美洲总部
Cisco Systems, Inc.
San Jose, CA

亚太总部
Cisco Systems (USA) Pte.
新加坡有限公司

欧洲总部
Cisco Systems International
BV 荷兰
阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices 中**。

思科 2013 年度安全报告

生活在当今的“任意互联”世界。

在当今“任意互联”的世界，个人可以使用任何设备访问利用分散化的云服务，访问网络环境中的商业应用网络。犯罪分子正是利用了其中快速扩大攻击面这一点。《Cisco® 2013 年度安全报告》基于真实数据，强调全球威胁发展趋势，并提供见解和分析，帮助企业和政府改善未来的安全形势。本报告将专业研究和汇集整个思科公司的安全智慧相结合，着眼于 2012 年收集的数据。

目录

设备、云和应用的中心

任意互联世界和“万物互联”是对连接性和快速展开的协作的变革。它是设备、云和应用的中心。

此发展并不超出预想。但从安全的角度来看，如今的企业可能尚未做好准备来应对“任意互联”的现实。

“任意互联”问题的核心是：我们正快速迈向这样一种情况，即用户越来越少地通过企业网络访问业务，”思科安全和政府组副总裁 Chris Young 是说。“它越来越和在开始影响网络的任何实例化的位置的任何设备有关。启用互联网的设备（智能手机、平板电脑等等）正试图连接到可以随处运行的应用上。”

与此同时，另外一种趋势也正在发展当中，这就是稳步迈向“万物互联”的趋势。它可以智能连接：

- **人员：**社交网络、人口中心、数字实体
- **过程：**系统、业务流程
- **数据：**万维网、信息
- **物品：**物理世界、设备和对象

> “它越来越和在开始影响网络的任何实例化的位置的任何设备有关。启用互联网的设备（智能手机、平板电脑等等）正试图连接到可以随处运行的应用上。”
>
> Chris Young，思科安全与政府业务高级副总裁

“互联网上人员、流程、数据和物品的不断增长和相互融合，将使网络连接比以往任何时候都具有更大的价值和相关性。”

思科杰出的工程师 Nancy Cam-Winget

“万物互联”的概念是建立在“物联网”[1]上的。它添加了网络智能，可将以前分离的系统进行融合和协调，并提供可见性。“万物互联”的连接不仅指移动设备或笔记本电脑和台式机之间的连接，还包括快速增长的每日在线的机-机交互 (M2M) 连接。这些“物品”通常是我们习以为常或日常依赖的物品，我们通常认为它们是不应该连接的，比如，家庭采暖设备、风扇或轿车。

“万物互联”是一种未来的状态，但说到“任意互联”的问题时，似乎就不那么遥远了。“任意互联”会为企业带来安全要求，同时也会带来新的机遇。“随着‘万物互联’的发展，将会发生一些有趣的事情，”思科的杰出工程师 Nancy Cam-Winget 说。“互联网上人员、流程、数据和物品的不断增长和相互融合，将使网络连接比以往任何时候都具有更大的价值和相关性。”最终，‘万物互联’将为各个国家、企业和个人，带来全新的功能，更丰富的体验和前所未有的商机。”

云是如何使安全问题变得复杂化的

保证各个应用、设备和用户安全 – 无论是在“任意互联”还是在“万物互联”环境下 – 均变得越来越严峻，原因是云已经成为管理企业系统的一种工具，越来越普及。根据思科汇总的数据，全球数据中心流量在今后五年内有望增加四倍以上，发展最迅猛的元素就是云数据。截止到 2016 年，全球云流量将达到数据中心总流量的近三分之二。

全球数据中心流量预期会在今后五年内增长四倍，增长最快的元素就是云数据。截止到 2016 年，全球云流量将达到数据中心总流量的近三分之二。

林林总总的安全解决方案（如，将防火墙用于可变的网络边缘）并不能保证设备、网络和云中不断移动的数据的安全。即使在数据中心里（其中存放着组织的“重要的资产”[大数据]），虚拟化正在逐渐成为一种常规而非特例。要应对虚拟化和云带来的安全的挑战，需要根据这种全新的模式来重新思考安全状况 – 需要改变基于边界的控制以及旧的访问模式，以保证新业务模式的安全。

互联的工人和数据隐私

在“任意互联”模式中，另一个复杂的因素是年轻一代的移动办公族。该群体认为：无论走到哪里，无论手头有什么设备，他们都应能把业务带到哪里。本年度的《2013 思科年度安全报告》包含《2012 思科互联世界技术报告》的调查结果。这是一个基于在 2011 年针对全球大学生和年轻专业人员对工作、技术和安全态度的转变进行的研究所做的调查。

最新的研究更加关注移动办公族对待安全的态度，尤其关注隐私和公司对员工在上班时间自由上网的意愿的干涉程度和频率。《2012 思科互联世界技术报告》研究也调查了网络隐私是否仍然是所有用户非常担心的问题。

在“任意互联”模式中，另一个复杂因素就是年轻的移动通信行业的工人。这群人认为：无论手头有什么设备，无论走到哪里，他们都能把业务带到哪里。

数据分析和全球安全趋势

《2013 思科年度安全报告》涉及在思科进行的研究基础上对网络恶意软件和垃圾软件趋势的深度分析。近年来，许多“地下经济”从业者在集中精力开发日益精密的技术，而思科的研究表明，网络犯罪往往借助众所周知的简单的方法来危害用户。

去年，分布式拒绝服务 (DDoS) 攻击数量增加，这只是网络犯罪“换汤不换药”趋势的一个例证。分布式拒绝服务攻击可以使互联网服务提供商 (ISP) 无法正常工作，并干扰往来于目标网站的流量。近几

“我们看到政府、公司和社会面临的网络威胁环境正发生一些令人不安的变化。”

John.N. Stewart，思科高级副总裁兼首席安全官

年来，该类攻击一直是不被众多企业所重视的 IT 安全问题。然而，最近几起针对知名企业 – 包括美国金融机构[2]的攻击活动提醒我们：如果一个企业不未雨绸缪，那么任何网络安全威胁均有可能造成重大破坏，甚至是无可挽回的损失。因此，在制定业务连续性管理计划时，企业考虑如何应对破坏性网络事件并恢复正常运营是明智之举 – 无论该事件是否采取针对公司的分布式拒绝服务攻击的方式；还是启用互联网的重要制造设备突然宕机事件；还是犯罪分子秘密进行的高级多阶段攻击；亦或是前所未有的其他事件。

“在过去几年里，IT 安全讨论经历的不只是其人人有份的危言耸听，我们看到政府、公司和社会正面临网络威胁环境一些令人不安的变化”，思科 高级副总裁兼首席安全官 John N. Stewart 说道。“网络犯罪不再令人烦恼，也不再是企业经营所要付出的另一个代价。 我们正接近网络犯罪造成的经济损失即将超过信息技术创造的经济效益这个临界点。显然，我们需要新的思路和方法，来降低网络犯罪对全球正常运行造成的损害。”

终端激增

“任意互联”的发展已经涉及到数十亿通过互联网连接的设备；2012 年，全球这些设备的数量已增加到 90 亿以上。[3]

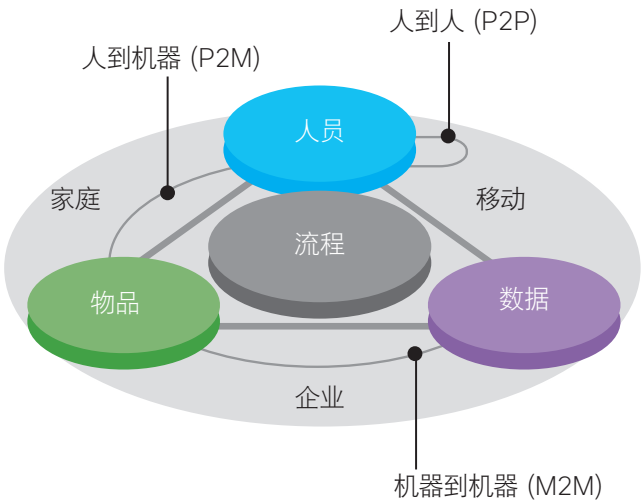
鉴于现在现实世界里只有不到 1% 的事物完成互联，“连接未连接的事物”的潜力仍然巨大。[4] 预计到 2020 年，通过已和约 500 亿“事物”连接的互联网，连接的数量将增加到 13,311,666,640,184,600。增加一个和互联网连接的事物（500亿 + 1），连接数量就将增加 500 亿。[5]

至于最终构成“万物”的具体“事物”，它们包括智能手机、家庭采暖系统、风轮机和车辆等。思科的首席未来畅想家、互联网企业解决方案小组的 Dave Evans 是这样阐述终端激增这个概念的：“日后当您的车辆与‘万物互联’相连接时，它只不过使互联网上的事物数量增加一个。现在，想想您的车辆能够连接的不计其数的其他元素 – 其他车辆、红灯、您的住宅、服务人员、天气预报、警告标志，甚至道路本身。”[6]

在“万物互联”上，连接是最重要的。在人、流程、数据和事物之间创造价值的是连接的类型而不是数量。但最终，连接数

> “日后当您的车辆与‘万物互联’相连接时，它只不过使互联网上的事物数量增加一个。现在，想想您的车辆能够连接的不计其数的其他元素 – 其他车辆、红灯、您的住宅、服务人员、天气预报、警告标志，甚至道路本身。”
>
> David Evans，思科首席未来畅想家

图 1: 万物互联
万物互联 (Internet of Everything) 是指人、流程、数据以及事物的智能连接。



在“万物互联”上，连接是最重要的。在人员、流程、数据和事物之间创造价值的是连接的类型而不是数量。

量的重要性会超越“万物数量”的重要性。[7] 新连接数量的激增已经成为“万物互联”的一部分，它主要是由启用 IP 的设备越来越多所导致的，而且也源于全球带宽可用性的提升和 IPv6 的出现。“万物互联”造成的安全风险不仅仅是数量不断激增的任意互联的端点（这正在使我们日益接近一个更加高度互联的世界），而且还包括不断增加的恶意攻击者利用更多攻击路径损害用户、网络和数据的各种机会。新连接本身也会带来风险，因为它们会在需要实时保护的活动中产生更多的数据 - 包括企业持续收集、存储和分析的迅速增长的大数据。

“‘万物互联’正快速成形，因此，安全专业人员需要考虑如何将其注意力从仅仅保护终端和网络范围的安全上转移过来。”
Chris Young，思科安全与政府业务高级副总裁

“‘万物互联’正快速成形，因此，安全专业人员需要考虑如何将其注意力从仅仅保护终端和网络范围的安全上转移过来”，Chris Young 说。“设备、连接、内容类型和应用数量将非常非常多 - 而且数量还将保持持续增长的趋势。在这种新形势下，网络本身也成为使企业可以扩展策略和控制不同环境的安全模式的一部分。”

思科 BYOD 更新

终端激增是在全球拥有 70,000 名员工的思科公司的一种现象，思科对此非常熟悉。自两年前制定正式的自带设备 (BYOD) 操作流程以来，公司内部在用的移动设备数量增长率达到 79%。

《思科 2011 年度安全报告》[8] 首先研究了思科快速的 BYOD 发展历程，这是公司持续和更加全面地向“虚拟化企业”转型的一部分。几年后，当思科进入其规划的发展历程最后阶段，公司对位置和服务的依赖性将日益下降，但企业数据仍将是安全的。[9]

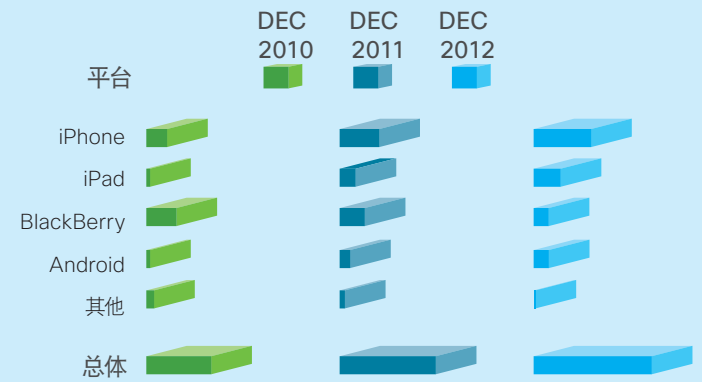
2012 年，思科在全公司范围内增加了约 11,000 部智能手机和平板电脑，或者说每个月新增大约 1,000 部启用互联网的设备。“2012 年底，公司内部在用的智能手机和平板电脑大约有 60,000 部 (包括不到 14,000 部 iPad)，所有的设备均为自带 (BYO) 设备，”监管思科 IT 移动通信服务的高级经理 Brett Belding 说。“思科的移动设备现在进入自带设备时期。”

思科增幅最大的在用设备类型是苹果的 iPad。“三年前这种产品还没问世，想想就觉得不可思议，”Belding 说。“如今，思科每天有 14,000 多部 iPad 被我们的员工用于各种活动 (个人以及和工作有关的活动)。员工除了使用智能手机外，还在使用 iPad。”

至于智能手机，在两年的时间内，思科在用的苹果 iPhone 数量几乎增加两倍，达到将近 28,600 部。思科的 BYOD 计划还涵盖 RIM BlackBerry、谷歌安卓和微软 Windows 设备。 员工作出交易选择，有权在有安全控制协议的个人设备上获取公司数据。例如，想要在自己的设备上检查电子邮件和日程表的用户，需要获得强制执行远程擦除、加密和通行短语的思科安全配置文件。

> “我们支持的设备数量比以往任何时候都要多，而与此同时，我们的支持案例却最少。我们的目标就是：有朝一日，员工可以将任何设备带入公司，自己使用思科身份服务引擎 (ISE) 进行配置，并创建我们的核心 WebEx 协作工具，包括会议中心、Jabber 和 WebEx Social。”
>
> Brett Belding，思科 IT 移动通信服务监管高级经理

图 2：思科移动设备部署



社会支持从始至终一直是思科 BYOD 计划的一个关键因素。“我们在很大程度上依赖 [企业协作平台] WebEx Social，将其作为我们的 BYOD 支持平台，它已为公司带来巨额的回报，”Belding 说。“我们支持的设备数量比以往任何时候都多，而与此同时，我们的支持案例却最少。我们的目标就是：有朝一日，员工可以将任何设备带入公司，自己使用思科身份服务引擎 (ISE) 进行配置，并创建我们的核心 WebEx 协作工具，包括会议中心、Jabber 和 WebEx Social。”

Belding 认为，思科 BYOD 计划的下一步是，通过提高可视性和加强对物理网络和虚拟基础设施上的所有用户活动和设备的控制，进一步提高安全性，同时提升用户体验。“注重用户体验是根本的 IT 消费化趋势，”Belding 说，“我们正设法将此概念应用于我们的公司。我们必须这么做。我认为目前我们看到的是用户的‘IT 化’。我们已经过了用户问‘我能在工作时使用该设备吗?’的时期，现在他们说，‘你需要确保企业的安全，这一点我理解，但是请不要影响我的用户体验’。”

服务存在于多个云中

全球数据中心流量正在上升。根据思科全球云指数，未来五年全球数据中心流量预计会增加四倍，2011 和 2016 年间的复合年增长率 (CAGR) 将为 31%。[10]

在这一快速增长阶段，增长最快的部分是云数据。未来五年，也就是 2011 到 2016 年，全球云流量将增加六倍，增长率为 44%。事实上，到 2016 年，全球云流量将接近占到数据中心总流量的三分之二。[11]

云流量的激增引发了企业能否管理该信息的问题。在云中，控制方式不清晰：一个企业如何在没有运行数据中心的情况下，在其云数据周围设置安全网络？如果不能定义网络边界，如何应用像防火墙和防病毒软件这样的基本安全工具？

无论引发多少安全问题，有一点很清楚，那就是越来越多的企业愿意接受云的好处 – 包括那些不可能重新采用专用数据中心模式的企业。对于企业而言，云的机会很多，包括节约成本、加强劳动力协作、提高生产效率、降低碳排放，但企业将企业数据和流程转移到云上会产生诸多潜在安全风险，包括：

未来五年，也就是 2011 到 2016 年，全球云流量将增加六倍，增长率为 44%。

虚拟机监控程序

如果受到损害，那么创建和运行虚拟机的该软件可能导致多台服务器受到大量的黑客入侵或数据损坏 – 给非法侵入者成功入侵提供虚拟化带来的管理和访问便利。非法的虚拟机监控程序（通过“虚拟机管理程序被劫持”被控制）可以完全控制一台服务器。[12]

降低进入成本

虚拟化降低了进入成本，可提供虚拟专用服务器 (VPS) 等服务。与以前的基于硬件的数据中心模式相比，我们看到针对犯罪活动的快速、低廉、易于获得的基础设施正不断增长。例如，许多针对地下犯罪的 VPS 服务供即时出售（能够使用比特币或其他很难追踪的支付方式购买）。虚拟化使基础设施的购买成本更低且更易于获取 – 活动几乎不受监管。

非法的虚拟机监控程序（通过“虚拟机管理程序被劫持”被控制）可以完全控制一台服务器。

“分离”虚拟应用

由于虚拟应用和它们所使用的物理资源是分离的，因此对于企业来说，应用传统的安全方法越来越难。IT 提供商们都试图通过灵活的产品组合来最大限度地降低成本。他们可以在产品组合中按需移动资源 – 与此相反的是，安全小组则努力地将一些安全状况差不多的服务配置在一起，使这些服务与那些不够安全的服务分离开来。

“虽然虚拟化和云计算产生的问题与 BYOD 类似，但它们使业界发生彻底变革，”Virtuata 公司前首席执行官 Joe Epstein 说。Virtuata 于 2012 年被思科收购，该公司提供保护数据中心和云环境中虚拟机层级的信息安全的创新方法。“高价值的应用和高价值的数据目前正在围绕数据中心移动。虚拟劳动力的概念使很多企业不安。在虚拟环境中，您如何知道您可以信任正在运行的东西呢？迄今为止，答案还是不得而知 – 这种不确定性已经成为云应用的一个关键障碍。”

但是 Epstein 注意到：企业越来越难以忽视虚拟化和云了。“世界正在共享一切事物，”他说。“一切都将虚拟化；一切都将共享。只继续运行私有数据中心将没有任何意义；混合云是 IT 业发展的方向。”

“虽然虚拟化和云计算产生的问题和 BYOD 类似，但它们给业界带来彻底变革.....高价值的应用和高价值的数据正围绕数据中心移动。”
Joe Epstein, Virtuata 公司前首席执行官

应对这些日益增长的云和虚拟化挑战的方法就是自适应安全和响应安全。Epstein 认为，在这种情况下，安全必须是一个能够无缝整合到底层数据中心结构中的可编程元素。另外，安全应在设计阶段植入，而不是在实施后嵌入。

将企业和个人应用相结合

千禧一代和工作区

现代工人 – 尤其是年轻的“千禧一代”– 希望自由地浏览网页，这种自由不仅体现在浏览的时间和方式上，而且体现在他们选择的设备上。无论如何，他们都不希望这种自由受到雇主的侵犯，这是情形会给安全专业人员造成压力。

根据《 2012 思科互联世界技术报告》研究，2/3 的受访者认为老板不会跟踪员工在公司所发设备上的上网活动。总之，他们认为老板没有权利监控这类行为。在被调查的工人中，只有大约 1/3 (34%) 的人说，他们不介意老板追踪他们的上网行为。

只有 1/5 的受访者说他们的老板追踪他们在公司设备上的上网活动，而 46% 的人说他们的老板没有这么做。最新的《互联世界》研究调查结果也表明：千禧一代对老板追踪员工的上网活动感到强烈不满，即使那些认为自己工作的公司不会发生这种跟踪情况的人也是如此。

只有 1/5 的受访者说，他们的老板追踪他们在公司设备上的上网活动，而 46% 的人说他们的老板没有这么做。

对于安全专业人员而言，使上述挑战变得更为严重的是，员工们认为他们可以使用公司发放的设备进行的操作与 IT 部门实际规定个人使用的政策之间似乎存在分歧。2/5 的受访者认为他们应当只把公司发放的设备用于工作活动，而 1/4 的受访者说他们获准将公司设备用于工作以外的活动。然而，90% 的受调查的 IT 专业人员说，他们公司确实有政策禁止将公司发放的设备用于个人上网活动，不过 38% 的人承认员工们违反政策，把这些设备用于工作以外的个人活动。（您可以在第 16 页找到有关思科应对这些 BYOD 挑战的方法。）

员工们认为他们可以使用公司发放的设备进行的操作与 IT 部门实际规定个人使用的政策之间似乎有出入。

隐私和千禧一代

根据《2012 思科互联世界技术报告》，千禧一代认为，互联网使个人隐私变得无关紧要。91% 的接受调查的年轻消费者认为，隐私时代已经结束，并认为他们无法控制其信息隐私，1/3 的受访者说，他们不担心自己的信息被存储和获取。

另外，千禧一代普遍认为他们的在线身份不同于离线身份。45% 的人认为这些身份通常因具体的活动而异，而 36% 的人认为这些身份是完全不同的。只有8% 的人认为这些身份是相同的。

另外，年轻的消费者非常期望网站能对他们的信息保密，如果大部分人提供匿名信息，他们往往会更加愿意和大型社交媒体或社区网站分享数据。46% 的人认为他们希望某些网站对其信息保密，而 17% 的人认为他们相信大多数网站会对其信息保密。然而，29%的人称，他们不仅不相信网站会对其信息保密，而且还非常担心安全和身份被窃问题。这与那些清楚知道员工身份和他们正在做什么的雇主分享数据的看法相似。

“千禧一代目前正步入职场，随之而来的是新的工作方法和对信息及相关信息安全问题的态度。他们认为隐私不复存在 – 它实际上根本不存在，公司必须采用这种模式来运营 – 这种观念对于老一代职场人而言简直是危言耸听，”思科 EMEAR 安全销售总监 Adam Philpott 说，“但是，公司可以寻求给其员工提供信息安全教育，以提醒他们注意风险，并指导他们如何最好地分享信息和利用数据安全领域的在线工具。”

“千禧一代目前正步入职场，随之而来的是新的工作方法和对信息及相关信息安全问题的态度。他们认为隐私不复存在 – 它实际上根本不存在，公司必须采用这种模式来运营 – 这种观念对于老一代职场人而言简直是危言耸听。”

Adam Philpott，思科 EMEAR 安全销售总监

为何企业需要增强防范社交媒体虚假信息的意识

Jean Gordon Kocienda
思科全球威胁分析师

社交媒体给许多企业带来好处：许多公司能通过 Twitter 和 Facebook 直接与客户和其他受众联系，有助于它们通过在线社交互动提高品牌知名度。

快速直接交流的负面影响是，社交媒体可以让不准确或误导的信息迅速传播。不难想象这样一个情景，恐怖主义分子使用旨在阻断公路或切断电话线或使他人进入危险道路的误导性的 Twitter 微博信息，进行地面攻击。有这样一个实例：今年夏天，印度政府封锁了数以百计的网站，并对短信进行管制[13]，试图平息因网上发布的多幅图片以及短信给该国东北部带来的骚乱。谣言四起，数以千计的惊慌失措的农民工纷纷涌向火车站和公共汽车站。

类似的社交媒体虚假信息活动同时也影响了市场价格。被截获的路透社 Twitter 反馈报告说，叙利亚自由军已经攻陷了阿勒颇。几天后，破获了一份 Twitter 源，声称俄罗斯最高外交官发布 Twitter 微博宣布说，叙利亚总统巴沙尔·阿萨德去世。来不及对这些报道进行质疑，国际市场的油价便一路飙升。[14]

安全专业人员需要注意这种快速传播和可能受造成破坏的社交媒体帖子，尤其在它们针对企业本身时。他们需要迅速采取行动来保护网络免受恶意软件的侵袭，提醒员工注意假冒钓鱼攻击，使船运改道或通知员工注意安全。安全执行人员需要做的最后一件事是，提醒经理们注意最后可能被证明是恶作剧的突发新闻。

防止听信捏造新闻报道的第一个措施是：通过多个渠道确认报道的真实性。以前，记者们帮我们做这些事儿，我们则阅读或收听经过审查的新闻。现在，许多记者获取新闻素材的 Twitter 源和我们相同，如果我们当中有几个人认为同一则新闻报道是真实的，那么我们可能认为报道经过确认，就很容易错误地转发 Twitter 微博。

对于需要快速采取措施的突发新闻，最好的办法是使用 老式的“取样测试法”。如果新闻看起来不可信，那么在重复转发或引用前请三思。[15]

对于需要快速采取措施的突发新闻，最好的办法是使用老式的“取样测试法”。如果新闻看起来不可信，那么在重复转发或引用前请三思。

大数据

当今企业的重要资产

商业界正在热烈讨论“大数据”- 分析师可能从企业生成、收集和储存的大量信息中“掘金”。

《2012 思科互联世界技术报告》审查了大数据发展趋势对企业的影响 - 更确切地说，是对他们 IT 团队的影响。根据研究结果，全球大约有 3/4 (74%) 的企业已经在收集和存储数据，管理人员正使用大数据分析结果进行商业决策。另外，7/10 的IT 受访者说，大数据将是他们公司及 IT 团队来年的战略重点。

随着移动通信、云、虚拟化、终端激增和其他网络趋势的发展和涌现，它们将为企业更多的大数据和商业分析机会铺平道路。但是，大数据存在安全问题。《2012 互联世界》研究结果显示，1/3 的受访者 (32%) 认为，大数据使数据和网络的安全要求和保护复杂化，因为数据过多，获取数据的方法也非常多。简而言之，大数据增加了企业安全团队（和安全解决方案）必须覆盖的媒介和角度。

韩国 (45%)、德国 (42%)、美国 (40%) 及墨西哥 (40%) 的 IT 受访者认为大数据使安全问题复杂化的比例最高。大部分的 IT 受访者 - 超过 2/3 (68%) - 认为整个 IT 团队应参与公司内的大数据工作的策略制定并发挥主导作用，以便确保安全。思科安全情报运营威胁研究主任 Gavin Reid 说，“大数据目前没有使安全问题复杂化，当然它存在这种可能。

全球大约有 74% 的公司已经在收集和存储数据，管理人员正使用大数据分析结果进行商业决策。

韩国、德国、美国和墨西哥的 IT 受访者中，认为大数据使安全问题复杂化的比例最高。

在思科，我们每天收集和存储 2.6 万亿条记录，形成了一个我们可以由此开始事故检测和控制的平台。”

至于旨在帮助企业优化管理和利用大数据价值的解决方案，应用上还存在诸多障碍。受访者认为这些障碍包括缺乏预算、缺少研究大数据的时间、缺少相应的解决方案、缺少 IT 人员，以及缺乏 IT 专业知识。全球有接近 1/4 的受访者 (23%) 认为，缺少专业知识和人才是阻碍企业有效地使用大数据的因素，这表明需要更多的专业人员进入该行业，接受该方面的培训。

《2012 互联世界》研究 50%的受访者认为，云也是大数据取得成功的一个因素。他们认为公司需要完成个云计划和部署，以使大数据成为有价值的投资。这种观点在中国 (78%) 和印度 (76%) 非常流行，超过 3/4 的受访者认为大数据需要依靠云才能够真正获得成功。因此，研究指出，在某些情况下，云的应用会影响大数据应用的速度和工作效益。

在所有 IT 受访者中，半数以上的人还证实公司内的大数据讨论尚未取得任何成果。这不足为奇，因为目前市场只是在试图理解如何利用他们的大数据，分析并有策略地使用它。但在某些国家，通过大数据讨论，正在策略、方向和解决方案方面，取得颇有意义的决策。中国 (82%)、墨西哥 (67%)、印度 (63%) 和阿根廷 (57%) 在这方面处于前列。这些国家的受访者中有超过半数的人声称他们公司的大数据讨论正在顺利进行，并因此制定有效的措施和取得了很好的结果。

至于旨在帮助企业优化管理和利用大数据价值的解决方案，应用上还存在诸多障碍。受访者认为这些障碍包括缺乏预算、缺少研究大数据的时间、缺少相应的解决方案、缺少 IT 人员，以及缺乏 IT 专业知识。

《2012 互联世界报告》中 3/5 的 IT 受访者认为，大数据能帮助他们的国家和经济在全球市场中变得更加具有竞争力。

在某些国家，因为大数据讨论，正在策略、方向和解决方案方面取得颇有意义的决策。中国、墨西哥、印度 和阿根廷在这方面面处于前列，这些国家的受访者中有超过半数的人声称他们公司的大数据讨论正在顺利进行，并因此制定有效的措施和取得了很好的结果。

漏洞的状况

危险潜伏在意想不到的地方

许多安全专业人员 - 当然还有庞大的在线用户群体 - 对人们在哪里最有可能遇到危险的网络恶意软件有一种先入为主的看法。

大家普遍认为，引发犯罪活动的网站（例如销售非法药品或假冒奢侈品的网站）最有可能是托管恶意软件。我们的数据表明这种旧观点是正确的。因为在当今威胁环境下，网络恶意软件攻击通常并不是“不良”网站的副产品。

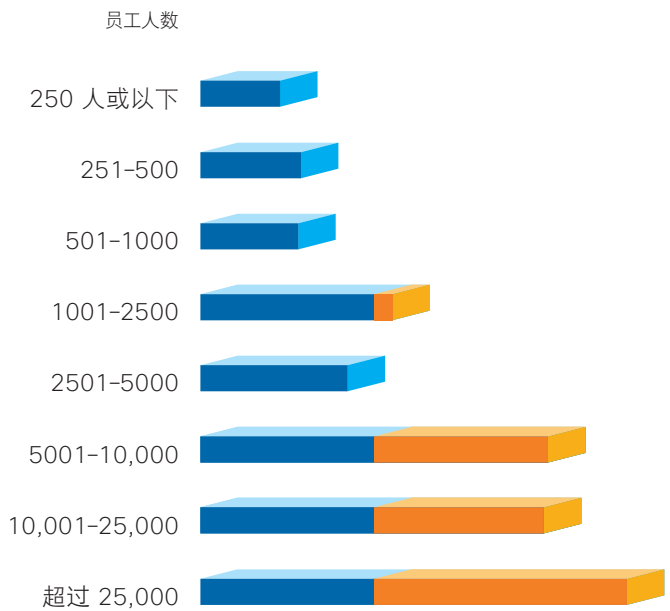
“只要人们访问互联网 - 包括他们即使出于商业目的频繁访问的最合法网站，遭遇网站恶意软件的情况就会随处发生，”思科高级安全研究员 Mary Landesman 说。“实际上，工商业网站是遭遇恶意软件攻击最多的三大网站之一。当然，这不是因设计的恶意商业网站而起。”但是，危险通常通过向合法网站发布的加载了漏洞的在线广告，或者通过针对用户最常使用的网站上的用户群体的黑客，隐藏在的不起眼的地方。

另外，在许多国家和地区，网站受到恶意软件感染的情况非常普遍。这不只是一两个国家的问题。这样一来，人们不再认为，某些国家的网站托管恶意软件内容的可能性高于其他国家的网站。“Web 是迄今为止最可怕的恶意软件传播途径，它可以悄无声息和有效地影响和感染

危险通常隐藏在充满探索诱惑的在线广告中的不起眼的位置。

图 3: 各种公司规模面临的风险

大公司遭遇网络恶意软件的风险最多高达 2.5 倍以上。



所有的公司，无论规模大小，均面临着遭遇网络恶意软件攻击的重大危险。每个公司都应该重视保护其网络和知识产权安全的原则。

大量的受众，这种能力甚至超过了繁殖能力最强的蠕虫或病毒，”Landesman 说。“企业需要通过更精密的检查和分析来进行保护，即使他们已阻止普通的“不良”网站。”

各种公司规模遇到的恶意软件情况

规模最大的企业 (拥有 25,000 名以上的员工) 遭遇网络恶意软件风险的几率为小公司的 2.5 倍以上。风险增加可能是因为大型公司拥有更高价值的知识产权，因此更加频繁地受到攻击。

尽管小公司的每个用户较少遭遇网站恶意软件，但必须注意到，所有的公司（无论其规模大小）都面临遭遇网站恶意软件的风险。每个公司都应该重视保护其网络和知识产权安全的原则。

各国家/地区恶意软件数量

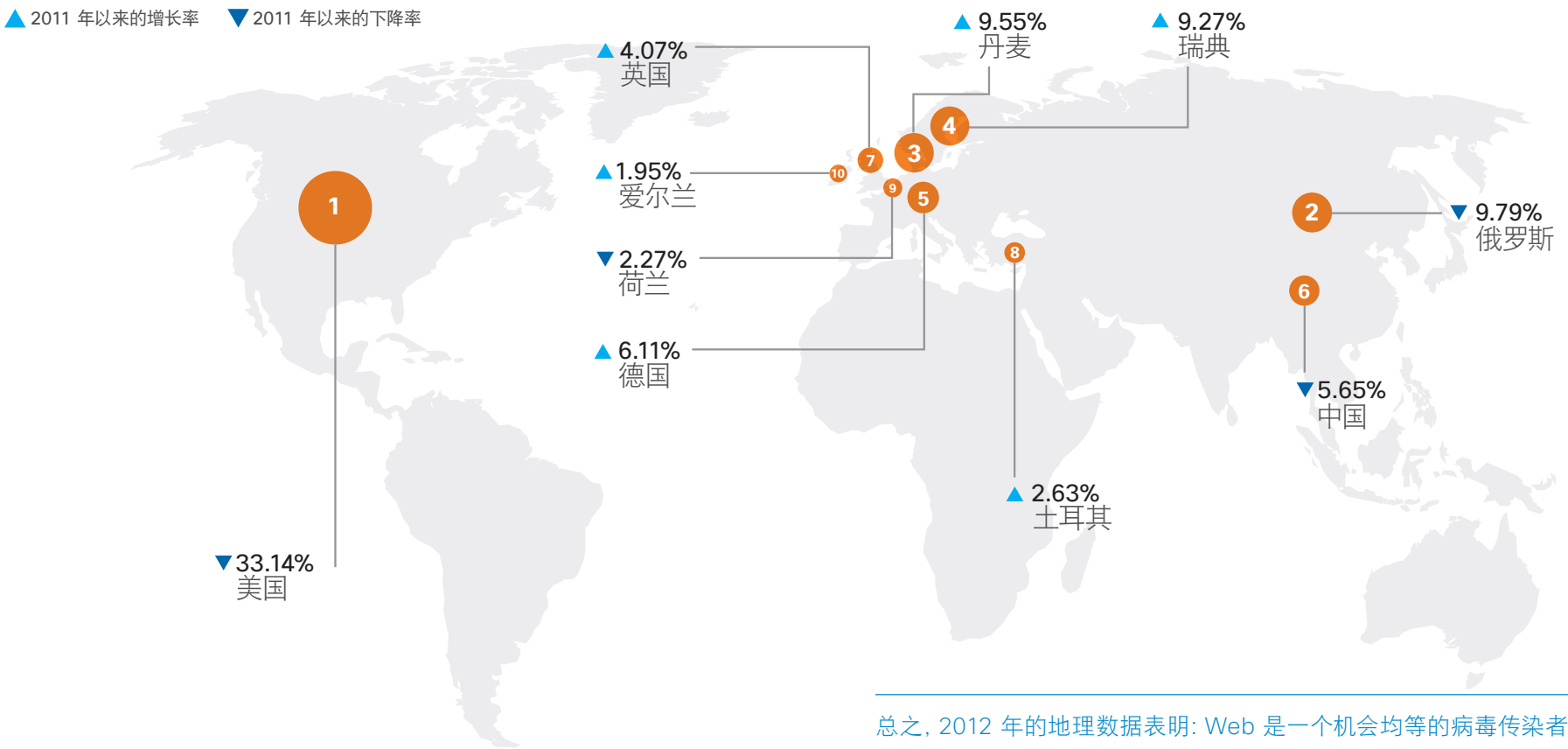
思科的研究显示，2012 年 Web 恶意软件在全球各国的排名发生重大变化。在 2011 年，中国的恶意软件数量居全球第二，2012 年急剧下降到第六位。丹麦和瑞典现在分别列第三和第四位。在 2011 年 2012 年，美国都名列榜首，在所有 Web 恶意软件中，33% 的恶意软件是通过美国托管的网站产生。

2011 和 2012 年之间，不同地理位置的恶意软件数量变化，可能反映了检测和用户习惯的变化。例如，2012 年同 2011 年相比，通过在线广告传播的“恶意广告”或恶意软件在 Web 恶意软件攻击中发挥了更加重要的作用。值得反复强调的是：Web 恶意软件最常见于正常浏览那些可能受到感染的合法网站或不经意中提供恶意广告的合法网站。恶意广告可以影响任何网站，与网站的所在地无关。

总之，2012 年的恶意软件地理分布数据表明：Web 是一个机会均等的病毒传染者。而相反的观点则认为，仅有一两个国家应对托管 Web 恶意软件负责，或者某个国家比其它国家更安全。正如 Web 2.0 的动态内容交付可帮助全球网站盈利一样，它也可以加速 Web 恶意软件在全球的传播。

图 4: 各国家/地区的 WEB 恶意软件数量

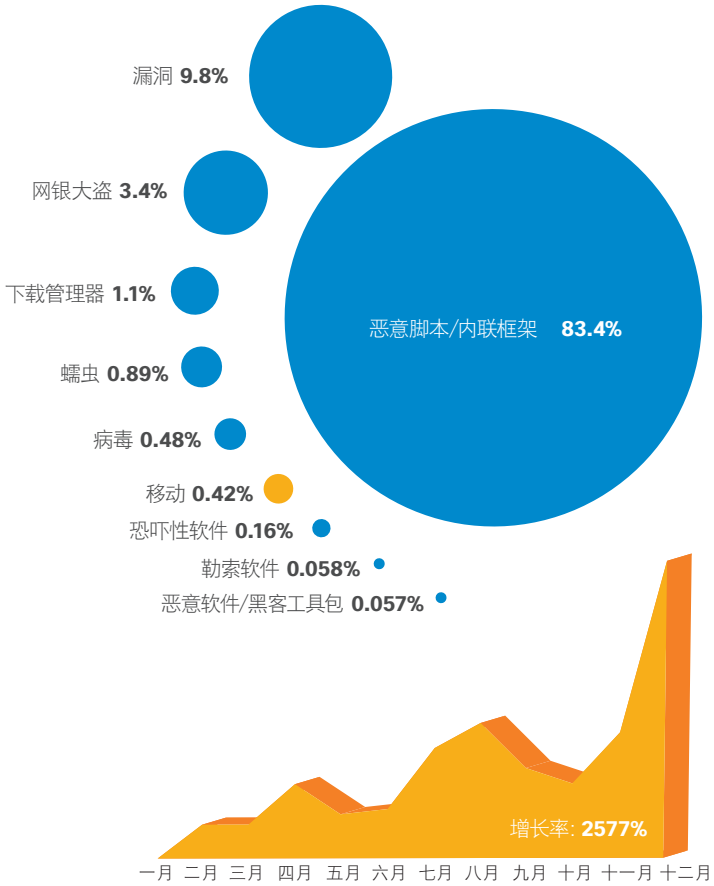
在所有遭遇网络恶意软件侵扰的事件中，有 1/3 是因在美国托管的域引起。



总之，2012 年的地理数据表明: Web 是一个机会均等的病毒传染者，与此相反，有观点认为仅有一两个国家应对托管 Web 恶意软件负责，或某个国家比另外一个国家更安全。

图 5: 最主要的 Web 恶意软件类型

2012 年安卓恶意软件数量增加 2577%，不过移动通信恶意软件仅占 Web 恶意软件数量的一小部分。



当然，发生恶意软件攻击的位置和实际托管恶意软件的位置之间截然不同。例如，恶意广告攻击通常在访问传播第三方广告的知名、合法网站时发生。然而，用于传播的实际恶意软件托管在完全不同的域上。由于思科的数据是基于攻击发生的位置，它和实际的恶意软件来源地没有任何关系。例如，在丹麦和瑞典，伴随着恶意广告风险的社交媒体和娱乐网站的日益普及，是通过在该地区托管（但不是实际的恶意软件来源地）的网站频繁遭遇恶意软件的主要原因。

2012 年排名最靠前的 Web 恶意软件类型

安卓恶意软件数量的增长速度要远远快于其他任何形式的通过 Web 传播的恶意软件。这个重要的趋势证明了安卓拥有全球最大的移动通信设备市场份额。必须注意到，2012 年移动恶意软件数量只占所有 Web 恶意软件数量的 0.5%，而安卓恶意软件数量占到所有这些 Web 恶意软件数量的 95%。另外，2012 年出现了第一个有记录的安卓僵尸网络，这表明 2013 年的移动恶意软件发展值得密切关注。

某些专家认为安卓是 2013 年“最大的威胁”，应引起企业安全团队的重点关注，而实际的数据表明情况并非如此。如上所述，一般来说，移动恶意软件数量只占全部恶意软件的不到 1%，离许多人所说的 “世界末日”还很远。BYOD 的影响和设备的激增怎么强调都不为过。但是各个公司应更关注事故数据丢失这类威胁，确保员工不会对设备进行破解，而且只安装来自正规和受信任的分销渠道的应用软件。如果用户不选择官方移动应用商店，那么他们在下载一个应用前，应确保他们知道并信任该应用设计者，并且能够验证代码没有被篡改。

鉴于 Web 恶意软件的影响范围扩大，2012 年恶意脚本和内联框架占到全部恶意软件数量的 83% 就不足为奇了。而这种情况与前几年基本一致，这是个

值得反思的结果。这些类型的攻击通常存在于用户每天都在访问的“受信任的”网页上的恶意代码中，也就是说，攻击者能够在不引起用户怀疑的情况下攻击用户。

漏洞排第二位，占去年 Web 恶意软件总量的 10%。然而，这些数字主要是发生的针对 Web 上实际存在的漏洞的阻止的结果。例如，83% 的恶意脚本及隐藏的内联框架是在任何漏洞提交前的较早的阶段进行阻止；因此，它们可能给人以观察到的漏洞数量下降的假象。

漏洞仍旧是通过 Web 感染的一个重要原因，它们持续存在，强调了提供商在产品生命周期内采取安全最佳实践的必要性。公司应该重视安全，将其作为产品设计和开发流程的一部分，及时披露漏洞，准时/定期打补丁。公司和用户也应该认识到使用提供商不再支持的产品的相关的安全风险。另外，公司必须坚持核心漏洞管理流程，而用户则必须保持更新硬件和软件。

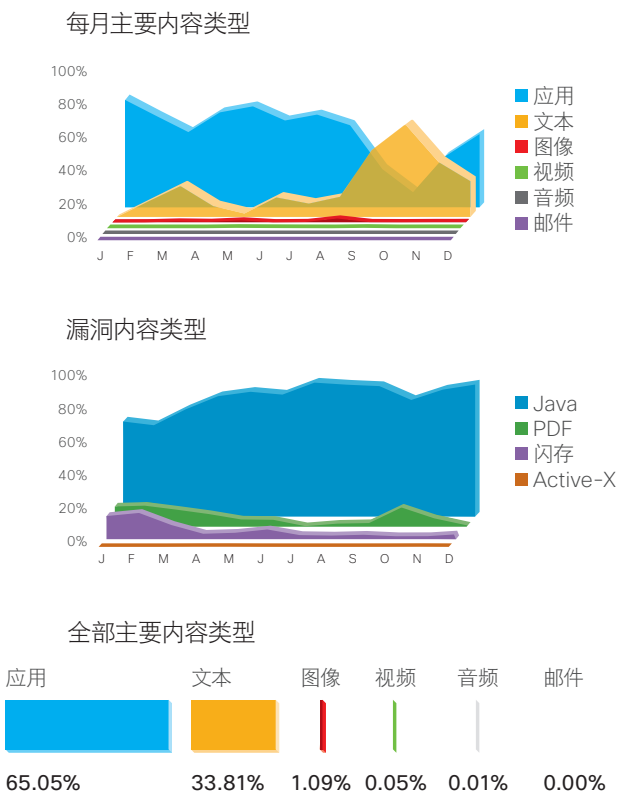
排在前五位的有网银大盗（2012 年占 Web 恶意软件总量的 3.5%）、下载管理器 (1.1%) 和蠕虫 (0.8%)。这些数字再度表明，阻止通常是在第一次遇到恶意脚本或内联框架时发生。因此，这些数字不能反映通过 Web 传播的网银大盗、下载管理器或蠕虫的实际数量。

排名最靠前的恶意软件内容类型

恶意软件创建者不断寻求投资回报率最大化 (ROI)，寻找途径，以最小的代价使受害者数量达到最大，并经常尽可能地利用交叉平台技术。为了达到这些目的，漏洞工具箱通常按照特定的顺序提交漏洞；一旦成功提交漏洞，则无需尝试提交其它漏洞。大量的 Java 漏洞（占 Web 漏洞总量的 87%）表明，相比于其他类型漏洞，Java 漏洞总是最先遭到攻击。这同时也表明，攻击者很有办法能够成功攻击 Java 漏洞。另外，有 30 多亿设备在运行 Java，[16] 这项技术为黑客在多个平台的攻击提供了道路。

图 6: 2012 年排名最靠前的恶意软件内容类型

Java 漏洞占全部网站漏洞的 87%。

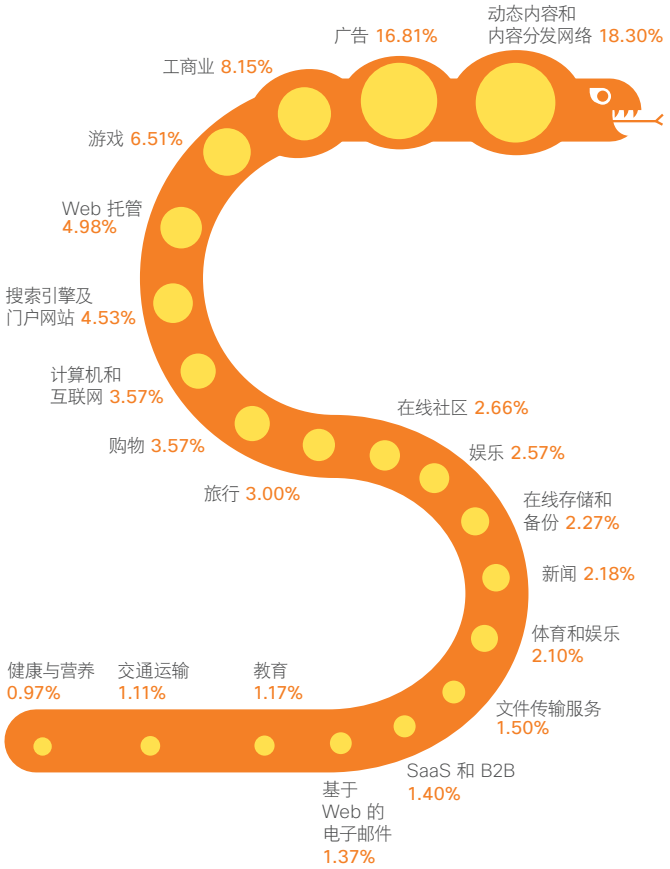


大量的 Java 漏洞表明，相比于其他类型漏洞，Java 漏洞总是最先遭到攻击。这同时也表明，攻击者很有办法能够成功攻击 Java 漏洞。

图 7: 排名最靠前的网站类别

在线购物网站提交恶意内容的可能性比假冒软件网站高 21 倍。

备注: 在思科的最可能受到恶意软件感染的位置排名榜单中，“动态内容”分类名列榜首。该分类包括内容分发系统，例如网站统计、站点分析和其他的与广告无关的第三方内容。



在思科对恶意软件传播的最主要内容类型的分析中，其他两项交叉平台技术（PDF 和 Flash）分别排第二位和第三位。虽然Active X 仍旧被漏洞所利用，但思科的研究人员发现，这项技术一直很少被用作恶意软件传播的媒介。然而，关于 Java，如前所述，某些类型的漏洞数量很少，主要反映了漏洞被攻击的顺序。

在审查媒体内容时，思科数据表明，基于图像的恶意软件数量几乎是非 flash 视频的两倍多。然而，一部分原因在于浏览器处理发布的内容类型的方式，以及攻击者通过发布错误的内容类型来操纵这些控件的操作。另外，恶意软件命令和控制系统经常通过隐藏在普通图像文件中的备注分布服务器信息。

排名最靠前的网站类别

思科数据表明，感染恶意软件的最常见途径是假冒软件等“有危险”网站的观点是错误的。思科分析表明，大部分遇到网络恶意软件的人实际上是通过合法地浏览主流网站而中弹的。换而言之，大部分的攻击是发生在在线用户最常访问和认为安全的地方。

排名第二的是在线广告，它占 Web 恶意软件总量的 16% 。综合性广告是一种常见的网站盈利方式，因此按照这种方式分布的一个恶意广告可能产生巨大的负面影响。

进一步查看出现恶意软件攻击的其它网站类别，工商业网站排在第三位，包括从公司网站到人力资源再到运输服务的所有网站。在线游戏排第四位，紧跟其后的是网络托管网站和搜索引擎，分别列

大部分遇到网络恶意软件的人实际上是通过合法地浏览主流网站而中弹的。换而言之，大部分的攻击是发生在在线用户最常访问和认为安全的地方。

网络犯罪分子始终密切关注现代浏览习惯，以便让 Web 恶意软件感染尽可能多的人。

第五位和第六位。名列前 20 位的网站类别不包括人们通常认为的恶意网站。有一种网站类型是热门内容与合法内容良好结合的网站，例如在线购物 (#8)、新闻 (#13) 和 SaaS/企业对企业的应用 (#16)。

网络犯罪分子始终密切关注现代浏览习惯，以便让 Web 恶意软件感染尽可能多的人。在线用户一到哪儿，恶意软件创建者就会利用受信任的网站，通过直接入侵或第三方分发网络跟到哪儿。

按点击量排名的流行应用

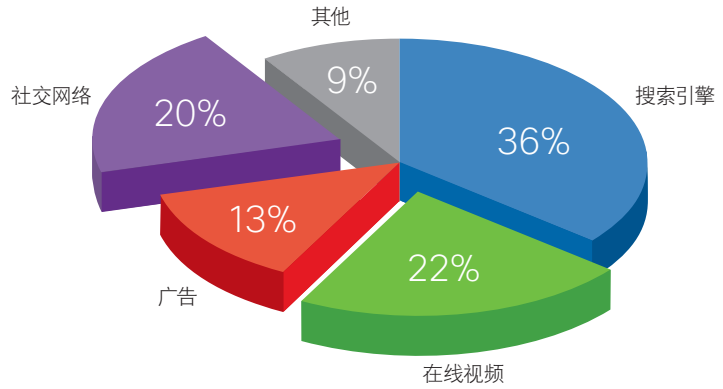
人们在网上打发时间的方式的变化，扩展了网络犯罪分子发布漏洞的平台。

各种规模的公司正在接受社交媒体和在线视频；绝大多数品牌均在 Facebook 和 Twitter 上建立页面，许多公司正将社交媒体和实际产品融为一体。由于这些 Web 网站吸引着大量的受众，并被企业环境所接受，所以也为传播恶意软件创造了更多的机会。

根据思科应用可见性和控制 (AVC) 数据，绝大多数 (91%) 的 Web 请求在搜索引擎 (36%)、在线视频网站 (22%)、广告网络 (13%) 和社交网络 (20%) 之间分享。

各种规模的公司正在接受社交媒体和在线视频；绝大多数品牌均在 Facebook 和 Twitter 上建立页面，许多公司正将社交媒体和实际产品融为一体。

图 8：按点击量排名的流行应用
社交媒体和在线视频改变了员工度过工作时间的方式，并且暴露出新的安全漏洞。



如果互联网上访问量最大的网站数据与最危险的网站类别有关，在线用户最容易受到恶意软件攻击的完全相同的位置，例如搜索引擎，是引发网站恶意软件攻击的最主要位置。

如果互联网上访问量最大的网站数据与最危险的网站类别有关，在线用户最容易受到恶意软件攻击的完全相同的位置，例如搜索引擎，是引发网站恶意软件攻击的最主要位置。这种相关性再次表明，恶意软件创建者致力于使其投资回报率最大化。因此，他们将把精力集中在用户数量最多和最容易受到攻击的位置。

当哥德式恐怖电影催生恶意软件

作者: Kevin W. Hamlen
德克萨斯州大学达拉斯分校计算机科学系副教授

*恶意软件伪装*是安全专业人员可能面临的一种日益上升的新威胁。大多数恶意软件利用简单的变异或迷惑方法变得多样化，并且增加自身逆向工程的难度，而自我伪装恶意软件则更隐蔽，它和已被其感染的每个系统上的特定软件完美融合。这可以躲避查找软件异常的防御系统，如，运行时解压缩或加密密码，这些异常通常会使更加传统的恶意软件原出原形。

最新的自我伪装恶意软件技术（被戏称为 Frankenstein [17]）是我们今年在德克萨斯州大学达拉斯分校网络安全研究与教育中心的一项研究产品。和 Mary Shelley 在 1818 年写的恐怖小说中虚构的科学狂人一样，“Frankenstein 恶意软件”通过从其接触的其他软件上窃取主干部分（即代码）创建突变体，然后将代码缝补到一起，创建独一无二的变体。因此，每个 Frankenstein 突变体完全由构无异常、看起来无害的软件组成；进行没有任何可疑的运行时解压缩或加密；并且有权访问通过其接触的许多程序获取的不断扩大的代码转换池。

Frankenstein 在上述操作的掩盖下，用一系列源自编辑器理论和程序分析的技术，将其创建的突变体变得更加有趣。首先扫描受到感染的二进制文件的短字节序列，短字节序列解码为可能有用的指令序列，指令序列被称为*小工具*。然后一个小的抽象解释器推断所发现的每个小工具的可能语义效果。然后，采用回溯搜索，发现小工具序列，序列如果按顺序执行，会对执行具有执行恶意软件有效载荷的恶意行为产生影响。

和 Mary Shelley 在 1818 年写的恐怖小说中虚构的科学狂人一样，“Frankenstein 恶意软件”通过从其接触的其他软件上窃取主干部分（即代码）创建突变体，然后将代码缝补到一起，创建独一无二的变体。

总而言之，我们的研究表明，下一代恶意软件可能越来越避免使用基于加密和压缩的简单突变，转而使用 Frankenstein 使用的那些高级变形二进制混淆技术。

发现的每个此类序列最终组合成一个新的突变体。在实践中，Frankenstein 每秒钟发现 2,000 多个小工具，仅五秒钟就从两三个受感染的二进制文件中累计发现 100,000 多个小工具。由于需要处理如此大量的小工具池，所产生的突变体很少共享任何共同的指令序列；因此每个突变体都看起来是独一无二的。

总而言之，我们的研究表明，下一代恶意软件可能越来越避免使用基于加密和压缩的简单突变，转而使用 Frankenstein 使用的那些高级*变形*二进制混淆技术。这类混淆技术易于执行，支持快速传播，可有效地使恶意软件不被大多数恶意软件检测引擎的静止分析阶段发现。为了应对这个趋势，防御者将需要部署某些用于开发 Frankenstein 的相同技术，包括基于语义（非句法）功能提取的静止分析，以及源于机器学习[18]而非纯手工分析的语义签名。

本文汇报了由国家科学基金会 (NSF) 奖 #1054629 和美国提供部分支持的研究成果 空军科研办公室 (AFOSR) 奖 FA9550-10-1-0088。此处表达的任何观点、成果、结论或建议，均为作者的意见，并不反映国家科学基金会或空军科研办公室的观点。

[17] Vishwath Mohan 和 Kevin W. Hamlen。“Frankenstein: 通过无害的二进制文件修补恶意软件。”在 *USENIX 攻击性技术研讨会 (WOOT) 的会议记录中*，第 77-84 页，2012 年 8 月。

[18] Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han 和 Bhavani Thuraisingham。“基于云的”恶意软件检测以改进数据流。*美国计算机学会* 管理信息系统会报 (TMIS)，*2*(3)，2011 年 10 月。

2012 年安全漏洞和威胁分析

安全漏洞和威胁分类表显示，威胁的总量大幅度增加 - 2012 年的网络威胁比 2011 年增加了 19.8%。威胁的急剧增加，对公司保持安全漏洞管理系统更新并打补丁的能力造成沉重的压力，在向虚拟环境转变时尤其如此。

公司也试图解决其产品及环境中所包含的第三方和开放源软件用量日益增加的问题。“第三方或开源解决方案中的一个安全漏洞都可能影响环境中的一系列系统，很难识别、修补或更新所有那些系统，”思科安全研究和运营经理 Jeff Shipley 说。

最大的威胁类型是资源管理威胁；通常包括拒绝服务漏洞，SQL 攻击和跨网站指令码错误等输入验证威胁，以及导致拒绝服务的缓冲区溢出。前几年，类似的威胁占大多数，随着威胁的急剧增加，预示着安全行业需要在检测和处理这些安全漏洞方面做好准备。

Cisco IntelliShield Alert 紧急程度评级反映了与特定漏洞相关的威胁活动级别。紧急程度 3 指标显著飙升，意味着有更多的漏洞实际正在被利用。原因可能是，研究人员或试验工具公开发布的漏洞数量，以及这些漏洞被纳入到攻击工具箱中。这两个因素使得更多的漏洞可以被黑客和犯罪集团获取和广泛应用。

Cisco IntelliShield Alert 严重程度评级反映了已得逞漏洞利用程序的影响程度。另外，严重程度评级显示，三级威胁显著增加 - 其原因和漏洞工具随时可用的原因相同。

图 9: 紧急程度和严重程度评级

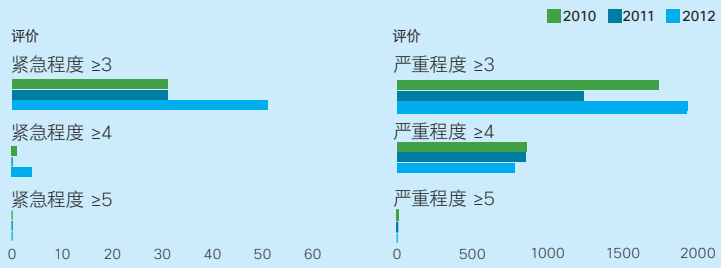
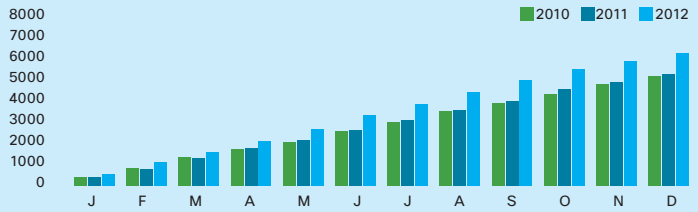


图 10: 安全漏洞和威胁分类

	2010 年每月警告的次数				2011 年每月警告的次数				2012 年每月警告的次数			
	总计	二次放大	新		总计	二次放大	新		总计	二次放大	新	
一月	417	259	158	417	403	237	166	403	552	344	208	552
二月	430	253	177	847	400	176	224	803	551	317	234	1103
三月	518	324	194	1364	501	276	225	1304	487	238	249	1590
四月	375	167	208	1740	475	229	246	1779	524	306	218	2114
五月	322	174	148	2062	404	185	219	2183	586	343	243	2700
六月	534	294	240	2596	472	221	251	2655	647	389	258	3347
七月	422	210	212	3018	453	213	240	3108	514	277	237	3861
八月	541	286	255	3559	474	226	248	3582	591	306	285	4452
九月	357	167	190	3916	441	234	207	4023	572	330	242	5024
十月	418	191	227	4334	558	314	244	4581	517	280	237	5541
十一月	476	252	224	4810	357	195	162	4938	375	175	200	5916
十二月	400	203	197	5210	363	178	185	5301	376	183	193	6292
	5210	2780	2430		5301	2684	2617		6292	3488	2804	



“第三方或开源解决方案中的一个安全漏洞都可能影响环境中的一系列系统，很难识别、修补或更新所有那些系统。”

Jeff Shipley，思科安全研究和运营经理

不断进化的威胁

新方法，相同的漏洞

对当今的网络漏洞而言，只要所选的方法能把任务完成，什么方法都行。

这并不是说地下经济参与者没有持续地致力于创建比以往更加精密的工具和技术来破坏用户并感染网络，并为了许多其他目的而窃取数据。但是，在 2012 年，人们在寻找新方法来制造破坏或避开企业安全保护方面，有一种回归“古典”的趋势。

DDoS 攻击是一个主要的实例 - 美国几大主要的金融机构是 2012 年下半年国外黑客组织发起的两大主要相关活动的主要目标（有关详细的分析信息，请参见“2012 分布式拒绝服务发展趋势”部分）。某些安全专家警告说，这些活动仅仅是个开始，以后，“黑客活动分子、有组织的犯罪团伙，甚至国家将”[19] 协同和独立地进行这些攻击。

“我们正在 DDoS 中发现一种趋势，攻击者对目标网站增加额外的情境，使中断情况变得更加严重，”思科安全情报运营威胁研究主任 Gavin Reid说，“现在的 DDoS 不进行 SYN 泛洪攻击，而是尝试操纵公司内的特定应用，即使失败，也可能造成一系列的破坏。”

在 2012 年，人们在寻找新方法来制造破坏或避开企业安全保护方面一种回归“古典”的趋势。

“即使和复杂而普通的威胁相比，目前最先进的网络工具往往也远不是对手 。”

Gregory Neal Akers，思科高级安全行动小组的高级副总裁

而企业可能认为他们可能在应对 DDoS 威胁方面得到充分的保护，而他们的网络则可能无法防御 2012 年所经历的大量、不间断的 DDoS 攻击类型。“即使和复杂而普通的威胁相比，目前最先进的网络工具往往也远不是对手，”思科高级安全行动小组的高级副总裁 Gregory Neal Akers 说。

网络犯罪领域的另一个趋势以威胁的“普遍化”为中心。我们正日益发现这些工具和技术（及有关如何利用安全漏洞的知识）正在当今的“地下经济”中“被广泛分享”。“间谍情报技术能力取得长足发展，”Akers 说。“我们现在发现，恶意攻击者变得更加专业，合作也更加紧密。威胁已经形成流水线作业：有人开发漏洞，其他人编写恶意软件，还有人设计社交工程组件，等等。”

制造潜在威胁将有助于他们获取网络上遇到的大量高价值资产，这是网络犯罪分子更加频繁地整合专业知识的原因之一。但是，与那些将任务外包的任何现实中的公司一样，高效、节约成本是网络犯罪领域中“确定威胁”方法的主要推动力。为这些任务聘请的“自由职业人才”通常会宣传其技能，并且通过秘密在线市场付费给更大的网络犯罪社区。

放大和反射攻击

DNS 放大和反射攻击[20] 利用域名系统 (DNS) 开放式递归解析器或 DNS 认证服务器，增加发送给受害者的攻击流量。通过破坏[21] DNS 请求邮件，这些攻击隐藏了真实的攻击源，并发送返回比 DNS 请求邮件大 10 到 100 倍的 DNS 响应邮件的 DNS 查询。这些类型的攻击配置文件通常可以在 DDoS[22] 攻击期间观察到。

公司将开放式递归性解析器留在互联网上，在无意中参与了这些攻击。他们可以使用各种工具[23] 和流量遥测[24] 技术检测攻击，还可以通过保护[25] 其 DNS 服务器或限制[26] DNS 响应邮件流量来保护他们自己。

2012 分布式拒绝服务发展趋势

以下分析来源于 Arbor Networks ATLAS 知识库，它包括从许多来源和 240 个 ISP 收集到的全球数据，监控 37.8 Tbps 的峰值流量。[27]

攻击数量继续保持向上趋势

去年平均攻击数量总体保持上升势头。攻击的吞吐量增加了 27%（从 2011 年的 1.23 Gbps 增加到 2012 年的 1.57 Gbps），攻击每秒使用的数据增加了 15%（从 2011 年的 1.33 Mpps 增加到 2012 年的 1.54 Mpps）。

攻击者统计数据

在去除了 41% 因数据匿名而没有确定归属的来源后，被监控到排行最前的三个攻击来源地是中国 (17.8%)，韩国 (12.7%) 和美国 (8.0%)。

最大的攻击

监控到的最大攻击是在100.84 Gbps 时测得的，持续了大约 20 分钟 （因数据匿名而无法知道攻击源地）。监控到的相应的最大攻击（单位：pps）是在 82.36 Gbps 时测得的，持续了大约 24 分钟 （因数据匿名而无法知道攻击源地）。

图 11: 实时入侵防御系统 (IPS) 规避

思科安全研究和运营设立了几个观察着恶意流量的恶意软件实验室。恶意软件在实验室里被故意发布出去，以确保安全设备有效；计算机也故意留有安全漏洞，暴露在互联网上。

现代入侵技术的武器化

网络犯罪分子通常不断改进避开安全设备的新技术。思科研究人员密切关注新技术和著名技术的“武器化”。

思科安全研究和运营设立了几个观察着恶意流量的恶意软件实验室。恶意软件在实验室里被故意发布出去，以确保安全设备有效；计算机也故意留有安全漏洞，暴露在互联网上。

在这样一个测试中，思科入侵防护系统 (IPS) 技术检测到一个熟悉的微软远程过程调用 (MSRPC) 攻击。经过仔细分析确定，攻击利用以前未发现的恶意软件入侵手段以避开安全设备。[28] 入侵发送了初始捆绑请求中的几个捆绑内容的 ID。除非 IPS 监控并确定哪些 ID 成功，这种类型的攻击才可以避开保护系统。

网络犯罪分子通常不断改进避开安全设备的新技术。思科研究人员密切关注新技术和著名技术的“武器化”。

案例研究

燕子行动

在 2012 年 9 月和 10 月之间，思科和 Arbor 网络监控到一个有目的、非常危险的 DDoS 攻击活动。该活动被称为“燕子行动”，目标就是位于美国的金融机构。”DDoS 攻击进行预先策划，目标明确，没有事先宣传，执行非常严格。攻击者能使数家主要的金融网站在几分钟之内无法对合法客户开放，最严重的可以使这些网站数小时处于不可用状态。在事件发生的过程中，几个组织声称对攻击负责；至少一个组织声称这么做是为了抗议美国的版权和知识产权法。其他组织则声称，他们参与此次行动是为了对一段冒犯了某些伊斯兰教徒的 YouTube 视频进行报复。

从网络安全的立场来看，燕子行动值得关注，因为它利用了普通的网站应用，以及应用广泛但易受攻击的托管服务器。在这一系列攻击中，另一个明显但罕见的因素是：在高带宽下同时针对同一行业 （金融）内的多家公司发起的攻击。

和安全行业常见的手法一样，换汤不换药。

2012 年 9 月18 日，“网络战士 Izz ad-Din al-Qassam”在 Pastebin 上面发布一个帖子 [29] 要求伊斯兰教徒将主要金融机构和商品交易平台作为攻击目标。发帖连续持续了四周时间，帖中公布威胁要攻击的特定目标。每周发布新威胁和新目标后，会在指定的时间和日期采取行动。到第五周，该组织不再公布攻击目标，但申明该活动会继续下去。如承诺的那样，活动果然在 2012 年 12 月重新开始，再度把目标对准美国多个大型 金融公司。

燕子行动的第二个阶段也在 Pastebin 上面公布。[30] 包括 Joomla 内容管理系统在内的各种 PHP Web 应用取代受到感染的机器，充当了这次活动主要的僵尸。另外，许多经常使用过时的 TimThumb 插件的 WordPress 网站，也在大约同一时间受到攻击。攻击者往往设法获取未维护的服务器来托管这些应用，并通过上传的 PHP webshell 部署以后的攻击工具。然而，“命令和控制”概念的应用方法不同寻常；攻击者直接或通过中间服务器、脚本和代理连接到工具。在 2012 年 9 月和 10 月的网络事件中，采用了大量的文件和基于 PHP 的工具，而不仅仅使用广泛报道的 “tsoknoproblembro”(aka “Brobot”)。第二轮活动还利用了更新的攻击工具，例如 Brobot v2。

“燕子行动” 在 HTTP、HTTPS 和 DNS 上部署了一组带载体交叉应用层攻击的工具组合，其中，体积攻击流量攻击各种 TCP、UDP、ICMP 和其他 IP 协议。思科的分析显示，数据包大多被发送到 TCP/UDP 端口 53 (DNS) 或 80 (HTTP)。UDP 端口53 和 TCP 端口 53 及 80 的流量通常代表有效流量、目的地址是 UDP 端口 80 的数据包代表应用不经常使用的异常。

有关“燕子行动”模式和有效负荷的详细的报告可以在思科的事件响应中找到：金融机构的分布式拒绝服务攻击。[31]

学习到的经验

尽管 IPS 和防火墙设备是任何网络安全组合产品的关键组成部分，但它们依赖于流量状态检测。在某些情况下，“燕子行动”中用到的应用层技术轻松地制服了那些状态表，导致它们无法发挥作用。智能 DDoS 迁移技术是唯一有效的应对措施。

受管理的安全服务和 ISP 存在局限。在典型的 DDoS 攻击中，人们普遍认为，要处理网络中的容量耗尽攻击。对于部署得离受害者比较近的应用层行动而言，应解决数据中心或“用户边缘”的容量耗尽攻击。因为多家公司都被同时设定为攻击目标，网络清理中心承受重压。

关键是要确保 DDoS 缓解设备上的硬件和软件为最新。旧的部署并非始终能够处理新威胁。确保合适的位置的容量适当也很重要。如果流量不能分到该技术已部署的位置，那么即使能够缓解大型攻击也无济于事。

云或网络 DDoS 缓解通常具有更高的带宽容量，应急解决方案提供了优化的攻击应对时间，并加强攻击的控制和提升可见性。将这两者结合起来可以产生一个更完美的解决方案。

通过采用云或网络 DDoS 技术，并作为“燕子行动”事件制作的附属品的一部分，思科在识别和缓解分布式拒绝服务攻击目标金融机构《应用缓解通告》时，已经列出了检测和缓解技术。[32] 这些技术包括使用过境访问控制列表 (tACL) 过滤，网络流量数据分析和单播反向路径发送 (uRPF)。另外，有多个最佳实践可以大大帮助企业对网络事件作出应对准备，应该经常审核、检验和实施这些实践。这些最佳实践库可以通过参考思科的 SIO 战术资源[33] 和服务提供商安全最佳实践找到。[34]

时刻存在垃圾邮件

根据思科的研究，全球垃圾邮件量持续下降，但是垃圾邮件仍旧是网络犯罪分子可以借助的工具。他们认为，垃圾邮件是使用户受到恶意软件感染和加速各种垃圾邮件传播的一个高效、便捷的方式。

然而，尽管大家认为，恶意软件通常是通过垃圾邮件附件来部署，但是思科的研究显示，现在垃圾邮件极少采用这种方法；相反，它们将邮件内的恶意链接作为更高效的传播途径。

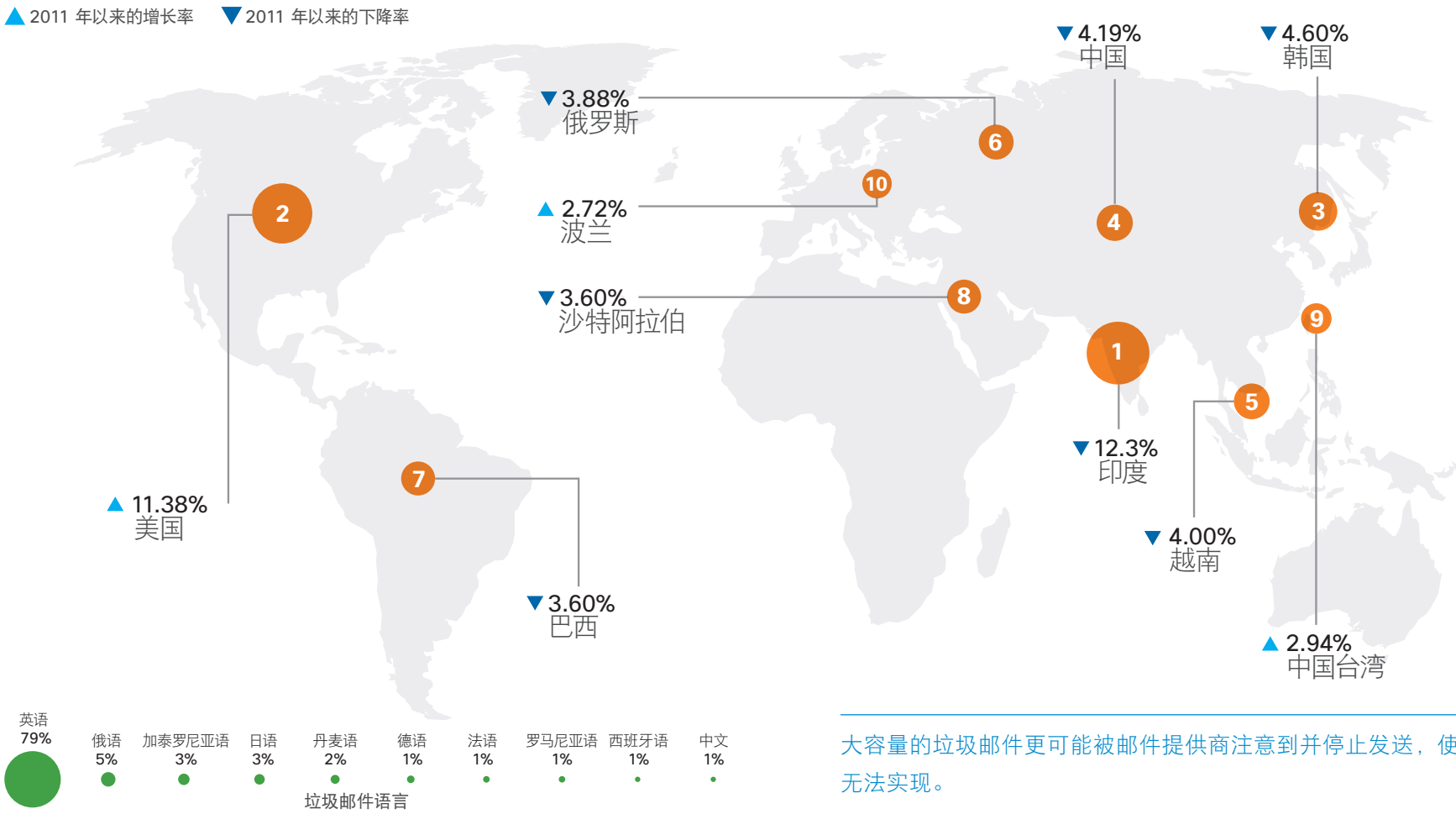
垃圾邮件不像过去那么随意，许多垃圾邮件更趋向于锁定特定用户群体，以获取更高的回报。名牌药品、豪华手表品牌和纳税季等活动，是垃圾邮件活动中宣传最多的内容之一。随着时间的推移，垃圾邮件发送者已经了解到：吸引点击量和购买（并创造收益）的最便捷方式是利用假冒的品牌和利用大量用户关的当前事件。

全球垃圾邮件发展趋势

自从 2010 年大量僵尸网络被关闭以来，大容量的垃圾邮件不再像从前那么有效了，垃圾邮件已经了解并调整其策略。基于世界大事件及特定的用户群体，朝更小、目标更明确的活动发展的趋势非常明显。大容量的垃圾邮件更可能被邮件提供商注意到并停止发送，使其目的无法实现。

图 12: 全球垃圾邮件发展趋势

全球垃圾邮件量下降了 18%，大多数垃圾邮件发送者只在周末安逸的工作几个小时。



大容量的垃圾邮件更可能被邮件提供商注意到并停止发送，使其目的无法实现。

2012 年，有几个使用全球事件新闻（甚至人间惨剧）的垃圾邮件的实例，以便达到利用用户的目的。

2011 年，全球垃圾邮件的总量下降了 18%。这远远比不上 2010 年僵尸网络被关闭后垃圾邮件数量急剧下降幅度，但是持续的下降趋势仍是一个积极的进步。

在使影响最大化的同时，垃圾邮件发送者继续将注意力集中在尽可能地降低工作量上面。根据思科的研究，由于周末用户通常不看邮件，垃圾邮件量会下降 25%。垃圾邮件量在周二和周三上升到最高值，比其他几天平均高出 10%。每周中间几天活动量增加，而周末工作量下降，这样，垃圾邮件发送者也可以过上“正常的生活”。

另外，这样一来，在一周的前几天，他们就可以把时间花在根据世界大事件专门设计的活动上，这将有助于提高活动的反响率。

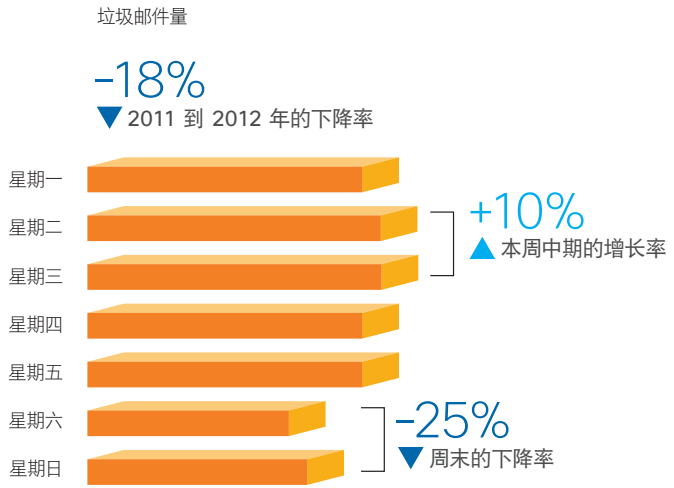
2012 年，有几个利用全球事件新闻（甚至人间惨剧）的垃圾邮件的实例，以便达到利用用户的目的。 例如，在飓风桑迪肆掠期间，思科的研究人员发现大量基于垃圾邮件活动的“哄抬和抛售”股票诈骗。垃圾邮件发送者利用既有的、鼓励人们购买关注自然资源利用的低价股的电子邮件消息，并附上具有轰动性的有关飓风桑迪的标题。这类活动的独特之处就在于：垃圾邮件发送者利用了唯一的 IP 地址发送一批垃圾邮件，且之后不会激活这些地址。

垃圾邮件来源地

一些国家在垃圾邮件排名中保持不变，而其他国家则正在发生巨大变化。2012 年，印度仍旧位居全球垃圾邮件来源地的榜首，美国由从 2011 年的第六位跃至 2012 年的第二位。前五名的垃圾邮件来源地还有韩国（第三）、中国（第四）和越南（第五）。

图 13: 垃圾邮件来源国

印度仍然是最大的垃圾邮件来源国，而美国则迅速攀升至第二位。



总之，大多数垃圾邮件发送者的主要工作是创建垃圾邮件，这些邮件采用经常使用电子邮件的最大的受众群体的语言。根据思科的研究报告，2012 年垃圾邮件消息最常用的语言是英语，紧跟其后的是俄语、加泰罗尼亚语、日语和丹麦语。值得注意的是，垃圾邮件的发送地和垃圾邮件使用的语言之间有差距，例如，2012 年印度是第一大垃圾邮件来源国，但印度当地方言并没有跻身从印度发送的垃圾邮件最常使用的前十种语言之列。对于韩国、越南和中国，情况也是如此。

图 14: 电子邮件附件

仅有 3% 的垃圾邮件有附件，而有效邮件为 25%，但是，垃圾邮件的附件比有效邮件的附件大 18%。

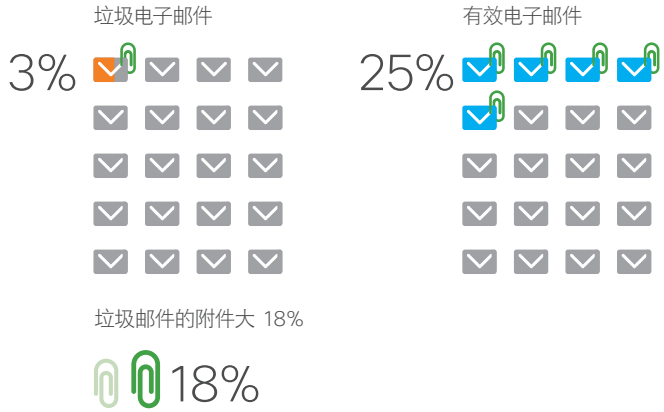
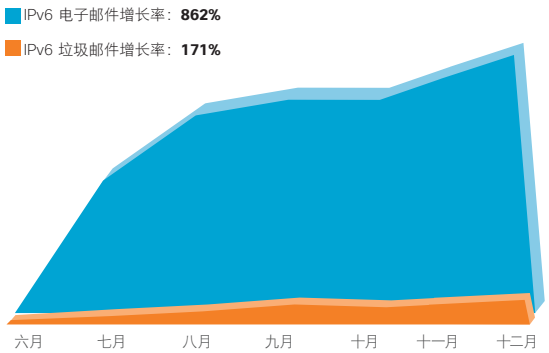


图 15: IPv6 垃圾邮件

尽管基于 IPv6 的电子邮件在总流量中仍旧占很小的比例，但随着更多的电子邮件用户转向启用 IPv6 的基础设施，该类电子邮件的比例正不断上升。



电子邮件附件

长期以来垃圾邮件被视作恶意软件的传播途径，尤其是带附件时。但是思科最近针对在垃圾邮件活动中使用附件的一项研究表明，这种观点可能是错的。

在全部垃圾邮件中，有附件的只占 3%，而有效的电子邮件却占 25%。在极少数情况下，当垃圾邮件消息确实包括附件时，它一般比有效邮件中包括的典型附件大 18%。因此，这些附件往往显得非常突出。

在现代电子邮件中，链接是至关重要的。垃圾邮件设计各种活动，说服用户访问其可以购买产品或服务（往往不可靠）的网站。然后，在用户不知情的情况下收集用户的个人信息，或者通过其他某种途径损害他们的利益。

本节后面的“假冒”品牌分析表明，大多数垃圾邮件来自试图销售非常特定的一组品牌商品（从豪华手表到药品）的群体，这些商品和药品大多数情况下是假的。

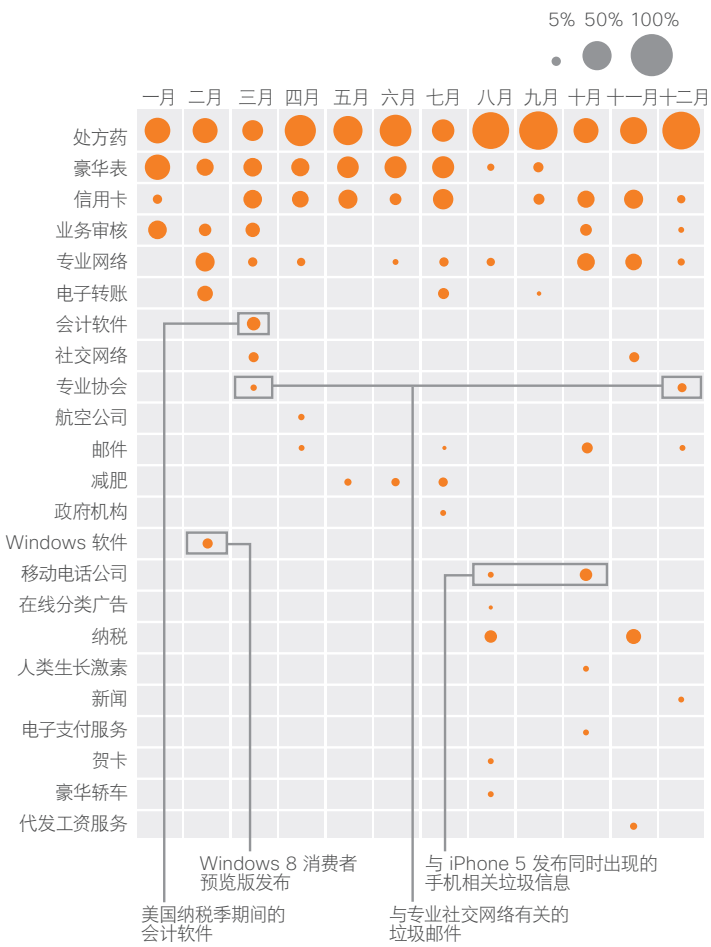
IPv6 垃圾邮件

尽管基于 IPv6 的电子邮件在总流量中仍旧占很小的比例，但随着更多的电子邮件用户转向启用 IPv6 的基础设施，该类电子邮件的比例正不断上升。

然而，当电子邮件总量快速上升，IPv6 垃圾邮件的情况就并非如此。这表明，垃圾邮件发送者为了避免浪费时间和金钱，正转向瞄准新的互联网标准了。对于垃圾邮件发送者而言，目前还没有向这方面转变的推动力，也不会获得物质利益。随着 IPv4 地址用完，移动设备和 M2M 通信推动 IPv6 飞速增长，预计垃圾邮件发送者会升级其基础设施，并加速这方面的努力。

在现代电子邮件中，链接是至关重要的。垃圾邮件设计各种活动，说服用户访问其可以购买产品或服务的网站。然后，在用户不知情的情况下收集用户的个人信息，或者通过其他某种途径损害他们的利益。

图 16: 假冒品牌
垃圾邮件的目标是药品、豪华表和纳税季。



假冒品牌

借助假冒品牌垃圾邮件，垃圾邮件发送者使用公司和产品发送其消息，希望在线用户点击链接或购买。大多数假冒品牌是药品处方，例如，抗焦虑抑郁药物治疗和止痛药。另外，豪华表品牌形成在全年始终保持的一个连续不断的“噪音”层。

思科的分析显示，垃圾邮件发送者也擅长将其活动和新闻事件捆绑。从 2012 年 1 月到 3 月，思科的数据显示，和 Windows 软件有关的垃圾邮件激增，这与 Windows 8 操作系统的发布有关。分析显示，在 2012 年 2 月到 4 月的美国 纳税季期间，税务软件垃圾邮件急剧上升。

从 2012 年 1 月到 3 月，然后又从 2012 年 9 月到 12 月（年初和年尾）和专业网络有关的垃圾邮件闪亮登场，这也许是因为垃圾邮件发送者知道人们通常在每年的这段时间内开始求职。

最根本的是，垃圾邮件发送者这么做就是为了挣钱，在过去几年里，他们已经认识到，吸引用户点击量和购买的最快捷的方法是：提供药品和奢侈品，并且根据全世界大部分人正关注的大事件来调整攻击策略。

从 2012 年 9 月到 11 月，在 iPhone 5 发布的同时，垃圾邮件发送者开展了一系列活动，伪装成移动电话公司 。

最根本的是，垃圾邮件发送者这么做就是为了挣钱，在过去几年里，他们已经认识到，吸引用户点击量和购买的最快捷的方法是：提供药品和奢侈品，并且根据全世界大部分人正关注的大事件来调整攻击策略。

漏洞管理：提供商必须做得更多，而不只是很矛盾地列举漏洞[35]

提供商如何公布其产品安全问题是其漏洞管理实践最显著的一个方面。在思科，安全通报[36] 经产品安全事故响应小组 (PSIRT) 研究后发布，该小组由了解如何保护思科必须与其携手合作的客户和公司的高级安全专家组成。

“安全通报公布我们最严重的产品安全问题，通常是对思科产品安全漏洞的首次公开证明，”思科安全研究和运营高级总裁 Russell Smoak 说，“因此，关键是它们必须是有效的通信工具，有助于通知客户作出决策并管理其风险。我们同时采用高级缓解技术[37]，使客户作好利用现有的思科设备的功能的准备，我们会提供尽可能多的细节，以作出快速自信的响应。”

但是，漏洞管理在漏洞的生命周期的很早的阶段开始，能够延伸到首次公布之后。“不断进化的威胁和新产品新技术，使安全环境发生日新月异的变化，要跟上安全环境变化的步伐，必须持续改进漏洞管理实践，”Smoak 说。

换言之，供应商如果未能跟随威胁技术一起进步（未能披露威胁），今后就会有风险。例如，已经在绑定第三方软件领域展开对思科的互联网漏洞管理工具的创新。第三方软件就是提供商产品中包含的不是由提供商自己编写的任何代码；这通常包括第三方商业软件或开源软件。

当第三方软件引起的安全问题可能会影响思科的产品时，思科会利用定制的工具，使用 Cisco IntelliShield[38] 的漏洞数据来通知产品开发团队。该工具被称为思科内部警报管理器，它大大提高了管理非思科代码引起的安全问题的能力。

> 供应商如果未能跟随威胁技术一起进步（未能披露威胁），今后就会有风险。

还应持续改进安全披露实践。在 2013 年初，思科将开始采用新的文件类型（思科安全通知）来披露严重程度为低到中的安全产品问题。思科安全通知将提高被认为严重程度不足以发布思科安全通报的安全问题的沟通效率。这些文档将对外开放，并按通用漏洞披露 (CVE) 标识符编索引，以提高可视性。

为了进一步改进更好地领会持续报告的安全问题的方式，提供商（包括思科）已经开始将通用漏洞报告框架 (CVRF)[39] 和开放式漏洞评估语言 (OVAL)[40] 格式纳入到披露范围。 这些新出现的标准可以帮助终端用户充满信心地评估多个平台和技术中的安全漏洞。而且，得益于机器可读的格式，这些标准还能够灵活扩展。Smoak 说，“通过确保我们的客户拥有正确评估网络威胁所需的工具，帮助降低风险，使他们可以优先处理保护基础设施安全所需的任务。”

有关明年额外的最新安全发展趋势和深入分析信息，以及和企业安全有关的思科最新出版物的相关信息，请访问思科安全报告网站。
http://www.cisco.com/go/securityreport

欲了解目前思科专家对各种安全主题的看法，请访问思科安全博客。
blogs.cisco.com/security

2013 年安全形势展望

目前的威胁形势问题不是因为未受过教育的用户访问恶意网站造成的，否则通过阻止 Web 上已知的“有害的”位置就可以解决。

本报告已经演示攻击者在跟踪非常受信任且用户最经常访问的网站、工具和应用方面是如何变得越来越熟练的。新威胁能够悄无声息和有效地感染大批受众，而不分行业、企业规模或国家。在当今“任意互联”的世界，个人可以使用任何设备访问他们的商业网络。犯罪分子正是利用其中快速扩大的攻击面这一点。

随着关键的国家基础设施、企业和全球金融市场继续转向基于云的服务和移动通信连接，需要采用一个综合的、分层的安全方法来保护迅速发展的“万物互联”。“黑客和网络犯罪分子利用每个私有或公共部门的企业都有自己的 IT 安全计划这一点，”John Stewart 说。“是的，我们去参加会议，彼此保持联系，但是我们真正需要的是从个人的 IT 安全转向一个基于实时智能共享和共同响应的 IT 安全。”

建立优化的安全基础设施并不意味着创建更复杂的架构。而事实正好相反。它意味着使基础设施和基础设施内的元素共同配合，通过更多的信息来检测并降低威胁。BYOD 的快速应用，每个用

新威胁能够悄无声息和有效地感染大批受众，而不分行业、企业规模或国家。

户有多台设备的事实，以及基于云的服务的增长，使每个终端上管理安全能力的时代一去不复返。“我们必须采取全面的安全方法，确保我们监控包含电子邮件、网站和用户本身的所有媒介的威胁，”Cisco SIO 的产品经理 Michael Covington 说。“威胁智能需要提升到个人平台以上的高度，以获得对网络全面的认识。”

由于威胁不断针对多个媒介上的用户和公司，因此，企业需要收集、存储和处理所有和安全有关的网络活动，以更好地了解攻击的范围和程度。然后，可以根据网络活动背景扩大分析范围，以作出准确及时的安全决策。随着攻击者水平提高，企业必须从一开始就借助解决方案，设计网络的安全功能。这些解决方案汇集威胁智能、安全政策和可在网络上的所有接触点执行的控制。

随着攻击者水平提高，因此，用于阻止攻击的工具也必须变得更加精密。由于网络提供不同平台之间通用的通信基本结构，因此，它还将用作保护经常使用它来交换敏感内容的设备、服务和用户的途径。未来的网络是智能网络，必须通过各个组件的集合，通过协作框架提供比以前更好的安全性。

未来的网络是智能网络，必须通过各个组件的集合，通过协作框架提供比以前更好的安全性。

关于思科安全智能运营中心

当前，如何管理和保护灵活的分布式网络已经成为一种日益严峻的挑战。

网络犯罪分子持续不断地利用用户对消费应用和设备的信任牟利，导致组织和员工面临的风险日益增加。传统的安全方法依赖于产品分层和多重过滤器的使用，而这已经不足以抵御最新一代恶意软件的攻击，因为它们不仅传播迅速、目标遍布全球，而且能够利用多种载体进行增殖。

思科采用思科安全情报运营中心 (SIO) 的实时威胁情报抵御最新的威胁，能够始终做到未雨绸缪。Cisco SIO 是世界上规模最大的云安全生态系统，其中来自部署的思科邮件、网站、防火墙和 IPS 解决方案的 75 T 以上的实时数据源每天都会进行分析。

Cisco SIO 汇总了来自威胁载体的数据，并使用自动算法和手动处理加以分析，以理解如何威胁如何传播。然后，SIO 对威胁进行分类并使用 200 多个参数创建规则。安全研究人员还会针对可能对网络、应用和设备造成广泛影响的安全事件，收集并提供相关信息。每三到五分钟，系统就会为已部署的思科安全设备动态提供安全规则。

Cisco SIO 是世界上规模最大的云安全生态系统，其中来自部署的思科邮件、网站、防火墙和 IPS 解决方案的 75 T 以上的实时数据源每天都会进行分析。

Cisco SIO 团队还将发布安全防护最佳实践建议，以及抵御安全威胁的战术指导。思科致力于为世界各地的组织提供一体化、及时、综合且有效实现全方位安全性的全面安全解决方案。有了思科，各公司就可以省下研究威胁与漏洞的时间，集中精力实施主动的安全做法。

如需预警情报、威胁和漏洞分析，以及久经验证的思科避险解决方案，请访问：http://www.cisco.com/security。

方法

本报告中的分析介绍基于从各种匿名全球资源收集的数据，包括思科邮件、网站、防火墙和入侵防御系统 (IPS) 安全解决方案；这些平台处于保护客户网络的最前沿，使其免受恶意内容和入侵者的侵扰。除了这些客户自有设备保护机制外，思科还通过全球部署的传感器收集数据，这些传感器执行捕获垃圾邮件和在网络上积极寻找新型恶意软件的功能。

通过利用这些工具和它们收集的数据，思科实现对网络的广泛覆盖，这让思科 SIO 系统和研究人员可以了解对互联网上合法和恶意活动的惊人的取样工作。没有哪个安全提供商能完全洞察到所有遭遇恶意内容的情况。本报告所载的数据反映了思科对目前威胁形势的看法，表明我们将尽最大努力使数据标准化，反映了基于目前可用的数据的全球发展趋势和模式。

思科通过全球部署的传感器收集数据，这些传感器执行捕获垃圾邮件和在网络上积极寻找新型恶意软件的功能。

Cisco Security IntelliShield Alert Manager 服务

Cisco Security IntelliShield 警报管理器服务提供了一种全面且经济高效的解决方案，可为组织识别、预防和缓解 IT 攻击提供所需的厂商中立型安全智能。使用这种基于 Web 的可定制威胁和漏洞警报服务，安全人员可获取及时、准确且可靠的威胁和安全漏洞信息，从而避免其环境受到影响。IntelliShield 警报管理器可以让企业减少对威胁和漏洞研究的投入，从而将更多精力放在主动式安全方法上。

思科提供为期 90 天的 Cisco Security IntelliShield 警报管理器免费试用服务。只要注册参加此次试用，您就能获取完整的服务使用权限，包括工具、威胁和漏洞警报。

有关 Cisco Security IntelliShield 警报管理器服务的详情，请访问：https://intellishield.cisco.com/security/alertmanager/trialdo?dispatch=4。

更多详情

思科安全情报运营中心
www.cisco.com/security

思科安全博客
blogs.cisco.com/security

思科远程管理服务
www.cisco.com/en/US/products/ps6192/serv_category_home

思科安全产品
www.cisco.com/go/security

思科企业安全计划部
www.cisco.com/go/cspo

[1] “物联网，”作者：Michael Chui, Markus Löffler 和 Roger Roberts, *McKinsey Quarterly*, 2010 年 3 月：http://www.mckinseyquarterly.com/The_Internet_of_Things_2538。

[2] “思科事件响应：针对金融机构的分布式拒绝服务攻击，”2012年10月1日：http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html。

[3] 思科互联网企业解决方案小组。

[4] “互联世界设备全球市场 - 2012 版，”新闻稿，《IMS 研究》，2012年10月4日：http://imsresearch.com/press-release/Internet_Connected_Devices_Approaching_10_Billion_to_exceed_28_Billion_by_2020&cat_id=210&type=LatestResearch。

[5] 思科互联网企业解决方案小组。

[6] “万物互联重在连接，”作者：Dave Evans, 思科博客, 2012 年11 月 29 日：http://blogs.cisco.com/news/internet-of-everything-its-the-connections-that-matter/。

[7] 思科互联网企业解决方案小组。

[8] 《思科 2011 年度安全报告》，2011 年 12 月：www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf。

[9] “远程访问和 BYOD：企业努力找寻与员工的共同点，”《2011 思科年度安全报告》，2011 年 12 月，第 10 页：http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf。

[10] “思科全球云指数：预测和方法，2011-2016”：http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html。

[11] 同上

[12] “深入了解劫持软件，”作者：Dimitri McKay,《安全周刊》，2011 年 2 月 3 日：http://www.securityweek.com/deep-dive-hyperjacking。

[13] 印度要求巴基斯坦调查恐慌的原因，”作者：Jim Yardley,《纽约时报》，2012 年 8 月19 日：http://www.nytimes.com/2012/08/20/world/asia/india-asks-pakistan-to-help-investigate-root-of-panic.html?_r=1&。

[14] “Twitter 谣言使油价飙升，”作者：Nicole Friedman, WSJ.com, 2012 年 8 月 6 日：http://online.wsj.com/article/SB10000872396390444246904577573661207457898.html。

[15] 这条信息最开始出现在思科安全博客上：http://blogs.cisco.com/security/sniffing-out-social-media-disinformation/

[16] Java.com: http://www.java.com/en/about/.

[17] Vishwath Mohan 和 Kevin W. Hamlen。*Frankenstein：通过无害的二进制文件修补恶意软件*。在 USENIX 攻击性技术研讨会 (WOOT) 的会议记录中，第 77-84 页，2012 年 8 月。

[18] Mohammad M. Masud, Tahseen M. Al-Khateeb, Kevin W. Hamlen, Jing Gao, Latifur Khan, Jiawei Han 和 Bhavani Thuraisingham。“基于云的”恶意软件检测以改进数据流。美国计算机学会 管理信息系统会报 (TMIS), 2(3), 2011 年 10 月。

[19] “DDoS 攻击：2013 预测，专家认为最近的攻击只是开始，”作者：Tracy Kitten, BankInfoSecurity.com, 2012年12 月 30 日：http://ffiec.bankinfosecurity.com/ddos-attacks-2013-forecast-a-5396。

[20] “恶意滥用 DNS 中的实现缺陷，”*DNS 最佳实践、网络防护和攻击识别*, Cisco.com: http://www.cisco.com/web/about/security/intelligence/dns-bcp.html#3。

[21] “IP 欺骗，”作者：兰德大学, Farha Ali, 可从以下网站找到：Cisco.com: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html.

[22] “分布式拒绝服务攻击，”作者：雅典国家技术大学, Charalampos Patrikakis, Michalis Masikos 和 Olga Zouraraki,《互联网协议杂志》 - 第 7 卷，第 4 册。可从以下网站找到：http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html。

[23] “DNS 工具，”测量工厂：http://dns.measurement-factory.com/tools。

[24] 欲知有关 DNS 工具的更多详情，请参阅 DNS-OARC (https://www.dns-oarc.net/oarc/tools) and The Measurement Factory (http://dns.measurement-factory.com/tools/index.html)。

[25] “固定绑定模板，版本 7.3 07, 2012 年 8 月，”作者：TEAM CYMRU, cymru.com: http://www.cymru.com/Documents/secure-bind-template.html。

[26] “域名系统的响应流量限制 (DNS RRL)，”RedBarn.org: http://www.redbarn.org/dns/ratelimits。

[27] Arbor 网络的 ATLAS 数据来自全球服务提供商网络内部署的“蜜罐”：ASERT 恶意软件研究；及按小时提供的基于 NetFlow、BGP 和 SNMP 关联的匿名数据。Arbor Peakflow SP 客户提供的匿名数据在 ATLAS 中进行核对和趋势分析，以提供对互联网的威胁和流量模式的详细信息。

[28] “IPS 测试，”Cisco.com: http://www.cisco.com/web/about/security/intelligence/cwilliams-ips.html。

[29] “美国银行和纽约证券交易正在受到攻击 unt [sic]，”Pastebin.com, 2012年9月18日：http://pastebin.com/mCHia4W5。

[30] “燕子行动的第二个阶段，”Pastebin.com, 2012 年 9 月18 日：http://pastebin.com/E4f7fmB5。

[31] “思科事件响应：针对金融机构的分布式拒绝服务攻击”：http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html。

[32] 识别和降低针对金融机构的分布式拒绝服务攻击的影响*应用的缓解通告*：http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=27115.

[33] “安全智能操作策略资源，”Cisco.com: http://tools.cisco.com/security/center/intelliPapers.x?i=55。

[34] “服务提供商安全最佳实践，”Cisco.com: http://tools.cisco.com/security/center/serviceProviders.x?i=76。

[35] Anagram courtesy of anagramgenius.com。

[36] 思科安全咨询：http://cisco.com/go/psirt。

[37] 思科应用缓解通知, Cisco.com: http://tools.cisco.com/security/center/searchAIR.x。

[38] Cisco Intellishield 警报管理器服务：http://www.cisco.com/web/services/portfolio/product-technical-support/intellishield/index.html。

[39] CVRF, ICASI.com: http://www.icasi.org/cvrf.

[40] OVAL, Oval International: http://oval.mitre.org/.