

Anchoriva 威胁报告 (2010 年第三季度)

作者: Anchoriva 安全实验室

目录

Malware 威胁概况	3
2010 年第三季度 Malware 类别比例图	3
Web Malware Top20.....	3
Web Malware Top20	4
Trojan/QQPhishing 家族弹出的虚假信息.....	5
Email Malware Top20.....	5
Email Malware Top20	6
恶意网站 Top20	6
恶意网站 Top20.....	7
中国地区政府、高校类网站篡改分析	7
中国地区政府、高校类网站篡改（分类）数量统计周报（第三季度）	8
某网站被插入的广告马	8
中国地区政府、高校类网站被篡改数量地区 Top10（第三季度）	9
中国地区政府、高校类网站篡改的恶意网站比例图（按注册地）	9
钓鱼网站	10
“QQ 安全中心”钓鱼网站	10
“腾讯周年庆”钓鱼网站 I.....	11
“QQ 宠物”钓鱼网站	11
央视“非常 6+1”钓鱼网站.....	12
江苏卫视“非诚勿扰”钓鱼网站.....	13
关于 Anchiva.....	13
关于 Anchiva 安全实验室（Anchiva RapidRX Labs）	14

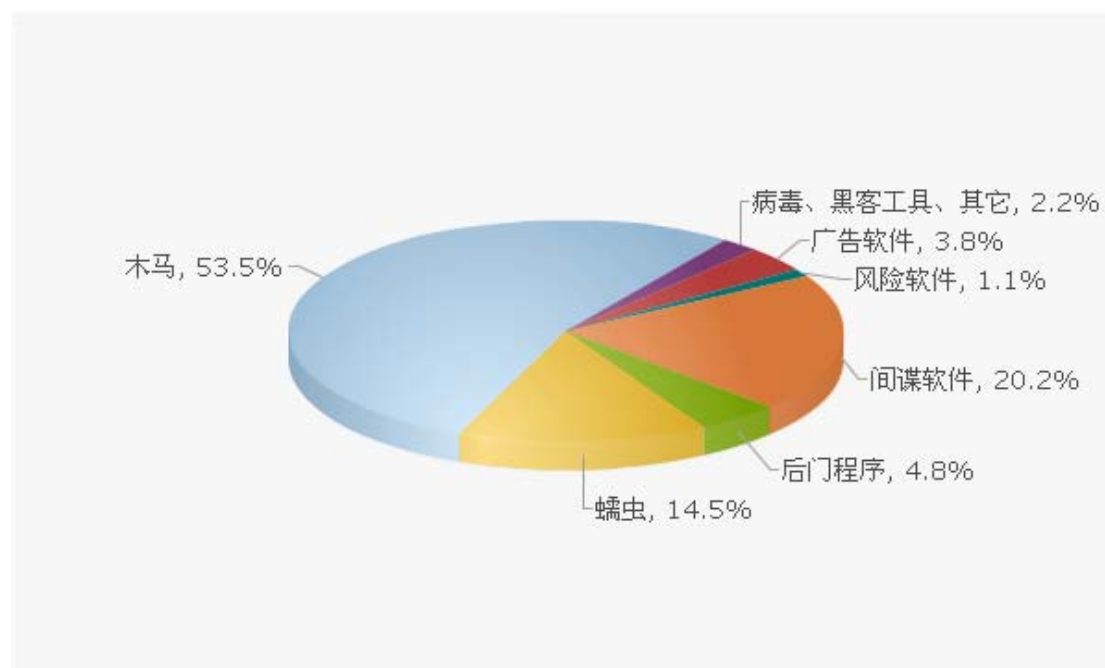
Q3 2010 Anchiva 季度威胁报告大事记

- Anchiva 截获各类 Malware 将近 220 万，间谍软件和蠕虫大幅上升
- 假冒杀毒软件传播猖獗，影响日益严重
- 中国地区网站被广告马、黑链篡改情况严重
- 用于篡改的恶意网站大多数利用免费域名转向服务
- QQ 依然是钓鱼网站热衷，热门电视节目成为新宠

Malware 威胁概况

本季度 Anchiva 安全实验室共截获各类 Malware 约 220 万。相较上一季度，截获数量大幅上升。其中木马所占比例大幅下降，但仍占恶意软件半壁江山，约为 54%。而间谍软件与蠕虫所占比例大幅上升，两者之和约为 35%。传统病毒和其它类别所占比例与上季度类似。

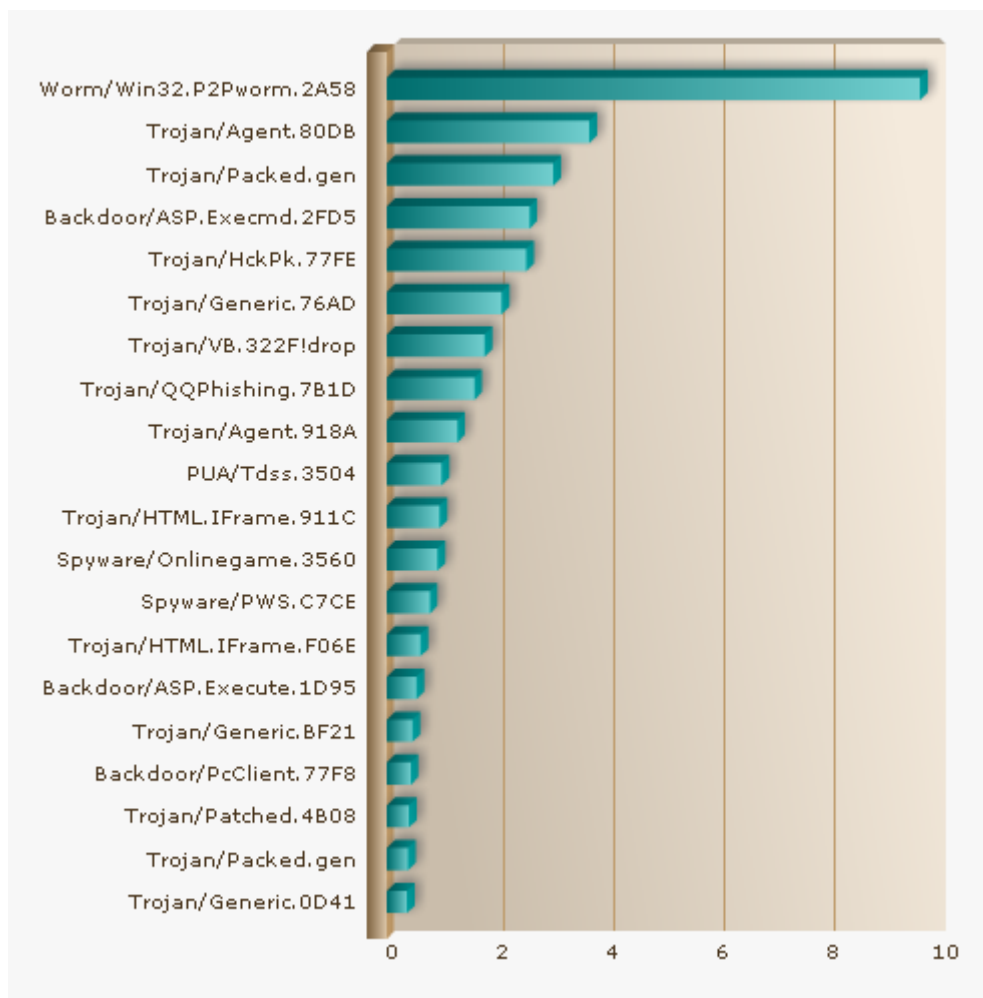
2010 年第三季度 Malware 类别比例图



Web Malware Top20

本季度的 Web 威胁中，其出现频率最高的前 20 个 Malware 如下图所示。

Web Malware Top20



本季度 Web Malware 威胁前 20 中，木马所占比例依然最大，与前文所述威胁概况一致。其中，ASP 类后门上升较快，前 20 中占据两个席位，显示恶意黑客通过脚本后门进行入侵的活动依然猖獗。其余恶意软件多为间谍、钓鱼软件。

Trojan/QQPhishing.7B1D: 该木马是 QQPhishing 家族的一员，一旦进入受害者的机器，它会弹出伪装的 QQ 消息，通知用户中奖消息，并引导用户至其钓鱼页面，最终窃取用户的 QQ 账号、密码等敏感信息。随着 QQ 一站式服务的普及，QQ 账号成为腾讯旗下各服务最重要的验证方式，账号、密码被盗意味着其网上虚拟财产面临损失的危险。

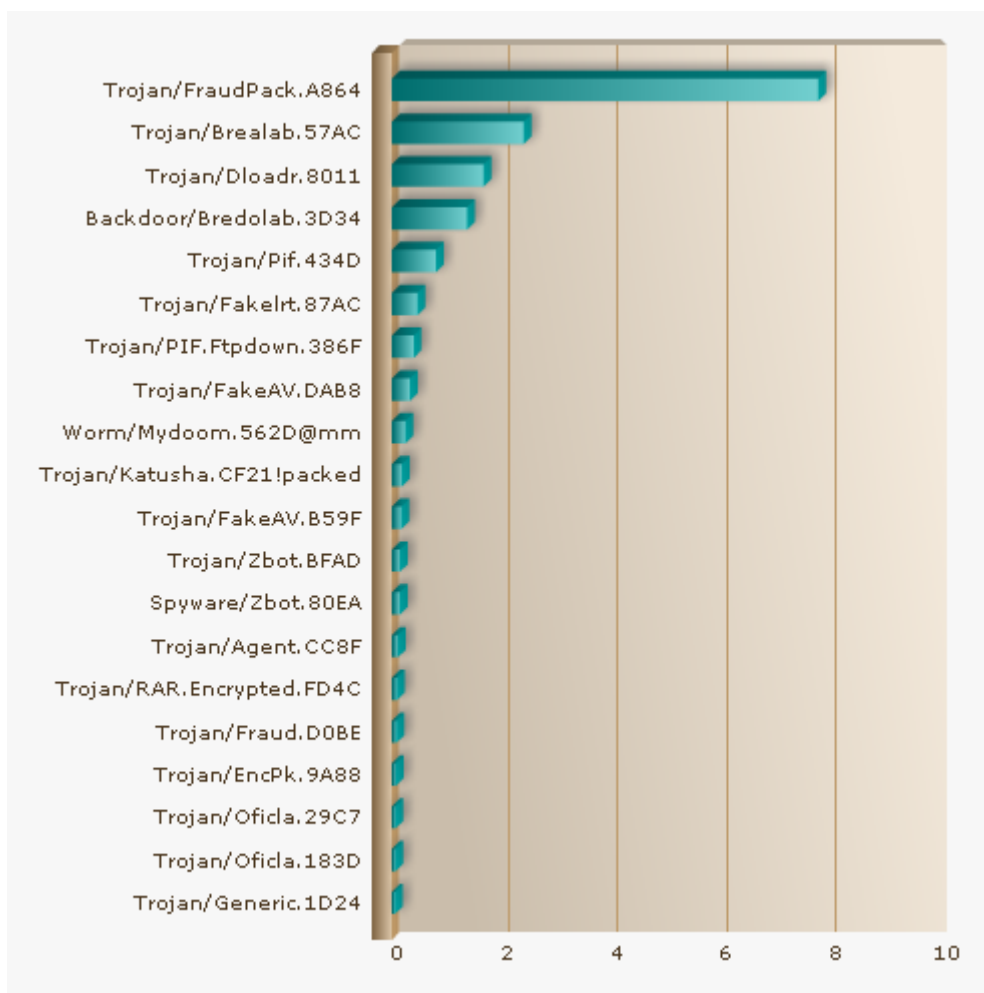
Trojan/QQPhishing 家族弹出的虚假信息



Email Malware Top20

根据 Anchiva Malware 监测网的监测结果, 本季度的邮件威胁中, 出现频率最高的前 20 种 Malware 如下图所示。

Email Malware Top20

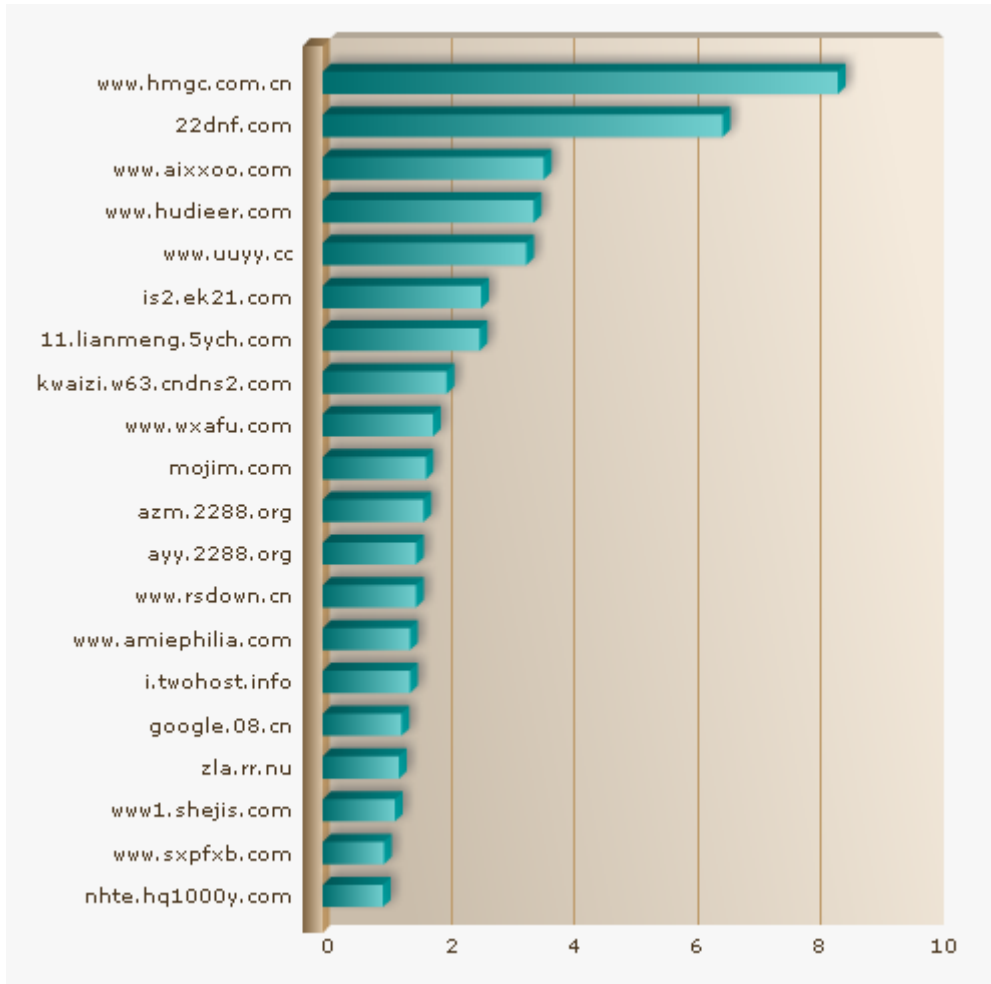


延续上一季度假冒杀毒软件家族的传播势头，该家族依然活跃。这表明假冒杀毒软件对个人电脑用户，甚至企业用户的威胁日益严重。该家族是恶意软件的集合，总的表现为伪装成杀毒软件，向用户发送虚假的病毒信息，提示一些并不存在的威胁，进而将受害者引向假冒杀毒软件的付费网站。它们同时也是发送垃圾邮件、传播其它恶意软件等的罪魁祸首。

恶意网站 Top20

根据 Anchiva Malware 监测网的监测结果，发布恶意软件数量最多的前 20 个恶意网站如下图所示。

恶意网站 Top20



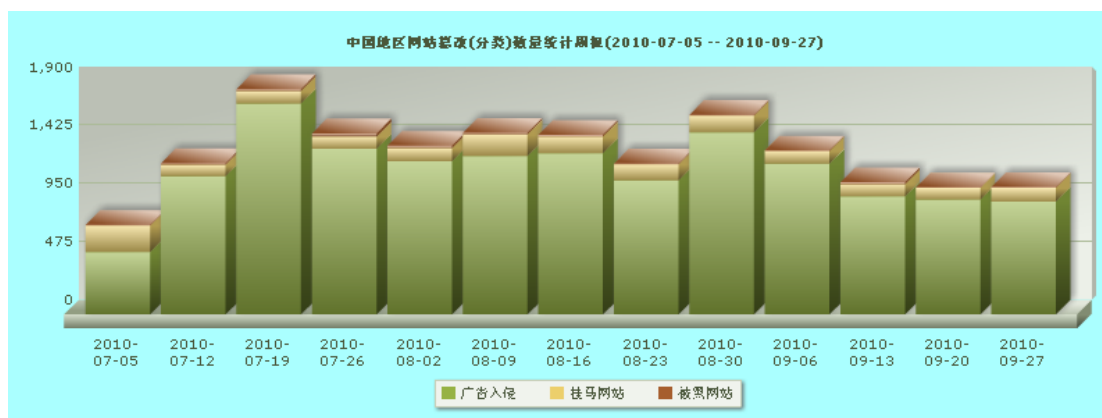
注意，以上所列网站部分仍然存在恶意链接，请勿直接访问！

本季度恶意网站 Top 20 中，延续上一季度正规网站被利用、寄存、传播恶意软件的上升趋势不减，依然占据半数以上。本季度 TOP20 中，所列多为小说、图片、成人网站等流量较高、访问量较大的网站。恶意黑客倾向于入侵该类网站，以扩大其恶意软件的传播规模。

中国地区政府、高校类网站篡改分析

Anchiva RapidRX 网络安全实验室针对中国境内的政府及高校类网站自动化监测、研究发现，广告马在互连网黑色地下产业链中非常猖獗。如下图所示，第三季度中“广告入侵”在篡改数量统计表中占绝大多数。黑客团伙在进行网站挂马的同时，通过事先安装的后门，对目标网站植入大量网络游戏、私服、股票、药品等广告，我们称之为广告马。

中国地区政府、高校类网站篡改(分类)数量统计周报(第三季度)



下图显示的是某网站被插入的广告马,或者说黑链信息。它通过设置高度、宽度为极小数值来达到隐藏的目的。有的则通过设置不可见属性来隐藏。

某网站被插入的广告马

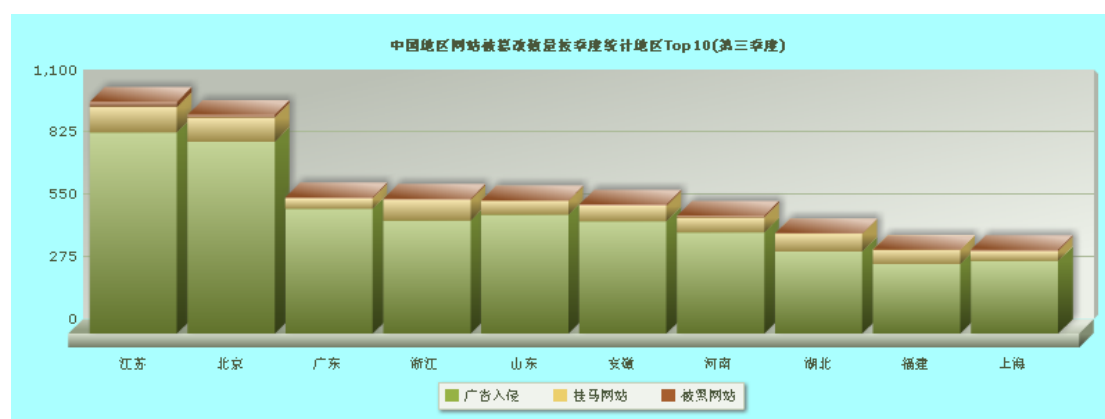
```
<marquee scrollAmount=5000 width="1" height="5" >
<a href="http://www.manoloblahnikshop.com/" target="_blank">manolo blahni
<a href="http://www.pandorajewelryonlinestore.com/" target="_blank">pando
<a href="http://www.okaykicks.com/" target="_blank">nike shoes</a>
<a href="http://www.mulberry-
bags-store.com/" target="_blank">mulberry bags</a>
</marquee>
<marquee scrollAmount=5000 width="1" height="5" >
<a href="http://www.snmack.com/" target="_blank">杂七杂八网</a>
<a href="http://www1.snmack.com/" target="_blank">天天基金网</a>
<a href="http://www2.snmack.com/" target="_blank">入股中心</a>
<a href="http://www3.snmack.com/" target="_blank">潜力股吧</a>
<a href="http://www4.snmack.com/" target="_blank">今日股票行情</a>
<a href="http://www5.snmack.com/" target="_blank">同花顺2010</a>
<a href="http://www6.snmack.com/" target="_blank">最热股票推荐网</a>
<a href="http://www7.snmack.com/" target="_blank">个股专家</a>
<a href="http://www8.snmack.com/" target="_blank">牛老大股吧</a>
<a href="http://www9.snmack.com/" target="_blank">李老太太股票吧</a>
<a href="http://www.tiantianqingsu.com/" target="_blank">天天倾诉网</a>
<a href="http://www.weixiouzhihiwang.com/" target="_blank">维修知识网
</a>
<a href="http://www.chinabaoyangw.com/" target="_blank">中国保养网</a>
<a href="http://www.xiaochangshiw.com/" target="_blank">小常识网</a>
<a href="http://yuye.snmack.com/" target="_blank">铝业网</a>
<a href="http://www.snmack.com/" target="_blank">365菜谱网</a>
<a href="http://gangye.snmack.com/" target="_blank">钢业</a>
```

广告马是网络营销者在搜索引擎优化中较为普遍的一种手段。通过插入这些链接,用以提高其反向链接率,进而提升其在搜索引擎的搜索命中率。这类广告马一般在页面上不会显示异样,仅在其源代码中才能发现被添加的代码。直观看来好像

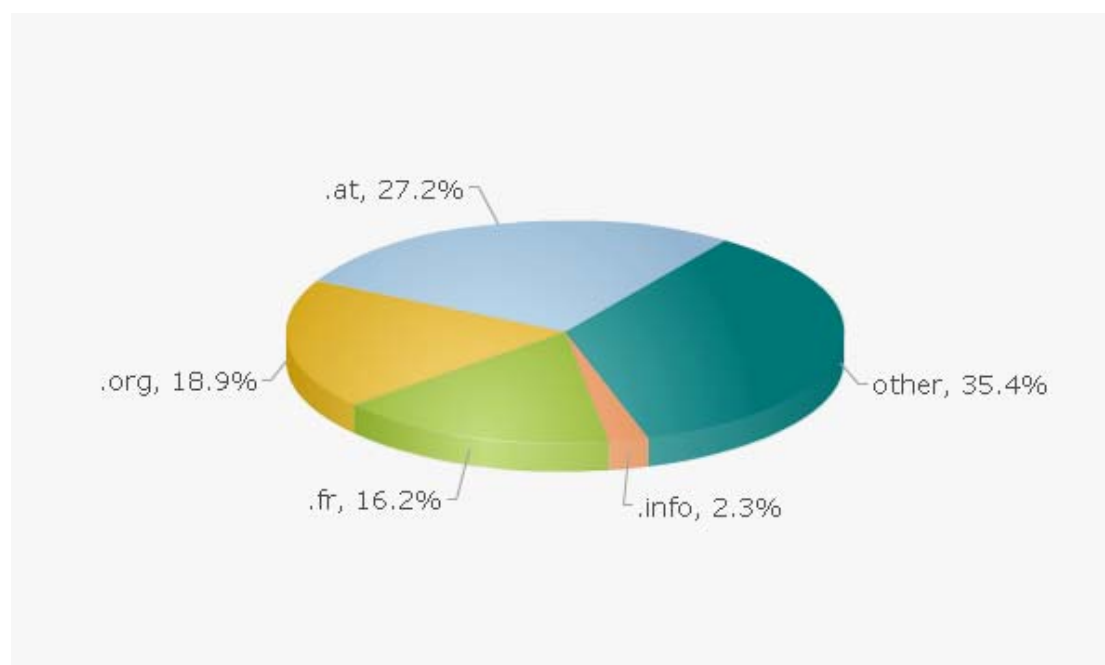
无害，其实会大大影响正常网站的信誉，甚至可能被安全软件所屏蔽。研究表明，上传组件、不安全的服务器配置、不及时更新的 web 应用，都是导致服务器被恶意黑客攻陷，沦为其寄存、传播恶意软件的原因。

通过统计中国地区被篡改网站数量地区前十，我们发现在今年第三季度排名情况如下图所示。被篡改的网站集中在 IDC 机房较多、网站较集中的省份和地区，如江苏、北京、广东、浙江等地。

中国地区政府、高校类网站被篡改数量地区 Top10 (第三季度)



中国地区政府、高校类网站篡改的恶意网站比例图 (按注册地)



通过统计第三季度我们的监控平台发现的恶意网站数据，我们认为针对中国地区网站的入侵、篡改多为自动化工具产生，而用于篡改网站、批量挂马等恶意行为的恶意网站绝大部分是使用 3322.org、8866.org、isgre.at 等免费注册的域名转向服务，使受害者在浏览正常网站时，不知不觉的载入其它恶意网站的恶意脚本，最终下载恶意软件，进而产生破坏。以上比例图中显示，仍有超过 1/3 的恶意网站是

通过被入侵的合法网站来进行恶意行为，小部分是通过注册 info 结尾的域名来传播。

钓鱼网站

电子支付平台、银行金融网站依然是第三季度钓鱼网站所热衷的目标。就国内用户而言，针对 QQ 账户、密码的钓鱼网站则是重中之重。利用国内热门的电视节目较高的收视率，如央视的“非常 6+1”、江苏卫视的“非诚勿扰”等，进行钓鱼活动的网站也屡见不鲜。

“QQ 安全中心”钓鱼网站



针对QQ账号、密码的钓鱼网站通过QQ群进行散播，通过木马在用户机器中弹出伪装的QQ消息，通知“中奖”等方式不一而足。QQ用户中，其游戏用户占有较大比重，伪装成QQ游戏网站的钓鱼页面，也时有发生。

“腾讯周年庆”钓鱼网站 I



“QQ宠物”钓鱼网站



利用热门节目的知名度，通过邮件、论坛中的帖子等方式，通知受害者“中奖”信息，诱骗到钓鱼网站。该类网站，大多数情况下其域名会与相应欺骗的节目名称一致，用以迷惑不仔细的受害者。

央视“非常6+1”钓鱼网站



江苏卫视“非诚勿扰”钓鱼网站



关于 Anchiva

Anchiva 公司成立于 2006 年，公司汇集了来自防病毒领域以及网络安全设备领域的优秀人才，创办人和高管曾经在 Cisco、Netscreen、Fortinet 等国内外著名的安全设备厂商中担任过重要职务。到目前为止，公司在北京、杭州、美国加州设立了三个研发中心，拥有众多优秀的研发人员；并在北京、上海、广州、杭州、香港、台湾、San Jose 设有销售办事处，产品及服务遍及亚洲以及北美洲。

Anchiva 是 web 安全网关的领导者，致力于加强企业网络边界安全。公司两条主要产品线 A 系列以及 S 系列，分别保护企业内部终端上网安全以及企业 web 服务器的安全。A 系列产品集安全威胁防御与上网管理功能于一身，强大的威胁防御功能，有效的过滤随 Internet 应用而来的病毒、木马、后门、蠕虫、间谍软件、僵尸网络以及其他各种恶意威胁，同时配合上网管理的 Internet 应用控制与带宽管理、上网行为内容审计、外发信息过滤与管控等功能来规范、过滤员工上网行为，提高办公效率，防止商业机密外泄，将员工上网所可能带来的综合网络威胁降到最低，是一款功能全面的上网安全网关。S 系列产品部署在 web 服务器群前端，有效地抵御 SQL 注入、XSS 攻击等 web 应用攻击，保障 web 服务器的安全运维与正常应用。

Anchiva 全系列产品均采用专门为网络信息安全网关而设计的操作系统 AnchivaOS，在自主研发的高性能 ASIC 芯片驱动下，打破了传统信息安全网关性能瓶颈，为企业提供实时、全方位的安全防护。其中 A 系列具有 ICISA 病毒检测认证和 ICISA 性能测试认证，不仅证明了其 100% 防御业界病毒研究权威组织 Wildlist 发布的所有病毒的能力；同时也证明了其全球领先的高性能特性。另外，Anchiva 非常关注技术创新，每个主流的技术都在中国拥有知识产权。

为了提供良好的客户服务，Anchiva 拥有自己的 RapidRX 威胁防御实验室，每天可处理数万个新的恶意程序，由经验丰富的病毒分析师和威胁研究员组成，他们战略性的分布在北美与中国，负责采集、交换恶意代码与攻击样本，搭建自动升级网络。Anchiva 网关特征库容量、覆盖率在业界遥遥领先。目前，Anchiva 产品的 Malware 特征库可检测的互联网中传播的恶意程序已在千万以上。RapidRX 实验室提供 7X24 小时不间断的升级服务，包括 Malware 特征库、恶意站点库、URL 分类库、Web 威胁特征库、僵尸网络数据库、应用协议特征库；并且具有启发式扫描技术与“零日保护”计划，Anchiva 确保用户网络随时处在最新技术的保护下。

Anchiva 的 A 系列产品线分为五个型号，S 系列分为四个型号，覆盖用户由 200 人到 10000 人，单台设备支持的带宽从 10M 到 1.3G，最高端单台设备在所有功能同时开启时支持的吞吐量超过 1G。Anchiva 的客户涉及金融、政府、运营商、能源、医疗、制造、科技、零售和教育等多个行业，在国内拥有数百位的重要客户。

通过持续不断的技术创新，Anchiva 致力于为企业客户提供更全面的 Internet 接入安全。

关于 Anchiva 安全实验室（Anchiva RapidRX Labs）

Anchiva 安全实验室成立于 2006 年，由经验丰富的 Malware 分析专家和安全研究员组成，为世界权威病毒研究组织 Wildlist 的成员。该实验室是 Anchiva 全球反病毒研究和产品支持中心，也是 Anchiva 安全服务基础设施的中枢系统，在亚太、北美和欧洲等地设有专门的病毒研究中心和样本采集网络，为全球客户提供持续的全天候病毒防范服务。更多安全资讯请访问 <http://www.anchiva.com/virus/>。