安全+
SECURITY
2009/07 总第005
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

揭秘RSA2009七大看点

DNS防护
—互联网安全中遗失的大陆

热点、焦点与观点：云安全与SaaS

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8668
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2009/07 总第 005

安全+ SECURITY+

目录 CONTENTS

RSA Conference全景扫描

国际拓展部 韩永刚

摘要：RSA Conference 已经有 18 年的历史。绿盟科技作为两度参加 RSA 盛会的中国厂商，将向国内同行全方位透视 RSA Conference 的前世今生。

关键词：RSA 安全 概览

作为信息安全领域每年最盛大的活动，RSA Conference 已经有 18 年的历史。RSA 大会就像安全界的奥林匹克，这里汇集了安全界最好的精英、研究机构、企业，成为了安全发展趋势的风向标。虽然每年都会在欧洲、日本分别举行，但其中最具影响力的，还是在旧金山举办的 RSA 大会。绿盟科技作为两度参加 RSA 盛会的中国厂商，将向国内同行全方位透视 RSA Conference 的前世今生。

大会起源

RSA 是信息安全中一个非常著名的公钥加密算法，1977 年被发明，以该算法的三位发明人 Ron Rivest、Adi Shamir、Len Adleman 的名字命名。该算法是目前 IT 系统中应用最为广泛的非对称算法。而 RSA 亦是美国一家著名的信息安全公司的名字，目前是 EMC 旗下的一个分支。RSA conference 自 1991 年开始由 RSA 公司主办，最初作为密码专家的论坛，用于分享在互联网安全方面的最新技术与知识。经过 10 多年的发展，逐渐成为全方位覆盖信息安全各领域的专业盛会。

会议议程

RSA 大会一般历经 5 天，分为展会与会议两个大部分，也在相隔一街的两个会展大厅进行。一边是逾期 3 天的市场气息较浓的厂商展览，而另一边则是学术气息主导的会议。其会议部分的设置也相当专业，分为：主题演讲（Keynote）、专业论坛（Track Session）、业内同行论坛（Peer2Peer Session）、创新沙盒（Innovation Sandbox）等。

1）主题演讲（Keynote）

汇集了来自全球安全界一些重量级人物对于安全在技术、市场、热点问题方面的观点，比如今年，Cisco 总裁 John Chambers、RSA 总裁 Arthur W. Coviello、Symantec 总裁 Enrique T.Salem、RSA 实验室的首席科学家 Ari Juels、McAfee 总裁 Dave Dewalt 等都进行了演讲。

2）专业论坛（Track Session）

RSA 上各领域安全专家最为关心的板块，专业论坛又细致的分为了 10 多个领域，包括:

1. 应用与开发	9. 黑客与威胁
2. 安全商业	10. 主机安全
3. 加密	11. 热点问题
4. 企业安全服务	12. 网络
5. 精选会议	13. 物理安全
6. 治理（Governance）– 法律	14. 研究成果发布
7. 治理（Governance）– 企业与政府	15. 战略与架构
8. 治理（Governance）– 风险与合规性	

这样细致的领域细分研讨，必然使得各领域专家都能够找到各自专注的方向。当你穿梭于各个分会场，可能只会恨自己分身乏术。RSA 2009 中，物理安全（Physical Security）与安全治理 - 风险与合规性（Governance – Risk & Compliance）两项，是今年新增加的议题。这 10 多个领域，总共 240 余个研讨中，又被分成了高级、中级、未分级别三类。高级研讨的演讲者需要在这个领域具备 10 年以上的经验，研讨中更多的讨论深度架构、代码、工具等内容，涉及的内容也更具学术性，很少涉及背景知识。而中级研讨会专注在引入一些概念、定义，介绍一些架构等，演讲者也需要有 5 年以上的行业经验。而未分级的部分则往往介绍一些新兴的技术领域。

3）创新沙盒（Innovation Sandbox）

RSA Conference 的特色，这个分会场利用一个下午的时间，引入了 10 家新兴的小公司的创新技术。他们给我们带来了新的创意、新的概念。这里的技术无所谓大小优劣，只要你够创意，并有较好的市场或技术前景，就可以在这里一显身手。而且最终的这 10 家候选企业，也得到了一个直接面对业内专家、媒体以及他们最迫切需要的风险投资者。通过他们一个下午的展示、5-10 分钟的演讲，来阐述他们的创新与产品。最终打动专家组的公司，会获得当年的 Innovation Sandbox Award 奖项。这也意味着这家公司找到了更好的发展机会。

4）同行论坛（Peer2Peer Session）

这个论坛给了某些专业领域的同行近距离接触的机会。一般每个议题，只有 20 多席的座位，采用先到先得的方式，使得关心此专题的人士可以有一个封闭的，面对面的深入交流的机会。

除了这些公开的论坛，更有一些小范围的特殊 workshop 讨论，如女性安全从业者论坛，使得活跃在信息安全行业中的聪颖的女性们能够借 RSA 大会的机会一同聚会。这些 workshop 也使得在 RSA 大会的主框架上，点缀了更多的有趣环节。

虽然绿盟科技已经参加过很多世界各地的安全展会，如欧洲的 Inforsec、日本的 Interope、新加坡的 CommAsia 等，但 RSA Conference 却是不同的，不同就在于“专业”。每年 RSA 会议都能吸引到世界上安全相关领域中最好的专家。虽然 RSA Conference 中的展会部分是世界最大规模的，但 RSA Conference 真正的主角却是密码专家、安全技术专家、各安全公司的 CEO 与 CTO、来自大学与研究机构的学者们。正是他们的精彩演讲与技术讨论，才奠定了 RSA 的峰会地位。聆听各领域专家的声音，再加上宽松的交流环境，使得身临其境的参与者都能满载而归。三、四天的会议往往能够回味很久，甚至很多新创意、新技术、新产品也就此应运而生。置身其中，你能切身体会到信息安全的前进脚步与魅力。

RSA 2009参展厂商速递

产品市场部 王伟

摘要：2009 年 RSA Conference 参展商数量减少到了大约 325 个，但还是引入了一些新的板块和议题吸引参与者，如 INNOVATION SANDBOX、物理安全和其他与安全相关的热点讨论，参与这次展览的厂商涉及到从 Physical Security、IT Security 到 Policy Compliance 的方方面面。

关键词：RSA 参展商 热点

RSA Conference 一直都是全球信息安全产业的年度盛会，历年来的会议议题都涉及到当时信息安全行业的热点及趋势性问题的分析和讨论。今年，RSA 会议区域副总裁兼总经理 Sandra Toms LaPedis 表示，一年一度的安全会议规模扩大到了 17 个环节和 240 个会议。不过由于今年受到全球经济的影响，2009 年会议参展商数量减少到了大约 325 个。

绿盟科技是第二次以参展商的身份参加此次产业盛会。今年的会议在细节方面比 08 年略有缩水，但是主办方为保持 RSA 这个盛会的含金量，还是引入了一些新的板块和议题吸引参与者，如 INNOVATION SANDBOX、物理安全和其他安全相关的热点讨论。

总体来看，各大主流厂商都在本次展会上亮相，如微软、IBM、Oracle、Symantec、McAfee 等具备综合性优势的厂商无一缺席，而 BARRACUDA、Fortify、NARUS、IMPERVA、Qualys、Websense、TippingPoint、Radware、Bluecoat 等专注于细分专业领域的安全厂商也继续展示着各自的核心产品或最新解决方案。在展会的每个研讨环节和各个机构的展台上，安全行业的各方精英们也充分展示着自己非常专业的一面，积极与同行们讨论最新的话题，切磋最近的技术心得。

参与这次展览的厂商涉及到从 Physical Security、IT Security 到 Policy Compliance 的方方面面。在主办方印发的名录中，根据各个厂商提供的解决方案、安全产品或服务的定位不同，325 家参展厂商被分为 73 个类别，产品线丰富的厂商自然曝光率更高一些。

绿盟科技对参展厂商的类别做了一个分析，发现安全市场的焦点定位在企业市场的应用安全领域，而合规性的市场也渐渐成为重点关注的领域。在传统的安全市场领域之外，某些新的领域也吸引了不少厂商的眼球，诸如 Cloud Computing、Physical Security、Virtualization、Software Code Vulnerability Analysis 等。我们对各个产品领域中参与厂商的数量进行了统计和排序，如图 1 所示。

图 1

值得关注的是，WEB 应用安全相关产品或服务领域注定是近年来一个持续增长的安全市场，这已经形成了一个明显的增长趋势。不仅参与的厂商更多，而且扮演的角色也越来越细分化。从应用开发的代码审计工具开发商，到 WEB 应用上线前的安全评估服务商；从应用保护的产品和解决方案提供商，再到本身虽不开发产品而仅利用第三方成熟产品做 SaaS 运营的增值服务运营商，有关 Web Application Security Lifecycle 的各类角色形成一个完整的解决方案链。这不仅说明这块市场的巨大吸引力，同时也证明了占据信息安全技术发展主导地位的北美同行们的精专程度，另外还反映了这些国家给这些靠技术吃饭的商业公司提供了一片生存和成长的沃土，这在国内有的时候是难以获得的，国内外的大环境对厂商的生存发展还是有非常大的影响。我们希望国内的生存环境随着行业的不断发展变得越来越好。

经济危机下的RSA 2009

决策委员会 吴云坤

摘要：绿盟科技已经是第二次参加 RSA 展会，也是这次所有参展的三家中国厂商中展位最大的，由于其强大的技术研发实力和中国经济在世界上不断攀升的地位，很多参展厂商都非常关注“NSFOCUS”这个品牌，甚至某些还没有进入中国的硅谷公司已经将我们列为竞争对手，也许这是有些缩水的 RSA2009 下另一道亮丽的风景!

关键词：RSA 安全公司 参展厂商

时差还没有完全倒过来，加上严重的热伤风，让 RSA 之行的第一夜并不安稳。清晨起来洗漱，发现去年酒店还提供的牙刷、牙膏和拖鞋，今年已经通通被“裁员”了，是否又是经济危机下节省成本之举呢？

步行去 Moscone Center，熟悉的街道，熟悉的店铺，只是 Apple Store 里没有了去年的人头攒动，挂在 Cable Car 上的人也少了很多，不过街上的行人依然在享受着阳光，即使是在星期一的工作日。思忖间，抬头发现到了 Moscone Center，这个已经有着近 18 年的全球安全展会已赫然眼前，这也是绿盟科技与之第二次相会。

Check in 的过程比去年更加自动化，通过电脑自助输入自己的名字和公司，确认按钮之后，在 Registion 那里已经现场打印出了参展商的身份卡，整个过程不超过 20 秒，确实高效。继续往下走，映入眼帘的已是各大厂商的展台，一家家浏览过去，世界级的厂商一个都不少，还发现了很多以前未曾听说过的厂商，第一次来 RSA 的同事感叹：原来做安全的公司这么多！也许这就是硅谷的魅力吧，不断有新的公司创建，推动着整个市场和技术的发展。

RSA2009，也有一些变化。首先，展商的数量明显减少，以前展位基本利用了展馆边边角角的位置，今年却空旷了很多，据 RSA 组织者介绍，2009 年参展商数量减少到了 325 个；其次，厂商的展台设计明显比 2008 年简洁和节省。想起去年赛车、攀岩等大手笔的展台设计，今年没有特别奢侈的“亮点”。有个展台上甚至打出了这样的标语：“No frills, No big booth, We are saving money and we will show you how.”；第三，RSA 展会还增加了一个环节，帮助因经济危机下岗的安全专业人员参加展会，同时还举办研讨会，提供工作机会信息并允许雇主搜索简历。

展会看点也是异彩分呈。从鼓励创新的 Innovation Sandbox 环节，到扩增至 240 个专题的会议群，以及新增加的物理安全和 IT 治理的热点，无不是年度最大信息安全展带给全球的新气息。

绿盟科技已经是第二次参加 RSA 展会，也是这次所有参展的三家中国厂商中展位最大的，由于其强大的技术研发实力和中国经济在世界上不断攀升的地位，很多参展厂商都非常关注“NSFOCUS”这个品牌，甚至某些还没有进入中国的硅谷公司已经将我们列为竞争对手，也许这是有些缩水的 RSA2009 下另一道亮丽的风景!

创造性合作(Inventive Collaboration)

—RSA执行总裁指明安全未来方向

国际拓展部 韩永刚

摘要：在 RSA2009 的开幕主题演讲中，来自 RSA 公司的执行总裁 Art Coviello 发表了他的观点：“创造性合作（inventive collaboration）”。Coviello 认为目前在数字犯罪（cyber criminal）方面，攻击者已经以利益为链条联系了起来，以合作的方式来设计和实施各类攻击，形成了他们自己的价值链。而信息安全方面的各类组织、企业、专家学者等，也应该采用合作的方式来应对，这样才能够确保不落后于攻击者，更好地保护公众的利益。

关键词：RSA2009 Art Coviello 未来方向

在RSA2009 的开幕主题演讲中，来自 RSA 公司的执行总裁 Art Coviello 发表了他的观点：“创造性合作（inventive collaboration）”。Coviello 认为目前在数字犯罪（cyber criminal）方面，攻击者已经以利益为链条联系了起来，以合作的方式来设计和实施各类攻击，形成了他们自己的价值链。而信息安全方面的各类组织、企业、专家学者等，也应该采用合作的方式来应对，这样才能够确保不落后于攻击者，更好地保护公众的利益。在他的主题演讲 “A Common Call: Architecting a New Information Security Landscape” 中，他呼吁用户、政府机构、信息安全企业等各方面力量，都能够联合起来应对网络与数字威胁。

演讲的最后，Art Coviello 还邀请了 Cisco 副总裁以及微软 Trustworthy Computing 的负责人，副总裁 Scott Charney 共同进行了讨论，来说明合作的重要性，以及三个公司在这方面的努力方向。在随后微软 Scott Charney 的主题演讲 “End to end Trust: A Collaborative Effort” 中，阐述了微软在近几年所努力搭建的新的安全体系架构模型，并指出了在模型中，微软与相关公司的合作。

在三位安全界重量级人物的阐述过程中，也有人问到，这种合作是否只是安全巨头之间的。演讲者也指出，合作需要是全方位的，而不仅仅是限于大公司之间。其实从绿盟科技的角度，我们也是非常赞同这点的。绿盟科技 2009 年加入与微软 MAPP（Microsoft Active Protections Program）项目进行合作，成为中国第一家加入 MAPP 项目的合作伙伴，从中绿盟科技可以提前获得有关微软月度安全公告的信息以评估所造成的威胁，并为绿盟科技与微软共同的客户提供更及时的保护。

除了关于创新合作方面的动向，今年的 RSA Conference 还有很多热点问题，比如各个专业论坛都对云计算（Cloud Computing）与 SaaS 中会产生的安全问题非常的关注，大家都在讨论此领域中的安全问题是否能够得到很好的解决，这可能将会极大地影响云计算与 SaaS 模式是否能在企业中得到普及与应用。

其他的方面，比如新型 WEB 攻击技术、虚拟化的安全、移动安全、如何提高性价比同时降低成本、基于信誉（Reputation）的安全机制、策略与合规性以及如何使安全更为贴近业务目的及工作流都是此次会议中关注的热点。

百家争鸣　百花齐放

—RSA Conference Keynotes 纪实

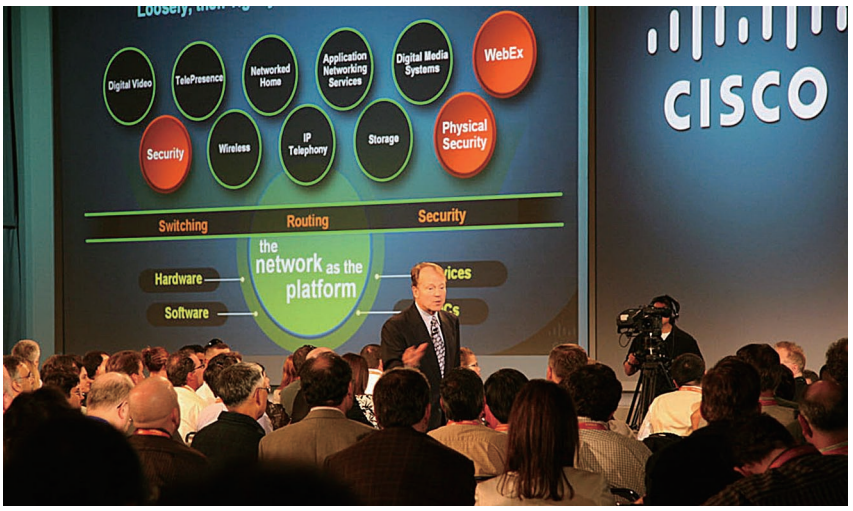
决策委员会 吴云坤

摘要：Cisco 介绍了在网络安全方面的战略、McAfee 分析了新型的攻击场景以及现阶段防护的思路、TippingPoint 专注在如何更灵活的设置 Policy 等一些技术上，RSA2009 的技术演讲引人入胜。

关键词：RSA2009　安全厂商　动向

错过了昨天的 keynotes，所以今天有机会去北馆听演讲特别珍惜。走进了大厅，被震撼了一把，不但是因其先进的硬件条件，更在于整体的风格和流畅的过程，每次演讲之后的广告或是介绍不仅精美而且艺术，和 Keynote 有机成为一个整体。虽然我去迟了一会，但是刚刚赶上了老钱同志的开始。

坐下赶紧仔细细听，钱伯斯延续着思科的风格，大气而沉稳，且不乏和台下的观众互动。首先钱伯斯提出了我们面临的三个主要问题：1）如何使用技术手段对攻击进行防护；2）我们访问的资源哪些是可信的；3）如何“好东西”进而“坏东西”出呢？在提出三个未来我们可能面临的安全问题之后，钱伯斯高举高打，从 Vision、Strategy 和 Execution 三个角度提出了思科在网络安全方面的战略，不仅给出了 12~18 个月的具体行动计划，还给出 2~4 年和 5 年以上的建议，印象最深的还是那“Network Becomes the Platform for Security”的口号，其实这就是 Cisco 基于其强大的核心竞争力在安全方面提出的宏图大略。随后，钱伯斯细数了思科 1999 年到 2009 年的成长历史，包括期间与竞争对手之间实力对比的变化，心里赞叹之余想到，或许只有这样心有多远的公司

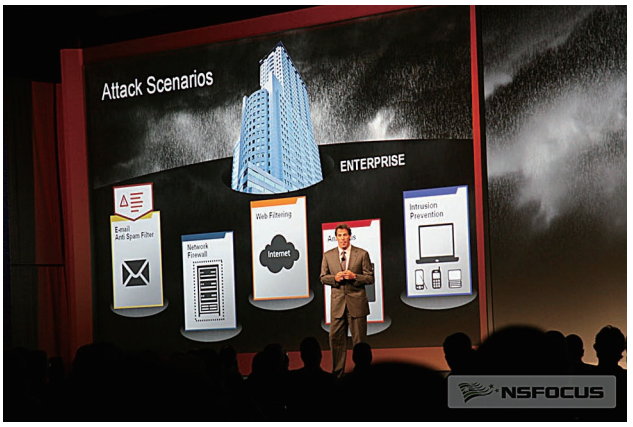


才能走的真正的长远吧。

与思科这样传统的网络厂商相比，McAfee CEO 的演讲更加偏重于老牌安全厂商的风格，专注而严谨。从美国经济危机开始，发现就业机会在下降、道琼斯指数在下降、消费者的信心指数更在严重下降，但是与之相反，08 年的恶意软件数量在上升、联邦贸易委员会的投诉在上升、数据破坏更在大幅攀升，不管是上升还是下降，都造成了万亿美元的损失。与 Cisco 的高屋建瓴不同，McAfee 分析了新型的攻击场景以及现阶段防护的思路，最后给出了 Cybersecurity 需要 Multi-Layered、Multi-Correlated 和 RealTime Visibility 的结论。也许和 McAfee 一样是专注于安全的公司吧，绿盟这么多年一直与这样的大公司保持着持续的交流与合作，它提出的一些新理念或是研发的产品都在安全行业有着启发性的效果，也是我们不断努力的方向。

紧接着 McAfee 做演讲的是 IPS 领导厂商 TippingPoint，与前两家公司都不同，演讲者是其博士 CEO，因为长期钻研于技术吧，所以更加的平易近人，没有西装革履，也没有太多的言辞修饰，甚至还会紧张的忘记了演讲中的下一个话题，但是他的演讲却非常精彩。尽管 TippingPoint 的 IPS 产品已经做得非常好，但是并没有宣传很多空洞的概念，而是专注在如何更灵活的设置 Policy 等一些技术上，深刻地体现了 TippingPoint 的风格。绿盟科技目前已经在国内成为第一大 IPS 产品供应商，也时常与 TP 竞争，对于这样尊重技术并持续研究的对手，心里不由升起一股敬意。

RSA 第三天的旧金山，天气转凉，听完 Keynotes 的我们走在夕阳下的 Market Street 上，海风拂过，几分快意。RSA Conference，魅力已经持续了十八年，不仅因为这里有最新的产品技术，有众多理念绽放，更因为这群 Focus On Network Security 的人们。



揭秘RSA 2009七大看点

决策委员会 吴云坤

摘要：介绍 RSA Conference 2009 中一些令人难忘的看点。

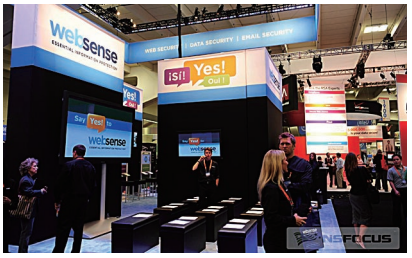
关键词：RSA2009 web 安全 看点

IBM ISS 总经理的 Keynotes 还没有听完，发现已是 15：40，迅速赶回展台撤展。八个大小伙子三下五除二就把一堆展架收拾妥当了，眼前的一堆箱子仿佛静静地告诉我们，2009 RSA Conference 已入尾声。

与三藩逐渐转凉的天气相反，RSA 这几天带给我们的兴奋越来越多。从第一天的 Innovation Sandbox，到后来的 Keynotes；从与 McAfee 科学家的交流，到 North Hall 中倾听钱伯斯关于 Cisco 的长远计划；从展台上送出的第一份中国特色的礼品，到 imperva 厂商代表认出绿盟后直说”You are our competitor!”，每一步的画面都历历在目。与往年 RSA Conference 相比，以前一些 Crossover 的厂商今年选择了放弃，让今年的安全味道更加浓重。

收拾完行李，放松心情，整理一下纷乱的思绪，发现 RSA Conference 2009 中一些令人难忘的看点：

1）WEB 安全成为热点



WEB 不仅在国内，乃至在全球都是热点问题，由于 WEB 成为获得各类信息和服务的主要应用方式，所以其蕴含的价值也越来越高，吸引了攻击者足够多的视线。这次众多厂商都提供了保护 WEB 安全的解决方案、产品和服务。从 WEB 应用的网关级防护，到 WEB 安全漏洞的扫描，WEB 内容的安全审计，甚至 WEB 应用的安全生命周期管理等等，覆盖面之广，足见 WEB 安全的重要性。

2）身份管理长盛不衰

今年展会上的另一个热点就是身份管理，随着电子商务和企业应用的日益广泛，加上各类信息终端的出现，身份问题成为应用安全中的一个焦点，不仅各家展商提供了软件型的解决方案，而且展会上新出现了许多提供硬件方案的厂商，Ukey、智能卡，包括软硬件结合的方案都是值得关注的看点。

3）云安全与 *aaS

虽然今年专注在云安全的厂商只有 5 到 6 家，但是几乎每个大型厂商都在强调云安全。一方面大家非常关心云计算的自身安全问题，尤其是云计算下的数据安全；同时大家都涉及到了如何借用云计算的思路开展诸如 SaaS、PaaS、IaaS 等的多种新的安全业务模式，热点必然带来了争论，有些专家甚至戏称“云计算”不如叫做“沼泽计算”，意指一旦选择云计算，由于其安全问题必然导致不可自拔的境地。

4）合规性无处不在

合规性是几乎所有展商都会提到的一个问题，不仅从商业逻辑层面合规性成为焦点，体现国家意志的政府机构也无一例外地将合规问题作为未来安全中最为重要的一个领域进行研究。此次展会上不仅有独立提供合规性咨询和产品的厂商，更多的是在其安全产品中逐步体现各领域合规性要求的产品，这种趋势在 Keynotes 的各类演讲中也无处不在。

5）Malware 成为缺省

展会上并没有独立的 Malware 防护产品，但是几乎每一种产品都宣称具有 Malware 处理的能力，不论是发现，或是阻断还是消除。与国内不同，美国安全市场对 Malware 的认识非常实际，虽然有类似于 Sandbox、云安全等新的手段，他们都很清晰的知道对抗 Malware 没有完美的方案，用户也非常理性的选择所需要的产品，而没有把 Anti-Malware 当作全部。

6）网络安全和社会安全

此次展会大家已经不再讨论单纯的网络安全，社会安全的意义提到了更高的层面，所谓 Malware 或是 Web 攻击，这些威胁的真正奏效都应用了大量社会工程学的方法；另一方面，国家对于安全的重视程度在不断提高，美国政府这次多个机构的参展以及 Keynotes 中对于网络战、信息监控的话题都体现强烈的国家意志。不仅如此，在谈到对于未来攻击的防护问题时，更多的学者和厂商都开始关注如何借用社会学的方法，如协同、关联等来构建新的防御体系。

7）实用甚于概念

今年 RSA 展会是在经济危机背景之下召开，自始自终都没有一个厂商推出新的概念，不论是展会还是 Keynotes，大家都在冷静思考用户真正需要的东西，类似于国内炒作甚火的 UTM 概念，在国外而言都认为是不切实际的解决方案，大家更多在考虑如何利用 IPS 或者下一代基于应用的防火墙产品来保护自己的网络和应用。同时在硬件上也没有像往年推出更高更快更强的产品，一方面受限于硬件投资和收益的难于平衡，更重要的在于应用和内容安全的处理需要极强的灵活性和可变性，而软件较之硬件具有更多的优势。

拉拉杂杂地想了很多，三天的行程似乎沉淀了一些，但思考中依然有很多混乱，虚拟化技术、物理安全，还有安全管理，在脑海中忽闪忽现。不知觉已步出了 Moscone Center，旧金山普通的一天又将结束，也让这群热爱安全的人与你挥手告别了，绿盟科技——这个来自东方文明古国的安全公司，明年还会与你相遇 ~~~

RSA Conference花絮集锦

决策委员会 吴云坤/研究部 左磊

摘要：国外的展会与国内的展会还是非常不同的，虽然是专业的安全展会，但是不尽都是技术氛围，其间很多轻松和快乐的元素弥漫在展会的每个角落，席间构思精巧的各类展出手段值得称道，而展会上的人又是另一道亮丽的风景。

关键词：RSA2009 展会花絮

国外的展会与国内的展会还是非常不同的，虽然是专业的安全展会，但是不尽都是技术氛围，其间很多轻松和快乐的元素弥漫在展会的每个角落，虽然 2009 年的 RSA Conference 没有往年展会经常出现的一些大手笔设计，或许是因为受到了经济危机的影响，但是席间构思精巧的各类展出手段却值得称道，而展会上的人又是另一道亮丽的风景。

花絮之一

大部分参展的公司都是欧美公司，绿盟科技是为数不多的中国公司。在展会上提供的纪念品是一个刺绣的工艺品，可以折叠为一个小的容器。由于带有中国文化特色，受到很多参观者甚至参展商的追捧，有一家从事邮件安全的厂商代表还拿容量为 4G 的 U 棒来与我们进行交换。

花絮之二

为了提高人气，各家安全厂商各显奇能，ArcSight 居然把 SMART 汽车也摆出来作为奖品吸引眼球，据说这是展会的参与者奖品，大家纷纷热议，如果“不幸”获奖，该如何开回中国？原来梦也可以这样做。

花絮之三

梭子鱼公司今年和去年一样，依旧开了一辆车到了展厅里面，不过今年是大卡车。最酷的是，梭子鱼公司每年都租一辆车，全身涂满

了梭子鱼的广告，围着场馆绕着圈地开，每次出去呆一会都看的眼晕，真是把营销做到了极致。

花絮之四

去年有开赛车的游戏，六辆游戏厅的大型赛车一字排开，美女促销陪你赛车。今年明显受到经济危机影响，展馆里没有了赛车，换成了打地鼠游戏，不仅占用空间小了很多，也符合绿色 IT 的趋势呀!

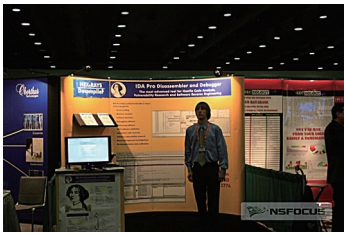
花絮之五

相对于打地鼠的暴力运动，场馆中也不乏智力型游戏，IT 和游戏的结合目的只有一个：吸引你的眼球，不知道明年会不会有“连连看”或者是“找不同”呀!

花絮之六

远亲不如近邻，虽然相隔大洋千里，但是在 RSA 上却成为了邻居。绿盟科技展位正对面就是 Tenable 公司，大家熟悉的 Nessus 扫描器就是他们的产品，他们也算是网络安全届的元老级产品了。

花絮之七



最著名的反编译软件 IDA Pro 也参展了，这是长期专注于漏洞分析和漏洞挖掘的绿盟再熟悉不过的工具了。年轻的展商代表在镜头前不知道是显得有些拘谨还是要摆出一副和招贴画中人物一样的 pose，说老实话，他可比那个头像帅多了。

花絮之八

最近国内流行魔星刘谦，没想到 RSA 展会上也见到了高科技的魔星。Fortify 公司从拉斯维加斯专门请来了魔术师来进行魔术表演，表演结束还把道具送了一个给我们，向我们揭示了其中的

奥秘，然后告诉我们：每个魔术都有漏洞。难道 Fortify 今天也能发现魔术中的漏洞呢?

花絮之九

三百六十行，展馆里快全了，这不，Radware 公司的代表已经兼职干上大夫的活了，工具还挺全，白大褂、听诊器一应俱全，开始问诊了。这一看就知道是西医!

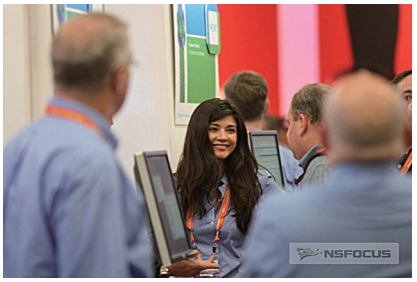
花絮之十

本以为又是一家诊所，回头一看打扮，发现像是生物学家，研究细菌的，再问问，原来发现是做数据恢复的厂商。他们正在演示破坏并恢复硬盘数据，带着口罩和玻璃罩是不是担心暴力破坏的时候有螺丝钉误伤群众和自己呀!

花絮之末

谁说安全界无美女，各大厂商都有自己看家的人选，长的美那叫天生丽质，关键是人家通过后天努力进入了安全界，让 RSA Conference 多了一丝柔美。选几位美女代表作为花絮的结束。

Tippingpoint 公司的美女代表



CA 公司的美女代表

与DNS DDoS搏斗 绿盟科技在行动

行业营销中心 卢联强

摘要：5月下旬国内发生了一起重大网络安全事件，绿盟科技在此次事件中凭借丰富的经验与周密的服务体系，协同各地客户在最短的时间内完成了对异常情况的处置工作。

关键词：DNS DDoS 绿盟科技

5·19 断网事件，网络安全警钟再响。5 月 19 日晚 21 点左右，中国出现大范围网络故障。江苏、河北、山西、广西、浙江、天津、内蒙古、黑龙江、广东等省份均有网民反映上网遭遇故障，出现打不开网页等问题。据工业和信息化部通信保障局发布的最新公告，确认该事件原因是暴风网站域名解析系统受到网络攻击出现故障，导致电信运营企业的递归域名解析服务器收到大量异常请求而引发拥塞。

在此事件发生的第一时间，绿盟科技作为网络安全厂商，伴随客户度过了惊心动魄的两小时，上演了一场与 DNS DDoS 搏斗的精险实战。

临危受命

5 月 19 日晚 9 点半左右，绿盟科技的安全专家小林正在回家的路上，出于职业习惯，小林路过广场旁边的几个网吧时，下意识地把视线扫了过去，现在应该是网吧人满为患的时候，但今晚有些异样：有的网吧没什么人，有人的网吧则是人声鼎沸，群情激愤，大家在嚷着什么？！

突然，急促的手机铃声打断了小林的思路，来电显示：某电信工程师。小林急忙接通电话，局方工程师非常焦急地说：“我们的网络出现重大故障，请马上赶到电信机房”。小林急忙调转方向赶过去，此时电信机房门口工作人员正焦急等待，小林一下车马上与他们赶往运维中心。

互联网危机四伏

进入运维中心首先经过客服中心，客服中心的电话此起彼伏，客服人员经常重复的几个词就是“网页访问特别慢”、“邮件无法接收”、“无法上网”。进入运维中心，发现里面灯火通明，监控中心网络、系统、业务技术专家都在现场，运维中心主任一脸严肃。人员到齐后，主任召集各条线的技术人员开了一个紧急会议，对当前问题做了总结。网络组技术人员反馈：网络设备 CPU 利用率、数据流量没有异常；系统组技术人员反馈：RADIUS 服务器工作正常，宽带客户认证授权正常；业务组人员反馈：城域网大面积出现宽带用户访问网页速度慢、无法上网现象。

小林一边迅速记录着网络的现场数据信息，一边与绿盟科技总部的技术支持中心联系，此时绿盟科技的另两位同事已经赶到了运维中心。

应急团队在响应

与此同时，绿盟科技总部技术中心也是一片忙碌。在当晚九点左右，总部就陆续接到华南、华北、华东等地分支机构的汇报，称运营商互联网出现故障，部分互联网用户的服务受到影响。鉴于此次网络故障影响范围广，技术支持中心立即向应急响应团队经理报告了情况，经过对现有数据分析发现这是一起重大的互联网安全事件，马上通知全国各地分支机构技术专家迅速组建应急响应团队，为各地随时可能出现的安全问题进行准备。

重大转机

运维中心现场人员在分析本地城域网故障的同时，与集团公司运维部也进行了汇报交流，反

映了本地网遇到的问题，询问骨干网是否出现异常。小林根据来自于总部技术支持中心的技术应急信息以及现场情况对网络故障进行了初步分析。随后对相关安全系统展开检查，突然发现部署在DNS系统网络出口的黑洞安全防护设备有异常告警，DNS系统的网络流量出现激增。针对此异常情况，小林即时启动设备自带的抓包功能进行抓包，然后对获得的数据包进行分析，发现超过50%的DNS解析请求是针对某互联网业务提供商的。随后，运维中心的现场人员对DNS系统进行了核查，发现DNS服务器群处于超负荷运行状态，DNS查询响应延迟非常大。

小林迅速将这一发现与绿盟科技总部进行了沟通，总部应急团队与小林等局方现场技术人员紧急讨论后，立即确定解决方案。随后小林向运营商局方人员介绍了故障原因及解决方案，局方人员与集团公司再次进行了紧急沟通，汇报了本地监控发现的DNS服务的异常情况，并与某互联网业务提供商求证该公司的系统是否出现异常情况，该公司负责人反馈系统服务出现异常，目前正忙于相关系统的升级抢修工作。

问题定位后，绿盟科技的技术专家与局方人员共同商讨，即刻确定了应急方案：一是在黑洞上开启模式匹配策略，对指向该互联网业务运营提供商相关域名解析请求进行过滤，减轻对DNS服务器的查询压力；二是在本地DNS服务器上针对该互联网业务运营提供商相关域名设置强解析策略，保障运营商以最小的代价保证绝大部分的应用正常开展。

平息危机

晚上11点，小林和局方运维人员迅速下发应急策略后，DNS系统网络流量从150M飞速下降为10M，DNS查询请求骤然下降70%，DNS系统快速恢复正常，随后用户的互联网接入业务逐渐恢复。

小林等技术专家进行应急支持的同时，华北区域的应急响应人员在也在华北某电信运营商的机房里忙得热火朝天——网络故障分析、数据抓包、数据分析……，再将现场情况向绿盟科技总部进行反馈。总部技术专家分析发现华北电信运营商遇到了与小林所支持的南方电信运营商相同的DNS大流量攻击问题，不过目前的DNS流量还只是处于快速增长阶段，为了防止DNS系统可能出现的瘫痪，总部马上与现场应急响应人员交流现状和制订应急处置方案，并经过与局方运维人员确认后立即启动相应的防护策略。应急策略下发实施后，防止了该地区互联网业务大面积中断的发生。

华东、华南、华北、西北等地省电信运营商陆续与集团公司取得联系，各省市电信运维部门采取紧急策略，对各地的DNS实施应急防护策略，随后DNS服务逐渐恢复正常，互联网业务渐渐恢复。5月20日凌晨全国互联网基本恢复正常运转。

后记

这次事件貌似由DNS的大量查询请求所引起，对DNS服务器形成了一次饱和的DDoS攻击，导致某些运营商的DNS瘫痪。事实上，DDoS攻击广泛存在于互联网中，而针对DNS服务器的DDoS攻击事件更是层出不穷，且形式越来越多样化，主要包括以下几种：利用缓冲期溢出；海量流量堵塞带宽；伪造源IP发送海量DNS查询；源端口53的UDP FLOOD（攻击负载均衡设备）；真实协议栈大量查询随机域名引起迭代查询。

针对这些广泛存在的DDoS攻击，绿盟科技专家指出，通过在运营商骨干网部署流量清洗系统，可以帮助运营商清洗网络中的DoS流量，利用抗DDoS安全产品的模式匹配以及IP地址信誉机制等独特的防护算法对形式多样的DDoS攻击进行安全防护，在运营商网络受到攻击时可以为运营商的DNS服务器提供有效和及时的安全保障。

运营商门户网站安全建设思路

行业营销中心 田民

摘要：在进行门户网站安全建设规划的时候，运营商越来越关注 WEB 应用层面的防护。对于定制化开发的 WEB 应用系统，应该结合 WEB 应用系统的生命周期，将安全防护的思路贯穿于门户网站的规划、开发、测试和运行的每个生命周期阶段，其中网站系统交付之后的运行阶段是防护的关键。

本文重点从事前主动发现、事中在线控制和事后及时恢复三个层面阐述如何进行有效的防护。同时人的因素不可忽视，包括安全评估、安全加固、渗透测试、安全职守、安全应急等服务都是保证门户网站安全运营的必要支撑。

关键词：网页防篡改 WEB 应用生命周期 WEB 应用扫描 WEB 应用防火墙

一．概述

运营商的门户网站是对外信息发布的窗口，是与外界进行网络沟通的桥梁，也是广大移动终端用户、集团企业用户办理业务的便捷通道，它能否正常工作不仅直接关系到运营商提供的服务质量，而且关系到各大运营商的公众形象。

然而，近年来，运营商门户网站所面临的 WEB 安全形势越来越严峻，安全威胁突出地表现出来，极大地困扰着各省公司门户网站的管理者，给中国运营商的信息网络和核心业务造成严重的破坏。比如，病毒、木马、蠕虫等等恶意程序都可以对网站造成可怕的威胁。通过各种渠道，网站服务器最终感染了病毒造成性能降低难以满足用户正常访问的需求；或者被种植了木马，对外开放的远程登录的端口形成威胁；大规模的 DDoS 攻击造成网站服务器的拒绝服务，不能对正常的应用进行响应等等都可能对网站系统的安全、正常使用带来威胁。

从企业自身层面来看，今年各大运营商都在主推 3G 业务，其中很多活动是通过网站进行发布的。而事实上，诸如网厅遭到暴力破解或门户网站遭受 DDoS 攻击等安全事件屡见不鲜。提高到国家层面上来看，今年的建国六十周年大庆和明年的世博会都是关乎国家意义的重大事件。由于运营商的门户每天都有大量的用户访问，在国家重大事件的背景下，一旦网页内容被恶意篡改，就有可能造成非常严重的政治影响。因此，保证运营商门户网站的安全正常工作和运行，首先是一个关系到企业形象和服务质量的问题，在某种情况下，也是一个至关重要的政治问题。

二． 运营商门户网站现状

2.1 门户网站分类

运营商门户网站系统可以分为以下五大类:

1) 运营商门户网站

门户网站一般分为一级门户和二级门户。一级门户是集团门户，二级门户为各省门户。

2) 业务支撑系统门户网站

业务支撑系统门户网站是集团和各省业务支撑系统（BOSS）面向外网的统一接入平台，典型的业务支撑门户网站如个人或集团网上营业厅。

3) 数据业务系统门户网站

数据业务系统门户网站是各省各个数据业务系统（如彩铃、彩信、LBS、PIM 等）面向外网用户统一业务接入和服务平台。

4) 运维支撑系统门户网站。

运维支撑门户系统是进入所有运维支撑系统的统一通道，主要为各类管理和生产人员提供综合运维工作的接入平台。

5) 企业信息门户（EIP）

企业信息门户（EIP）为企业员工、用户和合作伙伴提供单一的渠道，可以访问、抽取、分析、储存其所需的个性化信息。

上述五类运营商门户网站中，运营商门户、业务支撑门户网站和数据业务门户网站面向广大用户提供基于公众互联网的业务服务，相比之下，运维支撑系统门户网站和企业信息门户（EIP）主要面对企业内部的员工或合作伙伴。前三类门户网站以提供公众服务为主要目的，后两类门户以面向内部员工接入为主要目的。

在本文档中，主要关注在面向公众服务的前三类门户网站，提出相应的安全建设思路。

2.2 门户网站主要威胁

从门户网站所面临的安全风险来看，严格的讲，从物理层、到网络层，再到系统层和应用层，每个层面都存在着内在脆弱性和外在的威胁。对于运营商的门户网站而言，WEB 应用的安全威胁逐渐成为防护的重心所在。表 2.1 中，列举了常见的 WEB 应用攻击和相应的风险级别:

表 2.1 常见的 WEB 应用攻击

威胁	描述	风险级别
SQL 注入	利用 SQL 注入漏洞，攻击者通过在 URL、表格域，或其他的输入域中输入自己的 SQL 命令，以此改变查询属性，骗过 WEB 应用程序，从而对数据库进行不受限的访问。	高
跨站脚本	利用 XSS 漏洞，通过虚假的 WEB 页面内容伪装用户的常用方法。恶意攻击可以通过 XSS 来盗取用户的 cookie，将用户引导至其他的恶意页面，并且向其提供虚假的内容。	高
网站挂马	网页挂马相对比较隐蔽，其攻击目标是各类网站的最终用户。首先攻击者在服务器端插入恶意代码。用户访问恶意页面时，网页中植入的恶意代码触发客户端的漏洞从而自动下载并执行恶意程序，最终攻击者盗取客户端的敏感信息（如各类帐号密码），甚而可能用户主机沦为攻击者的肉鸡。这种情况下，WEB 服务器成为了传播网页木马的“傀儡帮凶”，严重影响到网站的公信度。	高
应用层 DDoS 攻击（资源耗尽型）	其具有易于发动、难于防范、破坏力强、危害面广、追查困难等特点。通常而言，网络数据包利用 TCP/IP 协议在 Internet 传输，这些数据包本身是无害的，但是如果数据包异常过多，就会造成网络设备或者服务器过载；或者数据包利用了某些协议的缺陷，人为的不完整或畸形，就会造成网络设备或服务器服务正常处理，迅速消耗了系统资源，造成服务拒绝。	高

从表 2.1 我们可以看到，SQL 注入、跨站脚本和网页挂马是门户网站面临的最主要的应用层威胁，同时又是导致网页被篡改的主要原因。除此之外，应用层 DDoS 攻击也是网站的主要威胁。上述几类安全威胁是保障网站安全正常运行最重要的的防范对象，是门户网站在业务上面临的最严重的威胁。在接下来的文章中，会着重阐述和讨论 WEB 应用层的安全防护思路。

三．门户网站安全防护思路

3.1 合规性的思路

在进行门户网站安全建设的时候，首先要求符合工业与信息化部下发的与门户网站相关的各项安全技术要求和规范。特别是《网厅安全防护要求》，是国家对运营商进行网上营业厅门户安全建设的指导性安全标准，也是工信部对各大运营商网上营业厅门户进行安全检查的执行标准。

除了需要遵循工信部下发的安全技术要求和规范之外，对于不同的运营商而言，还要满足该运营商自身下发的与网站安全相关的安全规范。这里以中国移动为例，中国移动集团先后制定了一系列的技术规范，其中部分规范与网站系统的安全建设有着直接的关系，如《中国移动网页篡改防护系统技术规范》、《省级业务运营支撑系统（BOSS）业务技术规范 - 门户网站分册》等；而部分规范与网站有着间接的关系，从不同层面对网站所涉及的通用系统或通用组件提出了安全要求，如《中国移动 XX 系统安全配置规范》、《中国移动防火墙配置规范》、《中国移动业务支撑网安全域划分和边界整合技术要求》等。

落实上述与门户网站相关的来自国家和企业自身制定的技术规范是对门户网站进行有效防护的前提和基础，换句话说，进行运营商门户网站安全建设首先需要考虑的就是合规性，即符合工信部和各大运营商下发的各项门户网站相关技术规范。

3.2 WEB 应用安全生命周期的思路

一般来说，一个通用的商业化软件系统，如 WebSphere、Oracle Database、Apache Server 和 Webmail 等，其系统开发厂商会不定期地提供相应漏洞补丁，使用者只要及时更新补丁程序就可以很大程度上避免安全事件的发生。因此，对于上述 Off-the-shelf 的 WEB 应用系统，最主要的安全手段就是更新厂商提供的补丁。

而对于定制化开发的门户网站来说，一般来说，系统开发结束上线运营后，开发厂商很少、甚至没有相应的补丁程序，而黑客往往利用定制化开发程序的漏洞进行渗透和入侵，因此对于门户网站系统而言，不能依靠传统的防护思路和防护手段进行防护，需要将安全防护的思路贯穿于 Web 应用系统的规划、开发、测试和运行维护的各个生命周期阶段进行分阶段、有重点地防护。

3.2.1 WEB 应用生命周期

如图 3.1 展现了门户网站的 WEB 应用生命周期:

门户网站的 WEB 应用生命周期包含四个阶段，分别是:

1) 规划阶段。规划阶段主要的工作是网站需求的调研和网站体系的设计。

2) 开发阶段。开发阶段的主要工作是编程人员的代码编写阶段。

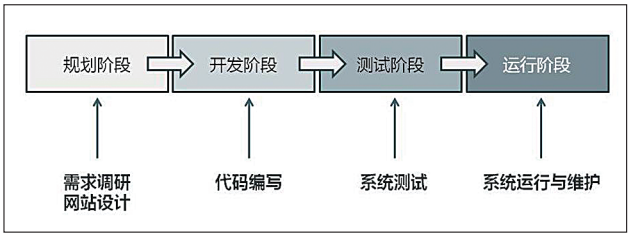


图 3.1 WEB 应用的生命周期

3) 测试阶段。测试阶段主要进行网站应用 / 业务的测试，包括功能测试、性能测试、安全测试等。

4) 运行阶段。运行阶段主要的工作是保障系统的正常运营，以及相应的维护。

在现实生产过程中，在规划阶段，往往由于开发时间短，工期要求紧等多方面因素导致安全规划和安全培训工作被弱化，使得最初阶段的安全设计和人员安全意识的培养流于形式；在开发阶段，代码审计（又称白盒测试）往往由系统开发厂商来进行，一来其专业性打了折扣，二来代码审计本身无法发现系统与系统间、模块与模块间的问题，而这些问题只有在网站运行和使用后才可以发现；之后的测试阶段，黑盒测试和渗透测试存在同开发阶段类似的问题，首先，渗透测试和黑盒测试的专业性和专业的安全厂商尚存在一定的安全水平差距，同时采用专业黑盒测试软件（如 APP SCAN 或 Web Inspect 等）测试的结果往往存在准确性不高和可读性不强的问题。

由此可见，诸如代码漏洞、程序漏洞、对用户提交数据缺乏有效检查，以及缺乏篡改后恢复等等问题均遗留到了网站的运行阶段。这样一来，运行阶段的安全防护就成为门户网站能否安全稳定运行的关键。

3.2.2 运行阶段的安全防护

由于在规划阶段、开发阶段和测试阶段积累了这样或那样的安全隐患，因此要求在门户网站的运行阶段必须通盘考虑网站各个层面、各个阶段的安全，必须形成多点或者纵深防护，单独依靠单点或者单个安全手段进行防护是不可行的。

我们建议可以在事前、事中和事后进行分阶段、多层面的完整防护措施。

事前防护是主动扫描发现网站的脆弱性以实现防患于未然的目的，主要依靠 WEB 应用扫描系统来完成。WEB 应用扫描器最关键的技术是网站智能爬虫技术。智能爬虫技术具有自动遍历整个 WEB 服务器的深度扫描功能，自动分析应用系统的代码，当发现了存在弱点的代码之后，会根据不同数据库的特点尝试进行数据获取，验证漏洞的真实性。绿盟公司的 WAS（WEB APPLICATION SCANNER）系统扫描结果准确，误报和漏报率低，全面检查网站各级页面中是否被植入恶意代码（如 SQL 注入、跨站脚本、网页挂马等），确保网站应用的完整性，有效避免网站成为恶意软件的分发、传播渠道。

事中防护是门户网站提供实际运营服务中，网站入侵者与网站维护者攻防两者之间博弈的关键阶段。WEB 应用防火墙是事中有效防护和控制的关键设备。WEB 应用防火墙需要对用户提交 WEB 服

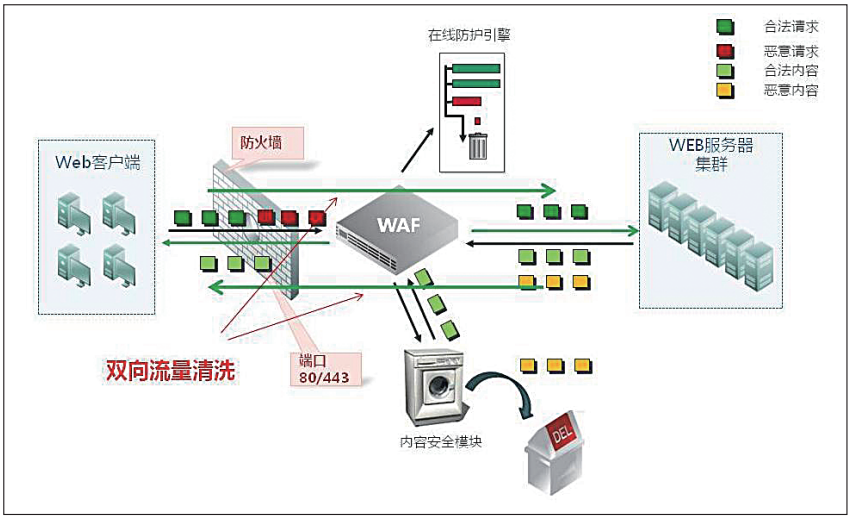


图 3.2　WAF 产品的双向流量清洗

务器端以及 WEB 服务器端向用户返回的双方向数据进行检查。绿盟公司的 WAF 产品可以实现用户→服务器以及服务器→用户双向数据的清洗。对于用户提交服务器端的数据，WAF 可以实时发现用户提交数据中的恶意脚本和问题代码 / 命令。此外，绿盟的 WAF 产品采用了专业抗 DDoS 设备——黑洞的部分核心功能，对于应用层的 DDoS 攻击，如 CC 攻击进行有效控制；对于服务器返回用户的数据，WAF 可以进行必要的内容过滤，如恶意脚本和代码，HTTP Error Response（4xx，5xx 等），关键敏感字等，充分保证了用户侧的安全，同时避免了服务器端重要信息的泄露。如图 3.2 为 WAF 产品的双向流量清洗。

事后防护是门户网站安全防护最后的防线。没有绝对的安全，一旦网站被篡改，如何及时阻断恶意网页反馈给访问者以及如何恢复被篡改的网页内容就成为事后防护最主要的目标。绿盟公司的 WAF 产品通过内置的 Cache 缓存可以至少保证用户看到的网页是安全的。这部分功能我们称之为“视觉恢复”。“视觉恢复”的方法是用存储在 Cache 中的网页备份替换被篡改的网页，确保用户看到的网站是安全的。而恢复 WEB 服务器上被篡改的文件系统可以通过安装绿盟公司的 HWAF 产品来实现。HWAF 产品实时对 WEB 文件系统进行监控，一旦发现文件被修改，立刻从备份文件中提取相应的文件覆盖被篡改的文件。

3.3 安全服务

人的因素始终是不可忽视的关键所在。诸多安全事件证明，即便部署了多种安全产品，规划设置了分层纵深的防护策略，网站也存在被攻破的可能。网站的攻击者是人，而制约黑客入侵的利器之一也是人。换句话说，安全服务是门户网站安全建设过程中必不可少的环节之一。

参考运行阶段三个层面，即从事前、事中和事后进行安全防护，从安全服务角度上讲，同样可以从这三个层面上提供有效的人的服务。

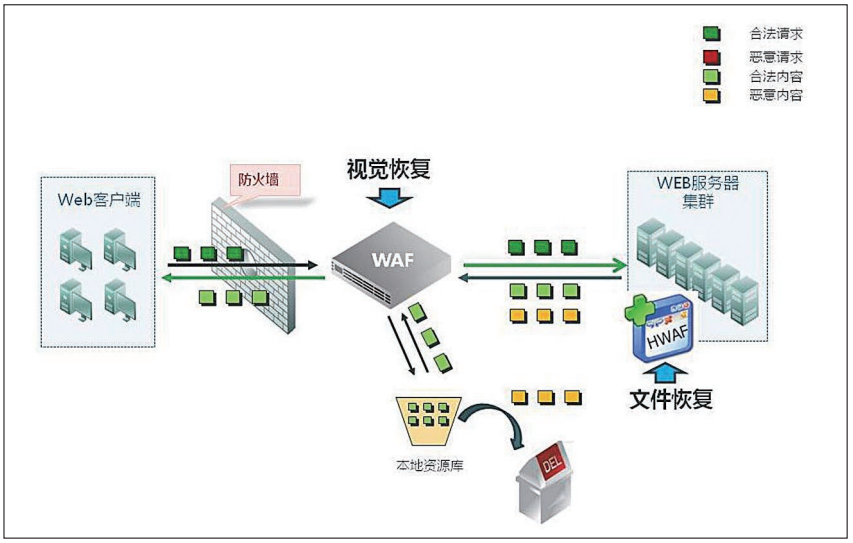


图 3.3 视觉恢复配合文件恢复

在事前，可以通过门户网站安全评估和加固，使系统有效地抵御外来的入侵和袭击，长期保持在高度可信的状态。其中，渗透测试是安全评估阶段必不可少的服务手段之一。渗透测试是模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试。通过渗透测试，可以发现门户网站系统中存在的系统漏洞、代码漏洞和程序逻辑问题（如绕过认证）等。在事中，可以通过安全职守服务保障在重大事件（如国庆六十年大庆）过程中网站随时处于安全人员的监控之下。在事后，可以通过应急响应服务确保发生安全事件的网站及时恢复正常。绿盟科技在安全应急相应方面也具有很多成功的案例。

四．小结

对于运营商的门户网站而言，安全建设首先需要考虑的就是合规性，即符合工信部和各大运营商下发的各项门户网站相关技术规范。其次，现阶段最主要的安全威胁在于 WEB 应用面上，WEB 应用的安全需要放到 WEB 应用的生命周期中，进行分阶段的防护。其中，网站开发厂商将网站系统交付运营商并上线运行之后的运行阶段的防护，事实上是需要重点进行各项安全策略和安全产品部署的关键；而在运行阶段，需要从事前主动防护（防患于未然），事中实时控制（攻防的关键），和事后及时恢复（最后的防线）三个层面提供全面的防护；最后，人的因素不可忽视。安全服务可以作为安全产品的重要补充，为网站的安全运行提供有效的支撑。

参考资料

[1] 吴海燕，苗春雨，刘启新，孙方成 .WEB 应用系统安全研究综述 [R]. 北京：清华大学计算机与信息管理中心 ,2007:2-4.

[2]Yue Chen,Barry Boehm,Luke Sheppard.Value Driven Security Threat Modeling Based on Attack Path Analysis[D].Calidornia:University of Southern California,2006:2-6.

[3]Mandeep Khera,Sameer Dixit. Web Application Security Trends Report Q3-Q4, 2008[R].Santa Clara:Cenzic Inc,2009:5-10.

政府网站面临的安全威胁及应对

行业营销中心 孙 铁/行业技术部 祝国鑫

摘要：本文从政府网站运营者和监管机构的角度，分析了政府网站进行信息安全建设的必要性以及相应的建设方法，并对政府网站安全建设目标做了展望。

关键词：政府网站 防篡改 防挂马 988 号文 公安部第 82 号令

对于政府机构来说，电子政务是政府实现政务公开的一种重要形式和发展方向，而电子政务的功能和内容主要是通过政府网站的形式表现出来的，外界对政府信息化的了解也是从政务网站开始的，政府网站是政府职能部门信息化建设的重要内容，主要实现国家对政府网站的三大功能定位：信息公开、在线办事、公众参与。政府门户网站是电子政务的窗口，也是政府的窗口，是政府部门履行职能、面向社会提供服务的官方网站，是实现政务信息公开、服务企业和社会公众、方便公众参与的重要渠道，是政府信息化绩效的表征通道，是对外宣传政府形象、发布所属行业信息、开展电子政务的主要平台。政府网站已经逐渐成为当前政府大力推进政务公开、不断提升行政效率和服务水平并让企业和公众更广泛地参与公共事务管理的最佳手段之一，是电子政务建设的风向标和晴雨表，是提高政府电子政务服务质量、服务效率、公众认知度和满意度的关键环节，是国家重要信息系统。

而近年来，随着政府网站所运行业务的重要性逐渐增加以及其公众性质使其越来越成为攻击和威胁的主要目标，政府网站所面临的 Web 应用安全问题越来越复杂，安全威胁正在飞速增长，尤其混合威胁的风险，如网页篡改、蠕虫病毒、DDoS 攻击、SQL 注入、跨站脚本、Web 应用安全漏洞利用等，极大地困扰着政府和公众用户，给政府的政务形象、信息网络和核心业务造成严重的破坏。

因此一个优秀的电子政务网站安全建设是电子政务是否能取得成效、充分发挥职能的基础，而合规、有效、全面的信息安全体系建设对保障其正常运行至关重要。

1.1 政府网站信息安全建设的必要性

政府网站是政府在网络世界中建立的永久据点。当前政府网站已积聚了电子政务信息化建设中大量的信息资源，成为政府成熟的业务展示和应用平台，是工作模式创新与流程改造、开展协同和电子服务的重要媒介。

政府部门的网站普遍存在业务数据机密性要求高、业务连续性要求强、网络结构相对封闭、信息系统架构形式多样等特点。而网站中不同业务功能模块的信息安全需求又各不相同。如对外便民服务信息系统具有相对开放的结构特点，用户一般为普通民众，便民服务业务对数据的可用性和完整性要求往往大于其对机密性要求，而在网站上独立

运行的业务信息系统具有相对封闭的结构特点，用户一般为内部用户，用户对数据的完整性和保密性要求往往大于可用性要求。因此政府网站安全风险贯穿前端 WEB 访问到后端数据处理和反馈整个过程。因此可以定性的认为：前一类信息系统面临的服务中断、外部黑客攻击、非法入侵、安全漏洞等威胁的概率比较大，而后一类内网泄密、监管审计不到位等威胁的概率比较大。

而推动政府网站进行全面信息安全体系设计和建设的动力目前主要来自三个方面：等级保护等合规性安全要求，面临的安全威胁，政府网站安全现状。

1.1.1 合规性要求

根据国家发改委、财政部最近下发的《关于加快推进国家电子政务外网建设工作的通知》（发改高技【2009】988 号）中的要求：尚未实现与国家政务外网连接的部门，要按照统一的标准和规范，于 2010 年初完成接入国家政务外网的工作，要尽快将各类可在国家政务外网上运行的业务系统向国家政务外网上迁移，各级政务部门要根据国家关于等级保护的有关规定，确定国家政务外网上运行的业务系统的信息安全等级，采取相应的信息安全等级保护措施，进行信息安全风险评估，保障各自业务系统的信息安全。

目前在已经基本完成的等级保护定级工作中，国家部委网站的安全级别基本定为 3 级，属于国家重要信息系统，是国家等级保护测评和检查重点。应按照《中华人民共和国计算机信息系统安全保护条例》（国务院令第 147 号）、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）、《信息安全等级保护管理办法》（公通字 [2007]43 号）等文件要求，参考《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护基本要求》（ GB/T 22239-2008 ）等等级保护相关标准，开展等级保护整改、测评工作，切实为将网站建成“信息公开、在线办事、公众参与”三位一体的业务体系，为“一站式”电子政务公共服务政务目标提供有力保障。

1.1.2 面临的威胁

近几年关于网站网络钓鱼、SQL 注入和跨站脚本等带来严重后果的攻击事件频频发生，严重影响了人们对 WEB 应用的信心，根据 Gartner 的数据分析，80% 基于 WEB 的应用都存在安全问题，其中很大一部分是相当严重的问题。WEB 应用系统的安全性越来越引起人们的高度关注。目前网络中常见的攻击已经由传统的系统漏洞攻击逐渐发展演变为对应用自身弱点的攻击。

与此同时，网站也因安全隐患频繁遭到各种攻击，导致网站敏感数据丢失、网页被篡改，甚至成为传播木马的傀儡。网站安全形势日益严峻，而政府网站被攻击后造成的巨大政治风险、名誉损失、经济损失已经成为电子政务健康发展的一个巨大障碍。

政府网站除了面临信息系统及网络通用的安全问题外，还有其自身特点的安全问题。政府网站面临的重要安全威胁主要有：

网页篡改

政府门户网站作为国家的行政管理机构发布的信息事关国计民生，一旦被篡改将造成如政府形象受损、恶意发布信息等多种严重后果。

从网站页面被篡改的角度来看，存在两种攻击的可能，一种是网站被入侵，也就是说网站页面确实被篡改了，另外一种

是网站被劫持，这种情况下网站的页面实际上并没用被篡改，但是攻击者劫持了网络访问并发送欺骗页面给来访者，进而造成页面被篡改的表象。

木马、病毒传播

木马是一种在远程计算机之间建立起连接，使远程计算机能够通过网络控制本地计算机的程序。木马本身不具备繁殖性和自动感染的功能，这是与病毒的最大区别。木马程序的危害十分大，它能使远程用户获得本地机器的最高操作权限，通过网络对本地计算机进行任意的操作，比如删添程序、锁定注册表、获取用户保密信息、远程关机等。木马使用户的电脑完全暴露在网络环境之中，成为别人操纵的对象。

因为工作需要政府办公人员会经常访问政府网站，一旦访问了被植入木马的网页，木马程序会自动搜集并传走电脑中的各种文档，将可能引发严重的泄密事件，后果不堪设想。

据安全公司比特梵德 (BitDefender) 在日前发表的 4 月份调查报告中称，木马程序仍然继续在互联网上传播，是互联网用户面临的最恶毒威胁排行榜中的主要威胁。

网络蠕虫

蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共同特征，如传播性、隐蔽性和破坏性等。同时具有自己的特殊特征，如不利用文件寄生 (如只存在于内存中) 引起网络拒绝服务故障及与黑客技术相结合等。在破坏性上，网络蠕虫也不是普通病毒所能比拟的，它可以在短短的时间内蔓延整个网络，造成网络瘫痪。使访问者无法获取自己需要的内容，政府发布的各种信息将得不到传达，影响了信息的发布和传播。

SQL 注入

SQL 注入是应用系统中最常见，同时也是危害最大的一类弱点。导致 SQL 注入的基本原因是由于应用程序对用户的输入没有进行安全性检查，从而使得用户可以自行输入 SQL 查询语句，对数据库中的信息进行浏览、查询、更新。基于 SQL 注入的攻击方法多种多样，而且有很多变形，这也是传统工具难以发现和定位的。

跨站脚本

跨站脚本攻击属于被动模式攻击，这种攻击的对象是应用系统的最终用户，通过在应用系统插入可执行的脚本，用以获取用户系统中存储的 Cookie 和 Session 信息，通过这些信息进行加工和重放，就可以轻而易举地进行用户身份仿冒。

1.1.3 政府网站安全现状分析

目前政府网站建设还存在比较突出的重应用轻安全的现象，比如在某部委所制定的网站绩效评估指标中，基本上均是从网站的业务应用出发制定的，对信息安全的考虑基本没有。

根据前期的调研发现，目前政府网站的安全控制与措施大多独立考虑，部分系统甚至缺少基本的安全策略，缺少安全主线和安全规划，导致只解决了局部问题，而未能从整体解决安全问题，从而降低了整体的安全效率，导致多个信息安全孤岛的出现，而且现有政府网站安全管理、防范措施、安全意识薄弱，极易遭到黑客攻击。当前政府网站系统面临的安全形势十分严峻，既有外部威

胁，又有自身脆弱性和薄弱环节，能否及时发现并成功阻止网络黑客的入侵和攻击、保证WEB应用系统的安全和正常运行成为政府网站所面临的一个重要问题。当前绝大多数政府网站部署了一些安全设施，如防火墙，防病毒软件等，而这些传统的安全设备，作为整体安全策略中不可缺少的重要模块，还不能有效地提供针对WEB应用攻击完善的防御能力。面对WEB应用攻击，这类给Internet可用性带来极大损害的攻击，必须采用专门的机制，对攻击进行有效检测，进而遏制这类不断增长、日趋复杂的攻击形式，因此围绕政府网站特定的安全需求开展系统的、有针对性的网站安全建设已经变得刻不容缓。

1.2 建设方法

1.2.1 从网站建设和运维者的角度

根据国家“谁主管谁负责，谁运营谁负责”的精神，政府网站设计、建设、运维者是网站安全保障体系建设的主要力量，在贯穿网站全生命周期的信息安全建设过程中，可从安全检测、安全防护、安全监控与安全恢复三个方面对政府网站信息安全体系进行设计和建设。

安全检测

目前对网站有新漏洞、网页被挂马等状况，绝大多数用户并不能及时察觉，仅寄希望于有限的传统安全防护设备，而一些对安全敏感的网站，设有专门负责网站安全的开发维护人员，负责安全开发验证，甚至灾难备份机制，但成本和代价太高，不是一般网站所能承受。由于缺乏网站安全检测，用户的响应往往在造成损失之后，发现事故才能去响应；这种响应无法有效阻止黑客获取利益、降低损失。

在安全检测方面建议采用针对性比较强的WEB安全自动化检测工具，使用自动化安全检测工具实时或不定期的对网站安全状态进行检测和评估，不但可以提高对安全隐患及现有安全问题准确、深层次的发现，而且也可以降低维护管理和人力成本。

针对目前的网站检测往往是发现造成伤害之后才有所察觉这种情况，政府网站安全检测的设计应从预警检测和事后检测两方面入手。预警检测目的是利用现有的安全技术，提供一种准确、实用、可行的预警手段，注重防患于未然。事后检测是对发生问题的网页进行问题定位、影响评估。

安全防护

除了采用信息系统传统的防护技术对网站的基础设施进行必要的防护外，还必须针对WEB应用攻击采用专门的机制，对其进行有效检测、防护。从安全角度考虑，需要针对目前泛滥的SQL注入、跨站脚本、应用层DDoS等WEB应用攻击，对来自WEB应用程序客户端的各类请求进行内容检测和验证，有效应对SQL注入、跨站脚本及其变形攻击、实时检测网页篡改、提供挂马主动诊断，提供细粒度应用层DDoS攻击防护功能，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护，降低攻击的影响，确保业务系统的连续性和可用性，降低网站安全风险，维护网站公信度。

安全监控与安全恢复

最后必须考虑最坏的情况，即政府网站被入侵。如果某个政务网站被攻破，那么必须在最短时间内进行网站的恢复。国内外发生的一些重大案例都表明着对WEB网页进行监控并在必要时提供恢复措施是非常必要的。

网站实时监控与自动恢复技术解决了 WWW 服务器网页文件被破坏后的自动恢复问题，它的保护对象是网站的文件或目录（也可以扩展到其他的文件和目录），从而保证它们的内容、属主、时间等属性不被非法修改；被保护对象不被非法删除；没有文件或目录被非法添加到被保护目录中。这项技术采用的方法是实时对网页文件的内容进行一致性检查，一旦发现有上述的非法情况发生，就使用备份进行自动恢复并及时报警和记录日志。

对于政府网站面临的最主要威胁—网页篡改，公安部第 82 号令《互联网安全保护技术措施规定》中第九条第三款明确规定：开办门户网站、新闻网站、电子商务网站的，能够防范网站、网页被篡改，被篡改后能够自动恢复。

1.2.2 从检查、监管、业务指导单位的角度

随着政务系统合规性安全需求的增多，政府网站的检查、监管、业务指导单位也迫切希望能对所属各级单位的门户网站进行必要的管理、检查和业务指导。

从业务指导的角度看，可进行如下工作：

设置网站安全基线，制定防篡改、防挂马安全规范，提出监测、防护与处置机制要求，下发各单位执行。

辅助以自动检测工具、检查列表定期开展检查工作，对各单位的执行境况进行检查不定期进行 WEB 扫描，对下属单位网站的不良使用形成威慑。

建立网站安全管理中心，在各下属单位门户网站部署探针，对收集的数据进行统计、分析，定期形成态势分析报告，指导网站安全建设 。

开展网站安全绩效评估活动。

WEB 检测、防护、实时监控与恢复的产品评测、推荐入围工作。

1.3 政府网站安全建设目标

综上所述，通过传统信息安全防护技术和专门针对网站的安全检测、防护、安全监控与安全恢复技术的综合采用，将完成政府网站安全保障体系如下建设目标:

1.3.1 政务信息发布不被篡改

政府门户网站是最权威的政务信息发布渠道，对信息的真实性、完整性有着非常高的要求。政府门户网站在信息发布上所遭受的威胁非常严重，在网络日益普及，民众越来越多地从网站获取相关信息的今天，政府门户网站一旦被恶意篡改，发布虚假信息，必将严重影响政府形象，在敏感时机，甚至可能酿成社会事件，影响国家安全。

因此，针对可能造成信息篡改的各种安全风险，政府门户网站在做好数据备份、恢复的被动准备之外，更应建立主动的自检查机制和良好的入侵防御措施，在“事前”做到防患于未然，在“事中”做到严密防御和快速响应。

1.3.2 在线服务不受攻击

政府门户网站承载了大量为公众和企业服务的业务系统，《国家电子政务总体框架》中要求：到 2010 年，50% 以上的行政许可项目能够实现在线处理。大量的业务系统在网站上运行，大大地提高了政府提供服务的效率，但也势必造成企业和公众对政府门户网站的依赖。门户网站一旦瘫痪或业务系统一旦终止，企业的经营和公众的生活不可避免就要受到影响，甚至造成较大的经济损失或社会事件。

因此，网站必须具备业务处理的连续性计划，除对各种业务处理软硬件做冗余配备之外，也要具备对于各种“拒绝服务攻击”的防护能力，避免网站应用弱点被利用，造成拒绝服务攻击而中断服务，影响业务的正常运作。

1.3.3 公众资料不被窃取

政府门户网站要对企业和公众服务，其内部必然要保存企业和公众的一些数据。有些数据对于企业而言是重要的商业机密，对于公众而言是个人隐私，一旦泄露，会对政府机构的公信力造成负面影响，甚至会引起诉讼。

在众多前车之鉴面前，我们必须对企业、公众的隐私数据进行更加严格的保护措施，防止恶意者从各种渠道入侵，对提供或接受 WEB 应用服务者造成伤害，保证数据的安全。

DNS防护——互联网安全中遗失的大陆

产品市场部 崔云鹏

摘要：鉴于 2009 年 5 月 19 日 DNS 断网的重大事件，本文针对现有的 DNS 系统的安全问题作了一些描述，特别是针对 DDoS、DRDoS、缓存投毒等重点威胁做了详细阐述。此外，笔者也根据绿盟科技长期的技术积累提出了一些 DNS 安全的解决方法和途径。

关键词：DNS DDoS 缓存投毒

如同 2006 年台湾大地震引起的网络瘫痪，2009 年 5 月 19 日，时隔三年，互联网借助 DNS 再次向网民展示了自身基础设施安全上的脆弱性和巨大社会影响。

5 月 19 日，笔者正在广西出差，晚上回到酒店，打开电脑，网络已经一塌糊涂了，所有网站几乎都打不开，邮件也发不出去。“是有人在 BT 下载吧？酒店也不做个 P2P 限制！”，笔者带着疑问试图找酒店前台解决问题，但是前台已经是电话不断了，都在投诉酒店的网络问题，还有人要求退房换酒店。“这不是我们的问题，电信正在进行线路升级”，酒店的服务人员也是一脸无辜。

第二天一早，很快就知道消息了，是因为 DNS 瘫痪了。5 月 19 日晚 21 时 50 分，江苏、安徽、广西、海南、甘肃、浙江等省发生网络瘫痪，黑客的一次小规模 DDoS 攻击导致 DNSPod 公司的 6 台 DNS 域名解析服务器瘫痪，直接造成包括暴风影音在内的多家网络服务商的域名解析系统瘫痪，遍布全国个人电脑的暴风影音软件无法找到自己的域名解析，于是一遍遍的进行 DNS 查询，大量的查询最终形成超大规模的 DDoS，导致各省的 DNS 服务器瘫痪，进而造成整个互联网瘫痪。

这次 DNS 断网事件，各方都损失巨大。个人用户无法上网，企业无法工作和运营，是必然的损失；暴风影音公司很无辜，虽然它的软件有缺漏，但是很多软件也都存在这种问题，只是最初的 DDoS 攻击的恰好是暴风影音的域名服务商，而恰好暴风影音软件保有量很大，而事件给暴风影音造成的品牌影响是不可估量的；运营商在事发后也是努力解决问题，降低影响，但依旧造成了自身的信誉和经济损失；DNSPod 公司同样也是受害者，自己的服务器被攻击，DNS 被迫关闭，业务、品牌全部受损；就连那几个黑客，可能损失也超出其想象，他们只想用 DDoS 打瘫一个游戏私服服务器，谁想到会把事情闹得这么大，成为众矢之的。

5.19 事件本身的确可以说是由一系列意外促成的，但是，它却向我们展示了一个窗口，告诉我们，和我们互联网息息相关的 DNS 系统是多么的重要，而又多么脆弱。一个小小的攻击，可能就会引发大规模的网络问题；而在一个互联网无所不在的时代，DNS 的瘫痪，其显性和隐形的损失则是无法估量的。更重要的是，5.19 事件的 DNS 问题，其实只不过是 DNS 众多网络安全问题的冰山一角。

DNS 是如何工作的

讨论 DNS 的安全问题前，我们首先简单介绍一下 DNS 系统，DNS 是域名系统（Domain Name System）的缩写，它用于命名组织到域层次结构中的计算机和网络服务。DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户友好的名称查找计算机和服务，当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的 IP 地址等信息。

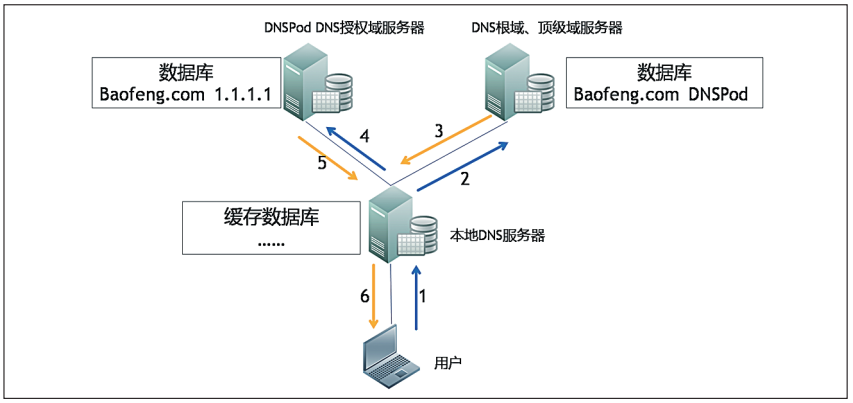


图 1、DNS 基本原理图

在 DNS 的系统中，有相当复杂的一套树状分布式域名数据库服务器构成，共同为我们完成一次域名解析工作。简单来看，一次域名解析过程主要涉及根域服务器、顶级域名服务器、授权域服务器、本地 DNS 服务器（解析、缓存）。如图 1 所示：

例如在 5.19 事件中，当用户需要查询 baofeng.com 的 IP 地址时，DNS 是按照如图箭头所示六个步骤进行工作的：

1. 用户首先向本地 DNS 服务提出请求，问 baofeng.com 的 IP 是多少，该本地 DNS 通常就是各省运营商的 DNS 服务器；

2. 本地的 DNS 服务器发现自己的缓存数据库中没有相关域名信息，于是开始查询 DNS 根服务器；

3.DNS 根服务器自己不会提供最终域名的 IP 地址，他会根据自己数据库中信息，并且经过一系列迭代查询，让本地 DNS 服务器最终知道，要想查询 Baofeng.com，应该去问 DNSPod；

4. 于是本地 DNS 服务器会继续向 DNSPod 发 DNS 查询请求，问 baofeng.com 的 IP 地址是多少；

5. 由于 DNSPod 是暴风影音的权威域名服务商，其本地数据库设置有相应的信息，故直接返回 baofeng.com 的 IP 地址是 1.1.1.1（笔者假设的）；

6. 于是本地 DNS 服务器会告诉用户，baofeng.com 的 IP 是 1.1.1.1，并且在本地 DNS 服务器的缓存中增加一条信息“baofeng.com: 1.1.1.1”。

当然，实际过程中的的查询过程会更复杂一些，各个节点涉及的 DNS 服务器也不止一台，并且会有更复杂的协议通讯，但 DNS 查询的构架和原理基本如此。

当第一次 baofeng.com 查询后，在本地 DNS 服务器会记录缓存信息“baofeng.com：1.1.1.1”，这个缓存是为了后续的其他用户查询更加方便；同时这个缓存也会有过期设置，以确保万一授权域服务器的数据库信息做了改变后，这些本地 DNS 服务器也能及时更新。这样几个小时缓存保留期结束后，本地 DNS 缓存的 baofeng.com 数据删除，重新进行上述 1-6 步的工作。

在 5·19 事件中，黑客为了攻击 DNSPod 下面的私服服务器，顺带把将 DNSPod 打瘫，导致图中的 4、5 两步长时间无法正常进行。遍布全国的大量暴风影音软件无法找到自己域名的 IP 地址，于是持续地向本地运营商 DNS 服务器进行第 1 步的查询，大量的查询报文最终导致本地 DNS 服务压力过大而瘫痪，进而影响了全网的用户。

DNS 安全问题

这次 5.19 DNS 事件，对于互联网安全的一个最大后果，不是这几个小时的断网，而是作为

一个意外发生的案例，它给全国各地苦苦思索各种攻击方式的黑客们说明了，对 DNS 的 DDoS 攻击是多么简单有效。

相对于运营商骨干网络上的高性能、封闭操作系统、比较安全的核心路由器，DNS 毫无疑问就像是互联网的七寸。现在绝大部分 DNS 服务器都使用了 BIND 的系统，（一款开放源码的 DNS 服务器软件，BIND 由美国加州大学 Berkeley 分校开发，现由 ISC 机构维护，全名为 Berkeley Internet Name Domain），尽管现在已经进入到 V9 版本，并进行了一系列功能和性能的改进，但是受制于历史原因，并且由于现在 DNS 服务器已经数以万计，遍布全球，相互之间密切关联，不可能统一进行大规模整改，因此，整个 DNS 系统依旧不可避免地存在着重大安全隐患。

分布式拒绝服务 DDoS 攻击

DDoS 分布式拒绝服务攻击是 DNS 面对的头号安全问题，如果说，本次 5.19 事件仅仅是合法软件的一次意外攻击，但以后如果大量用户的电脑是中了专门攻击 DNS 的蠕虫病毒，或者众多的个人用户是黑客完全控制下的僵尸网络的主机，那么有意识的、经常性地针对 DNS 的恶意攻击则是不可避免的。

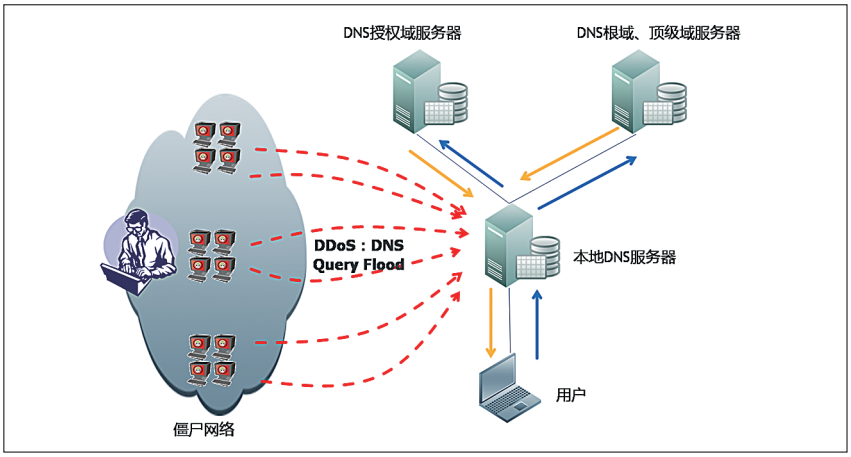


图 2、DNS DDoS 攻击示意

事实上，这几年全国各地都有检测到对 DNS 的 DDoS 攻击，只是由于影响地域范围相比 5.19 小得多，因此还没有受到太多关注。由于攻击 DNS 导致断网不容易给黑客带来直接的经济收益，因此黑客对 DNS 进行 DDoS 的攻击动机通常是政治性展示、对运营商报复、或者仅仅是个人技术表演。未来一段时间，如果再有传统的一些政治性、公众性的事件（例如国庆、运动会等）出现时，DNS 服务器难保不会成为黑客关照的重点了。

DNS Query FLood（DNS 查询泛洪攻击）是专门针对 DNS 服务器的最常见 DDoS 攻击类型。如图 2 中，黑客控制的僵尸网络的主机不断发出 DNS Query 的查询包，这些域名查询通常是一些不可能存在的域名，例如随机的 dlsafsied.com，本地 DNS 的缓存中不存在这种域名解析，故每个地址都需要进行完全的迭代查询，如果僵尸网络的查询数量过多，占据了全部 DNS 服务器的资源，则最终形成 DDoS，这样正常用户的查询就得不到 DNS 服务器的响应了。

尽管现在 DNS 做了很多安全工作缓解 DDoS 攻击，例如一个 DNS 节点会配置多台服务器进行负载均衡，提高 DNS 每秒查询的容量；设置 ACL 访问控制，只对本地本网的 DNS 查询进行响应，但依旧不可避免 DDoS 的攻击，因为相比

现在僵尸网络的规模，DNS 的这些防护实在是杯水车薪。

当前网络中 DNS 服务器，在不同服务器性能和功能启用（日志记录）等情况下，一般支持每秒几百到几千个 DNS 查询，性能好的可能会达到每秒数万条的查询能力。但是现在的一个僵尸网络，其主机数量是多少呢？根据 CNCERT/CC 2008 上半年的《中国互联网网络安全报告》，现在一个僵尸网络的主机数量通常控制了几百到数万台肉鸡电脑，甚至有大于 10 万台肉鸡的僵尸网络，假设一个黑客控制了一个小型的 1000 台肉鸡的僵尸网络，每个肉鸡电脑每秒发送 2、3 个 DNS 查询，就基本可以 DDoS 瘫痪一台中型 DNS 服务器，如果同时控制了若干个小型僵尸网络，或者控制了一个中型僵尸网络，黑客理论上可以在几分钟内瘫痪全国任何一台 DNS 服务器。

除了上述 DNS Query Flood 攻击，传统的流量型 DDoS 也可以对 DNS 服务器造成影响，如 SYN Flood、UDP Flood、ICMP Flood 等类型攻击，可以很容易阻塞 DNS 服务器的出口带宽，从而使 DNS 同样无法响应正常用户的需求。有消息说，本次 5·19 事件的 DNSPod，就是被流量型 DDoS（总共接近 10Gbps 的流量）攻击的。

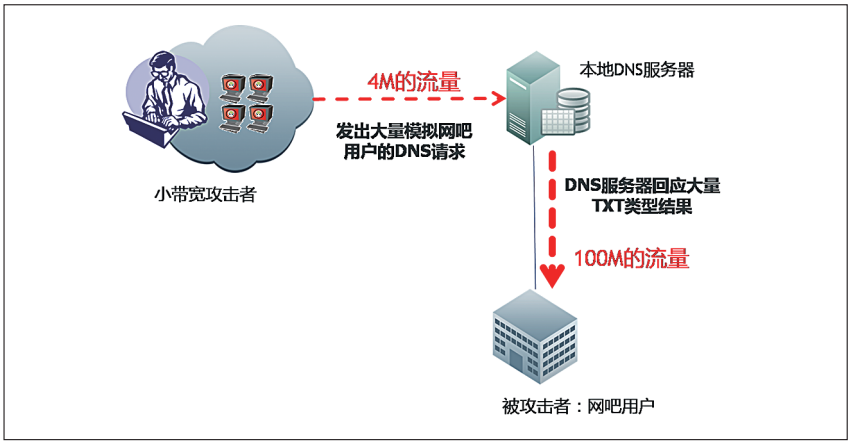


图 3、利用 DNS 进行 DRDoS 攻击的演示

折射式拒绝服务攻击 DRDoS

除了作为 DDoS 的受害者，DNS 服务器其实也可以成为 DDoS 的帮凶出现，这类攻击通常被称之为折射式拒绝服务攻击 DRDoS（Distributed Reflection Denial of Service Attack）。如图 3 所示，如果一个攻击者只有 4M 的出口带宽，但是想攻击一个出口带宽为 100M 的网吧。它完全可以借助 DNS 服务器进行折射放大式攻击。

DNS 服务器具备折射式 DRDoS 攻击折射器的全部条件:

1.DNS 是个公众性的服务平台，几乎任何人都可以访问它;

2. 为了提高 DNS 抗 DDoS 能力，DNS 服务器的性能和带宽一般都很大，因此作为攻击折射器，有优越的能力做保证;

3. 在某些条件下，例如 DNS 的查询类型不是 IP 地址，而是 TXT 类型，其响应报文最大可以达到 4K，几乎是请求报文的几十倍，符合折射放大条件。

于是攻击者可以首先利用僵尸网络发出特定的 DNS TXT 类型请求给 DNS 服务器，在图 3 中，攻击流量包含数以万计请求，总流量最高为 4M，这些请求包的源地址都被黑客设定为网吧用户的 IP 地址。于是 DNS 服务器会给网吧用户逐

一回应报文，由于这些回应报文长度比请求报文大，因此流量很容易被放大到了100M，这足以使一个大型网吧的出口带宽被堵死了。

DNS 缓存投毒

2008 年 7 月 9 日以来，思科、微软、ISC 等互联网域名解析服务软件厂商纷纷发布了安全公告，称其 DNS 软件存在高危漏洞，攻击者可以通过猜测 DNS 解析过程中的报文序列号来伪造 DNS 权威服务器的应答，从而达到“污染”高速缓存（Cache）中的记录的目的，即将错误的域名指向信息注入 DNS 服务器，最终导致受到污染的 DNS 服务器将对外提供错误的解析结果，此类攻击被称之为 DNS 缓存投毒。

如果有一天，我们在登陆某大型网络银行、游戏网站、或者是个人邮箱，看到登陆页面和以前一模一样，看看 URL 网址，也是我们熟悉的地址，最终我们的账号却被盗取了，这很有可能就是因为 DNS 缓存投毒。

此外，还有 DNS 劫持、DNS 重定向等各种攻击手法，但基本原理类似，就是用各种方式，将 DNS 的正常“域名 -IP”对应信息替换为黑客的网站 IP 地址，诱骗用户访问这个恶意网站，并进行下一步网站挂马或者钓鱼等攻击。

DNS 缓存投毒的基本原理如图 4

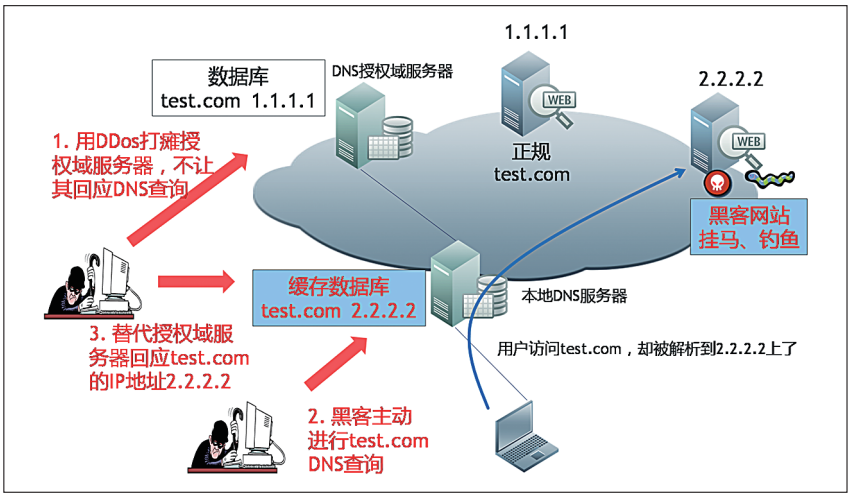


图 4、DNS 缓存投毒过程

假设，黑客的恶意网站地址为 2.2.2.2，要替代合法网站 1.1.1.1 下面的 test.com。黑客通常首先会利用僵尸网络进行 DDoS 攻击，将 test.com 的授权域服务器压制住；之后黑客主动进行 test.com 访问；由于本地 DNS 服务器会有缓存过期，因此，需要重新查询 test.com 的授权域服务器，但此时，授权域服务器正在被 DDoS 攻击无法进行正式回应，黑客不断尝试发送的假的回应报文 test.com:2.2.2.2，从而最终使本地 DNS 服务器缓存被改写。以后一旦正常用户访问 test.com 网站，就会被指向到了 2.2.2.2，在黑客的恶意网站上，通常是和 test.com 的外观一样，当用户填写用户名和密码时，账户信息被盗窃——钓鱼，恶意网站会秘密进行一些恶意下载软件——木马，用户的 PC 机也会被木马控制，成为僵尸网络的一部分——肉鸡，并发生进一步的信息泄露。

在 DNS 缓存投毒的过程中，黑客还可以针对具体情况改进攻击手段。例如在用户侧专门针对用户 PC 发出的 DNS 请求，进行回应，从而直接将用户劫持到恶意网站；或者在条件允许下，将用户

DNS 名称查询重定向到黑客可控的恶意 DNS 服务器，这样同样可以将用户劫持到恶意网站。

DNS 服务器权限入侵

由于 DNS 服务器通常采用 UNIX/LINUX 操作系统以及 BIND 软件，这样操作系统和软件不可避免出现的漏洞，为黑客的直接 DNS 攻击提供了可乘之机。例如利用缓冲区溢出方式，黑客可能轻易获得 root 权限，获得修改 DNS 服务器缓存内容的机会，并以之为跳板进行下一个节点的入侵攻击，或者直接利用缓存投毒进行下一步钓鱼和挂马行为。

DNS 国家级安全

除了这些 DNS 的网络攻击导致个人、企业用户上网不便，造成经济、社会影响外，DNS 安全建设其实也涉及国家安全建设的内容。首先，DNS 信息也是一个国家政府或军队的机密信息，如果某些机密部门的 DNS 的访问查询长期被监控，这本身就是一种泄密；其次在整个 DNS 查询体系中，我们能否完全掌握住相关 DNS 设施（从根节点到授权域服务器）、以及相应的数据和备份，不会在非常时期被国外机构中断 DNS 应用。这些可能都是 DNS 的安全建设过程需要好好规划考虑的。

DNS 安全加强

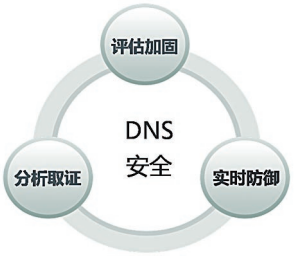


图 5、DNS 系统安全加强方案

DNS 安全问题和所有网络安全问题一样，没有一劳永逸的解决方案，不会有一个措施可以将威胁完全的消除，但是我们完全可以做一系列工作，持续的缓解攻击并提供更加严格的保护。针对 DNS 安全防护建设，笔者有如下想法，即按时间顺序，采用事前评估加固、事中实时防御、事后分析取证的三个阶段进行全面系统的安全建设。

评估加固

评估加固的积极防御，是在攻击发生前的一系列安全工作，期望在 DNS 的攻击前就已经发现各种问题和漏洞，并尽量提高防护抵抗能力，从而避免 DNS 系统被攻击。这主要包含几个方面:

1.DNS 标准系统加固。例如定期更新操作系统和 DNS 软件的补丁，增强管理账户安全性等，提高软件和系统的抗入侵能力。

2.DNS 系统应进行定期的安全评估。主要进行系统核查和配置检查，利用手工的方式，或者漏洞扫描工具等对系统安全漏洞、系统安全功能、系统配置安全、系统代码安全、系统日志审计，进行全方位的检查评估，并进行相应的整改。

3. 攻击验证与渗透测试。实际模拟黑客行为或者蠕虫病毒，利用各种 DDoS 攻击手段、或者采用系统入侵等手法，在可控的范围内对 DNS 系统进行模拟攻击测试，发现系统最脆弱的环节，并加以改进，这其实也是系统安全评估的特殊形式。

4. 而对于 DNS 的容量设计和规划也是必不可少的。除了对单个节点增加多台并行的 DNS 服务器，并安装负载均衡设备，提高相互冗余，增加整体的响应能力外，各个运营商在全国范围内，甚至在全国各个运营商之间进行合理的 DNS 容量调度和负载均衡也是需要综合考虑。

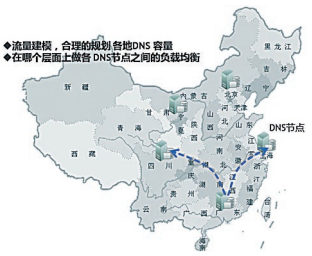


图 6、DNS 冗余和分布规划

实时防御

一旦针攻击发生了，我们的 DNS 系统需要有能力快速发现攻击类型，并有能力自动地或者在人工参与下快速准确地消除攻击影响，这应该是 DNS 防护建设的另一个重点。

针对各个运营商级或者企业级 DNS 服务器来说，为实现这个目标，我们可能需要部署一系列专业级安全产品，既能完成针对网络异常的监控，也能实现 DDoS 的清洗，并对抗 DNS 投毒、劫持等各种攻击。由于方案重点涉及对 DDoS 的防护，为了实现应对 DDoS 的防护特点——即尽可能将防护层面提高，需要考虑从运营商省级单位进行分级部署，实现对 DNS 攻击的监控、清洗、防护的综合部署，如图 7 所示：

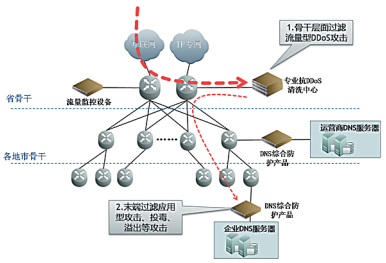


图 7、DNS 综合防御系统部署

1. 在网络中部署专业的流量监控设备，实时了解网络流量和路由信息，并及时发现 DDoS 攻击，实时监控进入网络中的异常流量；

2. 在省骨干部署大型专业抗 DDoS 流量清洗设备，把进入网内的针对 DNS 的各种流量型 Flood 攻击、查询型 DNS Query Flood 攻击清洗掉；

3. 在各个 DNS 服务器的节点出口，部署专业的 DNS 防护设备，对诸如特殊的小流量、特殊应用级 DDoS 攻击、DNS 缓存投毒、以及内存溢出等黑客攻击进行防护。同时也可监控 DNS 行为，不要让 DNS 成为 DRDoS 攻击的折射点。

除此之外，一些通用型的安全产品，例如防火墙、IPS、UTM 等安全网关，也可以部署在合适的位置，发挥其辅助的安全保护能力。但需要注意的是这些通用安全网关一般缺少针对 DNS 的专业防护手段，例如 DDoS 防护，通用安全网关一般只提供 SYN Flood 等几种常见的 DDoS 攻击防护，较少有更专业的 DNS Query Flood 等攻击防护的算法；同时由于通用安全网关算法和功能的限制，设备自身的抗 DDoS 性能能力就很差，在很多环境下，防火墙、IPS 或 UTM 自身甚至就成为 DDoS 最好的攻击目标。

分析取证

这一步实际上是为了保障攻击后的善后工作。在 DNS 攻击发生后，系统首先应具备还原分析能力，这可能需要利用相应的日志或其他分析系统数据，确定攻击的原因、系统的漏洞，从而为后续做进一步的加固改进做准备。另外，DNS 防护体系应具有抓包取证、攻击还原功能，为警方提供证据和线索，从技术上配合国家部门从法律层面打击那些违法犯罪行为，这也是震慑黑客再次攻击的重要手段。

后记

本文主要是针对现有的 DNS 系统的安全问题作了一些简单描述，因为要解决 DNS 的安全问题，首先是应该有更多人意识并了解这些 DNS 安全问题。另外，笔者也提出了一些个人了解的 DNS 安全解决方法和途径。当然，这些安全威胁描述和防护手段都还是停留在具体攻防的技术层面上。事实上，对 DNS 系统的整体研究改进、全方位的构架性的体系工作才是能解决 DNS 乃至互联网脆弱性更好的途径，只是，这便要涉及到一系列的系统构架、安全理念讨论，并需要研究机构、运营商、安全厂商、国家监管部门、执法机关等众多部门更加广泛的参与，题目过大，则不在本文讨论之列了。

WEB架构及安全防护剖析

行业营销中心 李钠

摘要：WEB 已经成为目前主流的信息交换途径，WEB 领域的信息安全已经越来越得到重视，很快将成为下一个信息安全的热点领域。本文对 WEB 领域主要的信息安全问题进行概要性描述。

关键词：WEB 信息安全 WEB 信息安全趋势 WEB 体系 WEB 系统基础架构

越来越重要的 WEB 技术

1990 年 9 月，世界上第一个 WEB 站点（nxoc01.cern.ch）由欧洲原子能中心（CERN）在 Internet 上建立 [1]。由于 WEB 站点从一开始就具备“所有见即所得”（WYSIWYG：What You See Is What You Get）的特性，非常适合用来检索和展示信息，因此 WEB 站点数量随着 Internet 的发展迅猛增加。到 2009 年 5 月止，Internet 上的 WEB 站点总数已经达到 235,890,526 个 [2]。同时随着 YouTube 为代表的在线视频网站的兴起，2007 年 WEB 站点所产生的流量占整个 Internet 流量的 46%，超过 P2P 的 37%，占 Internet 流量排行的首位 [3]。

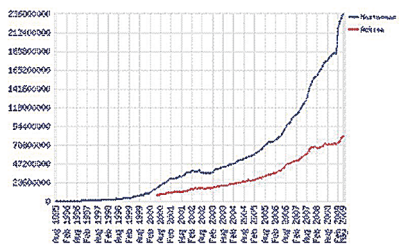


图 1.1 WEB 站点发展（1995-2009）

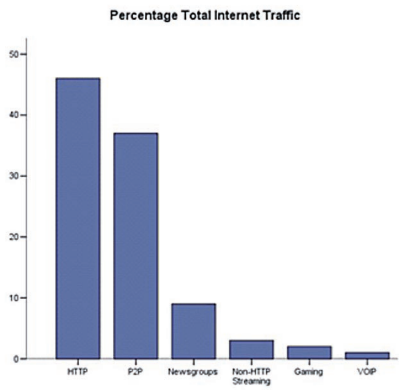


图 1.2 Internet 流量分析（2007）

随着 WEB 技术的发展成熟，越来越多的商业应用基于 B/S 架构开发：不仅客户关系管理系统（CRM）、财务系统、企业资源规划（ERP）这些企业级应用开始转向 B/S 架构，就连个人日常生活中所使用的网上银行、网上交易等都开始转向 B/S 架构。同时，随着 AJAX、云计算、富 Internet 应用（RIA）等一系列技术变革，像电子邮件、办公软件等越来越多的传统软件开始向 WEB 转向 [4]。

越来越危险的 WEB 环境

随着 WEB 技术体系的复杂度不断增加，越来越多针对 WEB 技术的攻击方法不断被安全研究人员发现。2007 年全球安全研究人员所发现的安全漏洞中有 59% 的漏洞为 WEB 应用安全漏洞，而 2008 年这项数据更是高达 63%。与此同时安全研究人员还发现，在所发现的 WEB 安全威胁中仅有很少的一部分会被修复——以跨站脚本（XSS）漏洞为例，在 2008 年仅有 3% 的跨站脚本（XSS）漏洞被修复 [5]。

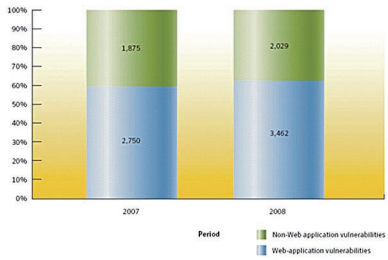


图 1. 3 WEB 应用相关安全漏洞(2007-2008)

由于越来越多的应用开始使用 WEB 技术开发，越来越多的 WEB 应用相关的漏洞被发现，攻击者也逐渐地把攻击目标转向了 WEB 站点。2007 年 7 月至 2008 年 6 月之间，全球地下经济规模已经达到了 2.75 亿美元，可能造成的潜在损失达 70 亿美元 [6]。而在 2008 年最后一个季度中，全球针对 WEB 站点的攻击流量占所有攻击流量的 14.5%[7]。而在国内，自 2006 年开始针对 WEB 站点的攻击流量始终占所有攻击流量的绝大部分 [8]。目前，针对 WEB 站点的攻击已经形成了自动化工具。仅 2008 年上半年，全球范围内就至少有 50 万 WEB 站点遭自动化的 SQL 注入攻击工具攻击 [9]。如图 1.4 和 1.5 所示。

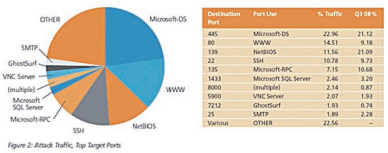


图 1. 4 全球攻击流量分析(2008Q4)

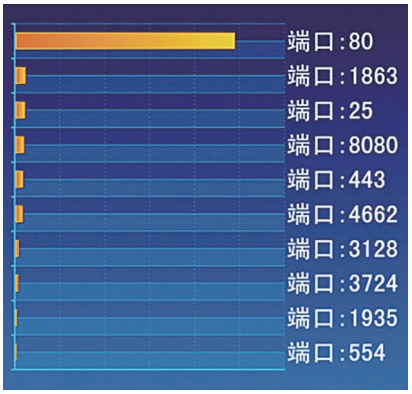


图 1.5 国内攻击流量分析 (2009 年 5 月 4 日 -2009 年 5 月 8 日)

随着 WEB 技术应用的范围越来越广泛，WEB 技术相关的安全漏洞越来越多的被挖掘出来，而针对 WEB 站点的攻击已经成为了最流行的攻击途径。如何保护 WEB 站点，在未来必将成为安全厂商最重要的任务之一。事实上，从 RSA Conference 2009 参展情况来看，参展的众多厂商都提供了保护 WEB 安全的解决方案、产品和服务。从 WEB 应用的网关级防护，到 WEB 安全漏洞的扫描，WEB 内容的安全审计，甚至 WEB 应用的安全生命周期管理等等，覆盖面之广，足见 WEB 安全的重要性 。

图 1.6 RSA Conference 2009 参展厂商统计资料

WEB 体系基本分析

在 WEB 系统中，基本的角色可以划分为四大类：服务提供者、网络提供者、浏览者和监管者。数量庞大的服务提供者和数量

更为庞大的浏览者端通过数量相对而言很小的网络提供商连接，而监管者对整个 WEB 环境进行监管、治理。

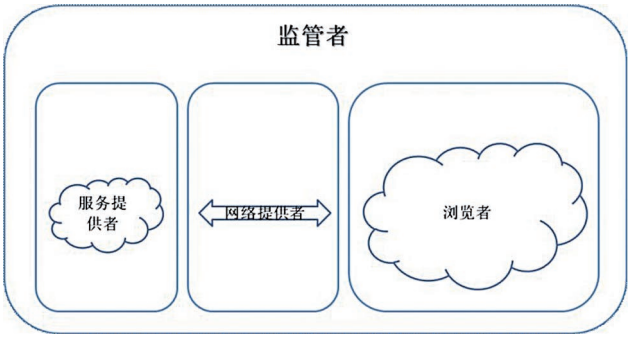


图 2.1 WEB 体系相关角色

在信息数据交换层面，服务提供者希望所有发布的信息数据能够随时被浏览者快速地获取到；而浏览者希望能够访问到自己希望访问的信息数据；网络提供者希望能够尽快的完成服务提供者和浏览者的信息数据交换；而监管者希望所有的信息数据都是真实、合法的，所有虚假的或不合法的信息数据都能被追溯并处置。

由于服务提供者和浏览者数量都很庞大，直接进行监管和治理比较困难。因此监管者一般从数量较少的网络提供者入手来实现对服务提供者和浏览者进行监管和治理；但在具有强约束力的组织内，监管者也会通过一定的技术手段对服务提供者和浏览者进行直接的监管和治理。

WEB 体系相关角色	安全目标
监管者	**确保所有的信息数据都是真实、合法的** 1. 能够找到所有的信息数据 2. 能够判断信息数据是否真实、合法 **确保所有虚假的或不合法的信息数据都能被追溯并处置** 1. 能够找到所有信息数据 2. 能够从中找到所有虚假的或不合法的信息数据 3. 能够追溯虚假的或不合法的信息数据传播路径（生产、存储、传播、消费） 4. 能够对虚假的或不合法的信息数据传播路径进行处置
服务提供者	**确保所有信息数据都是真实、合法的（被监管产生）** 1. 能够掌握自身所有的信息数据 2. 能够判断自身所有的信息数据是否真实、合法 3. 确保无法发布虚假的或非法的数据（被动的角度） **确保所有发布的信息数据能够随时被浏览器快速的获取** 1. 所有发布的信息数据能被获取 2. 所有发布的信息数据能被快速获取 3. 非发布的信息数据无法被获取
网络提供者	**监管者需求（所有监管者的需求）** **尽快的完成服务提供者和浏览者的信息数据交换** 1. 能够完成服务提供者和浏览者的信息数据交换 2. 能够快速的完成服务提供者和浏览者的信息数据交换
浏览者	**确保所有的信息数据都是真实、合法的（被监管产生）** 1. 能够访问的信息数据都是真实、合法的 2. 无法提交虚假的或非法的信息数据 3. 一旦访问或提交了虚假或非法的数据，可以被找到并被处置 **确保能够访问到自己希望访问的信息数据** 1. 能够访问到自己希望访问的信息数据 2. 不会访问自己不希望访问的信息数据 3. 当访问到自己不希望访问的信息数据时能够得知告警

WEB 体系基础架构

要对 WEB 系统提供安全防护，必须了解 WEB 基础架构。WEB 服务提供者的技术平台通常由网络平台、操作系统、一般服务组件、特定应用构成；而浏览者的技术平台通常是由浏览器、操作系统、网络平台构成；浏览器端和服务器通过技术平台交换信息数据，在整个 WEB 体系技术平台之上承载的是信息数据。

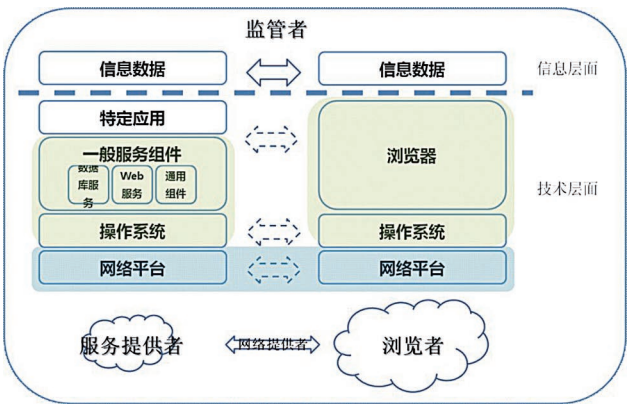


图 2.2 WEB 体系架构

对于整个 WEB 体系而言，各层次的安全需求的满足都依赖于下层提供的安全保障，例如：信息层面要求“所有未发布的数据都无法访问”，如果攻击者可以通过某种技术手段窃取，那毫无疑问信息层面的需求是无法得到满足的。

在 WEB 体系内，一般服务组件、操作系统、网络平台、浏览器一般都是通用的软件或硬件产品。除监管者以外，其他的各个角色一般仅仅作为使用者使用最终的通用软件或硬件，很难对其整个生命周期产生直接的影响。这些通用软件或硬件安全问题一直以来都是信息安全厂商所重点考虑的部分，目前已经有了较为成熟的解决方案。

用户特定应用千差万别，往往是用户为了满足自身需求而开发的，其整个生命周期都在用户控制范围之内。如何确保特定应用的安全，正是信息安全领域的难点和热点。从统计数据来看，WEB 体系的技术层面的风险目前已经集中在用户特定应用上，只有控制好用户特定应用的安全性，提高对特定应用的风险控制能力才能有效地控制 WEB 体系的整体安全风险。

WEB 系统技术平台的生命周期

任何 WEB 系统技术平台的生命周期无外乎设计、开发（包括测试）、部署、运维、消亡这几个阶段。

图 3.1 WEB 体系技术平台生命周期

对于整个体系而言，对安全风险的控制在整个生命周期中越早进行控制越有效、整体控制成本越低。但在整个 WEB 系统中，仅仅只有用户特定应用的整个生命周期被用户所掌控。如何在整个生命周期内控制特定应用的安全风险，必将成为 WEB 系统安全风险控制技术层面的核心部分。

	设计	开发	部署	运维	消亡
网络平台	不可控	不可控	可控	可控	可控
操作系统	不可控	不可控	可控	可控	可控
一般通用组件	不可控	不可控	可控	可控	可控
浏览器	不可控	不可控	可控	可控	可控
特定应用	可控	可控	可控	可控	可控

参考资料

[1] Connolly Dan. 2000.《A Little History of the World Wide Web》. http://www.w3.org/. [联机] World Wide Web Consortium, 2000 年 . http://www.w3.org/History.html.

[2] Netcraft. 2009.《May 2009 Web Server Survey》. http://www.Netcraft.com/. [联 机] Netcraft LTD, 2009 年 5 月 . http://news.netcraft.com/archives/2009/05/27/may_2009_web_server_survey.html.

[3] Ernesto. 2007.《HTTP Traffic Overtakes P2P, Courtesy of YouTube》. http://TorrentFreak.com/. [联 机] Ellacoya, 2007 年 6 月 18 日 . http://torrentfreak.com/http-traffic-overtakes-p2p-courtesy-of-youtube/.

[4] Gartner. 2009.《Gartner Says 20 Percent of Commercial E-Mail Market Will Be Using a SaaS Platform By the End of 2012》. http://www.gartner.com/. [联机] Gartner, Inc., 2009 年 4 月 . http://www.gartner.com/it/page.jsp?id=931215

[5] Symantec. 2009.《Internet Security Threat Report Volume XIV》. http://www.symantec.com/. [联机] 2009 年 4 月 . http://www.symantec.com/business/theme.jsp?themeid=threatreport.

[6] Symantec. 2008.《Symantec Report on the Underground Economy》. Symantec. [联 机] 2008 年 . http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.

[7] Akamai Technologies. 2009.《The State of the Internet: 2008 Q4》. http://www.akamai.com/. [联 机] 2009 年 . http://www.akamai.com/stateoftheinternet/.

[8] 国家计算机网络应急技术处理协调中心 . 2009.《协议流量监测》. http://www.cert.org.cn/. [联机] 2009 年 . http://www.cert.org.cn/servlet/SubChannelArticles?channel=chart&sub=1.

[9] ZDnet. 2008.《SQL 注入攻击第三波浪潮袭来》. http://security.zdnet.com.cn/. [联 机] 2008 年 7 月 . http://security.zdnet.com.cn/security_zone/2008/0708/968547.shtml.

2008年WEB攻击技术TOP 10

研究部 左磊

摘要：Whitehat Security 公司的 CTO Jeremiah Grossman 在 RAS 2009 大会上做了名为 2008 十大 WEB 攻击技术的主题演讲，在研究了 2008 年所发布的近 70 种 WEB 攻击技术之后，根据攻击技术的新颖性、影响范围选出了其中最具代表性的 Top 10。

关键词：RSA WEB 攻击技术 TOP10

Whitehat Security 公司的 CTO Jeremiah Grossman 在 RAS 2009大会上做了名为2008十大WEB攻击技术的主题演讲，在研究了 2008 年所发布的近 70 种 WEB 攻击技术之后，根据攻击技术的新颖性、影响范围选出了其中最具代表性的 Top 10。

这里的 WEB 安全包括了 WEB 服务端和客户端安全，其中浏览器以及富文本应用的安全问题是其中比较值得关注的。

1.GIFAR 攻击

这个攻击非常有趣。它的思想是将一张 GIF 图片和一个 JAR 文件拼在一起，然后命名成 aaa.gif，这个新文件的前一部分是 GIF，后一部分是 JAR 文件。很多 WEB 服务提供商为了安全只允许上传图片，但对文件内容的检查通常只是简单的检查一下文件头部分是否符合，因此我们新生成的文件就可顺利通过检查，从而绕过安全限制。这样一个包含有 JAR 内容的文件就被传上了网站，而 Sun 的 Java 解释器在解析这样的文件时，又十分“智能”地忽略了前面它不认识的 GIF 文件数据，从而导致 JAR 文件中的恶意 Java 脚本可以在客户端浏览器上被执行。如果这种恶意文件可以传到一些大的 WEB 服务网站上（例如 google.com），则可能产生极大的危害。

2. 突破 Google Gears 的跨域通信机制

Google Gears 是 Google 提供的一个 RIA（富客户端）工具。它的跨域安全机制在某些情况下可以被绕过，攻击者可能获取受害用户在另外一个网站上的敏感数据，例如论坛、WEB 邮件、社交网站等信息。

3.Safari 地毯式轰炸

Safari 是苹果公司开发的 WEB 浏览器。它在处理一个 Content-

type 无法被浏览器渲染的文件时，会自动将其保存在默认下载目录下 (Windows 下是桌面，OSX 下是 Downloads 目录)。但这个动作是自动完成的，并没有提醒用户，也没有要求用户确认。恶意攻击者只要创建一个包含大量引用恶意程序的网页，就可以迅速占满桌面或者 Downloads 目录，形成地毯式轰炸的效果。

4. 点击欺骗

眼见不一定为实，这对于网页浏览也同样适用。利用隐藏 iFRAME 的技巧，可以让你以为是在点击一个按钮或者一个链接时，实际上是在允许恶意程序访问你的摄像头或者麦克风，这样恶意网页就可以监视你的一举一动。

5.Opera 跨站脚本漏洞

Opera 的 opera:historysearch 功能存在一个跨站脚本漏洞，通过注入一个 iFRAME 页面，利用 opera:config 功能设置 E-mail 客户端改成执行任意命令，再打开一个包含 mailto: 的窗口，就可以执行任意命令。

6.HTML 5 结构化客户端存储滥用问题

HTML 5 版本引入了几种方式可以允许浏览器在客户端主机上存储大量数据，攻击者可以修改或者读取这些数据。如果一个使用这些数据的 WEB 应用程序存在跨站脚本漏洞，攻击者就可以插入恶意代码并让其执行。

7. 通过认证后的 CSS 获取站点登录信息

利用标准的 javascript API 就可以跨域载入一个 stylesheet，然后读取其中的 property 值。通常用户在登录一个网站前后，property 值的内容会有所区别，利用这种技术可以准确地判断用户是否登录某一网站。

8. 通过 SQL 注入实现 TCP 隧道

结合 Squeeza 和 reDuh 工具，可以利用一个存在 SQL 注入的 WEB 应用来实现 TCP 隧道，从而绕过防火墙的的限制。

9. 改变 ActiveX 控件的意图

ActiveX 控件往往会提供很多强大的功能，如果一旦设计上不够小心，就会带来致命的威胁。演讲者介绍了一个实例，首先诱骗攻击者去访问一个恶意页面，诱使用户进行控件安装和升级，将一个恶意的配置文件下载到本地，配置文件已将卸载程序改成了一个任意命令，恶意页面则再度调用卸载功能，就会导致任意本地命令的执行。ActiveX 控件的开发者除了要考虑不要出现缓冲区溢出等常见问题之外，也要特别小心不要被攻击者利用其提供的功能进行攻击。

10.Flash 参数注入

Flash 参数注入是一种新的攻击方式，可以将数据注入到一个 HTML 页面内嵌的 flash 电影的全局参数中。这些注入的数据可以让攻击者完全控制该 HTML 页面的 DOM 元素，利用 flash 与 HTML 页面之间的交互，攻击者可能造成更大的威胁。

威胁WEB安全的幕后黑手

行业营销中心 李钠

摘要：从 WEB 体系入手，对 WEB 体系信息层面和技术层面所面临的安全威胁进行综述，并对一些流行的攻击方法进行介绍。

关键词：WEB 安全威胁

从WEB 体系架构来看，WEB 服务提供者的技术平台通常由网络平台、操作系统、一般服务组件、特定应用构成；而浏览者的技术平台通常是由浏览器、操作系统、网络平台构成；浏览器端和服务器通过技术平台交换信息数据；在整个 WEB 体系技术平台之上承载的是信息数据。

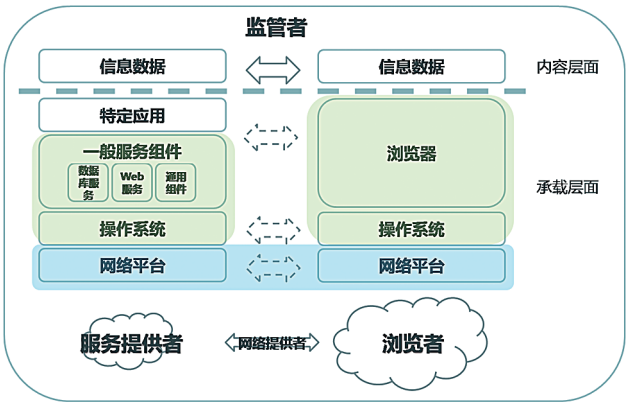


图 1 WEB 体系架构

在 WEB 体系架构中，信息层面的安全威胁主要来自于虚假信息、非法信息、信息失密等，我们经常听到的网络谣言、挂马站点、网络钓鱼、泄密等都属于此类型的安全威胁的具体形式。在信息层面中要降低安全威胁的影响，一方面要能及时发现网络中的信息数据，并能够通过计算机自动发现信息数据是否属于虚假信息或非法信息，是否存在泄密信息；另一方面，对于已经发现的虚假信息、非法信息、泄密信息，要能发现其传播路径并对其传播路径进行处置。监管者尤其重视这个层面的监管和治理，所有的监管手段和技术手段都是为了实现对信息数据的监管和治理。

而在技术层面，技术体系中包含的操作系统、浏览器、一般服务组件、网络平台层次所面临的安全威胁都是常见的安全威胁，包括恶意代码（病毒、蠕虫、流氓软件等）、暴力破解、拒绝服务等。而这些安全威胁通过良好的部署、运维策略，结合一些必要的技术手段，就能最大限度的降低安全威胁的影响。因此在整个 WEB 体系中，目前整个技术层面惟一缺乏的是针对特定应用的有效的体系化安全风险控制措施。而如何通过对特定应用整个生命周期的控制对安全风险进行控制，必将成为整个 WEB 体系技术平台对抗安全威胁的重点。

	设计	开发	部署	运维	消亡
开发团队	负责	负责	参与		
运维团队	参与		负责	负责	负责
安全团队	协助	协助	协助	协助	协助

图 2 WEB 体系技术平台生命周期

在整个 WEB 体系技术平台的生命周期中，由“设计”阶段转向“开发”是一个非常重要的控制点，整个具体的 WEB 应用将逐渐成型。这个控制点直接决定了整个系统的安全性，其他阶段只是落实设计阶段的要求或对设计阶段未考虑的问题进行弥补。而“部署”阶段转向“运维”阶段也是一个非常重要的控制点，整个 WEB 应用的建设已经告一段落。这个控制点直接决定了 WEB 体系技术平台整个生命周期中最长的“运维”阶段的安全基准水平。因此，如何在这两个控制点上有效的对安全威胁进行控制是对整个生命周期控制的整体基础。

在特定应用这个层面，各种安全威胁主要通过各种攻击手段对其的脆弱性发起攻击。在 OWASP 统计的 2007 年 WEB 应用面临的最常见攻击行为如下（针对详细攻击方式的描述请参考 http://www.owasp.org/index.php/Category:Attack）：

跨站脚本 Cross Site Scripting (XSS)

注入缺陷 Injection Flaws

不安全的远程文件执行 Malicious File Execution

不安全的直接对象引用 Insecure Direct Object Reference

跨站请求伪造 Cross Site Request Forgery (CSRF)

信息泄漏和异常错误处理 Information Leakage and Improper Error Handling

验证和会话管理缺陷 Broken Authentication and Session Management

不安全的加密存储 Insecure Crypto-graphic Storage

不安全的通信 Insecure Communications

URL 访问控制失效 Failure to Restrict URL Access

参考资料

[1] OWASP Foundation. 2007.《Top 10 2007》. http://www.owasp.org/. [联　机] OWASP Foundation, 2007 年 . http://www.owasp.org/index.php/Top_10_2007.

热点、焦点与观点:云安全与SaaS

国际拓展部 韩永刚

摘要：纵观此次 RSA 2009 Conference，云计算（Cloud Computing）与 SaaS 无疑是一个热点问题。你会感觉有无数的论坛与专家在关注云计算与 SaaS 的安全问题。不论从 Keynote 主题演讲中的钱伯斯、著名密码专家 Whitfield Diffie、Ronald Rivest，还是 Qualys 的 CEO Philippe Courtot，以及各个领域的安全专家都在讨论云计算、云安全、SaaS 方面的问题。

关键词：RSA2009 云计算 SaaS

热点：云与 SaaS

纵观此次 RSA 2009 Conference，云计算（Cloud Computing）与 SaaS 无疑是一个热点问题。你会感觉有无数的论坛与专家都在关注云计算与 SaaS 的安全问题。不论从 Keynote 主题演讲中的钱伯斯、著名密码专家 Whitfield Diffie、Ronald Rivest，还是 Qualys 的 CEO Philippe Courtot，以及各个领域的安全专家都在讨论云计算、云安全、SaaS 方面的问题。我们正在思考，但还没有明确答案的各种问题，也在各个会场被激烈讨论着。云与 SaaS 本已是热点，再加上安全，你能够理清思路吗？云计算、安全的云计算、云安全、Software as a Service、Security as a Service、Security as a (Cloud) Service…

焦点 1：云的安全

钱伯斯在 RSA Conference 第二天的主题演讲中，提到云计算时语出惊人：“对于安全，云计算是一场噩梦”。注意，他并不是对云计算有何异议，因为老钱同志也认为云计算是不可避免的趋势，而且云计算的发展肯定对 Cisco 的发展有着巨大的意义。但是由于云计算所引发的新的安全问题，则又是很难预测的。这些问题甚至会动摇我们已经形成的网络安全的体系方法。“它是网络安全的噩梦，而且无法采用传统的方法来解决”。

无独有偶，在几个著名的密码专家论坛上，云计算也成为了话题。虽然专家们有的对云计算的前景非常看好，但云计算产生了与以往不同的新安全问题也是共识。而这些安全问题，是我们无法回避且必须付出很大的努力来解决的。当然对解决云计算安全问题持悲观态度的人也不在少数。

焦点 2：*aaS 的安全

另一个方面，SaaS 也是热点议题。对于 SaaS 这种模式，安全问题存在于它的各个层次：基础设施、平台、上层应用。对于三个层次，所面临的安全问题是不同的。比如对于 IaaS（Infrastructure as a service），数据中心建设、物理安全、网络安全、传输安全、系统安全是主要的关注点。而对于 PaaS（Platform as a Service），数据安全、数据与计算可用性、灾备与恢复问题则更受关注。而到了最高层的 SaaS（Software as a Service），则对于数据与应用的安全问题更为关注。而且，当 SaaS 架构在云计算这个平台上时，最高层的这些安全问题很多是不可知，不可控的。原因在于，使用者再也无法自己实际掌握对安全便捷与数据的控制权。

观点：绿盟对云安全的认识

从我们的角度来看，云只不过是另一种数据中心，数量更多且分散的数据中心的集合，使得访问与使用更加的快速、便捷。再加上云端的 SaaS 应用，能够为众多企业，尤其是中小企业，带来更便捷、成本更低的、无所不在的 IT 服务。但同时，云计算与 SaaS 也带来了新的安全问题，与以往我们经验中不同的安全问题。因为在云中，没有边界，云计算与 SaaS 的使用者自己再也无法控制边界、控制数据，甚至都不确切地知道数据在什么位置上。而服务提供者往往还要同时面对 IaaS、PaaS、SaaS 三个层次的安全问题。

从云的外部，用户看不到云里面是什么样子的，也就是说云是不透明的。服务提供商承诺会提供各种层次的安全方案，从网络层到应用层、数据保护以及可管理的安全服务。但是作为云外的用户，你真的知道这些安全特性被提供了吗？或者说，这些安全措施的结果，是你所期待且满意的吗？这可能也是很多企业对云计算望而却步的原因，也是众多安全专家的争论所在。不过换个角度，对于很多本来就没有能力进行安全体系建设与维护的用户来说，看不清云的内部也不见得是件坏事。

随之而来的问题：云计算如何进行审计与监管？现实中的各种信息安全问题在云端依然存在，只不过之前是用户自己能看到的，而现在反而距离用户更远了，也更为离散。如果像钱伯斯所说云计算可能是无法避免的趋势，当然这还需要最终用户的认可。那么我们真的需要更多的工作，来接受这种新模式并克服它所带来的新安全问题。

未完的故事

其实涉及这方面的待解问题还有很多，比如在 IaaS 中，虚拟化（Virtualization）技术被更多的应用，物理边界变成了逻辑边界，对于安全的思考也会变化。再者，除了讨论安全的云，我们也能够同时利用云计算的方式，来促进安全的发展，将安全也作为一种云计算服务。新的事物总是能够带来新的挑战，迎接这种挑战，正是我们不断前进的动力。当这些问题正在被激烈的讨论时，你，准备好了吗？

WEB应用防火墙解读

产品市场部 赵旭

摘要：本文结合一家第三方互联网支付公司遇到的安全事件，介绍了来自 web 安全的挑战，以及 Web 应用安全的防护解决思路。并对如何正确选择 WAF、正确配置使用 WAF 提供了建议。

关键词：WEB 应用安全 WAF

作为一家第三方互联网支付公司的CIO，Dave 为公司近期发生的一系列安全事件忙得焦头烂额。虽然已经在公司的网络出口处部署了防火墙、入侵检测系统等安全设备，但是几个月前，公司网站和支付服务器还是遭受到拒绝服务攻击导致业务瘫痪。拒绝服务攻击事件还没处理完，Dave 又接到员工报告，公司门户网站被 Google 报出含有恶意软件。

来自 WEB 的安全挑战

Dave 的烦恼其实是目前众多 IT 管理者遭遇的缩影之一。随着机构的计算及业务资源逐渐向数据中心高度集中，WEB 成为一种普适平台，上面承载了越来越多的核心业务。WEB 的开放性带来丰富资源、高效率、新工作方式的同时，也使机构的资产暴露在越来越多的威胁中。现今 WEB 安全问题对我们来说已屡见不鲜，以下是收录于国际安全组织 WASC WHID 项目中的几起安全事件 [1]:

2009 年 5 月 26 日，法国移动运营商 Orange France 提供照片管理的网站频道有 SQL 注入漏洞，黑客利用此漏洞获取到 245,000 条用户记录（包括 E-mail、姓名及明文方式的密码）。

2009 年 1 月 26 日，美国军方两台重要的服务器被土耳其黑客渗透，网页被篡改，黑客采用的是 SQL 注入攻击手段。

2009 年 1 月 26 日，印度驻西班牙使馆网站被挂马（通过 iFrame 攻击植入恶意代码）。

WEB 应用安全防护解决思路

WEB 应用安全问题本质上源于软件质量问题。但 WEB 应用相较传统的软件，具有其独特性。WEB 应用往往是某个机构所独有的应用，对其存在的漏洞，已知的通用漏洞签名缺乏有效性；需要频繁地变更以满足业务目标，从而使得很难维持有序的开发周期；需要全面考虑客户端与服务端的复杂交互场景，而往往很多开发者没有很好地理解业务流程；人们通常认为 WEB 开发比较简单，缺乏经验的开发者也可以胜任。

针对 WEB 应用安全，理想情况下应该在软件开发生命周期遵循安全编码原则，并在各阶段采取相应的安全措施。然而，多数网站的实际情况是：大量早期开发的 WEB 应用，由于历史原因，都存在不同程度的安全问题。对于这些已上线、正提供生产的 WEB 应用，由于其定制化特点决定了没有通用补丁可用，而整改代码因代价过大变得较难施行或者需要较长的整改周期。

针对这种现状，专业的 WEB 安全防护工具是一种合理的选择。WEB 应用防火墙（以下简称 WAF）正是这类专业工具，提供

了一种安全运维控制手段：基于对 HTTP/HTTPS 流量的双向分析，为 WEB 应用提供实时的防护。与传统防火墙 /IPS 设备相比较，WAF 最显著的技术差异性体现在以下几个方面。

对 HTTP 有本质的理解：能完整地解析 HTTP，包括报文头部、参数及载荷。支持各种 HTTP 编码（如 chunked encoding、request/response 压缩）；提供严格的 HTTP 协议验证；提供 HTML 限制；支持各类字符集编码；具备 response 过滤能力。

提供应用层规则：WEB 应用通常是定制化的，传统的针对已知漏洞的规则往往不够有效。WAF 提供专用的应用层规则，且具备检测变形攻击的能力，如检测 SSL 加密流量中混杂的攻击。

提供正向安全模型（白名单）：仅允许已知有效的输入通过，为 WEB 应用提供了一个外部的输入验证机制，安全性更为可靠。

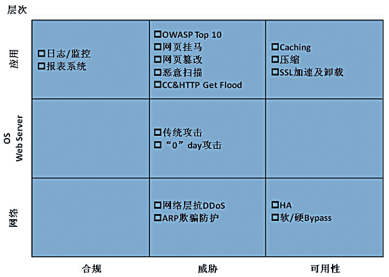
提供会话防护机制：HTTP 协议最大的弊端在于缺乏一个可靠的会话管理机制。WAF 为此进行有效补充，防护基于会话的攻击类型，如 cookie 篡改及会话劫持攻击。

如何正确选择 WAF

并非对 WEB 服务器提供保护的“盒子”都是 WAF。事实上，一个真正满足需求的 WAF 应该具有二维的防护体系：

纵向提供纵深防御：通过建立协议层次、信息流向等纵向结构层次，构筑多种有效防御措施阻止攻击并发出告警。

横向：满足合规要求；缓解各类安全威胁（包括网络层面、WEB 基础架构及 WEB 应用层面）；降低服务响应时间、显著改善终端用户体验，优化业务资源和提高应用系统敏捷性。



在选择 WAF 产品时，建议参考以下步骤：

结合业务需求明确安全策略目标，从而定义清楚 WAF 产品必须具备的控制能力；

评估每一家厂商 WAF 产品可以覆盖的风险类型；

测试产品功能、性能及可伸缩性；

评估厂商的技术支持能力；

评估内部维护团队是否具备维护、管理 WAF 产品的必需技能；

权衡安全、产出以及总成本。“成本”不仅仅意味着购买安全产品 / 服务产生的直接支出，还需要考虑是否影响组织的正常业务、是否给维护人员带来较大的管理开销。

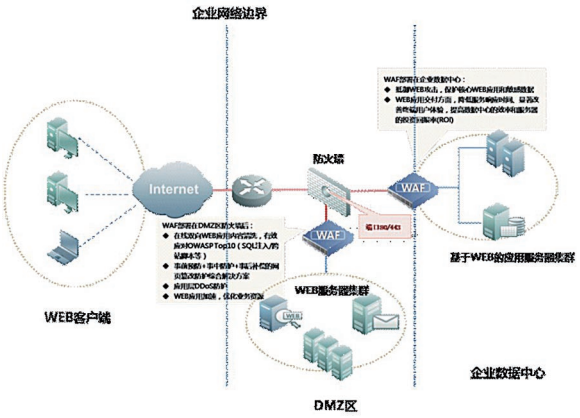
WAF 应用场景

通过前文的介绍，大家对 WAF 产品已经有了初步了解。但也可能存在疑问，部署 WAF，实际到底可以解决什么问题？下面将介绍几个典型的应用场景。

WAF 支持完全代理方式，作为 WEB 客户端和服务器端的中间人，避免 WEB 服务器直接暴露在互联网上，监控 HTTP/HTTPS 双向流量，对其中的恶意内容（包括攻击请求以及网页内容中被植入的恶意代码）进行在线清洗。

网页篡改在线防护

按照网页篡改事件发生的时序，提供事中防护以及事后补偿的在线防护解决方案。事中，实时过滤 HTTP 请求中混杂的网页篡



改攻击流量（如 SQL 注入、XSS 等）。事后，自动监控网站所有需保护页面的完整性，检测到网页被篡改，第一时间对管理员进行短信告警，对外仍显示篡改前的正常页面，用户可正常访问网站。

网页挂马在线防护

网页挂马为一种相对比较隐蔽的网页篡改方式，本质上这种方式也破坏了网页的完整性。网页挂马攻击目标为各类网站的最终用户，网站作为传播网页木马的“傀儡帮凶”，严重影响网站的公信度。

当用户请求访问某一个页面时，WAF 会对服务器侧响应的网页内容进行在线检测，判断是否被植入恶意代码，并对恶意代码进行自动过滤。

敏感信息泄漏防护

WAF 可以识别并更正 WEB 应用错误的业务流程，识别并防护敏感数据泄漏，满足合规与审计要求，具体如下:

可自定义非法敏感关键字，对其进行自动过滤，防止非法内容发布为公众浏览。

Web 站点可能包含一些不在正常网站数据目录树内的 URL 链接，比如一些网站拥有者不想被公开访问的目录、网站的 WEB 管理界面入口及以前曾经公开过但后来被隐藏的链接。WAF 提供细粒度的 URL ACL，防止对这些链接的非授权访问。

网站隐身：过滤服务器侧出错信息，如错误类型、出现错误脚本的绝对路径、网页主目录的绝对路径、出现错误的 SQL 语句及参数、软件的版本、系统的配置信息等，避免这些敏感信息为攻击者利用、提升入侵的概率。

对数据泄密具备监管能力。能过滤服务器侧响应内容中含有的敏感信息，如身份证号、信用卡号等。

WEB 应用交付

WAF 同时提供 SSL 加速及卸载、WEBcaching 及压缩等功能。

通过应用加速，有效补偿由于传统安全设备检测、过滤处理引入的时延，优化服务器侧业务资源，改善最终用户体验。

整合基础架构，降低维护的复杂性，节约基本建设费用及后期维护成本。简化及统一策略管理，极大提高效率。

加速加密流量。

参考资料

[1]The Web Hacking Incidents Database, URL: http://www.xiom.com/whid

OWASP:专注于WEB安全的社区

研究部 汪列军

摘要：OWASP (Open Web Application Security Project) 是一个世界范围的关注 WEB 应用安全的虚拟社区，其使命是提高 WEB 应用软件的安全性。本文介绍了该社区的基本内容，便于用户通过该社区了解最新 WEB 安全的研究成果和技术方向。

关键词：OWASP Web 应用安全 虚拟社区

OWASP (Open Web Application Security Project) 是一个世界范围的关注 WEB 应用安全的虚拟社区，其使命是提高 WEB 应用软件的安全性。社区采用自由开放的组织形式，用户可以自由地参与 OWASP 的活动，免费地使用其提供的各种资源。OWASP 提供了大量关于 WEB 应用安全相关的资源，包括文档、工具、论坛、邮件列表等，几乎囊括了你能想的到的 WEB 安全的方方面面，OWASP 凭借其独特的组织形式和强大的资源整合能力成为目前互联网上在WEB安全领域运作得最成功、最有影响力的组织。

区别于其他很多纯交流性质的自由安全组织，OWASP 下辖一个非赢利性的基金会。基金会专门执行鼓励、接收来自个人或企业的捐款的任务，这些捐助会被用于支持 OWASP 的项目、授权、活动或一些基础设施。从目前网站上的介绍来看，基金会已经得到了不少大型组织或企业的支持，比如微软、HP、诺基亚、赛门铁克等，一定的资金保证为组织得以长期发展提供了有力的支撑。

OWASP 另一个独特的内容是不定期的 AppSec 会议。从目前的实践来看，举行业界会议是扩展组织影响力的非常有效的手段，OWASP 从 2004 年开始每年在全球各地召开不定期的 AppSec 研讨会，把企业、政府、安全研究人员召集在一起讨论应用安全的问题，分享经验和教训。对于安全从业人员或爱好者，在 AppSec 会上可以追踪到最新的 Web 安全研究热点和技术动态，对于企业和厂商，可以在会上发布新产品、推广新概念。AppSec 会议已经在美国、欧洲、亚洲、澳洲及以色列成功举办，迅速成为 Web 应用安全方面的全球盛会。用户参加 AppSec 会议是需要交费的，但会议中的演讲资料可以从 OWASP 网站上免费下载。这类从有影响力的组织派生出来的会议，操作得当的话拥有巨大的商业价值，随着影响力的扩大，AppSec 会议可能成为 OWASP 获取收益支持运作的最主要资金来源。

作为参与 OWASP 社区活动的主要形式，OWASP 提供了接近 300 个邮件列表，

这在其他开源社区中是极少见的，用户可以根据自己的需要订阅。列表基本分为三类：第一类是全球性用于成员参与事务管理的，关注于项目、教育、本地协作及业界等方面；第二类是具体相关项目，基本上 OWASP 的每个项目都有对应的列表，用户可以通过它了解项目的最新进展，也可以发文提出自己的建议；第三类是地区性讨论，OWASP 甚至为几乎每个国家都设置了列表，方便本地 OWASP 组合的通信和协作。

对于一般用户，OWASP 的大量项目是最主要最实用的资源，项目主要涉及 WEB 应用的开发过程、安全性的检测评价、安全技能和意识的教育及应用的配置管理等方面。OWASP 的项目从形式上大致分为文档和工具两类，从功能上分主要分为检测和保护两类，这些文档或工具按成熟度标记为 Release、Beta、Alpha 发布状态，事实上 Release 和 Beta 状态的资源已经具有相当高的使用价值。目前 OWASP 大约包含了 55 个工具项目和 52 个文档项目，下面推荐 3 个有代表性的且非常实用的项目：

OWASP Top Ten

OWASP Top Ten 项目提供了目前一致公认的最严重的十类 WEB 应用安全漏洞列表，对每类安全问题提供了详细的威胁判定、成因分析及解决方案，可以使 Web 应用管理员对照列表结合自身环境尽快地梳理出影响自身应用安全的主要方面并采取对应的有重点的保护防范措施。目前有英语、法语、日语、韩语和土耳其语版本，以及正在开发的西班牙语版本。

OWASP WebScarab

WebScarab 是一种检测分析 WEB 应用安全问题的工具，使用 Java 编写，因此可以移植到很多平台。WebScarab 有多种运行方式，由多个插件实现。在最常见的使用中，WebScarab 运行为拦截代理，拦截 HTTP 和 HTTPS 通讯，操作者可以查看通过 WebScarab 所传送的会话数据，允许操作者在将浏览器所创建的请求发送到服务器之前查看并修改这些请求，并在浏览器接收到响应之前查看并修改返回的响应。WebScarab 还可以自动化地执行一些探测操作，比如自动遍历目标网站、检测 SQL 及 XSS 漏洞等。

OWASP WebGoat

WebGoat 是由 OWASP 维护的故意设计为不安全的 J2EE WEB 应用程序，用于教授 WEB 应用安全课程。在每节课中，用户必须通过利用 WebGoat 应用中真实的漏洞来显示对安全问题的理解。例如，在其中一节课程中用户必须使用 SQL 注入窃取伪造的信用卡号。该应用程序为真实的教学环境，为用户提供提示和代码以进一步解释课程。WebGoat 用 Java 编写，因此可以安装在 Java 虚拟机的任意平台上，有 Linux、OS XTiger 和 Windows 的安装程序。部署后用户可以体验各个课程并通过记分卡追踪进展。

还有更多其他有意思的项目，甚至不是安全相关的，具体请访问 OWASP 的网站:

http://www.owasp.org/index.php/Main_Page

市场动态

绿盟科技成功承办“2009 计算机安全专委会信息安全高级论坛”

6 月 16 日，由中国计算机学会计算机安全专业委员会主办，绿盟科技承办的“2009 计算机安全专委会信息安全高级论坛”在北京召开。本次会议以“RSA2009 国际信息安全技术热点及发展趋势”为主题，吸引了来自公安部、中国科学院、信息安全标准化委员会、网络安全企业等单位 的 100 多位代表参加。中国工程院院士沈昌祥、中科院

信息安全国家重点实验室教授翟起滨、绿盟科技副总裁吴云坤以及其他安全企业的代表在会上做了精彩的主题演讲。公安部网络安全保卫局副局长赵林、计算机安全专委会主任、北京邮电大学校长方滨兴院士、总裁沈继业做了热情洋溢的致词。

会议气氛热烈，计算机安全专委会常务副主任严明指出，“最近安全界的大事很多，现在召开此次会议非常及时也非常必要、意义重大”。会后，代表们还就会议主题展开了进一步的交流和讨论。

绿盟科技近三年持续领跑 IPS/IDS 国内市场

日前，国际权威调查机构 IDC 公布了最新的 2008 年下半年《中国 IT 安全硬件市场分析与预测》报告。报告称，2008 年国内入侵防御硬件市场凭借同比 100.6% 的增长比例，再次成为增长速度最快的安全子市场之一，其市场规模已经非常接近入侵检测硬件市场的市场规模，并且将在 2009 年全面超越后者。

相比高速增长的入侵防御硬件市场，入侵检测硬件市场成为了 2008 年国内惟一负增长的子市场，2008 年实际同比增长 -10.3%。对于该市场，IDC 仍保持乐观态度：从 2008 年到 2013 年五年的复合增长率为 1.2%，入侵检测硬件市场的市场规模在 2013 年将达到 6970 万美元。

根据 IDC 报告的统计数据显示，绿盟

科技的网络入侵防护系统和网络入侵检测系统表现强劲，近三年来持续占据国内入侵防御和检测市场的领导者地位。

作为漏洞研究和攻击防护领域的领导厂商，绿盟科技时刻关注各类安全威胁变化，通过不断的产品改进和服务完善，为用户提供最及时、有效的安全防护。历经四代入侵检测和防御技术的演变，绿盟科技的网络入侵检测系统和网络入侵防护系统已经成为业界领先产品，能够持续为用户交付高性能、高安全性，以及高可靠性的入侵防护解决方案。

绿盟科技成功举办“从 RSA 看安全行业整体发展趋势”媒体沙龙

6 月 5 日，绿盟科技“从 RSA 看安全行业整体发展趋势”媒体沙龙在京成功举办。会上，绿盟科技副总裁吴云坤就“经济危机下的安全机遇”做了主题发言，对目前全球安全行业的一些热点话题和趋势做了总结。绿盟科技产品市场部总监王伟和国际拓展部总监韩永刚也分别就 WEB 应用和云安全谈了自己的理解和看法。来自安全领域的 20 多家媒体记者参与了此次沙龙活动，并就这些热点话题，展开了深入的讨论。

吴云坤副总裁首先通过绿盟科技参加 2009RSA 展会的实地考察介绍了目前安全领域所关注的热点。他指出，“目前全球安全行业的热点主要集中在以下几个方面：WEB 安全、云计算、GRC、政府与国家关注的安全、身份管理、安全协作等等。”在记者问到安全行业的发展趋势时，吴云坤精辟地概括了自己的观点，“看趋势，一定要看价值，哪里有价值哪里就有攻击，地下产业链一定是瞄准价值高的地方。我们安全厂商的产品就要在价值高的地方保护我们的客户不受损失”就国内安全市场来说，吴云坤强调，“国内安全市场主要有三个趋势：一是 WEB 安全的应用将会更加广泛；二是高性价比的方案将会越来越多；三是合规和监管将进一步深化。”

WEB 安全作为目前安全领域的一个热点，吸引了众多媒体的关注。产品市场部总监王伟从四个方面阐述了 WEB 应用安全的方方面面。一是为什么 WEB 应用安全成为新的热点；二是 WEB 安全的市场格局；三

是 WEB 安全的关键技术趋势；四是绿盟在 WEB 安全方面的解决方案。这些话题都引发了在座媒体记者的热烈讨论。王伟指出，“由于越来越多的应用开始使用 WEB 技术开发，越来越多的 WEB APP 相关的漏洞被发现，攻击者也逐渐地把攻击目标转向了 WEB 站点。”不过，王伟对此也强调，“WEB APP 漏洞的增加不是其易遭受攻击的直接原因，而 WEB 应用蕴藏的价值才是根本原因。 对于多数组织而言，WEB APP 承载的数据是组织最重要的资产甚至是惟一资产，事关存亡。”这与吴云坤的安全价值论不谋而合。

云计算、云安全也是目前业界备受关注的一个热点，国际拓展部总监韩永刚就此话题最后做了深入阐述。他指出，“云计算更多的是一种商业模式上的更新。云计算是一种计算方式，通过互联网将资源“以服务”的形式提供给用户，而用户不需要了解、知晓或者控制支持这些服务的技术基础架构。”云计算也必定成为未来安全产业的焦点。韩永刚强调，“对于势不可挡的云计算，安全

也要漫步云端。随着云计算的深入应用，云安全也将会有更广泛的应用合作前景。”

这次媒体沙龙不仅就一些安全热点话题引发了在场媒体朋友的热烈讨论，同时也开创了一个全新的活动交流模式，在讨论中引发对于安全更深层次的思考。

绿盟科技在浙江地区连续召开渠道交流活动

为了提升绿盟科技的品牌知名度，开拓渠道市场，促进渠道销售工作，绿盟科技杭州办事处于 4 月 8 日、4 月 20 日、5 月 7 日在杭州大酒店、宁波文昌大酒店、温州国贸大酒店分别举办了三次有计划的渠道交流活动，渠道伙伴到会 120 余人。

各次会议主要由销售代表李建新讲解公司渠道政策，工程师杜用就公司概况、目前网络安全面临的形势、渠道产品介绍、市场定位等方面的问题进行介绍，同时通过现场提问、有奖问答等形式与渠道伙伴进行了充分的交流沟通，使与会合作伙伴深入地了解公司的渠道政策及有关产品、技术等，基本达到预期目标，为公司渠道政策在浙江三地区的推广工作奠定了良好的基础。


杭州会议现场


温州会议现场


宁波会议现场

绿盟科技荣获“影响十年”中国信息安全发展突出贡献奖

在 4 月 21 日举行的第十届中国信息安全大会上，绿盟科技荣获由中国电子信息产业发展研究院颁发的“影响十年”中国信息安全发展突出贡献奖以及“2009 年度中国信息安全优秀服务奖”。

伴随着用户信息安全意识的觉醒和信息安全产业的高速发展，新技术、新产品、新方法和新概念在不断涌现，寻找创新。2008 北京奥运信息安全保障已经体现了中国在等级保护方面的运筹能力，以及信息安全厂商在产品技术、风险管理、安全管理和服务运维等方面的发展。

绿盟科技是中国第一批专业网络安全产品和服务公司之一。在多年的发展过程中，获得了不同行业的近千家客户的认同，并已经成为国内领先的专业安全产品和服务提供商。自成立以来，绿盟科技一直以“巨人背后的安全专家”为己任，全力为客户服务，本着“诚信为本、客户至上、专业服务、面向国际”的宗旨，汇聚了国内安全领域最优

秀的技术研究、产品开发和服务实施队伍。多年来，开发出多款具有国内国际领先水平的安全产品，并通过独立的服务部门为用户提供专业的安全服务体系。

作为第 29 届奥运会安全保卫工作协调小组技术保障单位，绿盟科技在奥运期间凭借在入侵防范技术、异常流量分析检测与清洗、操作系统与应用安全、安全漏洞发掘技术、安全产品缺陷与检测、蠕虫及病毒原理与防范、漏洞库研究等领域的技术实力，通

过安全专家们对收集到的国内外恶意代码、拒绝服务、WEB 攻防及其它安全事件的信息实时反应、周密分析，形成处理意见并第一时间完成现场或远程处置服务，确保了奥运信息系统和公共事业设施信息系统信息的畅通无阻。

凭借多年锐意创新与优异安全服务能力，大会主办方特授予绿盟科技 “影响十年” 中国信息安全发展突出贡献奖以及 “2009 年度中国信息安全优秀服务奖”。

同时，行业营销中心政府营销经理孙铁在大会上发表演讲《安全融合应用的管理话题》，以烟草行业为例对安全管理所面临的挑战与解决之道做了精辟的阐述，得到与会嘉宾的一致好评。

绿盟科技再次组团赴旧金山参加 RSA 2009 大会

2009 年 RSA 大会（RSA Conference 2009）于 2009 年 4 月 20 日 -23 日在美国加州旧金山举行，绿盟科技再次组团赴美参会。绿盟科技此次参会人数超过去年，展位比去年扩大一倍（展位：#757），并带去了具有自主知识产权的多项安全解决方案和产品（中国首个 WEB 应用防火墙及综合 WEB 安全解决方案、安全网关 SG、入侵防御系统 NIPS 等），期望在本次大会上能够更多

地展现来自中国网络安全领军企业的实力，赢取商机。

RSA 大会是目前全球信息安全领域最具权威的年度峰会。大会吸引了来自全球的顶级信息安全企业，各行业 IT 决策者、资深安全专家以及学术界的领军人物。会议分为主题论坛、专业论坛、创新论坛、展会等多个部分，其中专业论坛涉及面极广，从加密算法数学原理的讨论，到安全合规性管理、WEB 安全、移动安全方面的热点话题，都会通过分会场进行。

2008 年绿盟科技第一次参加 RSA 展会，让国际上的同行首次近距离接触到来自中国的网络安全厂商，绿盟科技也获得了大量的安全前沿信息，发展了日本、新加坡等海外合作伙伴，对于指导安全技术研发和开展海外市场收到了良好的效果。在今年的会议上，绿盟科技会继续与业界同行沟通与交流，把握国际上最新的信息安全走向，密切关注国际安全发展趋势，跟踪产品技术动态，并将这些融入到绿盟科技的研发与市场体系当中，以继续增强绿盟科技在安全技术与市场动向方面的敏感触觉与领先优势。

通过对国际化工作的不断摸索，绿盟科技不但在海外展开了推广工作，也以国际一流的产品标准、服务标准、公司运营标准来不断提升自身能力。这种能力的提升，也将使绿盟科技能够为国内外的众多行业客户，提供更为优质的安全解决方案与高水平的服务。

绿盟科技参加 2009 通信网络和信息安全高层论坛

4 月 16 日，“2009 通信网络和信息安全高层论坛”在北京南粤苑酒店顺利召开。政府主管部门、运营商、厂商和咨询研究机构

各界的 200 多名来宾到场。工信部通信保障局副局长熊四皓、中国移动通信集团公司网络部网络安全处经理梁友、中国联合网络通信集团有限公司运行维护部互联网处经理徐海东、中国电信广州研究院数据通信研究部副部长金华敏等政府和行业专家到会并发表演讲。

绿盟科技行业营销中心田民在会上发表演讲《Botnet 的发现与防治》，从 Botnet 的威胁和危害、僵尸网络发现和防治手段、运营商防治僵尸网络以及如何开展僵尸网络防治服务运营等方面做了阐述。田民的演讲得到了参会来宾的一致好评。

作为绿盟科技的重要营销领域，我们多年来致力于服务通信运营企业，并为通信客户提供各类安全服务。凭借完善的产品和解决方案，以及在国内外广泛的应用，绿盟科技的产品得到了电信用户的普遍好评。经过大会组委会和行业专家的一致推举，绿盟科技凭借领先的研究、开发、服务和支撑能力，以及在通信行业内的影响力，荣获大会颁发的“通信安全卫士奖”称号。

绿盟科技参加“第四届政府 / 行业信息化安全论坛”

4 月 2 日，由公安部第三研究所《信息网络安全》杂志社主办的为期一天的“第四

届政府 / 行业信息化安全论坛”在北京召开，绿盟科技应邀参加了本次活动，行业营销线政府行业营销经理孙铁在会上做了题为《创建自主可控的关键信息安全技术》的专题演讲。此次参会对于树立良好的绿盟科技品牌、扩大绿盟科技在各行业信息中心的影响起到了很好的宣传作用。

绿盟科技荣获“中国软件渠道最佳选择奖”

3 月 27 日，第二届中国软件渠道大会在京召开，绿盟科技荣获“中国软件渠道最佳选择奖”。渠道总监白方代表公司领奖并发表感言，“面对快速成长的中小客户网络安全市场，绿盟科技秉承“立足长远、优势互补、相互尊重、相互学习、相互支持”的合作理念，逐步构建“以渠道为核心”的业务能力支持体系，与渠道伙伴共同打造中国最强大的网络安全营销服务网络，优化网络安全产业价值生态链，服务于广大的各行业中小客户，取得客户、渠道、绿盟科技的共赢，推动中国网络与安全产业的健康和谐发展。”在大会交流中，众多渠道商朋友前来接洽，对绿盟科技的技术实力与产品线表示了浓厚的兴趣。

本届渠道大会的奖项评选活动针对品牌形象、商业信誉、服务能力、产品质量、产品线完整性、渠道管理、市场推广、价格竞争力、利润空间以及供货保证等多方面对软件厂商评分，以调查投票的最终成绩作为本次评选的依据，绿盟科技以雄厚的实力荣获奖项，并将以荣誉为动力，更好地做好渠道工作，调动各方面的力量来共同完成对客户的安全承诺。

中国软件渠道最佳选择奖

技术动态

绿盟科技参加“2009 第二届（天津）国际软件测试技术大会”

“2009 第二届（天津）国际软件测试大会（TIST2009）”于 4 月 23 日至 24 日在天津高新区赛象酒店举行，本次大会由天津市科学技术委员会、天津新技术产业园区管委会、天津市外国专家局联合主办，天津市软件评测中心、天津市软件行业协会、天津华苑软件园管理中心共同承办，参会人员来自全国各省软件测评机构，绿盟科技作为主要被邀请厂商之一参加了此次大会。

会上，绿盟科技专业服务高级安全顾问白雷做了题为《信息系统设计与开发的安全评审与测试》的精彩演讲，主要从信息系统生命周期的安全保障出发，介绍了信息系统建设初期，在需求分析、系统应用设计、IT 架构设计等工作中的安全方案评审与安全风险评估方法，分析了在应用功能开发过程与系统集成过程中的安全评测方法，用于保证信息系统设计与开发中对安全需求的充分考虑，完善安全功能。

来自全国各省软件测评机构的与会代表对演讲内容产生了浓厚的兴趣，针对具体技术细节和问题与绿盟科技安全专家进行了充分交流。此次演讲同时受到了主办方的高度评价，通过此次大会使得绿盟科技与全国各测评机构以及天津地区客户的关系得到了进一步加强。

绿盟科技出席“中国石油通信技术研讨会”

3 月 24 日，由中国石油天然气集团公司—信息服务公司主办的“中国石油通信技术研讨会”在深圳市召开。参加本次会议的有中石油、中石化、中国海油下属部分区域的油田、炼化、管道和通信公司等单位的多

位信息化专家及领导。绿盟科技能源行业营销团队应邀出席了会议活动。

本期会议主题为“石油系统的专网通信与保障”。石油系统和各参与单位的多位专家和领导从“专网通信技术、协同业务、安全核查、适度安全保障”等方面阐述了诸多石油行业所关注的焦点问题，以及解决方案和技术成果的演讲。

会上，绿盟科技能源行业组张书嘉代表公司发表了主题演讲，从石油系统安全隐患如何产生、传统安全保障的缺失、石油信息系统的适度化风险控制与方案思路等几个方面论述了“石油系统信息安全建设—适度化保障思想”，获得了参会专家的好评。

本次会议活动使绿盟有机会接触到更多的石油企业领导和合作伙伴，集中展示了绿盟科技的企业形象、行业认识和技术实力，丰富了大客户的沟通机制和接口，为拓展石油行业市场打下基础。

NSFOCUS 2009年4月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2009-04-07 PowerPoint 畸形文件解析代码执行漏洞

NSFOCUS ID: 13168

http://www.nsfocus.net/vulndb/13168

综述

Microsoft PowerPoint 是微软 Office 套件中的文档演示工具。

PowerPoint 在解析特制的 PPT 文件时可能会导致访问内存中的无效对象，这可能允许攻击者执行任意代码。目前这个漏洞正在被名为 Exploit:Win32/Apptom.gen 的病毒积极的利用。

危害

攻击者可能利用此漏洞诱使受害者打开包含恶意内容的 PPT 文件，从而控制受害者系统。

2. 2009-04-16 Microsoft IE 多个内存破坏漏洞（MS09-014）

NSFOCUS ID: 13218

http://www.nsfocus.net/vulndb/13218

综述

Internet Explorer 是微软 Windows 操作系统中默认捆绑的 WEB 浏览器。

Internet Explorer 处理在网页间导航时的过渡方式及访问尚未正确初始化或已被删除对象的方式存在多个内存破坏漏洞。

危害

攻击者可以通过构建特制的网页来利用该漏洞，当用户查看网页时，就可能触发漏洞。

3. 2009-04-16 Oracle 2009 年 4 月紧急补丁更新修复多个漏洞

NSFOCUS ID: 13223

http://www.nsfocus.net/vulndb/13223

综述

Oracle Database 是一款商业性质大型数据库系统。

Oracle 发布了 2009 年 4 月的紧急补丁更新公告，修复了多个 Oracle 产品中的多个漏洞。这些漏洞影响 Oracle 产品的所有安全属性，可导致本地和远程的威胁。其中一些漏洞可能需要各种级别的授权，但也有些不需要任何授权。最严重的漏洞可能导致完全入侵数据库系统。

危害

攻击者可能利用此漏洞控制数据库系统，篡改或窃取重要数据。

4. 2009-04-15 Microsoft Windows NTLM 凭据反射远程代码执行漏洞（MS09-013/MS09-014）

NSFOCUS ID: 13216

http://www.nsfocus.net/vulndb/13216

综述

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 的 HTTP 服务没有正确地实现 NTLM 凭据反射保护以确保用户的凭据没有被反射和使用。如果用户连接到了攻击者的 WEB 服务器，Windows HTTP 服务处理 NTLM 凭据的方式存允许攻击者重放用户凭据并以登录用户的权限执行任意代码。

危害

攻击者可能利用此漏洞进行重放攻击。

5. 2009-04-03 Microsoft Windows GDI+ 库 GPFont::SetData() 函数单字节溢出漏洞

NSFOCUS ID: 13164

http://www.nsfocus.net/vulndb/13164

综述

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 的 GDI+ 函数库（gdiplus.dll）的 GPFont::SetData() 函数中存在单字节溢出漏洞。如果用户受骗打开了 EmfPlusFontObject 记录中设置有特制字体长度值的 EMF 图形的话，就可以触发这个溢出，导致使用该库的应用程序崩溃。

危害

攻击者可能利用此漏洞诱使受害者打开包含恶意内容的 EMF 图形，从而控制受害者系统。

6. 2009-04-15 Microsoft Windows WinHTTP 服务整数下溢漏洞（MS09-013）

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows HTTP 服务处理远程 Web 服务器所返回的特定值的方式存在整数下溢漏洞。如果用户受骗访问了恶意服务器的话，就可以触发这个溢出。

危害

攻击者可能利用此漏洞诱使受害者访问恶意的服务器，从而控制受害者系统。

7. 2009-04-15 Microsoft DirectX MJPEG 视频解码远程代码执行漏洞（MS09-011）

NSFOCUS ID: 13213

http://www.nsfocus.net/vulndb/13213

综述

Microsoft DirectX 是 Windows 操作系统中的一项功能，流媒体在玩游戏或观看视频时通过这个功能支持图形和声音。

DirectX 处理受支持格式文件的方式存在漏洞，如果用户受骗打开了特制的 MJPEG 文件就会导致执行任意代码。

危害

攻击者可能利用此漏洞诱使受害者打开包含恶意内容的 MJPEG 文件，从而控制受害者系统。

8. 2009-04-15 Microsoft Word 2000 WordPerfect 转换器栈溢出漏洞（MS09-010）

NSFOCUS ID: 13212

http://www.nsfocus.net/vulndb/13212

综述

Word 是微软 Office 套件中的文件处理工具。

Word 2000 所使用的 WordPerfect 6.x 转换器的转换代码没有对数据结构所分配的长度正确的验证计数器，如果解析了特制的 WordPerfect 文档就可能触发栈溢出。

危害

攻击者可能利用此漏洞诱使受害者打开包含恶意内容的 WordPerfect 文件，从而控制受害者系统。

9. 2009-04-15 Microsoft Excel 畸形对象远程内存破坏漏洞（MS09-009）

NSFOCUS ID: 13210

http://www.nsfocus.net/vulndb/13210

综述

Excel 是微软 Office 套件中的电子表格工具。

如果用户打开带有畸形对象的特制 Excel 文件，Office Excel 中的漏洞可能允许远程执行代码。

危害

攻击者可能利用此漏洞诱使受害者打开包含恶意内容的 Excel 文件，从而控制受害者系统。

10. 2009-04-09 Cisco PIX 和 ASA 设备多个拒绝服务和非授权访问漏洞

NSFOCUS ID: 13185

http://www.nsfocus.net/vulndb/13185

综述

PIX 是一款防火墙设备，可为用户和应用提供策略强化、多载体攻击防护和安全连接服务；自适应安全设备（ASA）是可提供安全和 VPN 服务的模块化平台。

Cisco ASA 5500 系列自适应安全设备和 Cisco PIX 安全设备中存在多个安全漏洞，远程攻击者可以利用这些漏洞导致拒绝服务或绕过限制执行非授权操作。

危害

攻击者可能利用此漏洞进行拒绝服务攻击和非法操作，降低系统的安全性。

NSFOCUS 2009年5月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2009-05-18 Microsoft IIS WebDAV Unicode 请求绕过认证漏洞

NSFOCUS ID: 13367

http://www.nsfocus.net/vulndb/13367

综述

Microsoft Internet 信息服务（IIS）是 Microsoft Windows 自带的一个网络信息服务器，其中包含 HTTP 服务功能。

IIS 的 WebDAV 功能在解析 URI 并发送回数据时没有正确地处理 Unicode 令牌环，远程攻击者可以通过提交恶意 HTTP GET 请求绕过受口令保护的文件夹的认证。

危害

远程攻击者可能利用此漏洞对 IIS 服务器进行非授权的访问，列出、上传或下载服务器文件。

2. 2009-05-15 Sendmail X-header 头远程堆溢出漏洞

NSFOCUS ID: 13359

http://www.nsfocus.net/vulndb/13359

综述

Sendmail 是很多大型站点都在使用的邮件传输代理（MTA）。

如果远程攻击者向 Sendmail 发送了包含有超长 X-header 头的畸形报文的话，就可能触发堆溢出，导致拒绝服务或执行任意代码。

危害

远程攻击者可能利用此漏洞控制 Sendmail 服务器。

3. 2009-05-05 Linux Kernel ptrace_attach() 函数本地权限提升漏洞

NSFOCUS ID: 13306

http://www.nsfocus.net/vulndb/13306

综述

Linux Kernel 是开放源码操作系统 Linux 所使用的内核。

Linux Kernel 在与 execve() 同步时 ptrace_attach() 使用了不充分的互斥体，本地用户可以通过附加到 setuid 进程获得 root 用户权限提升。

危害

本地攻击者可能利用此漏洞获取更高的访问权限。

4. 2009-05-13 Microsoft PowerPoint PP7X32.DLL 库多个栈溢出漏洞（MS09-017）

NSFOCUS ID: 13341

http://www.nsfocus.net/vulndb/13341

综述

Microsoft PowerPoint 是微软 Office 套件中的文档演示工具。

PowerPoint 的 PP7X32.DLL 库所提供的 PowerPoint 95 格式文件导入器中存在多个栈溢出漏洞。

危害

攻击者可能利用此漏洞控制受害者系统。

5. 2009-05-13MicrosoftPowerPointNotes 容器堆溢出漏洞（MS09-017）

NSFOCUS ID: 13343

http://www.nsfocus.net/vulndb/13343

综述

Microsoft PowerPoint 是微软 Office 套件中的文档演示工具。

PowerPoint 在解析 Notes 容器中某些结构时存在堆溢出漏洞。在读取 Notes 容器传播 C++ 对象过程中，Powerpoint 对为覆盖对象函数指针所分配内存错误的读取了过多的数据，之后在 mso.dll 的调用中使用。通过向容器中注入超长值，就可以触发堆溢出。

危害

攻击者可能利用此漏洞控制受害者系统。

6. 2009-05-08 Google Chrome 多个缓冲区溢出漏洞

NSFOCUS ID: 13331

http://www.nsfocus.net/vulndb/13331

综述

Google Chrome 是 Google 发布的开源 WEB 浏览器。

Chrome 的 boolParamTraits<SkBitmap>::Read() 函数在调用 bmp_data->InitSkBitmapFromData() 时存在堆溢出。

危害

攻击者可能利用此漏洞控制受害者系统。

7. 2009-05-05 暴风影音 Config.dll ActiveX 控件栈溢出漏洞

NSFOCUS ID: 13310

http://www.nsfocus.net/vulndb/13310

综述

暴风影音是在中国非常流行的万能多媒体播放软件。

暴风影音在其安装目录中所提供的 Config.dll 库没有正确地验证用户提供参数。当 SetAttributeValue() 的参数 lpQueryStr 是一个超长字符串时，就可以触发栈溢出。利用堆填充技术，攻击者可以轻易的利用此漏洞执行任意代码。

危害

攻击者可能利用此漏洞控制受害者系统。

8. 2009-05-14 Safari 3.2.3 版本修复多个安全漏洞

NSFOCUS ID: 13355

http://www.nsfocus.net/vulndb/13355

综述

Safari 是苹果操作系统中所默认捆绑的 WEB 浏览器。

Safari 中 WebKit 处理 SVGList 对象时存在内存破坏漏洞，访问恶意网站就会导致执行任意代码。Safari 处理 feed: URL 中存在多个输入验证错误，访问恶意的 feed: URL 就会导致执行任意 JavaScript。

危害

攻击者可能利用此漏洞控制受害者系统。

9. 2009-05-05 IBM Tivoli 存储管理器多个栈溢出漏洞

NSFOCUS ID: 13305

http://www.nsfocus.net/vulndb/13305

综述

Tivoli Storage Manager 是一种遵循 ANSI SAN 标准的可扩展解决方案，用于发现、监控和管理企业 SAN 架构组件，并可分配和自动操纵企业的附加磁盘存储资源。

Tivoli 存储管理器代理客户端（dsmagent.exe）的通用字符串处理函数中存在多个栈溢出漏洞。如果远程攻击者在所发送的请求报文中包含有多于 1025 个字符的超长字符串，或包含有多于 65 个字符的 NodeName，就可以触发这些溢出，导致执行任意代码。

危害

攻击者可能利用此漏洞控制服务器系统。

10. 2009-05-11 Discuz! 论坛 preg_match() 函数未初始化 $onlineipmatches 变量漏洞

NSFOCUS ID: 13332

http://www.nsfocus.net/vulndb/13332

综述

Discuz! 是一款华人地区非常流行的 Web 论坛程序。

在 Discuz! 论坛的 include/common.inc.php 文件中使用 $onlineipmatches 前并没有初始化，同时程序员没有判断 preg_match 函数的返回值，这样在某些特定情况下可能导致绕过正则的判断。

危害

攻击者可能利用此漏洞像服务器提交任意值的 $onlineipmatches 变量。

NSFOCUS 2009年6月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2009-06-01 Microsoft DirectX QuickTime 媒体文件解析代码执行漏洞

NSFOCUS ID: 13401

http://www.nsfocus.net/vulndb/13401

综述：

Microsoft DirectX 是 Windows 操作系统中的一项功能，流媒体在玩游戏或观看视频时通过这个功能支持图形和声音。

DirectX 的 DirectShow 组件（quartz.dll）在解析畸形的 QuickTime 媒体文件时存在错误，

用户受骗打开了恶意的媒体文件就会导致执行任意代码。由于用户可能在浏览器中安装媒体

播放插件，因此访问恶意网页就足以导致播放 QuickTime 文件，触发 Quartz.dll 中的漏洞。

危害：

攻击者可以诱使受害者打开畸形的 QuickTime 媒体文件控制受害者系统或利用此漏洞进行网页挂马。

2. 2009-06-10 Microsoft IIS WebDAV Unicode 请求绕过认证漏洞 (MS09-020)

NSFOCUS ID: 13367

http://www.nsfocus.net/vulndb/13367

综述：

Microsoft Internet 信息服务（IIS）是 Microsoft Windows 自带的一个网络信息服务器，其中包含 HTTP 服务功能。

IIS 的 WebDAV 功能在解析 URI 并发送回数据时没有正确地处理 Unicode 令牌环，远程攻击者可以通过提交恶意 HTTP GET 请求绕过受口令保护的文件夹的认证，或在受口令保护的 WebDAV 目录中列出、上传或下载文件。

危害：

攻击者可能利用此漏洞对服务器进行非授权的访问。

3. 2009-06-10 Microsoft IE DHTML 和 HTML 对象多个内存破坏漏洞 (MS09-019)

NSFOCUS ID: 13440

http://www.nsfocus.net/vulndb/13440

综述：

Internet Explorer 是 Windows 操作系统中默认捆绑的 WEB 浏览器。

Internet Explorer 在解析网页中的 DHTML 和 HTML 对象时存在多个内存破坏和未初始化或已删除对象访问漏洞。如果用户受骗访问了恶意网页，就可能导致拒绝服务或执行任意代码。

危害：

攻击者可以诱使受害者浏览包含畸形代码的网页从而控制受害者系统。

4. 2009-06-11 Microsoft Windows 打印后台程序 DLL 库加载漏洞 (MS09-022)

NSFOCUS ID: 13444

http://www.nsfocus.net/vulndb/13444

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 打印后台处理程序没有正确地验证可能加载 DLL 的路径。如果远程攻击者将恶意的 DLL 存储在了打印后台程序可访问的位置上然后向受影响的系统发送了特制的 RPC 消息的话，就可能导致打印后台程序加载恶意的 DLL 并以提升的权限执行代码。

危害:

攻击者可能利用此漏洞控制服务器系统。

5. 2009-06-12 Microsoft Windows RPC 分组引擎远程代码执行漏洞 (MS09-026)

NSFOCUS ID: 13453

http://www.nsfocus.net/vulndb/13453

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 远程过程调用（RPC）工具中存在权限提升漏洞，RPC 分组引擎未能正确的更新其内部状态，导致从错误的位置读取指针。在默认配置中，用户不会受到利用此漏洞的攻击。

危害:

攻击者可能利用此漏洞控制受影响的系统。

6. 2009-06-18 IBM AIX rpc.ttdbserver 库远程溢出漏洞

NSFOCUS ID: 13471

http://www.nsfocus.net/vulndb/13471

综述:

IBM AIX 是一款商业性质的 UNIX 操作系统。

AIX 的 ToolTalk 库 libtt.a 中存在缓冲区溢出漏洞。如果 /etc/inetd.conf 中启用了 rpc.ttdbserver 的话，远程攻击者就可以通过提交恶意 RPC 请求触发这个溢出，导致以 root 用户权限执行任意指令。

危害:

攻击者可以利用此漏洞控制服务器系统。

7. 2009-06-16 Firefox 3.0.11 版本修复多个安全漏洞

NSFOCUS ID: 13463

http://www.nsfocus.net/vulndb/13463

综述:

Firefox 是 Mozilla 所发布的开源 WEB 浏览器。

Firefox 中的多个安全漏洞可能导致泄露敏感信息、绕过安全限制或入侵用户系统。由于代码共享，Thunderbird 和 SeaMonkey 也受这些漏洞的影响。

危害:

攻击者可以利用此漏洞控制受害者系统。

8. 2009-06-03 ACDSee 产品 TIFF 及字体文件解析缓冲区溢出漏洞

NSFOCUS ID: 13413

http://www.nsfocus.net/vulndb/13413

综述:

ACDSee 是一款图象查看、转换、管理工具，可使用在 Microsoft Windows 操作系统下。

如果用户使用 ACDSee 产品打开了畸形的 TIFF 图形或字体文件的话，就可以触发多个缓冲区溢出，以用户的身份执行任意代码。

危害:

攻击者可以利用此漏洞控制受害者系统。

9. 2009-06-02 Apple QuickTime Player 7.6.2 更新修复多个安全漏洞

NSFOCUS ID: 13410

http://www.nsfocus.net/vulndb/13410

综述:

Apple QuickTime 是一款非常流行的多媒体播放器。

QuickTime 的 7.6.2 之前版本存在多个安全漏洞，其中包括多个缓冲区溢出和内存破坏漏洞，攻击者诱使用户打开畸形的媒体文件就可能导致应用程序意外终止或以用户的身份执行任意代码。

危害:

攻击者可以利用此漏洞控制受害者系统。

10. 2009-06-12 Microsoft Windows 内核参数和指针验证权限提升漏洞 (MS09-025)

NSFOCUS ID: 13452

http://www.nsfocus.net/vulndb/13452

综述:

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 内核没有正确地验证传递给系统调用的参数，以及从用户态传递的某些指针，导致权限提升漏洞。成功利用此漏洞的攻击者可以运行内核态中的任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

危害:

攻击者可以利用此漏洞对系统进行非授权的管理、控制操作。

巨人背后的专家

- 2008年：绿盟科技“极光”远程安全评估系统成为1996年以来全球六家获得英国西海岸实验室权威认证的漏洞扫描产品之一
- 2007年：再次入选国家级应急服务支撑单位
- 2006年：连续四年荣获中计报“值得信赖的安全服务品牌”
- 2005年：囊括年度入侵检测\保护系统全部奖项
- 2004年：入选公共互联网应急处理国家级服务试点单位
  首批荣获国家二级安全服务资质
- 2003年：进入中国电子政务IT百强
- 2002年：承担全国性电信网安全评估
- 2001年：入选国家网络安全服务试点单位
- 2000年：绿盟科技成立

www.nsfocus.com

THE EXPERT
BEHIND GIANTS

长期以来，绿盟科技致力于网络安全技术的研究，为政府、电信、金融、能源等行业提供优质的安全产品与服务。在这些巨人的背后，他们是倍受信赖的专家。

NSFOCUS

SECURITY+

THE EXPERT BEHIND GIANTS 巨人背后的专家

安全+ 技术版

与安全人士分享技术心得

Share technique experience with security professionals

Nsmagazine@nsfocus.com