中国地区 2012 年
第三季度
网络安全威胁报告

2012/11

目录

2012 年第 3 季度安全威胁

本季安全警示：

PE 病毒，宏病毒

2012 年第 3 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 **60** 万条。截止 2012.9.30 日中国区传统病毒码 **9.430.60** 包含病毒特征数约 **400** 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 **9850** 万次。
- 本季度趋势科技在中国地区发现并拦截新的恶意 URL 地址约 **30** 万个。

2012 年第 3 季度中国地区，木马病毒仍然占据新增病毒数量排名首位。大部分木马有盗号的特性，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。

第 3 季度的病毒检测数量排名中，PE 病毒超过木马跃居第一位。本季度 PE 病毒感染情况严重：

PE_MUSTAN 病毒在本季度爆发，该病毒由 WORM_MORTO（windows 远程桌面蠕虫）病毒演变而来。该 PE 病毒除了能够通过感染文件，网络共享，以及可移动存储设备传播。还能通过远程桌面传播，并且具有感染可执行文件的能力.

PE_CORELINK 病毒本季度进一步的扩散。在 2007 年这只感染型病毒使得大量电脑中招瘫痪。如今具有死灰复燃的趋势。该病毒会在系统 windows 目录释放 linkinfo.dll 使用 rootkit 隐藏自身,通过网络共享以及移动存储设备传播。

上季度提到的 2 种 PE 病毒 PE_PARITE.A，PE_SALITY.RL 在本季度仍在流行中，其中 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。而 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。

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

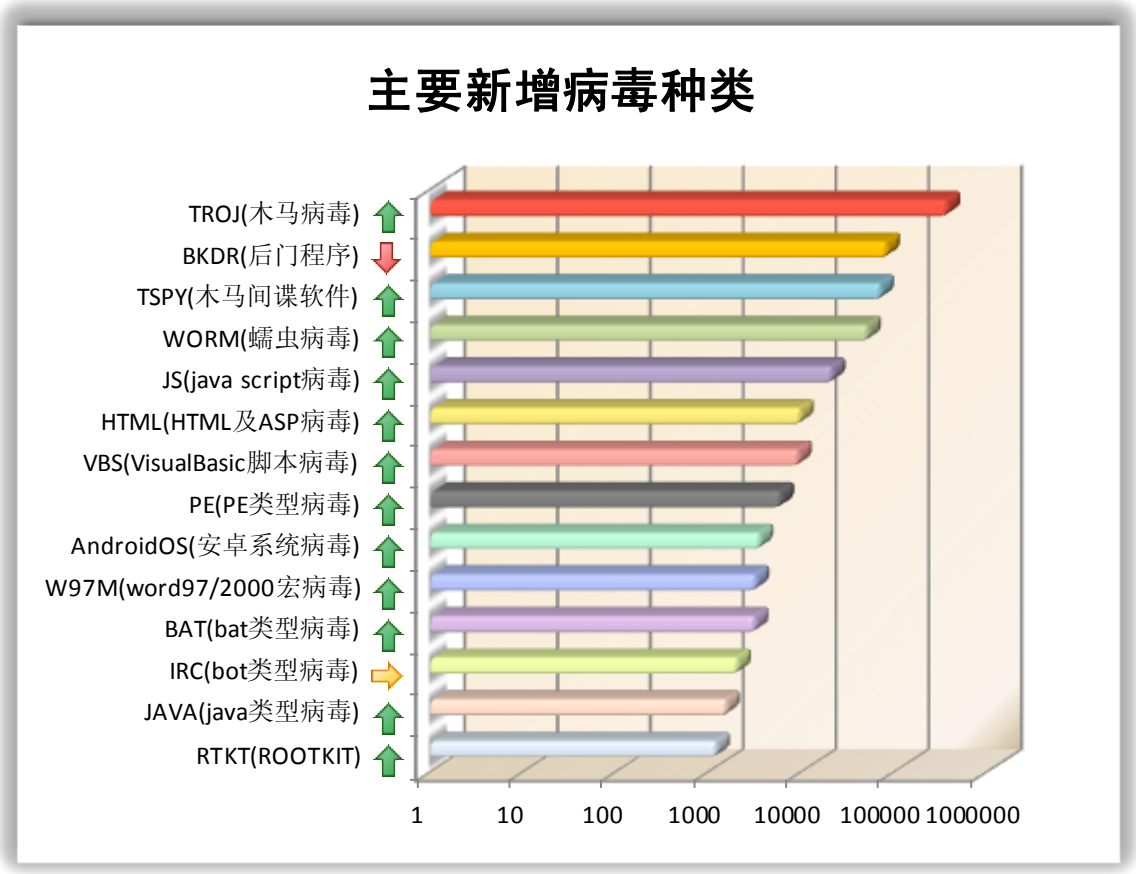
用安全软件进行扫描。

在 2012 年第 3 季度趋势科技拦截新的恶意网站中钓鱼网站约有 5000 个(以域名计数)。各种钓鱼网站仿冒目标中，淘宝网首当其冲。成为各钓鱼网站最喜欢仿冒的对象。由于微博的影响力的扩大，以微博抽奖、中奖为名进行网络钓鱼数量大大增加。

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) ,本报告中所有数据仅针对中国地区。

2012 年第 3 季度病毒威胁情况

2012 年第 3 季度新增病毒类型分析



2012 第 3 季度中国地区新增病毒（按类型分）

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 343621 个，大约占新增病毒数量的 60% 。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。

本季度除了新增的后门病毒类型病毒数量稍稍有所下降。其他类型病毒新增数量均有所上升。（上图中箭头表示与上季度相比的数量趋势）

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。Office 文件中往往保存了用户的重要数据和信息，宏病毒的增长也给数据安全带来了很大的挑战。

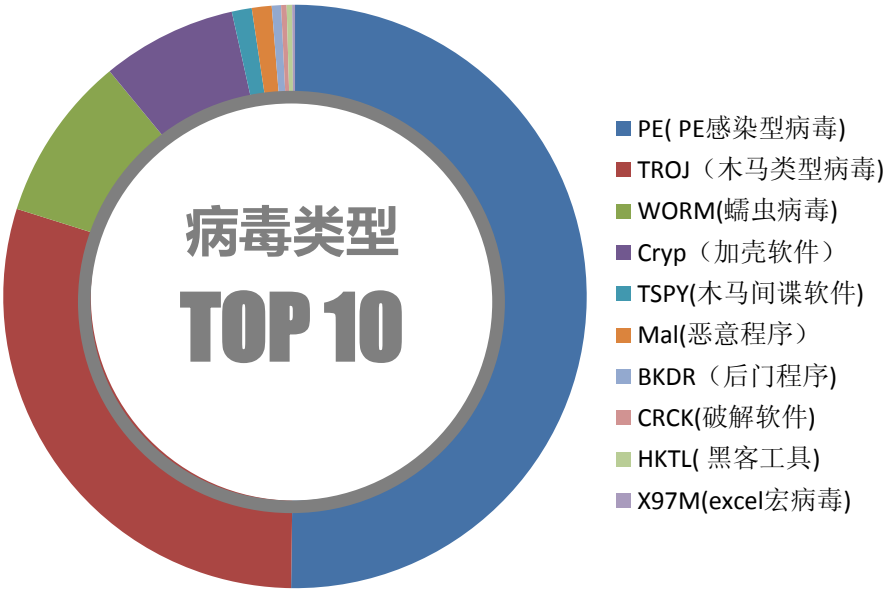
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

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。

ROOTKIT 是指其主要功能为隐藏其他程式进程的软件，可能是一个或一个以上的软件组合；广义而言，Rootkit 也可视为一项技术。病毒采用 rootkit 技术可以隐藏自身不被感染者甚至防毒软件发现。

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) ,本报告中所有数据仅针对中国地区。

2012 年第 3 季度各类型病毒检测情况分析



2012 第 3 季度中国地区各类型病毒检测数量比例图

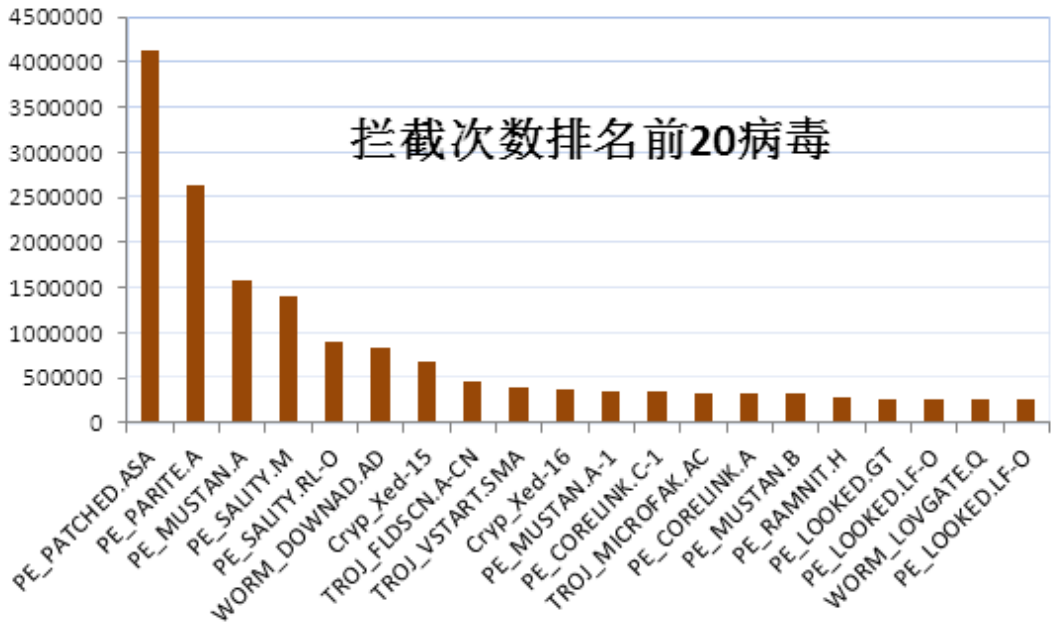
2012 年第 3 季度检测到的病毒种类中 PE 类型病毒感染数量已经超过木马病毒，大约占到总检测数量的 46%。PE 病毒为感染型病毒，该类病毒的特征是将恶意代码插入正常的可执行文件中。感染比率上升可能是因为在上季度多种 PE 病毒同时爆发所导致。PE 病毒通常会感染系统中大多数的可执行文件。一旦被感染，系统中会有大量文件被检测。

蠕虫病毒基本与上季度持平。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。第 3 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。

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) ,本报告中所有数据仅针对中国地区。

2012 年第 3 季度病毒拦截情况分析



2012 第 3 季度中国区拦截次数排名前 20 病毒

上图显示了 2012 年第 3 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。

2012 年第 3 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 410 万次。远远超过其他病毒。跟上季度相比略有下降。

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：

- 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
  使用前请看 readme:

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) ,本报告中所有数据仅针对中国地区。

http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/AvbTool/readme.txt

本季度 **PE_MUSTAN** 大规模爆发，仅 **PE_MUSTAN.A** 检测次数就达到将近 100 万条。该病毒最早在 2012 年 1 月份左右被发现。通过代码分析可以发现该病毒继承于先前发现的 WORM_MORTO 。

PE_MUSTAN.A

恶意行为：

- 利用远程桌面协议（RDP）3389 端口传播
- 通过解析 C&C server 的 DNS TXT 记录获得加密的恶意文件下载链接
- 会连接到恶意网站下载恶意代码
- 感染所有*.exe 文件
- 会将恶意代码写入注册表，使自己不容易被清除干净从而导致反复感染
- 会使用修改注册表的方式禁用某些安全软件的服务

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) ,本报告中所有数据仅针对中国地区。

感染方式：

- ✧ 该病毒可能通过网络下载
- ✧ 其他恶意软件释放
- ✧ 通过远程桌面传染
- ✧ 通过被感染的文件传染
- ✧ 通过共享文件夹传染

技术细节：

1. 创建互斥量

2. 将代码注入以下进程：
   Lsass.exe
   Svchost.exe

3. 添加自启动项：
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
   Services\wmicucltsvc
   ImagePath = "%System%\wmicuclt.exe"

4. 创建以下注册表键值：
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\`
   `Services\wmicucltsvc`
   `HKLM\SYSTEM\Select`
   `v = "{病毒代码}"`
   `HKLM\SYSTEM\Select`
   `p = "{登陆密码}`
   `HKLM\SYSTEM\Select`
   `pu = "{登陆账号} - {登陆密码}"`
   `HKLM\SYSTEM\Select`
   `ext = "{从 C&C server 获得的插件代码}"`
   `HKLM\SYSTEM\Select`
   `plg = "{从 C&C server 获得的插件代码}"`
   `HKLM\SYSTEM\Select`
   `rmt = "{执行的日期}"`
   `HKLM\SYSTEM\Select`
   `{受害者的 ip} = {执行的日期}`

5. 病毒会猜解以下账号密码：

   账号：

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) ,本报告中所有数据仅针对中国地区。

administrator
admin
user
test

密码表：

1234	88888888	1314521	asdf	11111
123	2222	00000000	qwer	232323
123456	2011	110110	yxcv	4444
admin	121212	100200	zxcv	rock
password	112233	147258	home	xxxx
1	zxcvbnm	123123123	xxx	aaaa
12345	999999	7758258	owner	4128
12345678	31415926	woaiwojia	login	3333
1qaz2wsx	12344321	147258369	Login	5555
user	12	aaaaaa	pwd	777777
server	1111111	222222	love	6666
111111	!@#$%^&*	20070315	mypc	admin!@#
test	!@#$%	555555	mypc123	P@ssW0rd
111	!@#$	112358	pw123	pass123
%u%	super	211314	mypass	user123
123456789	qazwsx	201314	mypass123	testtest
123321	computer	198612	pussy	123!@#
1111	abcd	333333	696969	pass123456
123123	987654321	Admin	mustang	soft
abc123	987654	Password	baseball	mima
888888	789456	54321	master	passpass
0	77777777	passwd	michael	1pass
pass	7777777	database	football	123pass
a	7777	oracle	shadow	pass123word456
654321	7	sybase	monkey	!password!
000000	4321	123qwe	fuckme	password1
aaa	159357	Internet	6969	!@#$%^&*()
1234567890	1314520	123asd	jordan	123456!@#
1234567	1313	ihavenopass	harley	!@#123456
%u%12	11223344	godblessyou	ranger	!@#123
abcd1234	root	enable	iwantu	qwertyuiop
1234qwer	3	xp	jennifer	asdfghjkl
admin123	22222222	2002	hunter	oapass
520520	1QAZ	2003	fuck	oapassword
369	111222	2600	2000	pass0rd
1q2w3e	%u%123456	110	batman	pa$$0rd
168168	%u%111111	123abc	trustno1	adm1n
!@#$%^	princess	007	thomas	admini
666666	dragon	alpha	tigger	admin!@#123

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) ,本报告中所有数据仅针对中国地区。

letmein	PASSWORD	patrick	robert	adminadmin
%u%1	qwerty	pat	access	windows
abc	5201314	administrator	killer	windows2003
520	7758521	sex	131313	windows2000
2010	5211314	god	xxxxxxxx	windowsxp
2012	521521	foobar	xxxxxx	qazwsx123456
secret	123654	test123	1212	123qaz456wsx
rockyou	woaini	temp	5150	1233211234567
iloveyou	11111111	temp123	zzzzzz	mypassword
%u%1234	3	win	2112	tasklist
%u%123	1415926	pc	xxxxx	fangyou
				sa

解决方法：

1． 升级防毒产品到最新病毒码并进行全盘扫描

2． 没有安装防毒产品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

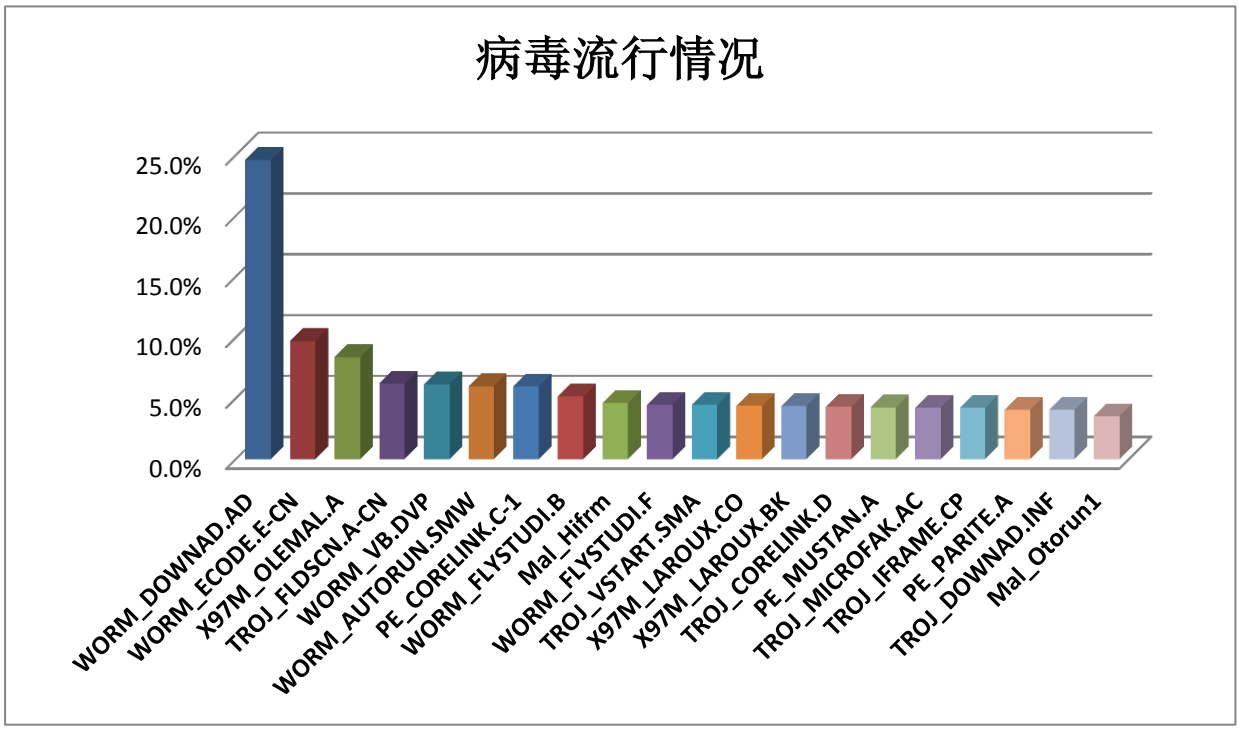
64 位 windows 操作系统请使用：
http://support.trendmicro.com.cn/Anti-Virus/Clean-Tool/ATTK_CN/supportcustomizedpackage_64.exe
（为了避免.exe 文件在下载到系统时被感染，请在下载时将该工具保存为.com）

防护方法：

1. 不要使用以上密码表中的账号密码
2. 尽量不要多台电脑使用相同密码
3. 使用 China RTL AVBtool 进行免疫
   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

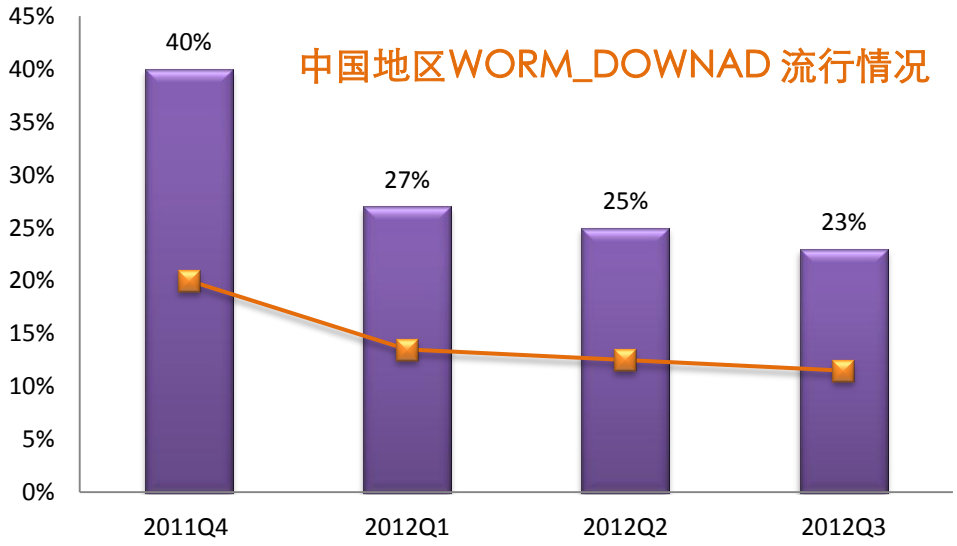
关于该病毒以及相关病毒的详细信息请参阅：
http://about-threats.trendmicro.com/us/malware/pe_mustan.a
http://about-threats.trendmicro.com/us/malware/pe_mustan.a-1
http://about-threats.trendmicro.com/us/malware/pe_mustan.b

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) ,本报告中所有数据仅针对中国地区。



2012 第 3 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**。



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) ,本报告中所有数据仅针对中国地区。

不过相对于去年以及第一，二季度，该病毒的流行程度仍然处于下降，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，第一季度度下降到了 27%左右。而本季度仅有 23%的客户环境中出现过此病毒，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。

另外需要关注的为流行度排名第 7 的 **PE_CORELINK.C-1.**这是一只在 2007 年时非常流行的 PE 感染型病毒。但是在近期有感染用户增加，死灰复燃的趋势.

PE_CORELINK.C-1

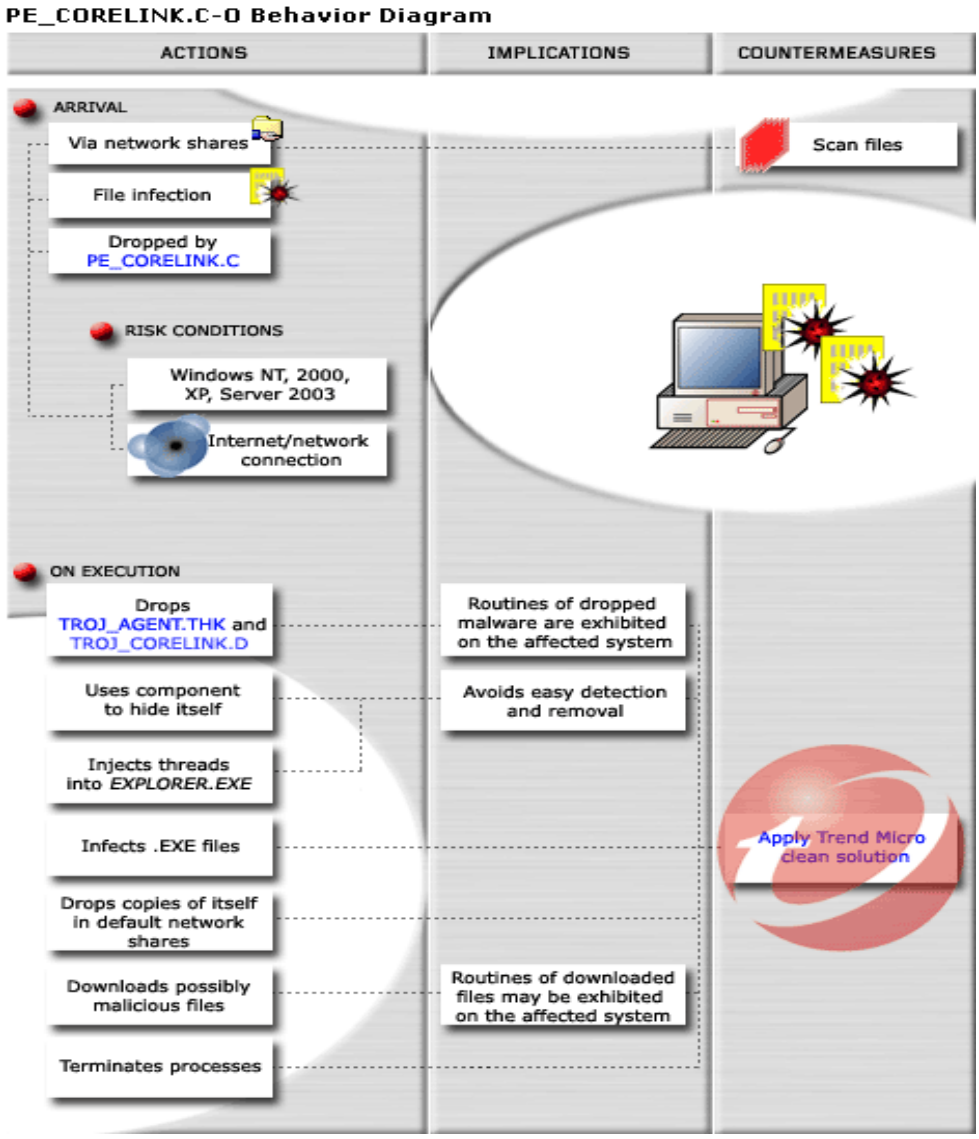
恶意行为：

- 该病毒会感染电脑中除某些特定目录以外的 exe 文件
- 该病毒会通过网络共享释放自身
- 该病毒会下载其他恶意文件
- 该病毒释放 rootkit 隐藏自身
- 该病毒会终止某些进程

感染途径：

1．通过网络共享传播
2．通过被感染的文件传播
3．通过可移动存储设备传播

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) ,本报告中所有数据仅针对中国地区。



技术细节：

1. 该病毒在系统的 windows 目录中释放 linkinfo.dll,利用 explorer.exe 调用 dll 的优先顺序使得自己被调用
2. 该病毒在释放以下驱动程序，起到 rootkit 作用,使 linkinfo.dll 以及相关的注册表键值被隐藏：

   %System%\drivers\IsDrv122.sys

   %System%\drivers\nvmini.sys
3. 添加以下注册表键值：

   `HKEY\LOCAL MACHINE\SYSTEM\CurrentControlset\Services\nvmini`
4. 通过网络共享，向可访问目录中释放 setup.exe (该文件为其自身的复制)

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) ,本报告中所有数据仅针对中国地区。

解决方法：

1．升级防毒产品到最新病毒码并进行全盘扫描

2．没有安装防毒产品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. 尽量避免网络中多台电脑使用相同的管理员账号密码
2. 使用 officescan 在 c:\windows 文件夹中爆发阻止 linkinfo.dll
3. 在注册表
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs
   添加
   REG_SZ linkinfo.dll
4. 安装防病毒软件并将病毒码更新至最新

X97M_OLEMAL.A 在本季度仍然流行程度排名靠前。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

防护方法：

鉴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：

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) ,本报告中所有数据仅针对中国地区。

目前趋势科技中国区病毒码 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/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

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

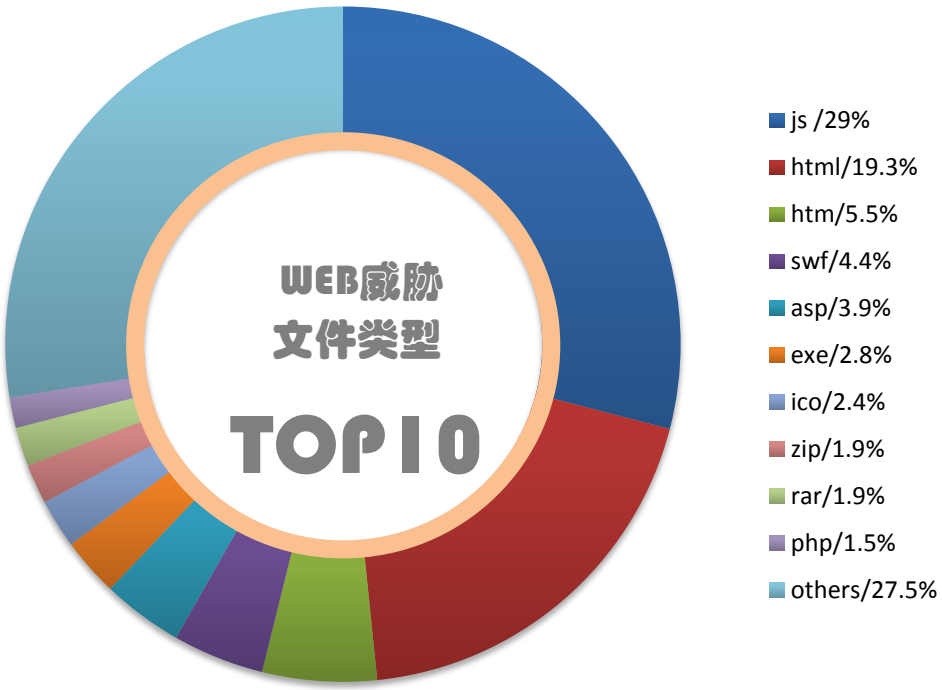
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2012 年第 3 季度 WEB 安全威胁情况

2012 年第 3 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 **29%**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而进行其他恶意行为。

.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。



2012 第 3 季度中国地区 web 威胁文件类型

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) ,本报告中所有数据仅针对中国地区。

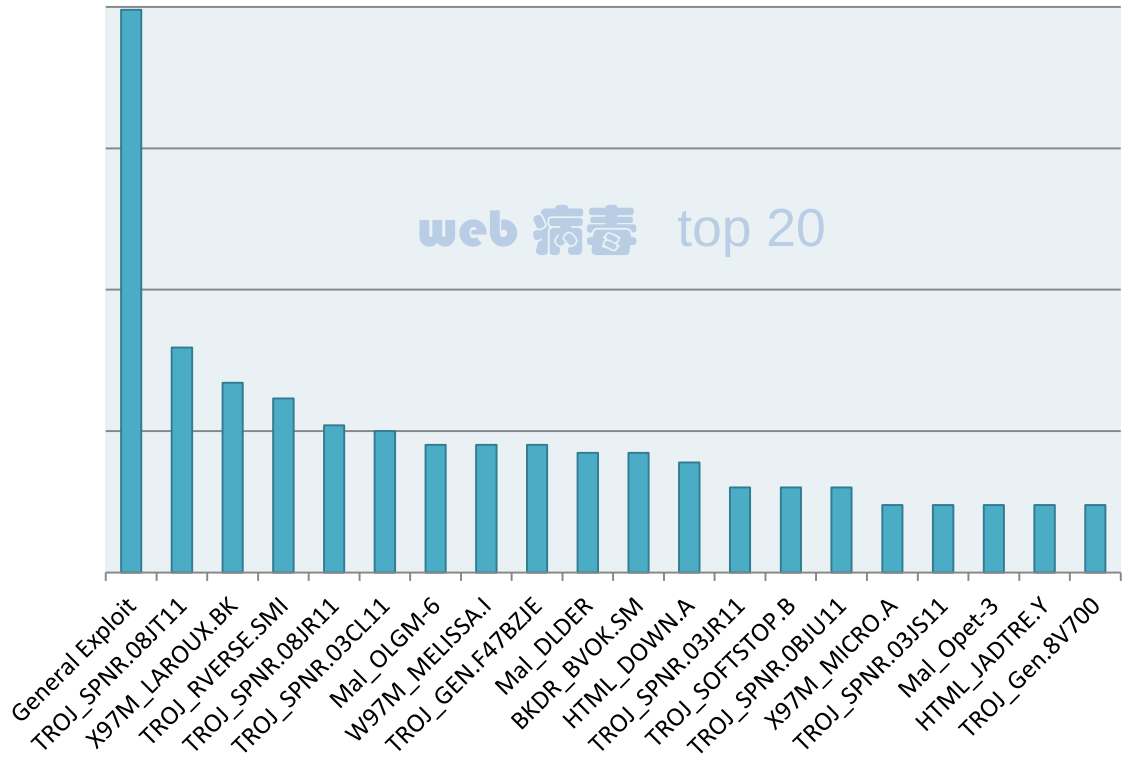
2012 年第 3 季度 TOP10 恶意 URL

TOP10 恶意URL		
恶意URL	病毒检测	描述
64.32.14.203:80/paul/paul.exe	TSPY_ZBOT.SMIG	网站直接或间接帮助传播恶意软件或恶意代码
trafficconverter.biz:80/4vir/antispyware/loadadv.exe	worm_downad	网站直接或间接帮助传播恶意软件或恶意代码
trafficconverter.biz:80/	worm_downad	网站直接或间接帮助传播恶意软件或恶意代码
38jjj.qvod790.com:80/kk55.exe	TROJ_SMALL.SMOK	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　网站直接或间接帮助传播恶意软件或恶意代码
d4.pc6.com:80/xy1/dnpms.zip		网站直接或间接帮助传播恶意软件或恶意代码
61.201.27.6:80/vct/vel19.rar	WORM_RIPLIP.SMI,TROJ_GEN.R4AC1JU,TROJ_SPNR.08JT11	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　网站直接或间接帮助传播恶意软件或恶意代码
baidu.9486.com		劫持google搜索弹出恶意网站
e.ppift.net	PE_MUSTAN	网站直接或间接帮助传播恶意软件或恶意代码
d.jfrns.in	PE_MUSTAN	网站直接或间接帮助传播恶意软件或恶意代码
fd1.ppiplg.net	PE_MUSTAN	网站直接或间接帮助传播恶意软件或恶意代码

2012 第 3 季度中国地区已被 wrs 阻止的恶意 url 排名

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) ,本报告中所有数据仅针对中国地区。

2012 年第 3 季度 WEB 威胁病毒类型分析



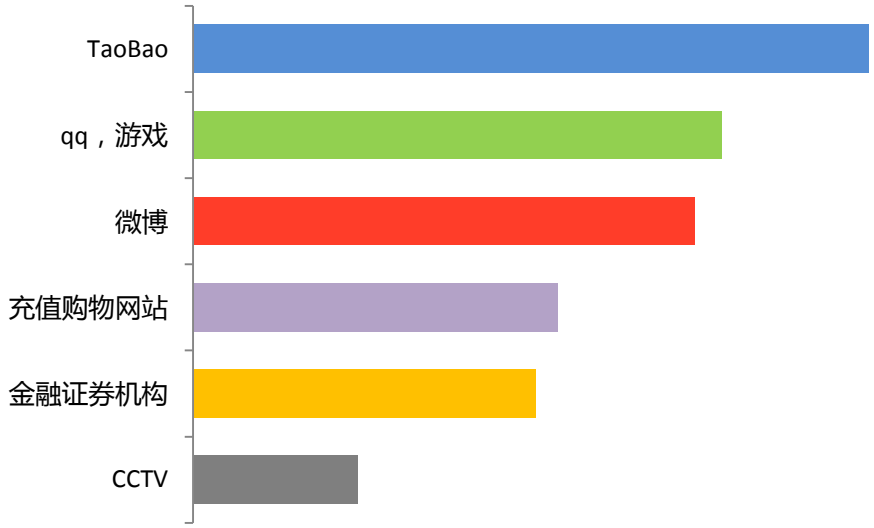
通过对拦截的 Web 威胁进行分析，我们发现。约有 68.8%的威胁来自于 General exploit（针对漏洞的通用检测）。

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。

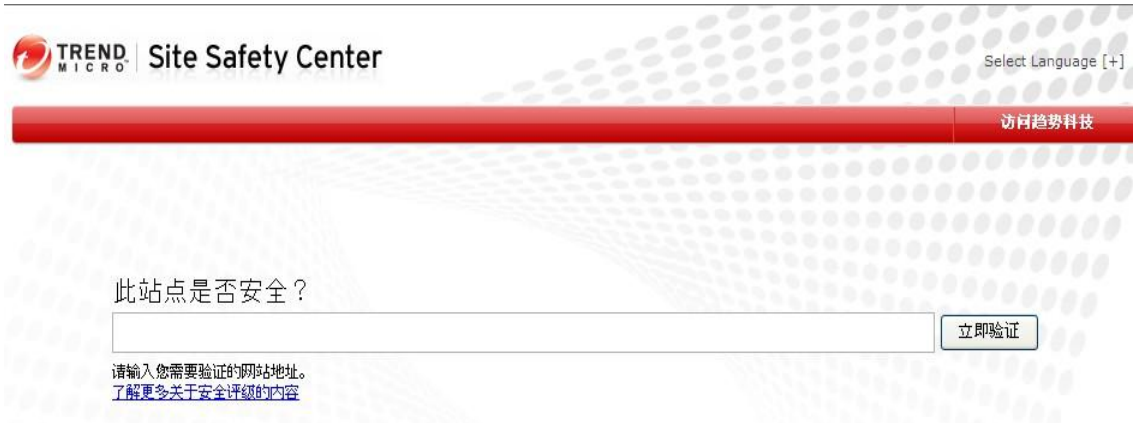
本报告数据来自趋势科技智能防护网(SPN)以及趋势科技 TMES 监控中心(MOC) ,本报告中所有数据仅针对中国地区。

2012 年第 3 季度 WEB 威胁钓鱼网站仿冒对象分析



从第 3 季度趋势科技捕获到的钓鱼网站数据来看，淘宝为钓鱼网站最喜欢仿冒的对象。
一些游戏的充值网站也是钓鱼网站制作者的目标。
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。

另外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



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) ,本报告中所有数据仅针对中国地区。

2012 年第 3 季度最新安全威胁信息

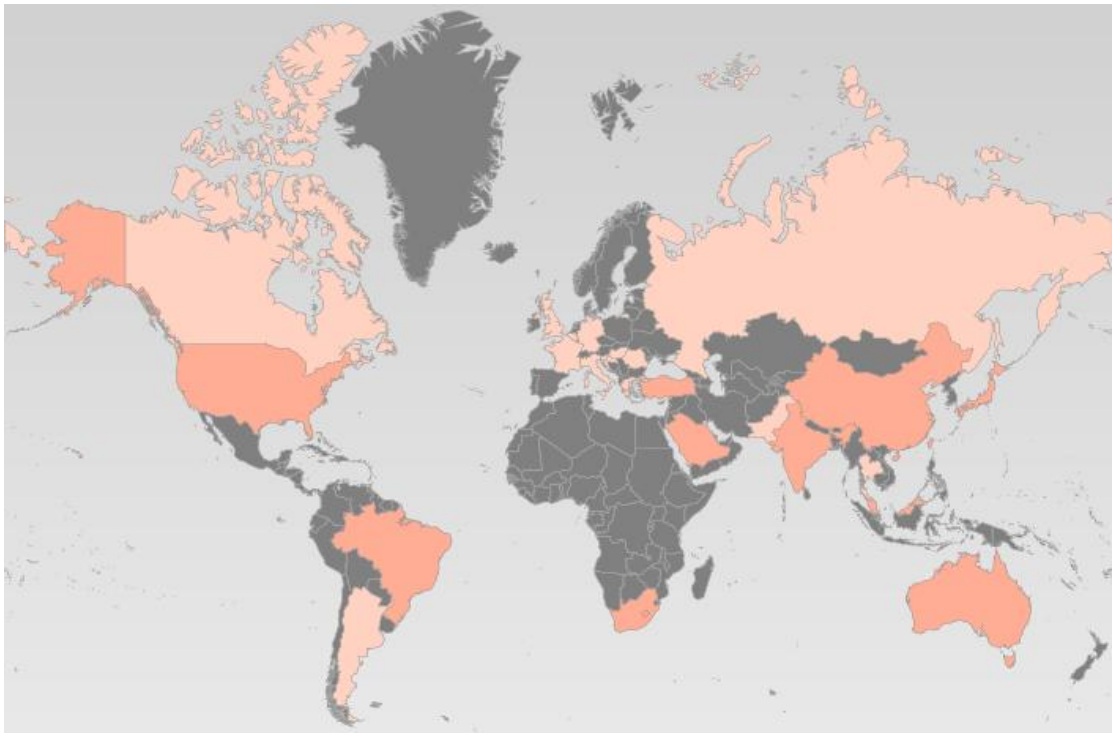
2012.8 首个 Linux、Mac OS X 的跨平台病毒被发现

日前，国外研究人员发现了一种只在 Linux 和 Mac OS X 上存在的木马，当计算机被入侵之后，该木马会在机器上安装 Wirenet-1 键盘记录软件，捕获用户输入的密码和敏感信息。包括 Opera、Firefox、Chrome 浏览器提交的信息，一些 app 存储的信息，以及 Email、Web 组件和聊天应用程序的密码。该恶意软件收集到数据之后会将该数据传送到荷兰一台服务器上。

跨平台的病毒非常罕见，但并非没有先例。其中一个著名的例子包括最近的 Crisis 和 super-worm。随着 1995 年 JAVA 语言的诞生，跨平台成为热点，“一次编译，跨平台运行”的“跨平台”概念成为可能。脱离平台限制正逐渐成为应用开发的趋势，而计算机病毒也同样不会放弃这样的机遇。因此可以预言，病毒也会进入真正的跨平台时代，并成为未来病毒的发展趋势。

相关链接：
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。



近期出现 PE_MUSTAN 的新变种，目前趋势科技检测名为 (Cryp_Xed-15 、

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) ,本报告中所有数据仅针对中国地区。

Cryp_Xed-16).(之后可能会被更名为 PE__MUSTAN.B)

该 PE 病毒是由 china RTL 之前公布过的 WORM_MORTO 病毒演变而来,并且具有感染可执行文件的能力

此病毒主要行为如下：

利用远程桌面协议（RDP）3389 端口传播
会连接到恶意网站下载恶意代码
感染所有*.exe 文件
会将恶意代码写入注册表，使自己不容易被清除干净从而导致反复感染
会使用修改注册表的方式禁用某些安全软件的服务

相关链接：
http://security.ctocio.com.cn/87/12438587.shtml

2012.10 趋势科技自身安全研究者 Rik Ferguson 对 Windows 8 安全问题的概述

微软在 win8 的安全性方面已经取得一些长足的进步。尤其是在数据安全、反恶意软件和用户认证等关键领域的一些改进大大提升了用户体验。

http://countermeasures.trendmicro.eu/windows-8-security-overview/

2012.9 新的 IE 零日漏洞

9 月趋势科技发现一个新的利用 IE 零日漏洞的病毒，趋势科技将它检测为 HTML_EXPDROP.II
该漏洞所影响的 IE 浏览器版本为 IE7,8,9.
该病毒会释放一个恶意的.swf 文件，该文件被趋势科技检测为 BKDR_POISON.BMN.

相关链接：
http://blog.trendmicro.com/trendlabs-security-intelligence/new-ie-zero-day-exploit-leads-to-poisonivy/

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) ,本报告中所有数据仅针对中国地区。