

Anchiva 威胁报告 (2009 年第四季度)

作者: Anchiva 安全实验室

目录

Malware 威胁概况	3
Web Malware Top20	4
Email Malware Top20	5
恶意网站 Top20.....	8
大型社交网站 Rockyou 被入侵，3200 万用户信息被泄露.....	9
Adobe 零日漏洞	10
微软 IIS 畸形文件扩展名绕过安全限制漏洞	11
内网肆虐横行的 Conficker	12
钓鱼网站.....	12
关于 Anchiva	14
关于 Anchiva 安全实验室（Anchiva RapidRX Labs）	14

图表目录

2009 年第四季度 Malware 类别比例图	3
Web Malware Top20	4
某客户中 Trojan/HTML.IFrame.EDA6 的部分拦截记录	5
某客户中 Trojan/JS.Shellcode.0F5D 的部分拦截记录	5
Email Malware Top20	6
假冒杀毒软件	7
某客户中 Worm/FakeAlert.4840@mm 监测统计	7
恶意网站 Top20.....	9
被公布的 rockyou.com 用户密码统计 Top20	10
利用 Adobe PDF 漏洞的攻击拦截记录	11
畸形文件扩展名攻击实例.....	11
某客户内网中 Conficker 的部分拦截记录.....	12
拍拍网钓鱼网站.....	13
某客户中拦截的社交钓鱼网站部分实例	13

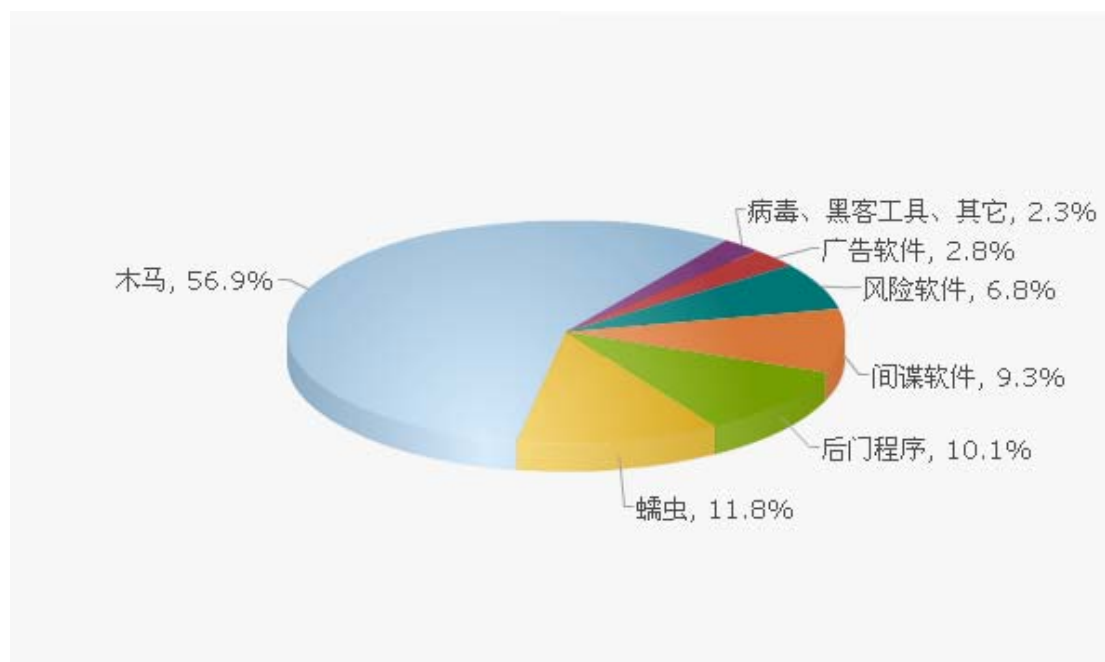
Q4 2009 Anchiva 季度威胁报告大事记

- 本季度 Anchiva 截获新生恶意软件超过 200 万
- 网页木马是 Web 安全的主要威胁
- 间谍软件通过邮件大量传播，骗钱并监控用户网银帐号
- 恶意网站持续增长，“.cn”域名位居前列
- 大型社交网站被入侵，3200 万用户信息被泄露
- Adobe 零日漏洞频现，用户打开 PDF 需谨慎
- IIS 服务器文件名解析缺陷致大量服务器被入侵
- Conficker 蠕虫继续在企业内网横行
- 短网址服务被钓鱼网站利用，社交/支付网站用户谨防被骗

Malware 威胁概况

本季度 Anchiva 安全实验室共截获各类 Malware 约 200 万，比上季度大幅上升。木马所占的比例与上季度相比略有上升，仍占一半以上。其余依次为蠕虫、后门程序、间谍软件、风险软件和广告软件，传统病毒和其它类别所占比例与上季度没有变化。

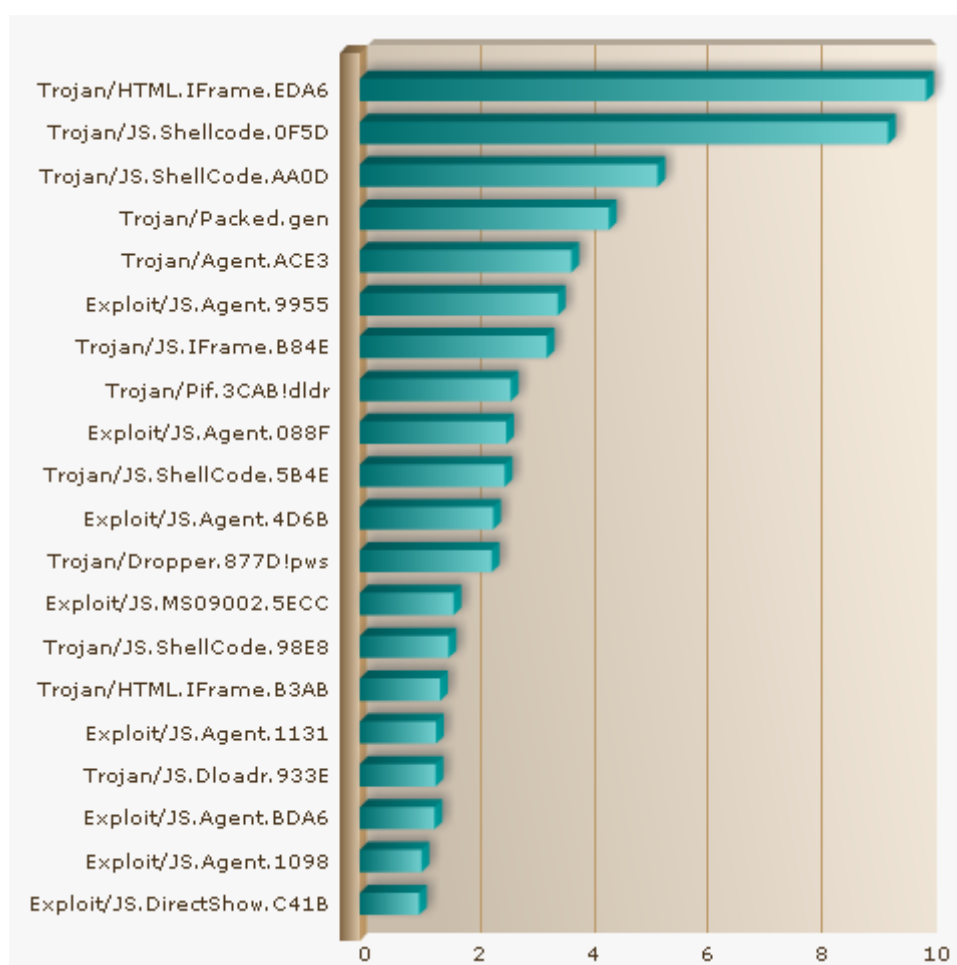
2009 年第四季度 Malware 类别比例图



Web Malware Top20

本季度的 Web 威胁中，网页脚本类占绝大多数，其出现频率最高的前 20 个 Malware 如下图所示。

Web Malware Top20



相较于第三季度，有些 Malware 依然很活跃，比如 Trojan/HTML.Iframe.EDA6、Trojan/JS.ShellCode.5B4E。Exploit/JS.Agent 和 Trojan/JS.Shellcode 两个家族活动非常频繁，分别在前二十中占了六个和四个席位。显示出当前流行的攻击方式依然是通过网页进行漏洞利用。这些 Malware 多数被挂马集团所利用，下载 Spyware、Banker 等木马，窃取敏感信息或进行系统破坏。拦截这些恶意脚本，可以有效的破坏其“挂马—下载恶意软件—造成破坏”这一工作链，从而减少损失。

Trojan/HTML.IFrame.EDA6: 该木马存在于恶意站点，通过其包含的隐藏 IFrame，利用相关漏洞，下载其它恶意软件。多见于挂马攻击中。

某客户中 Trojan/HTML.IFrame.EDA6 的部分拦截记录

date	name	url
2009-11-25 11:49:07	Trojan/HTML.IFrame.EDA6	rx0031.8866.org/xman/2.htm
2009-11-25 08:34:10	Trojan/HTML.IFrame.EDA6	fafa31.9966.org/nhll/6.htm
2009-11-24 13:47:42	Trojan/HTML.IFrame.EDA6	fafa33.8866.org/nhll/9.htm
2009-11-24 10:53:07	Trojan/HTML.IFrame.EDA6	fafa31.9966.org/nhll/6.htm
2009-11-24 09:58:13	Trojan/HTML.IFrame.EDA6	ft1114.3322.org/jj/4.htm
2009-11-24 09:29:44	Trojan/HTML.IFrame.EDA6	uuuuff.3322.org/nhll/7.htm
2009-11-23 17:39:52	Trojan/HTML.IFrame.EDA6	fafa33.8866.org/nhll/9.htm
2009-11-23 15:52:31	Trojan/HTML.IFrame.EDA6	uuuuff.3322.org/nhll/7.htm
2009-11-23 12:45:35	Trojan/HTML.IFrame.EDA6	fafa33.8866.org/nhll/1.htm
2009-11-23 02:41:09	Trojan/HTML.IFrame.EDA6	vava38.9966.org/dsq/6.htm

Trojan/JS.Shellcode.0F5D: 该木马利用系统漏洞, 或者 Adobe PDF 等第三方软件的漏洞, 执行任意远程代码。一般也是在挂马攻击中出现, 作为下载其它恶意软件的工具。

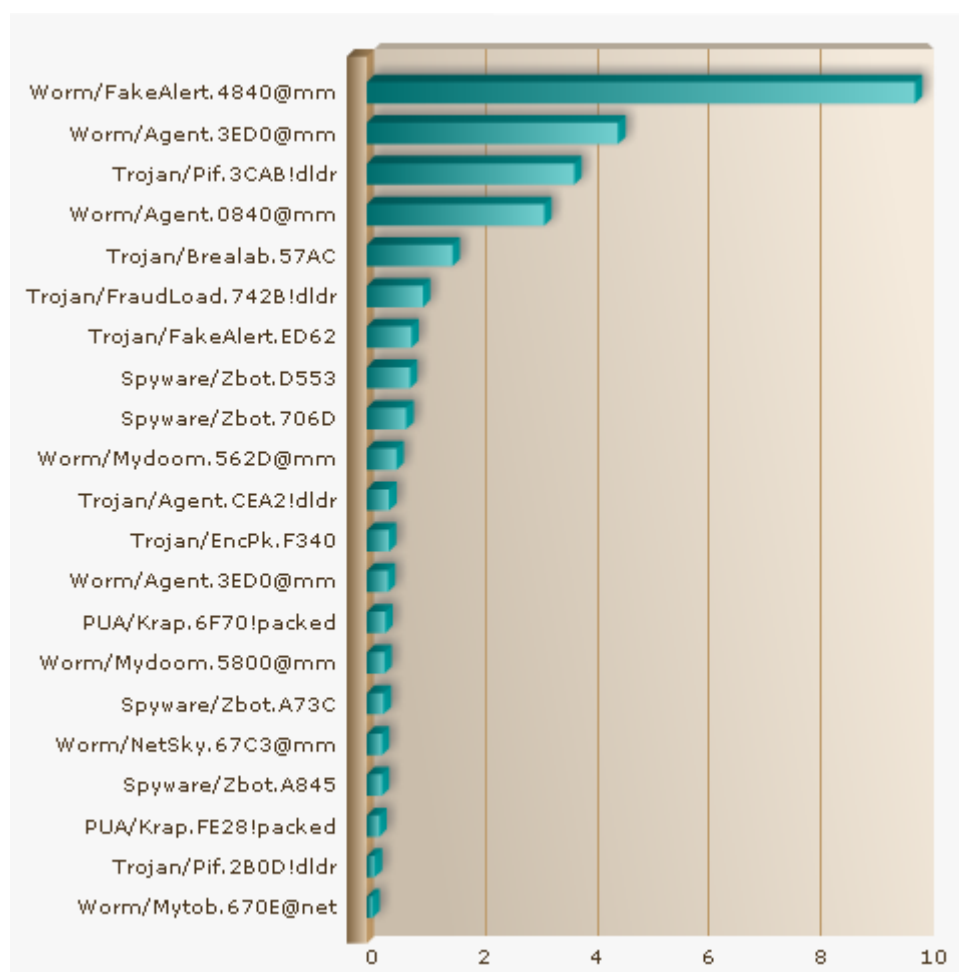
某客户中 Trojan/JS.Shellcode.0F5D 的部分拦截记录

date	name	url
2009-11-17 17:13:16	Trojan/JS.Shellcode.0F5D	871cc.cn/x123/lll.jpg
2009-11-17 17:13:09	Trojan/JS.Shellcode.0F5D	871cc.cn/x9/lll.jpg
2009-11-17 17:13:04	Trojan/JS.Shellcode.0F5D	abcd4.oicp.net/01/lll.jpg
2009-11-17 17:06:06	Trojan/JS.Shellcode.0F5D	871cc.cn/x212/lll.jpg
2009-11-17 17:04:46	Trojan/JS.Shellcode.0F5D	871cc.cn/x212/lll.jpg
2009-11-17 17:00:38	Trojan/JS.Shellcode.0F5D	img0.niupan.com/data/cache/lll.jpg
2009-11-17 16:58:20	Trojan/JS.Shellcode.0F5D	www.itonghui.com/html/88/lll.jpg
2009-11-17 16:44:13	Trojan/JS.Shellcode.0F5D	ii1122l.2288.org/05/lll.jpg
2009-11-17 16:29:51	Trojan/JS.Shellcode.0F5D	cnzz7.6600.org/aa/lll.jpg
2009-11-17 16:14:15	Trojan/JS.Shellcode.0F5D	ii1122l.2288.org/05/lll.jpg
2009-11-17 16:13:22	Trojan/JS.Shellcode.0F5D	ii1122l.2288.org/05/lll.jpg
2009-11-17 16:09:22	Trojan/JS.Shellcode.0F5D	871cc.cn/x76/lll.jpg

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



其中 **Worm/FakeAlert.4840@mm** 在本季度中从第三季度的第四位一跃上升到第一，显示出该蠕虫在第四季度依然很活跃。从一份美国联邦调查局发出的警告称，诈骗分子利用假冒的杀毒软件在 09 年获得了超过 1.5 亿美元的非法收入。从上图我们的统计也可看出，假冒杀毒软件的传播活动在第四季度的确非常频繁，计有 **Worm/FakeAlert.4840@mm**、**Trojan/FraudLoad.742B!dldr**、**Trojan/FakeAlert.ED62** 等三个变种，它们均位列前十。这些假冒杀毒软件通过垃圾邮件发送到受害者机器上，并诱使受害者打开、执行附件。随后它们会弹出一个假的警告，报告电脑中存在着恶意软件，并强制要求受害者注册，才能清除那些所谓的“恶意软件”。

假冒杀毒软件



某客户中 Worm/FakeAlert.4840@mm 监测统计



上图显示 10 月底 11 月初，我们针对 Worm/FakeAlert.4840@mm 在某客户环境中的部分拦截情况。它每天发送的邮件成千上万，而它仅仅是 Worm/FakeAlert 家族中的一个。所幸我们的客户已经得到很好的保护，不会受到该类恶意软件的威胁。

下列是本季度中新增的 13 个恶意软件，在前二十中占大多数。大部分是间谍软件、木马，用于窃取受害者敏感信息。

- Worm/Agent.3ED0@mm
- Trojan/Pif.3CAB!dldr
- Worm/Agent.0840@mm
- Trojan/Brealab.57AC
- Trojan/FraudLoad.742B!dldr
- Spyware/Zbot.D553
- Trojan/Agent.CEA2!dldr
- Trojan/EncPk.F340
- Worm/Agent.3ED0@mm
- Spyware/Zbot.A73C
- Spyware/Zbot.A845
- PUA/Krap.FE28!packed
- Trojan/Pif.2B0D!dldr

Worm/Agent.3ED0@mm: 这个蠕虫一旦运行，它会发送成千上万的垃圾邮件来传播。为了迷惑受害者，它会伪装成上司发出的通知邮件。

Trojan/Pif.3CAB!dldr: 这个木马是一个 PIF 可执行文件，通过垃圾邮件的附件传播。受害者运行后，它会生成一个 bat 脚本文件，并调用系统 ftp 命令，下载远程服务器上的其它恶意软件。

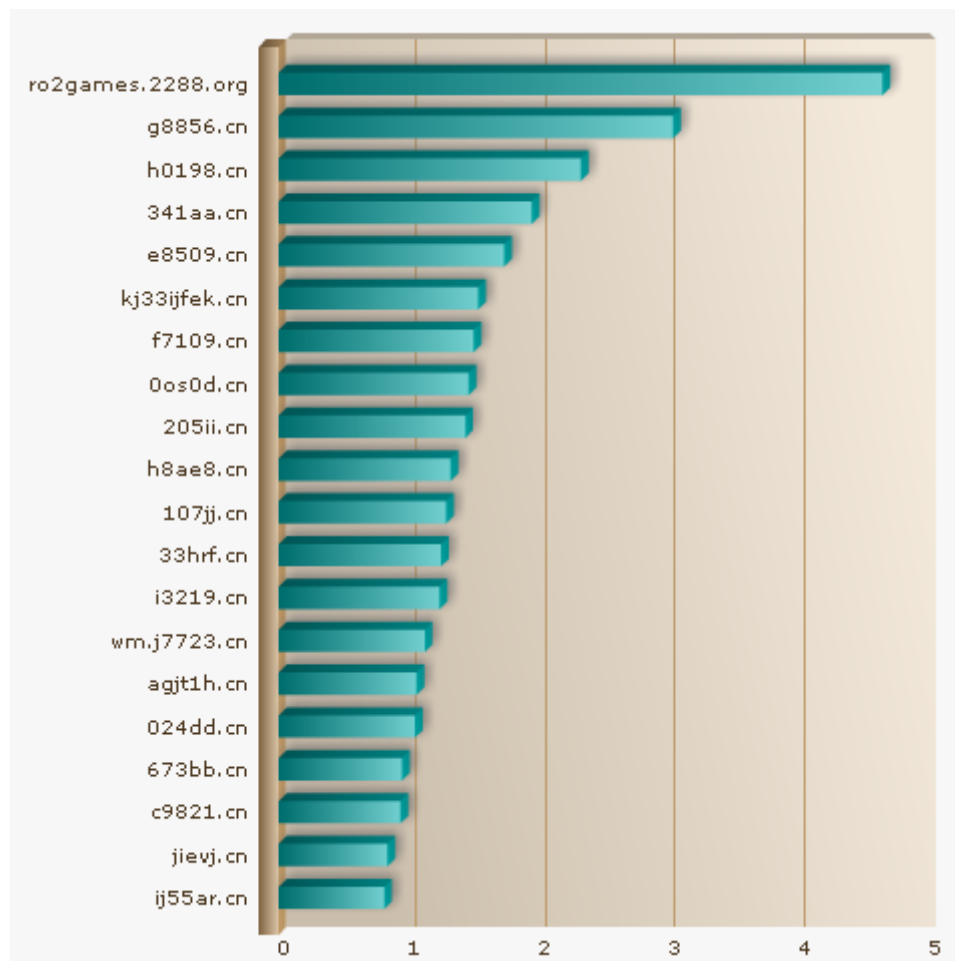
Trojan/Brealab.57AC: 这个木马可执行文件作为邮件附件发送、传播。它伪装成微软 Word 文档，诱使接收者打开该附件。运行后，它修改受害者的浏览器主页，安装一个 BHO（浏览器插件），并下载其它恶意软件。

Spyware/Zbot.D553: 这个间谍软件专门窃取个人网上银行信息。它通过垃圾邮件的附件传播，也可以通过其它恶意软件下载到受害者系统中。用户不小心运行后，它会隐藏在系统中，偷偷窃取受害者网上银行的帐号及密码等信息。同时，它会下载一系列的其它恶意软件，作为新的恶意软件的传播途径，从而为攻击者攫取利益。

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



前 20 位的恶意网站域名绝大多数都是“.cn”结尾。由于初期注册.cn 域名在国内比较容易，审核不严，后续监管不力，因而吸引黑客注册了大量的.cn 域名，专用于恶意软件发布、升级。随着 09 年 12 月后，中国互联网信息中心（cnnic）开始加强域名注册信息审核，个人注册.cn 域名将越发困难。可以预见该类恶意网站会逐渐减少。

大型社交网站 Rockyou 被入侵，3200 万用户信息被泄露

09 年 12 月份，国内外媒体争相报道了轰动一时的 rockyou.com 泄密事件。黑客通过 SQL 注入漏洞攻击 rockyou.com，窃取该网站 3200 多万用户的密码、个人资料等敏感信息，并把部分用户资料公布在网络当中。rockyou.com 的用户在注册帐户时，仅仅要求其密码多于五位字符，并不要求字母、数字及符号混合的强密码。它甚至不准用户密码中包含符号。rockyou.com 会提示用户输入第三方网站的用户名及密码，比如 facebook、myspace 等社交网站。而糟糕的是，用户们的所有这些密码、个人资料等敏感信息在数据库中并没有被加密，而是完全可见的。在这一系

列的错误之下，最终酿出被黑客入侵，用户信息被窃取恶果。

同时 SQL 注入作为一个成熟的技术，其所需的技术成本、门槛越来越低，而造成的危害却可以非常巨大、显而易见的。

研究者对 rockyou.com 泄露的密码进行研究发，使用频率最高的密码多数是一些有规律的数字或常用单词。而这样的密码如果在黑客的字典攻击下，将毫无安全可言，不用多少时间，黑客便可以暴力破解出来。

被公布的 rockyou.com 用户密码统计 Top20

passwords from the compromised database of RockYou.com
(password - percentage %):

1. 123456 - 0,8917%
2. 12345 - 0,2425%
3. 123456789 - 0,2355%
4. password - 0,1900%
5. iloveyou - 0,1583%
6. princess - 0,1081%
7. rockyou - 0,0693%
8. 1234567 - 0,0666%
9. 12345678 - 0,0630%
10. abc123 - 0,0538%
11. nicole - 0,0527%
12. daniel - 0,0503%
13. babygirl - 0,0494%
14. monkey - 0,0469%
15. jessica - 0,0465%
16. LOVELY - 0,0459%
17. michael - 0,0457%
18. ashley - 0,0439%
19. 654321 - 0,0429%
20. qwerty - 0,0425%

Adobe 零日漏洞

第四季度以来，用于零日攻击的 Adobe 漏洞如下：

- CVE-2009-3459
- CVE-2009-4324

以上两个漏洞都被挂马集团、定向攻击等所利用，通过邮件附件或者挂马者感染的网页来传播。在对受害者攻击过程中，它们一般释放或者下载其它恶意软件，来达到远程控制、窃取信息等目的。这类攻击一般比较隐蔽，受害者可能仅仅不小心点击了一个链接、打开了一个文档，而攻击者在释放、下载恶意软件的同时，一般会释放出一个其它安全的文档，以此麻痹受害者。

通过统计 Adobe 相关的 09 年 CVE 数目，我们发现总共有 100 个 Adobe 漏洞被上报。而随着 windows 7 的发布，在其底层安全框架越发完善的情况下，windows 平台上可利用的漏洞将越来越难以发掘。不难推测在不久的将来，Adobe Reader 等第三方的软件将越来越受到黑客的青睐，更多的 pdf、flash 等漏洞将被应用于攻击中。

下图是 Anchiva 某客户第四季度中截获的利用 PDF 漏洞进行攻击的部分实例。

利用 Adobe PDF 漏洞的攻击拦截记录

date	name	protocol	url
2009-12-14 09:26:01	Exploit/PDF.CVE-2009-0927.0D5A	http	c.8883.ss.la/4/sf.pdf
2009-12-10 16:19:39	Exploit/PDF.Pidief.EE3A	smtp	
2009-12-10 10:10:26	Exploit/PDF.Pidief.EE3A	http	65.129/att/GetAttachment.aspx?file=9a3c000d-4ff2-40a6-b2ca-deb146bd298.pdf&ct
2009-12-10 09:46:03	Exploit/PDF.Pidief.EE3A	http	64.49/att/GetAttachment.aspx?file=d6a2f39a-bf1e-46ab-9ddc-51d42f834b09.pdf&ct
2009-12-10 09:44:09	Exploit/PDF.Pidief.EE3A	http	64.49/att/GetAttachment.aspx?file=c44b2266-96a7-481a-9cd5-8007480764a2.pdf&ct
2009-12-10 09:44:05	Exploit/PDF.Pidief.EE3A	http	64.49/att/GetAttachment.aspx?file=691ac886-38bc-4d69-8d09-072f1e07e8f3.pdf&ct
2009-12-10 09:42:57	Exploit/PDF.Pidief.EE3A	http	64.49/att/GetAttachment.aspx?file=8513e40c-ce37-464d-8974-c77fbce6f98.pdf&ct
2009-12-10 09:42:31	Exploit/PDF.Pidief.EE3A	http	64.49/att/GetAttachment.aspx?file=449d2574-4f7f-4200-a0b5-55b4ca460b01.pdf&ct
2009-12-10 09:40:17	Exploit/PDF.Pidief.EE3A	pop3	
2009-12-09 19:06:46	Exploit/PDF.Pidief.EE3A	pop3	
2009-12-06 08:51:04	Exploit/PDF.Pidief.EE3A	pop3	
2009-12-04 14:35:48	Exploit/PDF.CVE-2009-0927.0D5A	http	fdgf22dg.6600.org/5/sf.pdf
2009-12-04 11:21:14	Exploit/PDF.Pidief.EE3A	smtp	
2009-12-04 05:13:52	Exploit/PDF.Pidief.EE3A	http	mail.ncku.edu.tw/cgi-bin/owmmbbox/openwebmail-viewatt.pl/%A4j%B3%B0%B8g%CO%D9%

微软 IIS 畸形文件扩展名绕过安全限制漏洞

微软 IIS 服务程序在解析文件扩展名时存在漏洞，对形如“malicious.asp;.jpg”的文件，将会以 ASP 文件方式在服务器上执行。黑客在攻击 web 服务器时，就可以利用该漏洞，上传 webshell，从而控制该服务器，造成破坏。微软认为这只是服务器权限设置缺陷，并不打算释放相应的补丁。我们建议不仅要按时打系统补丁，同时限制上传文件目录的可执行权限，以此来避免该类漏洞的利用。

畸形文件扩展名攻击实例



内网肆虐横行的 Conficker

Conficker 蠕虫传播途径很多，它可以通过 U 盘、RPC 漏洞、p2p 共享等方式在内网横行。一旦某台机器中毒，它会通过扫描的方式，在内网寻找有 RPC 漏洞、弱口令的 windows 机器。如果该机器还有外网 IP，它同时会扫描设定的外网 IP 列表，并伺机向外传播。因此发现某台机器中了该毒，必须马上断开网络连接，使用杀毒软件彻底查杀，再安装好系统补丁，才能彻底清除干净该蠕虫。

某客户内网中 Conficker 的部分拦截记录

time	url
2009-11-06 14:02:35	1 25:1789/yybxfib
2009-11-07 07:46:44	1 25:1789/bgncj
2009-11-09 10:14:25	1 216:5633/oyeyetav
2009-11-09 18:38:20	1 216:5633/oyeyetav
2009-11-10 10:29:29	1 216:5633/oyeyetav
2009-11-10 19:04:38	1 216:5633/oyeyetav
2009-11-11 09:18:43	1 .44:1279/gzvipe
2009-11-11 09:28:17	1 .44:1279/osucgao
2009-11-11 10:27:22	1 216:5633/oyeyetav
2009-11-11 11:48:43	1 .44:1279/wkedfiz
2009-11-11 21:01:05	1 216:5633/qomfbljs
2009-11-12 09:02:15	1 .44:1279/gaeh
2009-11-12 11:08:37	1 216:5633/qomfbljs
2009-11-12 21:27:19	1 216:5633/qomfbljs
2009-11-13 00:03:05	1 216:5633/qomfbljs

钓鱼网站

Twitter、facebook 等社交网络服务在 2009 年第四季度取得了更大的发展，用户数节节高升。人们通过它们交友、学习、聊天，甚至进行商业活动。而随着新浪微博客、twitter、facebook 等社交网络服务的逐渐流行，针对该类网站的钓鱼网站日渐增多。延续上一季度的威胁，淘宝、QQ 等国内网站依然是钓鱼者针对国内用户主要的攻击对象。

拍拍网钓鱼网站



某客户中拦截的社交钓鱼网站部分实例

time	host
2009-12-01 12:53:36	twitterrevlotion.com
2009-12-07 13:31:40	twitterrevlotion.com
2009-12-08 10:07:43	twitterrevlotion.com
2009-12-10 10:18:44	twitterrevlotion.com
2009-12-14 10:54:02	facebookchat.50webs.com
2009-12-14 10:54:02	twitterrevlotion.com
2009-12-16 14:17:06	myspacelogin2.rack111.com
2009-12-18 12:46:29	twitterrevlotion.com
2009-12-24 14:26:13	facebook-com-profile-id-548515.135.it

钓鱼网站可以通过仔细观察网站域名、网页上的内容、布局等来辨别。不要轻易点击邮件、聊天信息等发来的未知链接, 在提交个人密码、帐号、生日等敏感信息时, 也要确认安全才可以发送。随着短网址服务 (sinaurl.cn、tinyurl.com、bit.ly、tr.im等网站) 的盛行, 使得url在新浪微博、twitter等微博客服务中传播、分享带来便利, 但随之也带来不安全因素。黑客可以把url缩短以至无法辨别真伪, 用户点击就有可能下载恶意软件, 致使个人信息泄露, 从而造成不必要的损失。因此安全起见, 可以通过longurl.org之类的网址展开服务, 或者firefox中RequestPolicy插件, 来防范可能的钓鱼网站。

关于 Anchiva

Anchiva 成立于 2006 年 2 月，公司汇集了来自国内外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 Netscreen、Trend Micro、Fortinet、Cisco 等国际企业中担任过重要职务。到目前为止，公司在北京、杭州、台湾、美国加州设立了四个研发中心，拥有超过百位优秀的研发人员。并在北京、上海、广州、香港、台湾、San Jose 设有办事处，产品及服务遍及亚洲以及北美洲。

Anchiva 是 Web 安全网关的领先者，着眼于 Internet 应用安全领域，致力于高性能 Web 安全网关的研发，为企业提供整合反恶意软件、URL 过滤、Internet 应用控制、带宽管理、Web 服务器内容保护等诸多功能的 Anchiva 系列 Web 安全网关 (Anchiva SWG)，帮助企业防御网络威胁，加强信息安全管理，提高生产效率。

Anchiva SWG 采用专门为内容安全而设计的操作系统 AnchivaOS，在自主研发的高性能 ASIC 安全芯片的驱动下，打破了传统应用安全性能瓶颈，为企业提供实时、全方位的安全防护。Anchiva SWG 通过 ICSA 病毒检测认证，能 100% 覆盖流行病毒；同时通过 ICSA 性能测试，证明其全球领先的高性能特性。

Anchiva 拥有自己的 RapidRX 安全实验室，由经验丰富的病毒分析家和研究员组成，他们战略性的分布在美国，欧洲以及大中国区。Anchiva 特征库容量、覆盖率在业界遥遥领先，通过 Anchiva SWG 内置的 Malware 特征库可以找到多达 1000 万以上的威胁样本。RapidRX 安全实验室提供 24 小时不间断的升级服务，同时具有启发式扫描技术，确保用户网络随时处在最新技术的保护下，为了在最大限度降低误判的基础上提高查杀率，Anchiva 创新的开辟了多引擎的查杀技术。

Anchiva SWG 产品线分为高、中、低多个型号，覆盖用户由 100 人到 10000 人，为众多行业提供解决方案，客户覆盖金融、电信、教育、医疗、制造、政府、能源、零售等行业。

关于 Anchiva 安全实验室 (Anchiva RapidRX Labs)

Anchiva 安全实验室成立于 2005 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/>。