2012 年度中国地区
网络安全综述

2013/2

CHINA RTL

目录

2012 年中国地区网络安全威胁回顾

年度安全标签：

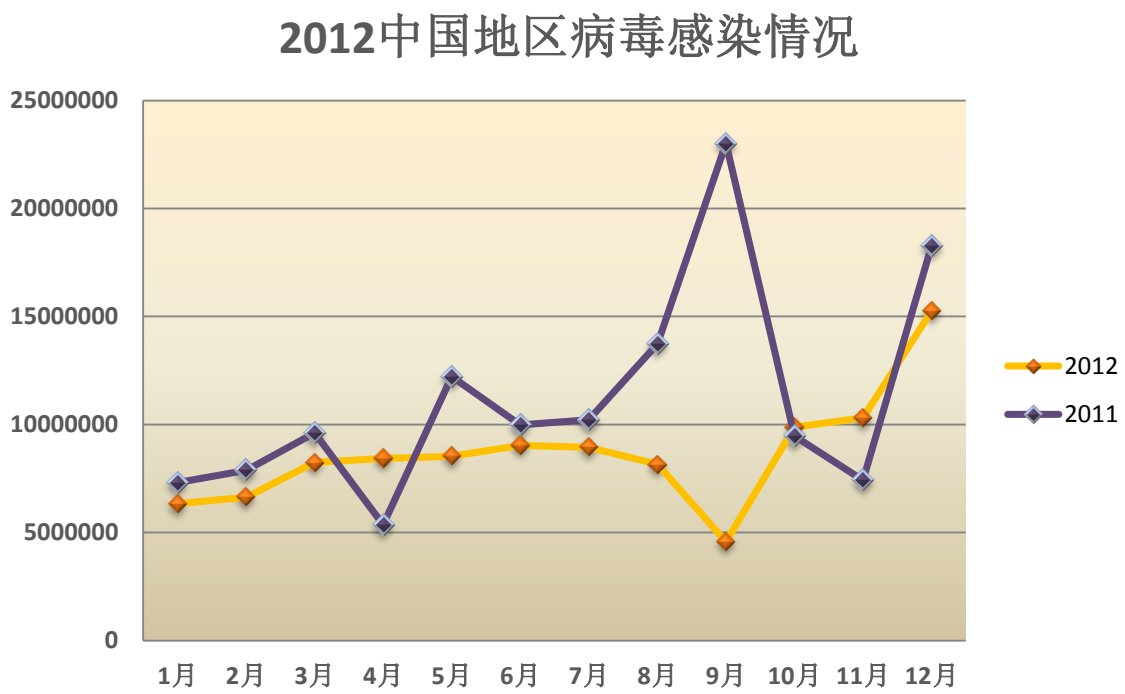
PE 感染型病毒，漏洞攻击，手机病毒

2012 年度中国地区病毒回顾

2012 年中国地区病毒情况综述

2012 年度趋势科中国区传统病毒码新增特征 229 万条。截止至 2012.12.31 日中国区传统病毒码 9.628.60 包含病毒特征数约为 424 万条。

2012 年趋势科技在中国区检测病毒次数约 1 亿 1 千万次。相较于 2011 年，病毒感染情况稳中有降。之前感染数量较多的 WORM_DOWNAD 病毒得到了较好的控制。2012 年中没有很大规模的病毒爆发事件发生，其中病毒感染最多的月份在第四季度。



2012 年中国地区病毒感染情况

2012 年中国地区毒感染数量排名

病毒感染数量 TOP20

1	PE_PARITE.A	5221494
2	WORM_DOWNAD.AD	2781458
3	PE_SALITY.RL-O	2012823
4	PE_MUSTAN.A	1282437
5	TROJ_VSTART.SMA	1219531
6	TROJ_FAKEALERT.BMH	1083386
7	PE_SALITY.DAM	1037962
8	WORM_TRAXG.F	1005224
9	WORM_AUTORUN.SMW	1002822
10	PE_CEKAR.SM	974684
11	TROJ_CORELINK.D	914617
12	PE_SALITY.RL	887371
13	WORM_LOVGATE.Q	765233
14	WORM_FLYSTUDI.B	723484
15	WORM_ECODE.E-CN	711676
16	PE_CORELINK.C-1	698044
17	PE_MUSTAN.B	656041
18	PE_PARITE.A-O	639650
19	WORM_SILLYFDC.DN	630751
20	TROJ_MICROFAK.AC	601866

2012 年可谓是 PE 病毒当道的一年，感染数量排名前 3 名中，PE 类型病毒就占据了 2 位。

PE_PARITE, 是 2001 年出现的一种 PE 感染型病毒。近几年一直都在持续活动中，但是我们发现，从 2012 年第一季度开始，这种病毒中国地区有增多的趋势。

这种病毒通过共享或感染文件传播，一般通过感染进程 Explorer.exe 注入系统，在 windows 临时目录中释放随机命名的.tmp 文件。

具有以下行为：

- 会连接远端的 IRC 服务器进行通讯
- 会下载其他恶意文件
- 会创建自启动的注册表键值
- 会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

WORM_DOWNAD，在 2012 年一直在平稳下降。但由于前几年的感染范围过大，导致在数量上还一直处于排名靠前位置。正如我们在去年年报中所描述的，由于该病毒的防护处理方案已经很成熟，除非在之后出现新的变种。否则，该病毒的感染情况在 2013 年也会保持持续下降趋势

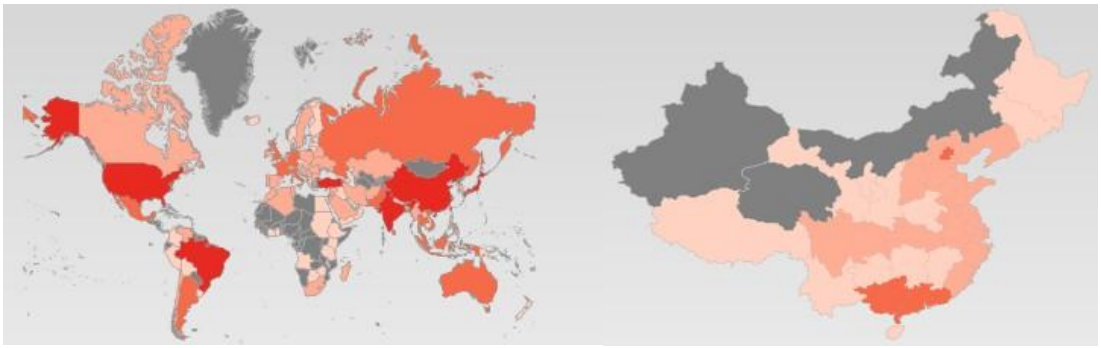
PE_SALITY, 也是 2012 年感染较严重的病毒之一，该病毒出现于 2003 年，从 2011 年年末开始在中国地区增长，按照目前的趋势来看在 2013 年该病毒仍然会给大量用户造成不小的危害。

该病毒具有以下行为：

- 会下载其他恶意文件
- 修改注册表键值
- 利用 windows 的快捷方式漏洞
- 感染系统中的可执行文件

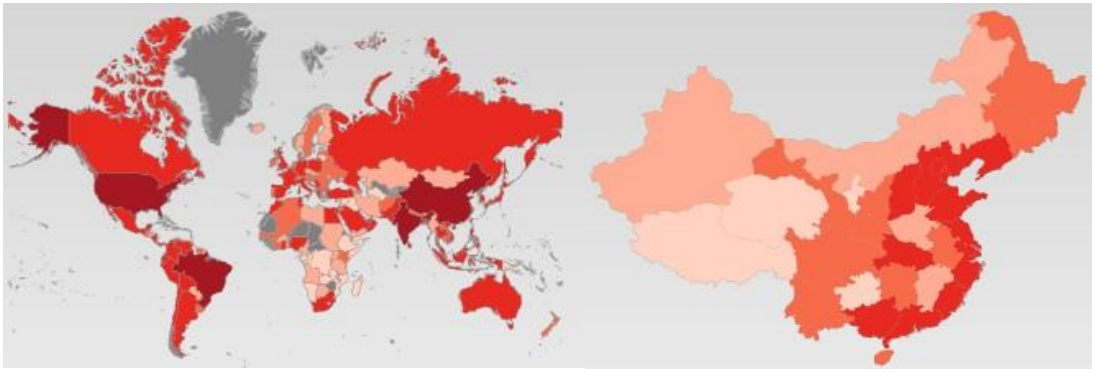
随着计算机技术的发展，木马，蠕虫以及 PE 病毒的差别正在逐渐缩小，每种类型的病毒都可能包含有其他类型病毒的特征，混合型病毒已经逐渐成为当前的主流。特别是 PE 感染型病毒更是可能包含有所有病毒类型的行为特征。也是目前相对难以处理的病毒。这种病毒在中国地区的增长可能会为防病毒体系带来极大的挑战。

PE_PARITE 全球及中国地区感染情况



PE_PARITE 在全球都有感染，其中较严重地区分布在中国，美国，印度，土耳其，巴西
在中国感染较严重的地区为南部沿海和北京

WORM_DOWNAD 全球及中国地区感染情况



WORM_DOWNAD 在全球范围都有感染，其中较严重地区分布在中国，印度，美国，巴西
在中国感染较严重的地区为东北部地区以及东南沿海地区

PE_SALITY 全球及中国地区感染情况

PE_SALITY 主要在亚太地区被发现，其中感染最严重的地区为印度
在中国感染较严重的地区在东南沿海地区

对于网络病毒的防护建议

对于个人用户：

1. 安装防毒软件并保持组件更新
2. 下载并安装软件之前先进行安全扫描，尽量不要从非正规网站下载，尽量不要使用破解软件
3. 注意移动存储设备的使用，尽量关闭自动播放功能，接入电脑之前进行安全扫描
4. 尽量提高 office 软件的安全等级，以防范宏病毒的感染
5. 不要随意打开来历不明的邮件，更不要下载执行其中的附件

对于安全部门：

1. 保证防病毒软件的部署率
2. 加强共享存储的管控
3. 部署相关的安全策略，建立完整的安全体系，做好病毒爆发应急预案
4. 加强员工的安全意识教育

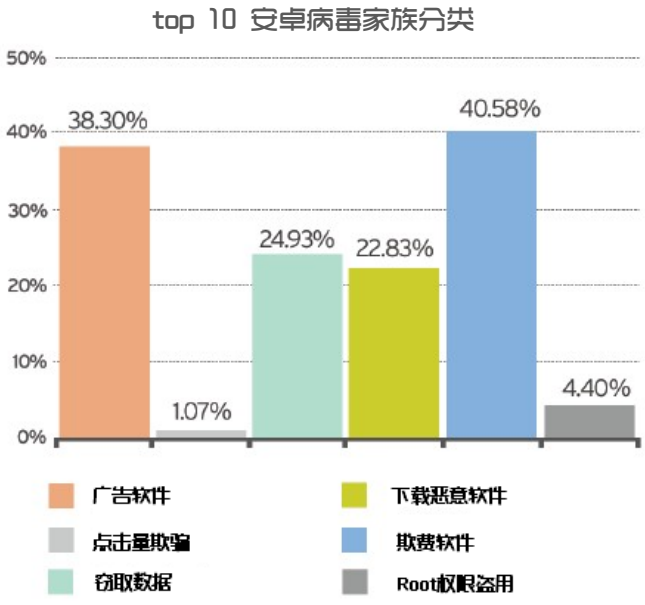
2012 年度手机安全回顾

2012 年手机病毒情况综述

毫无疑问 2012 年移动设备成了越来愈多网络罪犯的攻击目标，趋势科技监控到全球针对安卓平台的恶意软件从年初的 1000 个上升到了年末的 350000 个。恶意软件的爆炸性增长从某种程度上也反映了安卓系统本身使用量的快速增长.

2012 年有两种类型恶意软件占据了移动平台恶意软件的主导地位。第一，吸费软件。这种软件在用户不知情的情况下为用户订购付费服务，以谋取利益。第二，窃取用户敏感数据。这种高风险的恶意程序在未经客户允许，或者在没有明确的告知客户的情况下获取用户移动设备中的敏感数据。

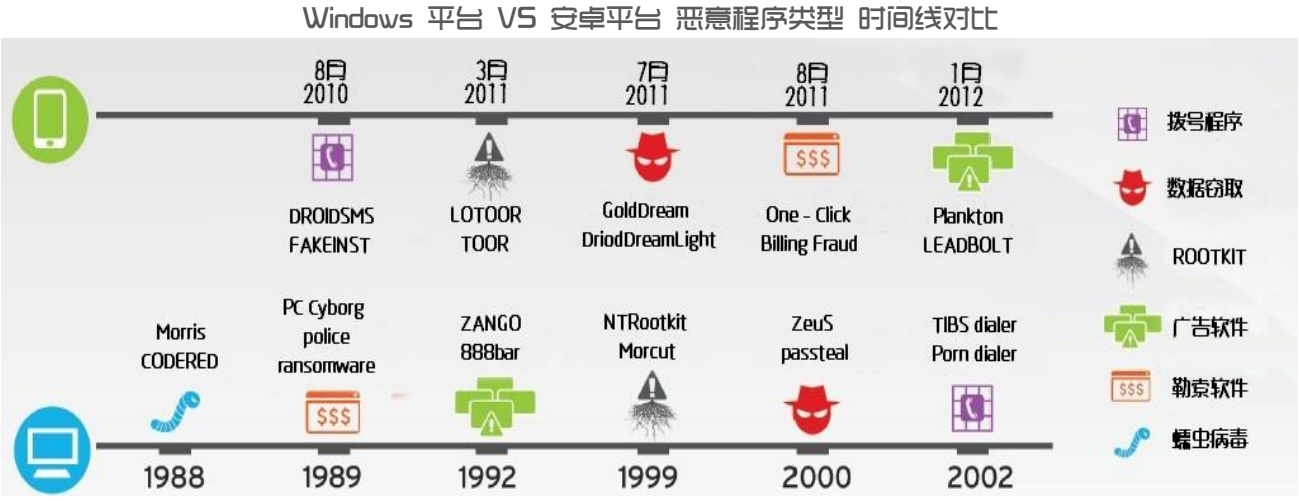
安卓平台恶意程序数量在 2012 年的第三季度末开始惊人的增长，其部分原因是因为吸费软件和一些高风险软件在 2012 年年末大量出现。



超过 70%的安卓平台恶意软件仅属于几个病毒家族类型，其中大部分是吸费软件以及有高度风险的应用程序。

目前移动设备的安全威胁很大一部分是针对安卓系统，它们的增长速度远远超过了 PC 平台。PC 平台操作系统 Windows 诞生 14 年后，恶意软件数量才达到 35 万，而 Android 移动平台则在 3 年内即迅速达到了这个数字。

针对 Windows 平台的恶意程序具有各种分类，在安卓平台上也是如此。在 2012 年大约有 600 多种新的病毒家族被发现.



随着安卓系统的更加普及以及使用率的增长，2013 年针对于安卓平台的恶意程序以及高风险程序的数量将达

到 100 万。安卓系统病毒将会出现新的传播方式，可能将会出现一些新的攻击手法。

对于手机安全威胁的防护建议

对于个人用户：

1. 不要忘记使用智能手机内置的安全功能
2. 避免连接免费但是不安全的 WIFI
3. 无论从哪里下载的应用程序都需要仔细检查
4. 在授予应用程序权限之前要仔细确认是哪些权限并了解这些权限
5. 安装针对手机平台的安全软件

对于安全部门：

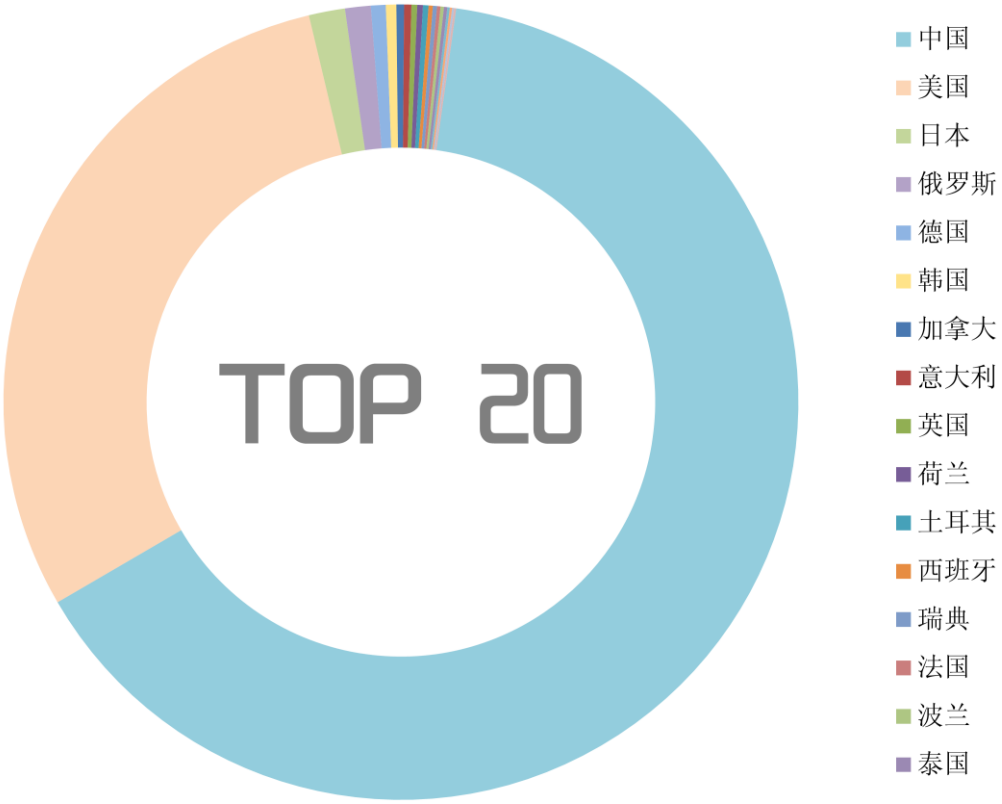
1. 加强员工手机安全使用教育（参照对于个人的建议）
2. 需要有一个关于手机安全管理的方案
3. 在安全架构中加入手机安全部分
4. 对于手机或移动设备连入公司内部网络需要有一定的访问控制或监控措施

2012 年度中国地区网络安全回顾

2012 年 web 安全综述

2012 年趋势科技在中国地区拦截恶意网页约 2 亿次。其中约 31%的网页为被挂马网站，其余的 69% 为恶意网站。

与去年相比分布在俄罗斯和日本地区的恶意网站比例有所减少，但是仍有约1/3的恶意网站在国外注册.

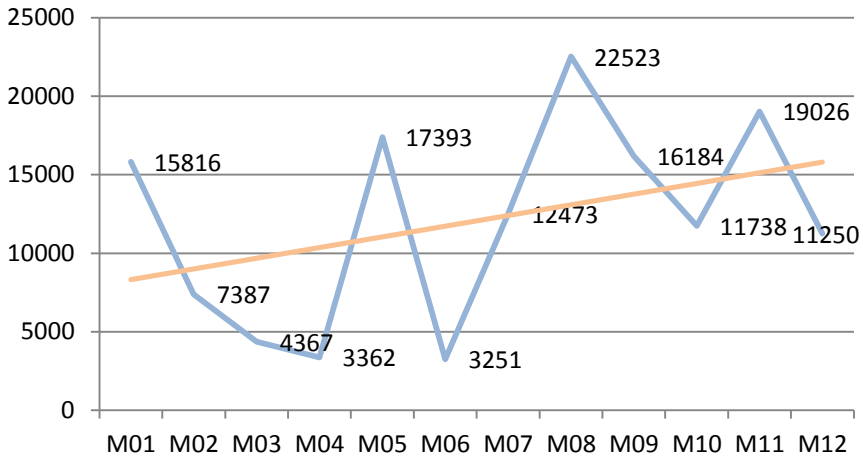


2012 年恶意网站域名所属地

除了恶意网站，也有一部分公司或个人在在国外注册域名.在注册方便与价格优惠的同时也伴随着一定的风

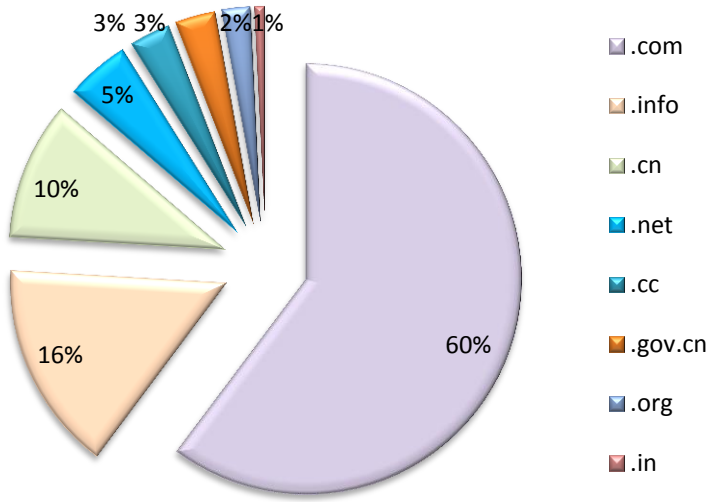
险.境外一些域名注册商管理上的漏洞往往会给一些不法分子提供便利的条件,而给域名注册者带来损失.一定要在国外注册域名的用户选择域名注册商时，应仔细的考察注册商的软、硬件实力。

2012年趋势科技在中国地区监测到约14.5万个网站被挂马，可以看到，挂马网站数量趋势在2012年呈现上升趋势，在8月份达到峰值，在6月份为全年最低值.



2012 年中国大陆挂马网站数量月度统计

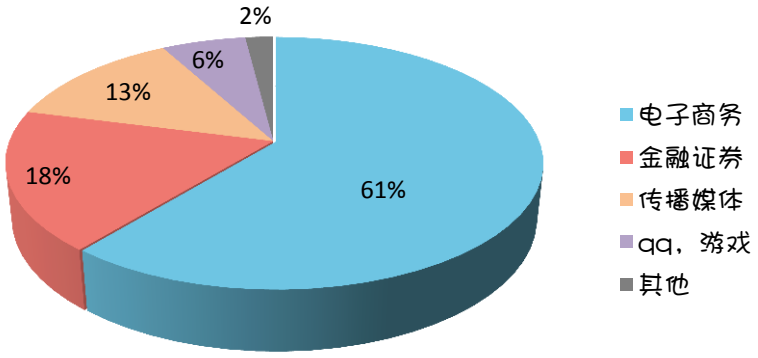
2012 年,挂马网站按照域名分类，比例排名前三位的是.com域名（60.7%）、.info域名（15.8%）和.cn域名（10.5%）。此外，被挂马的政府网站（.gov.cn域名网站）数量为4343个，占全部挂马网站总数的3%。



2012 年中国大陆地区挂马网站按域名分布情况

被挂马的网站中约有45%是色情网站，彩票网站.为避免感染病毒，应尽量避免访问这些网站.还有一些非正规的软件下载网站，以及图书网也是被挂马的对象.从非正规网站下载文件时一定要仔细检查.在不确定网站是否有危害时可以到http://global.sitesafety.trendmicro.com/index.php检测后再进行访问.

2012 年，钓鱼网站仿冒对象与前两年变化不大，主要还是集中在电子商务，金融证券，和媒体传播这几类。微博已经成为了新的钓鱼网站传播媒介，网络罪犯在微博上发起虚假中奖信息或者活动引诱用户中招。



钓鱼网站仿冒对象

钓鱼网站的手段花样繁多，但是最终都是要利用用户的“贪便宜”“不谨慎”来骗取重要信息或钱财。许多钓鱼网站虽然做的几乎可以以假乱真但是在访问时稍微仔细一些即可发现有很多“怪异”的地方。例如：应该是链接的地方贴的却是图片，URL 地址非常像仿冒对象但是却有细微差别等等。另外在线交易时一定要走官方的流程，切勿点击卖家通过其他方式发送给你的交易链接。在输入重要的账号密码前务必谨慎。

排名前十的恶意网站

域名	原因
traffi cconverter.biz	传播恶意程序，特别是DOWNAD
info.ejianlong.com	下载恶意程序
deepspacer.com	恶意主机的url地址，其注册人是已知的垃圾邮件发送者
mmi.explabs.net	木马请求连接的url
www.funad.co.kr	造成暴露的系统或网络的安全风险
www.trafficholder.com	传播恶意文件的网站
serw.clicksor.com	不停弹出非法消息
install.ticno.com	发布恶意软件
172.168.6.21	传播宏病毒，如X97M_LAROUX.BK，XF_HELPOPY.AW，XF_NETSNAKE.A，X97M_LAROUX.CO，X97M_LAROUX.CE

对于 web 安全威胁的防护建议

对于个人用户：

1. 不要轻信“中奖”，“免费”之类的信息
2. 在需要输入帐户、帐号、密码等敏感信息的时候，注意检查 URL 是否正确。
3. 尽量提高浏览器的安全等级。
4. 不要直接运行网页上下载的可执行文件或文档
5. 安装有网页防护功能的防毒软件并保持组件更新

对于安全部门：

1. 部署网关防护设备
2. 制定与网页访问有关的安全策略
3. 加强员工的安全意识教育

2012 年度漏洞与攻击回顾

2012 年，从 1 月份报出的利用 Windows Media 允许远程执行代码漏洞 CVE-2012-0003 的恶意程序，到 8 月份的 JAVA7 的零日漏洞被黑客工具利用，再到 9 月份新的 IE 零日漏洞被利用.....零日漏洞被利用事件在频繁的发生。

但是不代表攻击者一定要去寻找新的漏洞才能进行攻击，因为还有很多电脑使用者并没有更新相关的补丁程序，很多在一年两年甚至几年前已经修复的漏洞仍然在被大量利用。

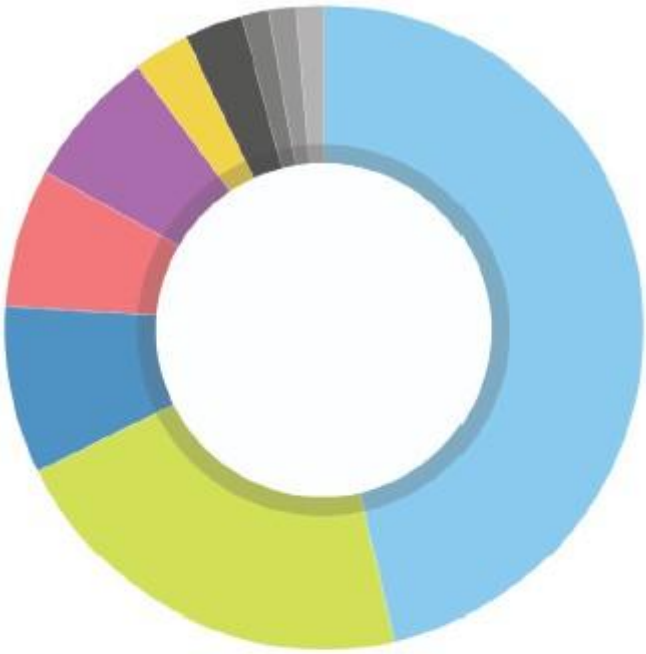
数据显示，2008 年爆出的一个服务器远程执行代码漏洞在 2012 年的在中国地区被利用次数排在第二名。很多企业和个人在被查出感染 WORM_DOWNAD 病毒时仍然没有安装相关补丁。

2012 中国地区被利用漏洞 top7

被利用漏洞	内容
FTP目录便利漏洞(CVE-2008-2894)	NCH Software Classic FTP 1.02 windows客户端软件存在漏洞，允许远端服务器通过返回一个。。来创建或者覆盖任意软件
MS08-067:服务器服务中的漏洞可能允许远程执行代码	这是一个远程代码执行漏洞。成功利用此漏洞的攻击者会完全远程控制受影响的系统。在基于 Microsoft Windows 2000、Windows XP、和 Windows Server 2003 的系统上，攻击者会在未经身份验证的情况下通过 RPC 利用此漏洞，并可运行任意代码。
微软IE浏览器跨域信息泄露漏洞	Internet Explorer在过滤HTML时处理使用特定字符串的内容的方式存在信息泄露漏洞。攻击者可以通过创建特制的网页来利用这个漏洞，如果用户查看了该网页就会导致信息泄露。成功利用这个漏洞的攻击者可以对用户执行跨站脚本，允许攻击者在用户的安全环境中对使用 toStaticHTML API的站点执行脚本。
Oracle 数据库 DBMS_CDC_PUBLISH 多个过程 SQL 注入漏洞	Oracle Database Change Data Capture组件提供属主为SYS的DBMS_CDC_PUBLISH PL/SQL包，这个包在DROP_CHANGE_SOURCE过程中存在SQL注入，恶意用户可调用这个包中有漏洞的过程，提交特殊构建的参数，以SYS用户特权执行SQL命令。 要利用此漏洞需要用户在SYS.DBMS_CDC_PUBLISH上有执行权限。
(MS11-002) Microsoft Data Access Components 中的漏洞可能允许远程执行代码	ODBC API(odbc32.dll)的SQLConnectW函数存在有符整数错误。通过向SQLConnectW传入超长数据源名称（DSN）字符串和畸形szDSN参数将导致DSN缓冲区溢出漏洞。
(MS11-001) Windows 备份管理器中的漏洞可能允许远程执行代码	如果用户打开与特制库文件位于同一网络目录下的合法 Windows 备份管理器文件，此漏洞可能允许远程执行代码。 要成功进行攻击，用户必须访问不受信任的远程文件系统位置或 WebDAV 共享，并从该位置打开合法文件，从而可能导致 Windows 备份管理器加载特制的库文件。
(MS11-006) Windows Shell 图形处理中的漏洞可能允许远程执行代码 (2483185)	如果用户查看特制缩略图，此漏洞可能允许远程执行代码。 成功利用此漏洞的攻击者可以获得与登录用户相同的用户权限

利用漏洞的工具包最常针对的应用程序，包括浏览器或者通过浏览器的插件功能来实现的技术，尤其 Internet Explorer，JAVA，以及 Adobe 旗下的 Acrobat,Reader,Flash 播放器。

浏览器漏洞工具攻击目标 top10



- JAVA 46.48%
- PDF 21.13%
- MS DATA ACCESS COMPONENTS 8.45%
- FLASH 7.04%
- IE 7.04%
- FIREFOX 2.82%
- WINDOWS 2.82%
- CHROME 1.41%
- MS XML CORE SERVICES 1.41%
- SAFARI 1.41%

对于漏洞攻击威胁的防护建议

对于个人用户：

1. 及时更新所有应用程序发布的补丁
2. 如果可以最好能够把程序和操作系统的自动更新功能开启

对于安全部门：

1. 建立集中部署更新的机制和确认客户端更新状态机制
2. 部署检测漏洞攻击相关的安全产品

2012 年度中国地区安全威胁大事记

第一季度

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
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

2012 年 3 月，趋势科技中国区病毒实验室发现一批欺诈网站

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

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

2012 年 3 月，MAC OS 现在也很容易遭到攻击
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/

第二季度

2012.6 中国区病毒实验室接到数起网络购物欺诈案件

2012.6《九阴真经》《暗黑 3》遭钓鱼网站围堵 玩家需小心装备不翼而飞
http://cn.trendmicro.com/cn/about/news/pr/article/20120619094755.html

2012.6 黑客攻破中国电信网络 发布 900 个后台密码
http://it.sohu.com/20120604/n344731733.shtml

2012.6 Windows 又现高危漏洞 “暴雷”轰然而至
http://technet.microsoft.com/zh-cn/security/advisory/2719615
http://www.freebuf.com/tools/4172.html

2012.6 Intel CPU 漏洞导致 64 位操作系统、虚拟化软件易受黑客攻击

http://news.mydrivers.com/1/231/231509.htm

2012.6 LinkedIn 用户的密码泄露
http://www.newhua.com/2012/0607/163032.shtml

第三季度

2012.8 首个 Linux、Mac OS X 的跨平台病毒被发现
http://www.freebuf.com/news/5500.html

2012.9 China RTL 发现一种新的感染型病毒 PE_MUSTAN 正在爆发。
http://security.ctocio.com.cn/87/12438587.shtml

2012.9 黑客组织从 FBI 获得超过 1200 万份苹果 iOS 用户信息，公开了 100 万份
http://www.guomii.com/posts/30926

2012.9 新的 IE 零日漏洞
http://blog.trendmicro.com/trendlabs-security-intelligence/new-ie-zero-day-exploit-leads-to-poisonivy/

第四季度

2012.10 微软正式发布 window 8 ，关于 windows8 系统的安全性成为热门话题
http://blog.trendmicro.com/trendlabs-security-intelligence/theyre-here-threats-leveraging-windows-8/

2012.12 伊朗信息安全中心（Iran CERT）发布声明，披露了一种可能具有针对攻击性的病毒。这种病毒会在指定时间删除感染电脑上指定磁盘中的文件。
http://blog.trendmicro.com/trendlabs-security-intelligence/unsophisticated-wiper-malware-makes-headlines/

2013 年网络安全威胁预测

恶意与高风险的安卓应用数量在 2013 年将突破百万

受安卓系统普及率大幅提升的影响，恶意与高风险的安卓应用数量在 2012 年底达到 35 万个，而这个数字在 2013 年当中或将攀升四倍，达到 140 万个。而且，这些恶意应用将越来越复杂。

APT 攻击广度以及深度将持续扩大

由于攻击的高精准度与高防范难度，APT 攻击在 2013 年将继续流行。而且，更多的黑客及不法组织会在 APT 攻击中进行持续投入，以改进攻击技术、提升攻击广度与深度。

网络犯罪者将大量滥用正当的云服务

在 2012 年，很多企业和个人受惠于云运算的强大性能，这引起了不法分子的觊觎。因此，2013 年必定将出现更多正当云服务被非法滥用的情况。

信息安全威胁将出现在更多的攻击管道

数字生活使得消费者的生活与网路的连结越来越紧密，而新技术则提供了新的攻击管道。除了个人电脑、平板电脑、智能手机之外，其它具备网络应用能力的设备（如智能电视）也可能成为信息安全威胁的管道。

消费者将使用多种网络应用平台，保护这些平台将更为困难

与过去只有少数几种网络应用平台不同的是，2013 年将会出现更多网络应用平台，每一种平台都需要不同的安全防护，这给统一防护带来了巨大的困难。同样，随著 App 应用逐渐取代浏览器的趋势，信息安全与隐私权问题就更难在通用的架构中得到解决。

以政治为动机的网络攻击将变得更具破坏性

在 2013 年，我们将看到更多以政治为动机的网络攻击，这些攻击往往会修改或破坏信息，甚至对某些基础设施建设造成破坏。

不论是否使用云端储存，信息外泄依然是 2013 年的威胁之一

随著企业开始将机密信息转移到云端，企业将会发现，那些用来保护企业服务器信息安全的解决方案，到了云环境中将无法发挥应有效果，信息泄密的可能性将大幅提升。IT 系统管理员必须确保云安全解决方案设定正确，并且在这方面拥有充分的防护能力。

网络犯罪防治法律可能需要三年后才会发挥实效

尽管很多国家已经拟定了网络犯罪防治法律，但大部分的工业化国家至少需等到 2015 年之后才能有效地强制执行相关法律。企业必须在自身的 IT 基础架构上采取更主动的预防措施，以降低法律缺位造成的负面影响。

传统的恶意程序威胁将缓慢演进，攻击的部署方式将日趋精密

在 2013 年，恶意程序将着重于改进攻击方式以应对安全防护软件的查杀。同时，不同网络犯罪地下团体之

间的彼此合作也将更加普遍，他们将会发挥各自的攻击专长，对于目标发动更具威胁性的攻击。

非洲将成为网络犯罪者新的避风港

由于经济基础较差，执法不严格，在非洲的网络犯罪者往往会因为促进当地经济发展而受到当地欢迎。因此，在 2013 年，非洲会逐渐成为精密网络犯罪的温床。

以上具体内容请参考趋势科技《2013 信息安全关键十大预测》报告

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)
本报告部分内容引用自 TrendLab MALWARE BLOG http://blog.trendmicro.com

关于趋势科技

趋势科技股份有限公司(TSE:4704)是全球云端安全的领导厂商，致力于保障企业与消费者数字信息交换环境的安全。趋势科技是业界的技术先驱，在服务器安全领域拥有超过 20 年的经验领先的整合式资安威胁管理技术能遏阻恶意程序、垃圾邮件、数据外泄以及最新的 Web 资安威胁，确保营运作业不中断，保障个人信息与财产的安全。请造访 TrendWatch 查询资安威胁详细信息，网址是：www.trendmicro.com/go/trendwatch。本公司弹性化的解决方案有多种型态可供选择，而且还有全球资安威胁情资专家提供 24 小时全年无休的支持服务。本公司许多解决方案均以 Trend Micro™ Smart Protection Network 为基础，这是涵盖网关外广大空间与客户端的新一代内容安全基础架构，专为协助客户防范 Web 资安威胁所设计。趋势科技是总部位于东京的跨国企业，其备受信赖的安全解决方案透过其业务合作伙伴营销全球。请造访 www.trendmicro.com。

TREND MICRO 趋势科技 全程护航 迈向云端

关于趋势科技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