中国地区第一季度
网络安全威胁报告

2011/4

目录

2011 年第 1 季度安全威胁

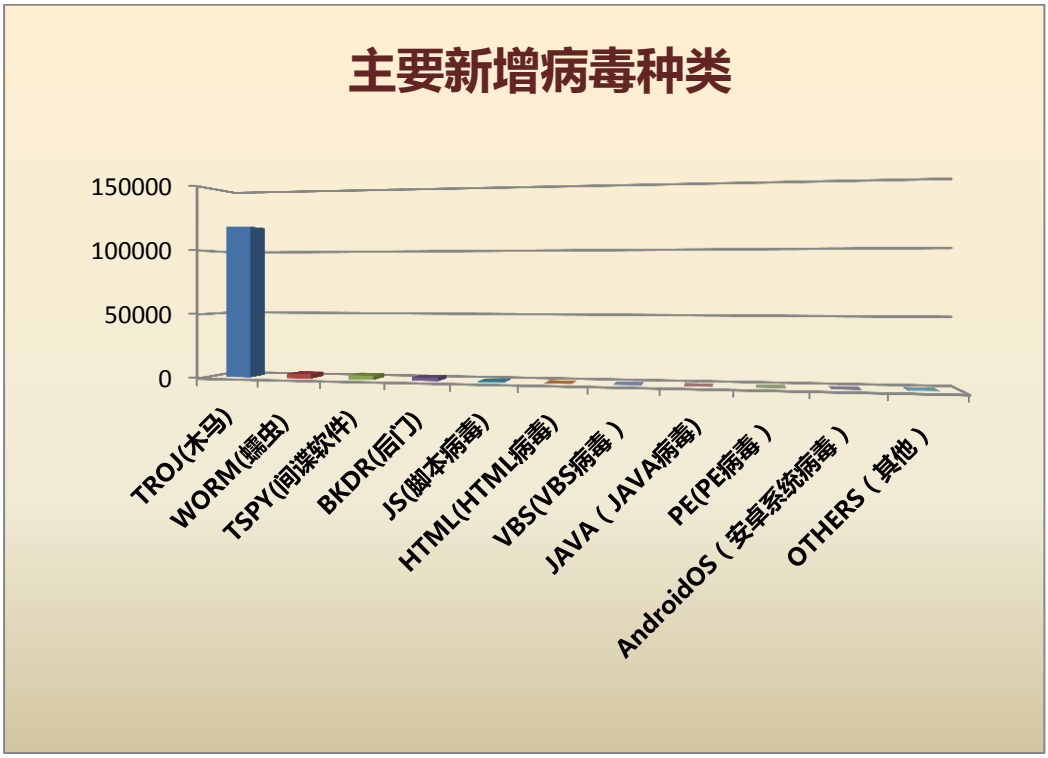
本季安全警示：
蠕虫以及 PE 感染型病毒

2011 年第 1 季度流行病毒概况

- 本季度趋势科技在中国地区发现新的未知病毒约 **13** 万种。截止 2011.3.31 日中国区传统病毒码 7.940.60 可检测病毒数量已超过 340 万种。

  新增的病毒类型最多的仍然为木马（TROJ），木马大部分有盗号的特性。木马的比其他类型的电脑病毒更加能够直接的使病毒制造者获益 。在经济利益的促使下，更多病毒制造者选择编写木马程序。

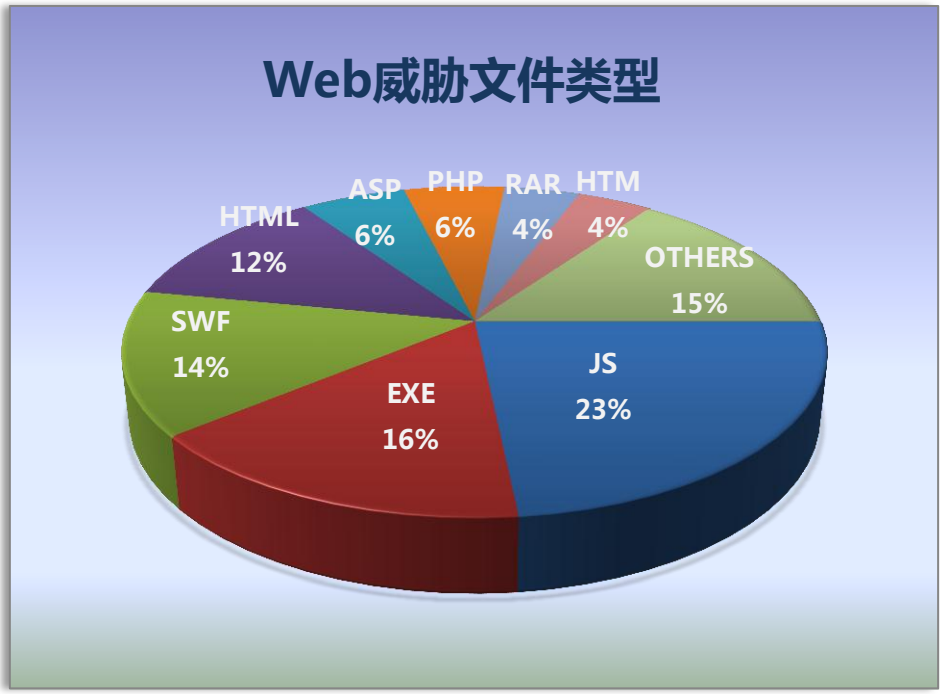
  值得注意的是本季度趋势科技中国地区新增病毒种类中 AndroidOS 类型病毒数量有明显增加。这是针对于安卓平台移动设备上感染的病毒，恶意程序的检测类型。



2011 第 1 季度中国地区新增病毒类型

- 本季度趋势科技在中国地区拦截到新的恶意 URL 地址以及相关恶意文件约 **31.1** 万个。比上季度有所增加（上季度为 **29.3** 万个）。

其中通过 Web 传播的恶意程序中，约有 **23%**为 JS（脚本类型文件）。向网站页面代码中插入包含有恶意代码的脚本仍然是黑客或恶意网络行为者的主要手段。这些脚本将导致被感染的用户连接到其它恶意网站并下载其他恶意程序，或者 IE 浏览器主页被修改等。一般情况下这些脚本利用各种漏洞（IE 漏洞，或其他应用程序漏洞，系统漏洞）以及使用者不良的上网习惯而得以流行。



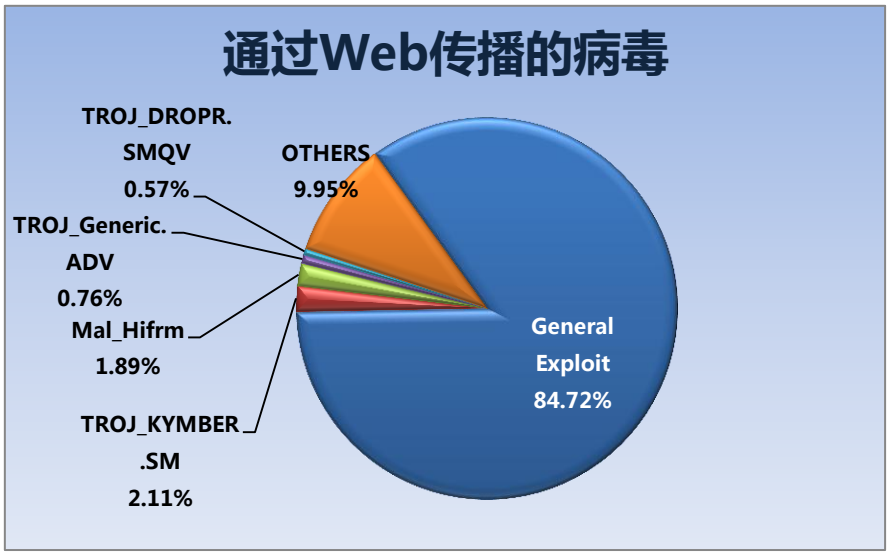
2011 第 1 季度 中国地区 web 威胁文件类型

通过对拦截的 Web 威胁进行分析，我们发现。约有 85%的威胁来自于 General exploit (针对漏洞的通用检测)。

其中包括利用 Adobe 软件的漏洞（例如：一些.SWF 类型的 web 威胁文件）。利用跨站脚本漏洞攻击，对正常网站注入恶意 JS 脚本，或插入恶意 php ，html 代码。

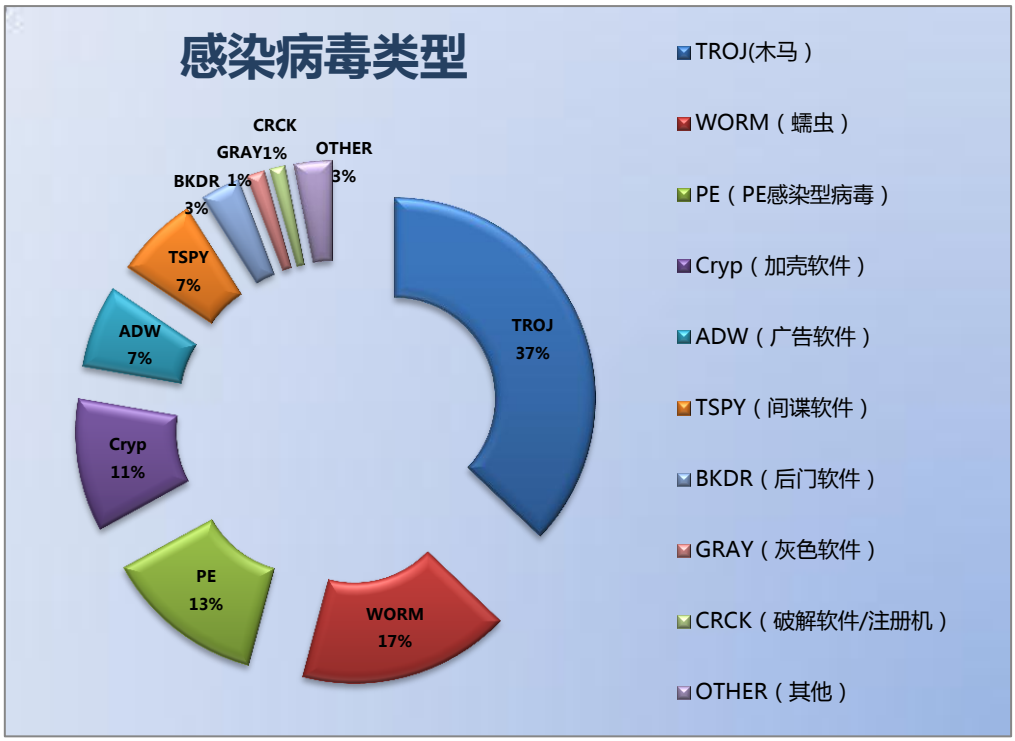
另外，在网页中置放恶意的可执行文件使用户误点或错误的下载并执行，从而导致电脑被病毒感染也是目前 web 威胁传播的一个重要类型。

Web 页面，也是木马类型病毒被下载以及传播的主要渠道。



2011 第 1 季度 中国地区主要几种通过 web 感染的病毒

- 本季度趋势科技在中国地区客户终端检测并清除恶意程序约 **6406** 万次。



2011 第 1 季度 中国地区各类型病毒感染数量比例图

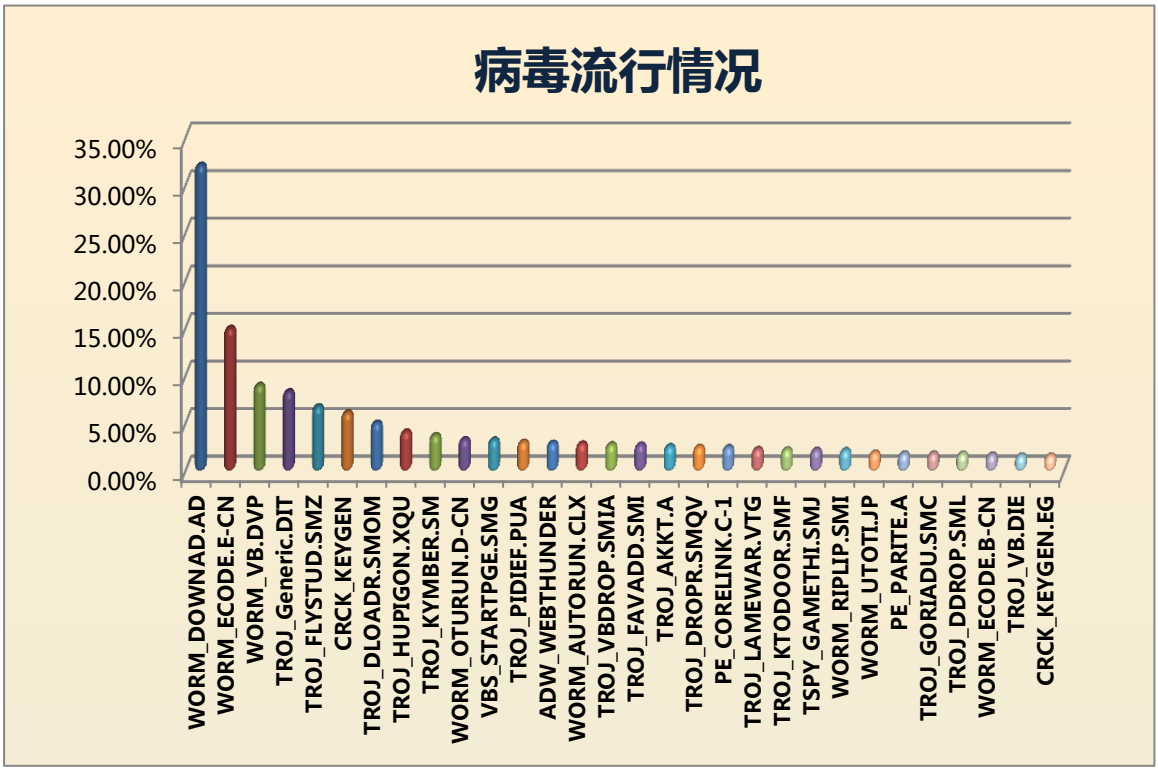
本季度木马病毒数量及所占比例均有明显上升，蠕虫病毒以及 PE 感染类型病毒比例也有所上升，分别达到了 17%和 13%。

蠕虫病毒最主要的特性是能够主动地通过网络，电子邮件，以及可移动存储设备将自身传播到其它计算机中。与一般病毒不同，蠕虫不需要将其自身附着到宿主程序，即可进行自身的复制

目前比较流行的 PE 病毒，会感染一些蠕虫或者木马病毒。随着木马病毒以及蠕虫病毒在网络内的传播导致网络环境中越来越多的电脑被 PE 病毒感染。

另外，这些病毒往往带有下载功能，被感染的文件又会连接网络下载新的木马及盗号软件。

2011 年第 1 季度流行病毒分析



2011 第 1 季度 中国地区病毒流行度排名

- 本季度最流行病毒依旧是 WORM_DOWNAD.AD,该病毒目前仍然在很多企业用户网络内流行。

该病毒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

由于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

- 本季度流行病毒中 WORM_ECODE.E-CN，WORM_OTURUN.D-CN.在前几季也有出现，但是在本季排名直线上升。

这两种检测名的病毒绝大多数为文件夹病毒。

文件夹病毒主要特征为： 被感染电脑会遍历本地磁盘目录以及映射到本地的网络共享文件夹，将查找到的所有文件夹隐藏并释放与文件夹名称相同的可执行文件 。这样用户一旦误点了伪装成文件夹的可执行文件，电脑即被感染

一般情况下，企业用户网络环境中的文件服务器或开放共享的计算机非常容易感染此类病毒。

在很多时候，防毒软件可以直接将病毒文件删除，但是如果网络内有感染该病毒的机器。则会导致被攻击电脑文件夹不断被隐藏，导致用户无法正常访问。

出现该情况的解决方法：

1. 使用系统审核策略或放火墙监控的方法找到感染源电脑
2. 对感染源电脑使用杀毒软件进行全盘扫描

- 本季需要关注的病毒 PE_VIRUX;

以上这种 PE 病毒，是 2011 年 1 季度在企业用户网络内出现的最需要关注的高危病毒。

这一系列病毒，感染手段极为复杂，并附带有多种病毒行为。能够极快的在企业用户网络中传播并感染电脑中正常应用程序。

传播途径：

1. 通过互连网下载而来
   当在互联网中搜索以下关键字时，搜索结果中即有可能包含此病毒:

keygen.exe	crack.exe	Microsoft
serial.exe	number.exe	world of warcraft
setup.exe	trend micro	f1 racing

2. 通过感染文件传播
   该病毒会感染系统中.exe 或.scr 类型文件，当感染文件被执行时，则会导致系统中更多文件被感染
3. PDF 漏洞传播。PDF 漏洞会从网上下载病毒文件，其中包括 PE_VIRUX
4. 网络共享传播
5. 可移动存储设备传播

病毒行为：

注入 winlogon.exe 进程，并开启后门从而将 windows 文件保护功能关闭

下载以下恶意文件：

- xhttp://megavipsite.cn/soft95/184/install.exe
- xhttp://85.114.143.2/is160719.exe
- xhttp://ahryafujpb.com/26.exe
- xhttp://bfahfmpyga.net/l26.exe
- xhttp://bglhnvxueb.net/exe1.exe
- xhttp://spaeioer.com/719f.exe
- xhttp://setdoc.cn/exe/0032.exe
- xhttp://59.125.229.78/x
- xhttp://horobl.cn/ex/0032.exe
- xhttp://thaexp.cn/dll/al.txt
- xhttp://thaexp.cn/ex/a.php
- xhttp://goasi.cn/ex/a.php

连接以下远程服务器：

- 61.235.117.80:80
- 61.235.117.81:80
- 58.65.232.34:80
- 58.65.234.90:65520

在受感染电脑上可能还会出现以下病毒：

- TROJ_AGENT.ALHH
- TROJ_DLOADER.UTI
- TROJ_FAKEAV.AID
- TROJ_INJECTOR.AR
- TROJ_AGENT.ATE – (supposedly a MARIOFEV)
- TROJ_DLOADR.IS

阻止用户访问以下站点：

ahnlab	computerassociates	fortinet	k7computing	pctools	sunbelt
arcabit	cpsecure	f-prot	kaspersky	prevx	symantec
avast	defender	f-secure	malware	quickheal	threatexpert
avg	drweb	gdata	mcafee	rising	trendmicro
avira	emsisoft	grisoft	networkassociates	rootkit	virus
castlecops	esafe	hacksoft	nod32	securecomputing	wilderssecurity
centralcommand	eset	hauri	norman	sophos	windowsupdate
clamav	etrust	ikarus	norton	spamhaus	
comodo	ewido	jotti	panda	spyware	

感染以下类型文件：

- .EXE
- .SCR

并在系统中以下类型文件中添加恶意脚本：

- .ASP
- .HTM
- .PHP

防护及处理方法：

1. 阻止病毒相关网站
2. 当网络中有电脑被此病毒感染时请尽快将它短网隔离处理
3. 加强共享的账号权限管理
4. 禁用移动存储设备的自动播放功能
5. 尽量避免使用破解软件及注册机
6. 及时将防毒软件病毒码更新至最新

如已经感染此病毒，请联系趋势科技中国区病毒实验室，我们将提供具有针对性的免疫工具及解决方案

2011 年第 1 季度最新安全威胁信息

- **2011 年 3 月，如果在 Google 上搜索 Lizamoon.com(中文称之为：丽莎月亮)，会发现有大量网站被 SQL 注入该网站的链接。**

报告中曾指出最近 sql 注入攻击包括了一个危险的网站——“lizamoon.com”。这里要说明，该网站并非受害者，而是于 2011 年 3 月 25 日通过注册虚假域名建立的。

这次事件涉及的其他一些网站可能真的是被利用了，但是却也都是可疑的。因为它们均过期将近一年，并使用 gmail 或 hotmailbox 账户注册域名，而且当前大部分已经失效了，只有一部分网页还能浏览。

趋势科技已经将所有涉及此次事件的网站屏蔽。使用了 Web Reputation 的用户不会受到此次事件影响。另外，Deep Security 能主动阻止 SQL 数据库注入攻击。

在这些攻击中，常见的案例是使用 FAKEAV 作为罪犯手段。FAKEAV 是一种攻击手段多样的恶意软件，常常欺骗用户以悄无声息地传播其他恶意程序。一些特定网站，如“defender-uqko . in”，在之前就与 FAKEAV 攻击有关，这些 FAKEAV 会携带其他恶意程序，如 koobface。另外于 3.12 日注册的“Alisa-carter . com”也携带了 FAKEAV。

其他涉及此次事件的受害网站还有“koreandvds . com”和“thailandmedicaltourismcluster . org.”。

应说明的是 sql 注入攻击并非才出现的威胁。事实上，它们和以社交网站用户为目标的恶意程序诈骗手法一样常见。

http://www.zdnet.com/blog/security/mass-sql-injection-attack-leads-to-scareware/8510

- **2011 年 1 月，很多中国银行网银用户收到网上银行 E 令升级的诈骗短信。随后登陆短信中提到的相关钓鱼网站，导致账号中资金被盗。**

首先，被骗用户会收到 132******** 手机发送的短信。内容是:”尊敬的网银用户：您的中行 E 领即将过期，请您登陆 www.boc***.com

进行升级，给您带来的不便敬请谅解[中国银行] 服务热线 ：95566”

中国银行的官方网站网址为 www.boc.cn，钓鱼网站名字和他很接近。 并短信末尾有中国银行的客服热线。不细心的用户往往会误认为短信即为中国银行所发。

一旦用户登录短信中提示的钓鱼网站，并且进行 E 令升级的操作就很可能导致账户失窃。

目前趋势科技已将我们已经收到的所有相关钓鱼网站加入 WRS 阻止列表中，请开启相关功能进行防护。另外如果您有发现此类网站请及时联系技术支持部以已获得帮助。

网路钓鱼

为窃取个人身分资讯（最终目的为窃取金钱）意图所进行之任何透过电话、电子邮件、即时通讯 (IM) 或传真尝试取得您个人身分资讯的行为。这些网路钓鱼行为大部分皆会以合法的目的做掩饰；也就是说，它们乍看之下合法，实际上却是由不法的企业组织所为。典型的电子网路钓鱼攻击包含两种元件：几可乱真的电子邮件和诈骗网页。这让网路钓鱼成为特别难以察觉对付的危险犯罪行为，因为犯罪者善于将其用来诱骗受害者，使他们认同其合法性。采用 HTML 格式的电子邮件通常包含公司标志、色彩、图形、字型样式和其他网页素材，且主旨通常为帐户问题、帐户验证、安全性升级，及新产品或服务赠送等。这些电子邮件中的 Web 连结大都具有复制自合法网站的外观，使诈骗行为几乎无法被侦测出来。

如何分辨您是否已遭网路钓鱼

现今，若出现任何要求私密资料的状况，应视为可疑行为。合法的公司企业 - 包括银行、信用卡公司、线上拍卖网站等 - 皆不会以电子邮件要求或验证个人资讯。此外，除非您已开始要求进行此类资讯的电话对谈，否则应将此类要求视为诈骗行为。

如何保护您的电脑和移动设备不受网路钓鱼的威胁

- 保持警戒。不要依赖个人判断力来分辨此私密资料的要求是否合法。从事网路钓鱼和网址转嫁的人都是十分狡猾的犯罪者，他们善于诈骗，即便是最精明的使用者也可能会上当。
- 绝对不要向陌生的个人或公司透露个人资讯 - 尤其是在您并未启动通讯时。

- 删除所有要求私密资料的电子邮件。如果您确信此为合法要求，请使用已建立的电话号码确认该要求；仅透过电话告知此资讯。
- 购买并安装网路钓鱼防护程式的软件
- 让所有的电子邮件和即时通讯安全补丁维持在最新状态。

本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC)