中国地区第二季度
网络安全威胁报告

2011/6

目录

2011 年第 2 季度安全威胁

本季安全警示：
Web 威胁与手机安全防护

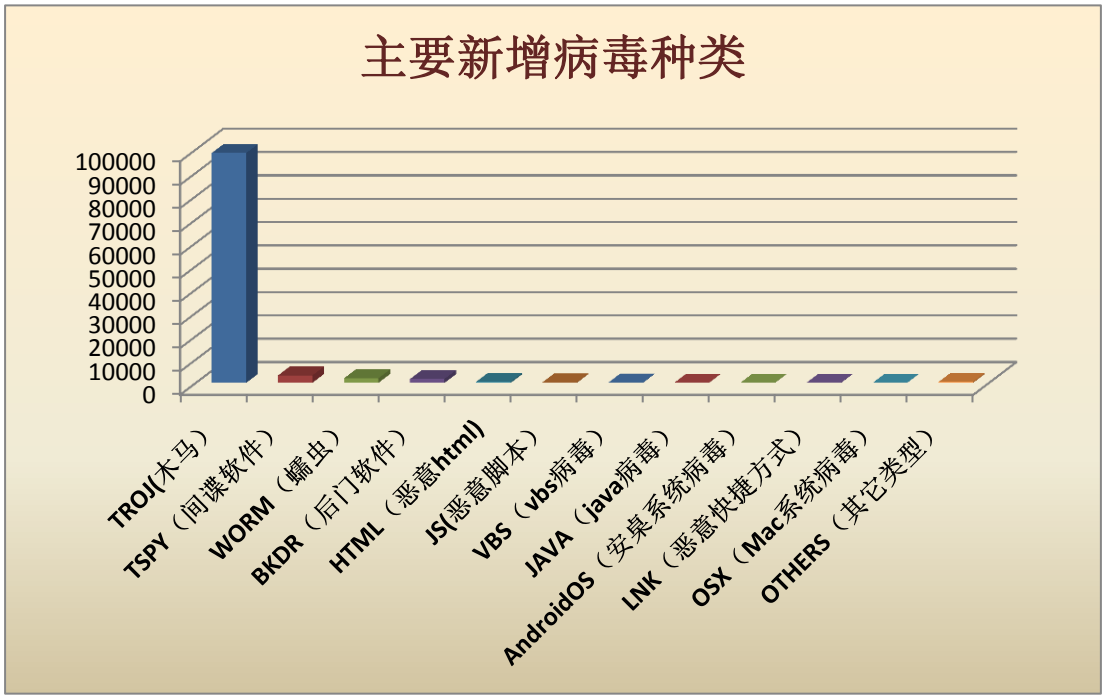
2011 年第 2 季度流行病毒概况

- 本季度趋势科技在中国地区发现新的未知病毒约 **10.7** 万种。截止 2011.6.30 日中国区传统病毒码 8.256.60 可检测病毒数约 340 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。

从以下列表中我们可以看到,本季度病毒码中新增检测病毒类型中的手机平台病毒数量有明显的上升,与上季度相比较不仅仅 AndroidOS 类型病毒数量增加，在塞班平台上的可检测病毒数量也有明显上升。

将手机平台的病毒检测码加入传统客户端病毒码中，可以阻挡恶意程序在电脑与手机进行数据传输时被载入手机，防止手机用户通过电脑错误安装带有恶意代码的软件到手机上。更全面地保护了手机平台安全。

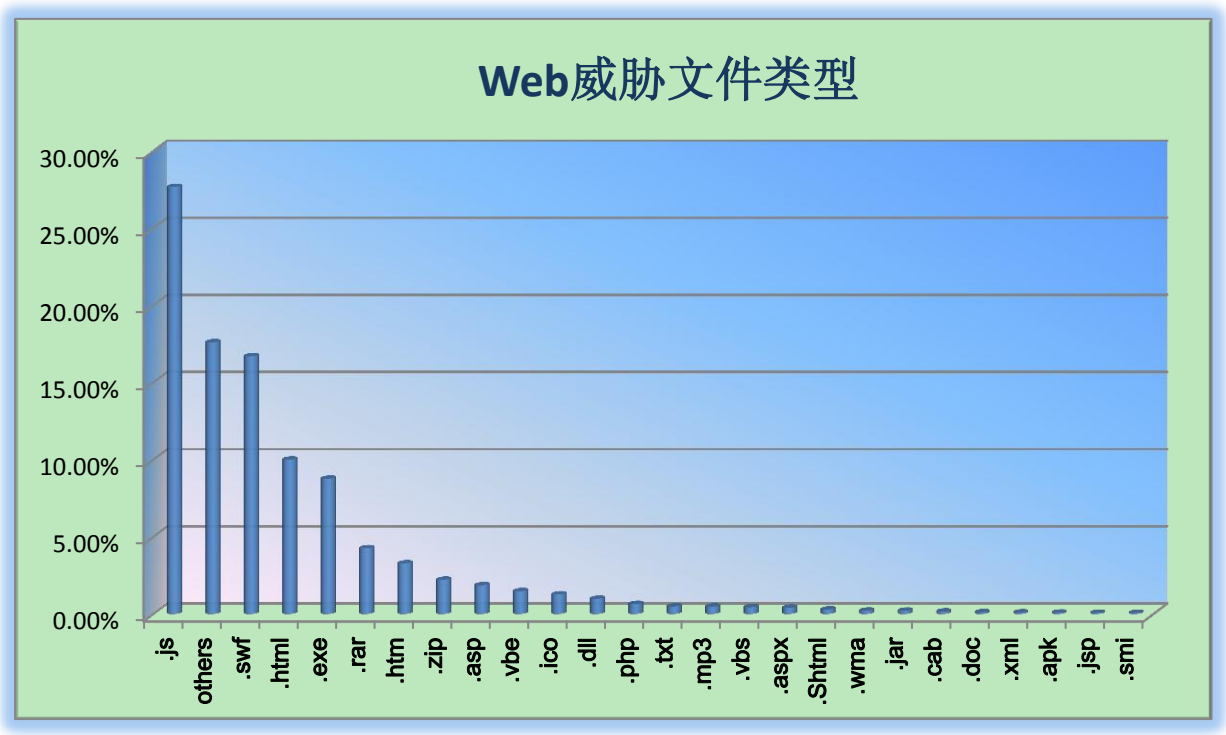


2011 第 2 季度中国地区新增病毒类型

- 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 **14.1** 万个。

其中通过 Web 传播的恶意程序中，约有 **28%**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。

我们注意到，有一些.txt 文件也在恶意 web 威胁文件类型中，并且排名靠前。虽然这些 txt 文件对电脑没有直接危害，但是其中常常包含了盗号木马回传的 email 地址，或是一些病毒要使用的恶意 URL 列表。是一些具有潜在威胁的文件。起到辅助恶意程序进行破坏及盗窃的作用。



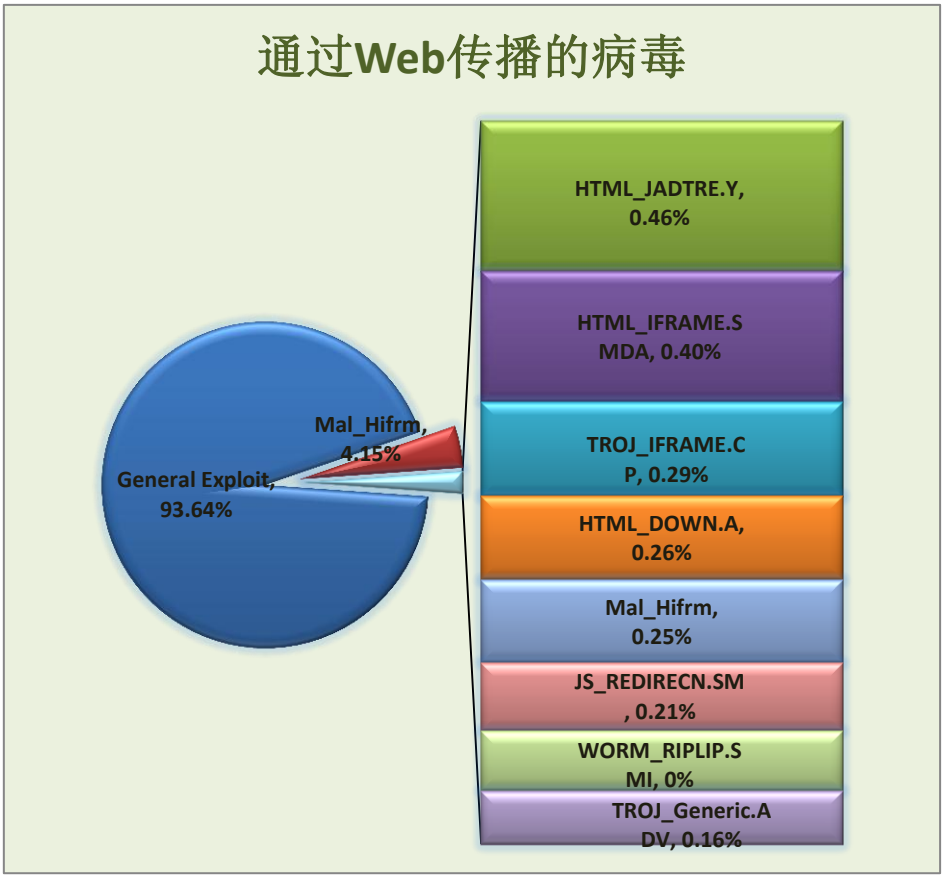
2011 第 2 季度中国地区 web 威胁文件类型

通过对拦截的 Web 威胁进行分析，我们发现。约有 90%以上的威胁来自于 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）。

另外，目前大多数 PE 感染类型病毒除了感染系统中可执行文件之外，常常会感染系统中的 html ,asp ,htm 等网页文件。通常的感染方式是将恶意网站地址写入这些页面文件中。

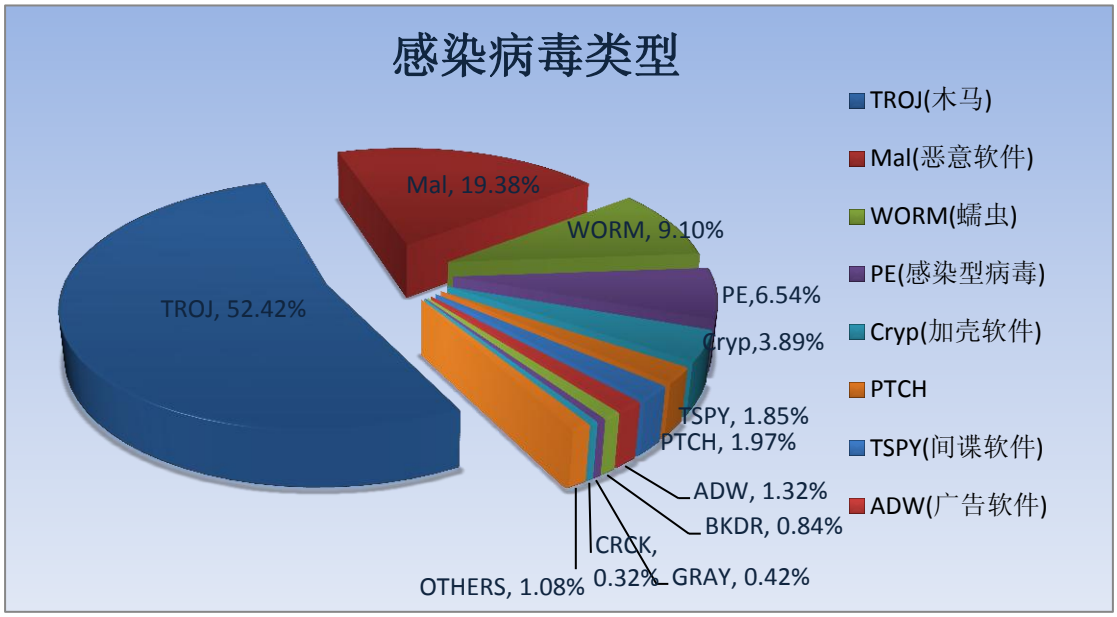
此行为不但会使感染客户机持续访问恶意网站下载病毒，更严重的是如果感染了 web 服务器，将会导致访问被感染的 web 页面的用户也受到病毒侵害。在检测排名中靠前的 HTML_JADTRE.Y 就是一个典型的被 PE 病毒感染 html 类型病毒。

我们观察发现，由于网站职能特殊性，某些政府网站也成为黑客乐于攻击的对象，在 2011 第二季度中我们发现的恶意.gov URL 近百条。社交类型网站，由于其庞大的用户数量，也成为黑客的目标。在 6 月底新浪微薄遭袭事件更反映出社交网站安全管理意识的薄弱。



2011 第 2 季度中国地区前 10 名通过 web 感染的病毒

- 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 **5240** 万次。



2011 第 2 季度中国地区各类型病毒感染数量比例图

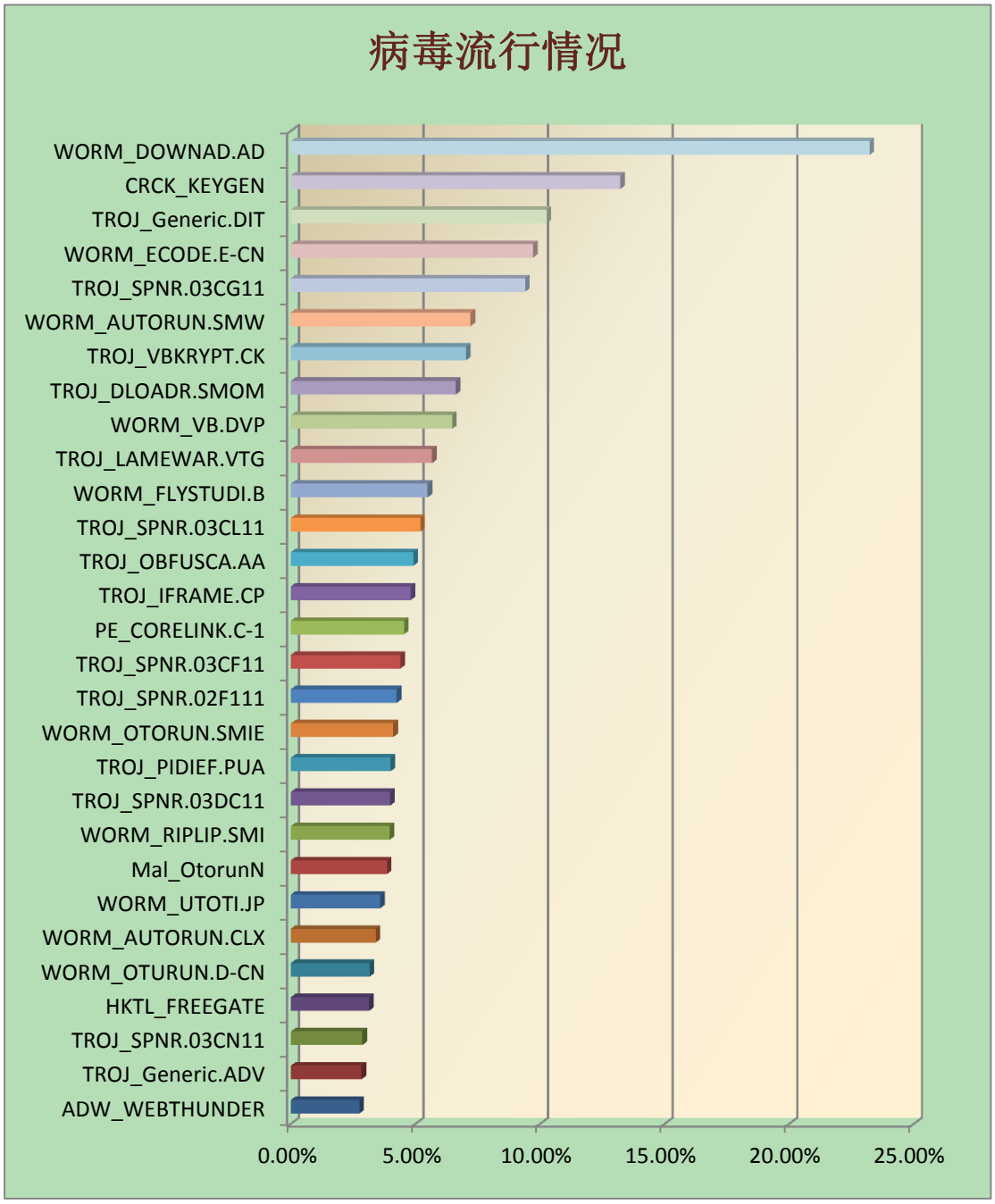
本季度各类型病毒感染趋于平衡，虽然木马类型病毒仍然占有 50%以上的比例，但其它各类型病毒所占比例均有上升。

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。

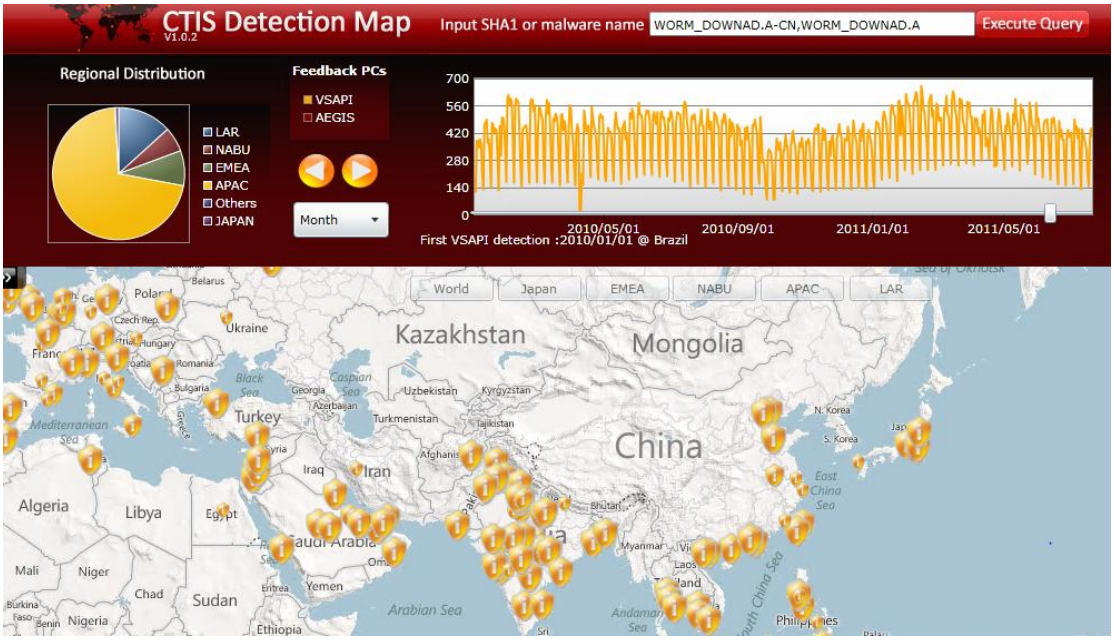
在本季度的感染类型排名中，我们看到一种新的病毒类型 PTCH，该类型病毒一般是由于合法的可执行文件的代码被其他恶意软件修改所致，恶意文件修改正常文件以作为其自动启动机制。也就是说正常文件被感染后成为调用病毒的工具。这样的感染行为使恶意文件隐藏的更深。受感染电脑在手动清理时更加难以处理干净。这种行为可能会被更多的 PE 感染类型病毒使用。

2011 年第 2 季度流行病毒分析



2011 第 2 季度中国地区病毒流行度排名

- 本季度最感染范围最广病毒依旧是 WORM_DOWNAD.AD,在 2011 年第 2 季度在 25%的客户曾经或正在感染该病毒。



从趋势科技 SPN 病毒流行情况监控地图上来看，该病毒在中国地区的数量已经急剧减少，并且多分布在华北华东地区以及中国的南部沿海地区。

从趋势科技客户服务中心接到的案件情况来看，该病毒对客户造成的不良影响也已下降。在安全防护策略执行的较完善的公司中，已不构成太大的威胁，目前要做的是集中处理部分具有安全缺陷的电脑。

这里再提示一下，该病毒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

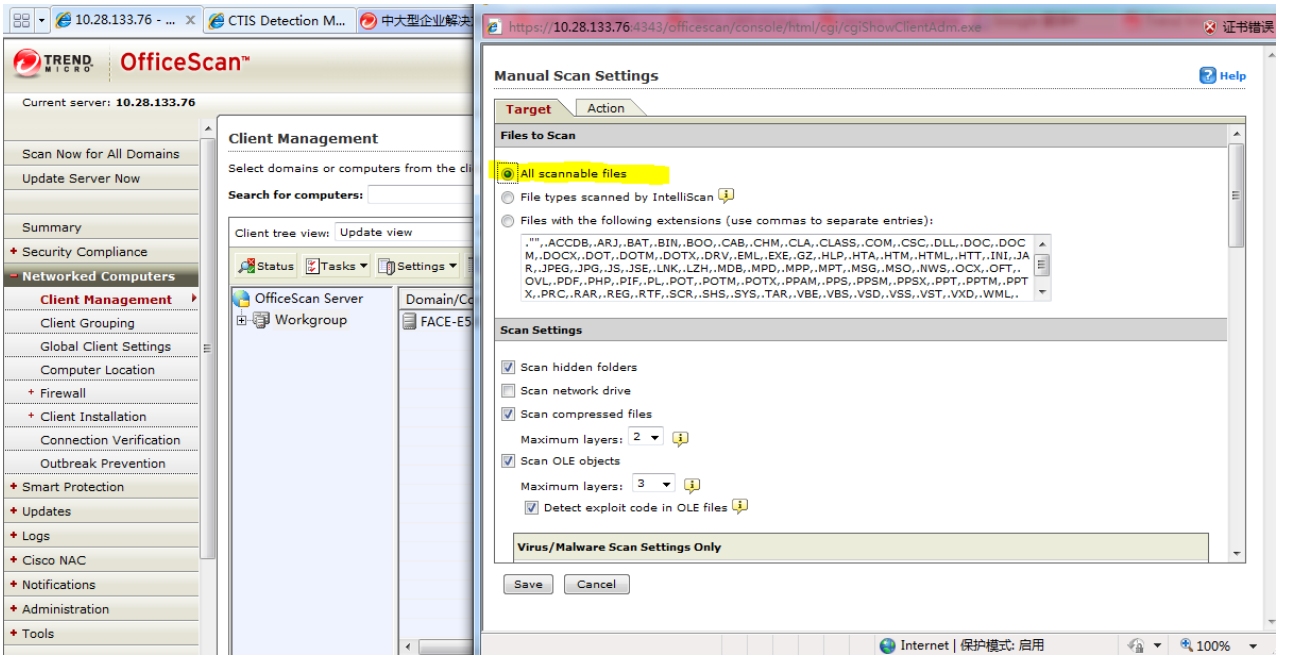
由于目前尚未发现关于该病毒的新变种，使用之前发布的专杀工具以及解决方案即可处理此病毒，该工具可以至趋势科技官方网站下载。

- 可能是本季度未出现新的大规模流行性病毒爆发的原因，流行病毒中 CRCK_KEYGEN 的感染范围排名急剧上升，这也凸现出目前用户环境中普遍存在的使用破解软件注册机的现象。

特别是 AUTOCAD 软件用户使用注册机，导致感染病毒的案件在本季度屡见不鲜。

对于 AUTOCAD 病毒的处理，我们建议用户对 officescan 进行如下设置：

登陆 officescan 服务器控制台，在客户机管理选项中，将实时扫描，手动扫描，预设扫描的对象设置为扫描所有可扫描对象：



由于 AUTOCAD 病毒通常是一种特殊的脚本文件，所以在杀毒软件智能判断其可执行类型时会略过对该文件的扫描。

另外，对于被病毒破坏的文档，如果是覆盖性感染可能无法恢复。但是有些被破坏的文档是可以通过手动方式或特殊工具恢复的。

如果需要恢复此类型文件，请与趋势科技技术支持中心联络。我们将会作针对性处理。

- 高清视频病毒变种出现 WORM_ECODE.B-CN;

  高清视频属于文件夹类型病毒的一种

  文件夹病毒主要特征为：被感染电脑会遍历本地磁盘目录以及映射到本地的网络共享文件夹，将查找到的所有文件夹隐藏并释放与文件夹名称相同的可执行文件。这样用户一旦误点了伪装成文件夹的可执行文件，电脑即被感染

  一般情况下，企业用户网络环境中的文件服务器或开放共享的计算机非常容易感染此类病毒。

  在很多时候，防毒软件可以直接将病毒文件删除，但是如果网络内有感染该病毒的机器。则会导致被攻击电脑文件夹不断被隐藏，导致用户无法正常访问

- 目前趋势科技病毒实验室已将高清视频病毒专杀更新，使之同样可以处理并修复被该变种感染的机器。

  如需获得新的工具，请与趋势科技技术支持中心联络。

2011 年第 2 季度最新安全威胁信息

- **2011 年 6 月 28，新浪微薄遭到 CSRF 攻击，病毒利用新浪微薄网站漏洞向中毒者的好友发送私信，在中毒微薄中发送恶意连接，并且强制关注带有病毒的微薄帐号 ，短短一小时时间内可能有超过 3 万网友中招。**

新华网北京 6 月 28 日电（记者顾洪洪）28 日晚，新浪微博遭遇到首次跨站攻击蠕虫侵袭，微博用户中招后会自动向自己的粉丝发送含毒私信和微博，有人点击后会再次中毒，形成恶性循环。据瑞星安全专家王占涛分析，这主要是因为新浪的广场页面有几个链接对输入参数过滤不严导致。

至记者发稿时为止，在新浪微博搜索，约有数十万条相关结果。王占涛说，此次蠕虫攻击的危害，仅限于滥发含毒私信和链接，未能实现窃取微博账号、窃取用户信息等功能，用户不必过于恐慌。此前，国内多家著名 SNS 网站、博客网站都曾遭到类似攻击，只不过未形成如此大的传播范围。

王占涛表示，随着用户的活动逐渐转移到云端，类似新浪微博蠕虫这样的攻击将会大量出现，SNS 网站将是被攻击的重点。

http://news.cntv.cn/society/20110629/100427.shtml

关于 CSRF 攻击

CSRF 是伪造客户端请求的一种攻击，CSRF 的英文全称是 Cross Site Request Forgery，字面上的意思是跨站点伪造请求。这种攻击方式是国外的安全人员于 2000 年提出，国内直到 06 年初才被关注，并使用 CSRF 攻击实现了 DVBBS 后台的 SQL 注射，同时网上也出现过动易后台管理员添加的 CSRF 漏洞等，08 年 CSRF 攻击方式开始在 BLOG、SNS 等大型社区类网站的脚本蠕虫中使用。

CSRF 的定义是强迫受害者的浏览器向一个易受攻击的 Web 应用程序发送请求,最后达到攻击者所需要的操作行为。CSRF 漏洞的攻击一般分为站内和站外两种类型：

CSRF 站内类型：该类型在一定程度上是由于程序员编写网站时变量使用不当造成的，一些敏感的操作本来是要求用户从表单提交发起 POST 请求传参给程序，但是在变量使用不当的情况下程序也接收 GET 请求传参。这样就给攻击者使用 CSRF 攻击创造了条件，一般攻击者只要把预测好的请求参数放在站内一个贴子或者留言的图片链接里，受害者浏览了这样的页面就会被强迫发起请求。

CSRF 站外类型：其实就是传统意义上的外部提交数据问题，一般程序员会考虑给一些留言评论等的表单加上水印以防止 SPAM 问题，但是为了用户的体验性，一些操作可能没有做任何限制，所以攻击者可以先预测好请求的参数，在站外的 Web 页面里编写 javascript 脚本伪造文件请求或和自动提交的表单来实现 GET、POST 请求，用户在会话状态下点击链接访问站外的 Web 页面，客户端就被强迫发起请求。

对于该类威胁还需要网站维护人员更加注意页面代码编写的安全性。做好网站的安全审查工作。

- **趋势科技 2011 Q2 全球安全威胁分析报告**

http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/2q_2011_threat_roundup.pdf

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)