中国地区 2012 年
第一季度
网络安全威胁报告

2012/04

目录

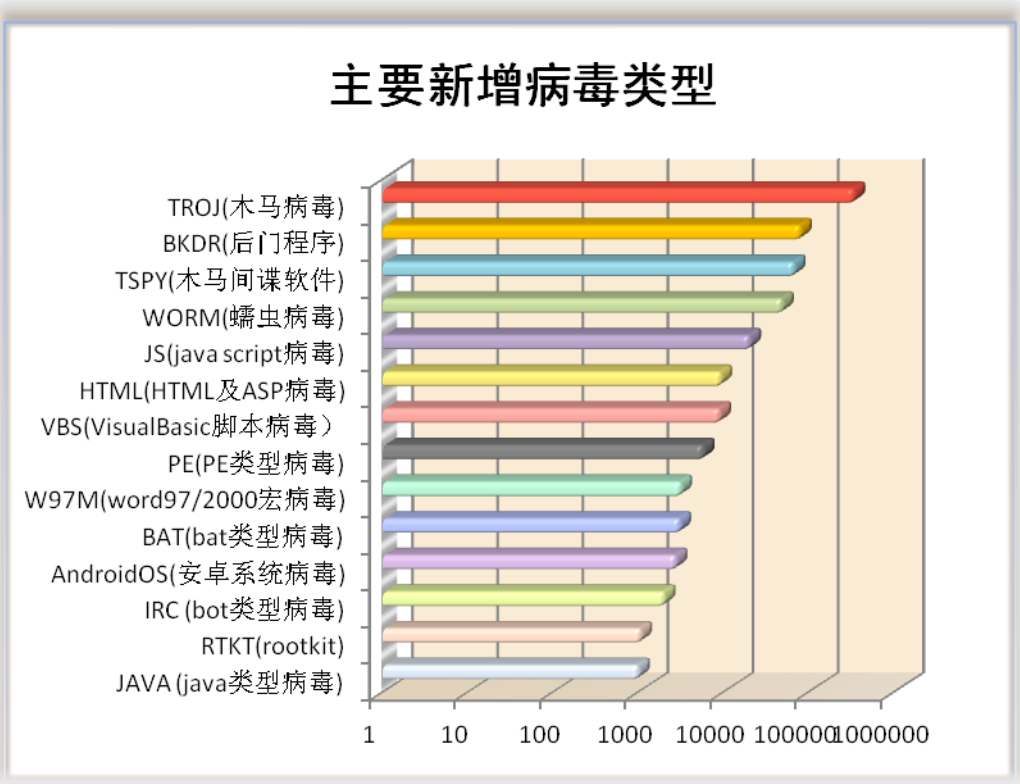
2012 年第 1 季度安全威胁

本季安全警示：

网络钓鱼、欺诈，宏病毒，PE 病毒，APT

2012 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 50 万种。截止 2012.3.31 日中国区传统病毒码 8.874.60 可检测病毒数约 370 万种。



2012 第 1 季度中国地区新增病毒类型

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。木马比其他类型的电脑病毒更容易编写且更容易使病毒制造者获益。在经济利益的驱使下，更多病毒制作者开始制造木马病毒。

2012 第一季度新增病毒种类中，java script 病毒上升到第 5 位。java script 是一种解释性的，基于对象的脚本语言，用户打开带有 Java script 的网页，网页里的 java script 就会被执行（除非用户禁用浏览器中的 js 功能）。这类病毒数量的上升可能由于更多的

网页被挂马导致。

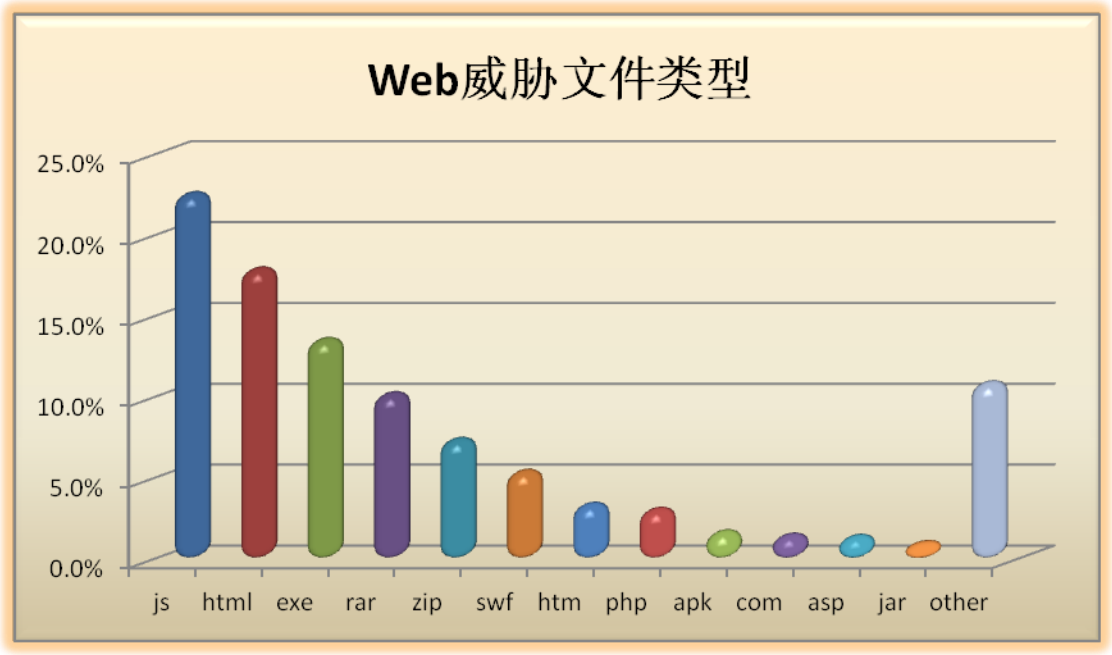
W97M/X97M(word/Excel 宏病毒) 也进入了新增病毒数量排名的前几位。宏病毒的传播速度十分快，并且不容易被发现。这是一种比较老的病毒，但是最近这种有了些历史的病毒又被翻新，并且采用了新的技术，使这种病毒可以做更多的事情。在 2012 年第 1 季度趋势科技中国病毒实验室更发现了一种新型的宏病毒 X97M_OLEMAL.A，该宏病毒除了能够通过感染 Excel 文件传播外，还会主动通过 Outlook，将正在编辑的被感染文件通过附件形式发送给其他收件人。此行为除了会使该宏病毒传播更广泛外，还可能会导致 Excel 文件的内容泄漏。

IRC 病毒(IRCBOT)也值得我们特别的关注。IRC（internet relay chat）是一款功能强大的即时聊天协议，IRCBOT 是一些运行在后台的恶意程序，通过登陆某一个频道，分析接受到的内容并做出相应的动作。近几年利用 IRC 协议的僵尸程序大规模出现。

- 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 **9.8** 万个。

其中通过 Web 传播的恶意程序中，约有 **22.6%**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。

.exe .rar .zip 仍然是占很大比例的 Web 威胁文件类型,企业用户建议在网关处控制某些类型的文件下载。



2012 第 1 季度中国地区 web 威胁文件类型

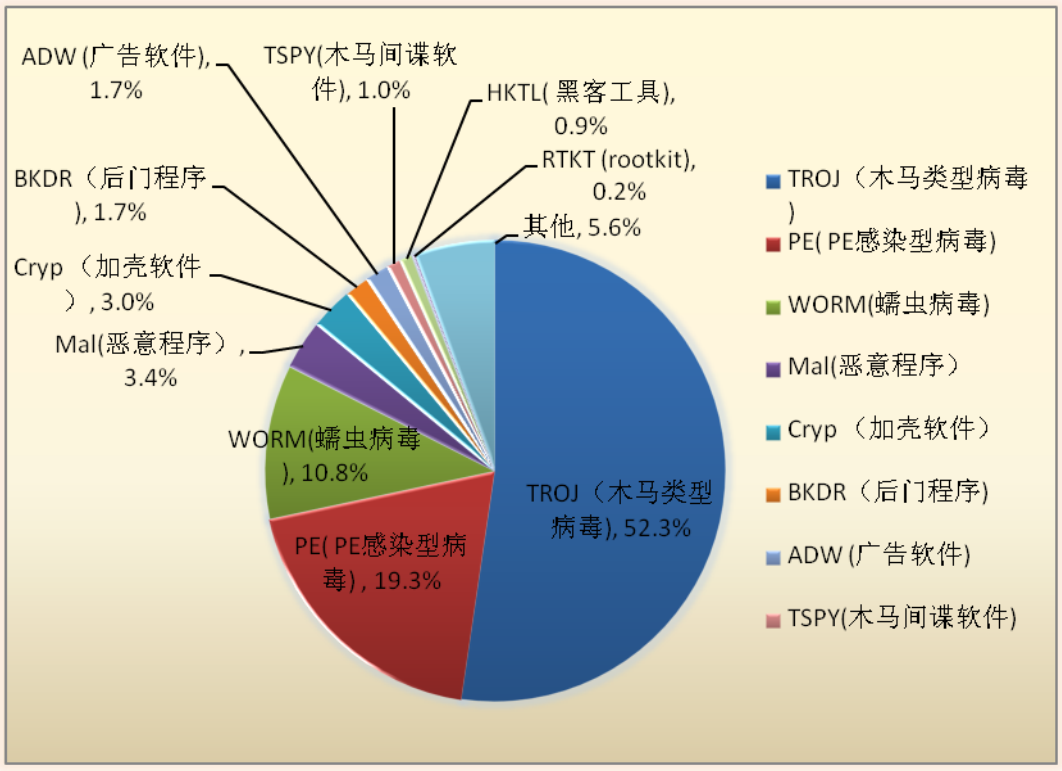
从网页下载带有宏病毒的表格文档，也是感染宏病毒的一个重要途径。感染了宏病毒的电脑使用者在不知情的情况下将带有病毒的文档上传至网站，会导致下载阅读文件的用户感染。

我们甚至发现有一些被感染了宏病毒的文档被上传在政府网站上：

hxxp://whxxp://www.*****.lss.gov.cn:80/html/upfiles/20111231175534908200.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20111231180342452020.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20111231180838017870.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20111231181025892870.xls
hxxp://*****.lss.gov.cn:80/html/upfiles/20111231181025892870.xls
hxxp:/*****.lss.gov.cn:80/html/upfiles/20111231175534908200.xls
hxxp://www.*****ss.gov.cn:80/jgsydwzk/201201/P020120118371831530766.xls
hxxp://www.*****.hrss.gov.cn:80/uploads/siteContentAttachment/1330910588752.xls
hxxp://sti.*****.gov.cn:80/publicfiles/business/htmlfiles/hzsti/cmsmedia/document/doc33109.xls
hxxp://www.*****.hrss.gov.cn:80/uploads/siteContentAttachment/1331084606305.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20120320093219595500.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20120320093121923620.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20111231180342452020.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20111231180838017870.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20111231181025892870.xls
hxxp://*****.lss.gov.cn:80/html/upfiles/20111231181025892870.xls
hxxp:/*****.lss.gov.cn:80/html/upfiles/20111231175534908200.xls
hxxp://www.*****ss.gov.cn:80/jgsydwzk/201201/P020120118371831530766.xls
hxxp://www.*****.hrss.gov.cn:80/uploads/siteContentAttachment/1330910588752.xls
hxxp://sti.*****.gov.cn:80/publicfiles/business/htmlfiles/hzsti/cmsmedia/document/doc33109.xls
hxxp://www.*****.hrss.gov.cn:80/uploads/siteContentAttachment/1331084606305.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20120320093219595500.xls
hxxp://www.*****.lss.gov.cn:80/html/upfiles/20120320093121923620.xls
hxxp://xxgk.*****.gov.cn:80/bmgkxx/fgw/fgwj/qtygwj/201104/P020110407327340735598.xls

提醒使用者：从任何网站上下载并打开 office 文档时，注意先将宏安全等级调高。

- 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 **5960** 万次。



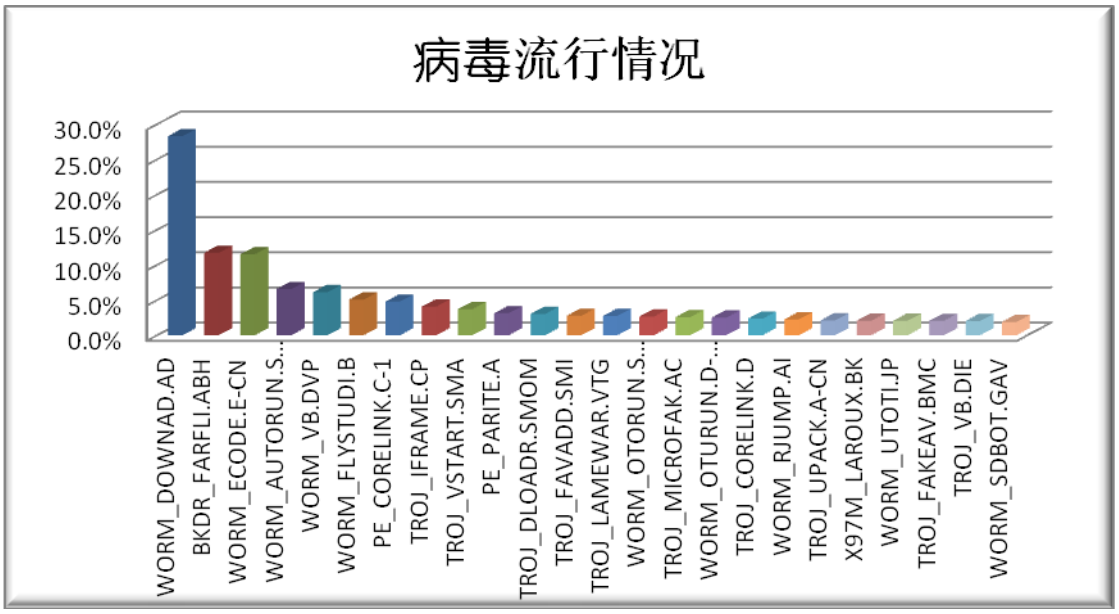
2012 第 1 季度中国地区各类型病毒感染数量比例图

2012 年第 1 季度病毒感染种类中 PE 类型病毒较上季度有很大的上升。PE 病毒为感染型病毒，该类病毒的特征是将恶意代码插入正常的可执行文件中。

蠕虫病毒也仍然占有很大比例。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。

2012 年第 1 季度流行病毒分析



2012 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。
  不过相对于去年该病毒的流行程度已经有了明显下降,2011 第 4 季度时有 40%左右的用户正在或曾经遭受过 Worm_Downad 的攻击，本季度下降到了 27%左右。从数据显示该病毒已逐步得到控制。

  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。

  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。

- 流行程度排名第 2 的 BKDR_FARFLI.ABH， 是一只后门病毒。这只病毒在大约 12%的用户环境中都曾经出现过。

这个病毒一般通过其他恶意文件释放或者是使用者在无意间下载而来。

感染这个病毒的特征：

病毒会在系统中释放以下文件：

%System Root%\Game.exe
%System Root%\Common\Utility.dll
%Program Files%\Jpxv\Hhafqonho.jpg

并且创建以下文件夹：

%System Root%\Common
%Program Files%\Jpxv

添加以下注册表项：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\SvcHost
sougou = Otklkp Pqumryac Jlb
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\281052745
ImagePath = "%System%\svchost.exe -k sougou"
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Enum\Root\LEGACY_OTKLKP_PQUMRYAC_JLB\
0000
Service = "Otklkp Pqumryac Jlb"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\SvcHost
sougou = "Otklkp Pqumryac Jlb"
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Otklkp Pqumryac Jlb
ImagePath = "%System%\svchost.exe -k sougou"
```

并为自己添加以下键值：

```
HKEY_LOCAL_MACHINE\SOFTWARE\281052745
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\323830095
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Enum\Root\LEGACY_OTKLKP_PQUMRYAC_JLB
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Otklkp Pqumryac Jlb
```

感染这只病毒的机器会连接 www.3322.org 网站。

3322.org 是一个动态域名注册网站，很多黑客使用此网站注册域名用以控制远端电脑，感染这只病毒的电脑很可能成为肉鸡。

解决方法：

目前趋势科技最新病毒码可以检测并清除此病毒。
请将病毒更新至最新并进行全盘扫描以删除病毒，没有安装杀毒软件的使用者可以到以下站点下载专杀工具进行查杀：

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

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

- PE_PARITE.A 也是 2012 第 1 季度比较流行的病毒之一，这是一只感染型病毒。

病毒特征行为：

PE_PARITE.A 的母体文件（被趋势科技检测为 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。

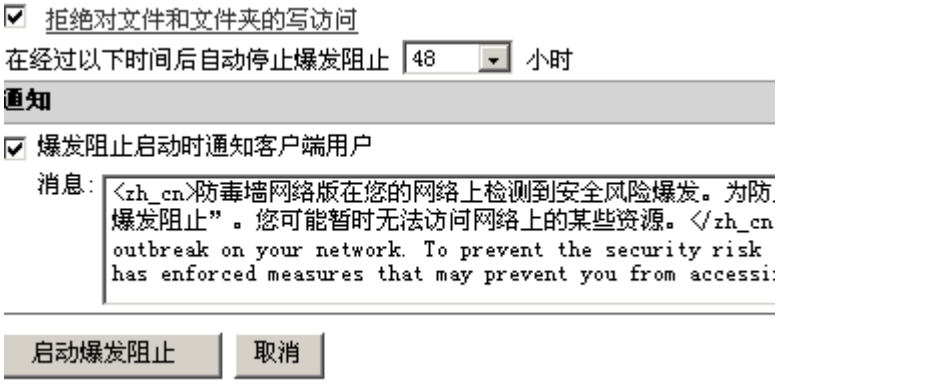
PE_PARITE.A 会向 windows 临时目录中释放随机命名的.tmp 文件，并且调用执行它。它会导出一个名为 INITIATE 的函数，该函数包含恶意行为，一旦被执行，该恶意软件将会创建以下注册表键值：

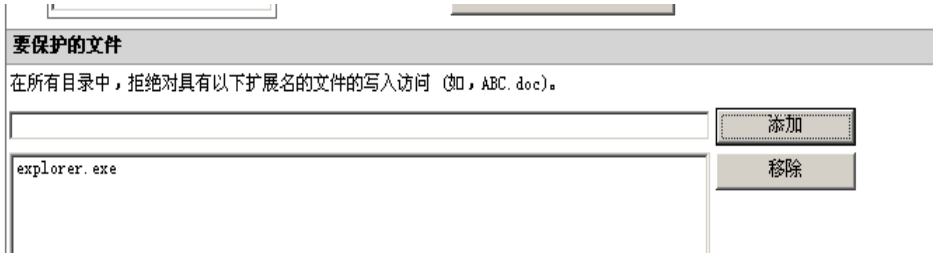
```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Explorer\PINF
```

这个病毒还会创建名为”RESIDENTED”的互斥量，用以确定自己已经在运行了。

传播途径及防护方法：

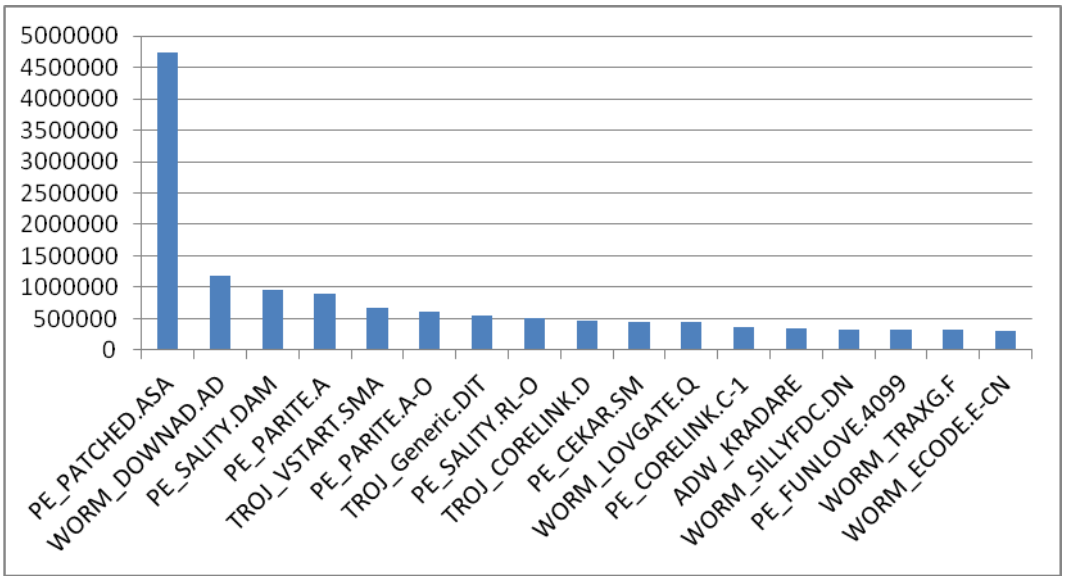
该病毒通过已被感染过的文件以及共享文件夹传播。
由于该病毒能够通过共享文件夹传播并感染，所以防护该病毒的一个重要环节即对共享文件夹进行控制。
介于该病毒首先会感染的是 explorer.exe 这个特性，我们可以在 officescan 服务器上设置爆发阻止策略，阻止对 Explorer.exe 的修改。从而达到防护的目的：





对于已感染的电脑，建议先断开网络然后使用最新的病毒码进行全盘扫描，等待病毒清理干净后再接入网络中。

对于反复感染的客户，请与趋势科技技术支持部门联络，我们将帮您分析感染原因并针对您环境中的情况制作免疫工具。



2012 第 1 季度 中国区拦截次数排名前 20 病毒

本季度我们列出了病毒被拦截次数的排名。被拦截次数多的病毒可能是感染文件数量较多的 PE 病毒，也可能是会反复感染难以清理的病毒。

2012 年第 1 季度被趋势拦截次数最多的为 PE_PATCHED.ASA。该病毒被拦截次数约为 470 万次。远远超过其他病毒。

恶意软件编写者正在尝试通过修改合法的文件这个不同于以往的途径来执行他们的恶意软件。

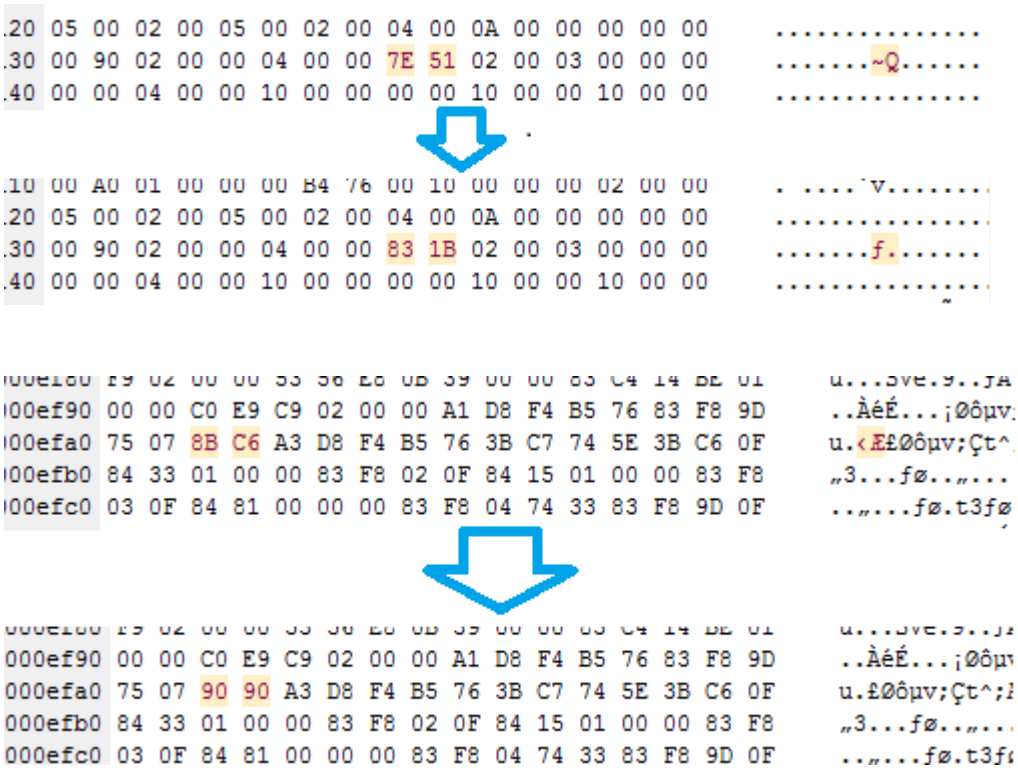
在很多的情况下，他们会将很小的一段代码注入到系统文件中，目的是用来加载其他恶意程序。因为系统文件会在电脑启动时被自动运行，这就使恶意程序达到了自启动的目的。

有时候修改合法的文件的目的也可能是为了躲避安全方面的检查。或者用于恶意文件的更新。

趋势科技将这种被插入了小段恶意代码的合法系统文件检测为 PE_PATCHED。

PE_PATCHED.ASA是趋势科技检测的被修改的sfc_os.dll 文件。这是一个用来保护 windows 系统文件的执行模块。以目前收集到的样本来看被修改的sfc_os.dll文件版本多为5.2.3790.3959 (srv03_sp2_rtm.070216-1710)，该版本的文件并没有数字签名。并且因为仅仅修改了几个字节,大小没有改变所以很不容易被发现。但正因为这小小的修改,使得sfc_os.dll这个文件失去了它保护windows系统文件的作用。

下图为被修改的文件内容：



由于该文件为系统目录下的系统文件，所以杀毒软件如果对它进行处理可能会引起系统崩溃或者其他系统问题。

对这只病毒目前的解决方法有两种：

%__ 将被修改的文件复制到其他目录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。

2012 年第 1 季度最新安全威胁信息

2012 年 1 月，利用 Windows Media 允许远程执行代码漏洞 CVE-2012-0003 的恶意程序被发现

这个漏洞刚刚被披露不久便出现了利用它的恶意文件。
当 windows media player(wmp)中的 windows 多媒体库无法处理一些特制的 midi 文件时,这个漏洞将被触发,从而使远程攻击者能够执行任意代码。
在 1 月 26 日趋势科技就检测到利用了此漏洞的恶意程序，包含了该恶意程序的 html 被检测为 HTML_EXPLT.QYUA 利用这个漏洞的 midi 文件和 js 脚本文件分别被检测为 TROJ_MDIEXP.QYUA 和 JS_EXPLT.QYUA。
微软在 2012 年 1 月 10 日已针对此漏洞发布了安全公告和补丁程序。
以下为相关链接：
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0003
http://blog.trendmicro.com/malware-leveraging-midi-remote-code-execution-vulnerability-found/
http://technet.microsoft.com/zh-cn/security/bulletin/MS12-004

2012 年 2 月，中文版 putty 等 SSH 远程管理工具被曝出存在后门

在 2012 年 1 月就有消息称中文版 putty 等远程控制管理工具存在后门，2 月这个消息得到证实。
该后门会在当用户填写要登陆服务器的用户名密码时将信息发送到特定的网站
以下为对中文版 putty 的分析：

```
.text:0041C803          cmp     esi, edi
.text:0041C805          jz      loc_41DBD3
.text:0041C80B          mov     ecx, ds:off_46B9CC
.text:0041C811          mov     edx, [ebp+44h]
.text:0041C814          push    ecx
.text:0041C815          mov     ecx, [ebx+0C4h]
.text:0041C81B          push    edx
.text:0041C81C          mov     edx, [ebx+0C0h]
.text:0041C822          lea     edi, [eax+1]
.text:0041C825          mov     eax, [ebx+1FCh]
.text:0041C82B          push    eax
.text:0041C82C          push    ecx
.text:0041C82D          push    edx
.text:0041C82E          call    net_send
.text:0041C833          jmp     loc_41CB89
```

比英文版多出的数据逻辑

这个函数对用户名密码进行处理，发送到作者空间。

2012 年 3 月，趋势科技中国区病毒实验室发现一批欺诈网站

趋势科技发现了一批诈骗网站，它们伪装成网上商城销售各类产品，以相对低价欺骗买家注册并购买“商品”，之后利用支付宝即时到帐方式的特点欺骗买家支付账单并造成经济损失。

以下列出了已找到的类似欺骗网站：

- 5ascc.com
- baibao126.com
- coolshop8.com
- dxll365.com
- fengyongo.com
- gougoubuy.com
- gu365.net
- hlgogo.com
- huangjiasp.com
- huigou8888.com
- jbc365.com
- kaixingouwu365.com
- legoush.com
- linggowu.com
- lly168.com
- longcheng888.net
- miaoshagowu.com
- mmlg365.com
- qcygshop.com
- quanqiugo.net
- ssm888.com
- truebao.com
- ttyongle.com
- xinxingsc.com
- yos58.com
- zhenxin8888.com

2012 年 3 月，趋势科技中国区病毒实验室监控到一起针对金融行业的 APT

3 月中国区网络安全监测实验室(China RTL)监控到一起针对金融行业的 APT（Advanced Persistent Threat），此威胁会导致用户重要信息数据泄露。该病毒具有潜伏性，病毒文件可能已在用户环境中存在一年或更久的时间，并且仍在陆续出现新变种，趋势科技提醒您关注该病毒。

病毒名称：[TROJ_JNCTN-CN]

其它相关的检测名：TROJ_JNCTN.A-CN, TROJ_JNCTN.B-CN, TROJ_JNCTN.C-CN,

TROJ_JNCTN.D-CN, TROJ_JNCTN.E-CN

恶意行为：

- ✧ 搜索系统中的 * .doc，*.xlsx,*.ppt ,*.xls,*.rtf,*.csv 类型文件并将它们上传至远端服务器
- ✧ 截取用户桌面的 msn 聊天窗口，并提取其聊天对象的历史记录上传至远端服务器
- ✧ 获取系统的账号密码
- ✧ 在正常的 jpg 图片中插入加密代码进行更新。
- ✧ 注入系统服务及进程
- ✧ 获得被感染终端的地理位置
- ✧ 通过 1418 端口接受远程指令，并可以通过被感染的计算机控制其他被感染计算机

2012 年 3 月，趋势科技中国区病毒实验室发现一种新型 Excel 宏病毒

3 月,趋势科技中国病毒实验室 （China RTL）发现了一个新的 Excel 宏病毒，该宏病毒除了能够通过感染 Excel 文件传播外，还会主动通过 Outlook，将打开的被感染文件通过附件形式发送给其他收件人。此行为除了会使该宏病毒传播更广泛外，还可能会导致 Excel 文件的内容泄漏。

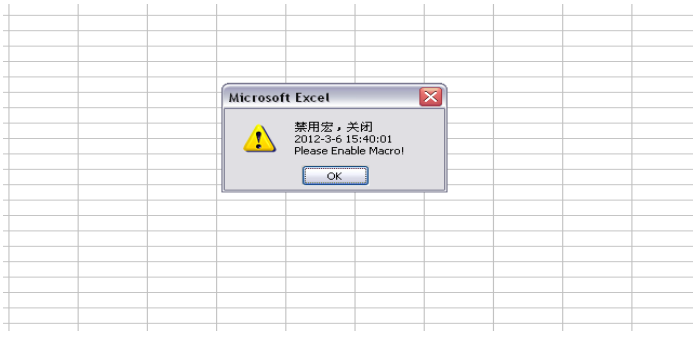
趋势科技率先对其进行正确检测，并对感染的文件进行清除。目前趋势科技将其检测为 X97M_OLEMAL.A。

另外，趋势科技制作了针对此病毒的专杀工具：

http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/Marco/TMCleanMacro(密码 novirus).zip

病毒行为如下：

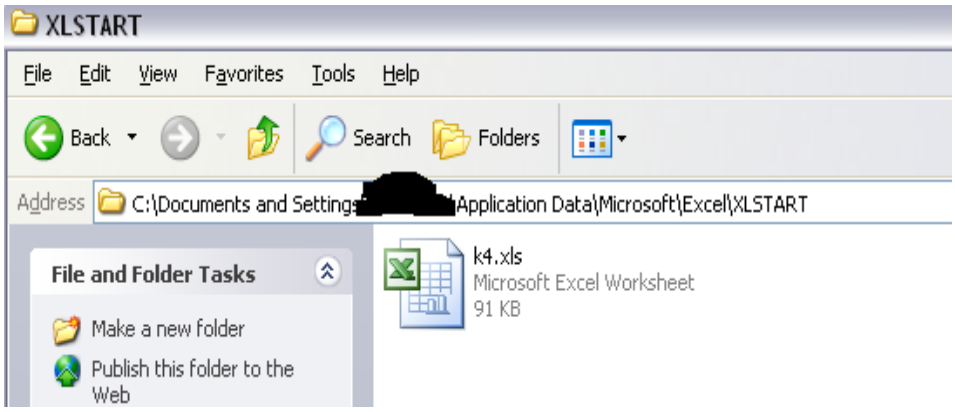
1.如果禁用宏，感染的文件打开的时候会弹出如下的对话框。或者打开失败。



2.感染的文件，会在 ThisWorkbook 下添加如下脚本。

```
x                                          workbookOpen
Public WithEvents xx As Application
Private Sub Workbook_open()
Set xx = Application
On Error Resume Next
Application.DisplayAlerts = False
Call do_what
End Sub
Private Sub xx_workbookOpen(ByVal wb As Workbook)
On Error Resume Next
wb.VBProject.References.AddFromGuid _
GUID:="{0002E157-0000-0000-C000-000000000046}", _
Major:=5, Minor:=3
Application.ScreenUpdating = False
Application.DisplayAlerts = False
copystart wb
Application.ScreenUpdating = True
End Sub
```

3. 在 Excel 的启动目录释放 k4.xls 文件，用于感染其他 Excel 文件。



4. 在 Excel 文件中添加模块，模块中包含恶意代码。

2012 年 3 月，MAC OS 现在也很容易遭到攻击

2012 年 3 月趋势科技发现数起针对于 Mac OS 的攻击，虽然 Mac 系统的病毒数量并没有 windows 那么高，但是这不代表我们可以对 Mac OS 的恶意程序掉以轻心。和 windows 系统的病毒一样，Mac OS 的恶意程序也可以对被感染系统进行严重的破坏。

以下为相关链接：

http://blog.trendmicro.com/a-look-into-the-most-notorious-mac-threats/

http://blog.trendmicro.com/game-change-mac-users-now-also-susceptible-to-targeted-attacks/

http://blog.trendmicro.com/news-of-malicious-email-campaign-used-as-social-engineering-bait/

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)