中国地区 2013 年

第一季度

网络安全威胁报告

2013/5

CHINA RTL

目录

2013 年第 1 季度安全威胁

本季安全警示：

PE 病毒，网络攻击，钓鱼网站

2013 年第 1 季度安全威胁概况

- 本季度趋势科技中国区病毒码新增特征约 **61** 万条。截止 2013.3.31 日中国区传统病毒码 **9.826.60** 包含病毒特征数约 **440** 万条。
- 本季度趋势科技在中国地区客户终端检测并拦截恶意程序约 **6560** 万次。
- 本季度趋势科技在中国地区拦截的恶意 URL 地址约 **1 亿 1 千**万次。

2013 年第 1 季度中国地区，并没有出现大规模的病毒爆发事件。但网络攻击事件仍时有发生，网络安全防护不容忽视。

第 1 季度，木马病毒仍然占据新增病毒数量排名首位。大部分木马有盗号或是窃取系统重要信息的特性。 与其他类型的电脑病毒相比木马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。另外，黑客工具类型恶意程序的新增数量增加，也表现为第一季度使用黑客工具进行攻击的事件增加，另外更加有效的新的黑客工具也不断地出现。

在第 1 季度的病毒检测数量排名与上季度大致相同，并没有新的危害较大的病毒出现。PE 病毒仍然排名第 1 位。该类型的病毒问题，往往较难处理和彻底的解决。预计这种状况仍然会持续一段时间。

本季度 PE 病毒感染情况仍然严重：

PE_PATCHED.ASA 已连续 3 个季度排名病毒检测数量首位，该病毒为被修改的 sfc_os.dll，sfc_os.dll 是用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能，该文件被修改预示着有其他会修改系统文件的恶意行为可能将会发生。

PE_SALITY.ER，**PE_PARITE.A** 在本季度仍在流行中，PE_SALITY.RL 除了常规的 PE 病毒感染方式还会通过微软的快捷方式漏洞传播(**MS10-046**),快捷方式漏洞也可能通过邮件到达被感染客户端。 PE_PARITE.A 除了通过感染文件，网络共享，还能够通过电子邮件传播。

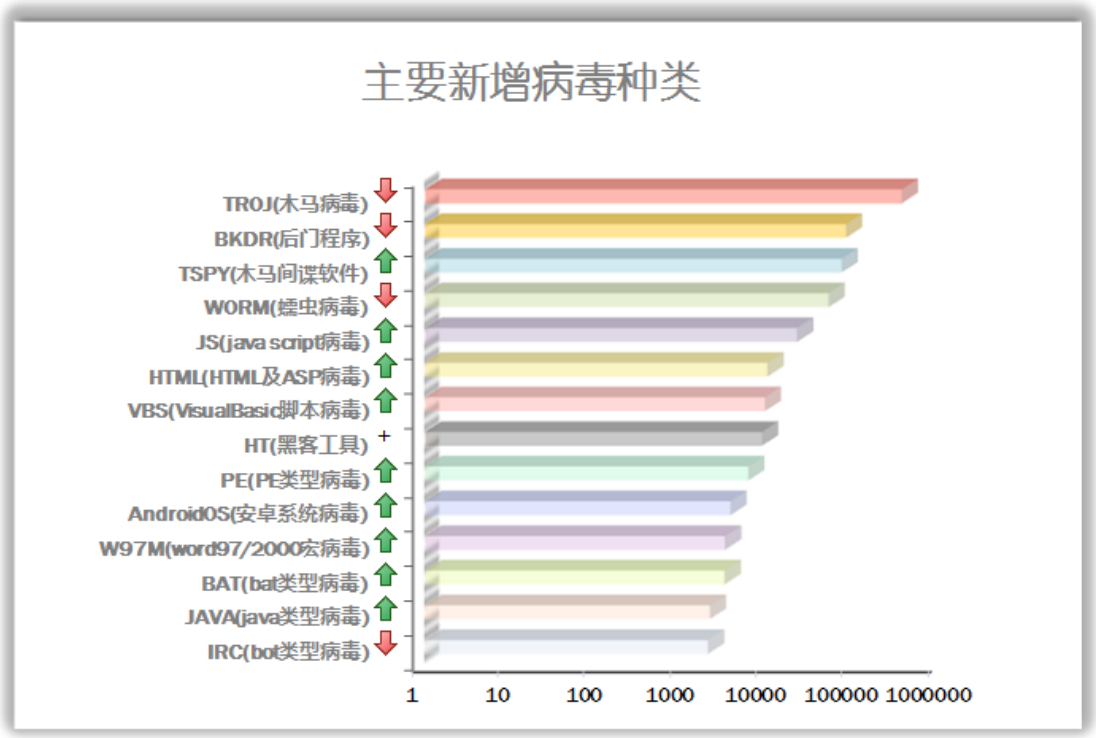
PE 病毒，是一种破坏性较大的恶意程序。对感染的用户系统可能造成很大的影响。某些 PE 类型病毒甚至会将原文件替换导致无法修复。对于 PE 病毒我们认为加强防范才是最好的解决方案。

本季度，宏病毒的感染形势依然严峻。很多网站提供的下载的 office 文档都带有宏病毒 ，再次提醒用户在打开网站下载，或者邮件附件中的 office 文档时请务必先使用安全软件进行扫描。

在 2013 年第 1 季度趋势科技拦截新的恶意网站中钓鱼网站约有 3000 个(以域名计数)。各种钓鱼网站仿冒目标中，金融证券以及网上在线支付仍然是钓鱼网页制造者主要的仿冒对象，另外一些电视台和热门节目也成为了钓鱼仿冒对象。

2013 年第 1 季度病毒威胁情况

2013 年第 1 季度新增病毒类型分析



2013 第 1 季度中国地区新增病毒类型

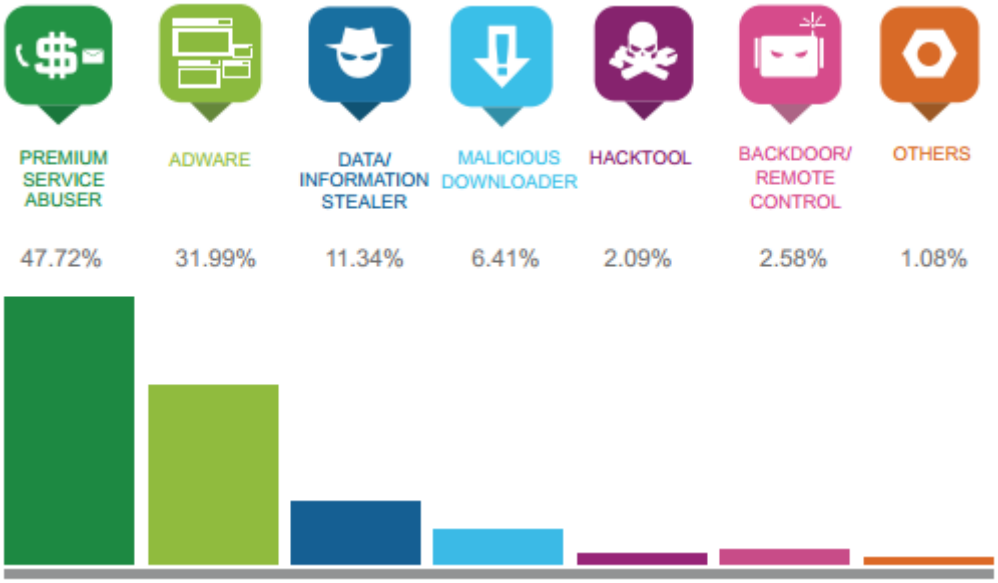
新增的病毒类型最多的仍然为木马(TROJ),本季度新增木马病毒特征336027个,大约占新增病毒数量的56% ,比上季度略有下降。木马可使病毒制造者更直接的获利，在经济利益的驱使下大量的木马被制造并通过各方式被传入互联网中。木马也是我国目前存在数量最多的病毒类型。

本季度新增的病毒类型中新增病毒类型中比上季度多了 HT 类型，趋势科技定义以 HT_开头的检测类型为黑客工具。2013 年开始，黑客活动异常频繁。第一季度中国境内外就爆出了多起严重的黑客攻击事件。在强大的黑客工具帮助下，越来越多的网站被脱库，服务器被攻击的事件也变得越来越频繁。

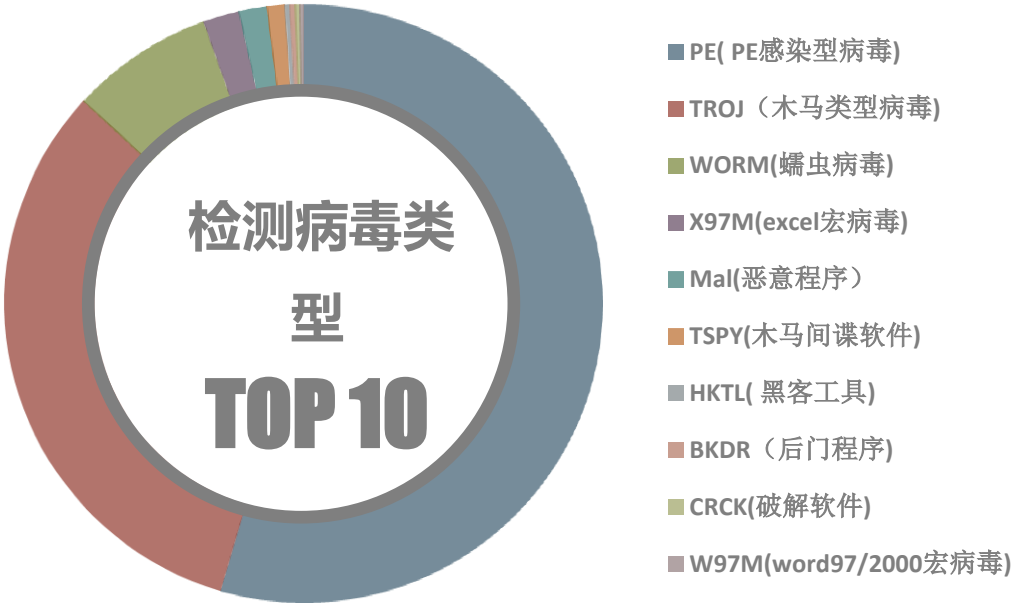
JS (java script 病毒), HTML(HTML 及 ASP 病毒)常常和网页挂马相关。恶意代码的制造者将代码植入网站中，这些脚本内容往往不容易被网站管理者以及浏览网页的用户发觉，正常的网站服务器成了扩散病毒，恶意代码的平台。另外，通过向网页插入恶意代码，网络罪犯可以进一步获得网站的 webshell ，甚至使他们能够控制网站服务器的机器。这样一来，网站用户的数据可能会被盗窃，服务器也可能成为这些恶意行为者的肉鸡，被用来进行网络攻击或其他一些非法的网络行为。

新的 AndroidOS(安卓系统病毒)数量，在 2013 年第一季度持续上升。

其中数量最多的为吸费软件占到所有新增病毒的 47.72%，广告软件排名第二占 31.99%，排名第三的是信息窃取软件占 11.34%。



2013 年第 1 季度各类型病毒检测情况分析



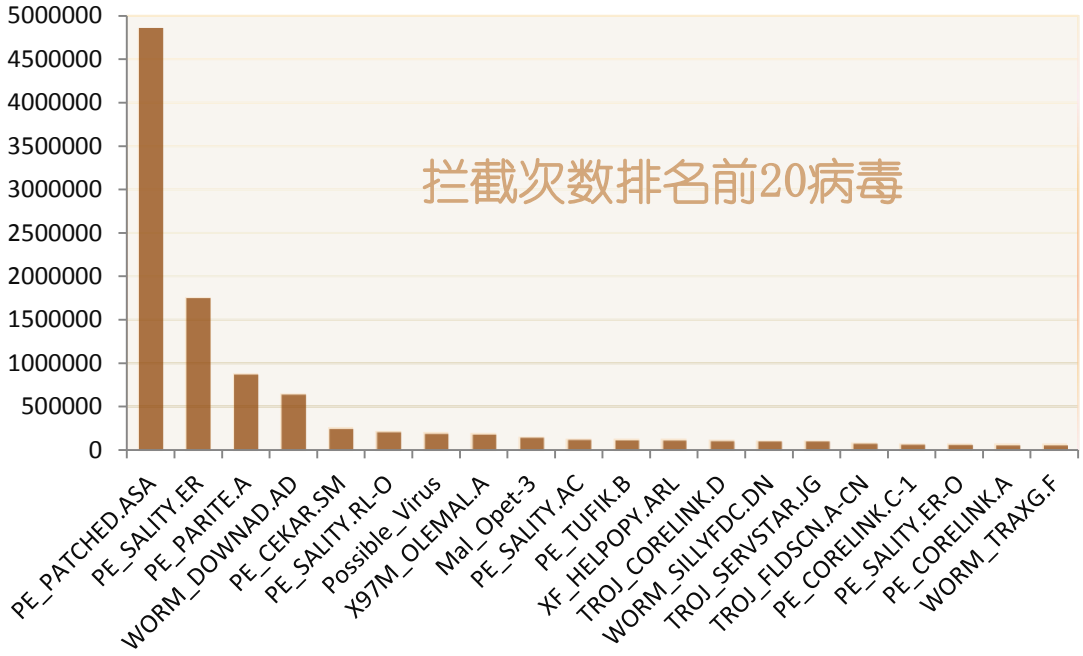
2013 第 1 季度中国地区各类型病毒检测数量比例图

2013 年第 1 季度检测到的病毒种类中 PE 类型病毒感染数量仍然居高不下。大约占到总检测数量的 53%。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。导致上季度 PE 病毒检测数量骤增的是 PE_PATCHED.ASA。该病毒为被修改的 sfc_os.dll，sfc_os.dll 是用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能。由于该文件是系统文件，防毒软件强行查杀可能会导致系统崩溃。此外 PE 病毒通常会感染系统中所有的可执行文件。一旦被感染，系统中多数文件都会被检测。

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。第 1 季度感染比较多的蠕虫病毒仍然为 WORM_DOWNAD 以及文件夹病毒。另外某些 PE 病毒的母体也以蠕虫病毒的方式传播

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。

2013 年第 1 季度病毒拦截情况分析



2013 第 1 季度中国区拦截次数排名前 20 病毒

上图显示了 2013 年第 1 季度被拦截次数排名前 20 的病毒。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。

2013 年第 1 季度被趋势科技拦截次数最多仍然的为 PE_PATCHED.ASA。该病毒被拦截次数约为 480 万次。远远超过其他病毒。

该病毒为被修改的 sfc_os.dll，sfc_os.dll 是用来保护系统文件的执行模块，该文件被修改后系统将失去文件保护的功能

由于该文件是系统文件，防毒软件强行查杀可能会导致系统崩溃。

对这只病毒目前的解决方法如下*（可以使用以下三种方法种的任意一种进行清理）*：

- 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。
- China RTL 已针对此病毒制作专杀，需要的用户可以到以下地址下载反病毒工具包进行处理：
  http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/Release.zip

本季度 **PE_SALITY** 病毒仍然排在病毒检测数量前三位中，这种 PE 感染型病毒利用了微软的快捷方式漏洞传播。

相关安全公告连接：

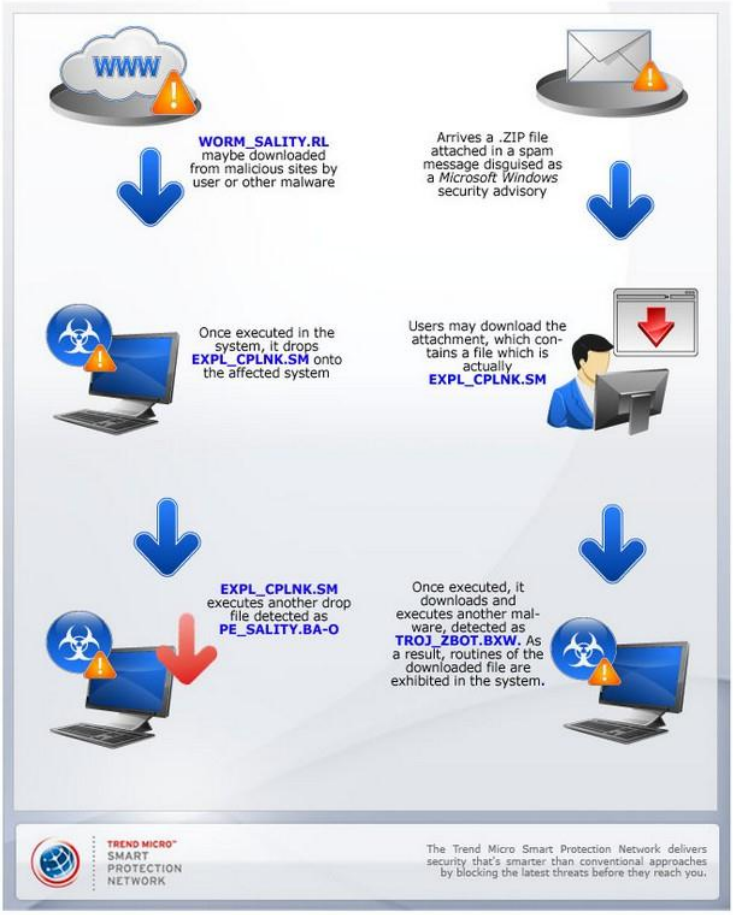
(MS10-046) Microsoft Windows Shortcut Remote Code Execution Vulnerability

http://about-threats.trendmicro.com/vulnerability.aspx?language=us&name=Microsoft%20Windows%20Shortcut%20Remote%20Code%20Execution%20Vulnerability

http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx

它可能是通过邮件到达被感染用户的电脑。 邮件附件中包含有带有漏洞的快捷方式文件，和一个.dll 文件。这个 dll 会导致下载相关的 PE 感染类型病毒文件，PE_SALITY.XX-O 如 PE_SALITY.ER-O。

一旦该 PE 病毒母体文件运行，他将会感染系统和所有可以访问到的共享设备中的.EXE 以及.SCR 文件，并释放 AUTORUN.INF 起到自启动的目的。被感染后的.EXE 或者.SCR 文件也会感染其它可执行文件，并且被趋势科技检测为 PE_SALITY.XX 如 PE_SALITY.ER。



PE_SALITY 感染过程

PE_SALITY.ER

感染途径：

通过母体文件，或是被母体文件 PE_SALITY.ER-O 感染过的文件感染。
运行后会将恶意代码注入 EXPLORER.EXE 进程。

恶意行为：

- 此病毒会修改被感染电脑的注册表选项来禁用一些系统服务。这种行为会导致很多系统的功能无法使用。
- 该感染文件会重写程序入口点的代码并将他指向病毒代码，这样就把病毒程序附加到了宿主中。当被感染程序运行时就会先执行恶意代码。
- 它会释放 AUTORUN.INF 以使他释放到各个目录中的病毒文件能够自动运行起来。

技术细节 ：

文件大小: 不固定
文件类型: PE
常驻内存: 是
第一个样本获得时间: 11.2, 2010
恶意行为: 禁用服务，中止进程，下载恶意程序

修改系统内容：

会在系统的 SYSTEM.INI 文件中添加以下内容

[MCIDRV_VER]
DEVICEMB={随机数字 }

安装后会添加以下注册表键值：
`HKEY_CURRENT_USER\Software\Afukx`

修改以下注册表键值，来禁用服务：
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\`
`Services\SharedAccess`
`Start = 4`

Start 的默认值为 2
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\`
`Services\wscsvc`
`Start = 4`

Start 的默认值为 2

修改以下文件隐藏属性的相关键值

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\AuthorizedApplications\
List
{malware path and file name} = {malware path and file name}:*:Enabled:ipsec
```

Hidden 的默认值为 1

创建以下注册表键值来通过防火墙：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\AuthorizedApplications\
List
%WINDOWS%\Explorer.EXE = %WINDOWS%\Explorer.EXE:*:Enabled:ipsec
```

删除以下注册表键值：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\
Control\SafeBoot\Minimal

HKEY_LOCAL_MACHINE\System\CurrentControlSet\
Control\SafeBoot\Network
```

文件感染：

感染所有 EXE，SCR 类型文件

该病毒会自动忽略文件命中包含 DAEMON,NOTEPAD.EXE,WINMINE.EXE 的文件 ，自动忽略文件名超过 250 字符的文件，自动忽略包含有 SYSTEM 的文件

删除后缀为.VDB ,.KET ,.AVC 的文件

删除文件名以‘drw’开头的文件

删除文件名中和安全相关的应用程序

传播方式：

这个感染型文件释放以下自身的复制到所有物理及可移动存储设备中

驱动:\{随机名称}.exe/cmd/pif

他会释放一个 AUTORUN.INF 文件来使他释放的这个复制在感染的系统中 自动运行

AUTORUN.INF 包含以下内容

```
;{garbage characters}
[AutoRun]
;{garbage characters}
shell\explore\command = {random}.exe/cmd/pif
;{garbage characters}
open = {random file name}.exe
;{garbage characters}
shell\open\command = {random}.exe/cmd/pif
shell\open\default = 1
;{garbage characters}
shell\autoplay\command = {random}.exe/cmd/pif
;{garbage characters}
```

会从以下站点下载恶意程序：

http://{BLOCKED}mediaproduction.com/images/xs.jpg
http://{BLOCKED}e.co.uk/images/xs.jpg
http://{BLOCKED}rnajd.com/images/logo.gif
http://{BLOCKED}l.net/images/xs.jpg
http://{BLOCKED}oletarianparty.org/logof.gif
http://{BLOCKED}scapeuk.com/xs.jpg
http://{BLOCKED}so.com.br/s.jpg
http://{BLOCKED}rtltd.com/img/xs.jpg
http://{BLOCKED}monline.com/s.jpg
http://{BLOCKED}wing-tomorrow.org/images/s.jpg
http://{BLOCKED}.{BLOCKED}.222.206/logos.gif
http://{BLOCKED}icoverseas.net/images/xs2.jpg
http://{BLOCKED}o.cz/logo.gif
http://{BLOCKED}nhotel.com/images/logof.gif

他会将下载文件存放在当前用户的 TEMP 文件夹中

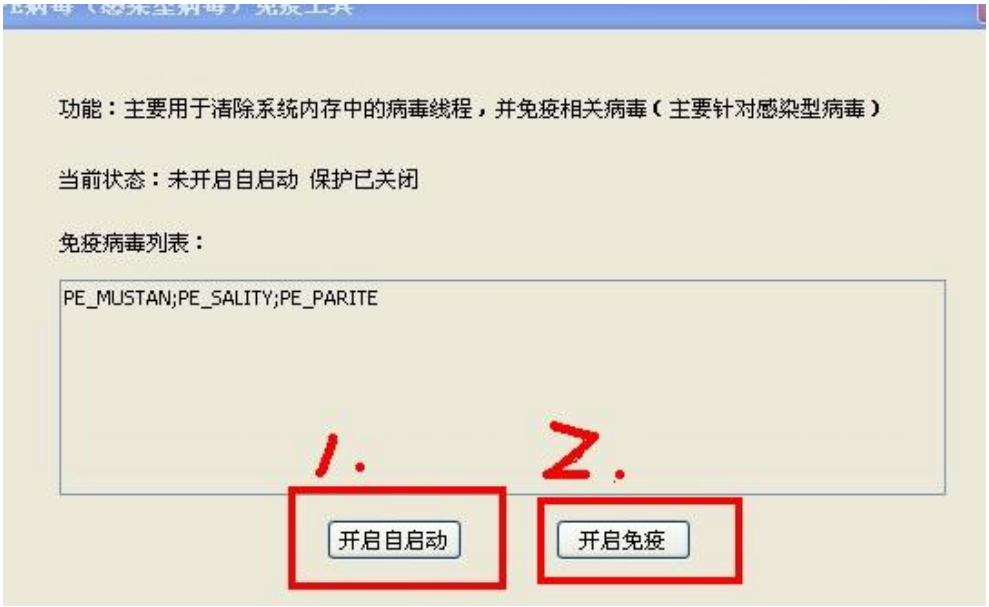
解决方法：

1. 到以下站点下载 AVB 工具

http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/Release.zip
解压缩密码: novirus

选择－增强工具 PE 病毒免疫

在随后的窗口先选择 开启自启动 在选择开启免疫



免疫成功后的表现：

a. 注册表可以打开

b. 任务管理器不再为灰色可以正常显示

由于此工具仅仅起到清除线程中病毒以及免疫作用。所以 免疫成功后仍然需要用 ATTK 进行全盘扫描.

2. 升级防毒产品到最新病毒码并进行全盘扫描

3. 没有安装防毒产品或者是防毒产品已经被破坏的用户请到以下站点下载 ATTK 进行扫描：

32 位 windows 操作系统请使用：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage.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
（为了避免.exe 文件在下载到系统时被感染，请在下载时将该工具保存为.com）

防护方法：

1. 及时更新微软补丁，特别是
http://www.microsoft.com/technet/security/bulletin/MS10-046.mspx

2. 如果没有必须需要使用 AUTORUN.INF 可以禁用 AUTORUN.INF 的功能

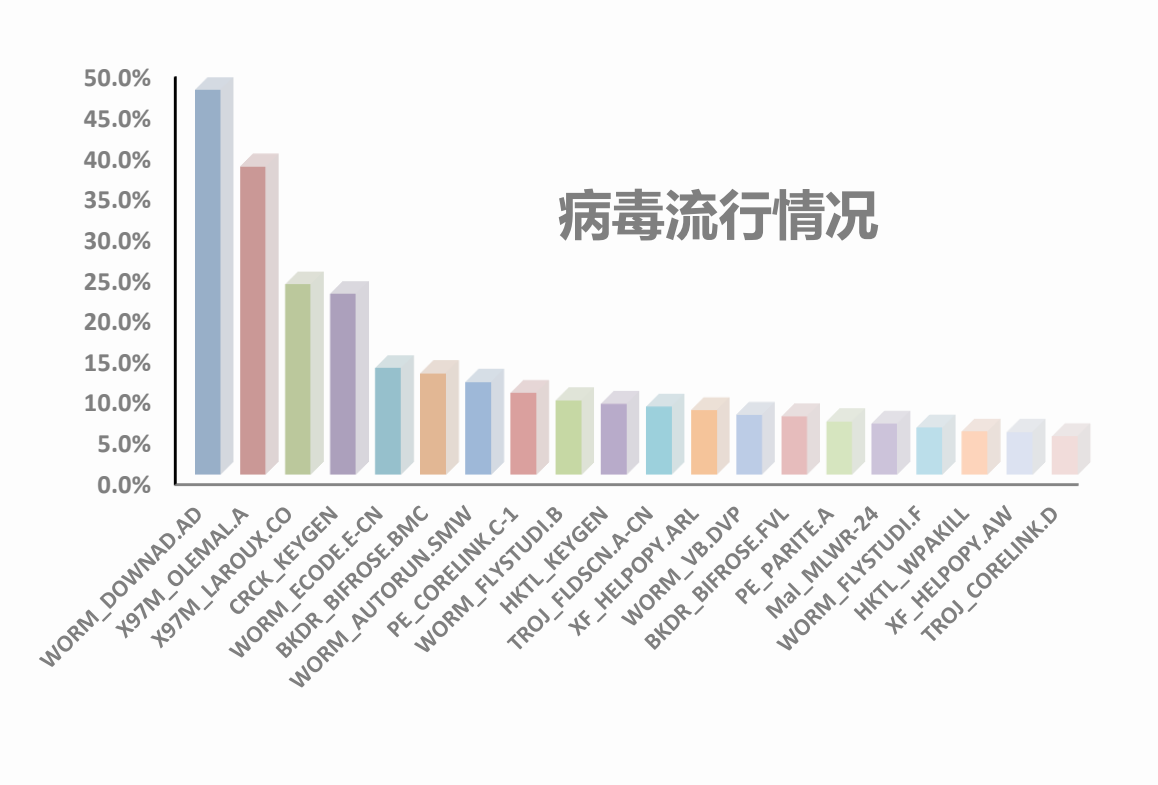
```
[HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Policies/Explore]
"NoDriveTypeAutoRun"=dword:000000dd
"CDRAutoRun"=dword:00000000
"NoSMMyDocs"=dword:00000001
"NoSMHelp"=dword:00000001
"NoRecentDocsMenu"=dword:00000001
"NoRecentDocsNetHood"=dword:00000001
```

3. 由于该病毒会破坏防毒软件，请将防毒软件的补丁版本更新至最新

4. 及时更新病毒码并定期执行扫描

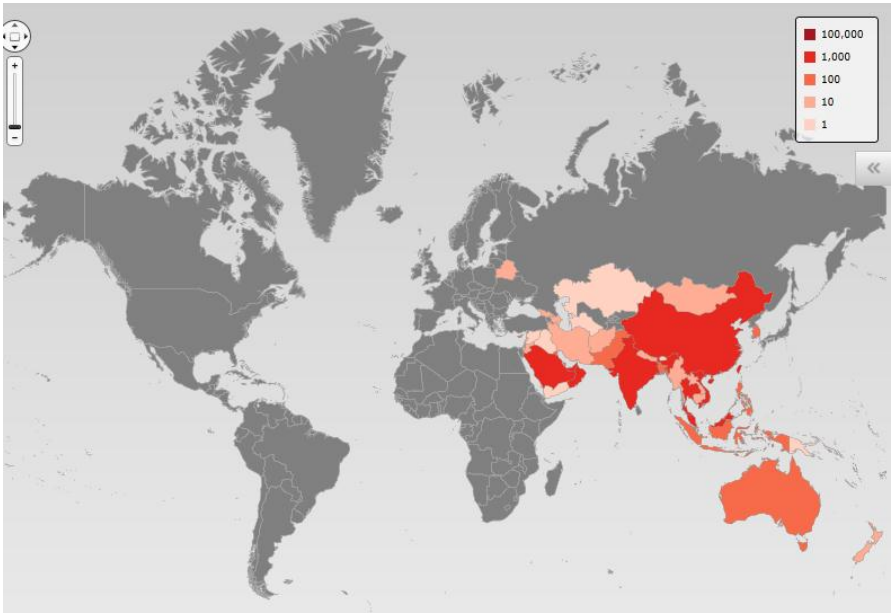
5. 也可以在未感染该病毒之前事先运行免疫工具

2013 年第 1 季度流行病毒分析



2013 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**。



Worm_downad 全球分布图

与上个季度相比 2013 年第 1 季度感染 WORM_DOWNAD 的用户数量有上升趋势。虽然目前的防病毒产品都能够检测并处理这些病毒，但是网络内一直有这种病毒存在，说明环境存在某些安全缺陷，使得病毒能够进入并且持续存活，针对这种情况需要及时处理和分析。

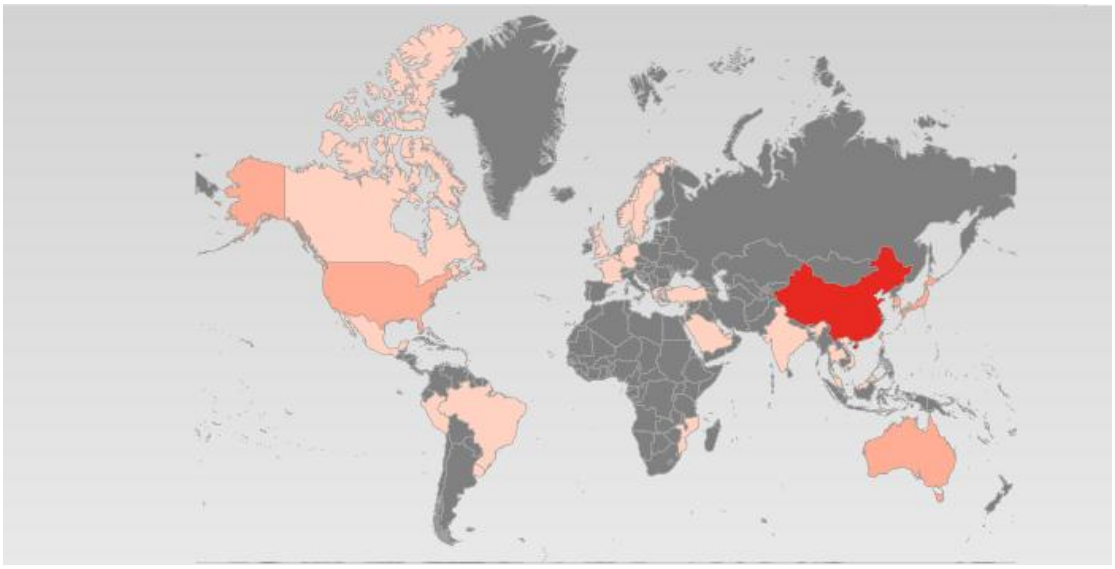
在这里仍然需要提醒用户，WORM_DOWNAD 持续流行的原因有几点：

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。

X97M_OLEMAL.A 在本季度流行程度比上季度又有所上升。这种宏病毒不仅仅能感染 EXCEL 文件，并且还会将感染系统中的 EXCEL 文件自动通过 OUTLOOK 发送

这种 excel 宏病毒是 2012 年 6 月，趋势科技中国区病毒实验室在中国第一次检测到，目前已经在世界各地都有机器感染



全球 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：

- 从网站下载而来
- 使用文件传输工具获得
- 通过邮件传送

病毒防护方法：

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：

目前趋势科技最新中国区病毒码 9.244.60 及以上版本病毒码以可检测此文件，感染此病毒机器请对系统进行全盘扫描

未安装趋势科技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 可以查杀此病毒：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/Release.zip
（解压缩密码：novirus）
使用前请看 readme:
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/readme.txt

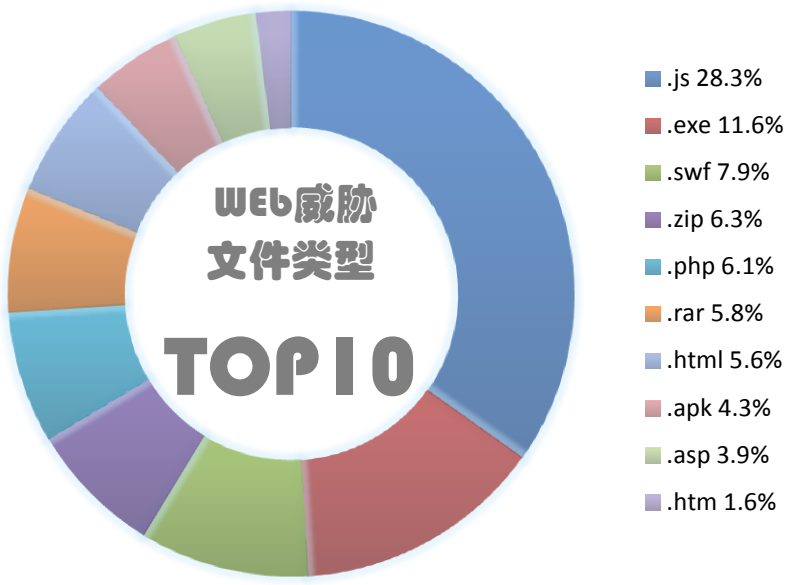
该病毒的详细信息请参考以下链接：
http://about-threats.trendmicro.com/us/malware/x97m_olemal.a

2013 年第 1 季度 web 安全威胁情况

2013 年第 1 季度 Web 威胁文件类型分析

其中通过 Web 传播的恶意程序中，约有 **28.3%**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来行其他恶意行为。

.exe 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。



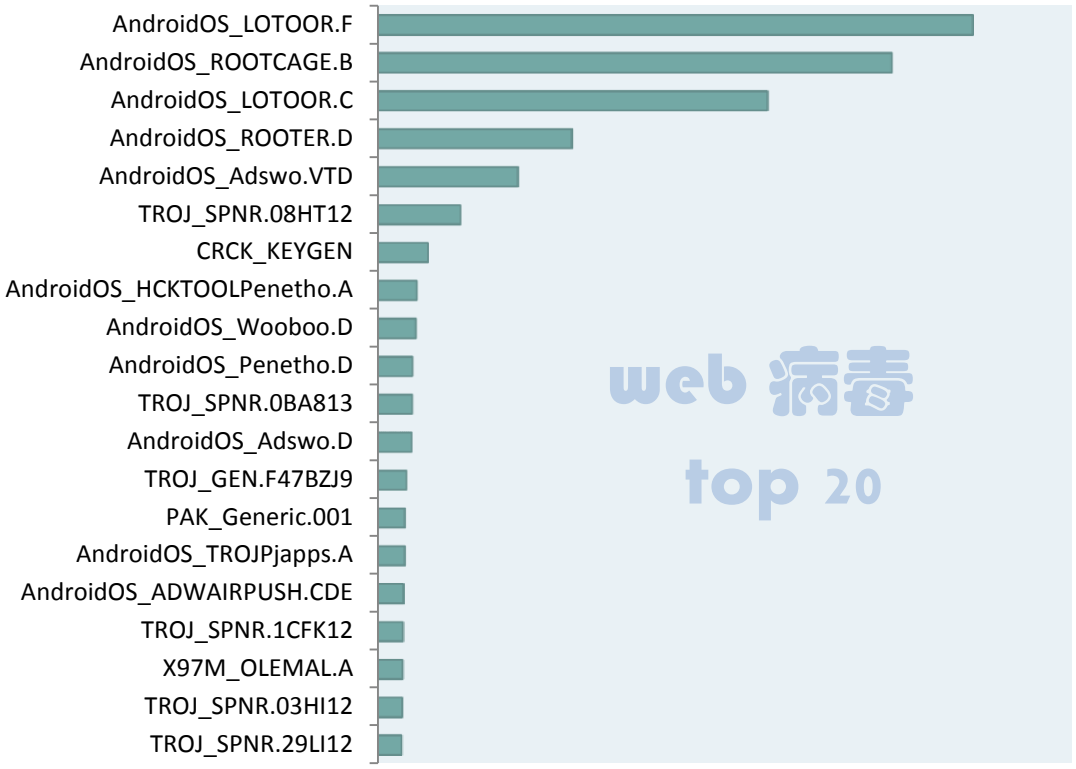
2013 第 1 季度中国地区 web 威胁文件类型

2013 年第 1 季度 top10 恶意 URL

TOP 10 恶意URL		
恶意URL	**描述**	**点击量**
hxxp://my.*****.****.com/fav/browser/do.php	网站直接或间接帮助传播恶意软件或恶意代码	10311920
hxxp://my.*****.****.com/fav/browser/link.php	网站直接或间接帮助传播恶意软件或恶意代码	2739293
hxxp://123.***.203.***:80/	网站直接或间接帮助传播恶意软件或恶意代码	1685331
hxxp://*****.stalker.***.com	网站直接或间接帮助传播恶意软件或恶意代码	1591658
hxxp://211.**.70.***/wpad.dat	模仿合法网站收集敏感信息的诈骗站点，例如收集用户名和密码	1520100
hxxp://disp.*****.com/dm.php?uid=16&tid=1&ref=1	站点被恶意程序利用，包括用于承载恶意软件升级以及存储被窃取的资料	1469670
hxxp://router.******.com	网站直接或间接帮助传播恶意软件或恶意代码	1196201
hxxp://211.**.70.***/wpad.dat	模仿合法网站收集敏感信息的诈骗站点，例如收集用户名和密码	506051
hxxp://update.**.****.com/index.php	网站直接或间接帮助传播恶意软件或恶意代码	492935

2013 第 1 季度中国地区已被 wrs 阻止的恶意 url 排名

2013 年第 1 季度 Web 威胁病毒类型分析

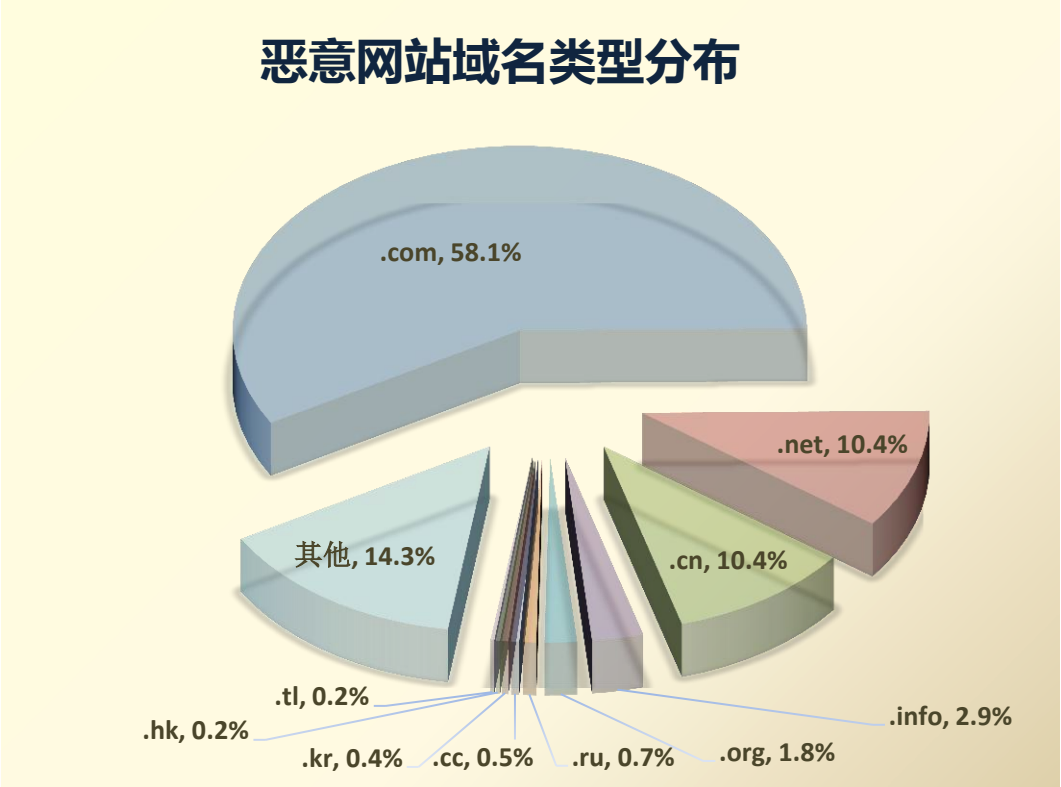


通过对拦截的 Web 威胁进行分析，我们发现。2013 年第 1 季度安卓平台的恶意软件检测数量大幅度提升。检测数量排名前五的病毒均为安卓平台病毒。 使用者需要尽量安装手机安全产品，尽量从可信的安卓市场中下载安装程序。程序安装过程中仔细观察安装画面，发现有不正常的权限请求时及时中止安装过程。

破解软件常常携带有木马被用户下载，在用户安装破解软件时往往在不知不觉中同时将木马安装到电脑上。并且不容易被发现。

另外一些带有宏病毒的 office 文档被挂在 internet 供公众下载，这些是宏病毒传播的一个主要途径。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。

2013 年第 1 季度 web 威胁域名分布



第一季度，恶意软件域名在各顶级域的分布情况如上图，其中使用.com，.net，.cn 的域名的站点占了 78.9%。其中.com 域名下的恶意页数量最多。

2013 年第 1 季度 Web 威胁网页挂马对象分析

网页挂马，指的是攻击者利用网页漏洞或使用其他一些手段将恶意代码或链接植入正常网站的页面代码中。当访问者浏览被挂马网页时，这些脚本或恶意代码可能会在不知情的情况下被执行，从而导致电脑被感染。还有一些被植入页面的恶意代码，可以使攻击者达到控制网站服务器的目的。类似于网站的后门，为他们进行进一步的犯罪行为提供途径。

从监控数据来看，2013 年第一季度被挂马的网站类型前三名为: 软件/下载类，视频/娱乐类，门户/论坛类。

这些被挂马的网站服务器很多是被托管在机房，缺乏安全管理规范，以及安全检查的流程。同一网段内一台 web 服务器如果出现安全漏洞，即可作为旁站，成为网络罪犯入侵其它同一网段内 web 服务器的跳板。另外这些网站的访问量比较大，在这些网站上挂马，可以使得更多的机器感染成为“肉鸡”,构建僵尸网络，以谋取利益。

除了上述的三种类型的网站以外，我们发现政府/机构网站，学校/教育网站，以及一些中小企业网站也是黑客热衷于攻击的篡改的对象。

政府/机构　　学校/教育　　公司/企业

很多地区的政府/机构网站，缺乏专门的技术人员维护，网页代码存在漏洞或者缺陷，很容易遭到黑客的入侵，并进行挂马。并且一旦这类网站受到攻击可能就会造成一定的舆论影响力。

学校/教育类的网站普遍存在安全意识较差的问题，黑客攻击这类网站成功率也会比较高 。另外一些热衷于网络入侵的学生也可能是导致学校网站被挂马的原因。

ZONE-H.COM.CN 中国被黑站点统计系统

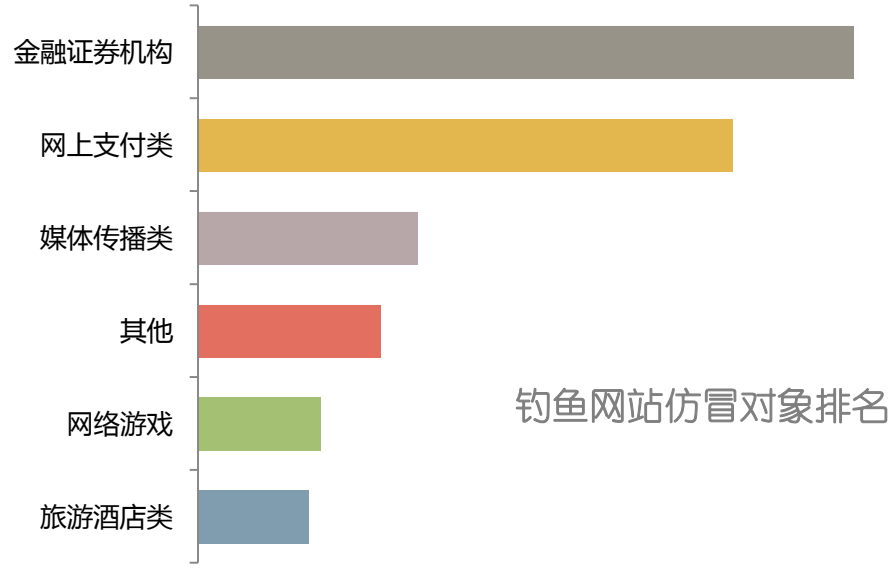
China Hacked Submit

Search: 提交者 组织名 IP 域名 精确 Search 黑 页 提 交

TOP50 User	时间	提交者	页面	查看快照
NO1:越南邻国宰相[9290]	2013-05-19	潘多拉	http://sunny.snut.edu.cn/xyadmin/test.html	快照
NO2:23026583[6131]	2013-05-19	失憶	http://ltc.synu.edu.cn/shiyi.htm	快照
NO3:左泪[4490]	2013-05-14	V	http://www1.gdou.edu.cn/wxy/v.txt	快照
NO4:ew[2848]	2013-05-10	Gooddog	http://cs.lcu.edu.cn/404.txt	快照
NO5:Learner[2617]	2013-05-10	日穿钢板	http://yyxy.hrbnu.edu.cn/	快照
NO6:D.H.T[2452]	2013-05-08	社工库	http://www.ny.ynu.edu.cn/index.php	快照
NO7:用幸福触摸 ...[2352]	2013-04-30	宇少	http://sports.njau.edu.cn/jyhack.html	快照
NO8:Any[2303]	2013-04-28	Learner	http://ocw.guet.edu.cn/Learner.txt	快照
NO9:Cracker-Mr.X[1801]	2013-04-24	M4sk	http://www.hziee.edu.cn/M4sk.txt	快照
NO10:QQ:124320170[1687]	2013-04-18	V	http://fgc.sisu.edu.cn/v.html	快照
NO11:霸业永峰[1681]	2013-04-14	浅蓝	http://jdgc.nxtvu.edu.cn/1.htm	快照
NO12:soojoy[1638]	2013-04-13	越南邻国宰相	http://www.gsdxlg.edu.cn/1937cN.html	快照
NO13:八神[1630]	2013-04-13	越南邻国宰相	http://www.ee.gxnu.edu.cn/1937cN.html	快照
NO14:网络小子[1272]	2013-04-13	越南邻国宰相	http://www.xrsdxx.edu.cn/1937cN.html	快照
NO15:QQ群:5761981[1241]	2013-04-13	越南邻国宰相	http://www.jt.imu.edu.cn/1937cN.html	快照
NO16:qq1281232825[1234]	2013-04-13	越南邻国宰相	http://www.whus.edu.cn/1937cN.html	快照
NO17:M4sk[1198]	2013-04-13	越南邻国宰相	http://www.mvlabyzh.fudan.edu.cn/1937cN.html	快照
NO18:寒水芊芊[1085]	2013-04-13	越南邻国宰相	http://www.ywb.hbnu.edu.cn/1937cN.html	快照
NO19:糊涂工作室[1080]	2013-04-05	knickers	http://daf.tsinghua.edu.cn/html/hacked.txt	快照
NO20:波哥VS布冯[1078]	2013-03-31	越南邻国宰相	http://www.law.ruc.edu.cn/library/UploadFiles_1636/201333123542516368.txt	快照
NO21:Timeless[1050]	2013-03-22	宅男の神	http://www.xsc.ldu.edu.cn/zhainan.html	快照
NO22:木鱼工作室[1049]	2013-03-07	宇少	http://www.lntc.edu.cn/xzdw/zzb/upfiles/news/20130307110629918.txt	快照
NO23:红领巾冲封心[928]	2013-03-07	宇少	http://www2.jci.edu.cn/jw/upfiles/news/20130307110255628.txt	快照
NO24:雪刺[866]				
NO25:HacKerCc[838]				
NO26:黑羽...燃[816]				
NO27:Mr.Cool[788]				
NO28:电脑迷[786]				
NO29:王可欣[749]				
NO30:流浪込[714]				

最后，一些中小型企业网站也是非常容易被攻击的对象，往往这类网站的投入更小，域名多数在国外注册，机器托管在国外的机房。为了降低成本他们会选择一些价格便宜的注册商。这恰恰会使他们的网站面临极大的安全隐患。很多网站在被挂马很长时间之后仍然没有人处理。

2013 年第 1 季度 Web 威胁钓鱼网站仿冒对象分析



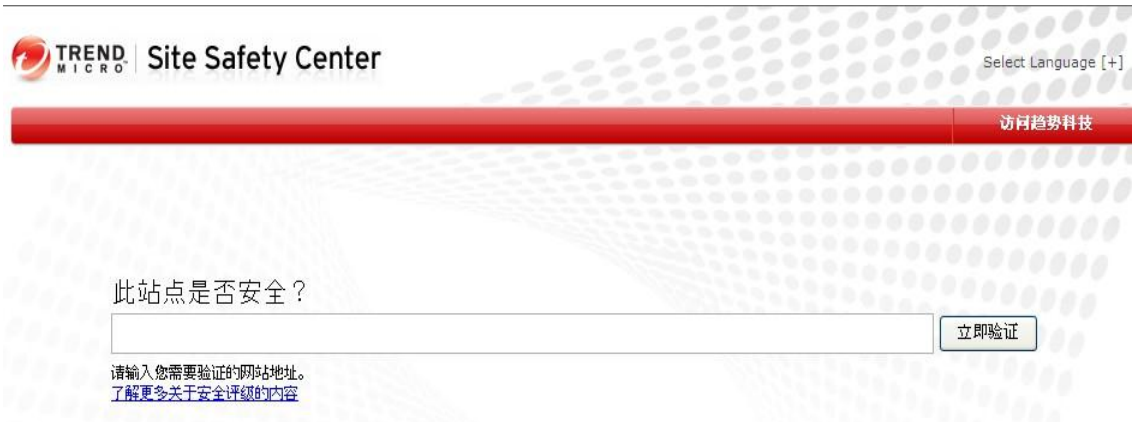
从第 2013 年第 1 季度趋势科技捕获到的钓鱼网站数据来看，金融证券机构，以及网上支付类网站这些能够直接为钓鱼网站制造者带来经济利益的站站仍然是钓鱼者最喜欢仿冒的对象。银行网上支付的钓鱼网站也制作的非常逼真使人防不胜防。

提醒用户在网络上面进行任何交易时请小心谨慎。特别是通过淘宝网站购物时尽量不要点击聊天窗口中的 URL 进入支付页面。

随着“中国好声音”“我是歌手”这一类受观众热捧的节目出现，一些仿冒电视台媒体对节目，选手进行投票和抽奖的钓鱼网站在第一季度也有增加。

对于无法辨别恶意与否的网站可以到趋势科技网站安全查询页面查询：

http://global.sitesafety.trendmicro.com/index.php



2013 年第 1 季度最新安全威胁信息

2013. 1 新的 java 零日漏洞（CVE-2013-0422）

近日，一个新的 java 零日漏洞(CVE-2013-0422)发现能够被一些黑客工具利用，此漏洞可以允许未经身份验证的远程攻击者在受害者系统上执行任意代码。

这些工具包括：Blackhole Exploit Kit (BHEK)以及 Cool Exploit Kit (CEK)等.

开发 Cool Exploit Kit (CEK)的正是迄今黑市最猖獗的 web-based 入侵工具 Blackhole Exploit Kit (BHEK)的作者。CEK 似乎是一个更容易上手的高端版本 BHEK。

这个漏洞在最开始是被纳入了 CEK 而在加入 BHEK 之后才被公开。据报道，CEK 被用于传播勒索软件，特别是 Reveton(一种隐蔽强迫式下载的欺诈软件)的变种。

Reveton 是当前很常见的一种欺诈威胁。它会锁定用户系统显示来自于当地警察机构的通知。其中包括通知用户必须支付$200-$300 罚款用以解锁其电脑。

目前，趋势科技将此零日漏洞检测为 JAVA_EXPLOIT.RG，含漏洞代码的页面被检测为 HTML_EXPLOIT.RG 相关的欺诈软件被检测为 TROJ_REVETON.RG 和 TROJ_REVETON.RJ.

此漏洞的相关链接：

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422

趋势科技相关 blog：

http://blog.trendmicro.com/trendlabs-security-intelligence/java-zero-day-exploit-in-the-wild-spreading-ransomware/

http://blog.trendmicro.com/trendlabs-security-intelligence/java-zero-day-exploit-and-ruby-on-rails-vulnerabilities/

http://blog.trendmicro.com/trendlabs-security-intelligence/what-to-expect-from-toolkits-and-exploit-kits-this-2013/

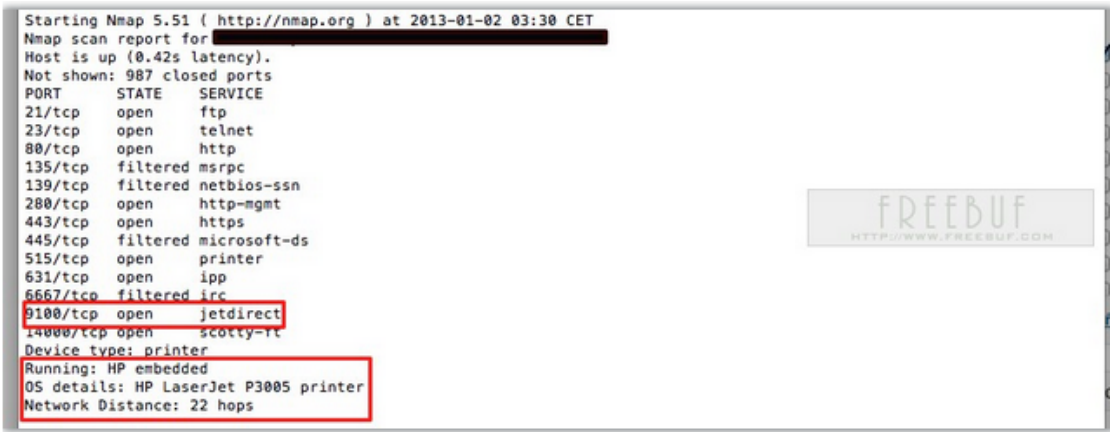
http://blog.trendmicro.com/trendlabs-security-intelligence/police-ransomware-evolving-at-a-tremendous-pace/

http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-2-0-beta-tests-in-the-wild/

2013. 1 惠普打印软件 JetDirect 漏洞致多款网络打印机受威胁

本月中，西班牙研究人员 Guerrero 研究发现惠普打印软件 JetDirect 存在漏洞，使攻击者可以绕过生物或刷卡的安全保护，访问部分打印文档，或通告网络对存在漏洞的网络打印机造成拒绝服务攻击。

JetDirect 虽然是惠普设计的，但是众多打印机都使用该软件，包括 Canon、Lexmark、Samsung 和 Xerox。该软件负责处理通过网络提交的打印请求。网络打印机通过 JetDirect 协议，侦听，接收打印请求数据，如下图所示是通过 nmap 扫到网络打印机的监听端口：



相关链接：

http://www.freebuf.com/articles/system/7115.html

2013.2 POSTGRESQL 爆出输入验证不当漏洞

PostgreSQL 是一款高级对象-关系型数据库管理系统，支持扩展的 SQL 标准子集。

PostgreSQL 9.2.3 之前的 9.2.x 版本，9.1.8 之前的 9.1.x 版本，9.0.12 之前的 9.0.x 版本，8.4.16 之前的 8.4.x 版本，8.3.23 之前的 8.3.x 版本中存在漏洞。该漏洞源于程序没有对 backend/utils/adt/enum.c 中的 enum_recv 函数进行正确地声明，从而使得该函数被错误的参数所引用。通过可触发数组索引错误和越界读取的特制 SQL 命令，远程认证攻击者可利用该漏洞导致拒绝服务（服务器崩溃）或读取敏感进程内存。

相关链接：

http://cve.scap.org.cn/CVE-2013-0255.html

趋势科技相关 blog：

http://blog.trendmicro.com/trendlabs-security-intelligence/postgresql-denial-of-service-vulnerability-found-and-patched/

2013.2 外媒称 上海一 12 层建筑为解放军黑客总部

多家西方媒体 2 月 19 日引述美国网络安全公司 Mandiant 拟于美国时间周二发表的一份 60 页报告称，近年美国遭受的网络黑客攻击多与中国军方有关。《纽约时报》19 日援引报告摘要称，该公司历时 6 年追踪 141 家遭受攻击企业的数字线索，证实实施攻击的黑客组织隶属于“总部设于上海浦东一栋 12 层建筑内的中国人民解放军 61398 部队”。对此，中国国防部新闻事务局 19 日回应称，中国军队从未支持过任何黑客活动，有关报道与事实不符。

相关链接：

http://news.xinhuanet.com/local/2013-02/20/c_124367203.htm

2013.3 韩国多家媒体遭到黑客攻击

20 日，据韩国联合通讯社报道，韩国广播公司、文化广播电台、韩联社电视台等媒体以及新韩银行、农协银行等金融机构的计算机网络当天全面瘫痪。

韩国广播公司工作人员说，公司内部计算机网络当天下午 2 时许突然瘫痪。韩联社电视台方面确认，不仅办公室计算机网络无法运行，电视节目编辑设备也出现死机。

韩国警察厅确认接到多家机构报警，派出网络安全应对小组展开调查。韩国军方已经将情报作战防卫级别上调一级。

韩国总统府青瓦台国家安全室室长提名人金章洙当天临时启动国家安全室工作，听取国防部、国家情报院、警察厅等机构汇报。

韩国政府 20 日初步证实，这次的计算机网络瘫痪由恶意代码所致。

当天，韩国政府从广播通信委员会、警察厅、韩国网络振兴院抽调专业人员，组成联合应对小组，前往韩国广播公司等机构，从受攻击的电脑里获取恶意代码样本并展开研究。

分析结果显示，网络瘫痪是由于恶意代码破坏了计算机的“启动系统”。韩国广播通信委员会当天下午对媒体说，依据分析结果推测，此次网络瘫痪是由恶意代码侵入上述机构的“更新管理服务器”所致，但目前尚不能确定散布恶意代码的具体始发地。

自当天下午 3 时起，韩国的网络危机警报级别上调为“注意”级，负责网络监控的人员数量增至平时的 3 倍以上。

相关链接：

http://finance.ifeng.com/money/roll/20130321/7802284.shtml

趋势科技相关 blog：

http://blog.trendmicro.com/trendlabs-security-intelligence/summary-of-march-20-korea-mbr-wiper/

关于趋势科技

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的1,500余名趋势科技安全专家可为各国家和地区的企业级个人用户提供7×24的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问: www.trendmicro.com.cn。

TREND MICRO 趋势科技 [全程护航 迈向云端]

关于中国区网络安全监测实验室

趋势科技“中国区网络安全监测实验室”是国际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。趋势科技“中国区网络安全监测实验室”利用趋势科技的全球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。

ChinaRTL

中国区网络安全监测实验室