IBM X-Force 2011趋势和风险报告

2012年3月

参与人员

IBM X-Force趋势和风险报告是全体IBM人员协作的结晶。感谢以下人员对本报告的发布做出了贡献和关注。

参与者	职位
Bryan Casey	市场经理，IBM Security Systems
Carsten Hagemann	X-Force软件工程师， Content Security
Colin Bell	安全解决方案架构师，实验室服务和支持，IBM Security
Systems Clay Blankenship	高级事故响应分析师
Cynthia Schneider	信息开发人员，
David McMillen	安全智能分析师，IBM Security Services
David Merrill	STSM， IBM 首席信息安全官，CISA
Dr. Jens Thamm	
Dr. Ashok Kallarakkal	数据库管理，内容安全
Gina Stefanelli	高级经理，Product Management and Beta Ops
Jason Kravitz	X-Force市场经理
Jason Kravitz	IBM Security Systems and E-Config Techline 专家
John C. Pierce	威胁智能分析师，AI， MSS
John Kuhn	安全智能分析师，IBM Security Services
Kimberly Madia	数据安全战略，InfoSphere Guardium & Optim
Leslie Horacek	X-Force Threat Response Manager
Mark E. Wallis	高级信息开发人员，IBM Security Systems
Marne Gordan	制度分析师，IBM Security Systems
Michael Applebaum	产品营销总监，Q1 Labs
Michael Montecillo	Managed Security Services Threat Research and Intelligence负责人
Michelle Alvarez	经理，MSS Global Operations Paul
Sabanal	X-Force Advanced Research
Phil Neray	Q1 Labs市场领导，IBM Security Systems
Ralf Iffert	经理，X-Force Content Security
Randy Burton	高级事故响应分析师
Robert Lelewski	高级事故响应分析师
Ron Black	高级事故响应分析师
Ryan Berg	云安全战略领导
Scott Moore	X-Force软件开人员兼X-Force数据库团队领导
Shane Garrett	团队领导，X-Force Advanced Research
Tom Cross	经理，X-Force Strategy and Threat Intelligence
Veronica Shelley	地区市场经理，IBM Security Systems

关于X-Force

IBM X-Force®研发团队负责研究和监视最新的威胁趋势，包括各种漏洞、攻击代码和有效攻击、病毒以及其他恶意软件、垃圾邮件、网络钓鱼和恶意Web内容。除了向客户和一般大众提供有关新兴和关键威胁的建议，X-Force还提供安全内容来帮助保护IBM客户远离这些威胁。

献辞

谨以IBM X-Force 2011趋势和风险报告纪念

我们的朋友和同事Marne Gordon，她在创建本报告的过程中不幸离世。作为IBM Security Division安全战略团队的制度分析师，Marne在云和社交媒体安全上的知识以及投入是本报告的灵魂。她是各种行业活动上活跃的演讲者，发表了大量有关安全与合规性主题的文章。我们将永远怀念Marne在安全性、合规性和对IBM做出的贡献。

IBM安全协作

- IBM Security拥有多个品牌的产品，这些产品提供了众多的安全功能。
- X-Force研发团队正忙于分析最新的趋势和攻击者使用的方法，而IBM内的其他小组正在使用这些丰富的数据开发各种技术来保护客户。
- IBM X-Force研发团队发现、分析、监视和记录大量的计算机安全威胁和漏洞。
- IBM托管安全服务(MSS)负责监视与端点、服务器（包括Web服务器）和一般网络基础设施相关的攻击代码。MSS跟踪通过网络以及电子邮件和即时消息等其他途径传送的攻击代码。
- 专业安全服务(PSS)提供企业级安全评估、设计和部署服务来帮助构建有效的信息安全解决方案。
- IBM X-Force内容安全团队通过爬网、独立的发现以及MSS提供的源来独立地搜寻和分类Web。
- IBM整理了过去几年由IBM AppScan® OnDemand Premium Service执行的安全测试的真实漏洞数据。此服务将从IBM AppScan获得的应用安全评估结果与手动安全测试和验证相结合。
- IBM Security Services通过两种方式来支持云：Security Services for the Cloud提供安全专业知识来帮助客户开启云之旅，基于云的模型中的安全机制可帮助客户降低成本和复杂性，改善安全状态并满足合规性要求。
- IBM身份和访问管理解决方案让组织能够高效地集中化和自动化授权用户的身份策略和访问特权的管理。这些解决方案可通过强身份验证、单点登录以及用于监视用户访问活动的审计/报告工具来进一步提高安全性。
- IBM数据和信息安全解决方案提供了帮助客户解决整个企业内信息生命周期安全的数据和访问管理能力。
- IBM InfoSphere® Guardium®提供了一个数据库安全与合规性方面可扩展的企业解决方案，可通过极少的资源来快速部署和管理该解决方案。
- 来自IBM子公司Q1 Labs的QRadar Security Intelligence Platform为SIEM、日志管理、配置管理和异常检测提供了一个一体化解决方案。它提供了一个统一的仪表板和跨人员、数据、应用和基础设施的安全与合规性风险的实时洞察。

目　录

第I部分

第I部分 威胁

本节探讨与威胁有关的主题，介绍安全专家面临的许多企业攻击。我们将探讨IBM在整个安全领域观察到的恶意活动，以及我们如何帮助您保护网络远离这些威胁。我们还会向您介绍IBM已发现的最新攻击趋势。

执行概述

2011年是一个引人注目的IT安全之年。截至年中，在频繁的数据泄漏、DoS攻击和社会黑客活动报告方面，IBM将2011年称为“安全违规年”。截至年末，这些事故的频率和范围一直居高不下，不断让人们知道在愈加互联的世界中运营业务并保护其资产的基本原则。2011年全年大量具有极高影响力和知名度的事故已成为高管和业务领导重新评估企业中现有结构、策略和技术的效率的催化剂。

任何重大的挑战都会带来一个不错的学习和改进机会。尽管一些公司已开始披露何时发现了一个安全违规以及它可能为客户带来哪些影响，但很少有公司谈到它是如何发生的以及如何预防它。我们在安全行业面临的一个难题是如何负责任地披露安全违规，这样各种技术细节可帮助我们确保其他企业不会受到类似的影响。在本报告中，我们将展示我们可能从这些不幸事故中察觉到的蛛丝马迹，以及我们如何采取积极的措施来公开可能在未来会影响有益的披露文化的安全违规信息。

通过披露已经发生的安全违规，我们仍然看到SQL注入是攻击者的一个切入点选择。自动化的SQL注入攻击（如LizaMoon）能够成功地扫描Internet并利用存在漏洞的主机。这些SQL注入攻击在很长一段时间内很常见。最近我们还开始发现，针对Shell命令注入漏洞的攻击在增多。在2011年末，X-Force看到的Shell命令注入攻击活动数量是我们在这一年早期看到的2到3倍。我们还注意到，在接近2011年末时，SSH密码破解活动显著增多。

我们还看到了前所未有的新攻击，如对多个证书颁发机构的损害。此类攻击破坏了用户的基本信任 – 访问加密的SSL页面意味着我们在安全地进行通信。传统的网络钓鱼和垃圾邮件等旧攻击方法已被部署恶意软件的新方法所取代。社交媒体攻击在不断增加，成为了攻击者们的首要目标区域，他们通过渗透到朋友和关注群体中来成功侵用目标的信任关系。

尽管存在这些困难，在整个报告中，我们还注意到一些积极的趋势和改进。所报告的Web应用漏洞总数比我们自2005年以来看到的要低，X-Force还看到已公开发布的真正攻击代码的数量也在显著下降。将攻击代码在Internet上发布后，可为攻击者提供一种轻松的方式来攻击漏洞。在过去几年，发布了15%已公开漏洞的攻击代码。今年，这一数字下降到11%。在过去4年中，针对Web浏览器以及文档阅读器和编辑器的攻击代码发布频率已下降到察觉不到的水平。公开曝光的漏洞还比以往更可能拥有补丁。未修复漏洞的百分比已从去年的43%下降到36%。

在Web应用漏洞测试中，IBM AppScan团队在跨站点请求伪造(CSRF)和跨站点脚本(XSS)领域都看到了显著的改善。

当我们自己和我们的企业沉浸在一个更加互联、开放、移动和社会化的在线状态中时，机会主义者也在发明灵活轻松的系统攻击新方式。使用最小公分母方法，他们不仅以技术为攻击目标，还直接利用人类的本性，掠夺人们的信任。社交媒体和移动设备继续让企业与外部世界之间的边界变模糊了。

在本报告中，沿着这些边界，我们将继续探索公司如何跟上移动设备和云的复杂性。移动设备的大量采用让“自带设备”(BYOD)计划的讨论成为热门话题，还有如何减轻与这些策略相关的风险，以及影响此平台的最大威胁。

云的采用面临着类似的讨论。问题不是云更安全还是更不安全，而是我们需要何种具体的控制和业务流程来致力于解决风险，帮助确保云环境中的安全性。

任何组织在计划更广泛地采用基于云的基础设施时，理解组织的角色都是至关重要的，类似地，在关系到提高安全性和减轻风险时，理解云服务提供商的角色也是至关重要的。

在整个2011年中，安全团队反复面临着要做到更好的挑战。许多人也面临着改进流程、技术，向员工和客户培训安全实践，以及通过提高企业安全状态的可视性来提升安全智能的挑战。IBM认为帮助客户抢先防御安全威胁的途径是在整个组织中与我们的分析和智能功能相联系，从而实现更高效的预测和检测。通过在2011年10月收购Q1 Labs并组建新的Security Systems部门，IBM前进了一大步。不断出现的有关我们如何完善安全智能平台的新闻表明，我们在认真应对各种市场需求。认识离不开行动和变革。我们希望的正是进行变革。

2011年要点

威胁：

恶意软件和恶意网站

- 数据违规行为的激增开启了2011年，而这一趋势延续了一整年，因此IBM X-Force宣称这一年是“安全违规年。”（第12页）
- SQL注入仍然是受攻击的公司中一个主要的攻击弱点。SQL注入已存在一段时间，但仍然是一种成功的攻击方式（第17页）
- 2011年，攻击者对一些证书颁发机构的攻陷是另一个重要事件，而曝光率最高的是荷兰公司DigiNotar。攻击者能够生成未授权的证书，他们可在以后使用中间人攻击类型作为监听加密连接的方式时拦截这些证书。这种类型的攻击打破了用户的基本信任 – 访问加密的SSL页面意味着在安全地进行通信。（第33页）
- 2011年发布了一个对通过SSL/TLS进行通信的服务器执行拒绝服务(DoS)攻击的概念证明工具。此工具表明一台使用普通连接的常用笔记本电脑就可能导致企业Web服务器瘫痪。（第33页）
- 来自IBM托管安全服务(MSS)团队的几个最大量的特征表明，攻击者最喜欢的方法是SQL注入，SSH暴力攻击和Shell命令注入活动也在增加，并且代理弹回继续位列MSS传感器流量的前列。（第16页）
- 与以往任何一年相比，2011年Mac恶意软件领域发生的事件最多。这不仅表现在与前几年的数量相比，还表现在功能方面。2011年，我们开始看到有些Mac恶意软件具有我们之前仅在Windows®恶意软件中看到过的功能。（第39页）

Web内容趋势、垃圾邮件和网络钓鱼

- 在2011年的第一个阶段，匿名代理在稳步增多，超过了前3年总和的4倍。但是，在这一年的上半年，我们自2009年以来第一次没有看到该数量增加。匿名代理是需要跟踪的一个关键网站类型，因为它们允许人们隐藏潜在的恶意意图。（第44页）
- 2011年，垃圾邮件继续减少，到年末，通过zip附件提供恶意软件的垃圾邮件成为了一种方法选择。（第49页）
- 在这一年发送垃圾邮件最多的国家中，印度继续名列榜首，发出了如今登记的所有垃圾邮件中的大约14%。美国在一年前名列榜首，如今已降到发送的所有垃圾邮件的2%以下。印度之后依次是越南、印度尼西亚、俄罗斯、巴西，并且澳大利亚以到2011年末发送所有垃圾邮件的5.6%这一比例第一次离开前六强名单。（第55页）
- 接近2011年末时，我们开始看到类似网络钓鱼的电子邮件开始出现，它们链接到不一定会执行网络钓鱼攻击的网站。这些电子邮件使用一个著名品牌的流行名称来吸引用户单击一个恶意软件链接，或在某些情况下单击其他无害网站（如零售网站）的链接。后一种电子邮件的一种可能解释可能是单击欺诈，垃圾邮件发送者向这些网站引入流量来获得广告费。无论作何解释，这些讨厌的人在继续推动该年度最后几个月中类似网络钓鱼的电子邮件的大量增加。（第56页）

操作安全的基础设施:

漏洞和攻击代码

- 2011仅报告了7000多个新的安全漏洞。尽管这与2010年比下降了许多，但我们仍然看到了比以往更多的漏洞，漏洞曝光量自2006年以来存在一个两年的高低周期，而且每个高点和低点的水平都在不断升高。(第74页)
- 在过去几年中，已曝光的安全漏洞中大约有一半是Web应用漏洞。但是，今年这一数字下降到了41%，这是自2005年以来比例最低的年份。(第75页)
- 一类易受已曝光漏洞和许多攻击活动影响Web应用是基于Web的内容管理系统(CMS)。我们分析了4个基于Web的流行内容管理系统，分析数据表明这些系统中最重要的缺陷来自它们支持的第三方插件。(第77页)
- 2011年，X-Force观察到被公开发布的真正攻击代码数量显著下降。这一数字从2006年以来创下了新低。这个数字在百分比上和实际数量上都较低。在过去几年中，具有已公开攻击代码的漏洞比例在15%上下波动，但今年该比例为11%。(第78页)
- 高危浏览器漏洞继续在增多，我们还观察到，针对第三方浏览器插件而不是浏览器本身的路过式下载攻击在增多。文档阅读器就是一个深受攻击者喜爱的第三方组件，因为恶意文档文件既可用在路过式下载场景中，也可附加到电子邮件中。(第78页)
- 我们继续看到多媒体播放器中曝光的漏洞数量在增加，2011年观察到的针对多媒体漏洞的公开攻击代码数量与2010年相当。这仍然是攻击者关注的一个领域。(第81页)
- 最大型的企业软件供应商占曝光的漏洞总数的比例不断在上升，已从2008年的19%上升到2011年的31%。我们不相信这仅仅是一种软件行业整合措施。安全开发实践已成为软件开发生命周期中越来越重要的一部分，负责任的供应商过去几年也在着手改进其识别和消除代码中各种漏洞的能力。(第84页)
- 在过去的7年中，社交网络已从非主流的消遣变为了全球最活跃的在线活动，甚至让搜索引擎的使用都黯然失色。自然地，这些集中化的活动代表了一个暗含大量犯罪元素的环境。多年前通过电子邮件大行其道的欺诈和诈骗如今在社交媒体论坛以及一个新鲜的潜在目标群体中找到了新的生机。(第89)

软件开发安全实践

Web应用漏洞

- 2010 OWASP Top Ten中的许多问题在提交到IBM AppScan OnDemand Application Vulnerability Testing Service的软件中频繁出现。在10个测试中，接近8个包含被破坏的身份验证和与会话控制相关的问题。许多进行测试的应用未能限制会话篡改，容易受到会话固定式攻击。此外，与会话终止和会话重用相关的问题也是导致这么高的统计数据的影响因素。（第113页）
- 在2011年执行的28%的测试中发现了跨站请求伪造(CSRF)，但这一数字与2010年的59%相比减少了许多。减少的部分原因似乎是对此攻击类型的更高认知度和用于包含CRSF令牌的方法改进。（第116页）
- 仍在超过40%的应用中找到跨站点脚本(XSS)的事实表明，可能仍有许多应用没有完全遵守安全编码实践。毋庸置疑，形势有所改善，但没有理由自鸣得意。40%的XSS漏洞概率仍然很高，尤其是对于一些很容易理解、很容易证明且很容易修复的漏洞而言。Web应用漏洞仍然是许多数据违规情况的关键所在，数据违规情况在2011年上半年继续增多。以至于X-Force将2011年称为“安全违规年”。（第114页）
- 我们采集的另一个重要的数据点是“每次安全测试找到给定漏洞的实例平均数量”。我们看到找到此漏洞的XSS实例有所减少。2009年的平均数为40多个，而2011年仅为3个。现在找到一个完全没有输入控制的应用的可能性要小得多。（第114页）
- 2011年，财务应用再次成为表现最佳的领域。政府应用是所有3个类别中表现最差的。出现此情况的原因并不明确，但名誉损害可能是一个因素。与财务应用相比，政府应用破坏不太可能推动对减轻安全问题方面进行投资。（第116页）

新兴的安全趋势：

移动设备

- 移动设备是另一个引起重视的区域。有许多移动操作系统漏洞被曝光，也有许多针对这些漏洞的攻击代码被公开发布。对移动设备进行越狱或root的期望是导致人们将移动攻击代码发布到网络上的一个动机。当然，一旦该代码可用，它就可能被用于针对未越狱的电话等恶意用途。（第82页）
- 被感染的移动设备组成的庞大僵尸网络已开始登上舞台，而这仅仅是开始。（第83页）
- 移动设备（因为它们通常拥有GPS硬件，以及语音、消息和数据服务）已检测到监视多方面用户行为（包括记录位置、消息、电子邮件和语音通话供攻击者查看）的间谍应用存在。与我们在个人计算机上看到的攻击类型相比，这尤其令人担忧。因为移动设备已真正成为“口袋中的办公室”，所以它们可能为间谍攻击提供机会。（第122页）

- 今年的一项最近的进步是，人们更加关注将企业应用和数据与员工的个人应用和数据分开的能力。显然，此进步的一个主要驱动因素是BYOD计划的普遍性和人们对它感兴趣。(第125页)

云安全

- 问题不是云更加安全还是更不安全，而在于我们应采用哪些具体的控制和业务流程来解决风险并帮助保证云环境中的安全性。任何组织在计划更广泛地采用基于云的基础设施时，理解组织的角色都是至关重要的，类似地，在关系到提高安全和减轻风险时，理解云服务提供商的角色也是至关重要的。(第126页)
- 安全云计算方面的成功不是一个简单的联系人管理问题，它可能对云部署的成功至关重要。创建一个考虑了帐户生命周期管理和退出战略的灵活服务水平协议(SLA)可能很有用。(第128页)
- SLA应是真正的协议，尤其是在条款和范围方面，只有在经过适当通告后才能进行更改，而且需要认识到组织的具体业务和信息安全需求。(第131页)

2011 - 安全违规年

从年中到年末 – 违规在不断上演

在年中，IBM X-Force将2011年称为“安全违规年”，其标志就是大量重要、广泛报告的外部网络安全违规事件和其他事故，不仅其出现频率引人注目，它们对许多受害者的操作能力造成的影响也引人注目。

2011年下半年仍然常常会看到每周出现大范围网络安全违规的报告，这些违规造成了客户数据泄漏、Web服务中断和数十亿美元的损失。IT安全现在是一项影响业务结果、品牌形象、供应链、法律披露和审计风险的董事会讨论议题。在IBM X-Force 2011年中趋势和风险报告中，我们分析了将2011年确定为安全违规年的基本动机、攻击方法和基本安全实践。

没有针对任何行业或部门区分这些事故。执法部门、政府、社交网络社区、零售、娱乐、银行、非盈利机构、财富500强甚至安全公司都受到了攻击。没有哪个地区是攻击的热门地点，显然这些攻击发生在全球各地。

直到这一年行将结束，攻击也没有减缓的趋势。在12月，一些对成本造成最大影响的攻击感染了多家中国庞大的社交和娱乐网站，造成了数十亿美元的潜在损失。

2011年按攻击类型、时间和影响分类的安全事故抽样

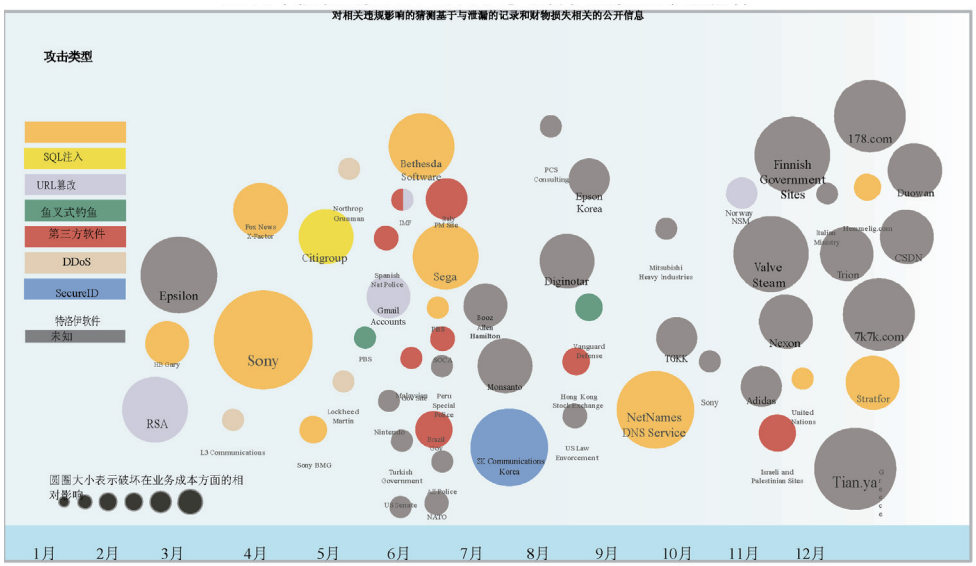


图1: 2011年按攻击类型、时间和影响分类的安全事故抽样

2011年下半年的形势巨变

如图1所示，SQL注入仍然是目标公司中一个被利用的主要缺陷。SQL注入已存在一段时间，但仍然是攻破公司防御体系的一种成功方式。后面我们将探讨SQL注入的复杂性，以及为什么如此难以察觉它和在网络中防御它。

让2011年安全违规形势变得更复杂的是，我们看到被攻陷的核心技术导致对其他目标的大规模攻击的多个示例。在年初，对RSA的一次攻击导致与该公司SecureID身份验证产品相关的敏感代码和数据被盗。随后曝光的信息表明[1]，被攻陷的技术用于获取至少其他3个企业的准入权。这提高了攻击的复杂性，

因为攻击者不仅攻击一个具体的最终目标，还攻破了更多潜在受害者使用的基础技术。

在2012年持续出现的另一个新兴趋势是，攻击者使用DNS服务器作为一种方式，将轻信的用户重定向到著名网站的恶意变体。每次用户在浏览器中输入一个Web域时（如http：//www.somecompany.com），该名称就会被转换为托管该站点的服务器的IP地址。

NetNames DNS名称服务器上的SQL注入允许攻击者更新多个著名网站的DNS记录，如The Register、The Daily Telegraph和UPS。[2]

通过攻陷DNS名称服务器本身，攻击者将请求重新路由到他们选择的服务器，常常会创建一个著名站点的具有类似外观的变体，其中包含用于获取敏感信息的

可下载恶意软件或表单。这类攻击会破坏基本的信任原则，也就是键入一个网站名称就会将我们带到正确的服务器。

攻击者对一些证书颁发机构的攻陷是另一个重要事件[3]，而曝光率最高的是荷兰公司DigiNotar。证书颁发机构会分发安全证书，其中提供HTTPS协议安全功能，用于加密从用户传到在线服务的流量。攻击者能够生成未授权的证书，他们可在以后使用中间人攻击类型作为监听加密连接的方式时拦截这些证书。这类攻击打破了用户的基本信任 – 访问加密的SSL页面意味着在安全地通信。在本报告的后面，我们将更详细地探讨与当前SSL信任模型有关的风险。在每种情况下，我们都看到攻击者使用一种多层的战略，其中包含某种核心技术，然后使用它编织一个庞大的潜在目标网络。

1 http：//www.nytimes.com/2011/06/04/technology/04security.html
http：//www.infosecisland.com/blogview/14142-RSA-SecurID-Breach-Spreads-to-L3-and-Northrop.html

2. http：//www.theregister.co.uk/2011/09/05/dns_hijack_service_updated/

3. http：//www.theregister.co.uk/2011/10/27/ssl_certificate_authorities_hacked/

学到的教训

从2011年的安全违规图中可以看到，对于在下半年公开报告的许多安全违规，我们没有这些违规发生方式的任何信息。有些不同的动机推动安全违规的曝光，但期望向公众通告被攻击者攻击的技术漏洞通常不在这些动机中。曝光常常是由告知其个人信息或企业数据可能已暴露的客户或告知受害者发明的技术已被攻陷的期望所推动。最近，财务分析师在评估投资决策时开始对使用计算机安全风险信息感兴趣。但是，公司因为希望将注意力转向其他公司可能面临的计算机安全问题，从而曝光安全违规的情况相对较少。我们认为这是不幸的，因为安全专家可从其他人学到的教训中获益。

一些航海和航空杂志每月会印刷专栏来描述非常危险或导致事故的真实情形。通过每月阅读这些报告，飞行员和船长可定期分析彼此的事后行动。通过此过程，他们可学习如何处理困难的情形并建立在危机中很宝贵的信心。类似地，负责保护计算机网络免受攻击的人们应定期了解安全故障信息，以便培养有关要避免哪些陷阱的良好本能。准确了解可导致破坏的技术和流程故障可以查明人们自己目前状况下的漏洞。、

通常，计算机安全被认为经营业务的一种代价，而业务部门希望避免投入资源来修复可能从不会被攻击的安全缺陷。人们期望找到一个“平衡点”，既将足够的钱花在保护公司正确的安全投资上，又不会多花一分钱。这意味着仅识别技术或规程差距通常不足以说服业务部门进行投资来弥补这一差距 –

必须有一个可论证的真实风险，那就是如果不弥补此差距，它可能被他人利用。安全违规的受害者曝光了导致他们违规的具体技术和规程差距时，此信息有助于为其他公司提供了获取弥补类似差距所需投资的必要业务理由。出现从技术上导致多家公司出现类似违规的情形时，曝光所涉及的具体技术漏洞可能推动整个市场对解决这类漏洞问题进行讨论。

计算机犯罪的受害者在曝光安全违规时，应考虑到与公众探讨“哪里出错了”等技术细节的价值。在某些情况下，曝光这类信息所涉及的风险可能超过收益。显然，提供太多技术细节可能会给未来的攻击铺平道路。但是，了解这种曝光可能有哪些收益很重要。帮助其他人从自己的不幸中汲取教训，这是一个可以阻止损害您网络的这类罪犯在未来继续获得成功的积极措施。

前进的道路

在我们的X-Force 2011年中趋势和风险报告中，我们确定了X-Force建议采取10个步骤来减轻这一年已发生的一些攻击。我们建议的步骤都不是什么IT安全专家的惊天内幕。挑战不是不知道要做什么，而是在一个复杂、分散化的组织中统一地实施某些措施。安全计划要想取得成功，必须拥有资源、政策支持以及确保在整个组织中遵守最佳实践所需的制度尊重。实现这种水平的有效性才是IT安全领导的真正挑战。

如果IBM X-Force运营IT部门

1. 定期执行第三方外部和内部安全审计
2. 控制您的端点
3. 划分敏感系统和信息
4. 保护您的网络
5. 审计您的Web应用
6. 对最终用户进行网络钓鱼和鱼叉式钓鱼培训
7. 搜索不安全的密码
8. 将安全整合到每个项目计划中
9. 检查业务合作伙伴的策略
10. 建立一个可靠的事故响应计划

有关任何上述步骤的详细信息，请下载和阅读《IBM X-Force 2011年中趋势和风险报告》。

IBM 托管安全服务 — 全球威胁形势

IBM 托管安全服务(MSS)每天监视着130多个国家的数百亿个事件，这一监视工作每分每秒都在进行。IBM MSS的全球存在性让我们提供了当前威胁的第一手资料。IBM分析师使用这些丰富的数据提供对计算机威胁形势的独到理解。威胁趋势识别对建立未来的安全战略和理解威胁的意义至关重要。

MSS—2011年数量最多的特征

数量最多的特征

表1显示了数量最多的托管安全服务特征，以及它们从2010年末到2011年的趋势线。2010年的10大特征中有4个仍在2011年末的列表中占有一席之地。SQL_ Injection和SQL_SSRP_Slammer_Worm连续两年占据了列表中前两名，

而Slammer活动已呈现出略微下降的趋势。SQL_ Injection的下降趋势在2011年被逆转。SSH_Brute_Force继续在前10名中占有一席之地，但已下降到第9名。在2011年的报告中，HTTP_Unix_Passwords仍位列前十，但它已从第六名下降到第十名，尽管其出现数目仍在增长。

事件名称	2011年排名	趋势	2010年排名	趋势
SQL_Injection	1	上升	2	下降
HTTP_Suspicious_Unknown_Content	2	下降		
SQL_SSRP_Slammer_Worm	3	略微下降	1	下降
SNMP_Crack	4	下降		
HTTP_GET_DotDot_Data	5	上升		
Cross_Site_Scripting	6	略微上升		
SSH_Brute_Force	7	略微上升	4	略微下降
HTTP_Unix_Passwords	8	上升	6	略微上升
Shell_Command_Injection	9	上升		
Proxy_Bounce_Deep	10	上升		

表1: 数量最多的MSS特征和从2010年末到2011年末的趋势线

SQL注入

我们的启发式SQL特征（在2010年位列第二）上升到第一名，呈现出上升的趋势。2011年是攻击SQL缺陷的标杆年，多个影响巨大且有新闻价值的成功SQL注入事件被公开。黑客团体Anonymous和Lulzsec是SQL注入战术的主要实施者，并且他们继续通过新的注入攻击提升自己的技能。此外，有一些可在Internet上扫描有漏洞主机的自动化SQL注入攻击，如LizaMoon，这是我们看到的大部分攻击活动的起源。IBM MSS在其安全信息和事件管理(SIEM)规则集中添加了多个其他的攻击途径范围，并继续监视和分析每天的任何新途径。下面的小节“仍然存在的SQL注入威胁”将深入探讨此威胁的性质，并介绍组织可采取哪些措施保护其Web应用代码、服务器和网络免受SQL注入的危害。

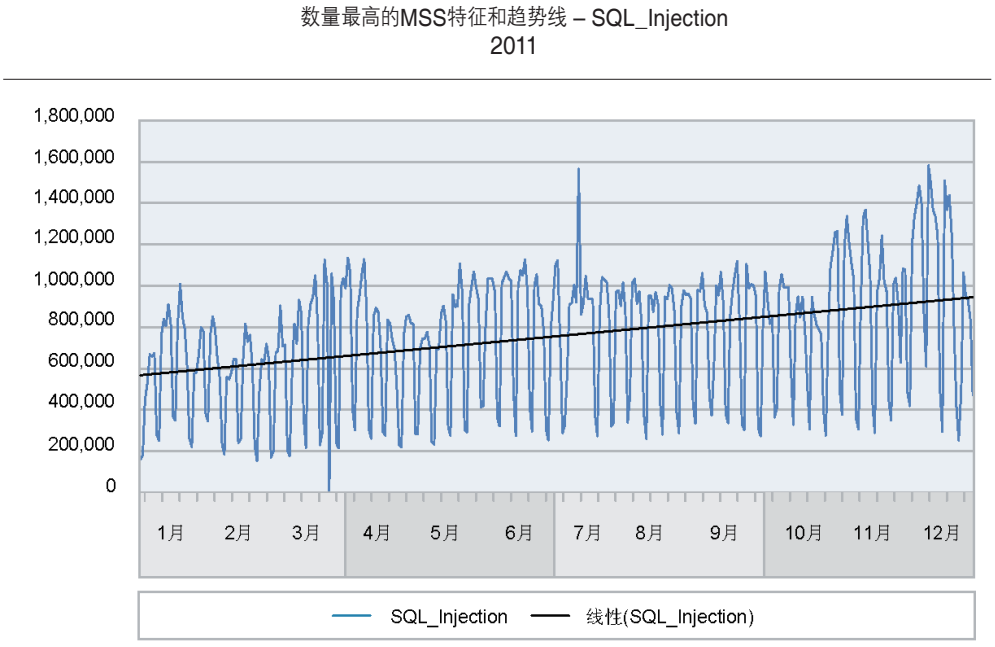


图2: 数量最高的MSS特征和趋势线—SQL_ Injection 2011

我们之中的Zeus?

触发我们位居第二的特征HTTP_Suspicious_Unknown_Content的HTTP活动可能很普通。但是，它可能表明您的网络上有一个僵尸网络（如Zeus）正在活动。Zeus是一个著名的银行业特洛伊木马，它于2007年7月首次被发现并从2009年中开始广泛传播。主要的感染途径是路过式下载和网络钓鱼。有许多不同的个人和团体安装了Zeus僵尸网络。Zeus僵尸网络的目标通常是盗窃个人信息。此信息常常是在线银行数据，可使用它访问银行帐户以进行转账。

FBI已在大力追查各种使用Zeus创建僵尸网络的团体。但是，尽管2010年成功关闭了许多最初的Zeus指挥控制服务器，但MSS发现了大量已感染Zeus的受害者。因为Zeus非常难以防御并且防病毒产品充其量只能临时阻止Zeus的传播，所以用户培训已成为主要的防御重点。培训员工不要单击电子邮件中或网页上不友好或可疑的链接，同时获取最新的防病毒更新，这已成为主要的防御战略。

SQL Slammer持续下降

2003年1月25日，一个利用Microsoft® Resolution Service中缓冲区溢出的侵略性蠕虫开始大规模感染联网的服务器。尽管这个蠕虫没有使用SQL漏洞进行传播，但绝大部分感染都发生在运行Microsoft SQL Server Desktop Engine (MSDE)的服务器上。Slammer多年来一直是一个很普遍的威胁，Slammer感染包在Internet上的UDP流量中仍占据很大的比例。事实上，2010年数量最多的特征是SQL_SSRP_Slammer_Worm。但是，在我们年中的检查中，此特征已降至第二位，在我们对年末数据的评估中已将至第三位。我们X-Force 2011年中趋势和风险报告中的“SQL Slammer消失之日”一节中探讨了2011年3月SQL Slammer活动的大幅减少，这导致了该特征在我们的列表排名中下降了。

在整个2011年，该活动发生了多次温和的起伏，如图3所示。

我们在12月注意到了高于平常值的Slammer数量，但没有出现会恢复3月前模式的迹象。我们正在监视该形势，将留意出现的任何新趋势。

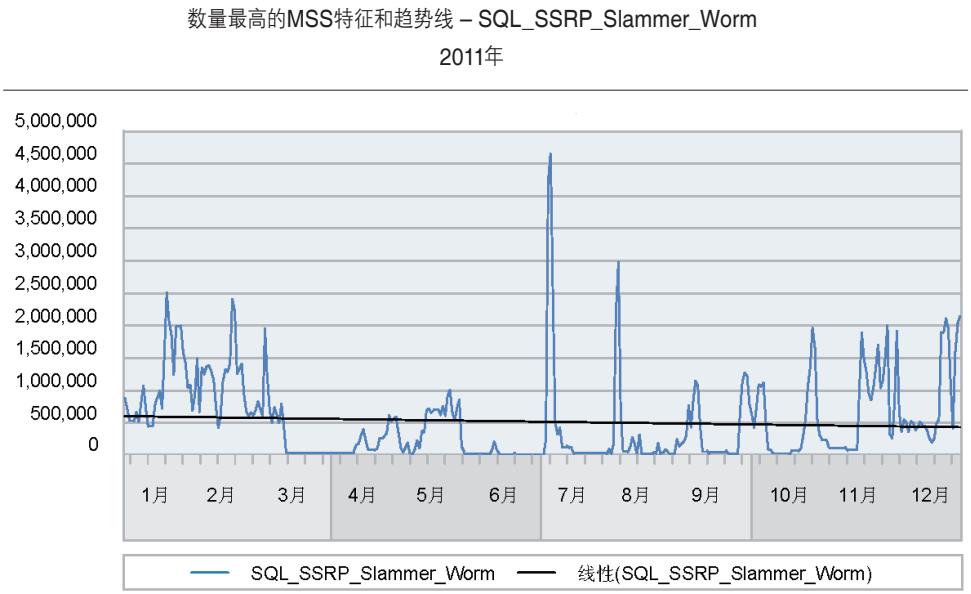


图3：数量最高的MSS特征和趋势线 – SQL_SSRP_Slammer_ Worm，2011年

SNMP漏洞

我们的SNMP_Crack特征表明了暴力破解SNMP社区字符串的企图。SNMP是一项服务，它让网络管理员能更轻松地监视网络设备的状态，以及有时控制其配置。操作系统、数据中心、交换机和路由器都在使用SNMP。SNMP使用密码等社区字符串保护对敏感信息和控件的访问。SNMP服务常常使用默认的社区字符串进行配置，攻击者首先会搜索该字符串。否则，攻击者会尝试通过暴力方式来猜测社区字符串。我们建议组织评估在其设备上激活SNMP的需求，如果没有必要，则禁用它。

数量最高的MSS特征和趋势线 – SNMP_Crack
2011年

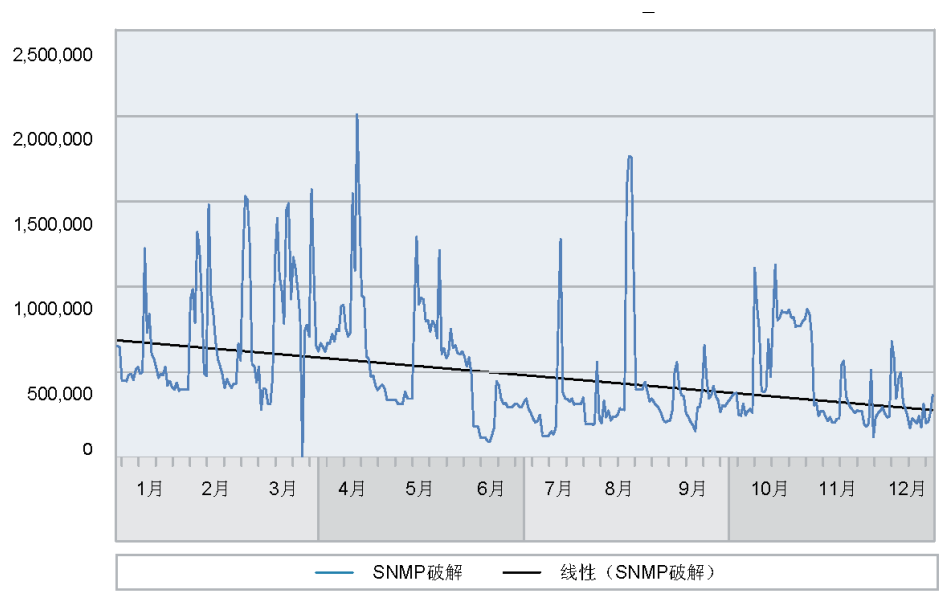


图4：数量最高的MSS特征和趋势线 – SNMP_Crack，2011年

遍历目录

HTTP_GET_DotDot_Data特征检测出一位攻击者试图绕过Web服务器执行的正常安全机制来访问平常受限制的文件。攻击者可在URL中使用“点点”(/../)序列遍历有漏洞的Web服务器上的目录，这样攻击者即可阅读目标HTTP服务器上公开的或可按HTTP进程ID读取的任何文件。例如，具有(http：//www.domain.com/..\..)形式的URL允许任何人浏览和下载Web服务器内容根目录外部的文件。(http：//www.domain. com/scripts..\..\)脚本名等URL可能允许攻击者执行目标脚本。攻击者可使用此目录的清单作为附加信息而计划一次结构化的攻击，或者可下载文件系统中其他地方的文件。

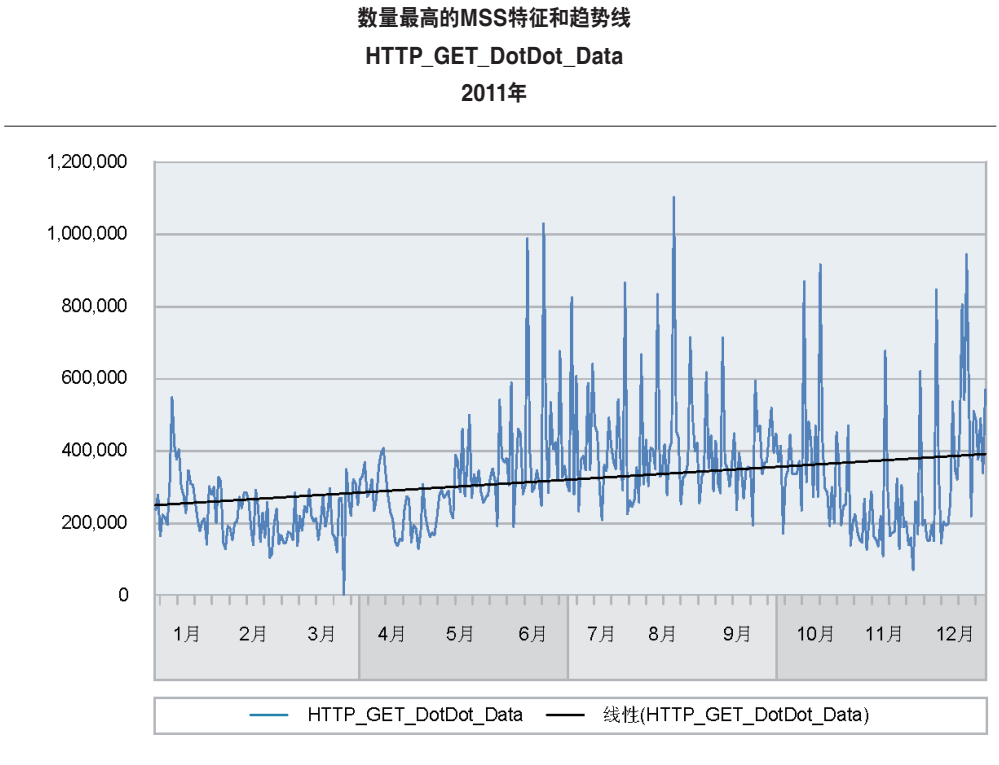


图5：数量最高的MSS特征和趋势线 – HTTP_GET_ DotDot_ Data 2011年

Cross_Site_Scripting

在Web应用中常常会发现，跨站点脚本攻击允许攻击者将客户端脚本注入其他用户查看的网页中。此攻击也可由攻击者用于绕过访问控制。此工具非常流行，是一个重大的安全风险。跨站点脚本自上世纪90年代开始流行，它是最常见的Web应用漏洞类型。我们的Cross_Site_Scripting特征名列我们按数量划分的10大特征列表中的第8名。减少该威胁在很大程度上需要多种战术，包括验证HTML输入、cookie安全性和禁用客户端脚本。现在的一些新兴技术（如Mozilla的Content Security Policy、Javascript Sandbox工具和自动转义模板）尽管仍在完善，但有助于减少该威胁。

数量最高的MSS特征和趋势线 – Cross_Site_Scripting
2011年

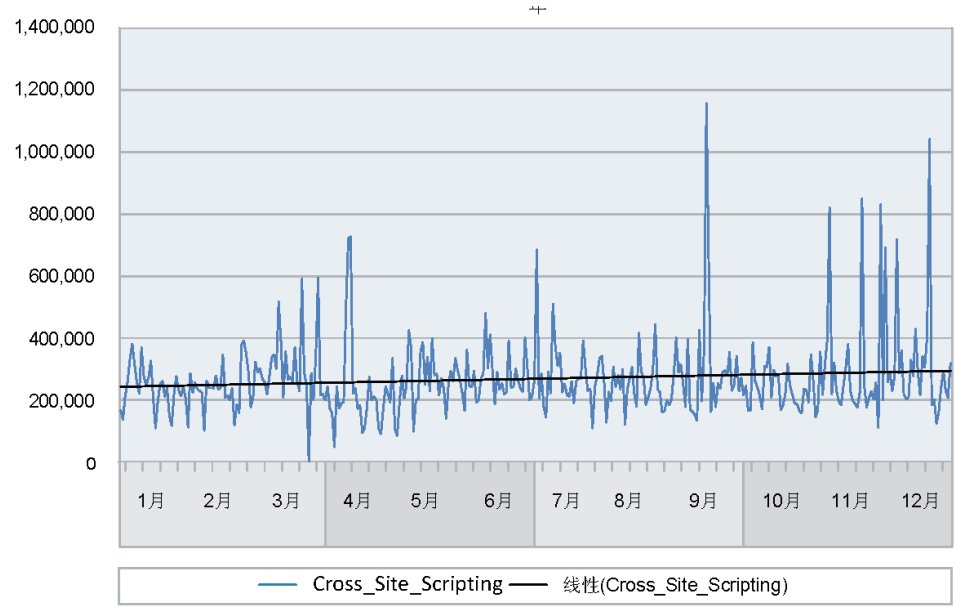


图6: 数量最高的MSS特征和趋势线 – Cross_Site_Scripting 2011年

暴力攻击

SSH_Brute_Force位居第7，与2010年的第4名相比下降了3位。在暴力攻击中，攻击者试图通过尝试大量可能的密码来获取对系统的未授权访问。此特征在指定的时间范围内从一个SSH服务器检测过量的SSH服务器标识。通过此类攻击，恶意的个人或许能够查看、复制或删除所访问的服务器上的重要文件或执行恶意代码。2011年，我们经常观察到在Internet上扫描具有弱密码的不安全SSH服务器的活动。组织应通过禁用对根帐户的直接访问并使用强用户名和密码，从而减轻暴力攻击的风险。

数量最高的MSS特征和趋势线 – SSH_Brute_Force
2011年

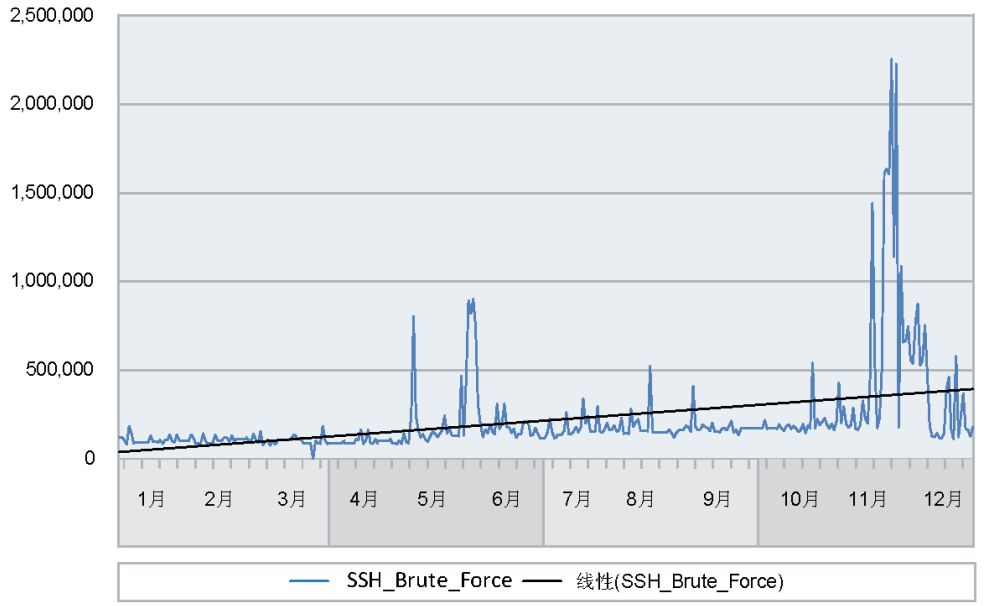


图7: 数量最高的MSS特征和趋势线 – SSH_ Brute_ Force，2011年

针对UNIX的攻击

尽管特征HTTP_Unix_Passwords仍然在数量最多的特征列表中并继续呈现上升趋势，但它已从2010年的第6名下降到了2011年的第10名。此特征检测通过Web(HTTP)服务器访问UNIX系统上的/etc/passwd文件的尝试。尽管此活动可能经过授权，但它有时是可疑的。这一种非常古老的攻击形式，但它如今仍然可能会攻击成功。

数量最高的MSS特征和趋势线 – HTTP_Unix_Passwords
2011年

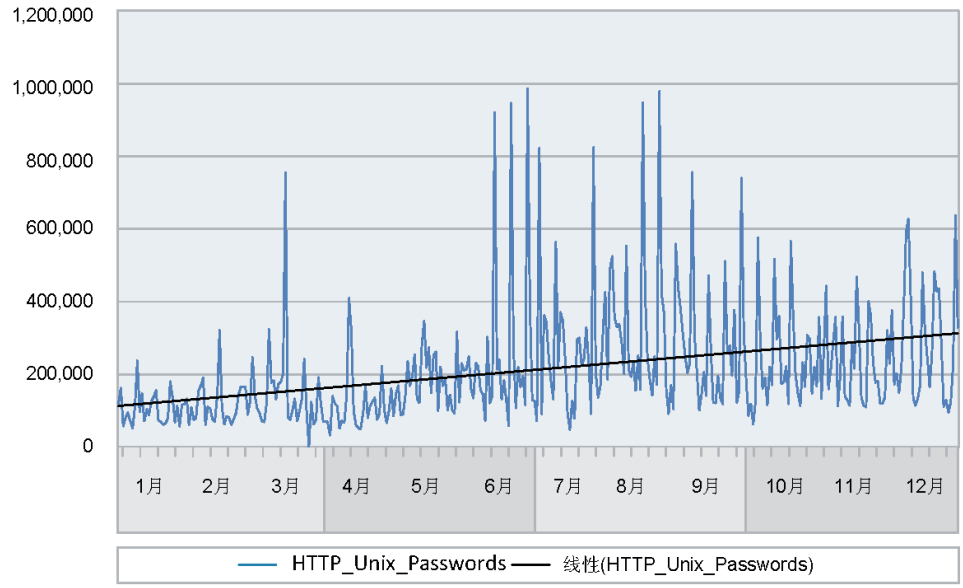


图8：数量最高的MSS特征和趋势线 – HTTP_Unix_ Passwords，2011年

远程命令注入

MSS已在全球跟踪远程命令注入攻击。用户输入未得到正确审查并且被用于执行系统shell命令的函数（如exec()和system()等PHP函数）时，就存在这些漏洞。这允许攻击者在Web服务器上执行命令。这是一种非常基本，但经常获得成功的攻击，原因与SQL注入相同，那就是没有在应用级别执行适当的审查。

我们看到的许多有效载荷包含让Web服务器通过wget下载一段远程脚本，将它存储在临时目录中，并最终执行它。该脚本旨在保持对系统的远程访问能力，收集情报，建立对攻击者服务器的指挥控制力。该服务器然后用于扫描和攻击它发现的其他服务器，无论是在本地还是通过Google远程发现的。这是攻击者获取数百个有漏洞网站控制权的非常快捷且有效的方式。2012年，我们预计会看到该活动的平稳增长，因为一些僵尸网络在增多，并且其他攻击者开始将漏洞用于自己的用途。

保护可能非常简单，只需审查来自您网站的任何输入，排除许多流行的shell命令，如passwd、wget、dir等。

另外，从服务器删除命令wget一定能阻碍攻击者不进一步挖掘而可执行的操作。

数量最高的MSS特征和趋势线 – Shell_Command_Injection
2011年

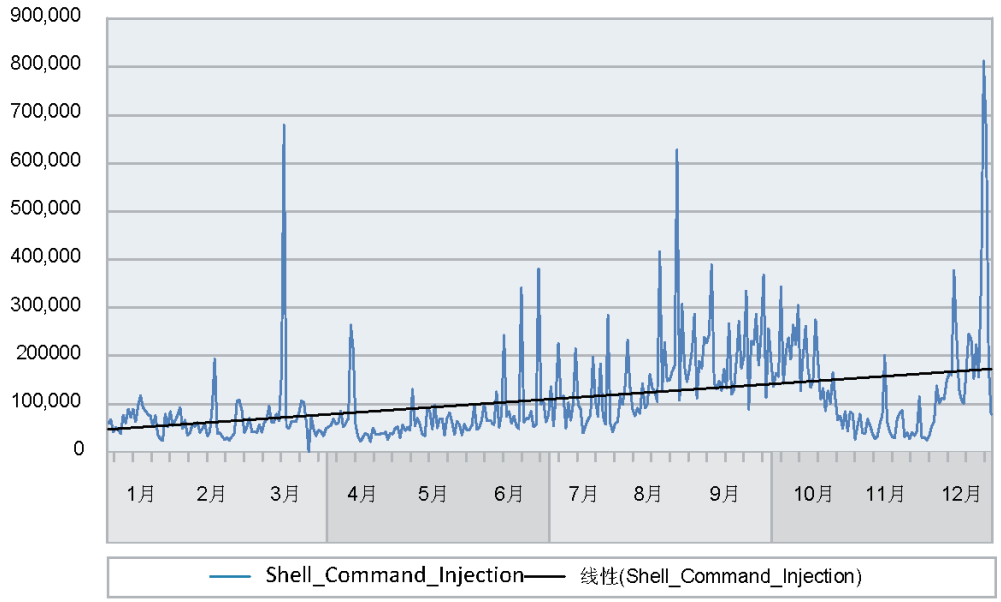


图9：数量最高的MSS特征和趋势线 – Shell_Command_ Injection，2011年

嵌套的匿名代理

X-Force Proxy_Bounce_Deep特征检测客户端通过一个HTTP代理链访问网站的尝试。我们已在不同客户端的网络上看到大量此类活动。这些活动可能是非常可疑但合法的冲浪行为，但攻击者有时会这么做，从而模糊化他们对Web服务器启动攻击的源地址。我们在过去几年内看到Internet上可用于此用途的匿名代理数量在显著增长。可在本报告的“Web内容中的匿名代理”一节中了解此主题的更多信息。

数量最高的MSS特征和趋势线 – Proxy_Bounce_Deep
2011年

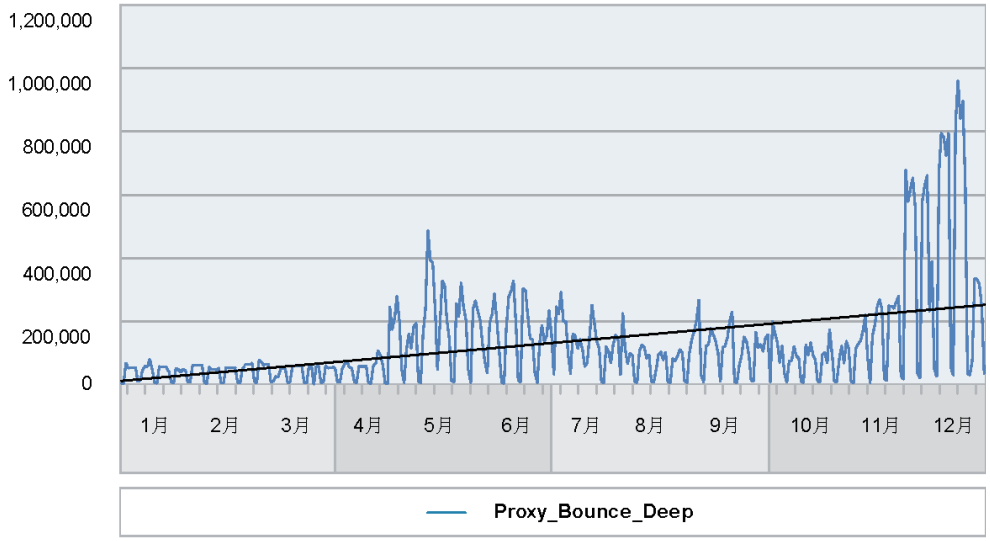


图10：数量最高的MSS特征和趋势线 – Proxy_ Bounce_ Deep 2011年

SQL注入的持续威胁

SQL注入

结构化查询语言(SQL) (最初于上世纪70年代发明) 是一种用于管理关系型数据库中各种数据的强大语言。尽管为在大型数据场中使用而发明, 但与Web的交互性相结合时, 关系型数据库扮演着新的角色。搜索表单、帐户管理、订单跟踪和协作工具都可能通过结合这两种技术来实现。这一组合带来了创新, 但也带来了数据泄漏的风险, 提供了一种有效的攻击途径。

多年来, 攻击者在Web表单中和针对Web应用编程接口使用了特殊格式的字符串。这些字符串设计为通过将SQL语句注入到Web应用代码中来操作底层数据库。此过程 (称为SQL注入) 可用于绕过身份验证, 访问未发布的数据库内容, 甚至是损害托管数据库的操作系统。

最初, SQL注入是一种针对性攻击, 因为每个站点的数据库模式和Web应用代码都不同。一旦攻击者找到一个存在漏洞的Web应用, 他就会使用精心设计的查询来描绘数据库。有了表和字段名称, 攻击者就可以访问信息和探索权限问题。这些攻击是缓慢的、有针对性的, 过程可能是高度手动的。这类针对性攻击仍然存在。当HBGary Federal CEO Aaron Barr声称他能够认出Anonymous的高层成员时, 该团体使用一种SQL注入攻击破坏了HBGary的网站。该攻击最终导致其攻陷了网络的根权限、泄漏了敏感数据以及Aaron Barr的离职。当Sony宣布

他们已在历史上最大规模的客户数据破坏发生后巩固其网络的保护时, LulzSec发布他们通过SQL注入获得的超过15万条客户详细信息予以回击。

从2008年开始, 出现了一种全新的SQL注入攻击类型, 它不再需要底层数据库结构或Web应用代码的知识。无需尝试访问数据库中存储的数据, 攻击者将注入一段脚本并让数据库执行它。因为这种攻击类型需要的唯一侦察工作是查找有漏洞的服务器, 所以它很容易自动化。第一次批量SQL注入攻击诞生了。这些攻击不关注数据库的内容, 它们一般会寻求获得根访问权限或使用Web服务器攻击那些正在访问站点的用户。这可通过将一个跨站点脚本(XSS)漏洞或其他恶意内容插入Web应用或它的缓存中来完成。

这些攻击的一个特征是，SQL注入尝试会包含DECLARE语句来插入脚本和包含EXEC语句来执行脚本。IBM托管服务看到2011年此类攻击的数量大幅增加，如图11所示，尤其是在下半年出现了jjghui和其他攻击ASP.NET站点的变体。jjghui是一种批量SQL注入攻击，它会再次引用将流量所重定向到的网站。

2011年出现了一种新的批量注入技术，它将一个脚本化的有效载荷与底层数据库结构的一些知识相结合。3月份在LizaMoon攻击中第一次看到的这种方法。这些攻击对一个有效表使用UPDATE和REPLACE命令，而不使用盲目的DECLARE和EXEC。这需要更多的工作，但更难使用简单的模式匹配来检测这种攻击 – 尤其是在该URL已被模糊化时。

威胁的性质

SQL注入攻击已存在较长时间，但它仍然是Internet上最常见的攻击类型。这种攻击经常获得成功，但一般可通过审查所有用户输入和保护数据库来阻止。从安全角度讲，有两种类型的系统容易受到此类攻击。有些连接Web的数据库是您知道的，而有些是您不知道的。您的网络可能包含具有登录帐户、员工服务、店面或任意数量公开网站的网页。这些是您知道的站点，它们可能包含敏感信息，如用户帐户、信用卡号或客户联系信息。如果包含这类信息的数据库与您的一个Web服务器交互，您可能已采取了措施来保护数据。但这就足够了吗？

您可能部署了一条安全编码策略，可能在部署您网站的第一个版本时执行了彻底的安全审核。但随着时间的推移，有许多机会出现漏洞。部署新功能时，它们的代码经过审核了吗？添加新脚本或软件应用时，它们经过漏洞研究和测试了吗？向数据库添加新表和字段时，适当设置了权限了吗？

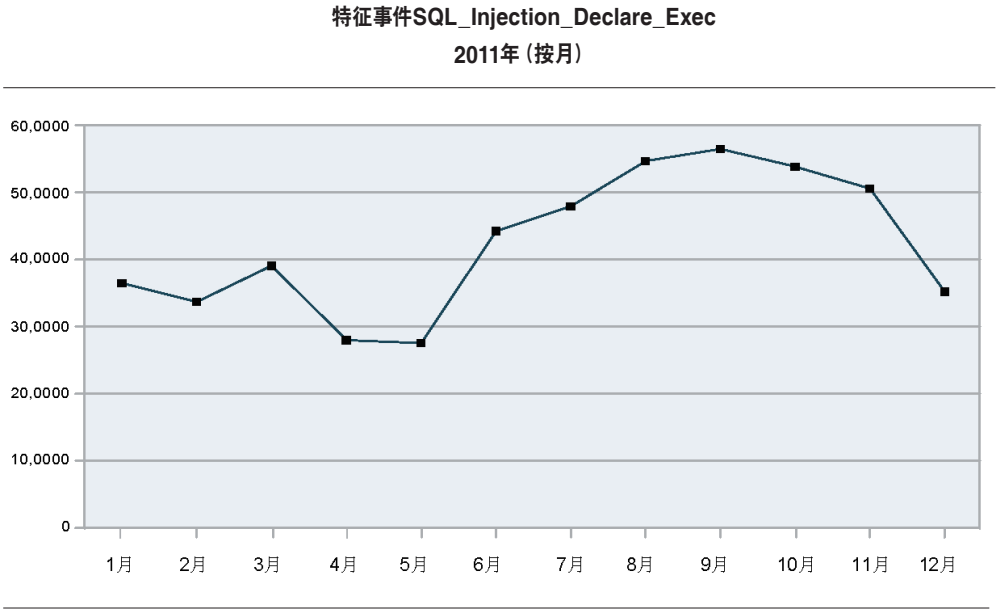


图11：特征事件 – SQL_ Injection_ Declare_ Exec，2011年（按月）

在招入新开发人员时，对他们进行了安全Web编程培训了吗？机密数据的丢失可能产生严重的后果。不仅会产生直接的财务成本，它还可能导致与您的客户出现信任问题。

除了您知道的服务器，您的网络中可能还有您不知道的服务器。随着开源数据库和Web工具的出现，整合数据库和Web服务器已变得非常简单。有了Apache Web服务器、MySQL或Postgres数据库，以及支持社区的Web代码，任何拥有构建新Web应用想法的人都可构建一个，只要他们愿意花时间去研究。知识库、协作工具、通知单跟踪和测试工具是这些内部应用的常见示例。尽管这可能带来伟大的创新，但这些应用的构建者可能没有接受过安全Web开发方面的培训。有许多资源可用于学习最佳实践，但与安全性相比，兼职Web开发人员一般更关心功能性。没有合适的培训，他们可能不知道或许会发生SQL注入。新开发人员也更可能下载封装的模块或复制示例代码 – 这两件事显著提高了成为批量注入攻击受害者的机会。

尽管这些类型的系统不太可能拥有信用卡帐号等信息，但它们仍然可能包含敏感数据。即使数据库中存储的数据不是敏感数据，数据库用户名和密码也可能是敏感的。如果数据库权限的设置太过宽容，攻击者可能获得对运行数据库的机器的根访问权限。在您的网络中找到立足点后，攻击者可继续攻击高价值的目标。它们也可安装僵尸网络并使用您的网络攻击其他目标。

帮助保护您的代码

像任何其他漏洞一样，帮助阻止SQL注入的关键是一种分层防御。Web应用代码是您的第一道防线。这是SQL注入攻击的入口点。要想帮助保护数据库不受这种代码的影响，可：

- 从用户提供的数据中删除所有SQL转义字符和无需保留的字符。我们建议使用您所选的编程语言提供的经过同行审核的库，而不要自行尝试进行审核。有许多方式来编码危险的字符，并且您可能对它们一无所知。
- 验证用户返回的编码和数据类型 – 如果您想要一个整数，则验证您是否得到了整数。
- 绝不允许用户提供的数据直接与数据库交互。即使您已审查用户提供的数据，也绝不应创建包含该数据的SQL语句。相反，使用准备好的语句、参数化的语句或已存储的过程来将您的SQL代码与用户提供的数据分开。
- 绝不向用户返回调试信息 – 将它记录在本地。
- 定期检查，查看您的编程语言、服务器框架或您使用的任何第三方软件是否拥有任何已知的漏洞。

如果审查用户提供的所有数据，那么您会阻止攻击者进入数据库。但是，不能完全依靠此方法，因为只需一个未检查的字段即可让攻击者有机会入侵。您应确保可更改Web应用中各种代码的每个人都接受了安全编程培训。考虑将其作为访问代码的要求并定期加强对安全代码重要性的认识度。

如果太匆忙或认为只是进行细微的更改，即使最优秀的开发人员也可能犯错误。解决此问题的最佳方法是采用同行代码审核。另一双眼睛有助于减少犯简单错误的机会。部署新技术、添加大型功能或对包含高度敏感数据的系统执行任何重大变更后，考虑执行外部代码审核或渗透测试，然后再公开此应用。

帮助保护您的服务器

您的第二道防线是与数据库的连接。您应该：

- 绝不允许Web应用使用根或超级用户帐户。
- 为您用于访问数据库服务器的帐户使用最受限制的权限。仅将权限授给数据库必须访问的字段，并且仅允许对必需的字段进行写入访问。
- 删除默认帐户、示例代码和可能已安装在数据库服务器上的测试应用。如果没有编写它且不再使用它，则没有理由保留它。
- 使用强密码，绝不以明文形势存储密码。
- 例行审计您的数据库和Web应用日志，查找陌生的或重复性的错误。
- 考虑使用数据库或日志监视软件预防或通知所遭受的损害。

拥有正确配置的数据库服务器可能是丢失一些数据与根系统被攻陷之间的区别。与Web服务器交互时，甚至在不认为数据是敏感数据时，您应确保数据库安全是一个优先事项。您应定期审计任何此类数据库，查找是否具有合适的权限和不必要的帐户。在添加新字段和表时，这些内容很容易被破坏。

如果攻击者设法执行SQL注入攻击并获取了足够的权限，您的操作系统安全将是最后一道防线。可采取一些步骤来帮助保护您的系统，包括：

- 保护您的数据库和Web服务器的帐户和文件系统权限安全。
- 使用可观察入侵企图的、基于主机的入侵检测或保护技术。
- 使用防病毒和恶意软件检测来查找bot感染。
- 监视Web应用、Web服务器和数据库日志中的可疑行为。

帮助保护您的网络

执行上一节中介绍的步骤有助于让您所保护的服务器远离SQL注入。但锁定这些服务器可能不足以保护您的网络远离SQL注入。如果您的网络上有未保护或未知的服务器，它们可能为攻击提供众多的机会。正确使用防火墙和基于网络的入侵保护或检测有助于填补这一空白。拦截对授权服务器以外的地址的入站Web请求可帮助您保护内部应用远离外部攻击。对于您允许进入网络的Web流量，应考虑使用Web应用防火墙或基于代理的防御。此外，所有基于网络的著名入侵检测供应商都提供了一定程度的SQL注入检测。检测方法可能因供应商的不同而不同，包括从对已知攻击字符串的简单正则表达式匹配到复杂的计分算法。在保护网络远离SQL注入的威胁时，请考虑以下事项：

- 阅读供应商提供的任何SQL注入特征的描述。一些特征非常有针对性且仅在有限的环境中会被触发，而其他特征是宽泛的且容易发生误报。了解为每种警报使用何种条件很重要。
- 在入侵检测系统看来，很多内容类似SQL，但其实不是。搜索结果、Yahoo查询语言(YQL)、Facebook查询语言和twitter源都是常见的误报。如果有大量流量来自同一个地址，则可能发生出站SQL注入事件，但在许多SQL注入特征中可能由于用户触发的事件而发生误报。我们更感兴趣的是入站SQL注入尝试，因为这些事件可能会损害您的网络。
- 定期扫描您网络中的未知Web服务器。如果找到一个，则跟踪所有者并确保已采取了某些措施来减轻SQL注入攻击。另外考虑外包的渗透测试或购买专门查找容易受到SQL注入攻击的站点的软件。
- 提供一条识别潜在安全问题并提供解决方案的安全策略或指南。

仅使用网络保护是不足够的，但是如果可以尽早识别和解决安全违规问题，您可以减轻攻击者可能导致的损害。这对于不包含敏感数据的系统特别重要，因为它们最不可能受到安全保护。即使系统本身不重要，对网络上的根级损害也是很危险的。

小结

如果采取了适当的预防措施，SQL注入攻击获得成功的机会很低。但是，保持警惕很重要，因为新的业务需求可能需要新的功能和技术。每次部署一个连接数据库的Web应用或对其执行代码修订时，您都会引入风险。所有代码更改都应经过审核，对Web开发人员的培训应是一个持续的过程。只要攻击者能够成功利用未检查的用户输入，他们就会继续尝试SQL注入攻击。而且随着形势朝僵尸网络驱动的批量注入攻击发展，几乎可以肯定有人会尝试攻击您的站点。您准备好了吗？

如需进一步了解如何保护您的服务器远离SQL注入，请访问以下链接：

保护Java：http：//today.java.net/pub/a/today/2005/09/08/handling-java-web-app-input.html

保护ASP.NET：http：//msdn.microsoft.com/en-us/library/ff648339.aspx

保护PHP：http：//php.net/manual/en/security.database. sql-injection.php

数据库安全技巧：

http：//en.wikipedia.org/wiki/Database_security

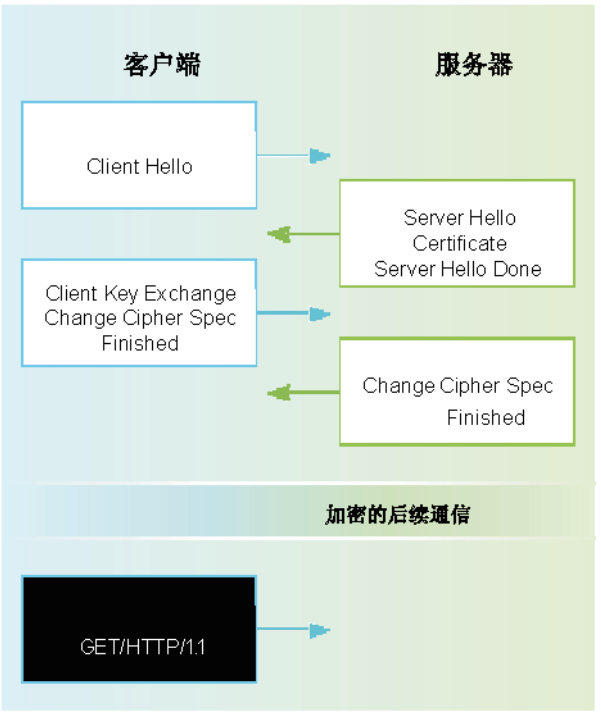
SSL安全挑战

2010年发布的Firesheep插件证明了HTTP内在的不安全性和它在托管敏感个人信息的流行网站上的广泛使用性。作为响应，Facebook和Twitter等站点相应地采用了HTTPS来为其用户带来更有效的安全和隐私保护。尽管取得了这一进步，但看到2011年发生了大量与支持HTTPS的SSL和TLS协议相关的高影响力问题，多少有些令人沮丧。本文详细分析了这一年影响SSL/TLS的3个最重要的事故和它们对威胁形势的影响。

THC-SSL-DOS

在2月（并且在10月更大范围公开），安全团体The Hacker´s Choice提供了一个概念证明工具来对通过SSL/TLS通信的服务器执行拒绝服务(DoS)攻击。该工具表明，具有普通网络连接的日常笔记本电脑具有让企业Web服务器崩溃的潜力。它利用了在TLS握手期间设置密码所需的计算资源的不对称性。

TLS握手



在典型的TLS握手期间会发生许多事情。客户端使用“Client Hello”消息发起握手，列出一系列它可能执行的密码套件。然后服务器使用“Server Hello”消息进行响应，表明它已选择了该密码套件来加密通信。在同一个数据包中，服务器还包含了一个“Certificate”消息，其中包含套件的证书，该证书建立它的身份并提供一个用于加密的公钥。

如果所提供的信息经过客户端核实，它会使用“Client Key Exchange”消息响应（然后是“Change Cipher Spec”和“Finished”消息）。“Client Key exchange”包含一个使用服务器证书的公钥加密的pre-master密钥。收到“Client Key Exchange”后，服务器使用它的私钥解密pre-master密钥（并使用它自己的“Change Cipher Spec”和“Finished”消息进行响应）。此时，客户端和服务器都可生成它们的主密钥并设置用于剩余会话部分的加密。

在握手过程（和以后对流量的对称加密）中，计算成本最大的部分是“Client Key Exchange”消息中pre-master密钥的加密和解密。尽管客户端和服务器都使用RSA算法，但服务器具有更高的计算成本（而且根据RSA密钥长度等因素，甚至可能更高）。此行为的具体细节很有趣，但不属于本文的介绍范围。

该工具可能对破坏服务器特别有效，因为它使用了客户端发起的密码套件重新协商功能。TLS协议中内置了加密通道的任一端重新协商所使用密码套件的能力。重新协商在本质上会导致另一次握手发生并产生同样的计算成本。客户端发起的重新协商使得在客户端请求TLS握手后，单个客户端会立即导致服务器执行TLS握手。使用重新协商允许攻击使用少量的机器，进而躲开典型的分布式拒绝服务(DDoS)连接阈值的限制。

减轻攻击的影响

可通过多种途径减轻攻击的影响，但所有这些方法都不完美。最简单的方法是禁用客户端发起的重新协商。99%的站点不需要支持此功能，所以在不需要时应禁用它。由于以前的TLS中间人(MITM)漏洞(CVE-2009-3555)，许多Web服务器默认会禁用此功能。

不是所有密码套件都会像RSA一样带来服务器端计算成本。不幸的是，并非所有浏览器都支持这些密码套件，并且在移动设备等低性能客户端上它们可能是糟糕的选择。不支持RSA不是一个可行的选项，尤其是考虑到它对TLS 1.1和1.2是强制性的。

如果禁用了客户端发起的重新协商功能，通过单个连接执行10,000次握手的计算成本可通过10,000个连接上的初始握手实现。此攻击然后会变成传统的DDoS攻击。可使用IDS的旧备用机器和/或投入更多硬件来减轻分布式攻击造成的损害。

值得注意的是，某些密码套件中的计算不对称性不会在TLS/SSL中修复。可通过一个“客户端谜题”将计算不对称性推送到客户端，这个谜题需要客户端执行更多工作，但这不是一个一般可接受的解决方案。正如Eric Rescorla在一篇有关此问题的帖子上指出的：“……DoS攻击者一般会使用僵尸网络（即其他人已被攻陷的计算机）来挂载他们的攻击，因此他们拥有非常多的CPU资源可供使用。这使得很难创建一个谜题来为攻击者营造足够复杂的挑战，以减少攻击威胁而不严重影响具有较少计算资源的人（如使用移动设备的人）。”[4]

BEAST

9月23日，安全研究人员Juliano Rizzo和Thai Duong为Ekoparty安全大会与会者演示了一次攻击，该攻击解密了一个客户端与paypal.com的HTTPS连接的会话cookie。该工具称为BEAST (Browser Exploit Against SSL/TLS)。该攻击利用SSL 3.0和TLS 1.0在使用密码分组链接(CBC)模式时所用的隐式初始化向量(IV)中长期熟知的缺陷。尽管此漏洞很早就为人所知，但在这两位研究人员证明了攻击它的可行性之前，它几乎被认为是假想情况。

前面对TLS握手中密码套件的讨论重点介绍了密钥交换算法。密码套件还定义了批量加密算法，用于加密在既定TLS连接上传输的数据。TLS支持两个系列的批量加密算法、流密码和分组密码。它是CBC模式中使用的分组密码。

分组密码首先将明文分解为具有固定大小的多个分组，然后加密它们。在CBC模式下，一个分组的明文首先会与前一个分组的密文执行XOR，然后被加密。但是，要加密的第一个分组之前没有密文，必须替换IV。该漏洞依赖于受影响的SSL/TLS版本在加密一条新记录时使用上一个分组密文的隐式IV方式。

攻击者必须满足一些要求才能完成攻击。首先，他需要能够监视客户端已加密的HTTPS数据。第二，他需要能够控制从客户端通过HTTPS通道发来的明文的各部分（如一个URL路径），还需要一种控制上一个已加密分组的明文的方式。尽管比路过式下载更难以实现，但第一个需求也不是无法克服。TLS/SSL协议的存在是因为人们不信任Internet上的中介；而且您可能使用的是一个不安全的无

4 http: //www.educatedguesswork.org/2011年/10/ssltls_and_computational_dos.html

线网络。研究人员指出，一些常用技术（如Java和Silverlight）满足第二个欺骗流量（包括cookie）的需求。在演示中，对第二个需求的攻击通过利用Java插件的同源策略(SOP)检查中的一个漏洞（现在已解决）来促成，该漏洞允许一个起源中的applet（假设为http：//www.attacker.com）向另一个起源（https：//www.paypal.com）发送请求。

有了这些，攻击者可一次一个字节地有效解密明文的未知部分。一般而言，攻击者让客户发出一个请求，其中对于给定分组，攻击者已知道除明文的一个字节以外的所有内容。然后会拦截并记住网络上加密的分组。之后攻击者猜测未知的字节是什么并将猜测值放在记录末尾，以便将它用作下一个记录的IV。平均而言，在攻击者找到与其所寻找的内容匹配的加密分组之前，需要猜测126次。现在，攻击者知道这个字节是什么并调整下一个请求，以解密下一个字节。此过程会继续，一直到攻击者解密了会话cookie（或他所寻找的其他内容）。

减轻攻击的影响

使用隐式初始化向量的问题已公开多年并已在TLS 1.1中修复。不幸的是，很少有浏览器真的支持TLS 1.1，所以让服务器仅使用TLS 1.1可能不是一个选项。流密码（如RC4）没有此问题，所以让服务器优先使用流密码进行通信是对此问题唯一合理的服务器端修复措施。此问题的解决方案需要在客户端上查找。不幸的是，一些SSL/TLS实现不支持向后移植的TLS 1.1修复版。供应商已开始解决此问题，但互操作性问题让此问题变得更加复杂。例如，Microsoft在2012年1月的每月更新中发布了一个补丁来解决此漏洞。

DigiNotar和Comodo损害

3月，一个与Comodo证书颁发机构(CA)相关联的注册机构(RA)被黑客攻陷，从UTN-USERFirst-Hardware的一个受信任的根证书发出了针对常见域（如“*.google.com”和“*.yahoo.com”）的9个欺诈性证书。这是一场安全灾难。为了继续保护与这些域的通信，Microsoft、Google、Mozilla和Apple等浏览器供应商不得不立即发布产品更新来撤销这些证书。幸运的是，根据Comodo报告，只看到一个伪造的证书（针对Yahoo）还在Internet上活动。

在7月中旬发生了另一次损害，这次针对的是DigiNotar CA。如果说Comodo是一场灾难，那么这就是一场毁灭性的灾难。发布了500个欺诈性证书，它们针对“*.google. com”以及难以置信的大量“*.*.com”域。Fox-IT对该漏洞的官方报告表明，超过300,000个唯一IP已访问一个针对Google的欺诈证书。像前一次破坏一样，应对此灾难需要浏览器供应商争分夺秒地发布产品更新，以尽快撤销这些证书。

产品更新可能看起来像是一种撤销证书的戏剧性举措，但考虑到当前的机制，这是可以理解的。

证书撤销

由于欺诈或信息更新而撤销证书的必要性得到了公众理解，而且已为它创建了解决方案。有两种常用于检查撤销状态的方法：证书撤销列表(CRL)和在线证书状态协议(OCSP)。不幸的是，这两种解决方案都不是真正有效的。

使用第一种方法，CRL信息可能包含在一个证书中。客户端验证一个证书时，它可下载指定的CRL，下载一个已撤销证书的序列号列表，以及检查并确定是否遇到任何已撤销的证书。另一方面，OCSP是一个协议，它让客户端能够发出对一个证书的请求（而无需下载整个列表）来检查其撤销状态。

两种方法都不是很有效，因为这些实现默认都是开放的。如果客户端没有收到撤销通知，它会假设服务器已关闭并且证书是有效的。此处明显的问题在于，如果一个MIMT可拦截流量并提供一个无效的证书，那么他也能拦截任何撤销响应。

比没有好方法撤销欺诈证书更重要的是，这些损害表明SSL信任模型自身存在更大的问题。

SSL信任模型

两个主要的SSL和TLS目标是建立通信的真实性和保密性。为了提供真实性并预防MITM假冒一个服务器，SSL的设计引入了证书和证书颁发机构(CA)的概念。如果一个站点希望提供HTTPS，它需要一个从证书颁发机构请求的证书。CA是受信任的实体，代表性的公司有Verisign、Thawte、Comodo或DIgiNotar等，他们的职责是验证该站点拥有它所声明的身份，然后颁发一个证书来表达此事实。

然后Web浏览器可预先安装这些受信任颁发机构的证书，以便在出现一个任意的证书时，浏览器可针对受信任的证书来检查该证书的有效性。但是，返回到MITM案例，攻击者可为一个站点创建一个伪造的证书，然后将它提供给尝试连接一个合法站点的客户端。因为攻击者的证书不是由受信任的证书颁发机构签署的，所以客户端的浏览器会显示一条警告，然后客户端就知道它没有到达可信的站点。

SSL信任模型的问题

此模型有几个问题。在该系统中，所有CA都被同等对待。一个CA颁发的证书与任何其他CA颁发的证书同样有效。例如，从一个随机CA针对“*.google.com”颁发的证书与从Google的实际注册机构颁发的证书同样对浏览器有效。

根据Electronic Frontier Foundation(EFF)的SSL观测项目，有600多个实体可颁发证书。考虑到有这么多公司，看到不同水平的站点安全质量以及所请求证书的各种验证水平就不足为奇了。没有必要因为向错误的实体颁发了证书而攻击CA。这在过去已发生过，未来无疑会继续发生。

该系统的另一个后果是，一旦某个CA受到信任，就会一直信任它。CA可为数百万个站点颁发证书。如果您认为不再信任一个CA，并且从存储器中删除了它的证书，那么就无法通过HTTPS访问该CA签署的所有站点。

修改SSL信任

人们已提议了某些解决方案来解决这些问题。有一些关于使用DNS来处理信任的提案，如DNS-based Authentication of Named Entities(DANE)和Certificate Authority Authorization(CAA)。这两个提案都允许将有关授权的CA信息嵌入到一个域的DNS记录中。CA可使用此信息检查谁应该颁发给定域的证书，帮助预防出现疏忽，将证书颁发给错误的实体。客户端可使用此信息验证一个证书是由一个合适的CA所颁发的。

DANE还允许采用CA信任的一种替代方式。一个站点可将证书信息嵌入到它的域记录中。一个客户端连接到一个站点时，它可将该域证书与所提供的证书进行对比。如果证书匹配，则可假设该站点通过了身份验证。这些方法的不足之处在于，CAA和DANE都需要域名系统安全扩展(DNSSEC)才能保障安全，但DNSSEC仍未得到广泛利用。

Moxie Marlinspike[5]在一篇博客中提出了当前的信任机制和DNS的一种替代方案，该文章随后发表在BlackHat USA上。他指出，DNS的使用不会使证书更值得信任。如果客户端担心一个政府CA颁发的证书被滥用于窃听流量，在依靠来自同一个国家的DNS服务器的证书数据时，如何改进这种情形？

Marlinspike呼吁SSL中的“信任敏捷性”的必要性。两条核心原则是，客户端可随时撤销对一个机构的信任，并可选择在何处给予信任。随后，Marlinspike为Firefox开发了一个名为“Convergence”的插件，它允许用户选择多个验证站点证书的“公证员”来满足这些需求，结果得到了一个灵活的系统，其中的公证员可自由地提出有关验证的安全需求，用户可自由选择他们所信任的公证员。

5 http: //blog.thoughtcrime.org/ssl-and-the-future-of-authenticity
http: //www.youtube.com/watch?v=Z7WI2FW2TcA

在目前的CA模型中，一旦CA获得信任，它基本上会永远受到信任。CA可颁发数百万个在Internet网站上使用的证书。例如，如果某个时刻您决定不再信任Verisign并从您的存储器中删除其CA，那么具有由它颁发的证书（甚至在过去您仍然信任时颁发的证书）的任何站点都将无法通过HTTPS访问。与此相比，信用敏捷性使用了Convergence，您可停止信任一个给定的公证员，但其他受信任的公证员仍然可保证站点证书的安全性。公证员系统看起来是一个不错的主意，尤其是对用户而言，但它不确定如果没有明确的财务方面的激励措施，组织创立并维护这种系统的动机是什么。

另一个也提供了信任敏捷性的解决方案是扩展TLS/SSL以支持多个证书。如果一个站点可提供由不同CA签署的多个证书，如一个来自DigiNotar，另一个来自Verisign，然后您决定不再信任DigiNotar，您将仍然信任Verisign并因此建立了一个安全连接。此解决方案的一个较大阻碍是，它需要更改TLS协议，并且供应商对新协议版本的采用速度比较慢。

未来有什么?

SSL最初于上世纪90年代初开发，旨在保护与少数站点的通信。它现在已发展到版本TLS 1.2并保护着超过200万个网站。TLS 1.1已被广泛采用，但由于之前认为只是理论上的问题已证实可成为事实，所以接受未来的版本的速度可能会更快。我们希望更新型的密码套件会得到更广泛的部署，如客户端和服务器上的ECDHE_RSA，它可提供正向加密(forward secrecy)，所以一个已泄漏的证书私钥不会被追溯性地用于解密以前所记录的流量。几乎不可避免的是，必须更改当前的SSL模型，但更改协议固有的缺陷可能需要很长时间。

Mac恶意软件的出现

简介

与以往任何一年相比，2011年出现了世界上最猖獗的Mac恶意软件攻击活动。[6]不仅在数量上是如此，在功能上也是如此。2011年，我们开始看到Mac恶意软件具有我们之前仅在Windows恶意软件中看到的功能。这可能表明计算机罪犯现在认识到攻击OS X可能有多大的利润。

让我们看看2011年发现的一些值得注意的Mac恶意软件。

MacDefender

MacDefender于2011年5月首次被发现，在接下来的几个月内发现了后续的变体（即MacSecurity、MacProtector、MacGuard和MacShield）。MacDefender最有趣的方面在于，这种恶意软件类型具有过去两年来在Windows世界中非常猖獗的扩散机制。

6 http: //blog.intego.com/dl/Intego-year-in-Mac-security-2011年.pdf

MacDefender属于名为“流氓防病毒程序 (Rogue Antivirus)”的恶意软件类别，它们将自身伪装成合法的防病毒程序。安装之后，它假装扫描您的系统，将随机的文件标记为恶意，使您的系统看起来受到了严重的病毒感染。

其用户界面具有专业的外观，这让用户更相信它是一款合法的应用。用户界面包含一个Register按钮，它会将用户带到一个网站，用户可在这里使用信用卡购买MacDefender的许可。MacDefender显示一条消息表明要删除已检测到的恶意软件，您应为许可的版本付费，所以用户可能感觉必须要注册。然后会通过用户的信用卡划款，并且也可能将其信用卡用于其他用途。

MacDefender及其变体通过SEO中毒攻击来扩散到目标用户，恶意软件的作者会操纵搜索引擎结果来创建它们的链接，这些链接托管着该恶意软件，显示在靠近搜索结果顶部的位置。用户单击一个链接时，Javascript将MacDefender安装程序下载到他们的系统中。

图12：2011年的MacDefende恶意软件屏幕截图

如果浏览器设置为在下载后自动打开安全的文件，该安装程序就会自动打开。

流氓防病毒程序是一种回报丰厚的诈骗手段，所以X-Force相信我们在未来会看到更多此类恶意软件。用户单击搜索结果中的链接时应谨慎。在单击一个链接前，检查该链接的域名是否与您查找的内容相关。另外，除非您确定软件来自信誉良好的来源，否则不要安装它。

Flashback

Flashback是一个特洛伊木马，它于2011年9月被发现。此恶意软件的变体在接下来的几个月中不断出现，每个变体都对母体进行了各种改进。Flashback将自己伪装成一个Flash Player安装程序，可在访问恶意网站时下载，显示一个下载或安装Flash player图标。

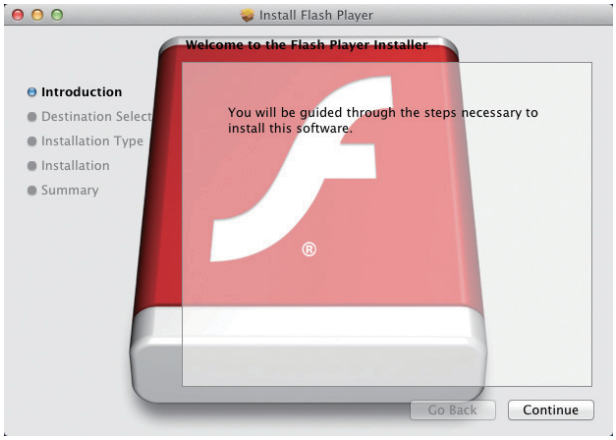


图13：2011年的Flashback特洛伊木马屏幕截图

在安装时，Flashback放置一个动态共享的库文件并使用DYLD_INSERT_LIBRARIES环境变量将代码注入到用户启动的应用中。以后的变体专门针对特定的应用（如Safari和Firefox）进行注入。注入的代码负责连接一个远程服务器来下载更新或从受感染的机器发送数据。在将代码注入Web浏览器时，这种代码注入技术类似于某种臭名昭著的Windows恶意软件（如Zeus）的行为。Zeus拦截从服务器发送到Web浏览器的网页并动态修改它们，然后在向用户显示修改后的内容。修改后的网页通常显示一个伪装的登录页面，允许恶意软件盗窃敏感信息。幸运的是，目前为止在Flashback的任何变体中都没有观察到Web注入功能。

Flashback还通过改写一些相关的文件，尝试阻止对XProtect的未来更新。XProtect是Apple内置的基本恶意软件保护系统，它使用字符串匹配来检测恶意软件。只要发现一个影响巨大的Mac恶意软件，Apple就会更新XProtect。

Flashback还尝试阻碍研究人员检测它是否在VMWare虚拟机上运行。使用此检测躲避机制在Windows恶意软件中很常见，但这是我们看到的第一个采用此技术的Mac恶意软件。这证明Mac恶意软件技术正在赶超Windows恶意软件技术。

DevilRobber

DevilRobber是2011年中最新的重大OS X恶意软件。它于2011年10月被发现，在11月和12月出现了变体。DevilRobber是在BitTorrent中非法共享的Mac应用中发现的，如Graphic Converter、Flux、CorelPainter和Pixelmator。

DevilRobber是我们目前看到的最复杂的Mac恶意软件，它包含多个组成部分。它主要是一个后门，在受感染的机器上打开一个端口以接收来自远程攻击者的命令，但它拥有的一个有趣的功能是BitCoin挖掘，它安装BitCoin挖掘应用DiabloMiner来使用受感染机器的CPU和GPU（针对具有高性能显卡的用户）的计算能力，以挖掘Bitcoin。它还尝试盗窃Bitcoin钱包（如果找到）。DevilRobber还会从受感染的机器盗窃用户的密钥链以及其他信息，将它们上传到一个远程FTP服务器。

DevilRobber还有能力检测受感染的机器是否在网关设备之后，然后启用通过UPnP转发端口。这让攻击者可使用DevilRobber打开的端口远程访问受感染的机器，即使受感染的机器位于网关设备之后也可以访问。

小结

您可能已注意到，刚提到的任何恶意软件都没有使用任何软件漏洞来扩散。我们猜测这是因为缺乏已公开的OS X攻击代码供人们重用。大部分使用攻击代码的Windows恶意软件常常重用已公开的攻击代码，如在Metasploit等攻击代码框架中找到的攻击代码，并进行细微的修改。但是，已公开的OS X攻击代码相对较少。这可能是因为人们缺乏针对一个具有相对较低市场份额的平台开发攻击代码的兴趣，或者因为

缺乏可用的技术信息。现在，借助最新版OS X中的最新安全改进，攻击的门槛更高了。OS X Lion默认实现了完整的ASLR、64位进程，还实现了一个沙盒框架。从2012年6月开始，Apple还将要求提交到Mac App Store的所有应用都启用沙盒，从而减少通过第三方应用进行的攻击尝试。

这不是说Mac用户可以高枕无忧了。正如上面的示例所示，恶意软件作者将找到替代的传送方式。而且，这些改进专注于攻击代码防御和缓解，没有真正解决我们上面提到的恶意软件类型问题，所以我们预计会在2012年看到更多的Mac恶意软件。

另一方面，Apple无疑正在采取措施进一步提高开发OS X恶意软件的成本。在最近发布的下一个OS X版本Mountain Lion中，它们添加了一个名为Gatekeeper的新功能。Gatekeeper允许用户根据应用的来源选择可在其系统上安装和运行哪些应用。用户可选择仅允许来自App Store或同时允许来自App Store和经过认可的开发人员的应用（具有相关Apple Developer ID的应用）。他们也可禁用此功能。默认情况下，只能安装或运行来自App Store或来自认可的开发人员的应用。我们相信这将对预防大规模和长期的恶意软件爆发大有帮助。

在攻击者关注OS X时，安全供应商也在关注。就此而言，X-Force预测下一波Mac恶意软件将采用逃避检测和分析的方式。奇怪的是，我们目前看到的大多数Mac恶意软件都没有任何逃避机制。我们预计人们将更多地使用Windows世界中常用的技术（如封装、反调试和虚拟机检测）。我们还预计会看到Mac恶意软件会采用Windows恶意软件中效果不错的更高级的技术，如Zeus风格的Web注入和rootkit等隐蔽技术。新的恶意软件最终还将必须应对前面提到的Gatekeeper，所以我们可能会看到恶意软件将尝试以某种方式回避它。

与我们看到的Windows恶意软件相比，Mac恶意软件的数量仍显得很苍白，但显然攻击者正开始注意到Mac正在成为可行的目标。Mac用户应意识到以前仅在Windows上看到的恶意软件现在也可能在OS X中出现。

Web内容趋势

IBM内容安全团队一直在审核和分析新的Web内容数据，每个月会分析1.5亿个新网页和图像。我们自1999年以来分析了160亿个网页和图像。

IBM Web过滤器数据库拥有68个过滤器类别和7000万个条目，每天新增150,000个新的或更新的条目。

本节介绍：

- 分析方法
- 网站的IPv6部署
- 匿名代理数量的增多
- 恶意网站

分析方法

X-Force通过统计IBM Security Systems Web过滤器数据库中分类的主机，采集内容在Internet上的分布信息。统计主机数量是一种确定内容分布的公认方法，可提供真实的评估结果。使用其他方法时，如统计网页和子页面，结果可能有所不同。

网站的IPv6部署

随着IPv4地址数量即将耗尽，我们预计越来越多的Internet站点会转而使用IPv6。但是，最近5个月的结果并不符合预期。为了度量网站的IPv6部署，我们每月对数百万个主机发出DNS请求（在DNS中检查AAAA记录）。

拥有至少1个支持IPv6主机的域所占的比例相对平稳，在2.2%与2.6%之间波动。

考虑到许多公司和组织都在计划实现永久的IPv6部署，在下一个世界IPv6日（2012年6月6日）查看IPv6支持是否出现显著增长一定会很有趣。

提供IPv6主机的域所占的百分比
2011年8月到2011年12月

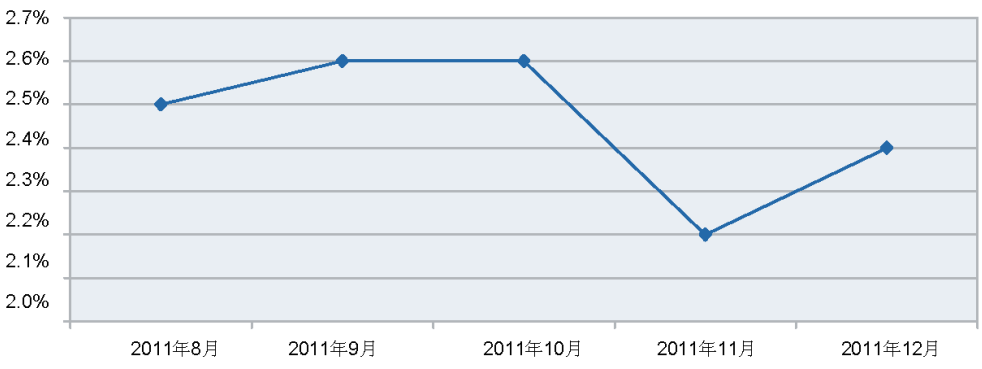


图14：提供IPv6主机的域所占的百分比 – 2011年8月到2011年12月

7 http: //en.wikipedia.org/wiki/World_ipv6_day

匿名代理的增多

随着Internet变成我们的家庭、工作和学校生活中更重要的一部分，负责在这些公共设置中维护可接受的环境的组织越来越发现需要控制人们可浏览的地方。

一种控制方法是阻止访问不可接受或不当网站的内容过滤系统。一些人尝试使用匿名代理（也称为Web代理）避开Web过滤技术。

Web代理允许用户在Web表单上输入一个URL，而不是直接访问目标网站。使用代理可向Web过滤器隐藏目标URL。如果Web过滤器没有设置为监视或拦截匿名代理，那么此活动（在通常情况下会被阻止）会绕过过滤器，允许用户到达不允许访问的网站。

新注册的匿名代理网站的增长反映了这一趋势。

在2011年上半年，已注册的匿名代理数量是3年前的4倍。在2011年下半年，已注册的匿名代理数量仍然是3年前的3倍。但是，这是自2009年开始以来我们首次没有看到此数量再次增长。或许Internet活动更多地关注社交网络。在许多情况下，不会在工作场所或学校中拦截这些网站，所以人们不再需要避开内容过滤系统。

新注册的匿名代理网站数量
2008年到2011年

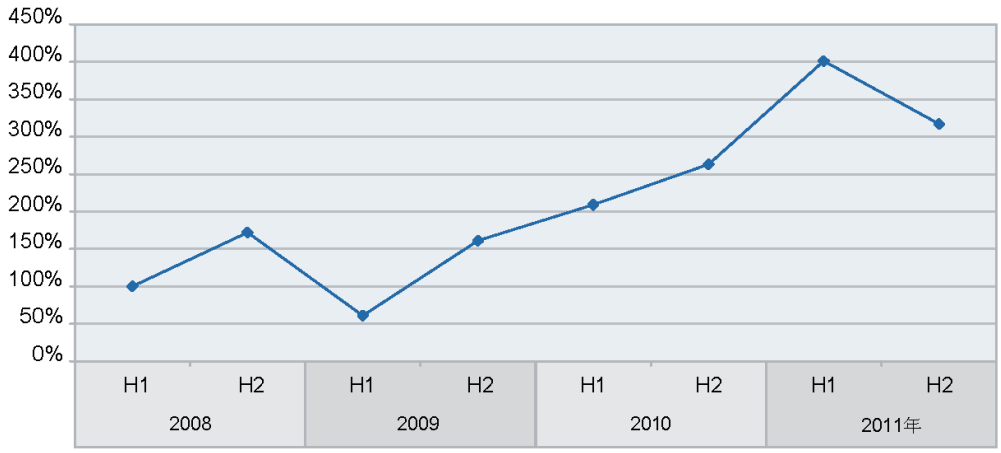


图15：新注册的匿名代理网站数量 - 2008年到2011年

但是，社交网络平台的使用带来了新的挑战，尤其是对需要控制与其他用户共享哪些信息和防止共享机密信息的公司而言。因此，许多公司开始使用Web应用控制系统，常常将其用作下一代防火墙的一部分。

匿名代理仍然是需要跟踪的一种关键的网站类型，因为很容易确定哪些代理允许人们隐藏潜在的恶意意图。

从新注册的匿名代理的顶级域中可以看出，2011年上半年的趋势（IBM X-Force 2011年中趋势和风险报告中已详细报告）仍在继续。.tk和.com域继续占据优势地位，占所有新匿名代理的70%以上。

恶意网站

本节探讨了托管恶意链接的国家或地区，以及最常链接到这些恶意网站的网站类型。2011年漏洞披露一节中在攻击代码上下文内提供了有关恶意网站的更多信息。

恶意Web链接的地理位置

美国仍然是提供恶意链接的主机数目最多的国家。所有恶意软件链接中超过1/3都位于美国。第二名是罗马尼亚，占8.5%。中国在过去2年中位居前两名，现在与法国并列第三，占5.7%，如图16所示。

第二级国家或地区已省略，但其数字变化在2010和2011年的数据中都不足1%。

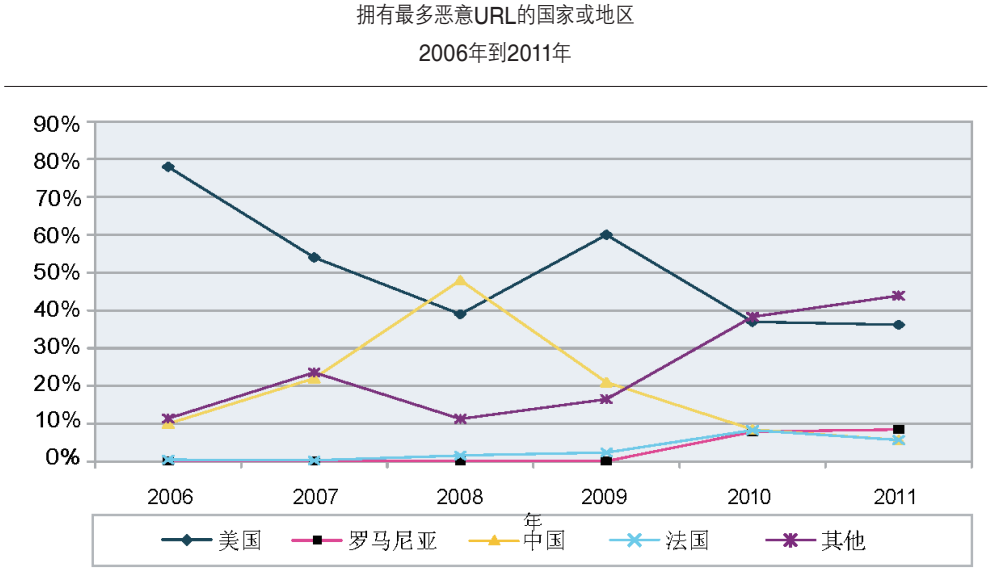


图16: 拥有最多恶意URL的国家或地区 - 2006年到2011年

包含恶意链接的流行网站

正如前面IBM X-Force趋势和风险报告中所报告的，攻击者越来越多地关注使用可信网站的流行名称来降低最终用户的防御力度，使用保护技术隐藏他们的企图。恶意Web内容的使用也是如此。以下分析简单介绍了最常包含已知、恶意内容的链接的网站类型。

一些顶级类别可能不足为奇。例如，人们可能预计色情和赌博内容位于列表顶部。这二者现在占所有恶意链接的近40%。但是，第二级候选内容属于一个更加可信的类别。

搜索引擎、博客、公告板和个人网站属于第二级类别。大多数此类网站都允许用户上传内容或设计他们自己的网站。换句话说，这些类型的网站不可能故意托管恶意链接。

下图显示了恶意链接的分布历史。

包含至少一个恶意链接的顶级网站类别
2009年到2011年

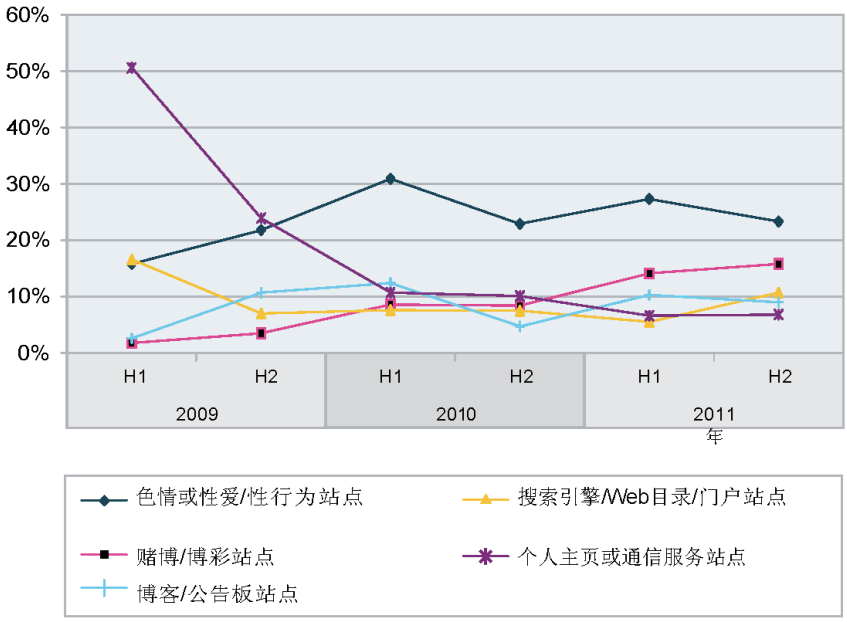


图17: 包含至少一个恶意链接的顶级网站类别 - 2009年到2011年

回头看看前3年，就会发现有趣的趋势。

- 色情和赌博等专业“坏”网站现在明显占主导地位并系统性地分发恶意软件。
- 色情内容位居榜首，一直稳定在23%左右。
- 赌博是唯一一个在每个阶段都出现显著增长的类别。在0.6%的成年人拥有赌博问题的背景下，8赌博站点成为了恶意软件分发者的一个流行目标。
- 博客/公告板在过去6个月已下降到9%。
- 个人主页（经典的Web 1.0网站）出现了大幅下跌。一个原因可能是，与社交或商业网络中流行的Web 2.0应用相比，个人主页已不那么时髦了。
- 搜索引擎、Web目录和门户站点死灰复燃，在两年半的时间内首次突破了10%。

8 http: //en.wikipedia.org/wiki/Gambling_addiction#Prevalence

垃圾邮件和网络钓鱼

IBM垃圾邮件和URL过滤器数据库提供了包含来自全世界的垃圾邮件和网络钓鱼攻击的视图。内容团队主动监视着数百万个电子邮件地址，已识别出攻击者使用的垃圾邮件和网络钓鱼技术中的众多进步。

目前，垃圾邮件过滤器数据库中包含4000多万个相关的垃圾邮件特征。每个垃圾邮件分解为多个逻辑部分（语句、段落等）。为每部分和数百万个垃圾邮件URL计算了一个唯一的128位特征。垃圾邮件过滤器数据库中每天有大约100万个新的、更新的或删除的特征。

本节介绍以下主题：

- 垃圾邮件量不断下降
- 2011年的主要垃圾邮件趋势
- URL垃圾邮件中常见的顶级域
- 垃圾邮件 – 起源国家的9趋势
- 电子邮件诈骗和网络钓鱼
- Flashback和垃圾邮件的未来前景

垃圾邮件量不断下降

在上一个趋势和风险报告中，我们提供了垃圾邮件在过去几个月，甚至是几年中的下降详细信息。我们相信这是由于之前的报告中讨论的多个僵尸网络减少所造成的。您可在下图中看到这些总数在持续下降。

垃圾邮件数量的变化
从2008年4月到2011年12月

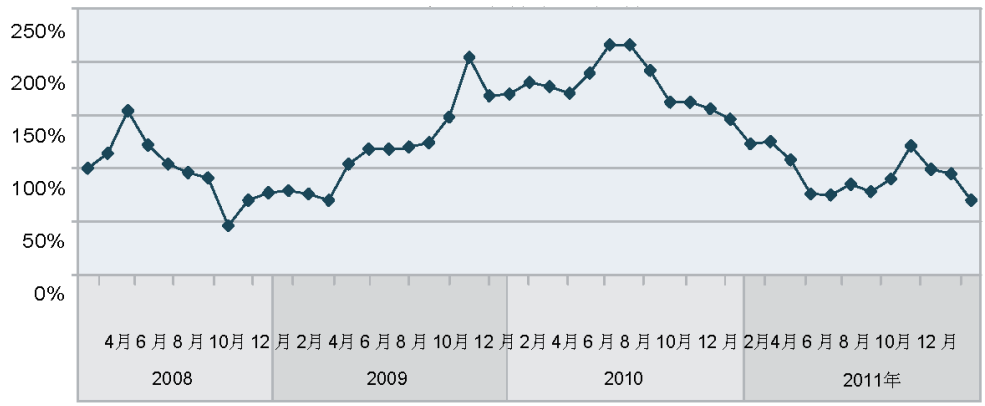


图18：垃圾邮件数量的变化 - 从2008年4月到2011年12月

9 本报告中的垃圾邮件、网络钓鱼和URL统计信息使用了WebHosting.Info提供的IP-to-Country Database(http：//www.webhosting.info)，可从http：//ip-to-country.webhosting.info获得。地理分布通过向IP-to-Country Database请求主机（对于内容分发）或发送邮件服务器（对于垃圾邮件和网络钓鱼)的IP地址来确定。

2011年主要的垃圾邮件趋势

下图总结了我们在2011年观察到的主要垃圾邮件趋势。

可以看到，2011年发出的垃圾邮件在多个方面都发生了变化。我们定义了多个阶段来突出这些变化：

- 阶段0—初始情形：

  2010年12月开始

- 阶段1—Rustock第一次关闭：

  2010年12月25日到2011年1月9日

- 阶段2—在Rustock两次关闭之间：

  2011年1月10日到2011年3月15日

- 阶段3—在Rustock第二次关闭之后：

  2011年3月16日到2011年5月18 日

- 阶段4—垃圾邮件量第一次恢复：

  2011年5月19日到2011年8月22日

- 阶段5—垃圾邮件量第二次恢复：

  2011年8月23日到2011年11月29日

- 阶段6—垃圾邮件量年末下降：

  从2011年11月30日开始

我们在IBM X-Force 2011年中趋势和风险报告中详细讨论了第0到第4个阶段。新的第5和第6阶段以ZIP或RAR恶意软件垃圾邮件（再次）和基于图像的垃圾邮件为主导，接下来的两节中将讨论该内容。

垃圾邮件量和纯文本、图像和ZIP/RAR垃圾邮件所占的百分比
2010年12月到2011年12月 (每周)

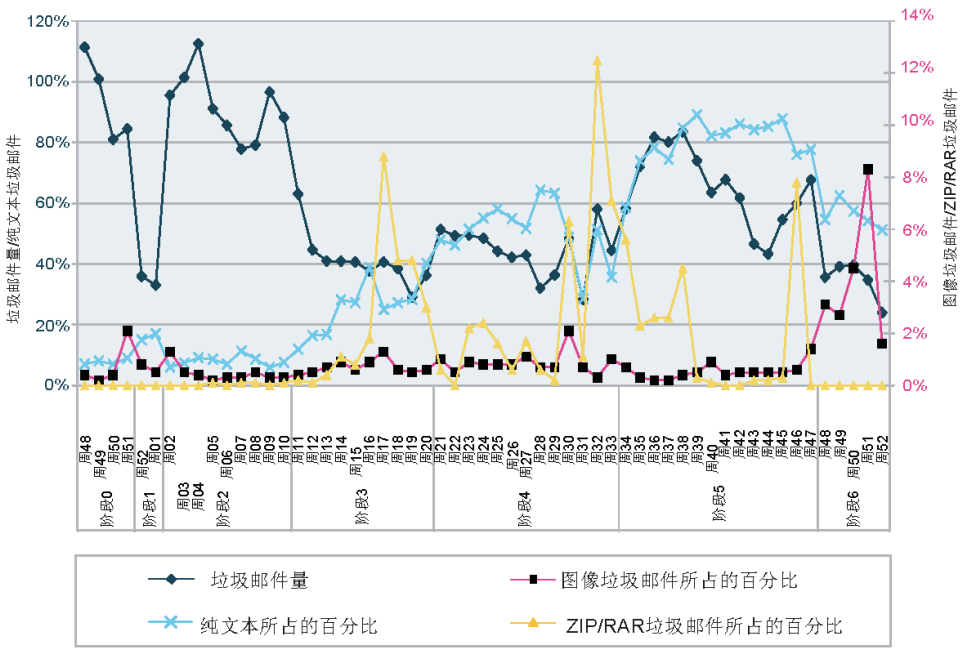


图19: 垃圾邮件量和纯文本、图像和ZIP/RAR垃圾邮件所占的百分比 - 2010年12月到2011年12月 (每周)

查看整个时期时，显然纯文本垃圾邮件几乎出现持续的增长。在前几年，我们看到以简单的纯文本编写的垃圾邮件在5%到30%之间。这是我们第一次在较长时期内观察到这些较高的值 – 有时占第5阶段的80%以上。在第6阶段，它下降到了55%左右。

纯文本形式的垃圾邮件使得根据内容进行垃圾邮件检测更加困难，因为没有像特殊的附件类型或恶意html代码序列这种可用于构建模式的固定特征。

但是，合法电子邮件出现了相反的趋势。只有少量其他的状态消息或时事通讯类型没有使用html。作为电子邮件特征，简单的纯文本迟早会变得越来越可疑。有一天它甚至会被用作拦截标准。

2011年的恶意软件ZIP垃圾邮件

第3阶段中垃圾邮件的ZIP附件已在IBM 2011年中趋势和风险报告中详细讨论过。

在2011年下半年，我们看到包含ZIP附件的电子邮件在18%到43%出现了3个峰值，每个峰值出现一天。特洛伊木马是最受欢迎的恶意软件附件类型。在7月末的峰值期间，超过一半的ZIP附件包含特洛伊木马Win32/Fivfrom.gen!B。为了鼓励用户打开这些附件并单击恶意软件二进制代码，垃圾邮件发送者使用了多个类似第3阶段中使用的垃圾邮件的变体。一个主要的变体是表明将从用户的信用卡扣除100美元，并且用户可在附加的文件中找到详细信息的消息。

我们可以在其他两个峰值期间看到类似的画面：8月中旬占主导的恶意软件类型为TrojanDownloader: Win32/ Cbeplay.M。出现此峰值两周后，ZIP附件的百分比大约为每天10%。此类的典型示例是伪装来自一个著名包裹服务公司的送货通知，试图说服用户打开附件并单击其中的二进制文件。

第3个峰值在9月20日发生。占主导的恶意软件类型为TrojanDownloader: Win32/Chepvil.N。

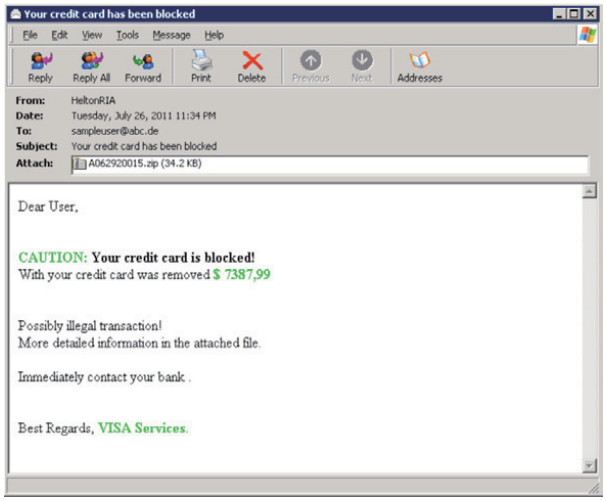


图20：有关已扣费信用卡的伪装消息 – 2011年7月

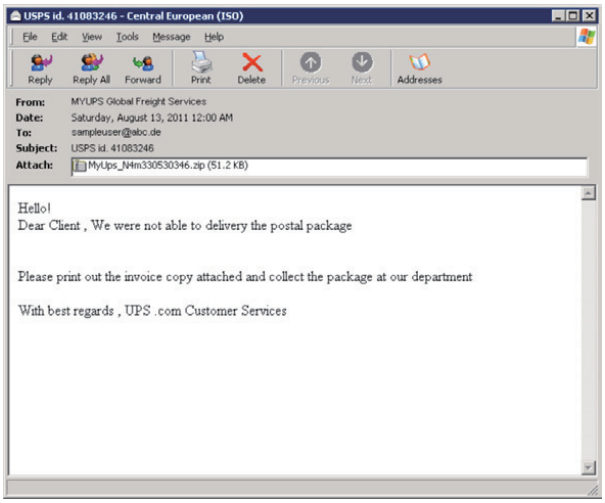


图21：伪装的送货通知 – 2011年8月

2011年的图像垃圾邮件

图像垃圾邮件的复兴让我们非常惊讶。在前两年，我们没有看到大量的此类垃圾邮件。在大部分时间里，此类垃圾邮件的百分比都在1%以下。但从11月末开始，我们在这些统计信息中看到较大的峰值。

以前的图像垃圾邮件使用图像来传输实际的垃圾邮件消息，如显示一些账单或显示URL并请求用户在其浏览器中键入该信息。仍然存在一些这样的老式的图像垃圾邮件，但大部分最新的图像垃圾邮件已是合法组织或公司的徽标。电子邮件的文本会声称以下类似内容：

- 您的交易失败，请单击该链接查看详细信息。
- 我们收到有关您的业务的投诉，请单击此处。

使用这些徽标的实际用途是让用户单击所提供的链接 – 一个感染用户机器的恶意软件链接。此类型的电子邮件类似于网络钓鱼。请查阅“电子邮件诈骗和网络钓鱼”一节，了解此类垃圾邮件的更多细节。

看到垃圾邮件发送者在2012年使用其他方法让用户单击恶意链接一定会很有趣。

基于图像的垃圾邮件所占的百分比（每天）
2011年11月到2011年12月

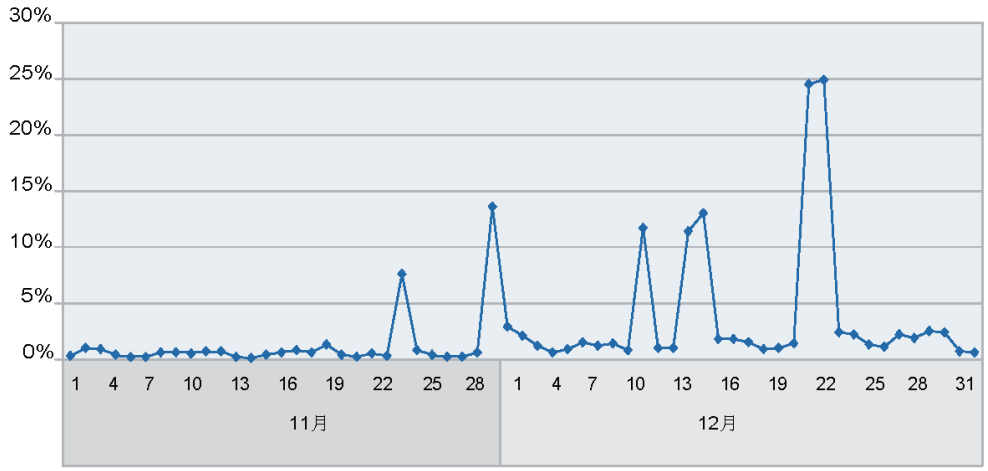


图22: 基于图像的垃圾邮件所占的百分比（每天） - 2011年11月到2011年12月

URL垃圾邮件中常见的顶级域，包含长期趋势

2011年垃圾邮件发送者使用的顶级域与2010年类似。一个例外是.ua，这是乌克兰的顶级域。此域用于获取Internet上的新内容，垃圾邮件和网络钓鱼始终希望让用户单击所提供的链接。值得查看一下恶意份子使用的顶级域的长期趋势。最近4年中这已发生了重大变化。

- 从2008年到2011年用得最多的顶级域是.com，它始终居于第一或第二位。
- 其他一般性的顶级域.net、.info和.org多年来仍然是垃圾邮件发送者热衷使用的域。但是它们在2011年显著减少。
- 从2010年初开始，.cn（中国）显著减少，从未进入过前15名。
- .cn被.ru（俄罗斯）取代，后者在2008年进入了前自2010年开始取代.com而占据了头把交椅。
- 2011年的新秀是.ua（乌克兰），它从2011年春季开始保持在第3名。

垃圾邮件URL中顶级域的使用
2008年第1季度到2011年第4季度

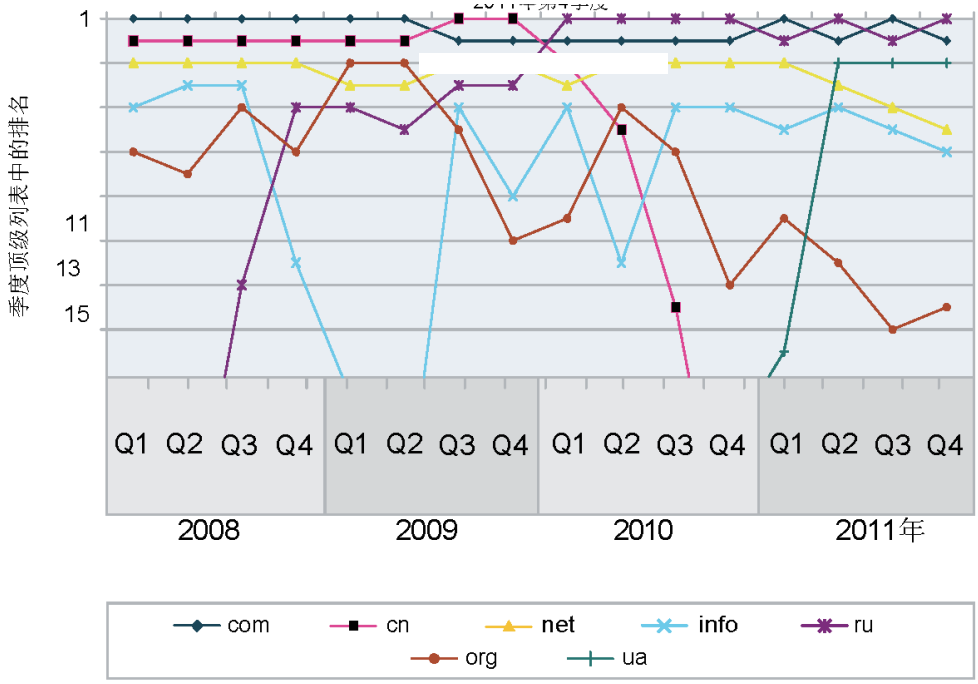


图23：垃圾邮件URL中顶级域的使用 - 2008年第1季度到2011年第4季度

根据这些长期统计信息，我们产生了一些有趣的疑问：

- 为什么.com在垃圾邮件发送者中如此流行？.com域是目前为止Internet中使用最多的顶级域。.com域廉价且容易注册。而且，电子邮件中的.com URL总体来讲是不可疑的。
- .cn（中国）顶级域发生了什么？在2008和2009年，中国的域是垃圾邮件发送者中最受欢迎的域。但是，由于中国从2009年12月中旬开始加严注册.cn域的规则[10]，这似乎对垃圾邮件发送者有一定的震慑作用。
- 为什么俄罗斯(.ru)与中国不一样？

他们尽力了。在2010年4月1日，俄罗斯NIC也加严了他们注册新域的规则。[11]18个月后，它们再次加严了规则。[12]但是，垃圾邮件发送者继续选择.ru域来提供其产品。目前，.ru仍然是垃圾邮件中使用最多的国家代码顶级域。

- 因为只有少数顶级域被广泛用于垃圾邮件中，这会是否为应对垃圾邮件的一个操作点？是也不是。如果注册机构将采取协同行动来应用与中国相同的规则，这可能会有所帮助。但这是一种不切实际的期望。

注册是一个法律问题，每个国家的处理方式都不同。可能始终会存在松散的注册机制为垃圾邮件发送者敞开大门。另外，注册域只是承载垃圾邮件内容的一种方式。另一种方式是使用其他不需要注册域的内容宿主。

10 http://www.cnnic.net.cn/html/Dir/2009/12/12/5750.htm

11 http://news.softpedia.com/news/Enhanced-Security-Measures-for-RU-Domain-Registrations-138234.shtml

12 http://www.abuse.ch/?p=3581

垃圾邮件 - 起源国家的趋势

查看前3年发出最多垃圾邮件的国家时，就会发现一些有趣的长期趋势。

- 3年前，巴西和美国在市场上占主导地位。
- 印度表现出接近持续的增长，现在仍占据着较大的比例，发出了所有垃圾邮件中的14%还多。
- 美国在一年前排名第一，现在仅发出了所有垃圾邮件的2%。
- 越南在2009年迅速增长，在2011年第一季度已显著下降，但在2011年下半年又恢复了显著的增长，发送了所有垃圾邮件中的10%以上。
- 印度尼西亚是一位新来者。它在3年来表现出了持续的增长，现在生成了所有垃圾邮件中的10%。
- 巴西在过去18个月里所占的百分比下降了一半。
- 澳大利亚是另一位新来者，到2011年末发出了所有垃圾邮件中的5.6%。

每季度的垃圾邮件起源
2009年第1季度到2011年第4季度

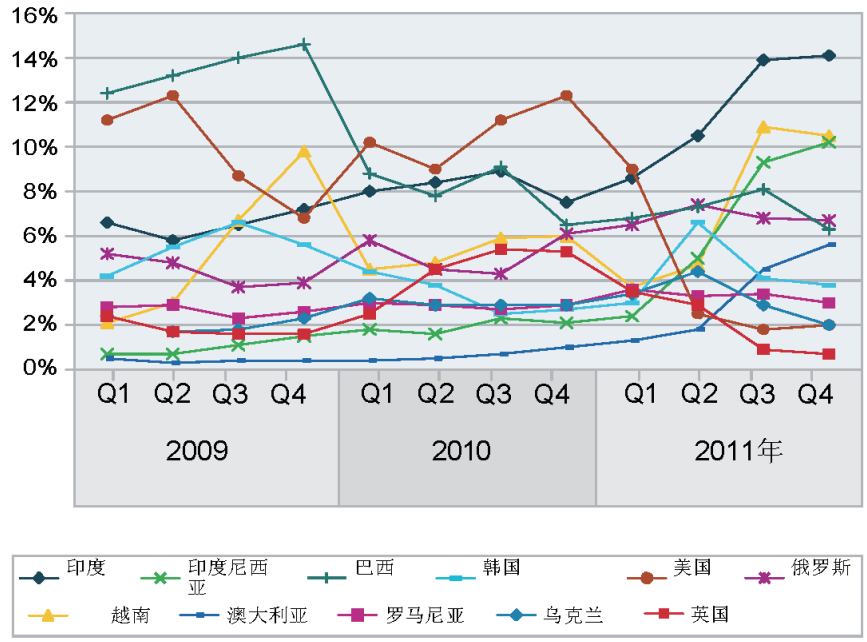


图24: 每季度的垃圾邮件起源 - 2009年第1季度到2011年第4季度

电子邮件诈骗和网络钓鱼

电子邮件诈骗和网络钓鱼提供的诈骗和网络钓鱼统计方法

正如早期的趋势和风险报告中所指出的，我们在2010年和2011年上半年看到了传统电子邮件钓鱼呈下降趋势。

但是，这个行业并没有彻底死掉。传统的电子邮件钓鱼已被不法分子使用的一些新方法所取代，但区别不那么明显。我们仍然看到大量类似普通网络钓鱼的垃圾邮件，如：

- 看似来自银行，要求用户单击所提供的链接以更新帐户、确认其数据等的电子邮件。
- 看似来自社交网络，有关一个可通过单击所提供链接来确认添加好友申请的电子邮件。

在传统电子邮件钓鱼上下文中，我们在一段时间后注意到了一个主要变化。许多钓鱼电子邮件中包含的许多网络钓鱼页面不再放在新注册的域上。这些域的优点在于，钓鱼者能够选择一个类似于钓鱼受害者的域名，如 hxxp：//www.<banknamewithsmallspellingmistake>.com。

钓鱼者利用（有时候结合使用）新的国际化域名。[13]一种对抗方法是迅速关闭这些域。已围绕这些钓鱼网站创建了新的域关闭服务。

通过聪明地进行尝试，钓鱼者找到了其他避开这种关闭问题的方式。如今，许多网络钓鱼页面被用作合法网站的子页面，如hxxp：//www.<legitimatesite>. com/<anyword>.html。这带给钓鱼者带来的优势在于，这些子页面的域是无法关闭的，因为它们属于一个合法的网站，在一些情况下甚至属于一个业务相关网站。为了放入这个子页面，钓鱼者需要攻击该合法网站。一旦攻陷了该网站，钓鱼者就能轻松地在Web服务器上添加其他页面 – 仅包含几KB的数据。第三，他们发出包含这个新子页面链接的钓鱼电子邮件。钓鱼者收集用户在这个子页面上输入的凭据，这个页面通常看起来像预期的银行登录站点。

钓鱼者甚至能够通过仅向一定比例单击此链接的用户显示此页面，让安全人员更难使用此方法检测这类页面。

但是，或许更令人吃惊的是，不是所有这些类似钓鱼的电子邮件都提供了这种钓鱼网站的链接。相反，它常常链接到以下内容：

a) 一个医疗产品、时尚配饰的在线商店或等同于普通垃圾邮件所提供链接的软件。

b) 可在单击链接时感染您的计算机的恶意软件。

那么为什么钓鱼者会将他们的方法更改为某种看起来不合逻辑的东西，尤其是在情况(a)中。一些原因可能是：

- 这是一种已经过验证的不错方法，让用户在电子邮件看起来像来自一个合法组织（如银行或社交网络）时单击链接。因此，它只是一种单击欺诈。[14]可能这些网站为钓鱼者付费推广其网站，他们不知道推广是如何进行的。
- 设置一个可能在几分钟内就被安全产品拦截的伪装银行站点需要太多的工作。在用户的计算机上安装特洛伊木马要廉价和方便得多，因为特洛伊木马可独立捕获银行凭据，无需用户的主要银行参与。

13 http：//en.wikipedia.org/wiki/IDN_homograph_attack

14 单击欺诈是按单击次数付费在线广告背景下的一种Internet犯罪（请访问http：//en.wikipedia.org/wiki/Pay_per_click）。这种欺诈通过模仿或鼓动单击广告来完成。每次点击都会生成收费。与对广告链接目标真正感兴趣的用户不同，这些单击没有任何趣味，因此支付的费用是没有报酬的。有关更多详细信息，请访问http：//en.wikipedia.org/wiki/Click_fraud

- 销售假冒的医疗产品、软件和时尚配饰仍然是一个有利可图的业务，一些用户可能没有思考为什么单击来自银行或社交网络的电子邮件中提供的链接时会出现这种在线商店。因此，这只是让用户访问其在线购物商店的许多方法中的一种。

我们还看到了这些最新网络钓鱼趋势的另一个数学和统计后果，特别是在2011年。许多看起来像钓鱼电子邮件的垃圾邮件是普通的医疗或恶意软件垃圾邮件。但是在许多统计数据中，它们被视为钓鱼电子邮件。这不一定是个错误，因为对于所提供的恶意软件链接，数据窃取恶意软件可能会骗取凭据，因此可认为将这些邮件称为垃圾邮件钓鱼是正确的。

普通的垃圾邮件、网络钓鱼和恶意软件垃圾邮件之间的界限变得越来越模糊。其他一些方面可能对网络钓鱼统计信息具有重大的影响，包括：

- 本节仅考虑来自普通电子邮件的网络钓鱼。它不包含来自社交网络内的网络钓鱼消息。
- 提供的统计信息统计了所收到的钓鱼电子邮件的绝对数量，与2008年相比，这些数字直到2011年中期一直在下降。另一方面，有许多关于网络钓鱼增多的报告。这没有冲突，因为这代表着攻击数量。可能存在更多的攻击，但每个攻击包含更少的电子邮件。对于鱼叉式钓鱼，（参见侧栏）可能只有一封电子邮件。
- 提供的统计信息没有考虑包含恶意软件附件或恶意软件链接，而且邮件文本与目标品牌不相关的垃圾邮件，即使恶意软件针对的是您的银行凭据也是如此。

因此，有许多因素可能导致不同的网络钓鱼统计数据。

考虑到前面提到的各个方面，下面的统计数据包含了这种“类似网络钓鱼的”垃圾邮件。度量和分析犯罪分子正在滥用哪些类型的品牌来让用户单击其恶意链接很有趣。这些欺诈性电子邮件一般可归类为“诈骗”。

鱼叉式钓鱼

鱼叉式钓鱼是一种个性化的网络钓鱼。首先，钓鱼者通过应用社会工程收集许多类型的个人数据。在第二步中，将此数据用于编写一条发送给受害者的个人消息。这种个性化的内容可让受害者确信消息是合法的，因此他会掉入陷阱。有关更多信息，请参阅http：//en.wikipedia.org/wiki/ Spear_phishing#phishing_techniques。

电子邮件诈骗和网络钓鱼的最新趋势

在我们考虑前面提到的方法时，我们看到传统电子邮件钓鱼在显著减少，尤其是在2010年。但在2011年下半年，使用可信品牌的名称让用户单击所提供的链接，这种趋势导致这些类似网络钓鱼的电子邮件或诈骗活动显著增多了。

诈骗/网络钓鱼量随时间的变化趋势
2008年第2季度到2011年第4季度

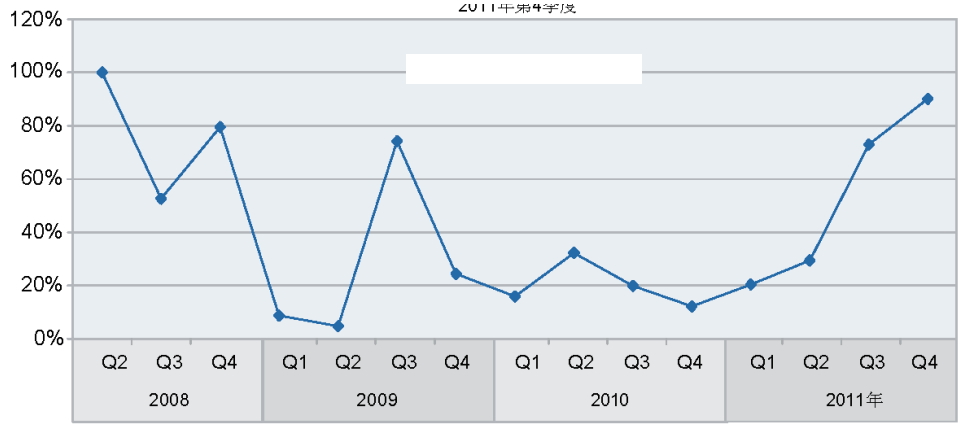


图25: 诈骗/网络钓鱼量随时间的变化趋势 - 2008年第2季度到2011年第4季度

下图显示了发出类似网络钓鱼的电子邮件的国家[15]。

网络钓鱼发出者的地理分布
2011年

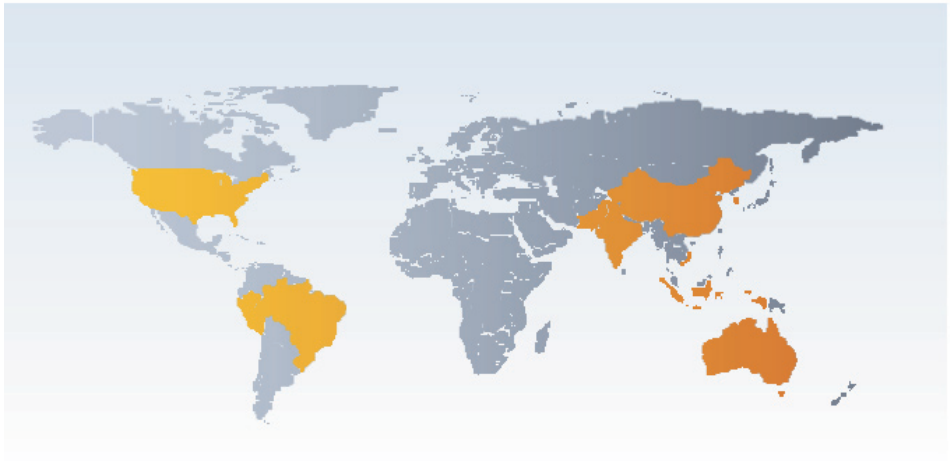


图26: 网络钓鱼发出者的地理分布 - 2011年

国家	钓鱼数量的%
印度尼西亚	15.1%
印度	10.7%
中国	6.9%
巴西	5.9%
越南	5.8%

国家	钓鱼数量的%
澳大利亚	5.0%
韩国	4.5%
美国	4.4%
秘鲁	3.8%
巴基斯坦	2.6%

表2: 10大诈骗/网络钓鱼源头国家—2011年

15 源头国家表示发出诈骗/钓鱼电子邮件的服务器所在的位置。X-Force认为大部分诈骗/钓鱼电子邮件是由僵尸网络发出的。因为可从任何地方控制僵尸网络，所以诈骗/钓鱼电子邮件背后的实际攻击者的国籍可能与诈骗/钓鱼电子邮件的源头国家不同。

本节开头介绍的电子邮件网络钓鱼/诈骗的变化也可在目标行业中反映出来。[16]

- 直到2009年，针对金融机构的传统电子邮件钓鱼仍占据主导地位，占所有钓鱼电子邮件的50%以上。它们在2010年到2011年秋季开始失去地盘，但到2011年末又恢复到了大约15%。
- 在线商店是2010年中期最受欢迎的目标，但在2011年可谓微不足道。
- 包裹服务在2010年第2阶段被广泛用于欺骗用户，它们在此阶段达到了所有诈骗/网络钓鱼式电子邮件中的大约20%。在2011年第二季度，超过50%的此类垃圾邮件使用了著名包裹服务的名称。这种攻击类型到2011年末几近消失。
- 从2010年开始（我们开始监视此类电子邮件时），社交网络在统计上占据主导地位，它始终位居前两名。在2011年年初，超过80%的著名合法品牌将电子邮件赌注压在社交网络上，在2011年第二季度稳定在43%。

不同行业的诈骗/网络钓鱼目标
2009年到2011年

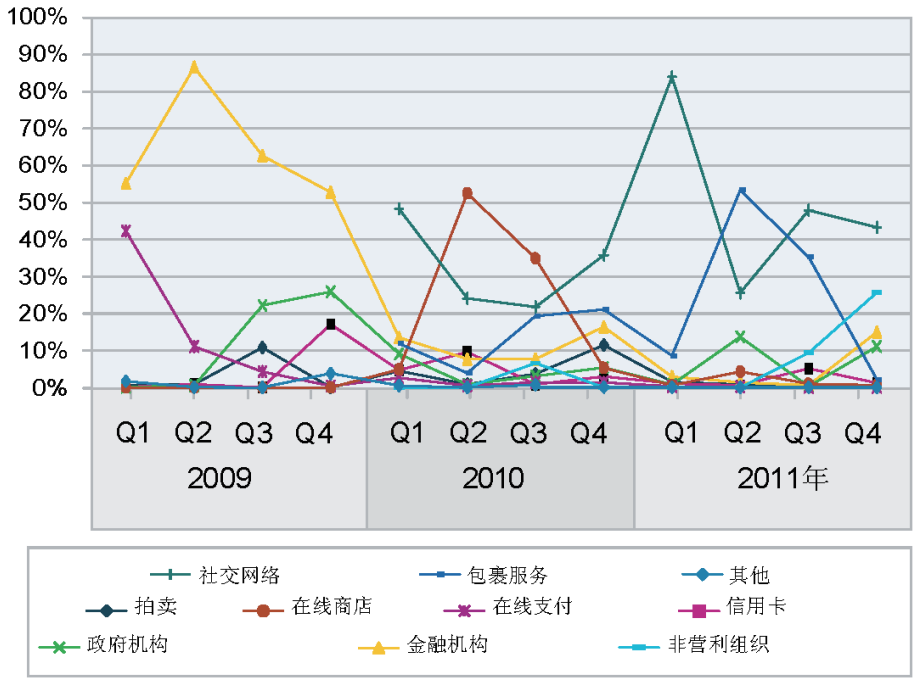


图27: 不同行业的诈骗/网络钓鱼目标 - 2009年到2011年[17]

16 在以前的趋势和风险报告中，得到的数值明显不同，因为它们没有并入社交网络、包裹服务和非营利组织。而且，“仅”误用品牌的名称而没有执行真实和传统的网络钓鱼的电子邮件未被考虑在内。

17 有关社交网络、包裹服务和非营利组织的数字从2010年初才开始记录。

垃圾邮件的演化

多年来，我们看到了在以前IBM X-Force趋势和风险报告中讨论的许多垃圾邮件趋势和类型。我们认为回头看看垃圾邮件随时间变化的方式应该很有趣。

垃圾邮件的演化
从2005年到2011年的趋势

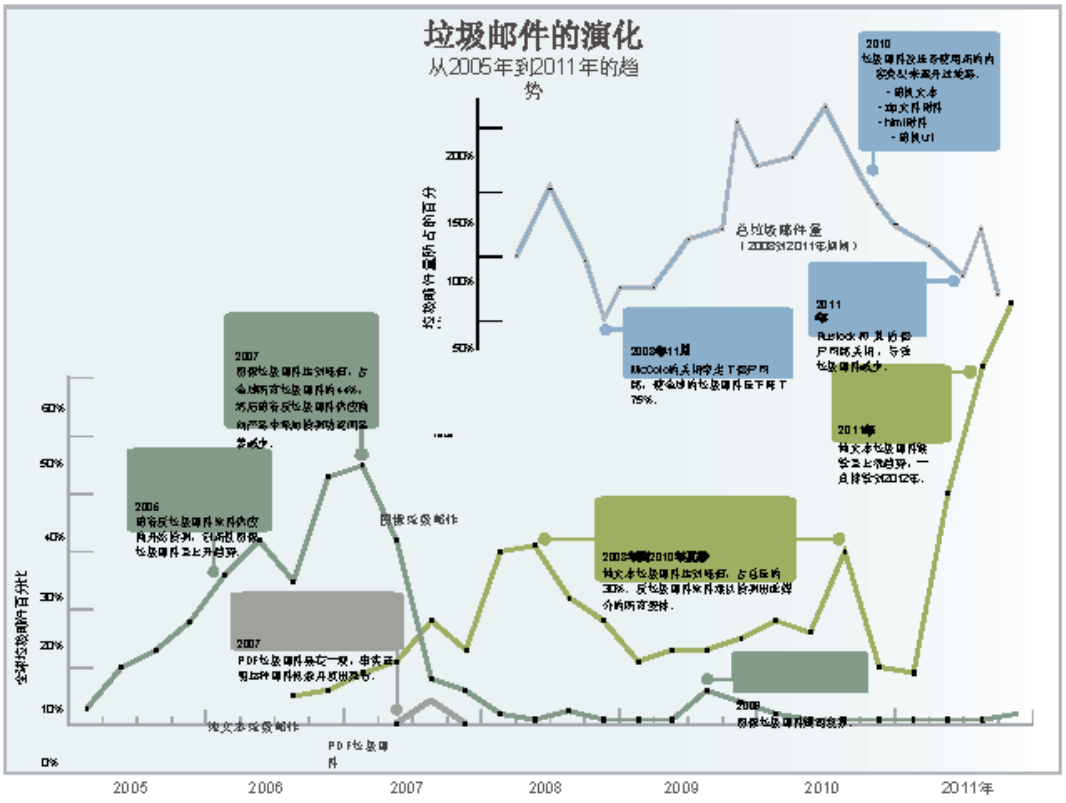


图28: 垃圾邮件的演化 – 2005到2011年的趋势

2005到2006年 — 图像垃圾邮件

在2005年，垃圾邮件发送者开始大量使用基于图像的垃圾邮件。到2005年末，所有垃圾邮件中近20%的是基于图像的，到2007年初达到了历史上的最高点 – 超过44%。随后显著减少。这是为什么？

最初，垃圾邮件发送者取得了不错的成果，因为当时大部分反垃圾邮件供应商没有预料到这种垃圾邮件，并且可能甚至认为附加的图像是合法电子邮件的迹象。但在基于图像的垃圾邮件出现两年后，甚至最落后的反垃圾邮件供应商都调整了其检测方法，以包含这种垃圾邮件类型。因为这种垃圾邮件类型预定义了垃圾邮件的许多特征，所以很容易检查可疑的模式，所以从2007年初开始，几乎所有这种类型的垃圾邮件都被可靠地拦截了。

2007年 — PDF垃圾邮件

在2007年春季和初夏基于图像的垃圾邮件显著减少后，使用PDF附件的垃圾邮件开始取而代之。在2007年8月，大量的PDF垃圾邮件占我们看到的所有垃圾邮件的近20%（在某些天）。可以在Frequency-X博客中看到有关这些PDF垃圾邮件线索的更多细节。

PDF垃圾邮件很短命。或许垃圾邮件发送者尝试过重复他们在基于图像的垃圾邮件上最初的“成功”，希望反垃圾邮件供应商没有准备好应对这种类型的附件。但其实不然，垃圾邮件发送者迅速放弃了这种方法。

MP3垃圾邮件甚至比PDF垃圾邮件还要短命。我们看到此技术在10月份出现，而它仅存在了几天。这种邮件的数量也比整个夏季PDF垃圾邮件的活动少得多。有趣的是，MP3垃圾邮件源代码非常类似于PDF垃圾邮件。有关MP3垃圾邮件的详细信息可在Frequency-X博客中找到。

2008年 — McColo关闭导致垃圾邮件第一次大幅减少

在2008年第一季度，纯文本垃圾邮件（不含HTML代码）所占的百分比显著增加。使用纯文本编写的垃圾邮件首次达到了30%的比例。在2010年夏季经历类似的峰值后，这种类型的垃圾邮件在2011年末创下了历史新高 –占据了超过70%的垃圾邮件。纯文本形式的垃圾邮件甚至更难检测，因为没有固定的特征，如暗示可建立哪些模式的异常HTML代码片段或特殊类型的附件。但是，合法电子邮件中的趋势正好相反。如今，不使用HTML的消息或时事通讯类型变得更少了。简单的纯文本垃圾邮件作为电子邮件特征，已变得更加可疑，并且有一天可能会被用作拦截标准。

但2008年对垃圾邮件发展的巨大打击是11月11日McColo的关闭。这一天，全球的垃圾邮件量下降了

惊人的75%! 或许更有趣的是，我们在垃圾邮件的起源国（一般而言，垃圾邮件将使网络所在的国家）中注意到了显著的变化。尽管McColo在美国境外运行，但在它关闭后突然且极端的数量和国家分布变化表明，McColo就是全球垃圾邮件僵尸网络的基本操纵者。多年来，美国一直在垃圾邮件起源国列表中位居第一。在关闭6天前，它仍然是第一名。

关闭6天后，美国的垃圾邮件量减少到了其原始容量的14%。所以，美国最终失去列表中的榜首位置就不足为奇了。

2009年 — 垃圾邮件量第一次达到顶峰

在3月，垃圾邮件发送者再次发起使用基于图像的垃圾邮件的多种威胁。从技术上讲，他们使用的方法中没有新技术，所以大部分反垃圾邮件过滤器肯定都能识别和拦截它们。但这些新垃圾邮件中附加的图像的内容有所不同。在2007年，大多数基于图像的垃圾邮件都以股票交易为重点。在金融危机发生后，关注的重点转向了利润更高的药品。有关重生的图像垃圾邮件的更多信息可在Frequency-X博客中找到。

那么，为什么垃圾邮件发送者会依靠一种过去的技术？尤其是在它的成功依赖于用户在浏览器中实际键入该URL（他在图像中只能看到URL，而不能单击该URL）时。一个答案可能是，在2009年，垃圾邮件发送者显著增加了垃圾邮件的总量。在这种意义上，图像垃圾邮件可能是全力进攻战略的一部分。

到2009年11月，也就是McColo关闭一年后，全球垃圾邮件总量达到了第一个峰值。

发送垃圾邮件最多的5个国家 在McColo关闭之前	
美国	14.2%
俄罗斯	11.0%
土耳其	7.4%
西班牙	5.9%
巴西	4.8%

发送垃圾邮件最多的5个国家 在McColo关闭之前	
中国	12.7%
俄罗斯	11.4%
美国	8.0%
韩国	6.2%
巴西	5.8%

发送垃圾邮件最多的5个国家 2008年末	
巴西	11.7%
美国	8.1%
中国	6.6%
土耳其	5.7%
俄罗斯	5.7%

表3：在McColo关闭前后发送垃圾邮件最多的国家

2010年 — 垃圾邮件量第一次长期减少，但包括HTML附件在内的垃圾邮件内容发生了重大且快速的变化

与之前的所有年份相反，这是我们第一年没有看到垃圾邮件水平出现显著增长。相反，我们看到了比之前所有年份更多的内容变化。2010年看到的示例包括：

- 结合随机文本与随机URL的垃圾邮件，显著增加了垃圾邮件的平均大小。
- 在2010年8月初，垃圾邮件发送者开始发送包含ZIP附件的垃圾邮件威胁。X-Force分析了这些消息，每个ZIP文件都包含一个恶意的EXE文件。有关包含ZIP附件的垃圾邮件威胁的更多细节可在Frequency-X博客中找到。
- 仅在一年内就看到垃圾邮件内容的多样化，这可能暗示垃圾邮件发送者更多关注“质量”，而不再是数量。数量不再是设法通过垃圾邮件过滤器的解决方案。

2011年 — 垃圾邮件的另一次减少，主要由Rustock关闭引起

3月16日，激动人心的是Rustock僵尸网络关闭后垃圾邮件量减少了一半。我们在以前的IBM X-Force年中趋势和风险报告内讨论了这次关闭的细节。与2008年11月的McColo关闭相反，我们没有看到垃圾邮件水平的迅速恢复。但是，垃圾邮件发送者并没有松懈，他们通过发送新的威胁来改变让垃圾邮件通过过滤器的方法：

- 夏季和秋季的恶意软件ZIP垃圾邮件
- 12月的图像垃圾邮件

这两种方法都已在前面的章节中详细讨论过。

长期垃圾邮件趋势 – 起源国

- 印度是唯一出现持续增长的国家
- 巴西是2009年McColo关闭的最大受益者，从那以后开始减少
- 俄罗斯受到了McColo关闭的巨大影响，但从2009年开始增长
- 印度尼西亚是2011年的新来者，是2011年3月Rustock关闭的最大受益者
- 美国有史以来第一次下降到4%以下，

主要原因是Rustock的关闭

- 韩国稳定在4%
- 法国、西班牙和土耳其失去了他们前几年的主导地位。

长期垃圾邮件趋势 – 没有改变

除了前面介绍的所有变化，一些基本点没有改变：

- 我们继续看到垃圾邮件在充分利用经典的主题，如假冒的手表、医疗产品和软件。这似乎是非法牟利的一种经过检验的方法。
- 仍然存在让用户单击所提供链接的垃圾邮件（特别是网络钓鱼）。但垃圾邮件发送者将垃圾邮件中提供的文本内容与用户单击该链接时发生的事情分离开。这催生了：

  – 尝试销售前面所提及产品的完美的网络钓鱼式垃圾邮件。

  – 通过提示用户单击链接获得更多细节，然后感染用户的计算机，从而利用时事新闻或其他热门主题的垃圾邮件。

  – 不包含文本而仅包含一个链接的大量垃圾邮件。

- 速度加快。垃圾邮件发送者迅速调整他们的方法，试图赶在拦截它的最佳方法出现之前取得成功。大量使用图像垃圾邮件持续了2年以上（2005到2007年），而在2011年中看到的不同垃圾邮件阶段持续了10到14星期。尽管如此，发送垃圾邮件的国家方面的变化要慢得多。对比而言，僵尸网络仍然在缓慢增长。查看垃圾邮件发送者是否能够在未来加速他们的僵尸网络获得过程，这会很有趣。
- 从2008年开始，垃圾邮件的平均大小返回到3KB。我们可以将这视为一种标准垃圾邮件大小。
- 垃圾邮件发送者始终在尝试新方法。请查看下一部分，了解有关可能发生的情形的一些观点。

垃圾邮件的未来前景

在2011年上半年，我们看到垃圾邮件量显著下降，没有过去的快速反弹特征。传统垃圾电子邮件的业务环境已经改变。

- 组织或公司成功地关闭了僵尸网络或发送垃圾邮件所需的基础设施，这从McColo或Rustock的关闭中可以看到。（我们在年中详细讨论了这些关闭事件。）
- 垃圾邮件过滤器继续改进。
- 出现了其他使垃圾邮件发送者的工作陷入瘫痪的方法，如“单击轨迹：垃圾邮件价值链的端到端分析。”[18] 研究表明，依靠垃圾邮件推广的产品中，95%的支付仅由3种银行处理。垃圾邮件受害者所用的银行可以拦截对这3种银行的支付。

这可能让犯罪分子关注其他区域，如社交网络内的垃圾邮件或执行分布式拒绝服务(DDoS)攻击。甚至还有经验丰富的垃圾邮件发送者认为垃圾邮件业务已失去吸引力。[19]另一方面，可能有些方面误导了旧的和新的攻击者发送更多的垃圾邮件。

- Internet用户数量仍在增长。因此，始终有新的垃圾邮件和网络钓鱼攻击受害者，即使1万封垃圾邮件中只有一封到达收件箱也是如此。
- 可用机器的数量仍在增长。而且，现在可以感染一种新的机器类型：智能电话。而且从垃圾邮件发送者的角度讲，这些手持计算机有另一个优势：它们始终在线，而不像桌面PC那样在不使用时关闭。如今我们在智能电话环境中仍然有带宽限制，因为大部分用户没有统一的移动Internet费率。这在未来可能会发生改变。请参阅“移动恶意软件视角”一节了解详细信息。
- 对于垃圾邮件内容的类型，仍然有一些方法未被垃圾邮件发送者所使用，如使用Open Office文档作为垃圾邮件附件。
- 垃圾邮件发送者可使用许多著名的品牌名称作为垃圾邮件的伪装发送者，让用户单击所提供的链接。
- IPv6也可能为垃圾邮件发送者提供新方法来烦扰用户和干扰反垃圾邮件供应商，尤其是在垃圾邮件发送者专门将精力集中在IP拦截上时。

18 http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf

19 http://www.itworld.com/security/178991/internet-evolves-there-place-spam

第II部分

操作安全实践

在趋势报告的这一节中，我们探讨的主题围绕如今的威胁所针对的流程、软件和基础设施中的缺陷。我们将探讨安全合规性最佳实践，降低操作成本的各种想法，自动化，更低的拥有成本，以及任务、产品和角色的合并。我们还将介绍在管理和减轻这些问题期间在整个IBM 跟踪的数据。

安全智能简介：一种一体化的实时安全保护方法

在过去几年，攻击的增多、计算模型（以及由此带来的攻击面）的扩大，以及数据的爆炸式增长为安全从业者带来了重大的挑战。组织正在防御比以往更多，而且更加多样化的威胁。

甚至确定已发生了一次安全违规也存在困难，这让许多在几个月内都对严重的损害一无所知。他们常常拥有原始的数据，但缺乏检测安全违规的可视性和分析。据2011年Verizon数据违规调查报告总结，在69%的数据违规情况中，组织的日志文件中都存在良好的违规证据，但由于数据过多，这些证据很少被找到。

因此，如今的威胁检测取决于两个要素：识别数十亿个数据点中的恶意活动，将庞大的可疑事故集细化到重要的事故。对于这两个任务，组织需要各种方法来1)分析所有相关数据，2)智能地识别噪音中的信号，以及3)以实用的方式提供该智能。

这导致一类称为“安全智能”的新解决方案的开发，这些解决方案在整个安全操作范围内提供了统一的可视性和实时分析。

认识到新的事实后，IBM向推动安全智能和分析的未来发展跨出了勇敢的一步。致力于通过一个Security Systems部门统一各个信息安全学科，并收购Q1 Labs（SIEM[安全信息和事件管理]和安全智能领域的领导者），IBM从正面应对这个问题。

定义安全智能

我们首先看看安全智能的定义：

安全智能 （SI)是对用户、应用和基础设施收集的，可影响企业IT安全和风险状态的数据的实时收集、规范化和分析。安全智能的目标是提供可操作且全面的洞察，减少任何规模组织的风险和操作工作。

安全智能解决方案收集和加入仓库的数据包含日志、事件、网络流、用户身份和活动、资产配置文件和位置、漏洞、资产配置，以及外部威胁数据。安全智能提供了分析来回答涵盖了风险和威胁管理时间线之前/期间/之后的各种根本性问题。

安全智能提供了组织安全和风险状态的一个统一视图，涵盖4个主要的风险领域：人员、数据、应用和基础设施。

熟悉SIEM和日志管理产品的人可能将安全智能视为这些技术旅程中的下一个逻辑步骤。加上代码攻击前的功能，更广泛的数据采集，以及更深入的智能，安全智能扩展了

SIEM和日志管理。它可实现更好的威胁（包括内部和外部）预防、检测和优先化，自动化了合规性监视和报告工作。

安全智能还可提供安全事故的广泛可视性。例如，通过深入的包检查来分析网络流，以及监视用户活动中的异常，安全智能可帮助您识别员工的操作何时看起来可疑，

建议可能的内部数据盗贼或外部对帐户的损害。而且，通过将IPS警报与漏洞扫描结果和网络拓扑结构知识相结合，安全智能可帮助您识别哪些入侵尝试正在攻击存在漏洞的资产以及可以忽略哪些攻击。

与商业智能的类比

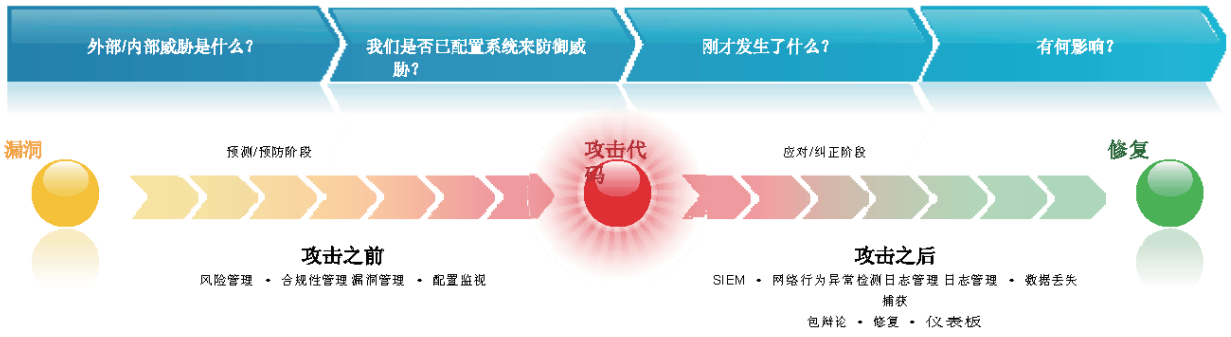
查看商业智能(BI)与安全智能之间的类似性大有裨益。BI会合成大量业务信息来收集实用的业务洞察：

哪些产品销量较好，在哪个客户领域？

哪些地区对最近的一次促销反响最强烈？

为什么我的一个产品线的利润在增长，但另一个在下降？

安全智能时间线



类似地，安全智能(SI)合成大量安全信息，以获得IT和业务线相关性的实用安全洞察：

我们最可能容易受到哪些类型的攻击？（我们应如何调整安全实践和控制方法？）

哪些业务合作伙伴和供应商可能为我们带来最大的安全风险？（我们应调整他们的访问权限还是在他们一端需要更强的控制？）

我们是否正看到来自移动计算的任何新安全或合规性风险？（如果是，我们应关注哪些风险？）

SI与BI之间的一个区别是，安全智能提供了实时的洞察和监视，而商业智能通常反映了时间点信息。二者都是宝贵的管理工具，但在安全与合规性世界中，最新的信息至关重要。

商业智能已成为业务规划和执行可视性的标准工具。类似地，安全智能正变成安全规划和执行可视性的标准工具。而且，它可用作IT与业务线之间进行安全对话的事实基础，以帮助您评估业务实践和产品的风险/回报因素。

安全智能原则

安全智能的3个原则（智能、整合和自动化）有助于让用户更快地提高效率。

以下是这个3个原则的一些实际示例：

1. 智能：理解大量安全与合规性相关数据的能力。这意味着在大数据级别存储、关联、报告和查询广泛的信息（安全信息"是"大数据） - 以提供实用的洞察。

2. 整合：智能的基础，支持对不同数据进行一致的规范化分析。通过收集和组合安全相关数据（在类型和数据量上），您可将一个安全事件的有限二维视图扩展为一个受上下文支持的三维富视图。

– 示例：安全智能解决方案提供的开箱即用整合功能对安全分析师的生产力产生了巨大的影响。对来自数百个来源的数据进行规范化有助于防止客户（和顾问）必须成为每个供应商的数据模式专家。例如，一项合规性指令可能要求记录各种身份验证事件（失败的登录、成功的登录、成功登录后进行特权升级等）。借助 SI，组织可以不再跨数十个资产（每个具有自己的数据模式）手动跟踪该事件。

3. 自动化：通过消除不必要的复杂性并降低总体拥有成本(TCO)，推动实现让安全智能进入现代化的元素。这包括使用更多数据（如网络流）任务自动化和为每个应用封装的知识产权。

安全智能与SIEM有何不同?

安全智能通过多种有意义的方式超越了第一代SIEM技术：

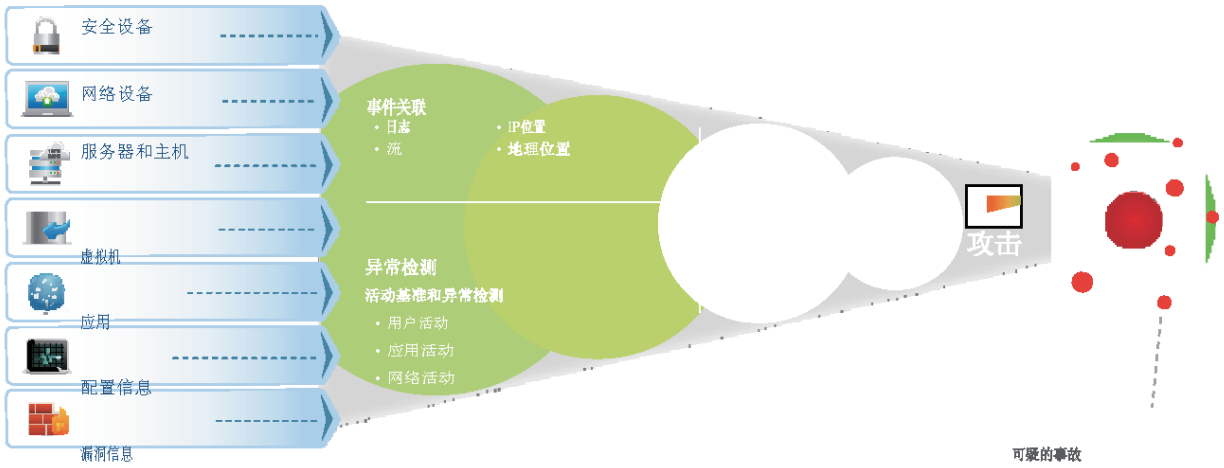
网络活动监视和流分析。过去，来自设备、应用、服务器和基础设施服务的日志可让您大体了解所发生的事情。如今，日志只是一个起点。网络流收集、深度入的数据包检查和数据包（内容）捕获是3维上下文和可视性所必需的。安全智能使用流分析来帮助提供用户行为、社交媒体使用、移动活动、云活动等的实时洞察。

该转换使用了端口80的Web流量还是隐藏的僵尸网络IRC通信?

入侵者是否使用了一个已被攻陷的员工

帐户来盗取敏感数据?

员工是否不当地访问敏感的知识产权?



向最广泛的数据应用高级分析

数据包级别的可视性（来自网络活动监视[内容捕获]与SIEM的整合）可提供此类洞察。

预测分析和代码攻击前感知。安全智能整合了攻击前配置和漏洞管理功能。这让组织能够识别、优先化并系统地解决错误配置的设备（如防火墙）和未修补的漏洞所带来的风险。

异常检测。许多传统安全解决方案专注于保护组织远离已知的威胁，如已曝光的漏洞和常见恶意软件。在如今的安全环境中，人们更加渴望检测复杂的、有针对性的攻击，这些攻击可能采用全新的攻击方法。此外，内部威胁常常只能通过分析已授权的行为来检测。以异常为中心的方法可发现这些类型的活动。

更容易部署和安置。第一款SIEM产品发布时，早期采用者愿意花大量时间和资金将它们部署到生产环境中。需要编写连接器和规则，需要培训用户等。部署到生产环境中后，它们的安置需求也可能很高，因为很高的“误报”警告率需要进行调查。安全智能解决方案现在使用更广泛的信息（事件、流、资产配置文件、网络拓扑、漏洞等）和更高的自动化水平，帮助您实现重大的数据精简和减少安置需求。

有哪些主要优势？

让我们看看组织从其SI部署中获得的收益：

更好的合规性

安全智能通过记录和主动监视整个企业的各种信息来为合规性活动提供帮助 – 哪些用户在访问高价值系统（是否适当）；是否有任何敏感信息未加密即在开放网络上传送；防火墙的配置是否合适等。SI也可通过自动化的报告和轻松的日志搜索和流来提高操作效率 – 在某些情况下，会节省数千个工时。

更快的威胁检测和修复

在后边界世界里，仅专注于预防或检测/修复的方法正失去地盘。组织需要同时执行二者。由于移动计算、社交媒体和云计算的存在，边界可能被他人渗透，导致Forrester Research所称的“零信任”环境。安全智能解决了这一问题，帮助企业更快地检测和修复破坏，还帮助企业从一开始就防御它们（参阅下面的“代码攻击前风险减少”）。通过实时关联大量数据，SI可帮助在大量的信息中查找有用的数据 – 分析来自网络和安全设备、服务器、应用、目录服务器的事件；网络活动流（借助数据包捕获）；资产信息；配置数据和漏洞信息。安全智能也可加速修复，帮助识别哪些资产和用户可能受到一次损害的影响，并利用内容捕获进行司法研究。

例如，Conficker蠕虫在2008年晚期开始扩散时，导致了Internet上TCP端口445的流量显著增加。安全智能系统将这种流量增加视为恶意的，甚至在安全研究者给Conficker命名之前就是如此。这种类型的抢先检测可帮助保护计算机网络远离高级威胁和零日威胁等可能没有特征或补丁的威胁。

内部欺诈、盗窃和数据泄漏的减少

外部攻击占据了大部分的重大新闻，但内部威胁可能危害更大 – 损害宝贵的知识产权，甚至危害国家安全。安全智能让组织能够识别和减轻这些类型的威胁，帮助检测：

- 未授权的应用访问或使用
- 数据丢失，如将数据传输到未授权或不熟悉的目的地
- 用户访问问题，如特权访问例外
- 应用性能问题，如服务丢失或过度使用

代码攻击前风险减少

安全智能根据基本的预防工具来构建，如防火墙和IPS设备，它提供的新关联可帮助组织预防各种攻击：

- 自动监视设备配置（如防火墙）并提醒安全空白和策略违规情况
- 根据网络拓扑和资产价值，确定VA（漏洞评估）扫描器发现的漏洞的优先级
- 预测性威胁建模和网络更改模拟

安全智能解决方案可向比以往更广泛的输入内容应用更先进的智能。举例而言，基于内容捕获的网络活动流可提供比配置数据本身更加可靠的的安全设备规则有效性视图。正如在一篇最新的博客帖

子中所发现的，“[单单配置数据可能]会错过这样一些情形，其中一种配置被视为足够了，但出于某种原因仍然允许潜在的有风险网络流量进行传播。”类似地，网络拓扑的知识可“最大限度减少漏洞扫描器中常见的误报，而且……得益于配置网络的方式，可轻松曝光[优先级较高的漏洞]。”

简化的操作和工作减少

SI解决方案正在应用智能自动化来简化安全操作，减少安全和网络专业人员的负担。这可能带来重大的成本节省。这些收益源于更高的效率和消除了单调的手动任务。

安全智能最佳实践

打造安全智能能力时，一些组织方法和技术能力可提高成功的机会。以下是一些优先考虑的方法：

定义事故升级策略。可将安全智能解决方案视为一个内部云服务，为防火墙管理、系统管理和网络管理等小组服务。就像公共云服务一样，SI解决方案的提供者（通常是安全和风险管理小组）应与解决方案的使用者定义一个合同，以控制安全事故的处理和升级。迅速向高层管理人员报告问题可能不是最佳的方法，也可能损害与用户的关系，导致他们在未来拒绝提供数据。

定义关键用例和报告初始部署。组织应决定它的监视和报告工作最初关注哪些主题。常见的类别包括一般外部威胁（如僵尸网络和来自黑暗网络的流量）、特定于行业的风险、内部威胁、策略违规和特权用户活动。

智能的异常检测。为了检测异常行为，该解决方案应跨多个兴趣维度（用户、应用和网络），根据所观察的行为来生成活动基准，然后识别位于正常范围之外的异常。可自动了解基准更改情况的动态基准方法可减少后续的手动工作。

基于深入数据包检测的流分析。如前所述，具有数据包捕获的流分析可提供安全和合规性风险的深入可视性。它可通过识别错误的网络配置来增强防御，通过数据包级洞察来增强检测，通过显示在一些用例中哪些人访问了哪些数据来改进司法调查。

预测分析。寻求更加主动的安全状态的组织也应确定一些功能的优先级，如设备配置监视、合规性策略监视和漏洞优先级。

小结

总体来讲，安全智能是企业安全性的一个强大推动力，可帮助企业通过实时洞察和深入的辩论来实现实用信息的合规性。它可通过更深入的智能、整合和自动化（这些领域在过去拥有大量的安全解决方案）向IT和业务线提供重大的收益。您可以为各种规模的组织合理地实现和管理安全智能解决方案，可为真实的需求带来实用的解决方案。

参考资料：

1. http：//www.verizonbusiness.com/resources/reports/rp_data-breach-investigations- report-2011_en_xg.pdf

2. http：//blog.q1labs.com/2011/07/28/defining- security-intelligence/

3. http：//blog.q1labs.com/2010/08/26/do-we-need-a-security-analog-for-business-intelligence- absolutely-we-do/

4. http：//q1labs.com/resource-center/white-papers/details.aspx?id=113

5. http：//blog.q1labs.com/2011年/10/20/three-ways- to-embrace-the-zero-trust-environment/

6. http：//q1labs.com/resource-center/case-studies/details.aspx?id=114

7. http：//blog.q1labs.com/2011/06/16/latest- gartner-report-shines-bright-light-on-qradar-risk- manager/

8. http：//q1labs.com/resource-center/white-papers/details.aspx?id=113

9. http：//blog.q1labs.com/2010/09/17/siem-is-a- security-intelligence-cloud/

10. http：//q1labs.com/resource-center/brochures/details.aspx?id=129

2011年的漏洞曝光

从1997年开始，X-Force跟踪了软件产品中各种安全漏洞的公开曝光。我们的分析师关注了曝光各种漏洞、修复信息和攻击代码的公共邮件列表和网站，我们记录了公开报告的漏洞。

在2011年，我们报告了7000多个新的安全漏洞。尽管这与2010年相比显著减少了，但在看到比以往更多的漏洞时，会发现自2006年以来漏洞曝光率有一个持续两年的高低周期，而且每个高点和每个低点的水平都在升高。

我们第一次看到漏洞总量下降是在2007年，这引起了对为什么漏洞形势出现变化的大思考。但是，回想一下就会发现，这只是数据方面的偏差，总量一直在增长。如果过去6年的周期今年再次出现，2012年将是漏洞曝光率的另一个破纪录之年。

Web应用

2011年增长最少的安全漏洞类别是Web应用漏洞。在过去的几年中，曝光的安全漏洞中有大约一半是Web应用漏洞。但是，今年这一数字下降到了41%，

这是自2005年以来首次降到这一比例。这从图30中可以看出，其中显示了自2010年以来的Web应用漏洞数量。看看已曝光的Web应用漏洞类型会发现，SQL注入仍然是看到显著下降的一个重要类别。

漏洞曝光数量的年增长情况
1996-2011年

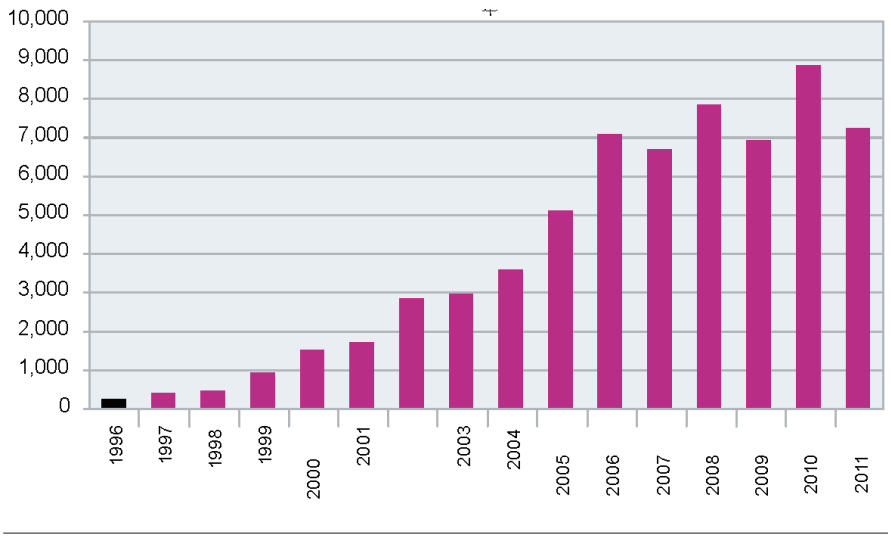


图29: 漏洞曝光数量的年增长情况 -1996-2011年

SQL注入漏洞特别重要，因为它们是IBM在其监视和帮助保护的全球数千个网络中看到的最常见的攻击类型。由具有财务动机的僵尸网络制造者发起的自动SQL注入攻击遮蔽了存在漏洞的网站的Web外观。这些网站可被JavaScript重定向器感染，将它们的访问者定向到恶意的攻击代码。SQL注入是在网络中搜索容易攻陷的目标的入门攻击者最喜爱的。SQL注入攻击也是更加老练的攻击者今年进行多项影响巨大的破坏方面的主要特征。

如果运行一个包含SQL注入漏洞的面向Internet的Web应用 – 它迟早会受到攻击。因此，修复这些漏洞很重要。我们看到数量上的下降可能意味着，Web应用的开发人员变得更聪明了，编写了漏洞更少的应用。如果是这样，这是一个积极的信号。但是，仍有大量工作需要做。

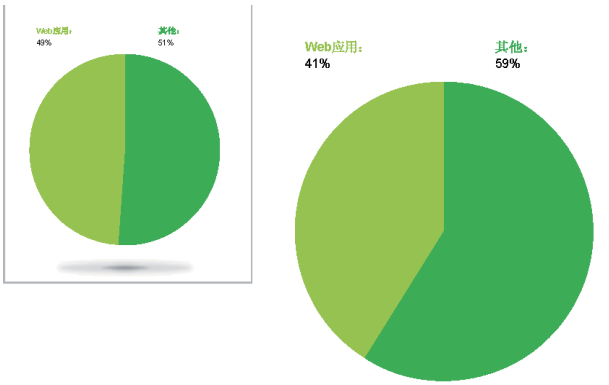


图30：Web应用漏洞2011年占所有曝光漏洞的百分比

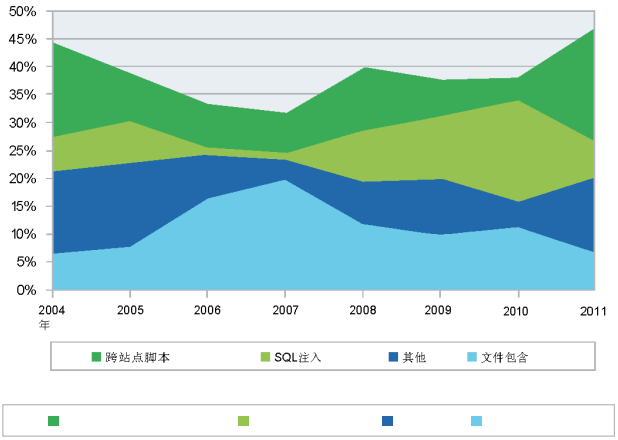


图31：按攻击技术划分的Web应用漏洞数量 - 2004-2011年

我们仍然看到2011年曝光了仅3000个Web应用漏洞，而且X-Force观察到的Web应用漏洞的总数只是开放的Internet上存在的漏洞的冰山一角。原因在于，X-Force仅跟踪了已曝光的漏洞。由公司或开源项目为第三方使用而维护的Web应用很容易被曝光漏洞。但是，大部分Web应用都是在内部开发或由私营公司开发来单独用于一个具体网站的自定义软件。这些自定义Web应用不容易被曝光漏洞 – 它们没有第三方用户，所以无需向公众告知其中的漏洞。

我们来自IBM AppScan OnDemand用户的数据提供了自定义Web应用状态的一些洞察，它也表明了一定程度的改进。但是，这一抽样可能是自行选择的 – 能足够聪明地与 IBM 一道改善其代码安全性的开发人员可能比普通开发人员更能从一开始就避免安全问题。因此，也可能Internet上Web应用的现状比我们的数据所表明的情况更糟。我们看到的攻击活动量无疑支持了这一结论。

一个容易曝光漏洞和受到大量攻击的Web应用类别是基于Web的内容管理系统(CMS)。我们查看了4个基于Web的内容管理系统，数据表明这些系统中最重要的不足源于它们支持的第三方插件生态系统。

Web应用平台和插件中曝光的漏洞
2011年

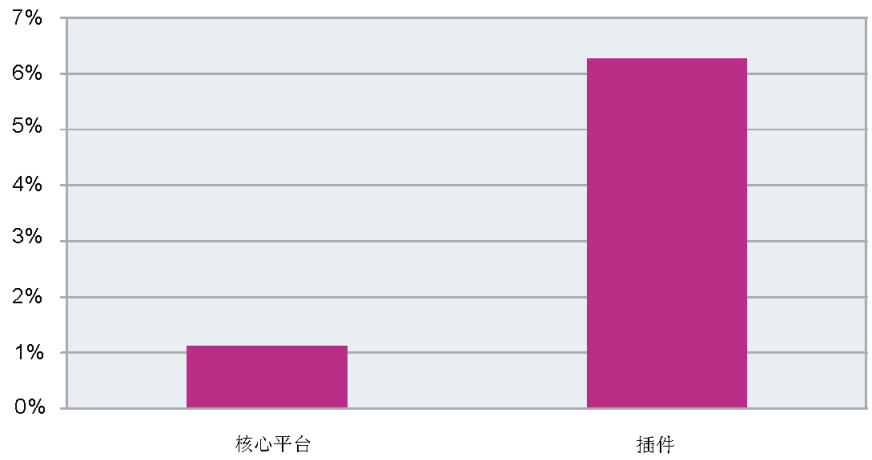


图32: Web应用平台和插件中曝光的漏洞 – 2011年

核心CMS平台中曝光的漏洞比其插件中曝光的漏洞要少得多，而且核心平台漏洞更可能拥有可用的补丁。此情形的部分原因在于，对各种插件开发人员带来的安全问题的支持和关注水平参差不齐。

Web CMS漏洞是攻击者最喜爱的目标，因为它们已曝光且影响着Internet上的大量网站。这些系统中的零日漏洞是今年受到大量攻击的一个因素。Web CMS软件的用户应注意评估其所用任何插件的维护者的安全实践。

他们应严密监视核心软件和插件的安全漏洞曝光，将修补它们作为优先事项。他们还应考虑使用应用层防火墙或入侵防御来进一步保护其网站。

2011年的CMS核心漏洞

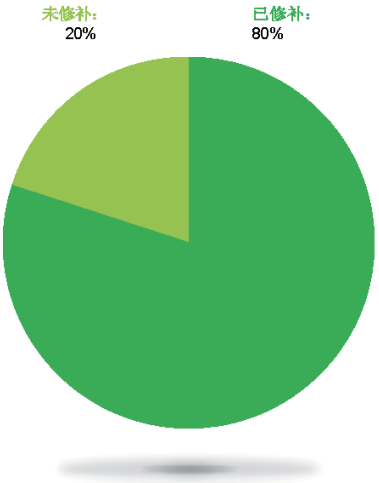


图33：核心内容管理系统中曝光的未修补与已修补的漏洞对比 – 2011年

2011年的CMS插件漏洞

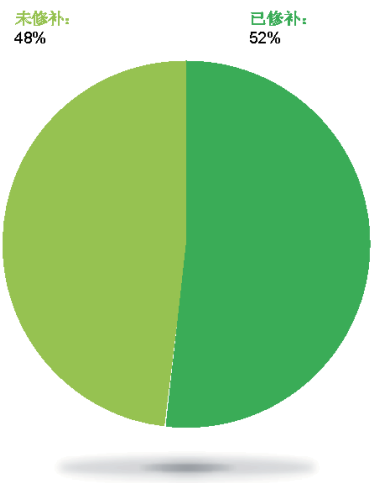


图34：插件内容管理系统中曝光的未修补与已修补的漏洞对比 – 2011年

攻击量下降

除了Web应用安全性的改进，乐观地讲还有另一个原因。在2011年，X-Force观察到公开发布的攻击代码量显著减少，达到了自2006年以来我们看到的最低值。这一数量在百分比和实际数量上都更低。在过去几年，具有已公开的攻击代码的漏洞百分比在15%上下波动，但在2011年，这一比例为11%。

这些降低反映了在过去几年已成为大量攻击的目标的具体区域。多年来，Web浏览器是路过式下载攻击的主要目标。尽管高危浏览器漏洞的数量在逐年上升，但公开的针对浏览器漏洞的攻击代码数量却比自2006年以来的任何一年都低。路过式下载攻击已转向针对第三方浏览器插件，而不是浏览器本身。

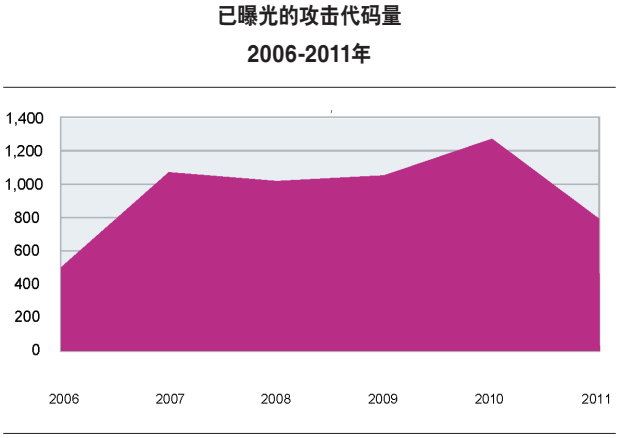


图35：已曝光的攻击代码量 – 2006-2011年

	2006	2007	2008	2009	2010	2011
已曝光的攻击代码	504	1078	1025	1059	1280	778
占总数的百分比	7.3%	16.5%	13.3%	15.6%	14.7%	11.0%

表4：已曝光的攻击代码量 – 2006-2011年

X-Force认为，这一进步是过去几年来对软件进行架构更改的结果，这些更改让攻击变得更困难。操作系统内存管理器现在包含各种检测内存损坏和安全停止执行任务的特性。许多浏览器和文档阅读器现在附带了执行沙盒，限制了成功的攻击代码的操作范围。结果，如果其他地方未被成功攻击，过去能迅速导致广泛传播攻击代码的漏洞现在需要几个月才能传播开来。

无可否认，漏洞的攻击如今不是不可能，尽管存在各种安全特性。X-Force Research发布了许多文章来描述在艰难的条件下获取代码执行权利的过程。在Blackhat USA 2012上，X-Force研究人员Mark Yason和Paul Sabanal发表了“在Reader X沙盒中播放”，探讨了恶意代码可能在沙盒应用环境中运行的方式。在2011年，Chris Valasek在Blackhat USA上发表了“理解低碎片化堆”，探讨了在受到高度防御的Windows堆中获取代码执行权的方法。

但是，这些文章中所描述的技术需要大量时间、工作和技能才能成功应用。我们今年在越来越多的情形中看到，在实验室环境中被攻击的关键漏洞未在现实中受到攻击。我们之前很少能这么说，而且它可能意味着我们正处在新的计算机安全时代的边缘。

已曝光的浏览器攻击代码量
2005-2011年

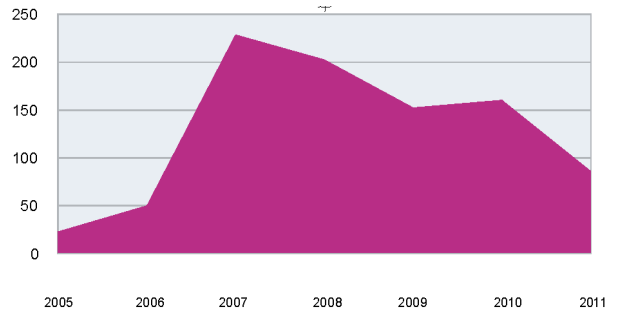


图36: 已曝光的浏览器攻击代码量 – 2005-2011年

高危Web浏览器漏洞量
2005-2011年

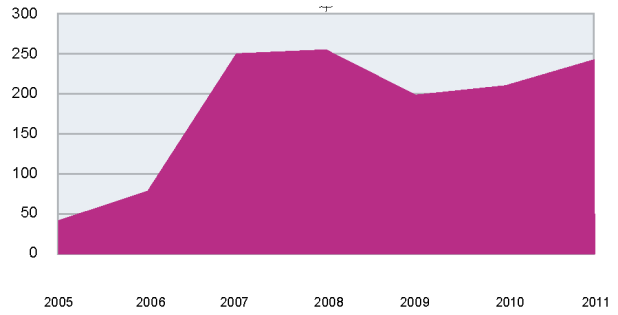


图37: 高危Web浏览器漏洞量 – 2005-2011年

影响文档格式问题的高危漏洞曝光数量
2005-2011年

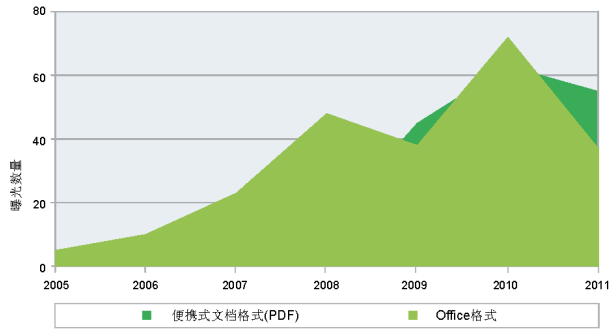


图38: 影响文档格式问题的高危漏洞曝光数量 – 2005-2011年

针对文档格式漏洞的攻击代码曝光数量
2005-20

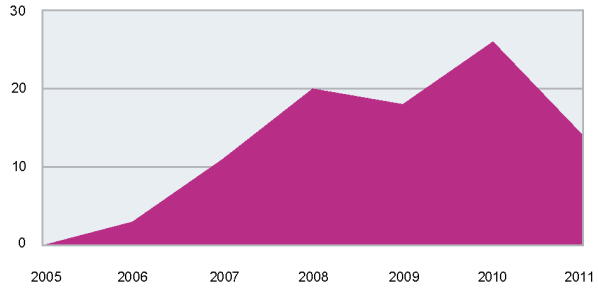


图39: 针对文档格式漏洞的攻击代码曝光数量 – 2005-2011年

影响多媒体软件的高危漏洞曝光数量
2005-2011年

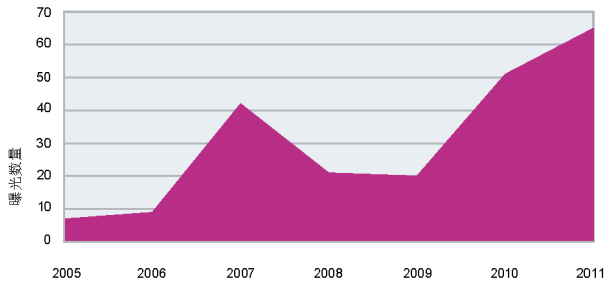


图40: 影响多媒体软件的高危漏洞曝光数量 –2005-2011年

针对多媒体漏洞的攻击代码曝光数量
2005-2011年

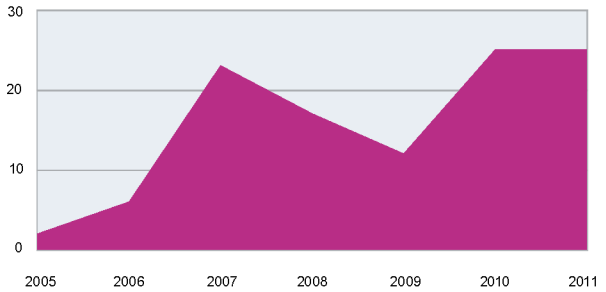


图41: 针对多媒体漏洞的攻击代码曝光数量 – 2005-2011年

攻击者将注意力转向新的关注区域

当然，仍然有重要的空白需要填补。我们继续看到多媒体播放器中曝光的漏洞数量在增长，在2011年看到的针对多媒体漏洞的攻击代码曝光数量与2010年相当。这仍然是攻击者关注的一个区域。

截至本文编写之时，今年早期曝光的多个关键多媒体漏洞仍在被与高级持续威胁相关的复杂、针对性攻击所使用。这些恶意文件可附加到电子邮件中，可与专为目标受害者精心设计的电子邮件文本一起发送给目标机器。至关重要的是，多媒体播放器在高度安全的环境中经过了严格修补或被完全禁用。

移动设备领域是值得重视的另一个区域。有许多移动操作系统漏洞被公开，有许多针对这些漏洞的攻击代码被公开释放。越狱或获得移动设备root权限的期望是导致人们在线发布移动攻击代码的一个动机。当然，该代码一旦可用，在针对未越狱电话的恶意用途中就可使用它。

移动操作系统漏洞总数
2006-2011年

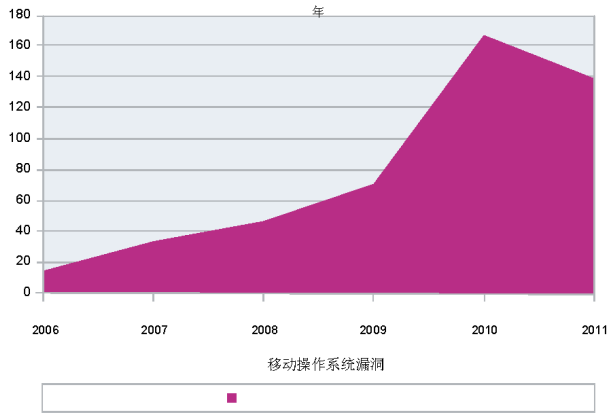


图42：移动操作系统漏洞总数 – 2006-2011年

移动操作系统攻击代码
2006-2011年

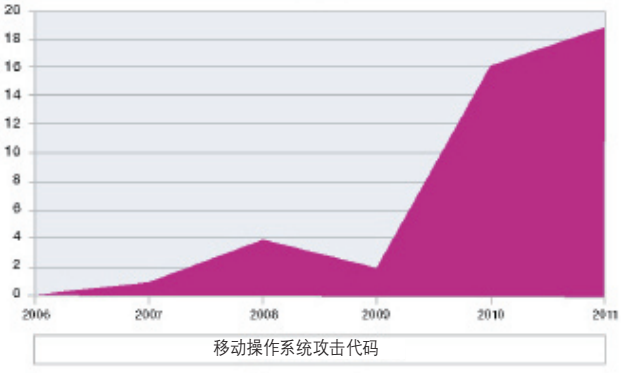


图43：移动操作系统攻击代码 – 2006-2011年

在2011年，我们看到针对移动设备的恶意活动在增多。一旦安装了已公开的越狱攻击代码，一些恶意应用会使用它来获取电话的提升特权。由于电话最终用户、电信公司和移动操作系统供应商之间的双层关系，电话上已曝光的移动漏洞可能在更长的时间内保持未修复状态，这为攻击者提供了较大的机会窗口。

不同的硬件平台以及制度需求的激增使这一情形更加恶化。如今的实际攻击活动量与针对传统工作站的活动量相比非常少，但我们预计攻击者对移动设备的兴趣在未来会直线上升。受感染的移动设备的大型僵尸网络已开始出现，而这仅仅是开始。

CVSS基础评分百分比
2011年

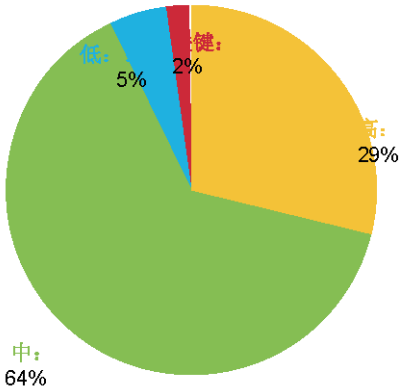


图44：CVSS基础评分百分比 – 2011年

我们看到2011年公开的关键漏洞数量与去年相比增加了70%。关键漏洞是在总分为10的通用漏洞评分系统(CVSS)中获得10分的漏洞。尽管这一增长让人担忧，但X-Force的观点是，该增长代表着一种数据偏差，我们预计这些类型的漏洞数量在2012年将逐渐趋于稳定。

“越狱”是一个允许您在设备上安装未经批准的第三方应用的过程。越狱常常涉及到使用特权提升攻击代码来获得基于UNIX式操作系统的电话的根访问权，因此有时也称为对设备执行“root”操作。获得根访问权后，可阻止安装未经批准的软件的安全控制机制可能被破坏。

CVSS评分	严重级别
10	关键
7.0-9.9	高
4.0-6.9	中
0.0-3.9	低

表5：CVSS评分和相应的严重级别

企业软件中的漏洞

一个重要的长期趋势是大型软件供应商曝光的漏洞所占的比例在不断增长。前10大曝光最多安全漏洞的软件供应商也是开发种类最丰富的企业软件大型供应商。真正的前10大供应商列表中还包括基于Web的内容管理系统的供应商，但我们在分析中排除了这些产品，以便将关注点放在流行的企业软件产品中各种漏洞的影响上。

这10大供应商曝光的漏洞总数所占的比例在不断增长，从2008年的19%增长到2011年的31%。我们不相信这只是软件行业整合的一项措施。

安全开发实践已成为软件开发生命周期中越来越重要的一部分，而且在过去几年中，负责任的供应商已采取措施改善其识别和消除代码中各种漏洞的能力。这些努力导致这些供应商的已曝光漏洞迅速增长，因为他们修复了所交付的代码并提供了补丁。

曝光漏洞数量最多的前10大软件供应商
2008–2011年

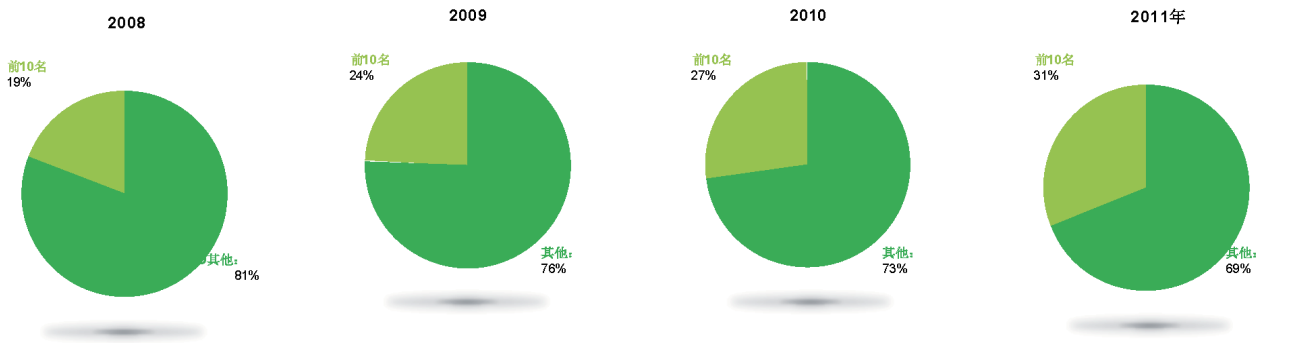


图45：曝光漏洞数量最多的前10大软件供应商 – 2008-2011年

最终，这成为了一个推动我们在今年看到的攻击代码公开数量减少的过程。但是在短期内，影响流行企业软件的漏洞数量的增长，以及关键漏洞的增长，意味着负责修补和保护生产计算机网络的IT人员还需要做比几年前多得多的工作才能应对这些漏洞曝光。来自前10大供应商真实漏洞数量自2008年以来增长了50%。在规划漏洞修复的人员安排时应考虑这一事实。

在被修复的漏洞中，大约91%是在曝光的同一天修复的，这是理想的情形。另外9%又如何呢？大多数在几周内修复，但最糟糕的情形可能延长到更长时间 – 有时从漏洞曝光到补丁发布会间隔数百天。甚至在将范围缩小到流行企业软件的供应商或具有公开攻击代码的漏洞时，这一情形仍然存在。X-Force在2011年仅发现29个案例中著名企业软件供应商修复具有公开攻击代码的已曝光漏洞的时间超过1周，但攻击者只需要一个这样的漏洞就能攻破一个计算机网络。

IT人员应采取什么步骤来保护网络远离已曝光的漏洞，这依赖于是否有可用的修复程序，以及多久才能用上修复程序。幸运的是，我们看到补丁的可用性有所改进。

今年，已公开的漏洞中只有36%未公开报告修复方法。这与前几年相比是一次重大的改善，前几年这一数字徘徊在45%左右。

CVSS评分	2006	2007	2008	2009	2010	2011
未修复漏洞所占的比例	46.6%	44.6%	51.9%	45.1%	43.3%	36.0%

表6: 公开报告的补丁所占的比例 – 2006-2011年

VSS评分修复时间表	所有	名供应商	著名供应商和 公开攻击代码
同日	4054	2263	138
第1周（第1到7天）	132	19	4
第2周（第8到14天）	55	15	5
第3周（第15到21天）	26	3	2
第4周（第22到28天）	27	10	2
第5周（第29到35天）	27	8	2
第6周（第36到42天）	33	7	1
第7周（第43到49天）	14	6	2
第8周（第50到56天）	9	2	1

表7: 所有软件供应商与著名软件供应商的补丁发布时间表对比 – 2011年 H1

这些空白不一定是供应商疏忽带来的后果。正确修复、封装和测试对商业软件应用的更新需要时间。在一些情形下，复杂的互操作性问题可能对不同的软件组件产生级联效应，需要大量更改才能解决单个安全问题。因此，将矛头指向软件供应商可能不是解决此问题的最佳途径。不可避免地存在这样一些情形，曝光和修复之间存在空白，因此网络经理需要能在这些空白期间保护其网络的战略。

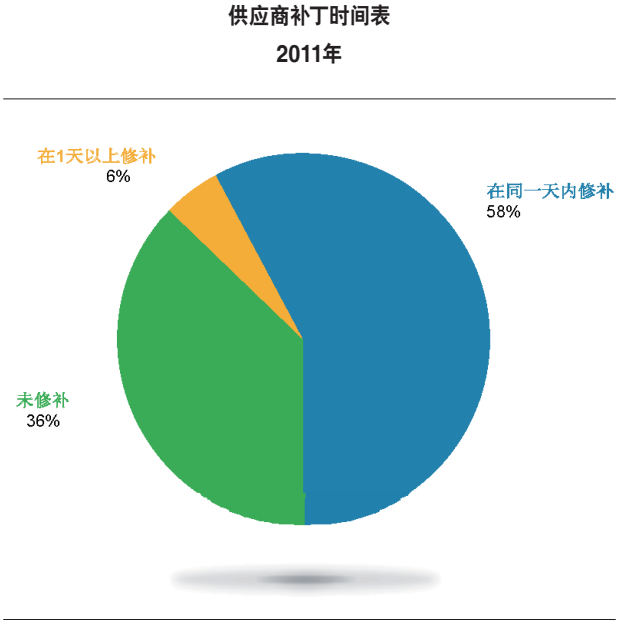


图46：供应商补丁时间表 – 2011年

当最严重的安全漏洞曝光时，X-Force会发布警告和建议。作为我们的趋势和风险报告的一个常规特征，根据攻击的难度和带给攻击者的价值，我们在一个二维图表上描绘这些警告和建议。这些因素有助于我们理解哪些漏洞可能在Internet上被广泛利用。

攻击工作与潜在的回报
2011年

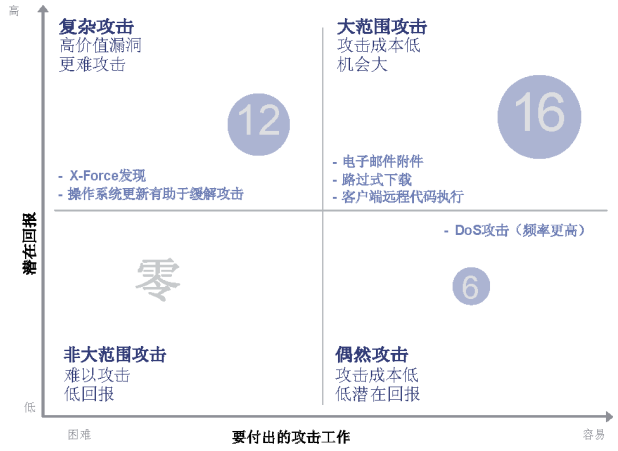


图47: 攻击工作与潜在的回报 – 2011年

X-Force在2011年发布了34个警告和建议。

其中16个漏洞属于关键类别，容易被攻击且具有极高的价值，这是恶意活动的一个最佳平衡点。几乎所有这些漏洞都表明存在可通过路过式下载或电子邮件附件来进行攻击的客户端软件远程代码执行问题。大部分目前已被广泛利用。

其中12个漏洞属于有价值但更难以攻击的类别 – 因为新操作系统特性使得更难以通过漏洞成功获得远程代码执行权限，X-Force发现属于这一类别的严重漏洞越来越多。

尽管我们仍然担忧老练的攻击者可能拥有其中一些漏洞的攻击代码，但我们预计不会在Internet上看到这些漏洞被广泛攻击。与关键漏洞象限相反，这一象限的漏洞增长表明在与计算机犯罪的斗争上我们取得了一定进步。

X-Force在2011年发出警告的漏洞中有6个是拒绝服务问题。尽管拒绝服务漏洞比远程代码执行问题的价值要低，但我们看到过去6个月中对这些漏洞的关注率在增高。具有政治动机的黑客群体（如Anonymous）对全球的企业和政府发起了拒绝服务攻击，以表达其各种政治主张。大部分这类活动涉及到看起来合法的流量分布式泛滥，与触发具体漏洞的攻击相比，这些攻击可能很难过滤。但是，我们已开始看到这些攻击者对使其攻击更有效的漏洞表现出一定的兴趣。

这些黑客开发的工具和技术现在越来越多地被具有财务动机、在竞争业务环境中使用拒绝服务攻击的攻击者所使用。考虑到今年美国的政治选举，以及与知识产权法律相关的全球官司，我们预计会在整个2012年看到更加突出的分布式拒绝服务攻击。

对社交媒体进行社会工程: 攻击者如何做

概述

自Internet得到广泛采用以来，很少有创新具有与社交媒体相同的影响。社交媒体正在转变社会联系、相互关联和共享信息的方式。这一转变的副产品是以前难以收集的个人和隐私信息大量涌入一个中央、可归档的位置 – 也就是Internet。这个信息宝库对具有入侵他人计算机恶意想法的人尤其有用。

在过去7年中，社交网络已从一种处于边缘的消遣方式，发展成为全球排名第一的在线活动，甚至超过了搜索引擎的使用。到2011年末，大约80%的全球在线用户群（超过10亿人）在使用社交媒体。[20]

自然地，这种人群聚集的活动对攻击者而言是一个富有的环境。以前通过电子邮件盛行多年的欺诈和诈骗方式在社交媒体论坛以及新兴的潜在目标群体中找到了新的生机。

用户向社交网络输入的大量隐私信息已改变了情报收集的模式。对于渗透公共和私有领域计算网络的攻击而言，从这些网络收集的情报已开始在攻击前的研究中发挥重要作用。

作为一个直接结果，2011年一些影响最大的黑客攻击都是从简单的开源情报(OSINT)收集和/或通过社交媒体执行的社会工程攻击代码着手。

20 来源: comscore It' s a Social World Report，2011年12月

这些攻击利用了组织边缘的一个灰色区域，目标指向个人和他们自愿提供的信息（通常是在非工作区上下文中）。与一个目标组织相关的个人可能疏忽（或特意）地提供有价值的信息，或者向企业系统中引入会导致企业数据资产被窃或受损的恶意软件。

尽管建立一个成功利用社交媒体的攻击可能具有挑战，但事实证明，攻击的成功率和相关的代价对付出的工作而言是值得的。本节探讨社交媒体对安全性的影响，重点关注情报收集方式的转变和剖析利用社交媒体平台的社会工程攻击。本节的目的在于向读者告知新兴的攻击方法以及它们对公共和私有领域实体的潜在影响。

情报收集

通常可接受的观点是，情报收集遵循一个相对简单的周期，其中涉及需求开发、规划和方向制定、实际收集、处理、分析和散播，但周期中的实际步骤数目可能有所不同。在此过程中收集的一些常见情报类型包括人类情报(HUMINT)、开源情报(OSINT)、信号情报(SIGINT)、措施和特征情报(MASINT)，以及图像情报(IMINT)。

在社交媒体出现之前，收集每类情报的方法相对比较直观，常常需要专门关注每种情报类型。社交媒体的出现将情报来源的收集从个人区域转向了简单的OSINT。

HUMINT不再需要物理联系方式来建立“人际联系”，比以前更加公开。SIGINT不再需要拦截信号，因为媒体在很大程度上是由各个实体共享的，图像情报通过全球最大型的图片库（Fotki、Webshots、Facebook等）得到了增强。

社交媒体现在为情报收集者提供了有史以来最大的信息存储库。想想一个乐意采用社交媒体的人不仅会自愿提供情报，还会提供这些情报的上下文。通过向公众提供舆论，社交媒体在本质上会容易出现秘密信息的意外或特意散播。有多个实例可以证明，美国官员错误地发布了机密行程的信息，或者一位国会议员在“返回华盛顿后，秘密情报简报在伊朗被收到。”但是，除了公然的轻率言行，用户还常常在社交媒体发布看似善意的信息，如个人电子邮件地址、目前居住的城市和教育背景。

开源情报收集

现在可供收集的大量公开或开源情报(OSINT)开启了一个新的信息安全和攻击领域。执行开源情报搜索的趋势在2011年快速增长，并且可能会在2012年继续增长。

这一显著增长催生了一个完整的搜索工具和技术领域。这些工具包括的实用程序不仅专注于实际搜索，还专注于所找到数据的对应关系。通常利用的工具（如Maltego）可帮助查找信息并以一种可轻松使用的方式表示这些信息。同时，Foca等工具可帮助您查找信息并使用该信息收集更多的情报。

众所周知，法律实施组织不仅利用现有的工具挖掘社交网络上的公共数据，还在搜索更强大且更细粒度的新工具。这些工作很有趣，它们表明OSINT收集不仅是攻击者的流行趋势，也是安全专业人员的流行趋势。诚然，大量的信息对确定谁在攻击很有用。

在计算机入侵上下文中，像这样的信息对社会工程攻击和身份验证逻辑攻击（如请求个人信息的密码重置）而言具有极高的价值。攻击者已在积极地利用社交媒体中的这些不足来保护目标组织的入口点。考虑到2011年执行的多个高影响力攻击获得了成功，通过社交媒体的社会工程攻击将成为在高级持续威胁中看到新兴趋势。

工作原理 – 不是尖端科学

例如，这个具体的代码攻击是一种三级攻击，结合了社会工程、鱼叉式钓鱼和零日执行来完成攻击步骤。就像骗子在拉斯维加斯赌场中游荡，

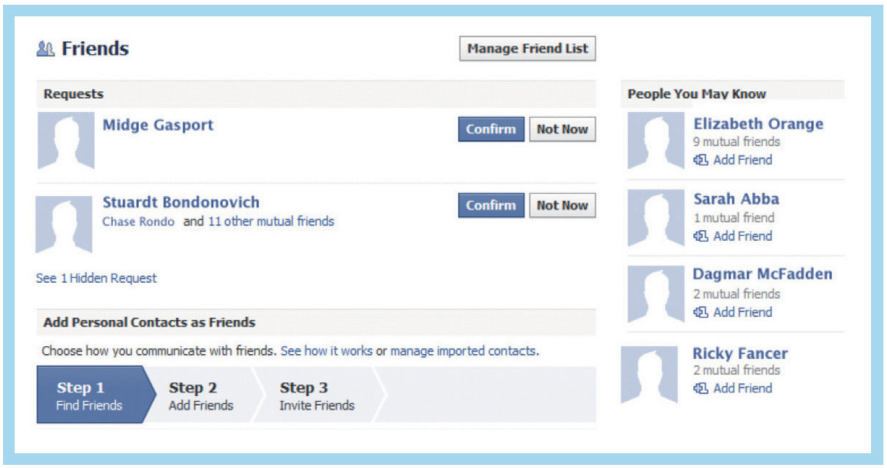


图48: 2011年可能进行鱼叉式攻击的联系人示例列表

寻找有弱点的商人，以及非洲猎豹在塞伦盖蒂草原游荡，试图发现跛行的斑马，攻击者也会在社交网络中游走，寻找具有庞大且活跃的好友名单的最终用户。

首先，攻击者选择一个目标组织。然后他们在社交媒体论坛（如LinkedIn）上创建一个帐户，设置一个暗示与该组织有关系的别名和履历，如前员工。在低迷的经济形势下，在经历大量并购活动的行业中，伪装成目标组织的前员工可让别名貌似可信。建立可靠的帐户后，Facebook和LinkedIn 等论坛就会向攻击者提供来自目标组织的潜在连接列表。

一旦攻击者知道接近谁，社会工程阶段就开始了。攻击者尝试与目标组织目前的员工建立联系。方法简单而多变 – 在多年后重新建立联系、换了工作并希望拓宽自己的专业网络、最近被解雇并希望返回到目标组织，或者希望在行业活动上见到后建立联系。如果攻击者接近大量个人，一种小心措辞、低调的方法很容易成功。建立第一个连接常常是最难的。有时攻击者会创建另一个来自目标组织的别名帐户并链接两个帐户，以建立信任关系。没有任何机制来审查在社交媒体论坛上所做的错误声明和表示，所以人们只会看到大部分用户帐户的表面价值并将其视为合法。

一旦攻击者在目标内建立一个合法的连接，收集其他信息就更容易了。举例而言，LinkedIn会帮助成员介绍第二个或第三个好友，Facebook也会通过好友的好友来这么做。除此之外，在著名论坛之间链接帐户的能力也可帮助攻击者通过与一个或两个合法个人联系人的关系来从各种来源建立更多联系人。

然后，攻击者开始分析每个合法联系人的履历，收集个人信息、组织相关信息，甚至衡量他感兴趣的方面，以确定接近每个人的最佳路径。与这些新联系人建立基本水平的信任关系很容易 – 询问简单的信息，

或者转发一些可能很有趣的信息。这让攻击者能够确定哪些最终用户最活跃，哪些用户最可能“帮助”他获得目标组织的访问权。

最后，攻击者足够地麻痹个人之后，攻击的鱼叉式钓鱼阶段就可以开始了。此攻击在攻击者拥有最终用户的企业电子邮件帐户的访问权限时最容易成功。甚至一两个企业电子邮件即可让攻击者能够理解命名约定并猜测其他电子邮件帐户。良好设计的电子邮件 – 针对一位不满员工的职位空缺公告、对找工作者的专业调查、针对处于职业过渡期的人们进行培训的视频链接 – 任何看起来合法且可能与工作具有松散的关联

的内容都可能吸引注意力并被目标组织的企业计算环境中至少一位最终用户接受。这些电子邮件通常包含恶意的有效负载、链接、下载或一个*.exe文件，正是这位最终用户完成了攻击最后阶段的工作。

然后攻击者就进入了企业“内部”并可以执行零日攻击了。一个好消息 – 失败的攻击与成功攻击的区别 – 在于最终用户必须执行一项操作，这样才能激活攻击代码。

组织减轻社交媒体风险的步骤

2011年9月的一份Ponemon Institute研究[22]表明，只有35%的回复者编写了社交媒体策略。在这些组织中，只有35%的组织积极执行了该策略。同一份研究还表明，企业计算系统上的病毒和恶意软件攻击自员工开始使用社交媒体以来增长了50%以上。不幸的是，没有可轻松部署的软件或端点产品套件可防御社会工程。与针对人类的大部分威胁一样，管理这类风险的最佳方式是策略和培训。

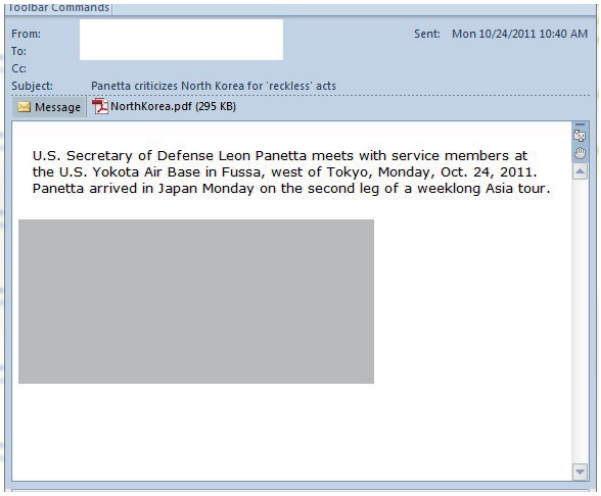


图49：2011年的鱼叉式钓鱼电子邮件示例[21]

21 来源：http：//contagiodump.blogspot.com/2011年/10/cve-2011年-0611-pdf-2011年-10-24-northkorea.html.

22 来源：http：//www.ponemon.org/ 2011年9月举行的全球社交媒体风险调查。该研究调查了美国、加拿大、英国、法国、德国、意大利、澳大利亚、新加坡、中国香港、印度、巴西和墨西哥平均拥有10年经验的4,640位IT和IT安全从业者。

这些工作可划分为两个具体的关注区域: 针对业务环境的操作和针对用户的操作。因为社交媒体主要是一种个人体验, 主要存在于工作区之外, 所以用户主要负责的是他自己的隐私和安全。但是, 企业急需创建各种策略和规程来帮助指导员工并保护公司的品牌和资产。这些工作类似于过去的 "安全感知" 计划, 但应独特地包含最终用户有何责任的指南, 如:

支持安全和隐私设置。著名社交媒体论坛都为用户提供了基本的隐私设置。重要的是, 最终用户理解可在他们常用的论坛中使用哪些安全和隐私控制, 即使他们认为自己不是活跃的用户。为了减少向垃圾邮件、诈骗和机会攻击者的暴露面, 应将安全和隐私控制设置为最高级别。

最终用户还必须认识到, 在其社交圈子中, 他们采取的任何安全和隐私操作都要降到最低的级别。举例而言, 如果一位好友仅使用最低的安全和隐私设置级别, 它会为暴露其圈子内的所有连接创造一种途径, 无论这些连接是否采用了更高的安全级别都是如此。换言之, 如果Facebook好友1将它的帖子和允许的联系人限制到他的好友圈, 那么发布到好友2公告墙上的任何信息都可被Facebook中的每个人看到。根据好友2的隐私设置, 甚至可在Internet上搜索到这些帖子。

鼓励最终用户在其社交媒体状态中采用一种 "默认拒绝" 设置似乎与加入社区的宗旨相矛盾, 但正是这种安全认知水平最终可保护他们远离社会工程攻击。

好友只是好友。如果在某些方面不够聪明, 社会工程攻击不会如此成功。就像真实的欺骗大师一样, 社交媒体攻击者在攻击之初会尝试获取其目标的一定信任水平。伪装成老同学、前同事或好友的好友, 这些方式很常见。例如, 通过LinkedIn伪装成一种与外围工作相关的关系会给攻击者带来几乎直接的可信度, 因为LinkedIn在社交媒体中被视为一种面向业务、不存在欺骗的论坛。但是, 使用以前的工作关系或在一场行业大会或活动上见过目标的虚假声明来通过LinkedIn建立连接, 这足以说服目标接受连接。希望改善其在线状态或影响面的最终用户通常会接受随机请求, 以增加他们的好友数。

尽管拥有大量不同的关注者和好友有各种诱因和回报，但一定要记住，这正是攻击者希望藏身的环境。最终用户应谨慎地考虑好友的请求，根据以前的真实关系或社交媒体论坛中一定的信任度（如论坛赞助的俱乐部、共同兴趣等）来接受请求。应谨慎地筛选基于第二或第三级相互连接的随机好友请求。应始终小心地查看来自新好友（最终用户仅通过社交媒体认识的人）的针对详细个人信息的私聊和私下请求，特别是在请求涉及到真实联系信息时。

小心地处理链接和下载。自上世纪90年代末电子邮件大量普及以来，链接和下载是攻击者向目标提供恶意软件时最喜欢使用的手段。该趋势已不断演化到社交媒体论坛中。最终用户必须万般小心，在单击任何链接或从未知或不受信任的来源下载任何内容（尤其是可执行文件）之前要谨慎考虑。许多新“好友”可能试图通过电子邮件将最终用户定向到有趣的YouTube视频、有趣的屏幕保护程序、伪造的爱好者论坛或不错的免费游戏，从而提供恶意的有效载荷。随机攻击者常常尝试通过垃圾邮件提供恶意有效载荷。Facebook和其他论坛在获得大范围攻击提醒时会定期发布警告。最终用户应订阅各个论坛提供的任何提醒服务。

对竞赛、礼品、奖品和特价产品要保持警觉。“您可能已获胜。”奖品和其他特价产品诈骗手段可追溯到电子邮件的早期，但仍然继续在社交媒体中盛行。诈骗者通常使用这种类型的产品（例如“向论坛成员提供免费的高价值礼品卡”）来将最终用户定向到一个会加载cookie或者甚至间谍软件的陷阱网站，或者更常见的是定向到类似合法的企业或品牌的伪造网站，要求最终用户填写复杂的申请或调查以获得参加虚假竞赛的资格。无论通过哪种方式，诈骗者都会从其目标收集个人信息。Facebook有一个名为Facecrook的用户社区向成员提供诈骗提醒，提供可用的细节和修复信息。最终用户应订阅其各自社交媒体论坛提供的任何诈骗提醒服务。

考虑限制与工作相关的信息。最终用户在传达有关组织、同事、客户、产品、服务和他们目前所参与项目的信息时，始终应遵照其雇主的社交媒体适当使用策略。除了具体的信息，最终用户可能还希望考虑仅使用一般性词汇引用其行业或雇主，以免意外暴露过多的信息。随着更多最终用户通过社交媒体寻找工作或联系机会，以及更多的雇主扫描社交媒体来评估当前或潜在的员工，小心地筛选与工作相关的信息变得越来越重要。[23]

在缺乏书面的企业策略时，常识可能是发布工作相关信息方面的最佳指导。

甚至不小心的引用有时也可能暴露比最终用户最初期望还要多的信息。在社交媒体论坛上发表任何内容的最佳经验规则是，尽管存在安全和隐私设置，尽管具有良好的意图和很少发生事故，但社交网络的设计宗旨是通过Internet在全球共享信息。所有帖子内容都应谨慎考虑，因为它们会立即公开并且可能无法撤销。

未来趋势

未来社交媒体攻击的影响和范围将继续增大。这一扩展包括冒险采用看似不相关的技术。例如，汽车已成为Internet和通过社交媒体互联的移动接口。借助这一扩展，社交媒体将继续演化，并对攻击者而言代表着一个容易攻击的场所。

企业组织需要开发和实施各种策略，用户在保护自身方面必须变得更加博闻强识。

23 尽管2011年这一趋势出现了消极反映，但许多雇主正在开放地使用社交媒体作为招聘流程的一部分，包括背景和信用检查。

10大常见的CSIRP错误

在规划对涉及网络、计算机或电子数据的安全事故的响应时，计算机安全事故响应计划(CSIRP)（任何具有比昂贵计算器更高级功能的环境中的基础）非常重要。在事故期间，CSIRP是引导您进行响应的地图。

本文介绍一些涉及CSIRP的最常见错误。IBM的应急响应服务(ERS)团队正在秘密参与CSIRP计划，因为我们经常会响应客户应急事件并为客户开发自定义CSIRP计划。ERS幸运地看到了哪些措施有效，以及哪些措施无效。本文将介绍CSIRP计划中一些最常见的不足。

#1 让CSIRP变得太复杂

设计CSIRP时，最好记住受众将在遇到危机时阅读该文档，而不是在在咖啡厅喝着咖啡且手里拿着糕点

的放松心情下，边听经典音乐边阅读材料。尽管我们可能梦想事故中有热腾腾的糕点且拥有无限的时间来消化一个计划，但通常这根本不会发生。受众可能面临着巨大的压力。个人可能会恐慌并担忧他们的工作。高管（无论是否理解所发生事情的技术要点）可能很烦恼，因为当地新闻媒体正在不断提问。一边叫喊，一边假想情况很快会恢复正常……您可以想象这一场景。

在上述情形中，您还有时间查阅庞大、详细的CSIRP计划吗？显然没有。CSIRP必须简明扼要、条理清晰且简洁。如果不熟悉文档的员工无法快速找到CSIRP中描述的流程，理解命令链和执行必要的操作，您的CSIRP可能就太复杂了。当然，将CSIRP设计得太简单也是一个潜在的陷阱；应努力在成功的CSIRP所必备的简洁性和实用性之间找到正确的平衡点。

#2 让重要人员负担过重

每个组织都有一个Joe。Joe知道每个人和每个系统、路由器、线缆和建筑物中最重要的3个咖啡机。Joe是我们在发生事故时都在寻找的人。毫无疑问，Joe是解决次要事故的最佳人选，可全程处理它们。当我们为客户开发CSIRP时，我们会在标准提问期间迅速找到组织中的Joe：谁负责防病毒软件？Joe。谁与高层沟通？Joe。谁计划公司的假期聚会？Joe。

Joe出色地完成了它从早上8点到下午5点所完成的工作。但是，当一个事故需要几天时间时，Joe不能72小时都一直在您身边。如果组织不希望一个被剥夺了睡眠、超负荷工作的员工来计划6月的假期聚会，那么有必要在事故期间分离职权并准备好以前指定的备份。

#3 将事故视为顺序过程

在大规模事故期间，多任务处理必不可少。仅将事故视为一个顺序过程的事故经理无法及时解决各个事故。尽管每个事故各不相同，但它们都包含许多短期目标。去除新的防病毒特征、修复系统、领导调查工作、向员工和客户通知您当前的状态、找到其他含咖啡因饮料的其他提供商，以及其他重要的任务都是独特的流程并应这样对待。一种常见的故障是公司一次仅专注于一个任务，忽略可能并行完成的其他重要任务。

#4 未能建立合适的通信线路

响应一个事故时，可能要求大量的个人和供应商提供帮助。事故经理（负责管理“兵力部署”的人）应是主要沟通人员。通信必须依序、有效且采用适当的渠道。

想象一个有25个人的作战室，每个人从另外15个人获取指令且没有合适的通信线路存在。进度几乎停滞，应该在24小时前解决的事故被拖延了。面对事故时，通信技能可能与技术技能同等重要。没有声音、没有愿景和指导员，团队的其他成员常常注定会失败。CSIRP应解决并制定通信线路，确保所有信息都在需要它的人手中，没有被阻止在已划分的地区中。

#5 专注于容易的事，而不是需要完成的事

在每个事故期间，常常会鼓励人们专注于轻松的任务，而不是需要完成的任务。这就像在引擎无法启动时加注玻璃清洗液一样。确实，玻璃清洗液最终需要填充，但没有能运行的引擎，您的车就毫无用处。事故也是如此。没有困难的任务和容易的任务，无论是否困难，某些任务都得完成。未能将您的精力集中在基本的问题上，无论该问题是容易还是困难，都可能导致长期的头痛问题和事故拖延处理。

#6 专注于刺激的事，而不是需要完成的事

在一些事故发生期间，响应者会发现一些有趣的信息并将精力集中在寻找不相关的兔子洞上。新发现的问题可能非常有吸引力，但它在解决事故方面没有发挥实质性作用。您在无休止地寻找兔子洞，而兔子早已跑到国外度假去了。请记住，您的目标是抓兔子，而不是观察兔子洞的结构变化。

#7 抛弃CSIRP

有时人们非常希望抛弃CSIRP，因为它无法解决手头的具体问题。文档无法解决最新的电子邮件病毒有一个原因。CSIRP并不是针对如何应对每个具体事故的全面指南。该文档是针对通信线路、角色、需要的通知和要采取的事故响应步骤的蓝图。尽管每个事故都是独特的，但该文档应允许形成一个响应方案，快速理解应包含的重要人员的身份、他们的角色和通信协议。有了这一结构，即可采取必要的步骤来解决手头的事故。

#8 制定一个策略，而不是一个计划

始终记住，CSIRP中的“P”代表计划而不是策略。有时，ERS审核的CSIRP看起来更像策略而不是计划。二者有何区别？计划包含可操作的步骤和角色，而策略表明要在组织内应用的总体指南。事故发生时，您真的希望阅读公司的策略来制定计划吗？当然不是。您要的是一个告诉您做什么的考虑周详的计划。

#9 未能指定负责人

您的CSIRP可能与您的猫有许多共同之处。二者都在不断发展，需要维护和关注，还应有一个负责人来负责它们的健康。有时，在发生一个事故时，从网络深处拉出CSIRP之后却发现文档的上一次更新还是在Vista刚推出时。

一个一个地找，发现重要人员的电话号码都联系不上。甚至最初设计为作战室的会议室也被重新设计为公司的日托中心。没有为文档安排负责人，没有看守人，文档就会过时，它的价值就会丧失。

建立CSIRP时，为文档安排一个负责人。这个负责人负责更新文档，确保它包含的过程仍然相关，协调手动测试。没有具体的负责人，文档可能失去活力，变得停滞并导致更长的事故响应时间。

#10 忽略了事后审核

来自任何事故的最宝贵的教训可从事后审核中学到。即使似乎在事故中所有事情都在按计划进行，也可能在事后审核中发现可能的改进之处。指出需要改进的错误或问题没什么让人羞愧的；任何这些都会让CSIRP更强大，更能够在未来的事故中满足您的需求。

在总结事故时，主要人员应开会探讨CSIRP的执行效果。不幸的是，为了匆忙地忘记过去几周的头痛问题，事后审核常常是CSIRP流程中被忽略的一个重要步骤。

事故响应 - 准备基础设施以实现大规模响应

事故响应(IR)并不是大部分安全人员在日常工作中所想的那样。我们考虑防御性和攻击性状态、身份管理、代码审核和其他日常操作。但严肃地讲，在这些机制失败后会发生什么？组织如何从入侵、病毒爆发或敏感数据泄漏中恢复？事故响应应该是一个计划好的流程，在需要之前就进行了精心设计，防止对后果考虑不足就快速制定决策。在最简单的形式中，IR规划主要涉及到识别您组织中最擅长识别和根除严重安全问题的故障排除专家。这些人不需要是专门的事故响应人员，但可直接参与。在此类场景中，事故响应通常不是系统化的。从业者倾向于玩打鼹鼠，

通过本地扫描敲打各个感染体，通过sneaker-net和一个CD来解决更多问题，而不是执行广泛的监视和大规模清理过程。

所有优秀的事故响应真正需要存储所有信息并随时理清其条理的能力。

对于小型组织，这可能足够了。它不是一种坏方法，但不能扩展到超出少量的机器。否则通常需要实际进行投资来建立基础设施，建立事故响应团队，使用工具捕获和分析整个企业的数据。有了如今所有可用的日志和分析平台与设备，很容易想象可扩展的事故响应只是另一种设备。

事故响应不容易，需要存储所有信息并具有随时理清其条理的能力。不幸的是，即使这种方法也不能扩展超过10台机器。一旦事故涉及到超过数十台机器，比较简单的事故响应模型就需要过量的人员才能运转。尽管俗语“如果暴力没有用，那就是您用得还不够”可能适用，但它带来的大部分流程都会非常昂贵且难驾驭。例如， 假设您的事故响应计划要求受信息盗窃病毒感染的系统必须关闭并建立镜像，能多好（和多快）地对50台机器完成这一工作？1500台呢？在您的防病毒解决方案检测到该病毒已感染机器几小时或几天时，您如何确定哪些机器受到了感染？本文将尝试探讨一些最有帮助的基本步骤，让您准备使用同时在财务和时间上可扩展的方式应对这些类型的场景。

准备: 所有事故响应的坚实基础

尽管具体的缩写可能不同，但传统的事故响应原则大纲始终在开头以 "P" 表示准备。大规模事故响应涉及到比更小环境多得多的准备工作，但在经过适当准备后，后续步骤中需要的工作基本是类似的。幸运的是，准备良好的事故响应所涉及的许多（如果不是全部）步骤都是一般的优秀基础设施实践，因此已是良好管理的环境的必要组件。诚然，许多系统管理可被视为 "低级的" 事故响应。集中化的身份验证、补丁管理、清单管理、日志记录、访问控制和自动化都是运行成功的计算基础设施的基本组件，其中每个组件都对事故响应具有特定的意义。探讨所有这些组件不属于本文的范畴，但其中的两个对扩展事故响应无疑很重要：日志记录和自动化。它们是我们看到客户常常遗漏的两个重要成功因素。

不记录日志对您的伤害比我更大

老练的事故响应人员首先会问的问题之一是 "您的日志在哪里？" 当响应人员遇到的情形的答案不太合意时，他们将竭尽所能来提供帮助，但对他们成功识别手头的问题并根除问题根源几率的认识正在快速丧失。他们已了解到，成功进行事故响应不是遥不可及的完美结果，而是完全可以实现的。如果客户无法识别参与数据破坏的人员，而只知道他在 "系统中停留了" 很长时间，让暴露的记录从数十条增加到数百万条，那么对客户的伤害会更大。

日志记录为事故响应人员和系统管理员都提供了帮助确定给定时刻（无论是过去还是现在）基础设施中发生什么事情的重要知识。不幸的是，与良好运行的安全环境中的其他人一样，普遍存在的日志可能是当代基础设施中第一批被砍掉的方面之一，因为它为了很少需要的内容而占用了宝贵的系统、网络和财务资源。

成功进行日志记录的主要秘诀是过滤和集中化。这是一个非典型的经过良好计划的环境，可支持全面记录每个操作。事故响应人员常常必须与系统管理员进行合作，确定可提供合理响应，同时又能避免使用过量资源所需的最小日志集合。关键是在保留资源和成本/性能之间找到一个平衡点。作为一个示例，很少有必要（但完全可能）记录Windows系统中的每次对象访问，但无法记录特权用户的使用情况可能对响应和管理都会产生严重的影响。想象在一个配置良好的域中，域管理员（可能使用低特权人员的凭据）短暂提升其特权以更改一个DNS设置，意外地破坏了它。在此情形下，管理员可快速看到所发生的事情、是谁做的和要修复的内容。现在想象一下：低特权凭据实际上不是该用户的，而是一个破坏凭据的攻击者的。

收集了日志后，必须存储它们，存储在几乎其他任何地方都比存储在生成它们的系统上要好。日志会占用宝贵的磁盘空间，可能在系统故障中丢失，或者甚至在入侵事件中被攻击者修改。集中化的存储有助于减轻或至少将这些问题转移到一个独立的系统。根据组织的需求和对导致可接受的日志丢失的要素进行风险计算，可采用多种方式将日志转移到一个中央系统。从事故响应人员的角度讲，理想的安排常常是实时传送，通过可靠事件日志协议(RELP)等机制实现端到端的保证，有效地消除入侵者修改日志的时间窗。RELP可通过网络提供可靠的事件日志记录。关键同样在于平衡，并且不允许将“最佳”与“不错”对立起来。拥有一个从系统批量拉取日志的欠佳日志收集系统，比什么都没有要强得多。

在确定拉取日志的频率时，一条粗略的经验规则是确定多长的时间窗才能让攻击者可以修改日志，然后将该时间窗除以2。一些组织避免集中存储日志，因为它似乎很昂贵，涉及到快速SAN磁盘的成本和应用服务器硬件价格。中央日志记录设备不需要这么昂贵。

无需理想地保持独立并与环境的剩余部分分开管理（没有信任或共享凭据），并且除非在系统上执行日志分析，否则硬件和可用性需求不应超过典型文件服务器的需求。

自动化是您的第二位、第三位和第N位最好的朋友

系统管理和事故响应中的自动化就像职业棒球大联赛与周末非正式垒球赛之间的区别。它允许一些组织以超过1000: 1的服务器与管理员比率来运营，允许事故响应人员精确地一次处理数千台损坏的机器。对事故响应，幸运的是通常在包含大量机器的环境中实现了一定程度的自动化，因为管理员一般不会选择在超过两个以上的系统上单独安装补丁，而不借助补丁管理工具来控制该流程。此外，许多环境安装了“代理”来提供端点安全、资产管理、防病毒管理和大量其他必要的日常管理职能。

事故响应人员在面对这些工具时，最大的困难常常是了解哪些工具可用以及如何使用它们。任何这些自动化工具都可用来为事故响应人员提供对各种系统状态宝贵的自定义查询，但应根据它们的不应期和它们对系统的修改程度来谨慎选择。

例如，假设您的事故响应团队已确定一个新病毒未被防病毒解决方案检测到，但知道它创建了一个与一组目录中的某个正则表达式匹配的文件。基础设施团队在所有可能受影响的系统上运行着补丁管理、资产管理和防病毒工具。一个解决方案可能是提供一个补丁文件，通过补丁管理工具在系统上搜索指示符文件，

通过将结果文件上传到中央服务器来进行报告。对于一些情形，这可能是唯一的方法，但它修改了可能受影响的系统，并且可能让响应流程更加开放，更容易被恶意方所干扰。但是，如果资产管理工具可报告与特定模式匹配的文件，它可能是首选的方法，因为它不会修改最终系统并且向恶意方显示为普通的活动。根据具体的情形，清理已感染的内容可通过补丁管理或防病毒系统很好地完成。关键在于首先认识到哪些工具/功能可在环境中使用（或供基础设施团队用于实现双赢的工具），然后选择正确的工具来完成工作。

在自动化方式中，最后但无疑同样重要的是编写脚本。尽管自动化工具常常可很好地利用自己的脚本语言，但在事故响应流程中，很少有工具比这样的事故响应人员更有效和高效：他们能使用Python或Perl等一般语言编写脚本来控制自动化工具和弥补可能遗漏的差距。在事故响应团队中有一位或者可在匆忙之中派上用场的老练系统管理程序员，可能对响应的速度和完备性而言是一笔宝贵的资产。

最后且最重要：身份验证

对于事故响应，第三个也是容易遗忘的关键是身份验证。有人可能注意到，上述许多步骤已（或应）断言具有强大的、集中化的身份验证。如果没有中央身份验证，那么不求助于残酷的战术，如收集和存储每个机器的，密码管理员和响应人员通常无法高效地查询系统，应用修复程序或处理系统。一些著名的大型环境确实没有集中化的身份验证，而是依靠在管理特权下定期执行脚本的远程代理，但此类设置的响应时间可能会妨碍实现良好的管理和事故响应，所以应全力避免这种情况。

聪明地工作并结交不错的朋友

良好的基础设施实践应直接转化为良好的事故响应。您需要用来构建容错能力更高、可重复且可扩展的计算基础设施的工具和过程，与用来顺利且快速地响应事故的工具和过程相同。与系统管理团队培养良好的关系并了解他们已有哪些工具，确保您理解并知道如何操作这些工具。这样，事故响应团队就可在必要时支持它们。

数据安全和隐私，理解区别以帮助实现合规性

公司依靠数据来支持其日常的业务运营，所以一定要确保隐私并保护数据，无论它位于何处。根据Verizon数据破坏调查报告，数据库服务器是违规数据的主要来源，占损坏记录的92%。不幸的是，与识别违规和修复违规所需的时间相比，攻击者渗透数据库所需的时间相差悬殊。攻击者花几天时间渗透防御层，而组织需要花几周或几个月才能确定他们是如何、在何处以及何时被损害，然后常常会再花几周或几个月来修复问题。

数据安全和隐私变得比以往更复杂，因为不同类型的信息具有不同的保护和隐私需求；因此组织必须采用整体方法来保护其信息。此方法包括：

- 数据发现和分类 – 组织需要理解数据存在于企业中的何处以及它有何关联。这让他们能够适当地分类敏感的数据，从而在数据的整个生命周期中适当对待它。
- 数据编写 – 敏感数据也位于文档、表单和扫描的图像中。保护这种非结构化数据需要隐私策略来编写（删除）敏感信息，同时仍然允许共享所需的业务数据。这些非结构化文档可能是数据库中的附件。
- 数据加密 – 许多监管指令可能要求加密数据库。组织需要一个可扩展的解决方案来保护异构数据类型。这可能是数据库活动监视的一个不错补充，因为组织可建立一种深度防御方法。
- 静态数据屏蔽 – 生产环境受到了更多的关注，但非生产环境的安全性也不应忽略。对生产数据库中的敏感数据去标识化，同时维护对应用开发、测试、培训流程和QA的适用性，

这不仅有助于简化业务流程，还有助于确保最低特权原则。没有有效业务的组织需要知道他们不应访问敏感数据。

- 监视 – 保护和持续监视对数据库、数据仓库和文件共享的访问，这会带来谁执行事务、事务的目标和事务执行方式方面的洞察，帮助组织验证数据的完整性。
- 漏洞评估 – 加固数据库，帮助减轻错误配置或默认设置等风险。

弄清谜团：为什么数据保护受到越来越多的关注？

根据Forrester Research2011年2月的独立报告《Forrsights：IT安全从2010到2011年的演化》，由于公司疲于应对更加险恶的威胁形势；应对越来越多的制度和第三方需求，以及适应前所未有的IT动荡水平，IT安全仍然是一些犯罪活动和增长的温床。大量关注落在新的计算机安全威胁，此报告主要关注的是一些重要的主题：新的计算机安全威胁（如Stuxnet和Aurora），不断变化的IT架构（如数据中心中的虚拟化）以及围绕第三方指令的更高压力。

在过去几年中，根据Forrester报告，“安全在可视性方面实现了稳定上升，获得了广泛的关注和支持。”例如，Forrester的研究表明，54%的企业首席信息安全官(CISO)向C级高管报告，42%向IT部门外的高管报告。这些百分比反映了安全在跨各种行业的所有类型组织中具有越来越高的业务相关性。将安全视为高或关键优先级的组织数量现在达到了几年来的最高水平。

对于有关促进对数据安全和隐私实施更多关注的许多因素，下面我们深入对此分析一下。

IT环境中的变化和不断演化的业务计划

随着组织采用新的业务计划，如外包、虚拟化、云、移动、Web 2.0和社交网络，安全策略和相应的技术应不断演化。这一演化意味着组织应更广泛地考虑数据所在的位置和访问它们的方式。组织还应考虑广泛的敏感数据，包括客户信息、贸易秘密、开发计划和竞争优势。

更聪明、更老练的攻击者

许多组织正在尽力应对攻击者的能力与安全防御之间越来越大的差距。外部攻击不断变化的性质、复杂性和更大的规模是组织关注的根源。根据同一个Forrester报告，与10年前相比，安全攻击现在拥有大得多的业务损害影响。以前，最关键的问题是病毒爆发或短期的拒绝服务攻击，

这将导致业务运营临时中断。如今，客户数据或企业数据（如贸易秘密）盗窃可能导致数十亿美元的业务影响、损失、罚金和诉讼，以及对组织声誉造成无法弥补的损害。

合规性指令

合规性指令的数量和种类繁多，它们影响着全球的组织。

伴随越来越多的合规性指令而来的是证明直接合规性的更高压力。企业面临着巨大的时间压力，需要向业务部门和股东直接展示目前的进展，否则面临着声誉损害和严厉的财务惩罚。

信息爆炸

电子信息的爆炸令人震惊。IDC估计地球上的每个人目前拥有45GB数据，或者总共拥有惊人的2810亿GB数据。尽管这些数据中只有5%最终位于企业数据服务器上，但它预计每年会增长60%，到2011年达到14EB的企业数据。信息爆炸让我们对公共和私有信息的访问成为日常生活的一部分。关键的业务应用通常会收集此信息用于合法用途。但是，考虑到Internet和信息系统，以及企业ERP、CRM和自定义业务应用的互联性质，敏感数据容易被盗窃和误用。

内部威胁

很高比例的数据违规实际上来自内部缺陷。例如包括员工误用支付卡号码和其他敏感信息，以及员工将机密信息保存在随后被盗的笔记本电脑上。组织有责任保护数据，无论数据位于何处，包括与业务合作伙伴、供应商或其他第三方一起采取措施。

总之，组织正在高度关注数据安全和隐私问题。它们的眼光超越了为特定难题开发单点解决方案，而是考虑在企业中构建安全策略、隐私策略和过程。

理解安全和隐私之间的区别

安全和隐私是相关的，但它们是不同的概念。安全是基础设施级别上的防范，基于授权来阻止或授予对某些区域的访问权。相反，隐私限制会控制被授权访问一组特定数据的用户的访问。数据隐私解决了对具有查看数据合法业务用途的人的限制。该业务用途通常由工作职能定义，而后者由合规性定义。

数据安全解决方案的一些示例包括数据库活动监视和数据库漏洞评估。数据隐私解决方案的一些示例包括数据编写和数据屏蔽。在一个演示这一区别的最新案例中，UCLA医疗中心的医生被抓住查看明星Britney Spears的医疗记录。该医院的安全策略得到了认可，因为医生需要访问医疗记录，

但在医生出于好奇心而不是出于合法的医疗用途而访问文件时，隐私问题就出现了。

赌注很高：与不足的数据安全和隐私相关的风险

根据2010 Ponemon研究声称，数据违规成本连续五年持续增长。2010年数据违规的平均组织成本增至720万美元，与2009年的680万美元相比上升了7%。总违规成本自2006年以来每年都在增长。2010年的数据违规花费了公司平均214美元/违规的记录，与2009年相比上升了10美元（5%）。

Ponemon在2010年研究的最昂贵的违规事件花了3530万美元才得到解决，与2009年相比上升了480万美元（15%）。最廉价的数据违规为780,000美元，与2009年相比上升了30,000美元(4%)。与前一年一样，数据违规成本似乎与违规记录的数目成正比。

其他潜在的负面影响包括罚金或刑事责任、投资者担忧导致的股票价格下跌，以及数据违规导致的负面公众形象。公司被视为无法信任时，就会导致无法弥补的品牌损害。

一些常见的风险来源包括：

- 过度的特权和特权用户滥用。当用户（或应用）被授予超过其工作职能需求的数据库特权时，这些特权可被用于获取对机密信息的访问。
- 未授权的特权提升。攻击者可能利用数据库管理软件中的漏洞将低级访问特权转换为高级访问特权。
- SQL注入。SQL注入攻击涉及到用户利用前端Web应用和存储过程中的漏洞来（常常以提升的特权）发送未授权的数据查询。使用SQL注入，攻击者甚至能够获得整个数据库的无限制访问权限。
- 拒绝服务。拒绝服务(DoS)可通过许多技术来调用。常见的DoS技术包括缓冲区溢出、数据损坏、网络洪流和资源消耗。后者是数据库环境所独有的，但常常被忽略。
- 备份数据暴露。一些最新的高影响力攻击涉及到盗窃未加密的数据库备份磁带和硬盘。

充分利用一种整体的数据安全和隐私方法

组织应拥有一种整体的数据保护方法。此方法应保护整个企业中不同位置的各类数据，包括保护生产和非生产（开发、测试和培训）环境中的结构化和非结构化数据。这种方法有助于仅关注有限的资源，而不会增加流程或复杂性。整体方法还可帮助组织证明合规性，而不会中断重要的业务流程或日常运营。

首先，组织应考虑4个关键问题。这些问题旨在帮助组织将注意力集中在最关键的数据漏洞上：

1. 敏感数据位于整个企业中的何处？

2. 如何保护、监视和审计对企业数据库的访问？如何保护数据免受授权和未授权的访问？

3. 能否保护文档中的机密信息，同时仍然支持共享必要的业务数据？

4. 能否保护您的非生产环境中的数据，同时让它们可用于培训、应用开发和测试？

这些问题的答案为一种整体数据保护方法提供了基础。它们可帮助组织关注那些使用当前方法可能忽略的关键区域。

1. 如果组织不知道数据存在，他们将无法保护它。敏感数据以结构化和非结构化格式存在于生产和非生产环境中。组织需要记录并定义所有数据资产和关系，无论数据来自何处。一定要分类企业数据，理解数据关系和定义服务水平。数据发现流程会分析数据值和数据模式，从而识别将不同数据元素链接到逻辑信息单元或“业务对象”（如客户、患者或发票）的关系。

2. 数据库活动监视为特权和非特权用户与应用提供了访问监视功能，这些功能与原生的数据库日志和审计功能独立。它可用作对特权用户职权分离问题的补偿性控制，可监视管理员活动。该技术还可改善数据库安全，检测来自应用层的不常见的数据库读取和更新活动。数据库事件聚合、关联和报告提供了一种数据库审计功能，而无需启用原生数据库审计功能（也是数据库活动监视的一部分）。数据库活动监视解决方案应该能够检测恶意活动或不当或未批准的数据库管理员(DBA)访问。

3. 数据编写可基于工作角色或业务用途从表单和文档中删除敏感数据。例如，医生需要查看症状和愈后数据等敏感信息，而结算职员需要患者的保险编号和账单地址。挑战在于提供适当的保护，同时满足业务需求和在“需要知道”的基础上管理数据。数据编写解决方案应保护非结构化文档、表单和图形中的敏感信息。

4. 对非生产环境中的数据去标识化是系统地删除、屏蔽或转换可能用于识别个人的数据元素的过程。数据去标识化让开发人员、测试人员和培训人员能够使用逼真的数据并生成有效的结果，而仍然遵守隐私保护规则。以这种方式擦除或清理的数据一般被视为可用于非生产环境中，有助于确保即使数据被盗、曝光或丢失，它对任何人也没有什么用处。

一种确保整体数据保护的三级方法

理解和定义

组织应发现敏感数据位于何处，分类和定义数据类型，并确定度量指标和策略，确保不断实施保护。数据可能分散在多个应用、数据库和平台上，具有很少的文档。许多组织过度依赖系统和应用专家来管理此信息。有时，此信息内置于应用逻辑中，隐藏了可能在幕后执行的各种关系。

查找敏感数据和发现数据关系需要小心地进行分析。应明确理解和记录各种数据源和关系，以便不会漏下有价值的敏感数据。只有在理解完整的形势后，组织才能定义合适的企业数据安全和隐私策略。

安全保护

数据安全和隐私解决方案应涵盖一个异构的企业，同时保护生产和非生产环境中的结构化和非结构化数据。它们应有助于保护数据库、ERP/CRM应用和非结构化环境（如表单和文档）中的敏感数据。关键的技术包括数据库活动监视、数据屏蔽、数据编写和数据加密。一种整体性的数据保护方法可帮助组织确保所有组织数据都得到保护。

结构化数据：此数据基于一种数据模型，可用于数据库或XML等结构化格式中。

非结构化数据：此数据位于手动编写或键入的表单或文档中，如文字处理文档、电子邮件消息、图片、数字音频和视频。

在线数据：这是每天用于支持业务的数据，包括元数据、配置数据或日志文件。

离线数据：这是备份磁带或存储设备上的数据。

监视和审计

找到并保护好数据后，组织可能需要证明合规性，为应对新的内外部风险做好准备，以及持续监视系统。用户活动、对象创建、数据库配置和权限的监视可帮助IT专业人员与审计人员在应用和数据库之间跟踪用户。这些团队可为合适的行为设置细粒度的策略，在这些策略被违背时收到提醒。组织应快速展现合规性，让审计人员有能力验证合规性状态。审计报告和签署应有助于简化合规性流程，同时保持较低的成本和最大限度减少技术和业务中断。总之，组织应对所有数据库活动创建持续、细粒度的审计线索，包括每个事务的“人物、对象、时间、地点和方式”。

小结

保护数据安全和隐私是一项细致、持续的责任，应该是每个最佳实践的一部分。组织应考虑通过理解和定义、安全保护及监视和审计的3层战略来实现数据安全和隐私方法。

第III部分

软件开发安全实践

在本报告的“软件开发安全实践”部分中，我们介绍解决软件开发期间各种安全性问题的流程和技术。我们探讨企业如何查找现有的漏洞和帮助预防引入新漏洞。如果您使用连网应用或Web应用来收集或交换敏感数据，您作为安全专业人员的工作将比以往要更艰难。我们将分析IBM AppScan小组在所有应用开发阶段执行的静态和动态安全测试，分享我们所发现的各种洞察。

来自真实Web应用评估的结论

方法

IBM AppScan OnDemand服务是一个基于云的产品，帮助客户识别和修复Web应用漏洞，而无需购买和维护软件或雇佣高技能且专业的应用安全人员。IBM应用安全分析师使用IBM AppScan Enterprise Edition软件分析应用的安全漏洞，如果不解决这些漏洞，可能导致安全违规和潜在的数据丢失，如客户和员工记录或企业知识产权。IBM AppScan Enterprise Edition软件可测试常见的Web应用漏洞，包括跨站点脚本、缓冲区溢出、flash/flex应用和Web 2.0泄漏扫描。此外，该产品还包含扫描和检测Web属性中的嵌入式恶意软件的能力，能提供对计算机攻击的进一步防御。

IBM整理了2011年执行的237次安全测试中发现的真实漏洞数据，同时使用IBM AppScan执行了安全评估。这些评估将从IBM AppScan获得的应用安全评估结果与手动安全测试和验证相结合。在所有情况下，都会从测试中删除误报，并将漏洞对应到OWASP（开放Web应用安全项目）10大类别：

1. 注入
2. 跨站点脚本(XSS)
3. 破坏的身份验证和会话管理
4. 不安全的直接对象引用
5. 跨站点请求伪造(CSRF)
6. 安全错误配置
7. 不安全的密码存储
8. 未能限制URL访问
9. 不足的传输层保护
10. 未验证的重定向和转发

对于每个类别，计算了两个核心度量指标：

1. 在该类别中找到至少一个漏洞的比例

2. 可能在该类别中找到的漏洞平均数量

该团队自2007年开始收集类似数据，还能够跟踪过去5年的结果。这些历史数据也对应到2010年OWASP 10大类别，以跟踪此趋势。

度量点

该团队还分析了其他度量指标，以帮助更深入地分析数据。这包括：

业务领域，将测试数据归为以下一种类别：

- 金融
- 工业
- 信息技术
- 物流
- 政府
- 其他

应用安全测试周期描绘了应用所涉及的测试类型：

- 一次性评估—首次测试的应用
- 季度评估—定期测试的应用
- 重新测试—跟进测试，确认通常来自一次性评估的发现已结束

备注：只有在抽样大小可得到合适的数据时，才会将信息分类到这些度量指标组。在抽样大小被认为太小时，度量指标值会被忽略。因此不会表示所有业务领域或技术。

2011年应用漏洞趋势

下表列出了在一个应用安全测试中找到与每个OWASP 10大类别匹配的漏洞比例。

选择OWASP 10大类别对应关系是因为它支持更有针对性的评估并与行业最佳实践进行对比。在发现与2011年发现 (OWASP 10大类别对应关系)

OWASP没有直接对应关系时，会针对安全错误配置类别来采集发现，因此该类别中的数量会自然地增加。

值得注意的是，这些评估都是对似乎决定减轻其应用中各种问题的组织执行的。他们可能已部署了安全程序，或者可能在过去已存在安全违规。因此，此数据不代表一般Web应用或从未检查过的应用的状态。一些漏洞的价值具有明显的下降趋势，这可能显示投资回报与其他任何因素同样重要。

在10个测试中，有近8个中都发现了破坏的身份验证和与会话控制相关的问题。许多测试的应用未能限制会话篡改，容易受到会话固定式的攻击。与会话终止和会话重用相关的问题也是这一较高统计结果的推动因素。

2011年在执行的28%的测试中发现了跨站点请求伪造(CSRF)，但此数字与2010年的59%相比有所减少。减少的部分原因似乎是对此漏洞类型的认知度提高和用于包含CRSF令牌的方法改进。

2011年发现 (OWASP 10大类别对应关系)

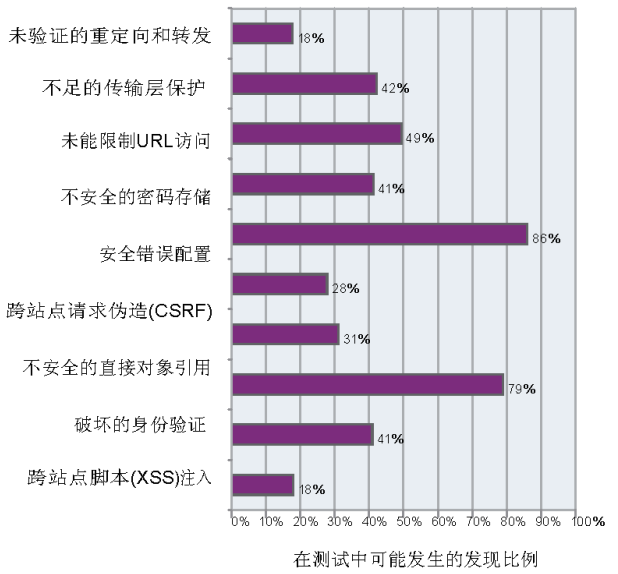


图50：2011年发现 (OWASP 10大类别对应关系)

年度趋势(2007—2011年)

自我们2007年开始记录应用安全统计数据以来，我们看到与输入控制相关的漏洞在稳步减少，如跨站点脚本(XSS)和SQL注入。2011年，我们的统计信息表明，在给定测试中遇到XSS的几率继续下降，但显示出发生几率稳定在40%左右的迹象。

尽管统计数据没有明确表明，但我们的测试发现，使用最佳实践和安全编码实践来过滤无效输入的应用具有甚少，甚至没有输入相关的问题（如XSS）实例。事实是，XSS仍然在超过40%的测试应用中找到，这表明仍然有许多应用未遵守安全编码实践。毫无疑问情况正在改善，但没有理由沾沾自喜。出现XSS漏洞的40%的几率仍然很高，尤其是对于很容易理解、容易证明和容易修复的漏洞。Web应用漏洞仍然是许多数据违规的关键，数据违规在2011年上半年继续增多。多得导致X-Force宣称2011年为“安全违规年”。

我们捕获的另一个重要数据点是“在每个安全测试中出现给定发现的平均数量。”我们看到所找到的XSS漏洞实例在减少。在2009年，平均数为40多个，而在2011年仅为超过3个。现在很难找到一个完全没有输入控制的应用。找到XSS的大部分应用现在似乎都部署了某种形式的输入控制，但没有专门的攻击途径能够应对这些过滤器/控制方法。

Web应用漏洞类型的年度趋势
IBM AppScan OnDemand Premium Service
2007-2011年

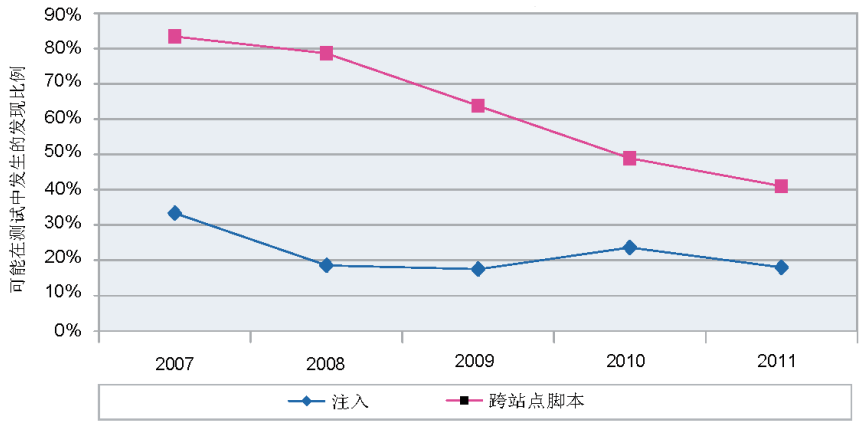


图51: Web应用漏洞类型的年度趋势
IBM AppScan OnDemand Premium Service – 2007-2011年

C年度趋势										
漏洞类型	2007		2008		2009		2010		2011	
	每个测试的平均漏洞数	一个漏洞发生的几率	每个测试的平均漏洞数	一个漏洞发生的几率	每个测试的平均漏洞数	一个漏洞发生的几率	每个测试的平均漏洞数	一个漏洞发生的几率	每个测试的平均漏洞数	一个漏洞发生的几率
注入	1.3	33%	5.3	19%	1.7	18%	2.3	24%	2.1	18%
跨站点脚本(XSS)	12.7	83%	17.9	79%	40.8	64%	5.8	49%	3.3	41%
破坏的身份验证	11.2	83%	4.8	84%	3.2	65%	2.5	53%	9.7	79%
不安全的直接对象引用	2.6	50%	3.2	54%	3.0	51%	1.9	33%	1.6	31%
跨站点请求伪造(CSRF)	1.9	22%	1.8	20%	7.9	59%	3.8	53%	2.0	28%
安全错误配置	46.9	83%	22.6	74%	23.5	68%	15.3	56%	10.7	86%
不安全的密码存储	21.7	38%	17.9	56%	29.1	38%	19.8	45%	11.9	41%
未能限制URL访问	7.2	13%	6.0	19%	9.7	13%	6.6	15%	5.0	49%
不足的传输层	7.3	28%	2.4	17%	2.5	35%	1.6	22%	9.8	42%
未验证的重定向和转发	1.7	7%	0.5	5%	0.1	3%	0.4	4%	0.3	18%

表8: Web应用漏洞类型的年度趋势, 2007-2011年, IBM Rational IBM AppScan OnDemand Premium Service

业务领域

与2010年一样，我们按业务领域对2011年的统计数据进行划分。我们可以将数据划分为数据点数量允许的5个类别。

2011年，财务应用再次成为表现最好的类别。下表显示了5个类别中的每一个在XSS、注入和CSRF漏洞方面的对比。政府应用是所有3个类别中表现最差的。出现此情况的具体原因不是很清楚，但声誉影响可能是一个因素。与财务应用相比，政府应用中的破坏不太可能推动对安全减轻措施的投资。

财务应用的CSRF比任何其他类别要少得多。可能这种形式的攻击在此类别中受到了高度重视，因为认识到了它的后果。此类型攻击的主要目的是诈骗受害者，可能银行应用和使用金融交易的应用是主要的目标。

各种Web应用漏洞类型在不同行业的趋势
IBM AppScan OnDemand Premium Service
2007-2011年

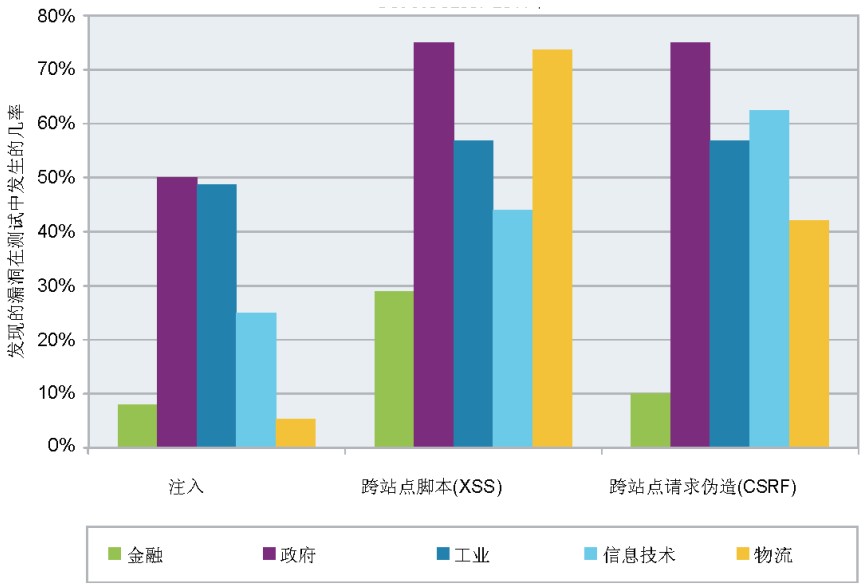


图52: 各种Web应用漏洞类型在不同行业的趋势
IBM AppScan OnDemand Premium Service – 2007-2011年

漏洞类型	业务领域									
	金融服务		政府		工业		信息技术		物流	
	每个测试中的平均漏洞数	一个漏洞发生的几率	每个测试中的平均漏洞数	一个漏洞发生的几率	每个测试中的平均漏洞数	一个漏洞发生的几率	每个测试中的平均漏洞数	一个漏洞发生的几率	每个测试中的平均漏洞数	一个漏洞发生的几率
注入	0.1	8%	3.5	50%	10.9	49%	0.6	25%	0.3	5%
跨站点脚本(XSS)	0.4	29%	5.8	75%	13.2	57%	6.1	44%	2.5	74%
破坏的身份验证	5.1	73%	12.7	94%	4.8	84%	26.5	100%	38.9	84%
不安全的直接对象引用	0.3	18%	5.6	94%	2.1	35%	4.8	63%	4.5	47%
跨站点请求伪造(CSRF)	1.1	10%	3.9	75%	3.0	57%	2.3	63%	5.7	42%
安全错误配置	2.9	82%	18.9	100%	25.9	97%	39.7	100%	10.5	74%
不安全的密码存储	4.8	22%	19.4	100%	12.3	51%	39.9	94%	37.1	79%
未能限制URL访问	1.0	44%	14.9	100%	0.9	19%	29.4	81%	15.2	79%
不足的传输层	3.8	25%	1.4	75%	13.6	59%	36.3	88%	34.3	79%
未验证的重定向和转发	0.2	14%	0.2	19%	1.1	46%	0.1	6%	0.0	0%

表9：各个行业中最盛行的Web应用漏洞，IBM AppScan OnDemand Premium Service

应用安全测试周期

在大部分情况下，收集此数据的IBM AppScan服务都提供了对任何测试的应用进行重新测试的选项。通常这次重新测试在初始测试之后的60天内进行，同时并非总是能够在该时间范围内解决所有问题。

无疑可以预测，应用重新测试返回的结果将比第一次应用测试所返回的结果要少。通过查看一个测试中发现的给定漏洞的平均数，就会发现这一差值有多大。对于OWASP 10大类别中的每一个，该差值不会超过一倍。

下图突出显示了在一次性评估和以后的重新测试中，每个测试中找到的平均漏洞数量的差。

测试周期之间的改进
IBM AppScan OnDemand Premium Service
2011年

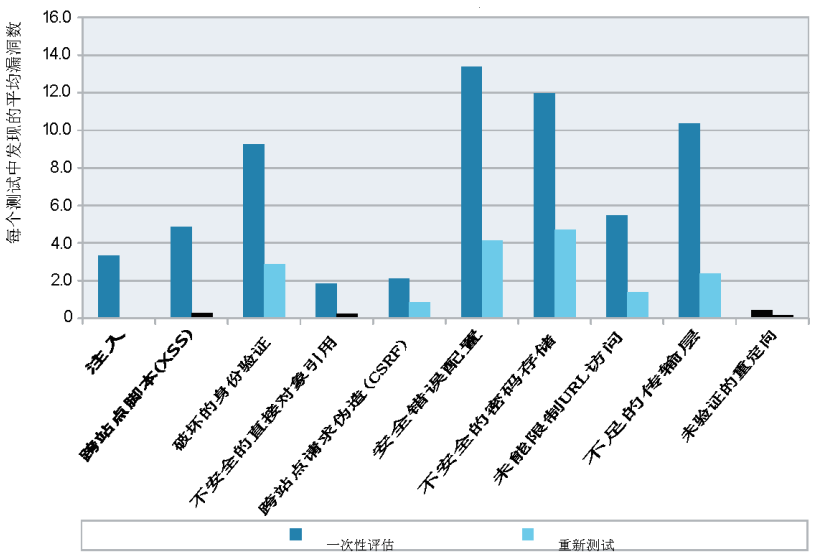


图53：测试周期之间的改进
IBM AppScan OnDemand Premium Service – 2011年

一般而言，我们的客户应重新测试结果以验证问题是否修复。如果初始应用测试操作已足够，那么我们的季度测试将得到与这些重新测试类似的结果。显然不会出现此情况。我们认为，知道应用将很快重新测试可激发开发团队的积极性；否则季度结果将与“重新测试”结果非常相似。此处的另一个因素是，执行季度定期测试的客户可能会受到合规性因素的影响，而不是缓解漏洞的紧迫需求。这表明，最佳实践是始终重新测试，确认各项问题得到了修复。要经济高效地实现此目标，客户应考虑使用内部工具和专家经验。

安全测试周期						
漏洞类型	一次性评估		季度评估		重新测试	
	每个测试的平均漏洞数	一个漏洞发生的几率	每个测试中的平均漏洞数	一个漏洞发生的几率	每个测试中的平均漏洞数	一个漏洞发生的几率
注入	3.3	27%	0.2	5%	0.1	4%
跨站点脚本(XSS)	4.9	46%	3.0	76%	0.3	21%
破坏的身份验证	9.2	82%	36.3	86%	2.9	70%
不安全的直接对象引用	1.8	37%	4.1	43%	0.2	15%
跨站点请求伪造(CSRF)	2.1	34%	5.5	43%	0.8	10%
安全错误配置	13.4	91%	14.1	76%	4.1	79%
不安全的密码存储	12.0	50%	35.7	76%	4.7	14%
未能限制URL访问	5.5	51%	13.9	76%	1.4	38%
不足的传输层保护	10.4	46%	31.0	71%	2.4	27%
未验证的重定向和转发	0.4	23%	0.0	0%	0.2	13%

表10：各种漏洞类型的安全测试周期，IBM AppScan OnDemand Premium Service 2011年

第IV部分

新兴的安全趋势

“新兴的安全趋势”部分介绍一些快速发展的技术，它们正在迫使企业考虑是否到了向这些未来领域进行投资的时机。我们将介绍在这些技术的早期采用中使用威胁和攻击代码的地方，以及企业保持关注的方式。

移动安全与企业 - 年终回顾

移动支持和相关的安全性问题是几乎每个企业的主要关注事项。他们不得不采用越来越高的移动水平，因为技术创新已帮助他们实现了能够提高效率的功能，以及允许几乎所有企业通过移动性驱动的始终连接的工作区加快发展步伐的功能。帮助保护移动设备的最佳实践还处在初始阶段，但这一领域正在不断进步。

帮助保护移动设备的最佳实践缺乏清晰度，这也让许多采用或至少推动以前从不允许或支持的自带设备(BYOD)计划的许多企业的情况变得更糟。由于越来越多的员工拥有这样的设备，高管和员工都对推进此计划充满了兴趣，而由于安全问题，企业的CISO常常是

发展的主要阻碍。尽管许多CISO继续在说“不”而不是说“如何做”，但有迹象表明此方法可能导致用多个项目来检测和预防员工绕过现有基础设施来提高自身能力。显然这不是企业希望自己处于的位置，采用的方法是通过关注数据元素的分类来支持并控制移动设备的有限使用。

对于努力确定需要哪些控制方法的企业，对与所讨论的数据元素相关联的现有安全需求进行合理分析，可增加一定的清晰度。这种关注数据的方法利用了现有的安全标准，最终将形成各种移动安全最佳实践。在许多方面，这只是一种保护任何计算设备上各种数据的常识方法 – 而且我们无疑都认识到如今的智能电话和平板电脑就是计算设备。

对于某些行业，这可能意味着BYOD方法：它们让个人拥有的移动设备上存在的一些数据元素变得不合适。它真正关心的是正在考虑支持的数据，然后应用相关的、必需的控制。

移动恶意软件可视性在去年已出现显著增长。一定要在企业面对的整个威胁形势的上下文中查看此趋势。已有许多主流IT媒体文章重点介绍了移动领域独有的恶意软件攻击，这些文章会导致用户相信移动领域比传统Windows XP威胁的领域状况要好。当然，这可能离事实并不远，但它提供了一个不错的数据点，因为移动恶意软件正在增多，而且必须为这一挑战制定合理的安全计划。

与移动设备相关的恶意软件不是去年增多的唯一数据。显然，新的移动管理解决方案（通常称为MDM或移动设备管理解决方案）似乎每周都在出现。这是可预见到的，而且就像许多技术创新专注于移动空间一样，这应该导致对这些解决方案有更高的需求和机会。选择和竞争始终对客户有利，会提高一些具有合理价格的解决方案涵盖企业所需的所有安全控制需求的几率。在以后，安全隔离或分离解决方案的数量也会增多。这些方案有时称为数据泄漏解决方案，但在移动上下文中，它们与针对工作站的传统DLP解决方案有很大区别。尽管这些解决方案带来了能够更好地解决BYOD计划中员工拥有设备上各种企业数据和应用问题的最终承诺，但大部分都相对有限并且在目前还不太成熟。

移动恶意软件视角

我们对去年移动恶意软件威胁形势变化的分析发现，它日益成为一个关注领域。在某些方面，这带来了一定的好处，让IT高管知道预计结果的实际可能性，让企业能够计划合适的控制。以前的X-Force趋势和风险报告的读者可能已注意到，IBM已在关注和预测这些增长。

值得提一下去年曝光的移动恶意软件威胁的性质。在几乎每个案例中，它们都存在并且在被视为合法、与移动平台关联的应用商店中提供给设备。还值得注意的是，这发生在所有主要的移动平台和商店中，并不局限于某个平台和商店。这一现象的重要性有多个原因。随着几乎所有应用商店的应用选择激增，审核所提交内容的效率并未增加

（除了下面将强调的Google应用市场），并且我们开始看到此情形的后果。另一个重要方面是，大部分设备所有者（和企业员工）都期望将应用下载限制到合法的应用商店会阻止恶意应用。这是一个谬论。

公平地讲，流行应用商店的管理者肯定在用反应式的方法响应恶意应用的出现并删除它，但这常常是在许多用户下载之后，并且这只是反应式的。避免大部分无法撤销现有应用的第三方应用商店也是一种最佳实践指南。可以想象，随着监督力的下降，遇到恶意应用的几率就会增长。还没有什么有效的模型供安全研究人员向管理者提供认知，因为它没有提供方法将其研究转化为资本。不幸的是，由于我们假定了应用商店模型代表着信任，所以用户和企业才是真正的受害者。

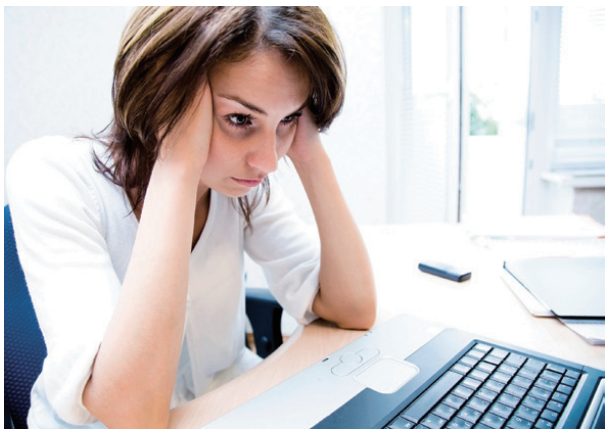
为了帮助企业解决此问题，安全供应商提供了越来越多的恶意软件预防方法。尽管许多企业最初忽略了这一需要，但越来越多的企业已接受移动恶意软件将继续增多的事实，并为制造大部分恶意软件的犯罪企业提供了更多的机会（和对企业的威胁）。这些解决方案可用于大部分平台，而且随着市场决定哪些平台将幸存下来，平台覆盖将变得越来越容易。

如果没有必需的检测，一些恶意应用将不会被设备用户检测。我们应强调部分恶意应用，因为其他执行欺诈性交易的恶意应用在用户查看其每月账单时就会被检测出来。与个人计算机恶意软件一样，金钱攻击仍然是一个主要的关注点，支持SMS的移动设备提供了极富吸引力的目标。

由于移动设备的性质（它们通常拥有GPS硬件，以及语音、消息和数据服务），我们观察到的另一个比较独特的实际示例是：我们检测到存在监视用户行为多个方面（包括记录位置、消息、电子邮件和语音呼叫供攻击者审核）的间谍应用。与我们在个人计算机上看到的攻击类型相比，这特别令人不安。因为移动设备真正已成为“您口袋里的办公室”，它们为间谍攻击提供了大量机会。

最近，Google公开一个应用审核功能的实现，开始对其应用市场中以前被接受和维护的应用执行安全监督。这非常值得注意，因为它向主动改善其商店中各种应用的安全性迈出了一步，是其他应用商店管理者学习的榜样。尽管应该预料到这不是很完美，并且可能是Google与试图提交恶意应用的人之间的猫捉老鼠游戏，但它明显是要对保护用户远离恶意应用所采取的操作和需求的声明。时间将告诉您其他应用商店所有者/管理者是否会跟进。

对于移动恶意软件，应该关注的一个风险区域是移动操作系统的流行。尽管我们未看到底层平台漏洞导致铺天盖地的恶意软件攻击在移动操作系统之间自我复制，但这种事的发生可能只是时间问题，毋庸置疑，某些平台在解决此问题上比其他平台做得要好。从单纯的企业角度讲，几乎所有可用的MDM解决方案都支持基于操作系统版本来控制企业信息的同步（进而允许企业中断对存在漏洞的未修复操作系统版本的支持）。这可能会让企业员工感到受挫，他们可能遇到了运营商的这种支持问题（尤其是在BYOD计划中，通常无法像企业提供的具有合同控制的计划那样全面管理各种型号和运营商）。我们可能会在不久的将来看到，员工和设备所有者艰难地使用不受其企业支持的有漏洞的设备，他们的唯一选择是在完成当前合约之前升级设备，



这时有补助的合约型号就会流行。许多人怀疑硬件OEM特意让设备在支持上落后，迫使设备所有者更频繁地升级。这个具体的问题可能在一定程度上证明了用户接受程度上的一种挑战，因为它与用户所接受的其他用户计算设备（如笔记本电脑）型号有很大区别。

BYOD和安全隔离

前面已经强调，今年一项最新的发展是人们更多地关注可提供将企业应用和数据与员工个人应用和数据隔离的能力。显然，此发展的主要推动力是移动设备的普遍存在和对BYOD计划的兴趣。尽管在今年以前就存在一些解决方案，但选择仍然很少，而且大部分解决方案在功能和适用性上有限。在过去的一年中，这一领域的解决方案可谓百花齐放。我们应预计，大部分都有待完善，或许每个解决方案都有其自己的限制、适用性特征和实现阻碍，但它们显然表明这一问题已被认识到，同时整个行业都已听到和认识到企业的需求。这与去年相比是很大的进步，当时这些解决方案只是被特定行业使用的机会性产品，因为相关企业对哪些数据可到达员工的移动设备进行了非常具体和严格的控制。

随着这一市场领域日益成熟和不断改善，我们预计会看到解决方案分为两个不同的类别。Android领域正在执行一些活动和集体工作来打造一些使用基于硬件虚拟化的方法。此方法的创建进度受限于是否广泛采用这种芯片级功能，然后相应地采用和支持全球大量运营商所运行的不同设备，这样它才能成为大型跨国企业的有效方法。尽管这可能需要24到36个月才会广泛发生，但这一“运动”无疑正在进行，因为芯片制造商、硬件OEM和运营商认识到这种企业需求和相应的市场机会。我们将会关注此方法是否会大量普及，以适用于大型企业中的BYOD方法。

与此同时，一些支持隔离（无论是通过容器、虚拟容器还是资产管理方法）的解决方案正在填补早期采用者的空白。这些方法让企业能够对员工设备执行一定的水平隔离和其他控制，而无需继续控制整个设备，但仍然需要实际工作来确定在设备级别上需要哪些控制，从而将它当作隔离解决方案的宿主。尽管同样的问题也适用于上面提及的虚拟化方法，但同一个移动操作系统实例内的应用容器或隔离方法更可能存在恶意软件或恶意应用。这是另一个还未定义最佳实践的领域，但随着企业采用这些解决方案并执行了所需要的安全技术测试，公认的实践可能就会出现。

设备管理与基于角色的企业相融合的重要性

随着企业中移动设备的使用率继续激增 –无论是纯企业拥有、员工拥有还是二者混合拥有 – 在企业风险管理上下文中管理它们的需要将变得越来越重要。在采用其他计算设备（如笔记本电脑）的竞争产品时尤其如此。在笔记本电脑、平板电脑和智能电话方面，用户与设备的比率很可能达到每个员工两三台设备。这将意味着企业数据的分布可能会继续增加，并挑战着基于角色的安全配置文件和企业风险管理的使用。

随着企业寻求基于角色的用户安全配置文件问题的解决方案（这些配置文件为与特定用户角色相关联的数据角色和类型量身定做），此方法将变得更加困难，因为设备管理分散在多个设备管理解决方案

上。事实上，随着企业摆脱在纯企业提供的计算计划中存在的全能程序，而依赖于管理BYOD计划中通用的更多操作平台，这种将设备管理融入到单个平台的能力可能成为在合理成本内推广BYOD的主要因素。对于更小的相似企业，由于缺乏大量不同的角色和在大部分人群中使用了相同的数据分类，这种情形可以避免。它们能够让两个解决方案（或许一个用于标准计算资产，一个用于智能电话和平板电脑的移动资产）共存，但对于大型企业，这可能是一种严重的限制，最终导致满意度下降。想象一家大型企业必须保护所有资产（无论是否为移动的），

以满足特别敏感的合同、客户或项目所需的最高安全水平，因为他们无法跨员工使用的不同类型设备有效地实现多个角色。最后，效率的损失和无法为不同角色支持最佳的设备规格，会真正导致人们必须寻求统一的平台来管理所有端点设备。

融合所有端点设备管理的第二个且同等重要的原因是，集体可视性和企业风险管理的需求。尽管完全有可能将不同的管理系统结合到单个企业风险控制台中，但如果这可受到单一框架技术的支持，就会容易得多并且更可能获得成功。而且更可能将这个单一平台整合到高级持续威胁(APT)分析和响应中。

基本来讲，对于大部分担忧高级持续威胁的企业，将操作分析和分析学结合在一起，使其包含端点状态、信息以及与端点系统实时交互的能力，这会成为提供封闭的检测/响应生态系统的能力基础。要使用良好定义并受控的安全策略来一致且程序化地管理所有端点，选择正确的安全管理技术应该就可以轻松完成，并提供高效率和监督功能来改善整个企业的安全状况，方法是专注于整个端点群体。

回顾云中的安全状态

对于云环境中的安全状态已讨论得太多了，组织已开始寻找答案，尝试理解如何采用云解决方案并确保其安全。随着越来越多的组织考虑采用云，安全仍然是最重要的优先事项。许多组织仍然在犹豫是否将业务关键型应用迁移到公共云，并在许多情况下选择了利用私有云。这种想法类似于Internet诞生之初时的情况，许多组织对将业务关键型应用迁移到这个"新"网络犹疑不决，因此转而依靠专用网络（常常基于租用的线路）。就像规模经济最终将一些最重要的业务应用推到Internet上一样，同样的转变正在云计算中发生。问题不是云是否更安全，而是应使用哪些具体的控制和业务流程来帮助减少风险，确保云环境中的安全。对于寻求更广泛地采用基于云的基础设施的任何组织，重要的是在考虑到安全和风险减轻时理解组织的角色，而不是云服务提供商的决策。

与任何业务关键型应用或服务一样，业务组织应确保特定于组织的风险与服务提供商提供的策略和规程协调一致。在采用任何新Internet技术时应遵守安全最佳实践，而云计算没什么不同。考虑任何云部署时，思考跨所有云部署阶段的安全性很有帮助。

为云采用安全保护

许多组织拥有的一个疑问是，基于云的应用和服务是否比传统Internet和内部网应用更安全。尽管没有一个部署场景提供了更高的内在安全，但一个共同的发现是，在考虑基于云的部署时安全性是一个较为重要的关注区域。通常，服务被视为在组织的信任边界内部时，组织的应用和服务部署会受到更多信任。显然，单单一次围绕安全的转变不足以实现更高的安全性，但是因为在考虑云部署时安全是首要因素，所以在许多云应用和服务活动中常常会看到有关安全的严格控制、流程以及规程。

设计考虑因素

应拥有并遵守企业安全开发实践。考虑第三方云应用提供商时，确保他们的安全开发标准和实践满足或超出您自己的需求，这一点很重要。

应具备适当的网络和端点安全防护。在多租户环境中，如果没有适当的安全专区和数据隔离流程，一定要确保敏感和关键的应用没有共享同一个虚拟机管理程序。

理解数据安全需求。组织、政府以及适用的标准和制度对许多利用敏感和隐私信息的应用制定了严格的安全需求。您必须确保云服务提供商充分满足了这些需求。

部署考虑因素

以管理非虚拟端点的方式管理虚拟端点。重要的是，在补丁和配置管理方面，虚拟库和目录不会受到“安全偏移”的影响。

跨云和非云环境一致地执行安全控制。确保部署到虚拟环境中的应用受到了与公共Internet应用相同的安全监督 – 尤其是常常缺乏基本安全控制的开发和测试环境。

定期扫描所有云应用。利用源代码和动态应用服务限制部署到云中的任何应用的安全暴露面。

使用考虑因素

适当的身份和访问管理。相应地行使身份和访问权限，在考虑到第三方云SaaS服务时考虑身份联合。

日志和安全事件管理。拥有有效的虚拟设备日志和安全事件管理。

数据取证。如果考虑第三方，理解如何在发生安全事故时管理数据取证。

遵循安全设计方法是在迁移到基于云的基础设施时，可帮助您实现更高安全性和减少风险的最佳方式。迁移到云对许多IT组织有着很大的吸引力，而且由于缺乏控制，所以在安全方面更加重视最前线的安全。在许多情况下，高度关注如何解决您无法完全掌控的环境中的各种挑战，会带来更高的安全性。即使基础设施的细节不太透明，坦诚地讲，结果也可能是模糊的、更高的安全性。

通过SLA改善云安全

简介

对云中的数据违规而言，2011年是重要的一年。许多大型知名组织都被攻击，数百万条用户记录处于风险之中，2011年第一季度对一个大规模云实体的破坏带来了连锁反映，影响到了零售商和金融机构的客户数据库，随后他们的用户财务记录被曝光。2011年被IBM X-Force称为安全违规年，让许多组织怀疑云计算是否能够得到合理的保护。

安全云计算中的成功不仅仅是一个简单的联系人管理问题，它是云部署的成功关键。人们编写的标准合同和服务条款(TOS)通常对云提供商有利，定义了基本的服务和限制曝光与责任。云供应商很少修改它的标准合同来适应客户组织的需求。服务水平协议(SLA)是更加灵活的文档，允许客户组织定义其业务模型所独有的需求、法律和制度需求，或者其他考虑因素。不幸的是，云计算的性质（灵活性、可扩展性和快速部署能力）可能导致难以构建和维护有意义的SLA。

要考虑的问题

由于组织可在云计算环境中真实体验到的影响有限，所以管理信息安安全最有效方式可能是通过SLA。因此，组织在其方法中采取主动并从尽可能长远的角度审视其每个云计算项目，这很重要。有太多的早期采用者只看到了眼前的利益，主要关注供应商的选择和服务启动，而没有考虑生命周期管理和退出战略。

恢复能力是大部分云SLA的核心，云供应商常常关注的是其标准服务声明。恢复能力包括对正常运行时间、性能和响应时间、错误更正时间等的保证。有的可能还包括多租户情形中的划分和隔离等问题，或者变更管理策略和规程。标准SLA往往仅包含与信息安全相关的一般表示。组织必须仔细审视提供作为标准服务的策略、规程和控制措施，然后在每个特定的工作负载将要处理、传输或存储的数据的推动下，为这些工作负载创建自定义需求。

对于长期、有效的信息安全管理，组织在创建SLA时应考虑以下因素：

- 所有权。在将任何敏感或关键的数据、流程或知识产权交到云提供商手中之前，组织应扫描云提供商的标准合同、TOS、SLA和其他文件，查找与应用、功能、数据集或由云活动带来的相关工作产品的联合或直接所有权相关的任何规定。组织应以书面形式保证它保留了向云提供商公开的数据或资产的所有权，以方便将该资产转移到另一家服务提供商或随时收回该资产。这对使用基于云的功能即服务(XaaS)的任何组织尤为重要。如果组织需要在内部启动项目或将项目转交给另一个提供商，那么就无法轻松地复制供一个云供应商专用的软件和流程。如果在事后发现组织作为服务条件而放弃了其资产的部分或全部权利，会让困难的情形将进一步恶化。
- 访问管理。就像组织为内部敏感或关键数据的授权用户设定限制一样，它应该监督云环境中所部署的访问管理策略和机制。云提供商的人员对组织数据的具体访问管理需求应取决于工作负载的独特需求。但是一般而言，组织应透彻理解在云提供商的有效生产环境中如何应用最低特权原则。这在多租户公共云环境中无疑至关重要。就像每个租户的部署应在共享的承载环境中相互隔离一样，访问应限制（在合理的程度上）到一组指定为向客户组织提供服务的技术员工。这依赖于云提供商的业务模型，但组织必须准确理解云提供商如何管理对租户环境和数据的物理、逻辑、远程以及新出现的访问。组织应评估工作负载中各种数据的法律和制度需求，确保云提供商理解并可满足这些需求，以及提供善意的工作可论证证据。下一部分将更详细地探讨云中的访问管理。
- 治理。云提供商如何就其信息安全状态和功能做出表示，这应该是组织在确定适合工作负载的云类型和提供商时的重要因素。组织应检查云提供商公开的任何文档中的信息安全功能，包括编写的审计报告或摘要（如SSAE 16 SOC 2报告或SOC 3封条）、认证（如产品环境的ISO 27001登记）或其他与合规性标准（如BITS Shared Assessments AUP或COBIT）有关的一致性文档。组织应陈述它访问提供商的这些文档的需要，以满足任何法律和制度需求。组织应与云提供商协其SLA：
  - 验证安全培训和认识技术员工。
  - 访问与租户环境直接相关的日志和监视信息。
  - 在安全违规事件中记录的安全责任和职责。存在复合SLA时这尤为关键。

– 出于用户通知和法律调查的用途，访问与数据违规相关的取证信息。

– 介绍云提供商将如何响应执法部门对信息、调查、传票等的请求的文档。

- 终止。大部分云提供商的标准合同和TOS声明都包含与提供商因故（如未付费）或客户方因故（如未能满足正常运行时间保证）而终止合同的相关规定。除此之外，组织应检查这些标准文档中是否有任何其他的合同破坏条件，应该明确定义退出战略，以防提供商提供的服务或提供商能力发生实质性的更改，或者它自己的业务模型发生更改，或者只是由于云项目失败。组织应保留终止其与提供商的合同的合理权利，而避免遭致不合理的罚金包括：

– 更改云提供商的业务模型，如在启动服务活动后引入复合SLA，而没有充分通知或为组织提供采取适当行动的机会。

– 更改云提供商的所有权，如并购。

– 显著更改费用而没有充分通知。

– 取消或显著更改服务而没有充分通知。

理想情况下，组织应计划终止其云服务，留出足够的时间来实施过渡计划。当然，前提是组织已制定了一个书面过渡计划。具体原因可能取决于工作负载、云类型和提供商绩效，但云部署可能由于许多原因而失败 – 预期的成本节省从未真正实现、项目太难以在外包情形下管理、产品或服务本身发生故障等。无论组织有什么原因，它都应有一个退出战略，计划好如何满足将项目迁移到另一个外包提供商或收回职能的需求。已备案的过渡计划应包含：

- 记录的对云提供商有利的终止原因。
- 足够的过渡时间，以防职能或服务最初没有设计为功能完备的。
- 过渡帮助，包括数据格式和从云提供商转移回组织中。
- 返回属于组织的所有数据和资产，包括备份。
- 云环境中残留数据的安全处置和/或销毁，包括备份。
- 数据加密所形成的难题可能带来哪些意外事故。

显然，这不是组织应考虑的问题的全面列表。工作负载的具体需求可帮助组织选择最合适的云类型（公共、私有、混合或托管）以及最合适的供应商来提供云服务。这些考虑因素依赖于组织部署到的云模型类型。例如，当组织部署到私有托管云时，多租户环境中的隔离不适用。但是一般而言，这些是常常被忽略的关键问题，组织应该计划和记录这些因素才能成功地管理自己的云部署。

小结

云计算正在快速从新兴技术转变为主流技术，其快速增长预计会持续到2013年末。云技术的早期采用者提供了宝贵的教训，尤其是在信息安全问题上。从长远角度审视任何已提议的云计算项目，小心地审核工作负载所规定的服务和安全需求，这样组织即可选择合适的云模型和提供商。

协商严格且受欢迎的SLA可能是该任务成功的关键，会为参与的各方带来好处。此工作需要仔细规划，避免那种具有标准的、不可协商的条款且没有商量余地的标准协议。如果云提供商不愿意协商SLA，他们可能不是部署的合适提供商。SLA应具有具体的期限和范围，只有在正确告知后才能更改，而且认识到了组织的具体业务和信息安全需求。SLA可视为一个被动的工具，但它们可能是在外包环境中管理和维护有效安全状态的最有效方式。

云中的身份和访问管理

云环境中的安全挑战

借助其灵活性、经济高效性和可扩展的“按需”模型，云计算变得越来越流行。与各个部门、合作伙伴和客户共享服务和信息的能力是云计算的一个主要优势。作为一项附加优势，云计算可增强用户的体验而不增加复杂性。用户不需要知道有关底层技术或实现的任何信息。

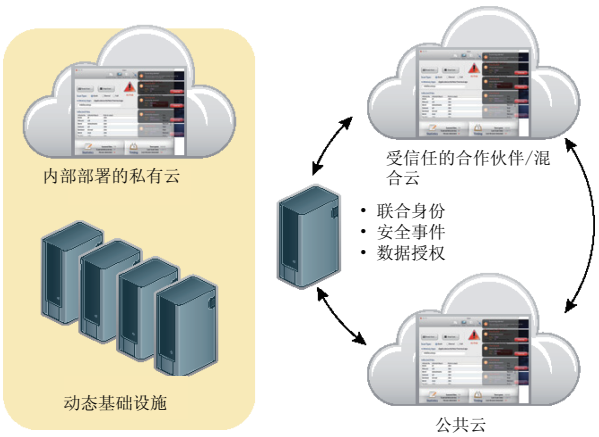
尽管云计算的优势很明显，但在云实现中开发合适的安全性的需求也很明显。随着越来越多的组织正在采用或考虑云计算，他们也在担忧相关的安全风险。IBM商业价值研究院举行的一次全球风险调查发现，云计算带来了对数据访问、使用和控制的高度担忧：77%的回复者认为采用云计算会使隐私保护变得更加困难；50%的人担忧数据被破坏或丢失；23%的人担忧企业网络安全变弱。

数据和应用常常承载于公共域上，所以访问管理成为一个关注点。云计算会像数据中心一样安全吗？当业务部门开始结合使用公共云服务和数据中心或私有云时会发生什么？您如何确保只有授权的人在访问您的敏感数据和应用？您的云提供商能够提供审计报告来证明您对行业和政府制度的合规性吗？解决这些问题是成功实现云安全的关键。

组织应平衡关键资源的保护、隐私、治理和可访问性 – 无论在传统数据中心、私有云还是在公共云中。云计算需要巧妙地平衡共享资源的需求与保护这些资源远离未授权访问、数据泄漏和其他信息曝光的需求。显然您不希望不适当的个人访问您组织的私有数据和应用。要帮助确保公司的IT资源是安全的，无论它们位于何处以及何时需要它们都是如此，并且身份和访问管理必须内置到云结构中。

云中的安全需求不应被忽视或“拖延”到过渡期间的末期，而应内置到总体的云实现计划中。这些计划可能要包含对业务流程和策略的更新，因为云安全需要的不仅仅是技术。就像传统安全环境一样，组织应同意备案和对云环境执行安全指令，以满足其业务和制度目标。这些指令可能包含与云提供商的服务水平协议、各种云用户组的职权分离需求，以及创建“信任专区”将数据与共享相同物理硬件的其他云客户相隔离。

对基于云的应用和服务访问进行保护
企业IT组织



借助身份和访问管理(IAM)解决方案，组织可集中控制大量用户对外部提供商（如salesforce.com）承载的、基于云的服务的访问。

针对云的身份和访问管理(IAM)解决方案

无论您决定将哪些应用或信息迁移到云，可靠的身份和访问管理(IAM)解决方案都应先行。它可同时涵盖云和传统计算环境，所以您无需管理两组凭据。主要目标是帮助确保授权用户能够在需要时访问他们需要的应用、数据和工具，同时阻止未授权的访问。借助仅允许已授权和合适用户才能访问的能力，IAM解决方案是任何云安全计划中一个具有重要价值的组成部分。

借助IAM解决方案，您可为谁可在何时、从何地访问何种信息，以及他们可在设定的时间段内访问多少信息来设定并实施各种策略。您可使用该解决方案来不断重新确认授权，在必要时迅速撤销授权。还应有工具可用于监视、报告和主动防御策略违规现象。

与在传统IT环境中一样，针对云的IAM解决方案应合并以下功能：用户配置（包括职权分离、基于角色的访问控制和细粒度授权）、密码管理、Web和联合单点登录、日志记录，以及审计报告功能。最后，特权身份管理特别重要，故意或意外的内部人员破坏可能会带来灾难性的损害。

借助身份和访问管理(IAM)解决方案，组织可集中控制大量用户对外部提供商（如salesforce.com）承载的、基于云的服务的访问。

云将服务、应用和资源扩展到了一个庞大、多样化的用户群体，这个群体可能包含来自受信任和不受信任的外部位置的员工、客户和合作伙伴。组织应将基于云的应用与内部应用紧密结合，让用户能够通过单点登录轻松访问它们。必须拥有身份联合以及快速启动的能力，从而协调企业的后端或第三方系统的身份验证和授权。联合身份管理提供了一种方法来管理云中的和传统计算基础设施中的身份与访问。它还可简化云自助服务环境中的配置。基于标准的单点登录功能简化了内部承载的应用和云的最终用户登录工作，让最终用户能够轻松、快速地利用云服务。

在典型的场景中，用户的身份验证在云外部进行。然后将用户的身份联合到云中。整个过程是对用户是透明的。单点登录功能让用户能够直接访问基于云的应用和信息，无需在云中管理身份。

对于合规性，组织应拥有企业级功能来帮助确保内部和外部访问都受到有效身份验证的控制，监视授权和网络流量，以及通过完备的审计和报告功能来支持系统。无论用户类型是什么，解决方案都应加强安全性，帮助填补安全措施中的空白。它应减轻威胁风险，如欺诈、知识产权盗窃或客户数据丢失。它应帮助降低成本，简化并加速向用户授予资源访问权限的业务和IT流程。

总之，身份和访问管理提供了提高用户生产力的切实的运营收益，还减少了安全违规风险。自动化的身份和访问管理(IAM)解决方案可应对各种云安全挑战，同时涵盖云计算和传统计算环境。

© 版权所有 IBM Corporation 2012
IBM Corporation Software Group Route 100
Somers, NY 10589 U.S.A.
在美国印制
2012年3月
IBM、IBM徽标、ibm.com、AppScan、Guardium、InfoSphere和X-Force是国际商业机器公司在美国和/或其他国家（地区）的商标或注册商标。如果上述及其他IBM商标词汇在本文中第一次出现时标记了商标符号（®或™），均代表在本文出版之际，它们是IBM在美国或其他国家注册的商标或普通法规定的商标。这些商标也可能是其他国家/地区的注册商标或普通法规定的商标。有关IBM商标的最新列表，请访问ibm.com/legal/copytrade.shtml的“Copyright and trademark information”部分。
Microsoft和Windows是Microsoft Corporation在美国和/或其他国家（地区）的商标。
其他公司、产品或服务名称可能是其他公司的商标或服务标记。
本文中与非IBM产品相关的信息是从这些产品的提供商、发布的公告材料或其他公开来源获得的。有关非IBM产品功能的问题应提交给这些产品的提供商解决。
本文仅在初始发布之日是最新的，随时可能由IBM更改。不是所有产品都可用于IBM运营的每个国家（地区）。
所提供的性能数据和客户示例仅用于演示。根据具体的配置和操作条件，实际性能结果可能有所不同。通过IBM产品和程序来评估和验证任何其他产品或程序的操作是用户自己的责任。
本文中的信息“按原样”提供，不含任何明示或暗示的担保，包括但不限于任何适销性担保、特定用途的适用性和非侵权性的任何担保或条件。IBM 产品的担保依据的是它们所遵循的协议中的条款和条件。客户应负责确保遵从适用的法律和制度。IBM不提供法律建议，也不表示或保证它的服务或产品将确保客户遵守任何法律或制度。与IBM未来方向和意图相关的陈述随时可能变更或收回，恕不通知，而且仅代表目标和目的。
第三方数据、研究和/或引用材料的使用不代表IBM对发布组织的认可，也不一定代表IBM的观点。

请回收利用

WGL03012-CNZH-00