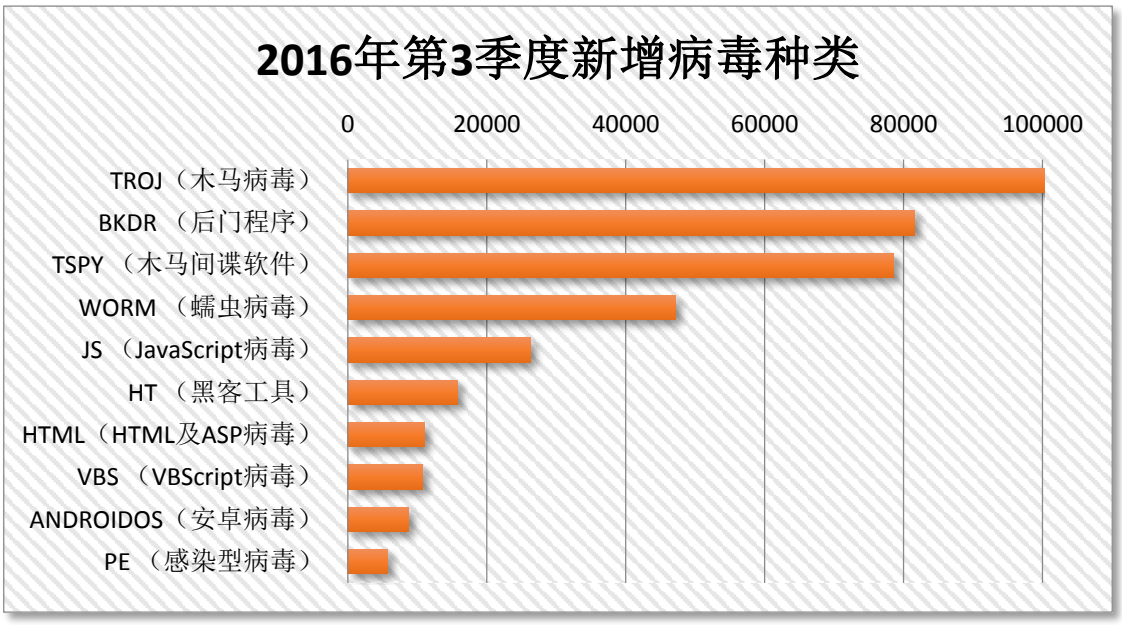
黑客入侵儿童智能手环改变地理位置并强制让用户下线



2016 年第 3 季度病毒检测数量图

2016 年第 3 季度病毒威胁情况

2016 年第 3 季度新增病毒类型分析



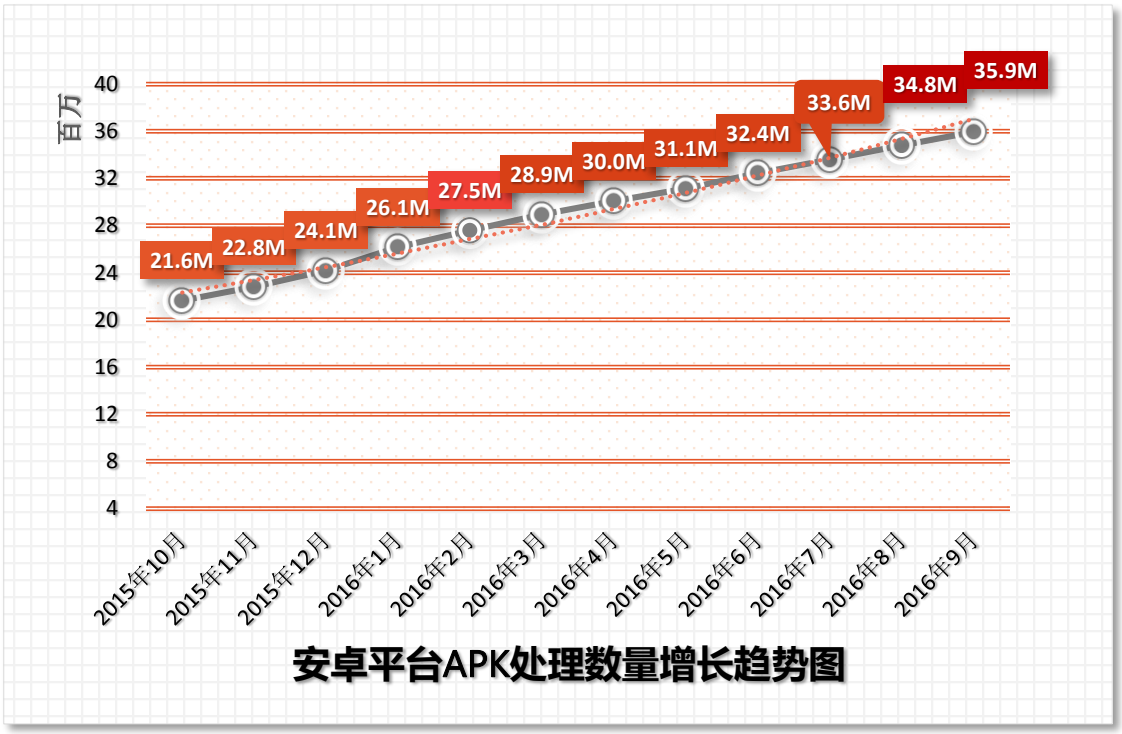
2016 年第 3 季度新增病毒类型分布图

在 2016 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 368,538 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 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。

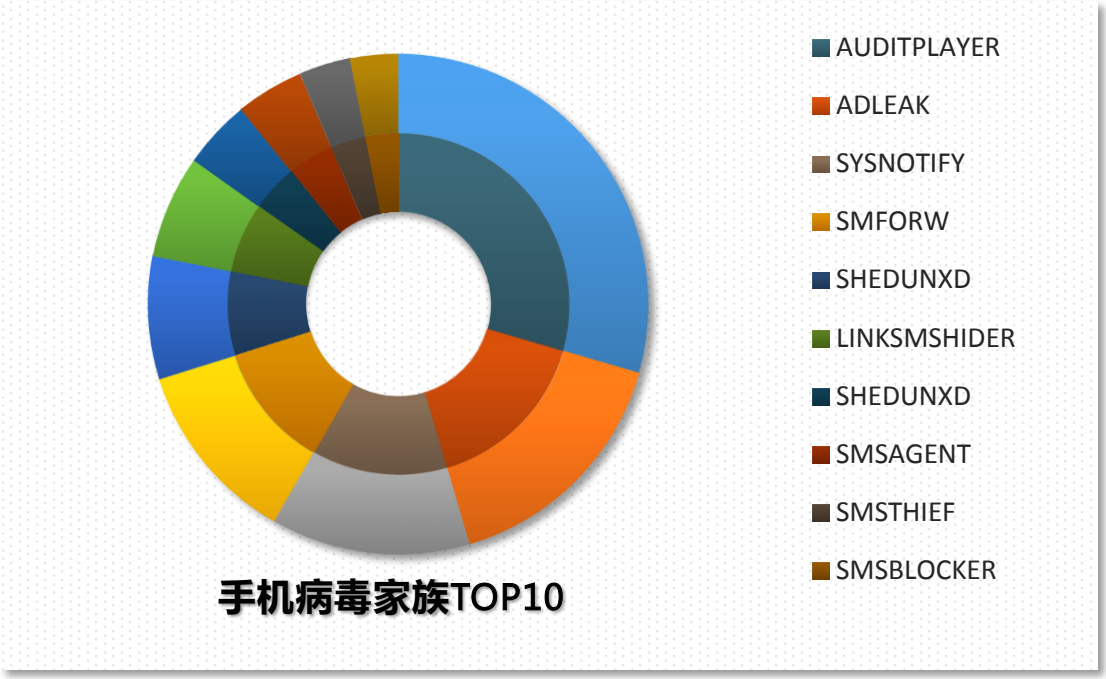
其中 JS(JavaScript 病毒)、HTML(HTML 及 ASP 病毒)类型病毒与网页挂马有关，网页挂马是攻击者常用攻击类型。一些正常网站由于自身存在的缺陷漏洞，导致被入侵者挂马，之后浏览被挂马网页的访问者就会在毫不知情的情况下自动下载恶意文件到本地。

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 3 季度安卓平台 APK 处理数量走势图

2016 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 3,595 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 3 季度手机病毒家族 TOP10 分布图

在 2016 年第 3 季度感染安卓平台的手机病毒家族中，AUDITPLAYER 家族数量最多，占到总数的 29.50%；ADLEAK 家族位列第二位，占总数的 15.94%；SYSNOTIFY 家族居第三位，占总数的 12.84%。与上季度相比，AUDITPLAYER 家族涨势凶猛，而上季度排名第一的 SYSNOTIFY 家族则有明显减弱趋势。

在 2016 年第 3 季度中，《Pokemon GO》 手机游戏风靡全球，随之而来的假冒 APP 更是接踵而来，谷歌应用商店上的一款《Pokemon GO》手机应用程序实则是假冒 APP，其实际是下载恶意程序，谷歌目前已经下架该类仿冒 APP。

另外，勒索软件也盯上此次热潮，亚信安全截获一款仿冒《Pokemon GO》APP 的勒索软件，亚信安全将其命名为 Ransom_POGOTEAR.A，该款勒索软件不仅能加密文件，还会跳出下图所示画面。

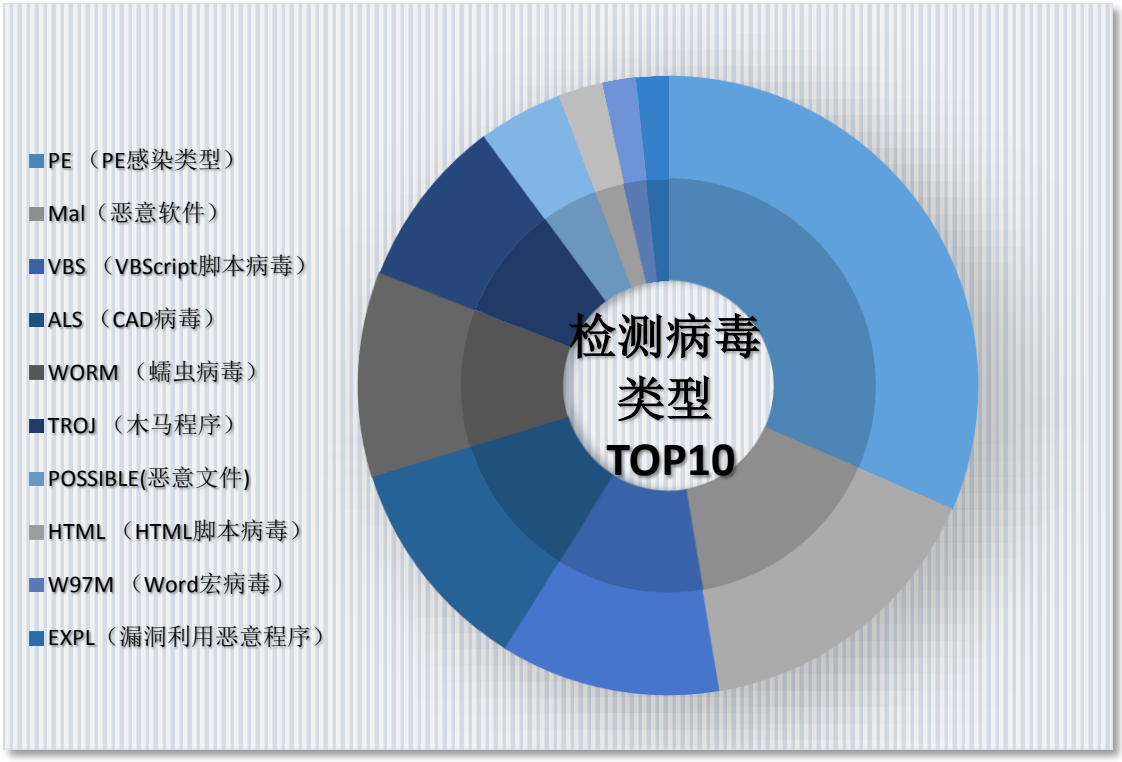
本季度中另外一个移动安全热门话题便是苹果 iOS 系统被曝出存在“三叉戟”0day 漏洞，它可导致黑客远程控制手机，让用户信息在网络攻击中完全处于开放状态。不过，苹果公司对此也采取了紧急措施，发布了 iOS 9.3.5 系统更新，以帮助全球用户化解系统危机。

此次 iOS 9.3.5 系统的紧急发布是为了修复 iOS 的三个 0day 漏洞组合，他们分别是：

- CVE-2016-4655：该漏洞将有可能导致应用程序泄漏系统内核内存中的数据；
- CVE-2016-4656：该漏洞将有可能导致应用程序以内核权限来执行任意代码；
- CVE-2016-4657：访问了精心设计的恶意网站之后，攻击者或可利用该漏洞实现任意代码执行。

这种被称为“三叉戟”0day 漏洞很容易被黑客利用，一旦用户点击黑客发送的恶意链接，就会造成短信、邮件、通话记录、电话录音、存储密码等大量隐私数据的失窃，而 iPhone 用户的则毫无察觉。

2016 年第 3 季度各类型病毒检测情况分析



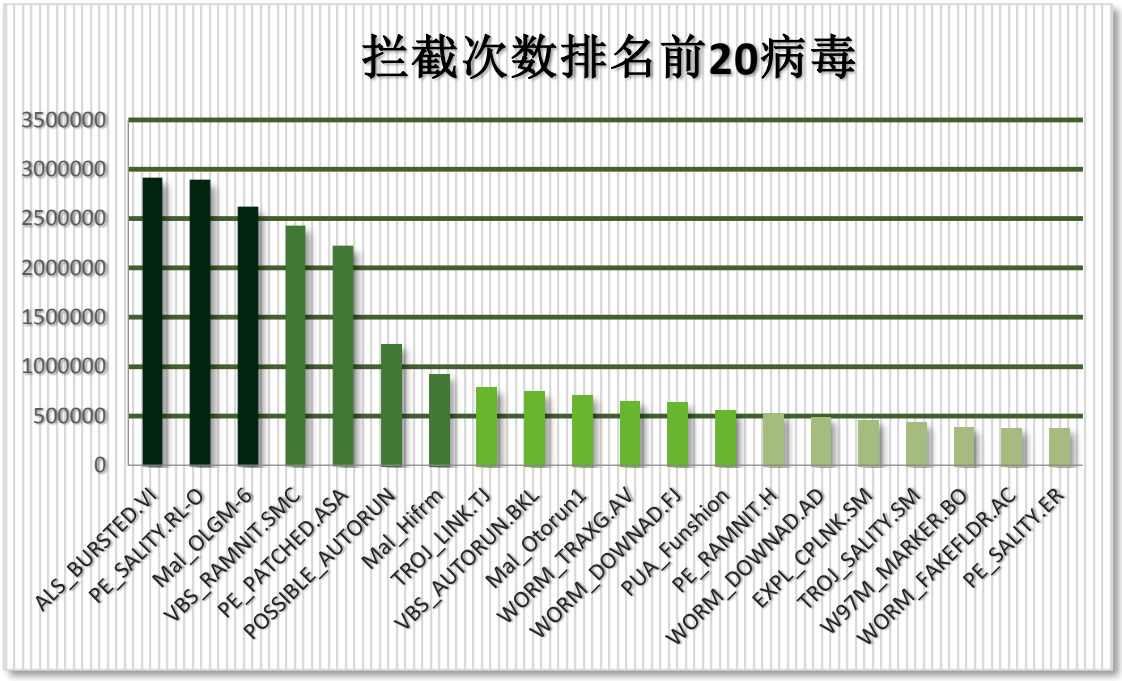
2016 年第 3 季度病毒检测类型分布图

2016 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 31%以上。在本季度中，ALS_BURSTED.VI 检测数量排名第一，此外 PE_SALITY.RL-O、Mal_OLGM-6、VBS_RAMNIT.SMC 家族检测数量排名靠前。ALS_BURSTED.VI 病毒是 AutoCAD 病毒，其主要是感染 AutoCAD 图纸文件。

本季度蠕虫病毒占检测类型总数的 10.70%，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。

本季度木马病毒与上一季度相比有所下降，该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。

2016 年第 3 季度病毒拦截情况分析



2016 年第 3 季度病毒拦截情况图

在 2016 年第 3 季度拦截次数排名前 20 位的病毒检测名中，ALS、PE 及 MAL 的感染类型病毒检测数量远高于其它检测名。

ALS_BURSTED.VI 在本季度被检测到的拦截次数约为 290 万多次，拦截次数位居榜首。该病毒为 AutoCAD 病毒，其主要是感染 AutoCAD 图纸文件。

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，Mal_OLGM-6 病毒，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。

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 3 季度热门新型病毒分析

本季度热门病毒 OSX_MOKES.A，该病毒感染目标是 OSX 系统。

OSX_MOKES.A 病毒行为流程图

病毒的详细信息如下：

病毒检测名：OSX_MOKES.A
文件类型：Mach-O
常驻内存： 是
病毒行为：链接特定 URL 或者 IP，破坏系统安全。

抵达细节：

该病毒由其他恶意软件生成或者访问恶意网站下载到本地计算机上

自启动方式：

该病毒生成如下文件：

- /Users/{Username}/Library/LaunchAgents/{Dropped Copy filename}.plist

后门功能：

- 该病毒会执行如下来自于黑客命令：
  - Record Audio every 30 seconds
  - Monitor Removable Drives
  - Take screenshots and images from installed camera
  - Search and Download MS Office documents (doc, docx, xls, xlsx)

- 该病毒通过如下 IP 地址发送和接收黑客命令
  - http://{BLOCKED}.{BLOCKED}.241.141/v1
  - http://{BLOCKED}ck12and67.com/v1
  - http://{BLOCKED}rcameand33212.com

生成文件：

- 该病毒生成如下文件保存其收集到的信息
  - $TMPDIR/ss0-{Date}-{Time}-{ms}.sst (Captured Screenshots)
  - $TMPDIR/aa0-{Date}-{Time}-{ms}.aat (Captured Audio, WAV)
  - $TMPDIR/kk0-{Date}-{Time}-{ms}.kkt (Keylogs)
  - $TMPDIR/dd0-{Date}-{Time}-{ms}.ddt (Arbitrary Data)

- 该病毒在如下路径生成自身拷贝文件
  - $HOME/Library/App Store/storeuserd
  - $HOME/Library/com.apple.spotlight/SpotlightHelper
  - $HOME/Library/Dock/com.apple.dock.cache
  - $HOME/Library/Skype/SkypeHelper
  - $HOME/Library/Dropbox/DropboxCache
  - $HOME/Library/Google/Chrome/nacld
  - $HOME/Library/Firefox/Profiles/profiled

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

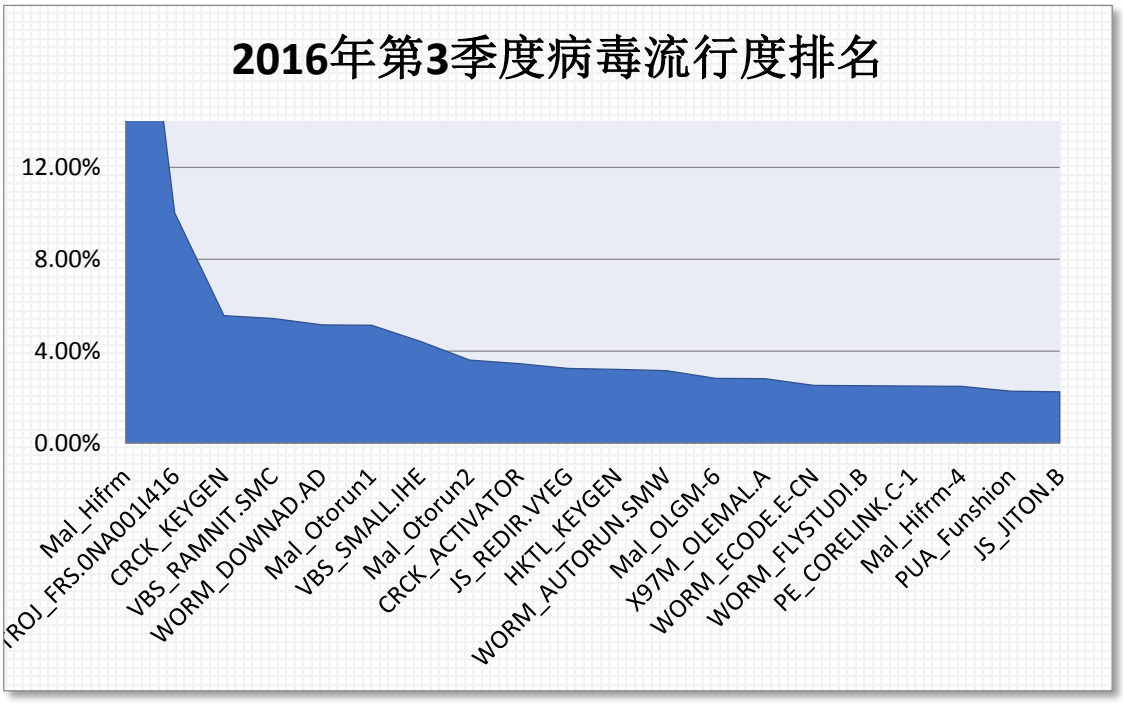
64 位 Windows 操作系统请使用：

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/osx_mokes.a

2016 年第 3 季度流行病毒分析



2016 年第 3 季度流行病毒排名情况图

2016 年第 3 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 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 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.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

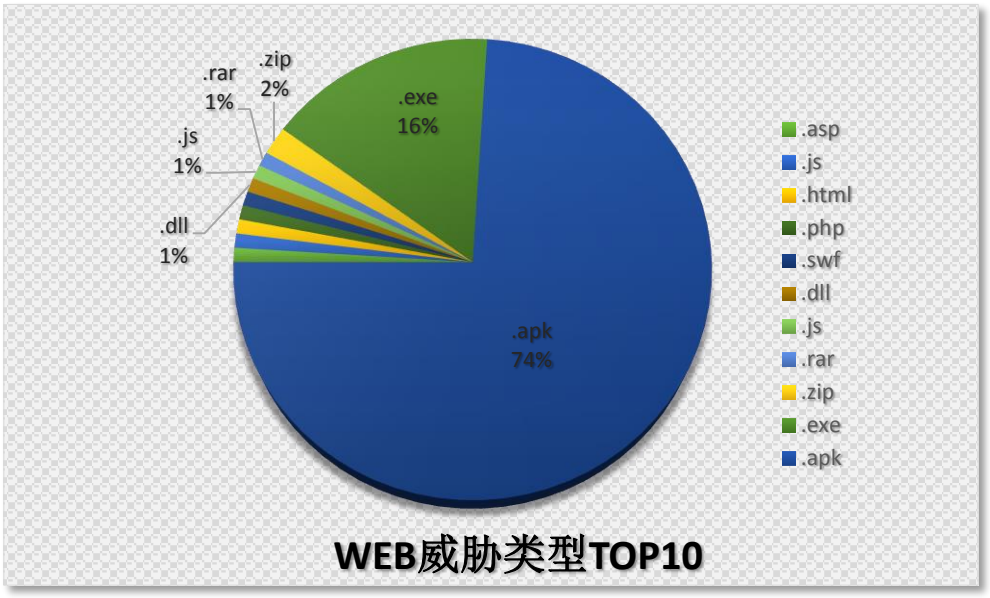
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2016 年第 3 季度 WEB 安全威胁情况

2016 年第 3 季度 WEB 威胁文件类型分析

在 2016 年第 3 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 74%，所占比例比上一季度 25%的占比有明显上升。.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.EXE、.ZIP 类型的文件位居第三位。

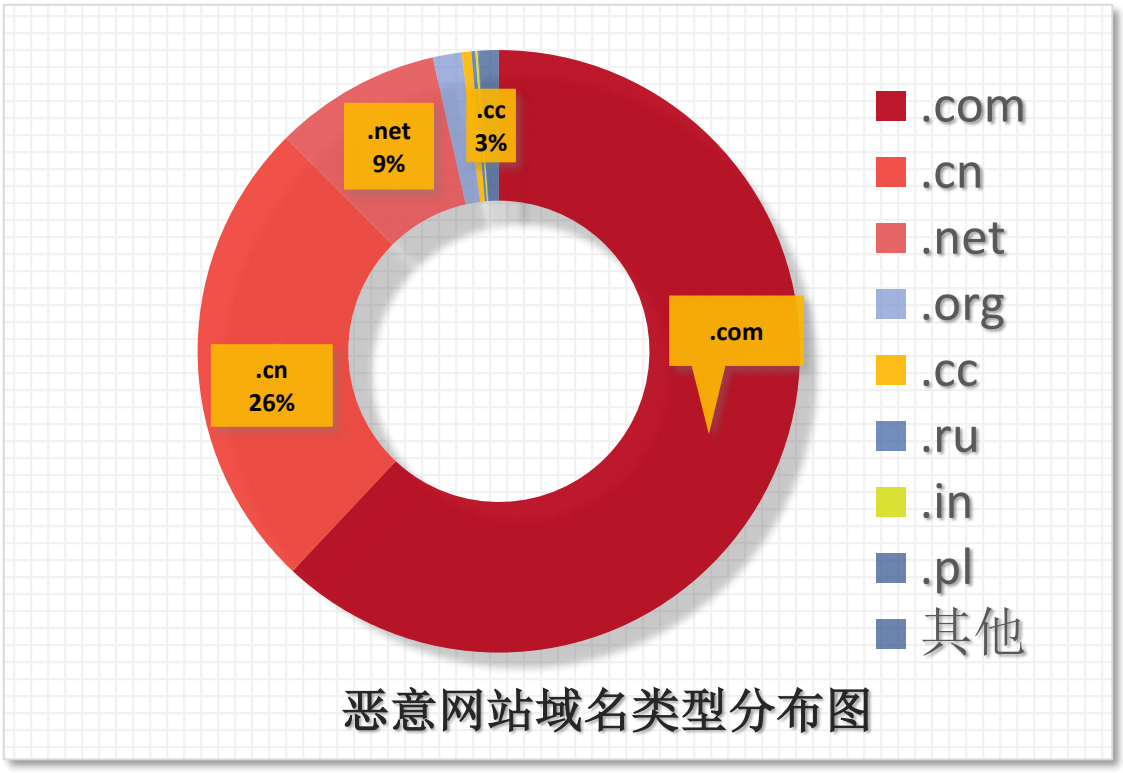


2016 年第 3 季度 WEB 威胁文件类型分布图

2016 年第 3 季度 TOP 10 恶意 URL

TOP10 恶意 URL		
恶意 URL	**描述**	**点击量**
http://api.meituvi**.com/	网站直接或间接帮助传播恶意软件或恶意代码	2217685
http://www.11**oyu.com/	网站直接或间接帮助传播恶意软件或恶意代码	1027664
http://download.****.cn/2345zhushou/2345zhushou_v3.1.5565_silent.exe	广告软件	732392
http://bb.ah***.com:8080/	网站直接或间接帮助传播恶意软件或恶意代码	615836
http://101.***.162.149/cgi-bin/micromsg-bin/statusnotify	钓鱼网站	448220
http://www.szf***herad.com/	网站直接或间接帮助传播恶意软件或恶意代码	361315
http://optimize.****.net/uninstall/00/1408698299.zip	网站直接或间接帮助传播恶意软件或恶意代码	304423
http://110**yu.com/	网站直接或间接帮助传播恶意软件或恶意代码	273431
http://140.207.***.149	钓鱼网站	211255
http://neirong.***shion.com/download/fairyland/files/tk/9891/117278/FunKoala.dll	网站直接或间接帮助传播恶意软件或恶意代码	208085

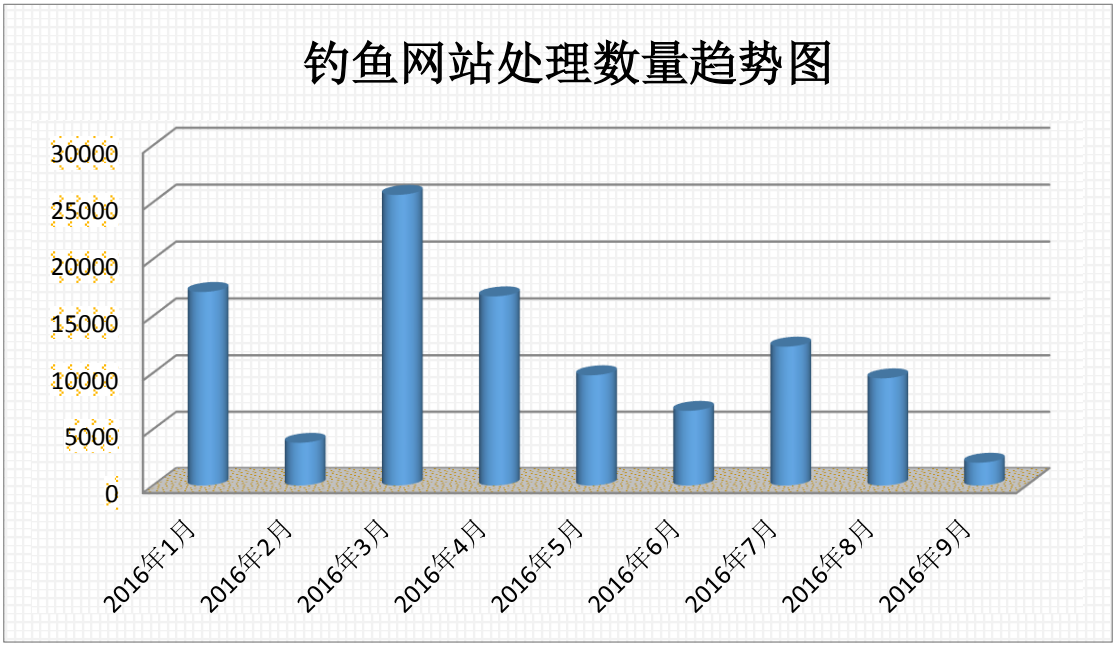
2016 年第 3 季度 WRS 拦截恶意 URL 排名 TOP10



2016 年第 3 季度恶意网站域名类型分布图

2016 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 97.00 %。其中.COM 域名的恶意网页数量最多。

2016 年第 3 季度 WEB 威胁钓鱼网站仿冒对象分析



2016 年第 3 季度钓鱼网站数量

从中国反钓鱼联盟得到的数据：2016 年 7 月至 2016 年 9 月处理钓鱼网站共计 **23,960** 个。

2016 年第三季度，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。

第三季度的钓鱼网站域名中，主要的域名来自于.COM、.CC、和.PW 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 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	573565
MS08-067	935
CVE-2010-0806	34
CVE-2010-2568	22
CVE-2014-4113	12
CVE-2014-4148	12
CVE-2014-6271	7
CVE-2010-3333	6
CVE-2012-0507	3
APSA15-02	1

2016 第 3 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-2014-2568	*http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2014-2568*
CVE-2014-4113	*http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2014-4113*
CVE-2010-4148	*http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2010-4148*
CVE-2012-6271	*http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-6271*
CVE-2012-3333	*http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2012-3333*
CVE-2013-0507	*http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2013-0507*
APSA15-02	*https://helpx.adobe.com/security/products/flash-player/apsa15-02.html*

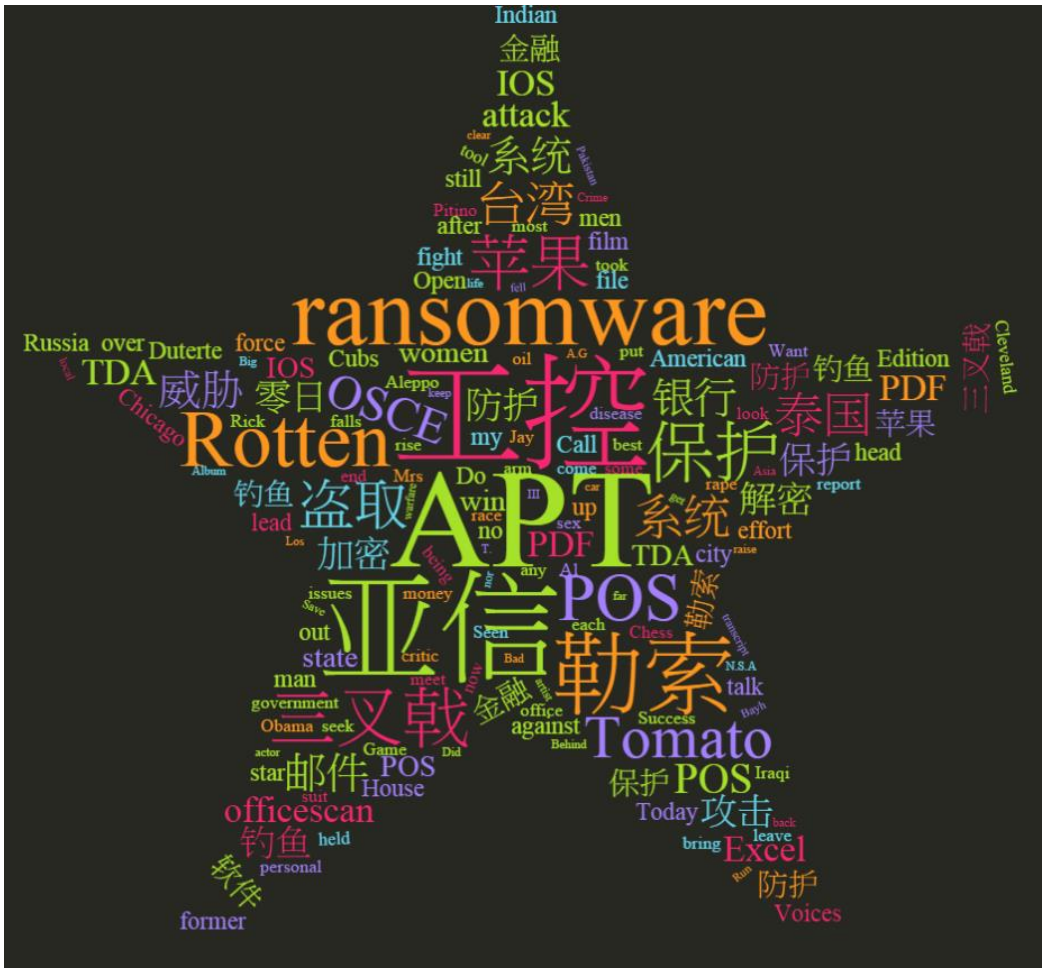
漏洞介绍链接

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 3 季度最新安全威胁信息

2016 年第 3 季度安全威胁信息摘要



2016 年第 3 季度国内外安全威胁信息关键词

❖ DDoS 攻击再发难，游戏产业竟成俎上之肉

最新调查显示，从 2015 年第二季度至今，DDoS 攻击总数已增长了 129%。在这里面，超大型攻击的数量呈上升趋势，最大 DDoS 攻击规模已达到 363Gbps。

犯罪集团之所以喜欢通过 DDoS 攻击来攻击服务器，一方面是因为犯罪者可通过网络便捷获取 DDoS 攻击工具，攻击难度大幅降低；另一方面，攻击服务器可以为犯罪分子带来高额的利润，它每秒发送的数据量是 PC 端的 100 倍，这些数据很容易消耗目标服务器的系统资源，造成数据丢失乃至崩溃，方便犯罪分子通过威胁或者被竞争对手雇佣的方式获得经济收入。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650576271&idx=1&sn=3a4b33444672958b09bf37640048e514&chksm=beede711899a6e0771d3e98d94a51cd0e2e65f54dd3435b9c13c01380f563cbd41a8b72294b8&scene=4#wechat_redirect

❖ 勒索病毒频“变脸”，从 RAR 到 JavaScript 迷乱用户

网络犯罪分子经常利用 JavaScript、VBScript 和 Office 宏文件等文档类型来躲避传统的安全解决方案，各类电子邮件附件及勒索病毒在这些文档类型中也不断产生着变化。在今年上半年，亚信安全中国病毒实验室封锁和侦测到了 8,000 万次的勒索病毒威胁，绝大部分都来自电子邮件附件档，这其中 Locky 的垃圾邮件中传递最快、勒索攻击最为活跃。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650576261&idx=1&sn=4069604d89f9452f5c9f9eb557bb7e0f&chksm=beede71b899a6e0dc2cf03c55634abe92b3fa662f9d4e8f42841364e862f187758d7a83f39d6&scene=4#wechat_redirect

❖ 【黑客新玩法】捣毁 ATM 系统，坐等“千万红包”!

台湾第一银行自动提款机现金被盗事件估计大家还记得，当时的网络黑客利用远程操控模式让银行的 34 台提款机自动吐钞，直接盗取 7,000 万新台币；而后，八月份在泰国出现的自动提款机盗窃事件，使得资金损失达到了 1,229 万泰铢。由于这种盗窃事件的数量不断攀升，银行自动提款机已逐渐成为财产损失的重灾区。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650576191&idx=1&sn=019acc1b0e84e45d422595cc134c67c8&chksm=beede7a1899a6eb7e5f7b8df43d02c5fd32acdbb925369c48c156a7d460b079cf13d677914ba&scene=4#wechat_redirect

❖ Cerber 勒索病毒霸占云平台服务　已成企业发展的拦路虎

很多企业认为，企业云是互联网发展的重要节点，它构建了网络技术的新格局。然而，网络犯罪分子总能与时俱进，他们利用云平台服务传播恶意程序和病毒，这让一些还没完全了解云服务的企业颇为困惑：云到底怎么用才有利而无害？

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650576176&idx=1&sn=d83d1a8092ffeeb62b292e507852129f&chksm=beede7ae899a6eb8016c30bfd7b7eef5b63aec98a77c3e03105c9462489d537358e7f3ac5f80&scene=4#wechat_redirect

❖ APT 攻击涉入采矿业，网络威胁已影响社会经济命脉

高级持续性威胁（APT）到底有多凶险？它不仅侵蚀着互联网的信息与资产，就连现实中的天然资源都成为了侵占目标。网络黑客把罪恶之手伸得如此之长无疑是关乎着巨大的利益链。今天，就由小编带领大家探秘 APT 黑客是如何攻击矿产资源、他们的目的又究竟在何处？

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650576158&idx=1&sn=01c32f07fb3fffbdc3777daba3cf9c86&scene=4#wechat_redirect

❖ 看!!! 黑客是如何利用“你”的好奇心传播病毒

收到带网址链接的陌生短信你会怎么处理？打开？回复？不理？删掉？可能你有一定的警惕性，不会直接打开，以防手机中毒；但是如果你出于好奇，认为回复一下没事，那么就“恭喜”，你-中-招-了！

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650576151&idx=1&sn=4126bff2a3dfc296f0c018543c122d4f&scene=4#wechat_redirect

❖ 【APT 威胁预警】HangOver 降临中国企业，网络钓鱼一触即发！

一个来自于南亚的 APT 组织 HangOver 在近段时间格外活跃，该组织主要从事网络间谍活动，专门窃取敏感信息。从 2009 年至今，HangOver 对不同国家至少发动了 3 次攻击行为和 1 次疑似攻击行为。它利用大量系统漏洞，制造繁杂的恶意代码（目前数量已达千余个），对 Windows 系统进行打击，同时，Mac OS X 系统和 Android 系统也依次成为了该组织的侵占目标。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575995&idx=1&sn=ac15fb38b0d1ac482678c8e83228fc83&scene=4#wechat_redirect

❖ WARNING!! 2016 全球最可怕的网络病毒都是哪些？

2016 年是个名副其实的勒索之年，而且攻击手段变化多样、不断翻新。从亚信安全 2016 上半年的全球安全资讯评估报告中看出，目前已进入一个“勒索病毒当道的时代”。其中，勒索病毒已增长了 172%；同时，擅于攻击漏洞的变脸诈骗攻击（BEC）也造成了 30 亿美元的损失，可以说，网络用户被黑客接连勒索敲诈，祸不单行。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575947&idx=1&sn=4a88bb42a5f7a89b8a6fd990e81c1e46

&scene=4#wechat_redirect

❖ Dropbox 再曝泄密危机，亚信安全建议企业用户部署安全的私有云存储

公有云脆弱的安全性再次成为风口浪尖上的热门话题。近日，美国云存储服务公司 Dropbox 确认，2012 年时发现并披露的一次数据泄露事故影响要比之前预计的更严重，此次数据泄露事故影响范围超过 6800 万账号。亚信安全建议企业用户在对数据资产进行共享、协同办公时，应选择高安全、强加密的私有云存储解决方案。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575942&idx=2&sn=3994aff8d45100ee87f6e154e46bfade&scene=4#wechat_redirect

❖ 解药来了|如何不让你的网络存款人间蒸发

网络银行为用户提供了许多便利，但也给诈骗分子带来了可乘之机。不少黑客利用网络技术窃取用户资金，制造了多起诈骗事件。今天，我们就一起看看近几年发生的著名银行木马案例，同时，小编也带着满满的诚意，为大家献上解毒良药。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575902&idx=1&sn=4ba4f557343216a39366aef0b1b80879&scene=4#wechat_redirect

❖ 【揭秘最牛黑客】竟让 ATM 机源源吐钞，这也是没 sei 了.....

如今，信息安全界和执法机关已经意识到，自动取款机（ATM）已成为网络黑客的重要攻击目标。早在几年前，安全人员针对 ATM 机的恶意程序出台过一些解决措施，但是这种网络恶意行为没有被遏制，反而呈现愈演愈烈的趋势。从以往的盗窃案例看得出，犯罪者采用恶意程序窃取提款机中的现钞或磁卡信息，这样会更轻松、更隐秘，积累的“财富”也更丰厚。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575480&idx=1&sn=13baa49fd02f61ad2d01b7088f1182d4&scene=4#wechat_redirect

❖ 轻易相信网络广告=坐等中毒

一些网友认为只要不点入可疑网站就万事 OK。这主要是因为当前的主机安全系统的级别限制，无法对未知网站的威胁做出判断和应对。为了防范来自网络的各种骚扰，需要把工作系统和软件升至到最高版本，从而减少电脑漏洞引发的网络威胁。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575476&idx=2&sn=126a300c864587d92b746767f6256b08&scene=4#wechat_redirect

❖ 勒索病毒不仅仅是加密，更可怕的在这里.....

能让企业如此惊慌的网络攻击非勒索软件莫属。亚信安全并不建议受侵害企业向其支付赎金，因为这不仅无法保证受损文件能够救回，而且在未来过程中更容易成为勒索软件反复攻击的目标。不过，受害企业们却在不断倒苦水：中了勒索软件自己没的选择，现实的业务运营要中断，公司名誉受到损毁，这比损失金钱打击更大。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575397&idx=1&sn=f5d2f40f5ee759394cd305912a0a8f49&scene=4#wechat_redirect

❖ 【预警】最新变种 Locky 竟是办公狗最大的病毒威胁

遇到了可疑文件怎么办？千万不要着急打开，因为这很有可能是勒索软件的变种体。如今“变种勒索软件”肆虐猖獗、疯狂散播，犹如蔓延的瘟疫，一旦侵入到你的电脑系统，所有重要文档就会被加密锁死！近日，亚信安全截获了最新 Locky 勒索软件变种 JS_LOCKY.DLDVF。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575306&idx=1&sn=b5893d3d164f871ed3bd90c9d03f3374&scene=4#wechat_redirect

❖ 中国成为勒索软件感染最严重国家之一，2016 增长数量超过 67 倍

今天，亚信安全发布了最新的勒索软件风险研究报告，分析了 2015 年 9 月-2016 年 6 月的勒索软件增长以及防治态势。报告指出，在监测的十个月内，全球传播的勒索软件数量增长了 15 倍，中国勒索软件数量增长更是突破了 67 倍，这凸显了勒索软件日益严峻的威胁形态。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575276&idx=1&sn=4c626b1596b84076a9adbf3b2286de75&scene=4#wechat_redirect

❖ 金融再遇难，超级“隐形木马”洗劫台湾第一银行 7000 万新台币

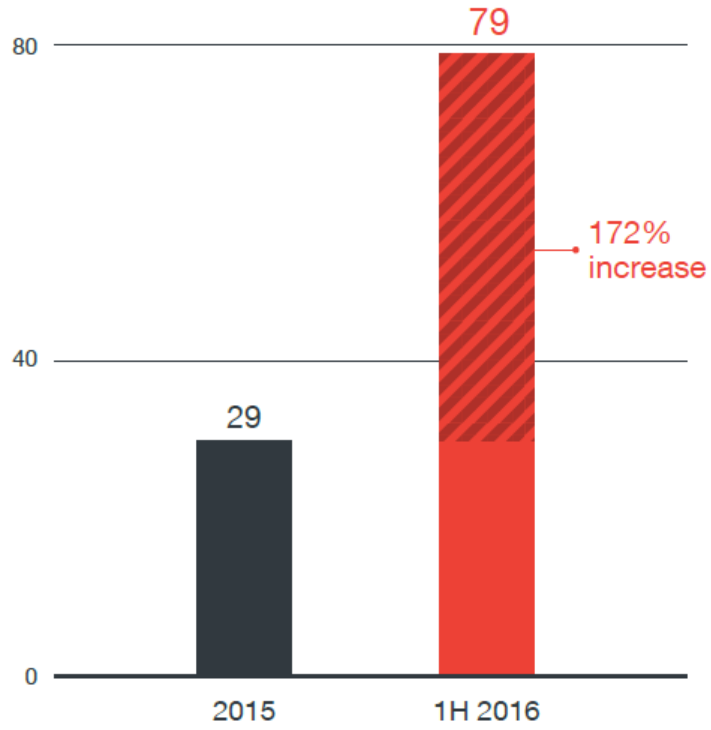
根据台湾“中央社”7 月 12 日报道，由于黑客系统的侵入，造成台湾第一金控旗下第一银行（简称“一银”）部署的 34 台自动取款机（ATM）被恶意操控，致使该银行超过 7000 万新台币被盗领。

http://mp.weixin.qq.com/s?__biz=MjM5NjY2MTIzMw==&mid=2650575253&idx=1&sn=bf4a9babbf47c3318744fb71fda9f31c&scene=4#wechat_redirect

全球区最新安全威胁概要

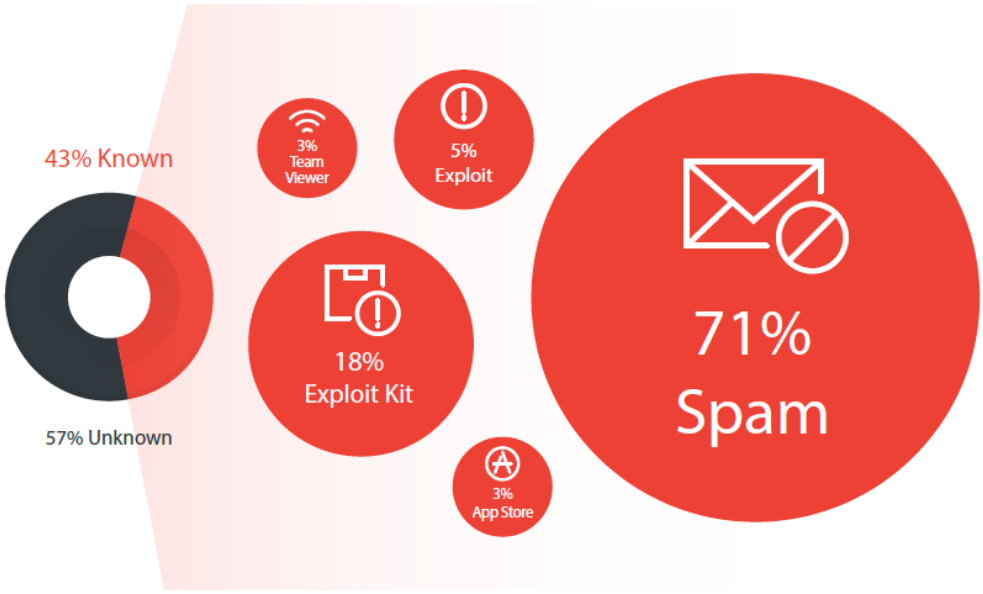
以下是来自 2016 年第 2 季度全球区安全报告的数据。

2016 年被预测为勒索之年，上半年勒索软件种类大增，与 2015 年相比，增加了 79 种，增长幅度达到 172%



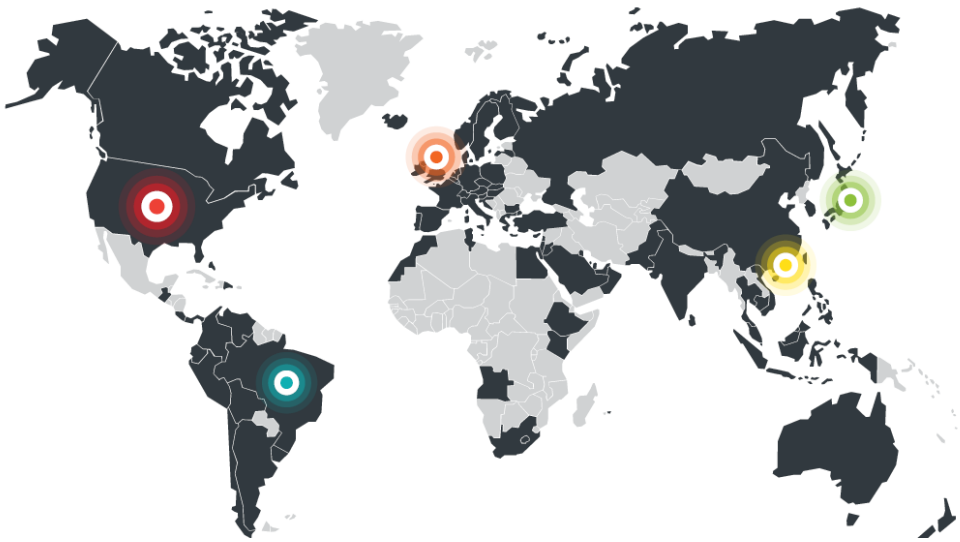
2015 年与 2016 年勒索软件种类数量对比图

勒索软件主要通过垃圾邮件传播，还有一些是通过 URL 下载或者是漏洞利用工具包。



勒索软件传播方式分布图

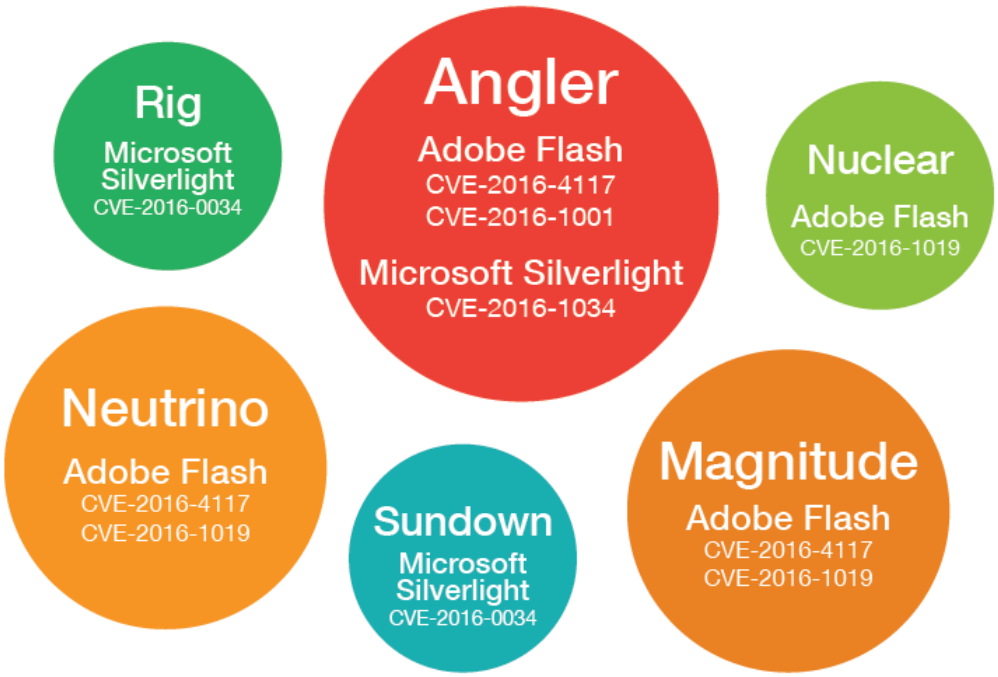
企业邮件诈骗对企业威胁巨大，据 FBI 统计，2015 年 1 月-2016 年 6 月共有 22000 受害者，累计损失达 30 亿美元



受 BEC 感染地区分布图

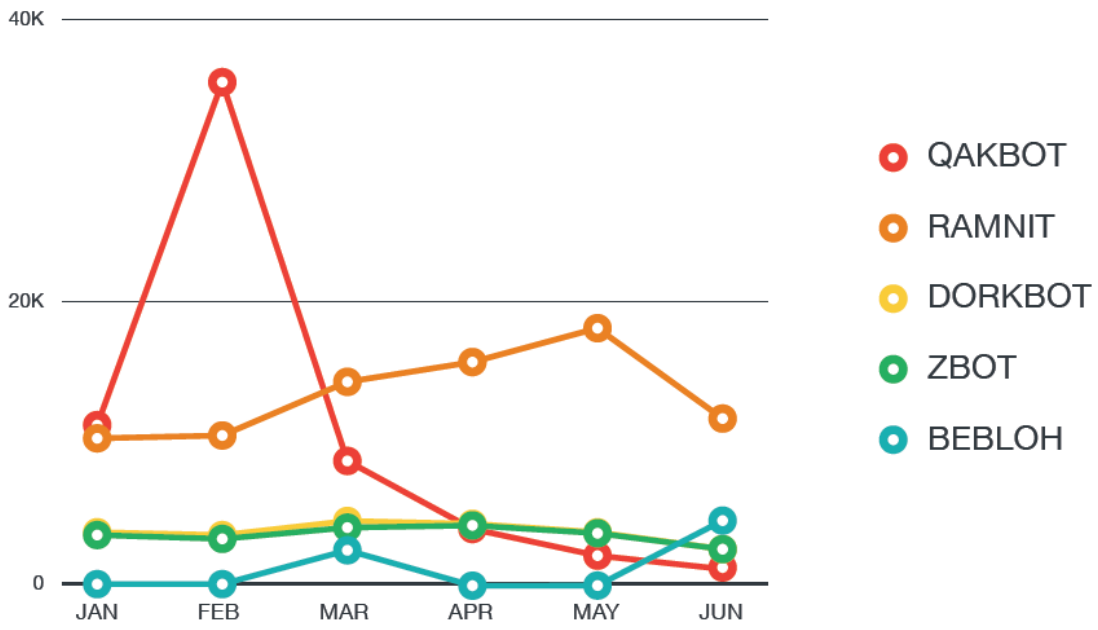
本报告数据来自亚信安全智能防护网(SPN)以及亚信安全 TMES 监控中心(MOC)

2016 年新增漏洞工具包主要是针对 Adobe® Flash Player、Microsoft Internet Explorer 和 Microsoft Silverlight



2016 新增漏洞工具包

2016 年上半年银行类木马中，QAKBOT 木马居首，其次 RAMNIT



2016 银行类病毒排行表

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