

Anchiva 威胁报告 (2010 年第四季度)

作者: Anchiva 安全实验室

目录

Malware 威胁概况	2
2010 年第四季度 Malware 类别比例图	3
Web Malware Top20	3
Web Malware Top20	4
Email Malware Top20	5
Email Malware Top20	5
恶意网站 Top20	6
恶意网站 Top20.....	6
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（第四季度）	7
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（第四季度）	8
钓鱼网站	9
网站仿“腾讯 QQ - 系统消息”提示中奖信息.....	9
“腾讯周年挖宝行动”钓鱼网站 I	9
“腾讯周年挖宝行动”钓鱼网站 II	10
“腾讯周年挖宝行动”钓鱼网站 III.....	10
关于 Anchiva	12
关于 Anchiva 安全实验室（Anchiva RapidRX Labs）	13

Q4 2010 Anchiva 季度威胁报告大事记

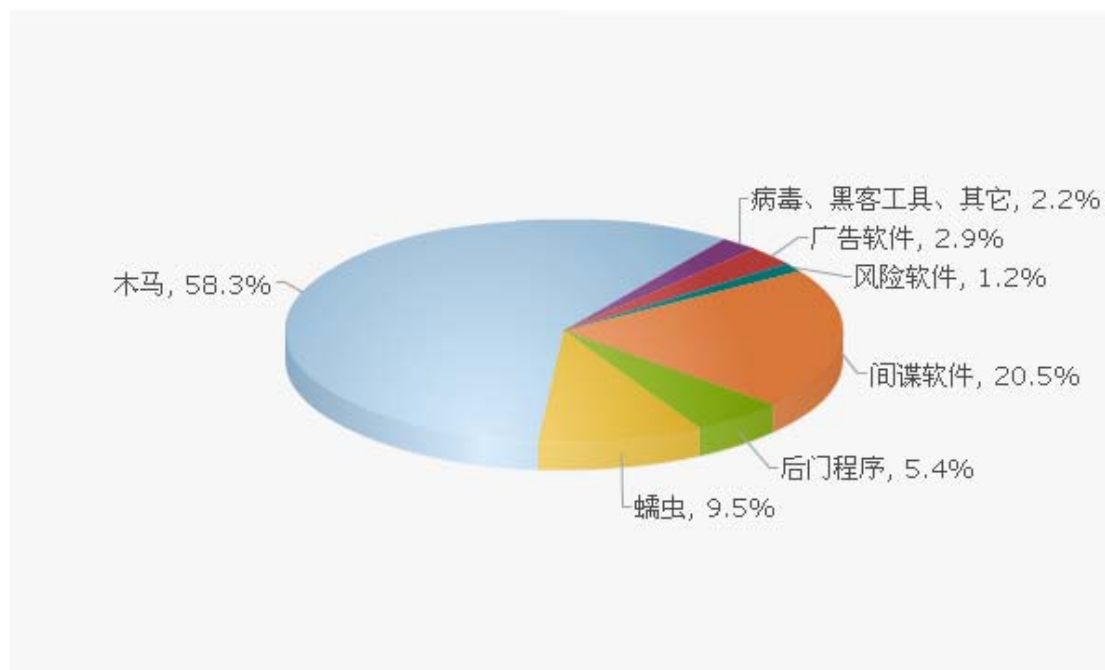
- Anchiva 截获各类 Malware 将近 350 万，蠕虫小幅下降。
- P2PWorm 肆虐，游戏盗号木马横行。
- 假冒杀毒软件得到抑制，老牌蠕虫焕发“第二春”。
- 免费域名转向服务成为恶意网站的温床。
- 中国地区网站被广告马、黑链篡改情况依然严重。
- 挂马也钓鱼。

Malware 威胁概况

本季度 Anchiva 安全实验室共截获各类 Malware 约 350 万。相较上一季度，截获数量大幅上升，增长超过 50%。其中蠕虫所占比例下降较大，约为 10%，而木马

所占比例小有上升，仍占恶意软件半壁江山，约为 58%。传统病毒和其它类别所占比例变化不大，与上季度类似。

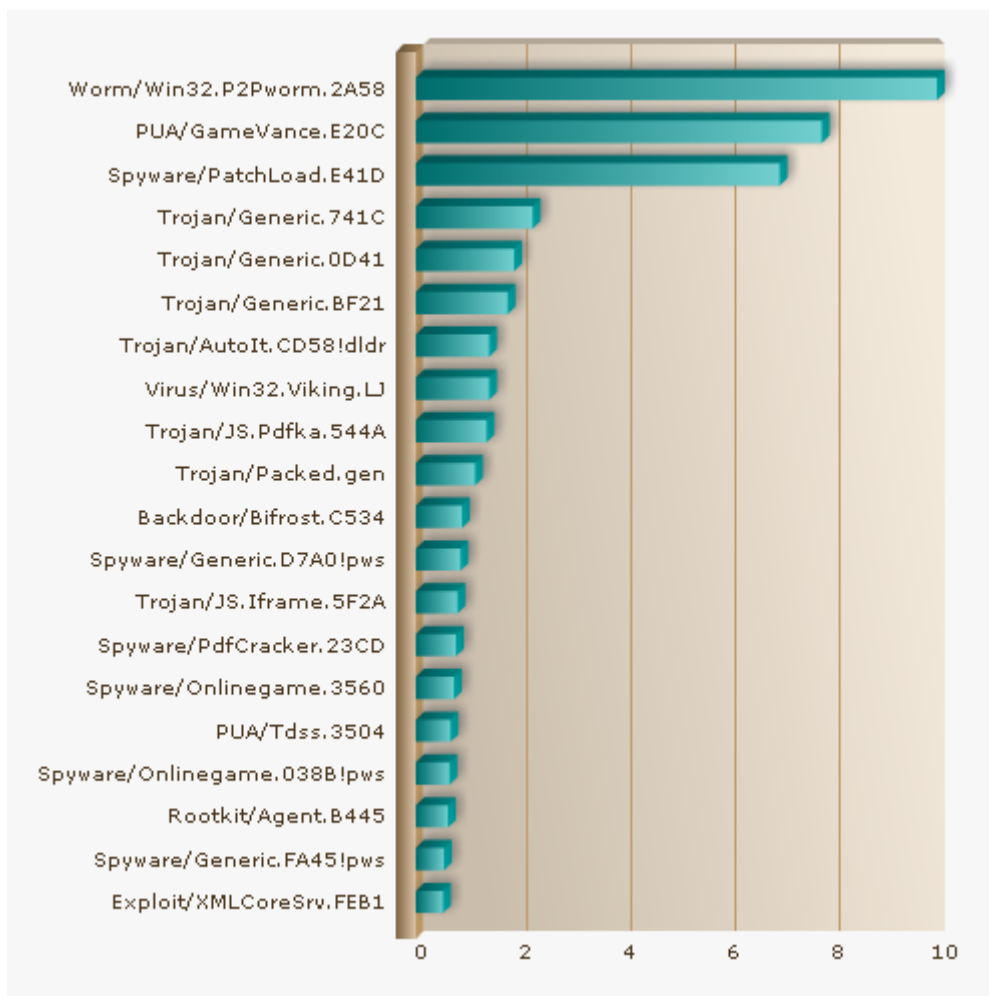
2010 年第四季度 Malware 类别比例图



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



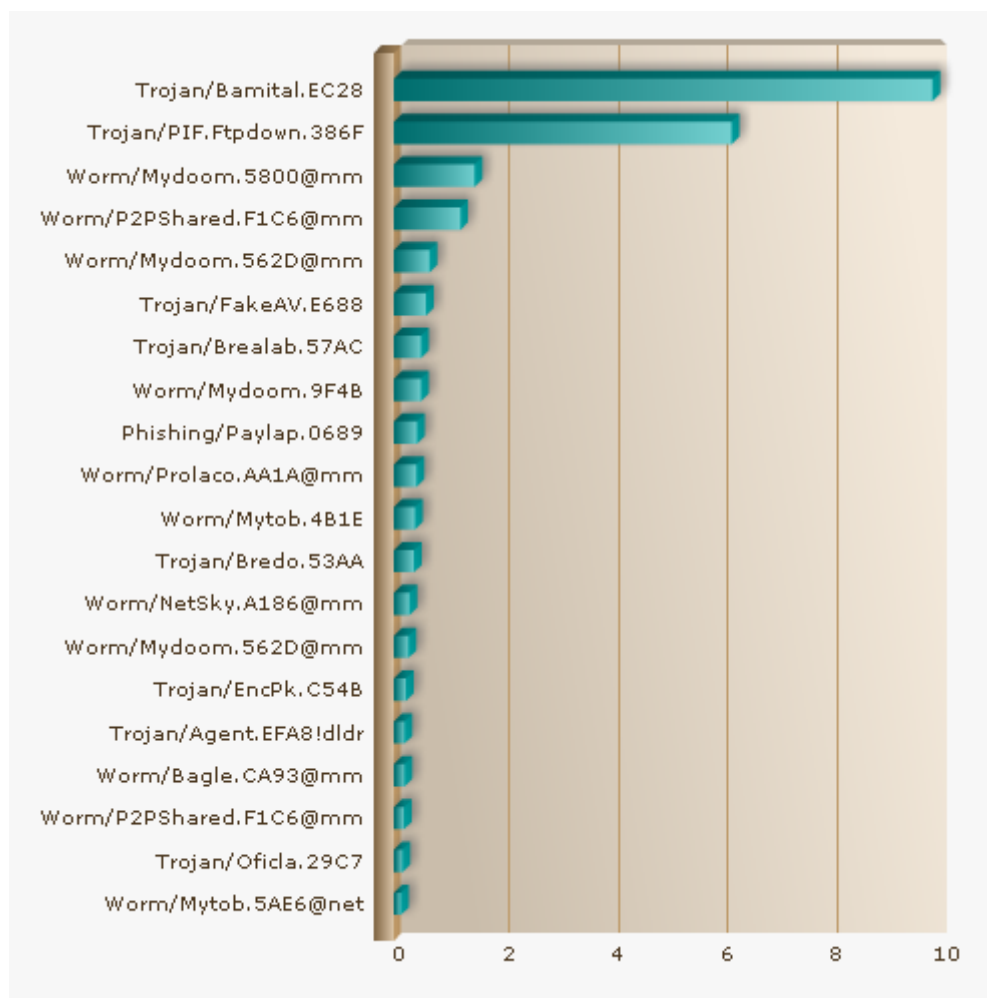
本季度 Web Malware 威胁前 20 中，相较上一季度，Worm/Win32.P2Pworm 家族依然占较大比例，为本季度所拦截恶意软件总数第一。木马 Trojan/Generic 家族在前十中占据三个席位。从分类上看，间谍软件（spyware），特别是针对游戏盗号的恶意软件依然在本季度 Web Malware 威胁中占据大多数。

Worm/Win32.P2Pworm.2A58: 该蠕虫是 P2Pworm 家族的一员，它主要通过 P2P 网络共享传播，伪装成 IE 浏览器清除工具，一旦进入受害者电脑，它会进行下载其它恶意软件、大量传播垃圾邮件等恶意行为。

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



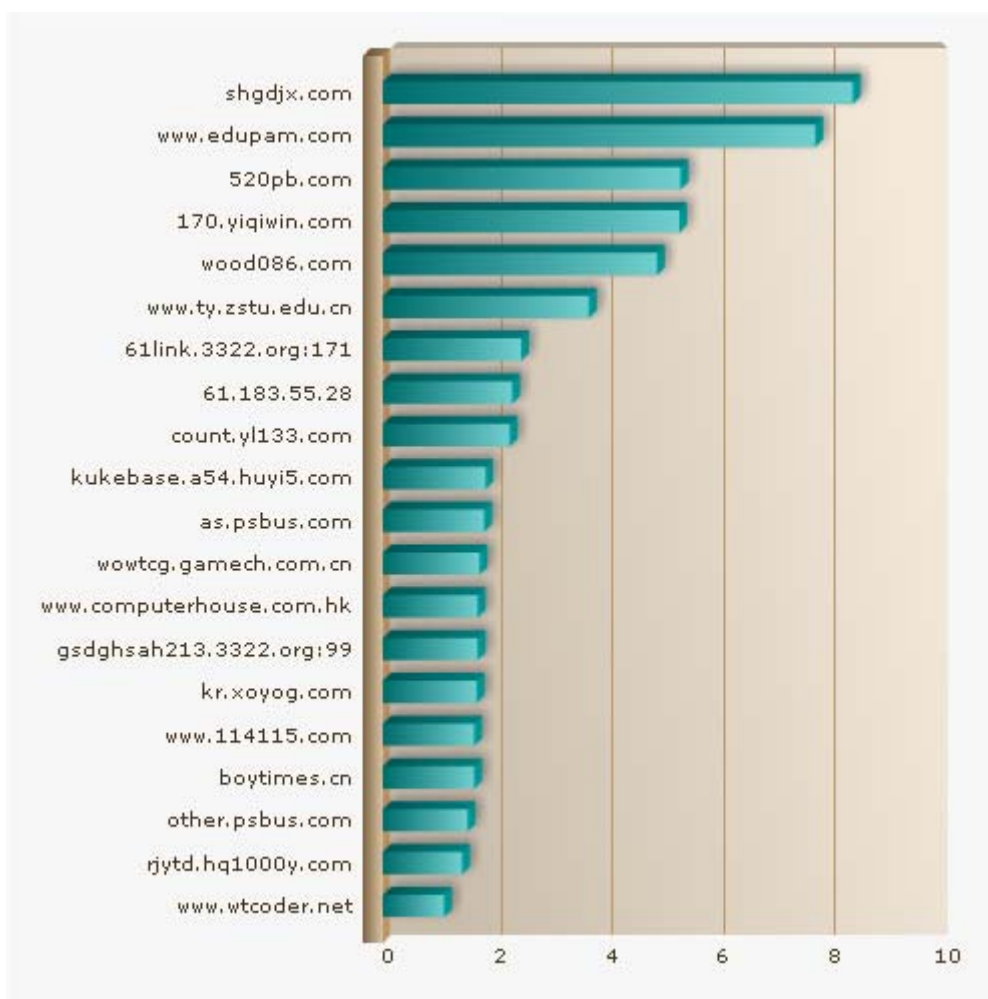
本季度假冒杀毒软件家族的传播势头得到有效抑制，一些老牌的邮件蠕虫则焕发了“第二春”，比如 Mydoom、Netsky、Bagle 等家族合计占有 6 个席位。

Trojan/Bamital.EC28: 该木马通常由其它恶意软件安装到受害者电脑中，一旦运行后，它会监控用户的网页搜索内容，并相应的进行更改，显示由攻击者控制的内容，比如推送广告等。它也会连接其它网站，下载更新指令或其它恶意软件。

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



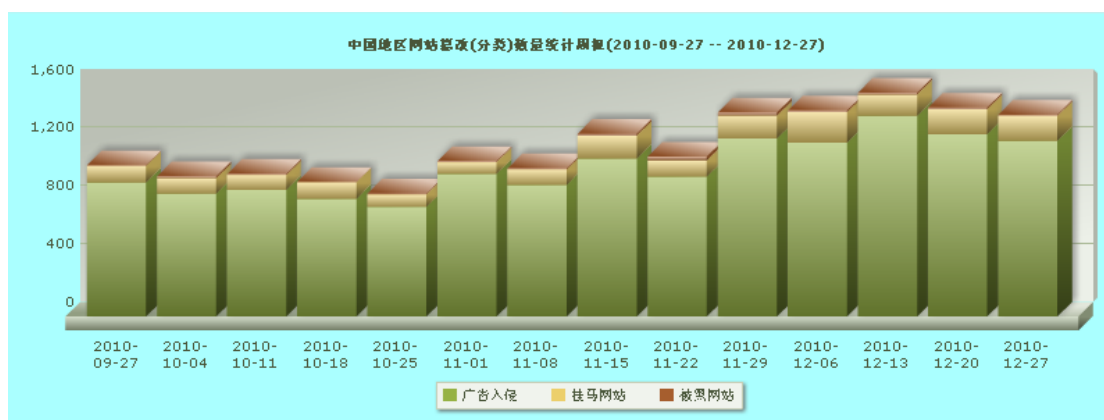
注意，以上所列网站部分仍然存在恶意链接，请勿直接访问！

相较上一季度恶意网站 Top 20，被拦截的网站变化较大，显示黑客用于传播恶意软件的“前沿”阵地变化多端，但万变不离其宗，多数为正规网站被利用、寄存、传播恶意软件。与上一季度 TOP20 类似，所列多为小说、图片、成人网站、私服等流量较高、访问量较大的网站。用户在浏览该类网站时，宜做好病毒安全防护、打好电脑补丁，减少或者不浏览不明网站，更不要轻易相信通过邮件、聊天软件等收到的不明链接。

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结果如下图所示。与上一季度相比较，“广告入侵”依然占绝大多数，黑客在网页源代码中植入黑链代码，为其它网站提升搜索排名，并以此牟利。广告马通过其后门种上指定关键词后，普通用户访问相关站点，无形中点击了该关键词，使得该类关键词在搜索引擎中排名靠前，达到恶意搜索引擎优化的目的。黑客“偏爱”政府和教育类网站，尤其是省市县等级别的网站，究其原因这类网站的维护管理相对较差，但网页级别高，在搜索引擎中排名更靠前。

中国地区政府、高校类网站篡改（分类）数量统计周报（第四季度）



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

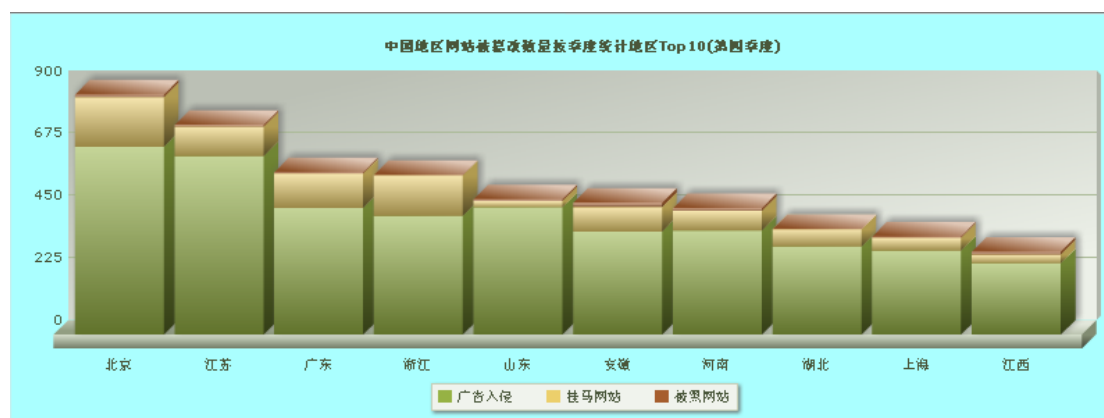
```

</a>
</div>
<MARQUEE onmouseover=this.stop() onmouseout=this.start()
scrollAmount=1 direction=up width=1 height=1 delay="1">
<A href="http://www.073151.com/" title="湖南人才市场">湖南人才市场</A>
<a href="http://www.lmzs.cn" title="长沙装饰公司">长沙装饰公司</a>
<A href="http://www.hncdsy.cn/" title="密码锁">密码锁</A>
<A href="http://www.0731jj.net/" title="长沙家教">长沙家教</A>
<A href="http://www.hnyjdw.com/" title="长沙贷款">长沙贷款</A>
<A href="http://www.csxhzs.com.cn/" title="长沙美容美发装修">长沙美容美发
装修</A>
<A href="http://www.newcaipiao.cn/" title="双色球">双色球</A>
<A href="http://www.zxdc007.cn/" title="湖南侦探公司">湖南侦探公司</A>
<a href="http://www.lmzs.cn" title="长沙家装公司">长沙家装公司</a>
<A href="http://www.hnrc.com/" title="湖南人才网">湖南人才网</A>
<a href="http://www.67gu.com" title="股票">股票</a>
<A href="http://www.xielw.cn/" title="免费论文">免费论文</A>
<A href="http://www.hnrcjob.com/" title="湖南人才网">湖南人才网</A>
<A href="http://www.qqpei.cn/" title="中国福利彩票">中国福利彩票</A>
<A href="http://www.zxdc007.cn/" title="长沙侦探">长沙侦探</A>
<A href="http://www.csxfbg.cn/" title="湖南文件柜">湖南文件柜</A>
<A href="http://www.lzxnsg.cn/" title="电子鞋柜">电子鞋柜</A>
<A href="http://www.hn365zl.cn/" title="长沙空调安装">长沙空调安装</A>
</MARQUEE>
<MARQUEE onmouseover=this.stop() onmouseout=this.start()
scrollAmount=1 direction=up width=1 height=1 delay="1">
<A href="http://www.caipiaoliu.cn">3d</A>
</MARQUEE>

```

通过统计中国地区被篡改网站数量地区前十，我们发现在今年第四季度排名情况如下图所示。相较上一季度，被篡改的网站地区分布、排名变化很小，表明 IDC 机房较集中的省份、地区，其保管的网站更容易成为黑客攻击的目标。

中国地区政府、高校类网站被篡改数量地区 Top10 (第四季度)



通过统计第四季度我们的监控平台发现的恶意网站数据，黑客多为利用自动化工具针对中国地区网站的进行大批量的入侵、篡改，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，盗窃个人信息、网上银行账户等。

钓鱼网站

在检查我们的中国地区网站防篡改监控平台的日志时，我们发现了一起当时正在进行的针对腾讯 QQ 用户的钓鱼活动。

网站仿“腾讯 QQ - 系统消息”提示中奖信息



攻击者通过其事先在受害网站上安装的后门，插入一条指向另一恶意网站的链接，当用户浏览该网站某些页面时，弹出如上图所示的消息。它伪装成腾讯QQ的系统消息，告知用户中奖信息，引导受害者至攻击者控制的钓鱼网站。

“腾讯周年挖宝行动”钓鱼网站 I



受害者进入其指定的网站后，接着会提示“获奖通知”及其“幸运编码”。

“腾讯周年挖宝行动”钓鱼网站 II



输入前面提示的“幸运编码”后，钓鱼网站接着提示获奖信息。

“腾讯周年挖宝行动”钓鱼网站 III



最终进入上图所示的页面后，要求输入真实姓名、证件号码、详细地址、银行账号等个人敏感信息。经过重重曲折，这个最终页面所要输入的信息才是钓鱼者所最关心的。

电子支付、网上银行等“潮流”已经势不可挡的进入寻常百姓家，在畅享网上购物的便利、快捷的同时，我们要捂紧自己的“口袋”，对于要输入个人敏感信息的网址小心确认，不给钓鱼者以任何机会。

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 ICSA 病毒检测认证和 ICSA 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/>。