中国地区第四季度
网络安全威胁报告

2011/1

目录

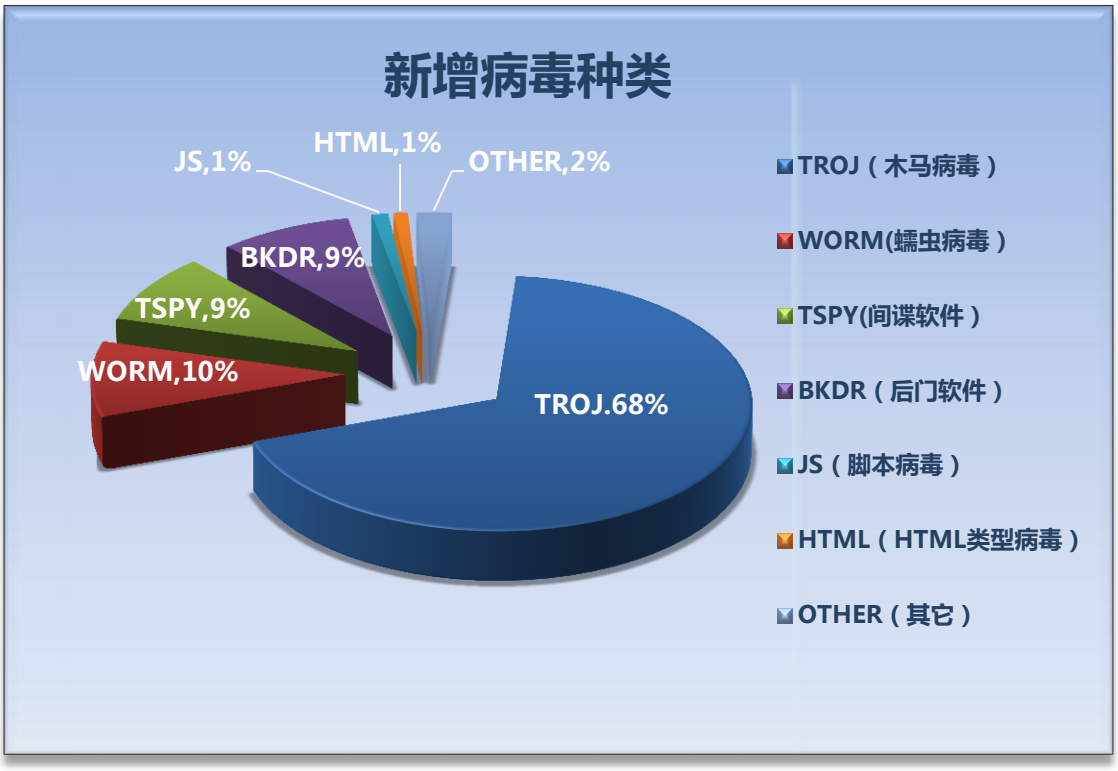
2010 年第 4 季度安全威胁

本季安全警示：
网络共享传播与混合型病毒攻击.

2010 年第 4 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 **5.6** 万种。截止 2010.12.31 日中国区传统病毒码 7.738.60 可检测病毒数量已超过 300 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。
  蠕虫类型病毒（WORM）所占比例排名比第三季度有所上升，这可能与网络共享以及可移动存储设备传播的病毒数量增加有关。另外一些蠕虫病毒变种速度加快，也是新增病毒种数上升的原因。



2010 第 4 季度中国地区新增病毒类型分布饼图

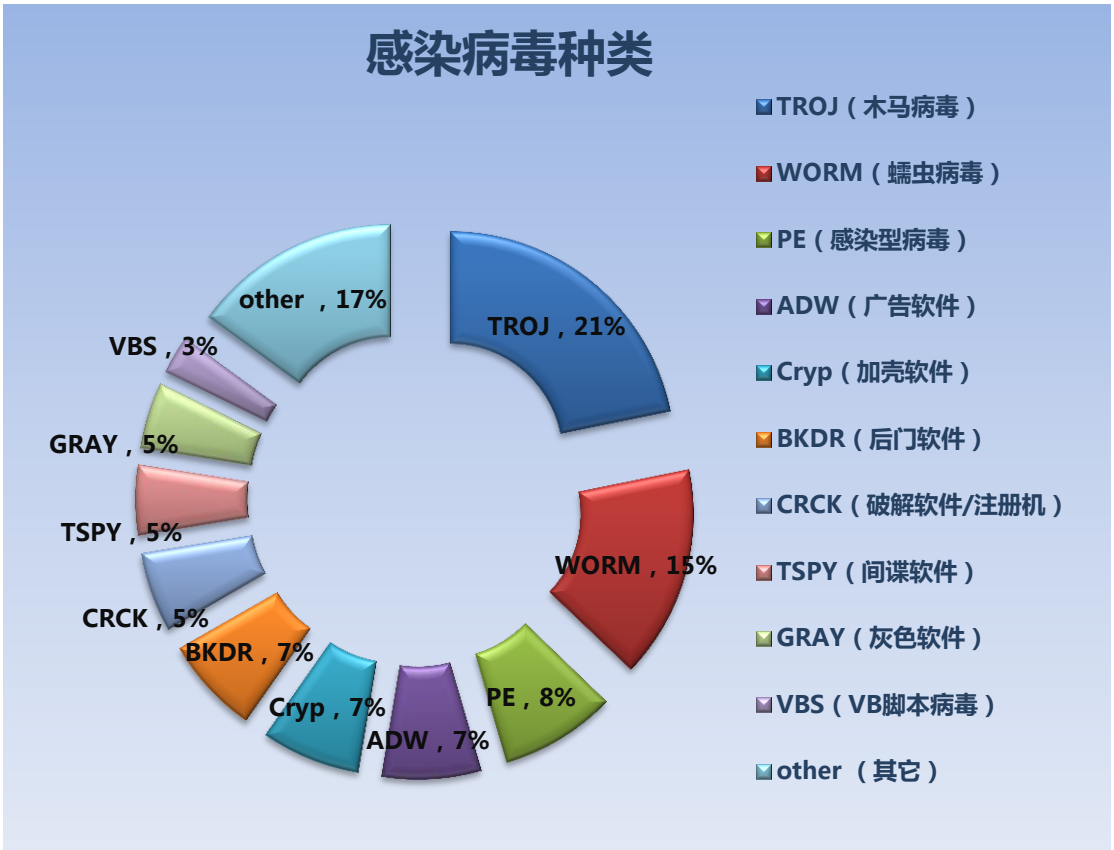
- 本季度趋势科技在中国地区拦截到新的恶意 URL 地址以及相关恶意文件约 **29.3** 万个。比上季度增加了近一倍。

其中通过 Web 传播的恶意程序中，约有 **27%**为 JS（脚本类型文件）所占比例与上季度持平。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。

另外 .swf 类型恶意程序，在本季度以及上季度都持续占有较大的比例。此文件类型的病毒，通常是恶意代码编写者利用 flash 的漏洞，将恶意代码插入 swf 文件中。之后将带有恶意代码的 swf 文件注入网站页面。用户访问网站播放 flash 即会导致感染病毒。这也是很多电脑使用者在不知不觉中就感染了病毒的原因之一。

2010 第 4 季度 中国地区 web 威胁文件类型

- 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 **5601** 万次。



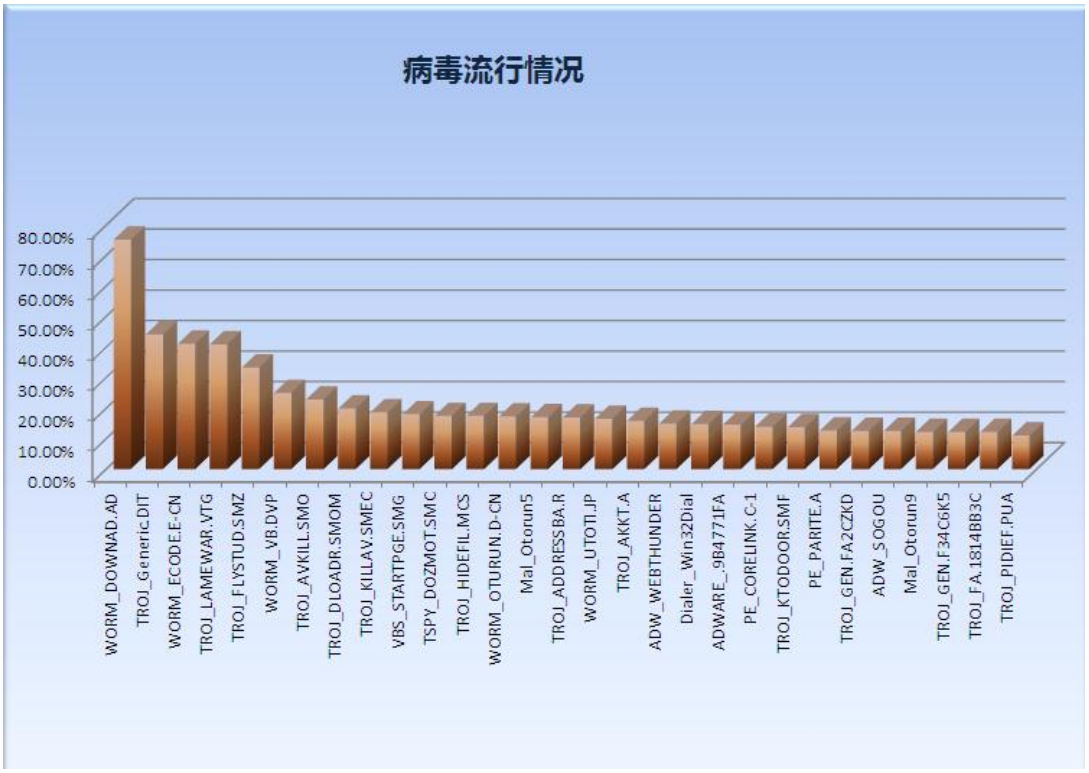
2010 第 4 季度 中国地区各类型病毒感染数量比例图

其中感染最多的病毒类型是木马，达到所有检测到的病毒类型数量的 **21%**。蠕虫病毒感染数量以及所占感染病毒总数的比例比第 3 季度明显上升，达到了 **15%**。在第 4 季度，蠕虫病毒大约有 **565** 万次检测。

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

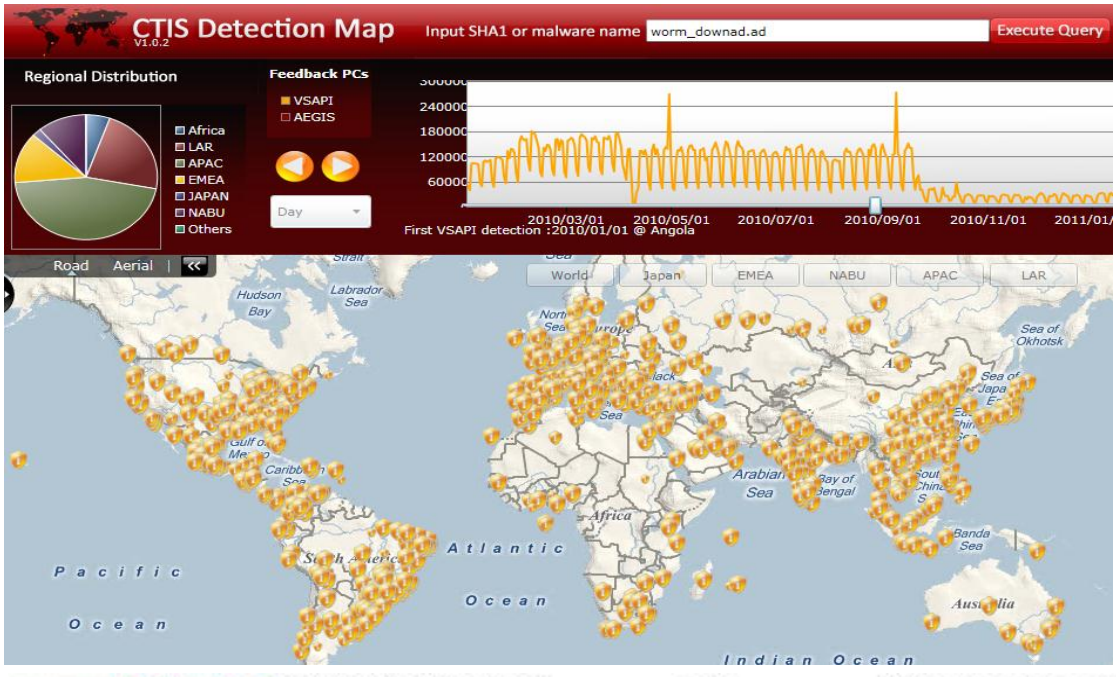
能够感染可执行文件的 PE 病毒依旧位居第三。一些没有母体的 PE 病毒，本身不具备主动复制自身到网络内其他机器的传播特性。此类 PE 病毒的爆发往往伴随着网络中严重的蠕虫或者木马问题。

2010 年第 4 季度最流行病毒分析



2010 第 4 季度 中国地区病毒流行度排名

在第四季度感染客户数量最多的病毒依旧是 **worm_downad.ad**(又名:Conficker,飞客病毒)。本季大约超过 **70%**的客户公司网络内部，曾经或者仍然存在有 **worm_downad** 病毒。



从全球 **worm_downad** 病毒的感染情况来看，该病毒在第 4 季度初期全球范围内数量大幅度减少。但是亚太地区仍然是该病毒的重灾区。第四季度全球约 50% **worm_downad** 病毒在亚太地区被检测。

中国地区 **worm_downad** 虽然感染范围依然很广，但已明显开始走向衰减。第三季度约 40%的客户感染此病毒，检测次数达到 **50** 多万次。在本季此病毒检测数量下降到了 40 万次左右。此项数据说明计算机被重复感染或是感染后无法清除的事件正在减少。越来越多的用户采用了正确的防护与处理方法，使该病毒逐渐得以控制。

流行程度排名第二位的 TROJ_GENERIC.DIT，是能够窃取用户计算机中账号密码信息的木马。他可能是用户在访问恶意网站时无意间下载，或是由其他恶意软件释放。该病毒试图窃取被感染用户登录某些银行或金融相关网站时使用的信息。他会连接到某恶意网站将信息发送。目前趋势科技最新版本的病毒码及扫描引擎可以成功处理此病毒。并且相关恶意网站都已加入 WRS。

关于该病毒的详细信息可参考：

http://about-threats.trendmicro.com/malware.aspx?language=cn&name=TROJ_GENERIC.DIT

本季最需要关注的流行病毒为检测名为：**TROJ_HIDEFIL.MCS, TROJ_FLYSTUD.SMZ，TROJ_LAMEWAR.VTG ,TROJ_AVKILL.SMO ,TROJ_KILLAV.SMEC** 的系列病毒。它们又被称为**”高清视频”**病毒,或**“文件夹”**病毒

该病毒在目前非常流行，并且具有爆发趋势。其最主要的特征是：被该病毒感染的机器，会自动向网络共享目录中释放名称为{高清视频}.exe 的文件夹图标病毒文件。

通常情况下，首先被感染的即是网络环境中的文件服务器。而由于文件服务器是公司内部进行共享访问频率较高的特殊服务器，更加速了病毒的扩散。

该病毒不仅具有文件夹病毒特征，还带有 AV 终结者病毒特性，对感染电脑进行映像劫持。使其无法使用某些安全软件，注册表等

该病毒不但变种速度很快，并且带有自我保护机制。一旦网络中爆发，处理工作将变得极为困难。

TROJ_HIDEFIL.MCS （又名：”高清视频” 病毒）

”高清视频” 病毒是一种利用网络共享传播的混合型病毒。他具有蠕虫，木马，间谍软件的特性。又同时具有文件夹病毒以及 AV 终结者病毒的病毒特征某些变种还带有 worm_downad 病毒特性。该病毒在中国地区从 2010 年第四季度中下旬开始流行。

病毒分析：

该病毒具有以下行为：

- 在桌面释放包括 IE 浏览器，免费电影 C，改变你的一生，淘宝购物四个快捷方式。
- 在以下目录释放病毒文件：

  C:\ 随机字母名称的 bmp gif jpg txt dos 类型文件
  C:\ VSPS\VSPS.exe
  C:\ Program Files\Common Files\BOSC.dll
  C:\ Documents and Settings\All Users\「开始」菜单\程序\启动 buknnvfgwg.exe
  C:\Windows\system32 目录下创建两个随机字母的文件夹，分别放有 explorer.exe 和 smss.exe
  某些变种会修改 QQ 安装目录中的 Tasktray.dll 文件，
  并在 C:\windows\system32\drivers 目录中释放 kpscc.sys

  遍历并向每个磁盘根目录添加 my documents.exe 文件夹图标文件

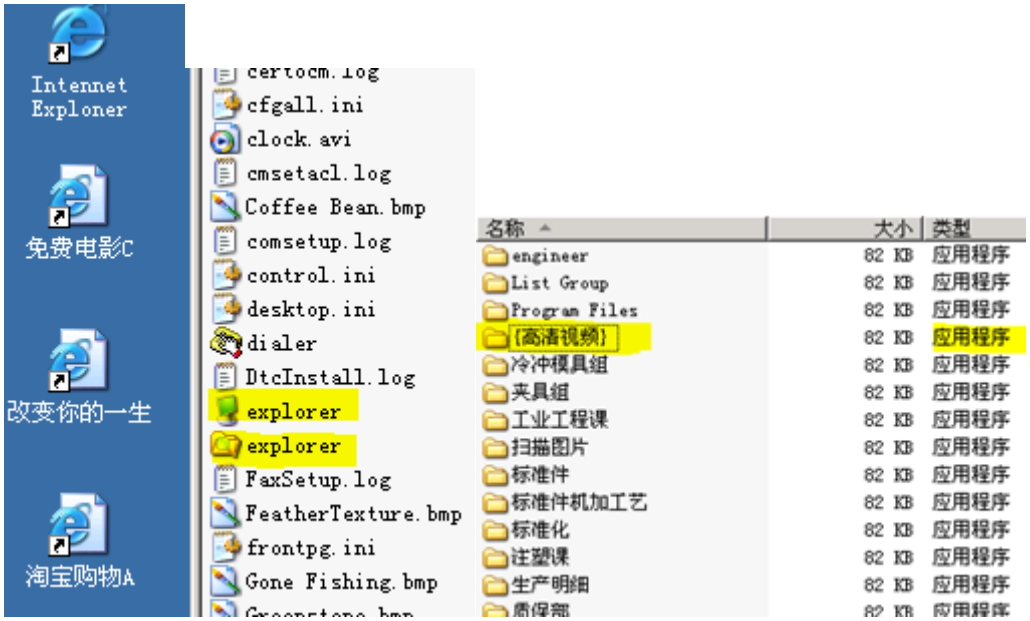
  向网络中可访问的共享目录中释放{高清视频}.exe，并将该目录中所有文件夹添加系统和隐藏属性。释放与文件夹同名 exe 文件夹图标文件文件

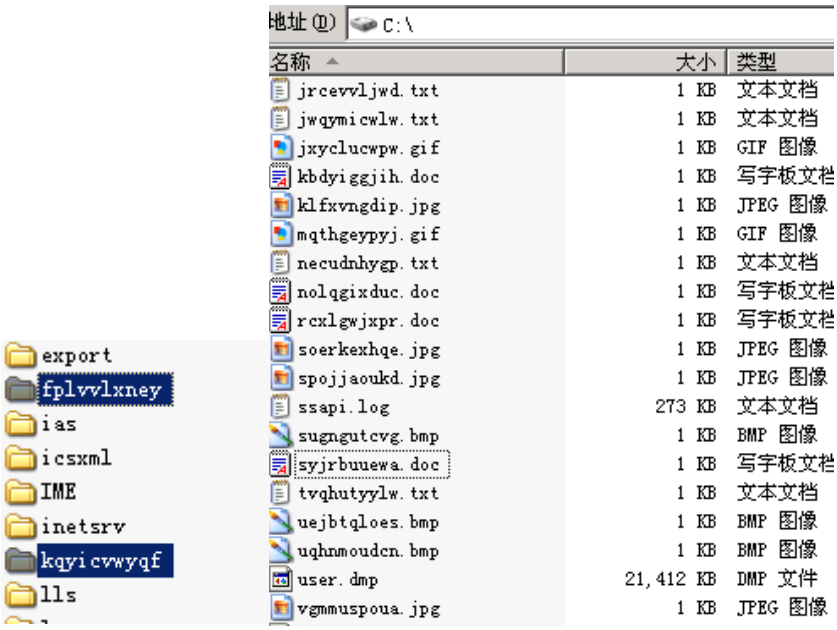
- 锁定注册表，使其无法打开
- 修改注册表使感染机器无法查看隐藏文件，无法显示.exe 文件后缀
  某些变种会修改注册表 HKEY_CURRENT_USER 键值权限，导致使用者无法对注册表先进行修复
- 在注册表中添加映像劫持导致以下程序无法运行

360rpt.exe	mcconsol.exe	irsetup.exe	rstrui.exe
360Safe.exe	mmqczj.exe	isPwdSvc.exe	runiep.exe
360safebox.exe	mmsk.exe	jisu.exe	safeboxTray.exe
360sd.exe	mngreg32.exe	kabaload.exe	safelive.exe
360sdrun.exe	Navapsvc.exe	KaScrScn.SCR	scan32.exe
360tray.exe	Navapw32.exe	KASMain.exe	ScanFrm.exe
799d.exe	NAVSetup.exe	KASTask.exe	ScanU3.exe
adam.exe	niu.exe	KAV32.exe	SDGames.exe
AgentSvr.exe	nod32.exe	KAVDX.exe	SelfUpdate.exe
AntiU.exe	nod32krn.exe	KAVPF.exe	servet.exe
AoYun.exe	nod32kui.exe	KAVPFW.exe	setup.exe
appdllman.exe	NPFMntor.exe	KAVSetup.exe	setup32.dll

AppSvc32.exe	pagefile.exe	kavstart.exe	sevinst.exe
ArSwp.exe	pagefile.pif	kernelwind32.exe	shcfg32.exe
ArSwp2.exe	pfserver.exe	KISLnchr.exe	SmartUp.exe
ArSwp3.exe	PFW.exe	kissvc.exe	sos.exe
AST.exe	PFWLiveUpdate.exe	KMailMon.exe	SREng.EXE
atpup.exe	photohse.EXE	KMFilter.exe	SREngPS.EXE
auto.exe	printhse.EXE	knsd.exe	stormii.exe
AutoRun.exe	prwin8.EXE	knsdave.exe	sxgame.exe
autoruns.exe	ps80.EXE	knsdtray.exe	symlcsvc.exe
av.exe	psdmt.exe	KPFW32.exe	SysSafe.exe
AvastU3.exe	qfinder.EXE	KPFW32X.exe	tmp.exe
avconsol.exe	qheart.exe	KPfwSvc.exe	TNT.Exe
avgrssvc.exe	QHSET.exe	KRegEx.exe	TrojanDetector.exe
AvMonitor.exe	qpw.EXE	KRepair.com	Trojanwall.exe
avp.com	QQDoctor.exe	KsLoader.exe	TrojDie.kxp
avp.exe	QQDoctorMain.exe	KSWebShield.exe	TxoMoU.Exe
AvU3Launcher.exe	QQDoctorRtp.exe	KVCenter.kxp	ua80.EXE
CCenter.exe	QQKav.exe	KvDetect.exe	UFO.exe
ccSvcHst.exe	QQPCMgr.exe	KvfwMcl.exe	UIHost.exe
cqw32.exe	QQPCRTP.exe	KVMonXP.kxp	UmxAgent.exe
cross.exe	QQPCSmashFile.exe	KVMonXP_1.kxp	UmxAttachment.exe
Discovery.exe	QQPCTray.exe	kvol.exe	UmxCfg.exe
DllNXOptions	QQSC.exe	kvolself.exe	UmxFwHlp.exe
DSMain.exe	qsetup.exe	KvReport.kxp	UmxPol.exe
EGHOST.exe	Ras.exe	KVScan.kxp	upiea.exe
enc98.EXE	Rav.exe	KVSrvXP.exe	UpLive.exe
FileDsty.exe	ravcopy.exe	KVStub.kxp	USBCleaner.exe
filmst.exe	RavMon.exe	kvupload.exe	vsstat.exe
front.exe	RavMonD.exe	kvwsc.exe	wbapp.exe
FTCleanerShell.exe	RavStub.exe	KvXP.kxp	webscanx.exe
FYFireWall.exe	RavTask.exe	KvXP_1.kxp	WoptiClean.exe
ghost.exe	RegClean.exe	KWatch.exe	wpwin8.EXE
guangd.exe	rfwcfg.exe	KWatch9x.exe	Wsyscheck.exe
HijackThis.exe	rfwmain.exe	KWatchX.exe	XDelBox.exe
IceSword.exe	rfwProxy.exe	KWSMain.exe	XP.exe
install.exe	rfwsrv.exe	kwstray.exe	xwsetup.EXE
iparmo.exe	RsAgent.exe	KWSUpd.exe	zhudongfangyu.exe
Iparmor.exe	Rsaupd.exe	loaddll.exe	zjb.exe
	rsnetsvr.exe	logogo.exe	zxsweep.exe
	RsTray.exe	MagicSet.exe	_INSTPGM.EXE
			~.exe

- 其释放的 explorer.exe 及 smss.exe 互相守护，发现终止后启动。
- 修改 IE 主页为 hxxp://www.sfc007.com/XXX 的钓鱼网站。
- 某些变种会利用其修改的 QQ 组件 Tasktray.dll 劫持 IE 浏览器，当 IE 首页被设置为空白页面（/blank）时强行使其跳转至其相关恶意网站





小贴士：

以上为病毒现象的一些截图。通过这些截图我们可以发现：即使病毒隐藏了.exe 后缀，系统无法显示隐藏文件。但是当我们在查看文件夹内容时，显示文件夹内容选择”详细信息”视图。会发现所有文件夹图标的文件，文件类型却为应用程序。如果我们不去执行这些服务器上伪装成文件夹的病毒文件。则感染此病毒的概率将有极大的减少

防护方案：

由于该文件夹病毒变种速度极快。应对此病毒如果采用一些防护的动作，将比仅仅等待病毒码的更新会更加安全。

- 禁止或有条件阻止对共享文件夹（特别是文件服务器的共享文件夹）直接写入.ExE
- 阻止可移动存储设备的自动播放功能

以上防护措施均可以通过趋势科技防毒墙网络版，或其他安全产品实现。

解决方案：

- 及时更新安全产品的病毒码
- 如发现网络中有该病毒爆发现象，应优先解决感染源点脑
- 趋势科技病毒实验室提供专杀工具可清理此病毒，如有需要请与趋势科技技术支持部门联络

2010 年第 4 季度最新安全威胁信息

- **2010 年第四季度，趋势科技中国区病毒实验室连续收到数起 BKDR_BIZOME.SMD 病毒爆发的案件。**

该病毒通过在局域网内查找 Radmin server，并使用自身携带的密码表进行密码攻击。
一旦 Radmin server 密码被攻破，即获得了该机器的控制权

该病毒使用 SSL 进行数据加密上传数据，并且因为利用了 Radmin server 使之具有远程登录控制的功能

该病毒攻击 IBM4758 系列密码处理器

该病毒会通过命令行 ipz.exe /i 在感染机器中添加以下服务
IPZ
IntelligentP2P Zombie

并将 ipz.tmp 文件释放到 \windows\systm32 目录中并将 tmp 文件转换成 ipz.exe 进行安装。

并在运行过程中生成日志文件，记录系统相关信息。

该病毒的密码表保存在其自身携带的数据库 ipz-db.bin 中，该数据库中还保存其他相关信息

由于 Radmin 通常为公司中网络管理所使用的正常工具，所以网络管理员往往无法发现它正是病毒传播的渠道。以至于在病毒出现的初期未能采取正确的处理措施而使病毒状况变得严重。

在几起病毒爆发事件中我们还发现感染该病毒的用户网络中均有严重的 **PE_VIRUX.A** 病毒现象。由于 **PE_VIRUX.A** 病毒没有复制自身的传播能力，我们不排除该病毒会携带 **PE_VIRUX.A** 病毒在网络中散播，导致 **PE_VIRUX.A** 病毒爆发。

往往 **PE_VIRUX.A** 病毒的爆发会让网络管理员更加头疼。

以下为趋势科技中国区病毒实验室目前截获的 BKDR_BIZOME.SMD 所携带的密码表。如果您正在使用 Radmin 工具，并且 radmin server 的管理员账号密码又恰巧在此密码表内。则您的系统很有可能会被该病毒入侵，请及时将 Radmin server 管理员账号密码加强，以防止该病毒的侵害。

账户：

1	Administrator
admin	User
q	User
123	Billgates
111111	A
123456	Microsoft
Admin	Radmin
administrator	Internet
skynet	Host
login	Computer

密码：

american	supply	missile	987654321	doomsday
internet	imageboard	warhammer	america	fuckyou
1q2w3e	predator	sunlight	windows	qweasd
1q2w3e4r	propeller	children	microsoft	qweasdzxc
1q2w3e4r5t	alien	burning	machine	bender
starcraft	sattelite	hell	trollface	11111111
qwertyui	archer	deathcore	utorrent	aaaaaa
qwertyuiop	thieft	processor	Cannon	aaaaaaaa
metall	stinger	memory	Satan	qwerty
washington	nigger	atmel	Jesus	654321
people	terminator	xlinx	Aerial	callofduty
asdfghjk	police	altera	receiver	rastaman
asdfghjkl	europe	income	transmitter	smoking
ignore	ubuntu	incoming	tranciever	lineage2
gothic	debian	thread	microchip	coolface
horizon	samael	username	grinder	solder
skynet	skywalker	desu	Bullshit	shcool
anchorite	oracle	billgates	emperor	folder
godzilla	suxxxx	brutal	deathstar	happy
aeroplane	lurkmore	minigun	darthvader	happiness
1	keyboard	guitar	thunderbird	stalin
q	mouse	atmosphere	horishima	kremlin
a	cdrom	prototype	Israel	whitehouse
123	harddisk	evangellion	scientology	revolution
1234	display	kamikaze	"brentcorrigan"	war
123456	speaker	youandme	Insane	boeing
12345678	annihilation	freedom	Pretty	emokid

123456789	destroy	zeitgeist	nekoboy	atomic
123123	elimination	hardcore	shadow	nuclear
12341234	domination	unknown	latitude	reactor
12121212	router	secure	longtitude	enigma
121212	motorbike	rocketman	altitude	elephant
password	negative	jetpack	copyright	qazwsx
87654321	positive	fighter	copyleft	qazwsxedc
secret	fallout	superman	deltaplane	topsecret
radmin	kiss	battle	helicopter	lucifer
monkey	music	pilotage	creative	1234567890
qqqqqq	forward	aerodynamics	creator	warcraft
qqqqqqqq	backward	disable	Hippie	overmind
111111	tolerance	enable	Hitler	emoboy
google	youtube	mozilla	wireless	

目前，在保证 Radmin server 不具有弱密码的情况下，趋势科技防毒墙网络版病毒码 7.738.60，扫描引擎既 9.205 即以上版本可以成功查杀此病毒。

BKDR_BIZOME.SMD 中国地区用户感染情况

- **2010.11　Adobe 又一个之前未被披露的零日漏洞已被木马利用释放病毒。该漏洞影响到 Flash Player,Reader,以及 Acrobat.成功利用该漏洞的病毒可能会对电脑造成严重影响，包括失去对系统的控制权限。**

  由于 Adobe 尚未将沙盒功能完整的应用到其产品程序中，建议用户在下载及观看 pdf 和 swf 文件时需要小心谨慎。 另外也需要在第一时间更新 Adobe 发布的相关应用程序补丁。

  利用该漏洞的木马被趋势科技检测为TROJ_PIDIEF.SMQA，该木马释放的病毒文件被检测为TROJ_WISP.SMA.

  http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/76_latest_adobe_zero-day_exploit_leads_to_a_trojan_dropper__110810_.pdf

- **2010.11　Microsoft Internet Explorer 6, 7, 和 8 有漏洞被病毒利用。该漏洞允许远程攻击者通过层叠样式表（CSS）相关的令牌序列和剪辑属性，又称“无效标志引用”问题执行任意代码。**

  “无效标志引用”问题是 Internet Explorer 内使用了一个无效的标志引用。删除对象后，无效标志引用可能在特定情况下被访问。

  利用该漏洞的恶意代码被趋势科技检测为 HTML_BADEY.A

  http://about-threats.trendmicro.com/Vulnerability.aspx?language=us&name=Vulnerability%20in%20Internet%20Explorer%20Could%20Allow%20Remote%20Code%20Execution%20(2458511)

何为零日漏洞

目前“零日漏洞”攻击已经成为了网络安全行业中的热门话题，很多电脑使用者更是“闻之色变”、深恐自己也不幸“中招”，然而究竟何为“零日漏洞”？

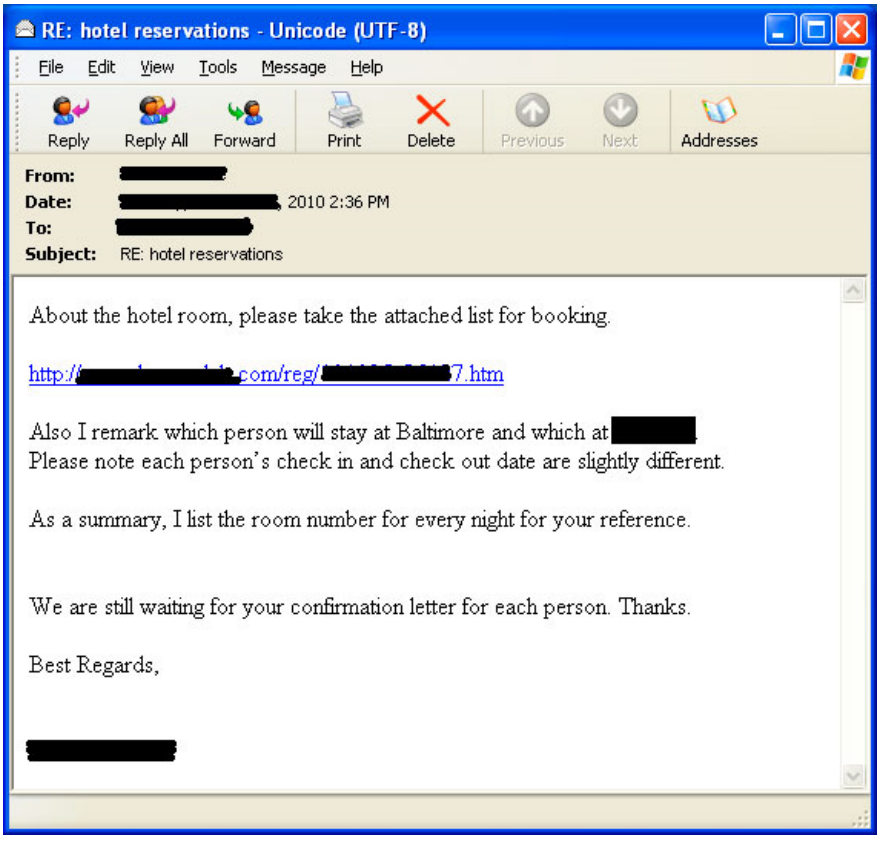
随着现代软件工业的的发展，软件规模不断壮大，软件内部实现的逻辑也变得异常复杂，在中、大型企业中，测试环节在软件生命周期中所占的地位已经上升，有些大型的公司，比如微软、Apple 等，其测试环节(QA)所耗费的资源甚至已经超过了开发。即便如此，不论从理论上还是工程上都没有任何人敢声称可以完全消灭软件中的所有逻辑缺陷。

我们将这类能够引起软件做一些“超出设计范围的事情”的 bug 称为漏洞(Vulnerability)，而那些未被公布或未被修复的漏洞则被称作 “零日（0-Day）漏洞”。

零日漏洞存在于 Windows 系统、Office 软件、做图，视频软件、甚至安全软件中。而恶意程序编写者则会利用这些使用者电脑中这些未被修复漏洞进行攻击，侵入用户系统，从而实现数据破坏和信息窃取等其他恶意目的。

利用 IE 零日漏洞的病毒

黑客通过给某些特定的组织发送一封特别的邮件，比如伪装成合法网站的确认邮件等。邮件中的 URL 可能是黑客之前已经入侵后的合法网站，在合法网站内添加一个恶意的页面文件，然后将邮件中的 URL 定位到此页面，邮件格式如下(图一)：



(图一)

由于特定的漏洞页面只能工作在 **IE 6**、**IE 7** 或 **IE 8** 上，此链接中的网页包含了一个恶意脚本，用来判断当前点击此链接用户使用的系统版本和 IE 版本(图二)。当触发条件满足，此脚本会将用户的页面重新定位到触发此漏洞的页面。当然，用户除了看到一个空白页面外，不会有任何察觉。

```
49
50 if (os=="WINXP" && ie=="IE7")
51 window.location = '[redacted]7b.htm';
52
53 else if (os=="WINXP" && ie=="IE6")
54 window.location = '[redacted]7a.htm';
55
56 else
57 window.location = '[redacted]7c.htm';
```

（图二）

因为浏览器 E 处理特定组合的网页样式标签定义时，存在着内存相关的漏洞，漏洞的触发导致修改内存中会被调用对象的虚表指针。黑客通过精心构造这么一个内存中的数据同时结合多种技术手段，就可能利用此漏洞远程入侵操作系统并在其上随意执行恶意指令代码程序。

防范对策

及时更新补丁，关注厂商发布的临时解决方案

目前，微软公司已经发布了针对该漏洞的安全公告（编号：2458511），但还没有发布相应的漏洞补丁程序。我们建议 Windows 用户在安装该漏洞补丁程序之前，可以采用临时解决方案来避免受到该漏洞的影响，这些措施虽然不能阻止漏洞的触发，但是可以一定程度上阻止该漏洞的恶意利用。

公告网址：http://www.microsoft.com/technet/security/advisory/2458511.mspx

针对上述情况，我们建议广大计算机用户采用如下方法防范：

- 采用用户定义的 CSS（层叠样式表单）覆盖网站 CSS 风格；
- 应用增强的缓解体验工具，下载网址: http://go.microsoft.com/fwlink/?LinkID=200220&clcid=0x409；
- 启用浏览器 IE 的 DEP 功能，即数据执行保护功能，方法如下：

方法 1. 下载安装微软提供的开启 DEP 补丁
http://download.microsoft.com/download/C/A/D/CAD9DFDF-AF35-4712-B876-B2EEA708495C/MicrosoftFixit50285.msi

方法 2. 手工开启全局 DEP

对于 Windows XP 用户，如果之前没有手工调整过 DEP 策略，请点击开始菜单的“运行”，输入“sysdm.cpl”，点击“确定”。程序运行以后，点击“高级”分页，然后点击“性能”分栏中的“设置”按钮。选择“数据执行保护”分页，选择“除所选之外，为所有程序和服

务启用数据执行保护”。然后点击下面的“确定”按钮。这个操作可能需要重新启动系统后生效。

- 以纯文本格式阅读邮件；
- 把互联网络和本地内部网络安全区设置为“高”，在这些区域封锁 ActiveX 控件和 Active 脚本。

使用网络安全产品进行防护

趋势科技最新研发的 **Browser Exploit Prevention** 技术可以成功阻止此漏洞的利用，此项技术目前包含在 PC-cillin2011 中，如果您不是 PC-cillin2011 的用户，您可以使用趋势科技提供的独立工具 **Browser Guard:**

http://free.antivirus.com/browser-guard/