思科 2014 年度安全报告

执行摘要

信任问题

信任利用是网络攻击者和其他恶意攻击实施者采用的通用操作模式。他们充分利用用户对系统、应用程序以及用户日常互动往来的人员和公司的信任。此方法屡试不爽：有充分证据表明，网络攻击者不断采用新方法，将恶意软件嵌入网络，长时间潜伏，并窃取数据或破坏重要系统。

从利用社交工程窃取密码和证书到数分钟内完成的视而不见的隐秘渗透等各种不同的方法，恶意攻击实施者继续利用公众信任，以实现危害结果。但是，信任问题的危害已超出罪犯利用漏洞或者通过社交工程捕食用户：它破坏上市和私营企业的自信。

当今的网络正面临着两种形式的信任侵蚀。一种是客户对产品完整性的信任度日渐下降。另一种是恶意攻击实施者击溃信任机制，因此导致用户质疑网络和应用程序保证、身份验证和授权体系结构的有效性。

在本报告中，思科列出大量数据论证顶级安全问题，并提出深刻洞察，例如恶意软件移位、漏洞趋势以及分布式拒绝服务 (DDoS) 攻击再现。该报告还论述了瞄准特定企业、群体和行业的网络攻击活动，以及试图窃取敏感信息之人的技能日益老练。报告最后建议全盘检查安全模式，并使连续攻击全程清晰可见 – 攻击之前、期间和之后。

恶毒的行动者不断想出新的办法利用公众的信任来对危害性结果施加影响。

关键发现

以下为*思科 2014 年度安全报告*的三大关键研究结果：

正在瞄准全球重要互联网资源的基础结构进行攻击。

- 恶意攻击正获得权限访问网络托管服务器、域名服务器和数据中心。建议完成 überbot 成型，以寻求声誉卓著且资源丰富的资产。
- 主要威胁是缓冲区错误，占据常见缺陷列表 (CWE) 威胁类别的 21% 份额。
- 恶意软件遭遇正转向电子制造业和农业和采矿业，约是全行业纵向市场平均遭遇率的六倍。

恶意攻击实施者正使用受信赖的应用程序渗透并利用外围网络安全漏洞。

- 垃圾邮件继续呈下降趋势，虽然恶意垃圾邮件的比例保持不变。
- Java 占 Web 攻击的 91%；使用思科网络安全服务的公司中有 76% 的公司正在运行 Java 6 - 寿命终止的不受支持的版本。
- “酒吧”攻击正瞄准特定行业相关网站，以传播恶意软件。

跨国公司的调查显示其存在大量内部泄漏证据。从其网络流出大量可疑流量，并试图连接到可疑网站（100 的公司调用恶意软件主机）。

- 入侵指标显示，可能长时间未发现网络渗透。
- 威胁警报数年复增长 14%；新警报数（未更新警报）正在逐年上升。
- 2013 年，99% 的移动设备恶意软件全部针对 Android 设备。Android 用户遭遇所有形式的网络传播恶意软件的遭遇率也最高 (71%)。

报告内容

*思科 2014 年度安全报告*提供四大关键领域的安全洞察：

信任

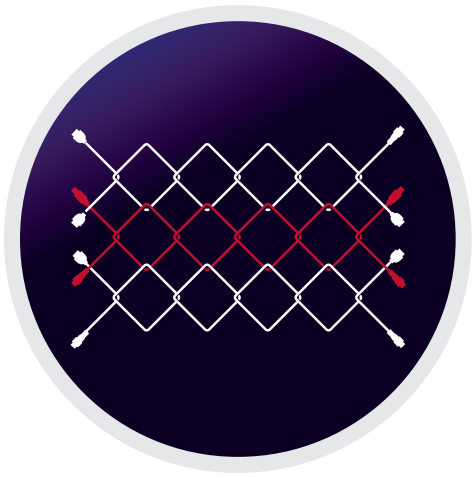
所有企业都迫切希望找到信任、透明度和隐私之间的绝佳平衡，因为此事事关重大。在这方面，我们详细论述安全防护从业者试图帮助所在企业实现这种更具挑战性的平衡而面临的三大压力：

- 攻击面扩大
- 攻击模式扩散且手法熟练
- 威胁和解决方案异常复杂

威胁智能

思科和 Sourcefire 使用现今最大的检测遥测套组，共同分析和汇集去年的安全洞察。

- 正在瞄准全球重要互联网资源的基础结构进行攻击。
- 恶意攻击实施者正使用受信赖的应用程序渗透并利用外围网络安全漏洞。
- 入侵指标显示，可能长时间未发现网络渗透。



行业

在本章节，思科安全智能运营中心（SIO）调查员提起有关超出思科遥测范围，但仍影响安全实践的行业趋势的讨论：从暴力登录尝试、大规模 DDoS 攻击活动和勒索努力，到不断增长的云计算依赖、缺乏安全防护人才和其他问题。

建议

众多企业面临攻击面扩大、攻击模式不断扩散且手法日益熟练以及网络威胁和解决方案日益复杂等三大压力。许多组织努力制定有效战略，使用新技术，简化自身体系结构和运营，并增强安全团队实力，以巩固安全愿景。

本章节论述以威胁为中心的安全模式如何使防卫者解决横跨所有攻击载体的连续攻击，并以连续方式随时进行响应 – 攻击之前、期间和之后。

思科如何评估威胁环境

鉴于思科解决方案极为盛行，安全智能广度超广，思科在评估威胁方面起到重要作用：

- 思科云网络安全每天检查 160 亿个网络请求
- 思科托管电子邮件解决方案每天检查 930 亿封电子邮件
- 每天评估 200,000 个 IP 地址
- 每天评估 400,000 个恶意软件样本
- FireAMP 每天评估 3300 万份端点文件
- FireAMP 每天评估 2800 万次网络连接

此项活动导致思科检测到以下威胁：

- 每天有 45 亿封电子邮件被阻止
- 每天有 8000 万个网络请求被阻止
- FireAMP 每天检测 6450 份端点文件
- FireAMP 每天检测 3186 个端点网络
- 每天检测到 50,000 次网络入侵

目录

信任 8

经商新方式、新安全漏洞 9
信任侵蚀 11
2014 年度主要安全挑战 12
值得信赖的透明系统 16

威胁智能感知系统 20

威胁警报日益增多 21
垃圾邮件总量呈下降趋势，但恶意垃圾邮件仍具威胁 24
Web 攻击：Java 居首 28
BYOD 和移动性：设备成熟惠及网络犯罪 32
针对性攻击：驱逐持续且到处渗透的“访客”的挑战 36
恶意软件快照：观察到的 2013 年度趋势 38
主要目标：行业纵向市场 41
脆弱生态系统断裂 43
通常是针对性攻击征兆且可在所有企业网络中检测到的恶意流量 48

行业 52

暴力登录尝试受青睐的入侵网站战术 53
DDoS 攻击：去而复返 55
DarkSeoul 57
安全人才短缺和解决方案漏洞 60
新的云外围网络 61

建议 63

2014 年度目标：验证可信度和提高可见度 64

附件 67

安全机构需要数据科学家 68

关于思科 SIO 77

思科 SIO 78

关于本文档

本文档包含可搜索和可共享的内容。

寻找本图标以打开 Adobe Acrobat 中的查找功能。

寻找这些图标以共享内容。

推荐软件

Adobe Acrobat 版本 7.0 及以上

信任

所有企业都迫切希望找到信任、透明度和隐私之间的绝佳平衡，因为此事事关重大。

经商新方式、新安全漏洞

技术供应链的薄弱环节是当今复杂网络威胁和风险特征的其中一个方面。

因此，任意点到点基础结构应运而生，任何位置的任何设备均可通过任何网络例示面世。[1] 具备连网功能的设备数量亦日渐增多—智能手机、平板电脑等—尝试连接到可随时随地运行的应用程序，包括公用软件服务（SaaS）云、私有云或混合云。[2] 甚至基本互联网基础结构服务都已经成为黑客的攻击目标，黑客希望充分利用网络托管服务器、域名服务器和数据中心的声誉、带宽以及连续正常运行时间和可用性，开展越来越大的黑客攻击活动。（参阅第 43 页“脆弱生态系统断裂”。）

虽然诸如云计算和移动性等趋势正在减少能见度，增加安全复杂性，但由于这些趋势对许多企业维持自身竞争优势和业务成功至关重要，因此这些组织仍必须接受它们。但是安全漏洞不断涌现和扩大，尽管安全团队不断尝试使用迅速演化的新经商方式调整传统解决方案。与此同时，恶意攻击实施者正加快利用安全漏洞，非集成式单点解决方案根本无法修补这些安全漏洞。由于掌握诸多资源，可以更敏捷应对，因此他们日益成功。

基本的互联网基础设施已经成为黑客的目标。

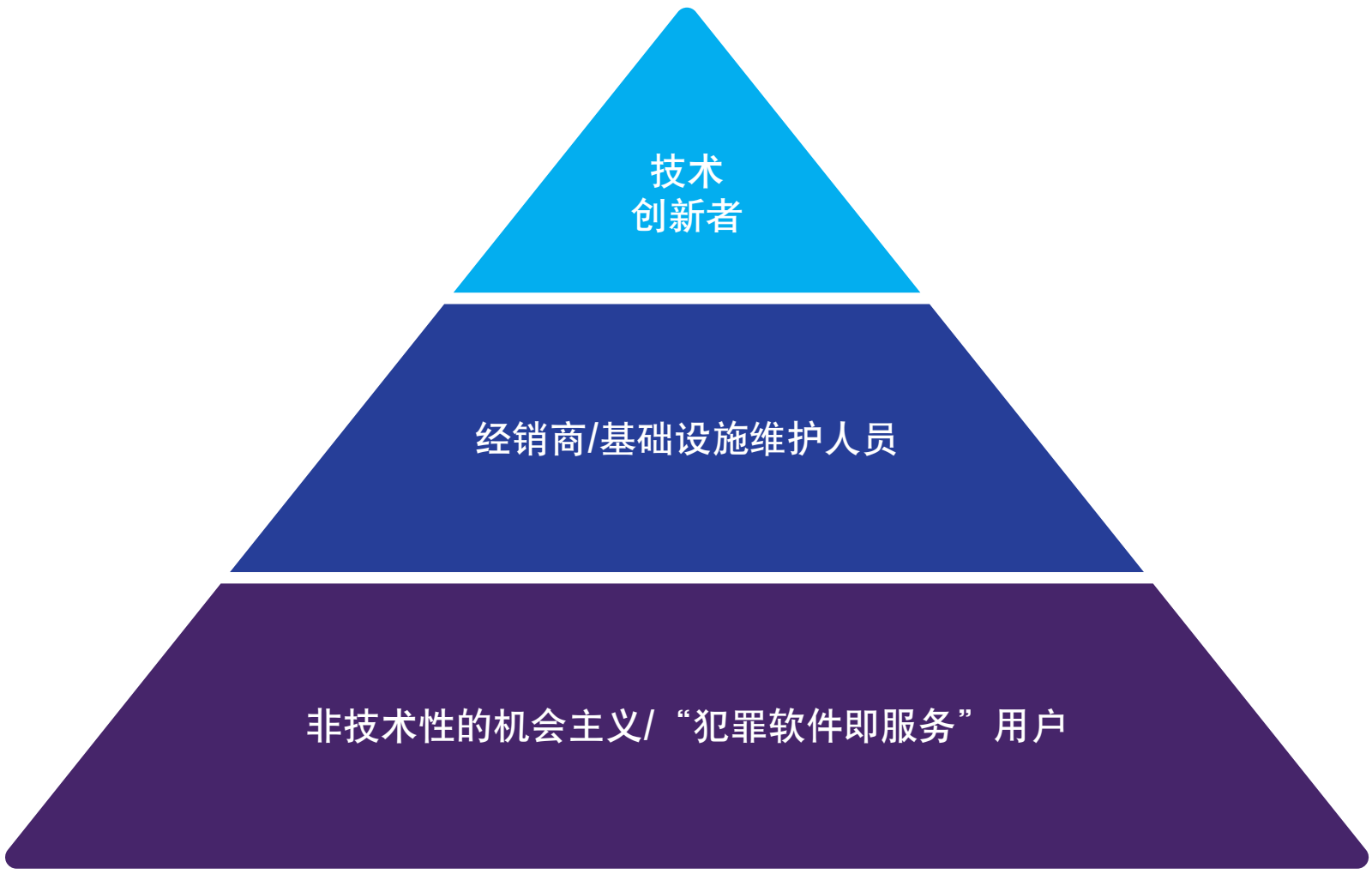
网络犯罪网络正在扩大，实力逐步增强，以及越来越像任何合法、成熟的商业网络那样运行。今天的网络犯罪层次呈金字塔状（见图 1）。底部为非技术机会主义者和“犯罪软件作为服务”的用户，他们想要利用犯罪活动赚钱，发表声明，或两者兼得。中间为中间商和基础结构维护者—“中间人”。顶部为技术创新者—执法机构最想找到，但极力寻找的重要罪犯。

发动攻击时，现代网络犯罪分子通常拥有明确的业务目标。他们知道他们要寻找什么信息，或他们想要取得什么结果，并且他们知道他们需要采取什么途径以实现这些目标。网络攻击者会花费大量时间研究目标，往往是通过社交网络上的公开资料研究目标，并规划他们的战略目标。

“灰色经济”行业内的许多从业者现在还会发送恶意监控软件，以收集环境相关信息，包括已经部署哪些安全技术，以便锁定攻击目标。此类预攻击侦察有助于一些恶意软件编写者确定其恶意软件如何起效。一旦嵌入在网络，他们设计的高级恶意软件能与外部指令控制服务器进行通信，并横向蔓延至整个基础结构，以执行任务，不论是盗取重要数据或破坏重要系统。

图 1

网络犯罪分子等级



信任侵蚀

网络世界恒久存在的现状是，网络犯罪分子运用威胁，以充分利用用户对系统、应用程序以及他们知道的人员和企业的信任。

详细分析几乎所有的计划，核心是滥用信任：将恶意软件交付给合法浏览主流网站的用户。垃圾邮件看似由知名公司发送，但包含恶意网站链接。第三方移动应用程序被植入恶意软件，并从知名在线应用程序市场下载。消息灵通人士利用信息访问权限，窃取雇主的知识产权。

所有用户或许都应设想网络世界内的一切都不能或不应信任。专业安全人员可以通过不信任任何网络流量，为所在企业提供服务[3]—或者通过不完全信赖为企业提供技术的供应商或供应链的安全实践。但是，公共和私营部门的企业、个人用户和国家之间仍希望得到保证，以致他们可以信任他们每天依赖的基础技术。

所有用户都应该假设，网络世界中的一切都不可信，也不应信任。

这种安全信心需求推动信息技术安全评估通用标准（简称“通用标准”）、语言和框架进一步发展，可使政府机构和其他团体定义技术产品必须遵守并满足的要求，以确保这些技术产品值得信赖。目前共有包括美国在内的 26 个国家签订《通用标准互认协议》，此多边协定参与国将互认经评估的技术产品。

但在 2013 年，大体而言，信任遭受了倒退。催化剂：爱德华·斯诺登 (Edward Snowden)。前美国政府承包商向英国*卫报*泄露机密信息 —在完成美国国家安全局 (NSA) 交办任务时获取的信息。[4]

斯诺登向卫报披露的资料包括美国国家安全局的电子监控和数据收集计划 PRISM[5] 以及独立的 NSA-GCHQ[6] 计划 (被称为 MUSCULAR)，美国国安局通过这些计划窃听光纤网络传输的知名互联网公司海外数据中心的流量。[7]

斯诺登揭露的这些计划和其他政府监控行为削弱了许多层面上的信任：国家之间、政府和私营部门之间、公民个人与政府之间以及公民个人和公共和私营部门企业之间。这些事实也自然引起人们担忧技术产品非故意漏洞和故意预留的“后门”的当前和潜在风险，以及供应商是否采取足够措施，以防止出现这些弱点并保护最终用户。

2014 年度主要安全挑战

[由于信任受到侵蚀，因此更难定义哪些系统和关系值得信赖，哪些不值得信赖，并且企业面临如下几个严重破坏其解决安全问题的能力的关键问题：

1 | 攻击面扩大
2 | 攻击模式扩散且手法娴熟
3 | 威胁和解决方案异常复杂]

这些问题共同创建和加剧安全漏洞，可使恶意攻击实施者在企业修补其安全漏洞之前发动攻击。

这些威胁和风险将在后续几页进行更详细说明。

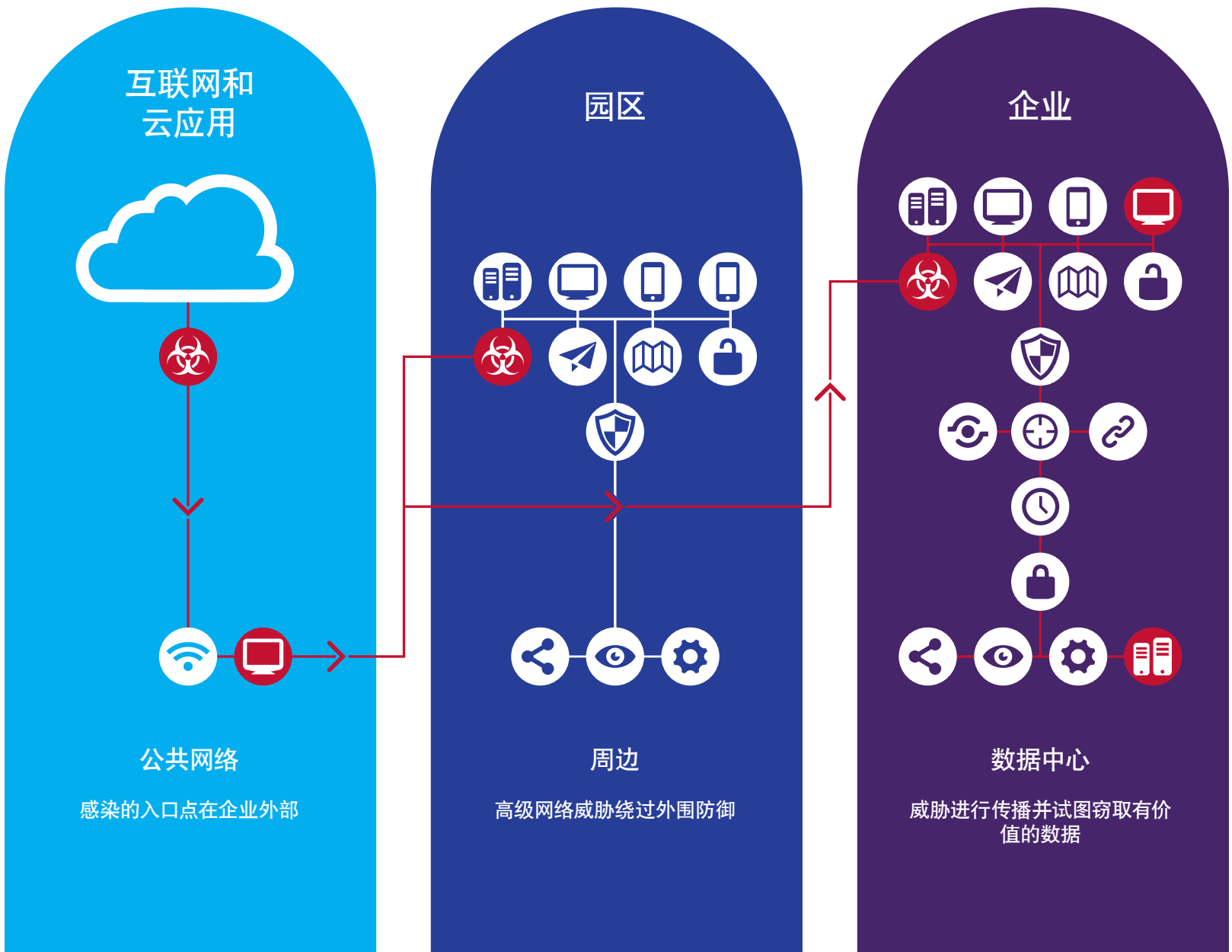
1 攻击面扩大

当前的攻击面非常广，可使恶意攻击实施者随意破坏庞大而脆弱的安全生态系统。攻击面呈指数级增长，并且仍在不断扩大，不受企业控制端点、侵袭和数据实在太多。

大多数网络攻击者想要通过攻击活动获得的奖励是数据，因为数据本质上是货币。如果数据拥有任何“街头黑市价”，不论是大公司的知识产权或个人的医疗资料，均处在危险之中。如果目标的价值大于攻击风险，即会被黑客攻击。即使小型企业亦存在被黑客攻击的风险。大多数大型和小型企业已被入侵，但仍不知情：思科分析的所有商业网络均有流量流向托管恶意软件的网站。

图 2

现代威胁剖析



现代威胁的分析结果概述于图 2，着重说明了许多网络犯罪活动的最终目标如何达到数据中心，并窃取重要数据。在本示例中，公司网络之外的设备受到恶意攻击。它导致设备感染病毒，进而蔓延到校园网。该网络充当企业网络的起跳板，然后威胁直达宝库：数据中心。

网络犯罪活动的最终目标是进入数据中心并泄露宝贵的数据。

鉴于黑客扩大攻击面和瞄准高价值数据，思科安全专家建议企业在 2014 年回答两大重要问题："我们的关键数据驻存在何处？"和"我们如何创建安全环境以保护数据，尤其是云计算和移动性等新业务模式导致我们几乎无法控制它时？"

2 攻击模式扩散且手法娴熟

当前的威胁环境完全不同于 10 年前。导致损害可控的简单攻击早已让位给现代网络犯罪，复杂严密，资金雄厚，并能导致企业遭受严重破坏。

众多公司已成为针对性攻击的焦点。这些攻击极难察觉，长时间留在网络内，并积累网络资源，以便在其他地方发动攻击。

要控制住连续攻击全程，企业需要使用可随处运行的解决方案访问各类攻击载体。威胁可在网络、端点、移动设备和虚拟环境内自我显现。

> "我们的关键数据在哪里"以及"我们如何建立安全的环境来保护我们的哦数据，尤其是在云计算和移动性等新的业务模式使我们几乎不能控制数据的情况下？"
>
> 思科安全专家说

3 威胁和解决方案异常复杂

垃圾邮件拦截程序和反病毒软件以往曾帮助防范大多数威胁入侵容易定义的外围网络，如今却已一去不返。当今网络已超越传统界限，持续演进，并产生新攻击载体：移动设备、具备联网功能的移动应用程序、管理程序、社交媒体、网络浏览器、家用电脑和汽车。时间点解决方案难以应付恶意攻击实施者使用的种种技术和战略。这使得安全保障团队更加难以监控和管理信息安全。

由于企业采用无组织的单点解决方案和多管理平台，因此组织漏洞日益增多。结果导致横各跨控制点的诸多技术迥然不同，且其从未被设计成可共同协作。这导致客户信息、知识产权和其他敏感信息被入侵的可能性增加，并使企业声誉面临受损风险。

时间点解决方案无法对恶意行动者使用的各种技术和策略做出反应。

需要能够持续找到最佳机会，以应对复杂威胁环境的挑战。残酷无情的攻击并非只在某个时间点发动，而是会持续发动。因此，企业必须时刻防范。

鉴于威胁的复杂性和相应的解决方案需求始终非常高，企业需要反思其安全战略。他们可持续在其网络内集成安全特性，最大持续减少复杂性，而并非依赖单点解决方案，因此网络能：

- 持续监控和分析文件，并在恶意攻击开始后，确定后续恶意攻击行为。
- 帮助企业逐步加强执行力度，扩大网络设备的部署范围。
- 加快检测，因为可借此发现更多流量。
- 使企业能够聚集独特的环境意识，这种意识不可能仅依赖安全特定设备获得。

转向移动性和云计算服务导致端点和移动设备所承担的安全责任日益增加，在某些情况下，这些这边从未连接到企业网络。事实是，使用移动设备访问企业资源时，即会带来安全性风险；这些设备可以轻松连接到第三方云服务和计算机，其安全特性可能未知，并且不受企业控制。此外，移动设备恶意软件日益增多，导致安全性风险进一步增加。如果缺乏基本可见性，大多数 IT 安全团队均无法确定这些设备的潜在威胁。

使用移动设备访问公司资源时会带来风险。

诸如持续能力等高级方法在使用大数据分析化解高级恶意软件威胁方面发挥更大作用；大数据分析会聚合更大网络的数据和事件，提供更大可见性，即使是在文件被移进网络或端点之间。这不同于时间点端点安全，端点安全会在初始时间点扫描文件，以确定恶意软件配置。高级恶意软件会规避此类扫描，迅速在端点建立，并在整个网络内扩散。

值得信赖的透明系统

鉴于攻击面扩大，攻击模式日益扩散且手法娴熟，以及威胁和解决方案的异常复杂，我们需要信任我们消费的信息，以及传输这些信息的系统，不论我们如何访问联网服务。

随着政府和企业大量投资开发移动性、协作、云计算以及其他形式虚拟化，打造真正安全的网络环境变得越发复杂。这些能力有助于提高灵活性，提高效率，并减少成本，但也会导致风险增加。随着伪造和篡改产品问题的性质和形势日益严重，生产信息技术产品的制造流程目前亦存在安全性风险。因此，网络安全及其相关的信任问题毫无疑问成为当今政府和企业领导人关注的首要问题。安全从业人员应该询问的问题是：如果我们知道系统破解迫在眉睫，我们该如何化解？

恶意攻击实施者努力寻找并利用技术供应链的任何安全漏洞。技术产品的漏洞和故意预留的后门最终会被他们利用，以窃取整个系统的访问权限。后门是长期以来一直存在的安全问题，应当引起企业重视，因为它们的存在仅有助于促进网络攻击者实施暗中攻击或犯罪活动。

开发值得信赖的系统意味着从头开始，在产品生命周期内从始至终为系统构建安全防护盾。思科安全开发生命周期（CSDL）[8] 规定了可重复且可测量的方法，其旨在产品概念阶段构建产品安全，在开发阶段最大程度减少漏洞，并提高产品对攻击的抵御能力。

恶意行动者会找到并利用技术供应链中的安全漏洞。

值得信赖的系统为不断改进的、旨在预测和阻击新威胁的安全方法提供基础。此类基础设施不仅能保护关键信息，而且更为重要的是，亦有助于避免关键服务中断。受可信任的供应商支持的值得信赖的产品可让用户最大程度降低因为信息盗用、服务中断和信息泄露付出的代价和声誉损失。

但是，值得信赖的系统不应与免受外部攻击混为一谈。信息技术客户和用户在维持值得信赖的系统有效抵御干扰其运行的尝试方面发挥重要作用。这包括及时安装专注安全的更新和补丁，持续保持警惕以识别异常系统行为，以及有效反制攻击。

现在的首席信息安全官 2014 年最关心的问题

首席信息安全官 (CISO) 调查现在的威胁环境时，他们面临的压力不断增加，他们要保护数以 TB 计的数据、满足严格的合规要求、评估与第三方供应商合作的风险，他们需要利用缩减的预算和精简的 IT 团队做这些工作。CISO 需要管理比以前更加多、更加精细和复杂的威胁。向 CISO 为其公司推荐了安全方法的思科安全服务的主要的安全战略家，制订了这一 2014 年最紧迫的问题和挑战列表：

管理的合规性

CISO 中最普遍的问题可能是，需要保护整个渗透性越来越高的网络中的数据，同时还要在合规性方面花费宝贵的资源。只有合规不等价于安全 — 合规只是专注于对特殊监管环境的需要的最低底线。同时，安全是一个包罗万象的方法，涵盖所有商业活动。

信任云

CISO 必须就如何利用分配给他们的有限预算和时间安全地管理信息做出决定。例如，云已经成为管理不断增长的数据仓库的划算而灵活的方法，但是也给 CISO 带来了更多担忧。首席执行官和董事会把云当作淘汰昂贵的硬件的灵丹妙药。他们希望将数据卸载到云来获得利益，并希望 CISO 安全快速地实现这一点。

接下一页

技术不会止步不前，攻击者当然也不会。确保系统值得信赖需要涵盖网络的整个生命周期，即从初始设计到制造、系统集成、日常运营、维护和更新以及解决方案的最终停用。

对于值得信赖的系统的迫切需求早已超出企业自身的网络，包括企业与之连接的网络。思科安全研究和运营团队已观察到去年“数据透视”的使用量增多。网络犯罪的数据透视方法包括使用后门、漏洞或在攻击链的某一时刻利用信任作为跳板，发动针对更大目标的更加复杂的攻击 – 如大型能源公司的网络或金融机构的数据中心。有些黑客利用企业间的信任作为数据透视的基础，利用某个受信任的企业合作伙伴瞄准并利用其他不知情的受信任的企业或政府合作伙伴。

当前网络威胁随处可见，因此保持警惕很有必要。安全防范措施必须立足于独立可证实的数据和流程，使用可测量的方法客观验证系统的可信度，以适应作为企业信息技术环境有机组成部分的全部暂态。最可持续的方法是根据企业的独特信息技术环境量身定制动态防御系统，其包括持续演进的安全控制措施，以保持相关性。[9]

值得信赖的系统可在此类环境中存在，而透明对于创建值得信赖的系统至关重要。“值得信赖的系统必须拥有坚实的基础：产品开发实践、值得信赖的供应链以及包括网络设计、实施和政策的体系结构方法”，高级副总裁兼首席安全官 John N. Stewart 说道。“但是，最重要的属性是供应商的透明度”。

接上一页

信任供应商

利用云，公司发现提供专业的解决方案的供应商。与第三方合作的成本模型变得有意义。但是这些供应商也是罪犯的高价值目标，他们知道第三方的防御可能不是很坚固。

从安全漏洞迅速恢复

所有公司都应假设他们受到黑客攻击，或者至少同意，他们是否会成为攻击目标不是问题，问题是何时成为攻击目标。最近的黑客攻击有运营夜龙攻击 (Operation Night Dragon)、RSA 漏洞和 2012 年针对大型石油天然气公司的 Shamoon 攻击，许多 CISO 对这些攻击记忆犹新。（参阅第 48 页的思科对公司网络中的流行恶意行为的研究。）

更高的透明度意味着更少的隐私，但是可通过合作找到两者的最佳平衡，进而导致更多机会，以校准威胁情报和最佳安全实践。所有企业都迫切希望找到信任、透明度和隐私之间的绝佳平衡，因为此事事关重大。

从长远来看，所有用户均可享受到更安全网络带来的福利，并且新兴的物联网[10]经济的潜能亦会得到完全发掘。但是，这些目标的实现取决于有效的隐私政策和强健的网络防御能力，其可以跨端点和在整个网络内智能分配安全责任。在短期内，甚或更紧迫的时间内，任何现代企业均需要使用现有的最佳方法和信息，帮助保护其最重要的资产，并确保其没有直接促进网络安全挑战加剧。

企业目前必须考虑其安全实践会对更大且日益复杂、相互连接的网络安全生态系统造成什么影响。缺乏此类大局观可能会导致企业声誉受损，这意味着领先的安全提供商都不会允许用户访问该企业的网站。一旦企业被列入黑名单，想要移出黑名单绝非易事，有些企业可能永远都无法做到。

欲了解思科值得信赖的系统实践，请访问 www.cisco.com/go/trustworthy。

威胁智能

思科和 Sourcefire 使用现今最大的检测遥测套组，共同分析和汇集去年的安全洞察。

威胁警报日益增多

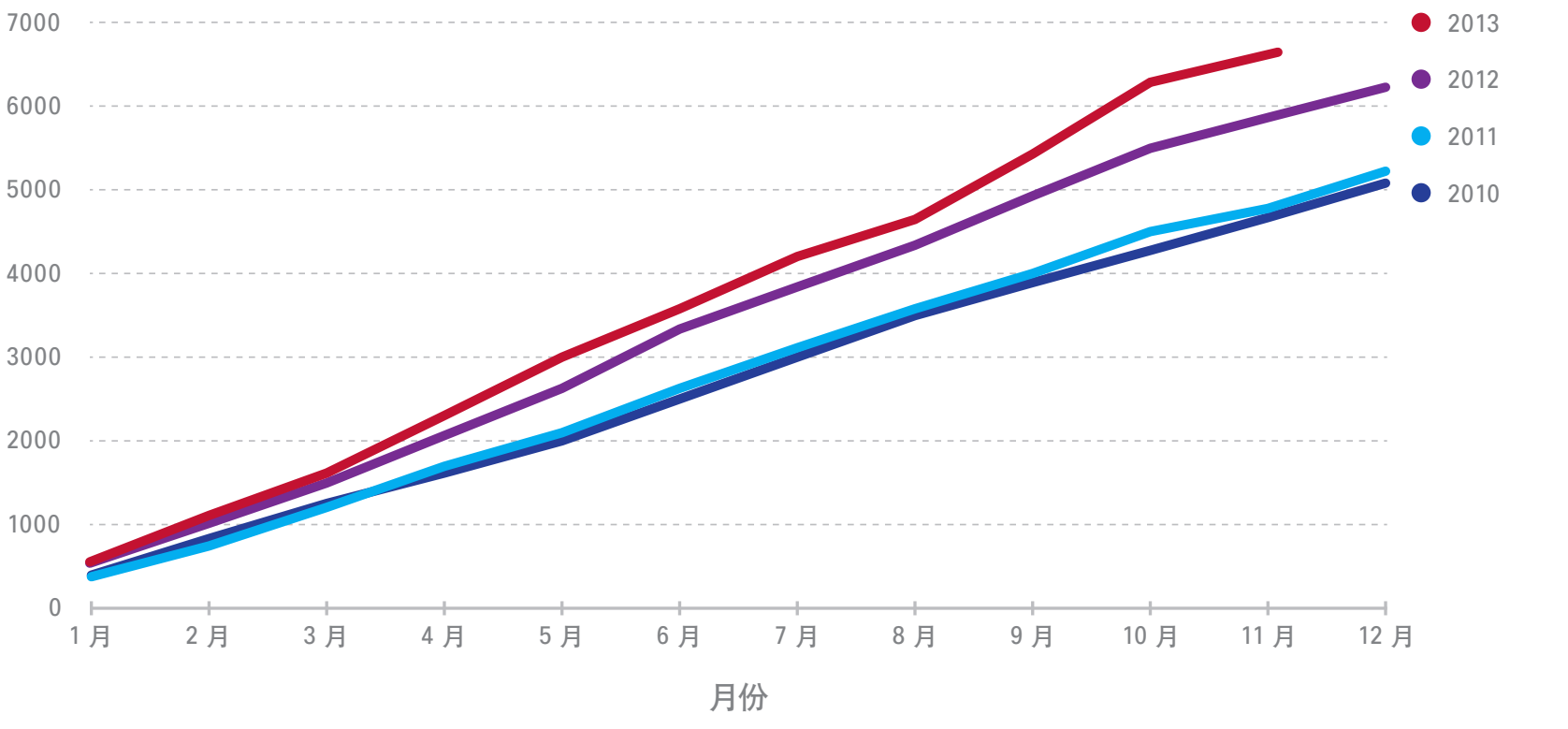
思科 IntelliShield® 报告显示，漏洞和威胁在 2013 年稳步增多：截止 2013 年 10 月，全年累计警报总数相比 2012 年增长 14%（图 3）。

2013 年 10 月报告的警报总数为 2000 年 5 月 IntelliShield 开始记录以来的最高月份。

另外值得注意的是，IntelliShield 的跟踪数据显示，新警报数相比更新警报数显著增加（图 4）。技术供应商和研究机构发现越来越多的新漏洞（图 5），导致其更加注重使用高安全性开发生命周期，以及增强自身产品的安全性。 新漏洞数的增多亦可能预示供应商会检查其产品代码，修复安全漏洞，然后再发布产品，并且安全漏洞被黑客利用。

图 3

年度警报累计总数 (2010-2013 年)



更加关注安全软件开发有助于建立对供应商解决方案的信任。安全开发生命周期不仅能减少安全漏洞风险，允许供应商在开发早期检测潜在缺陷，而且能告诉购买者他们可以信赖这些解决方案。

图 4

新增和更新警报数 (2013 年)

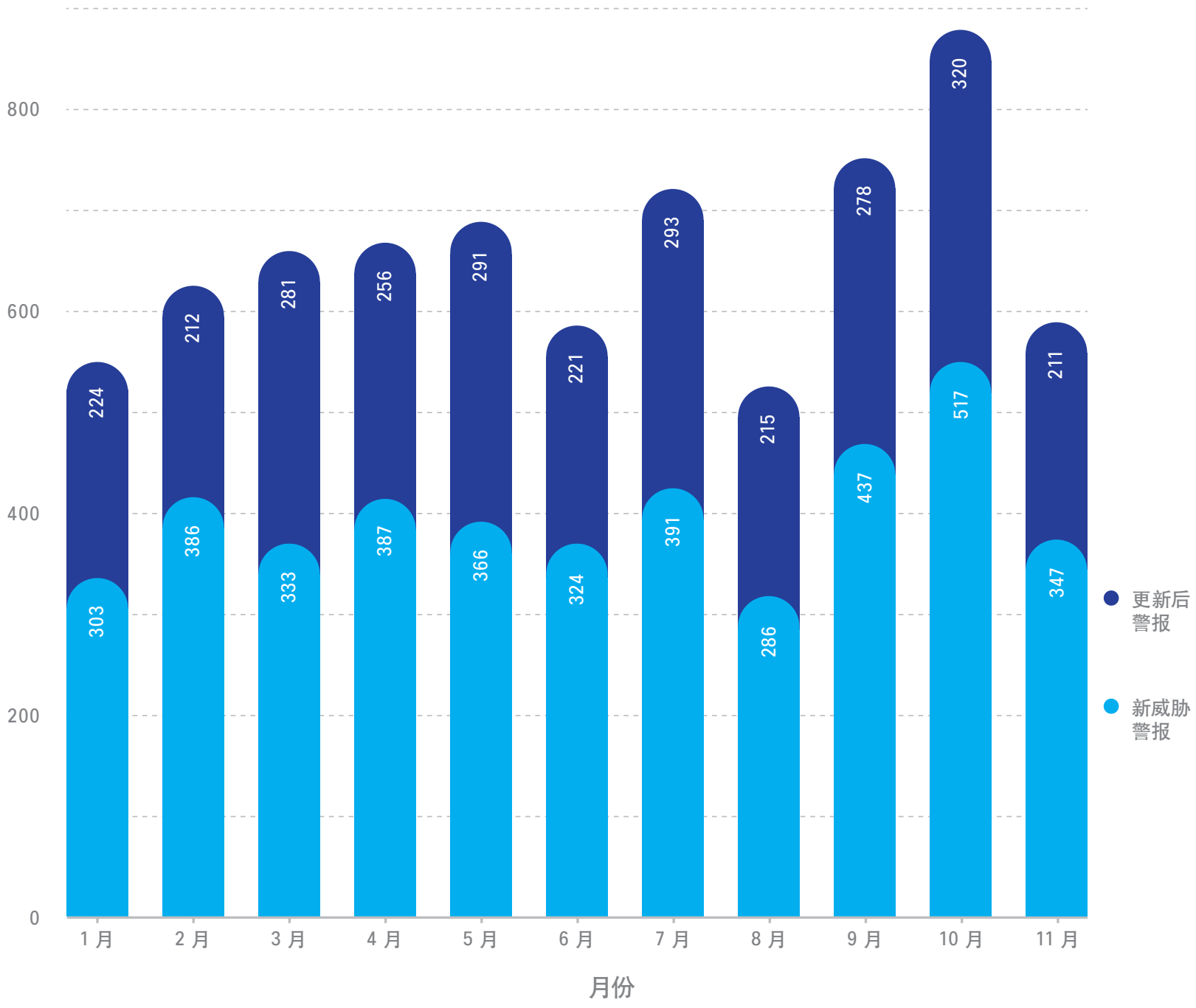


图 5

思科 IntelliShield 追踪的常见威胁类别

备注：这些 CWE（常见缺陷列表）威胁类别（依照美国国家漏洞数据库定义（https://nvd.nist.gov/cwe.cfm））列载了恶意攻击实施者用来攻击网络的方法。

1
CWE-119：缓冲区错误

2
其他 Intellishield 警报（活动、问题、CRR、AMB）

3
CWE-399：资源管理错误

4
CWE-20：输入验证

5
CWE-264：权限、特权和访问控制

6
CWE-200：信息泄漏/披露

7
CWE-79：跨站点脚本 (XSS)

8
CWE-94：代码注入

9
CWE：设计错误

CWE-310：密码问题

CWE-287：身份验证问题

CWE-352：跨网站请求伪造（CSRF）

CWE-22：路径遍历

CWE-78：OS 命令注入

CWE-89：SQL 注入

CWE-362：争用条件

CWE-255：凭据管理

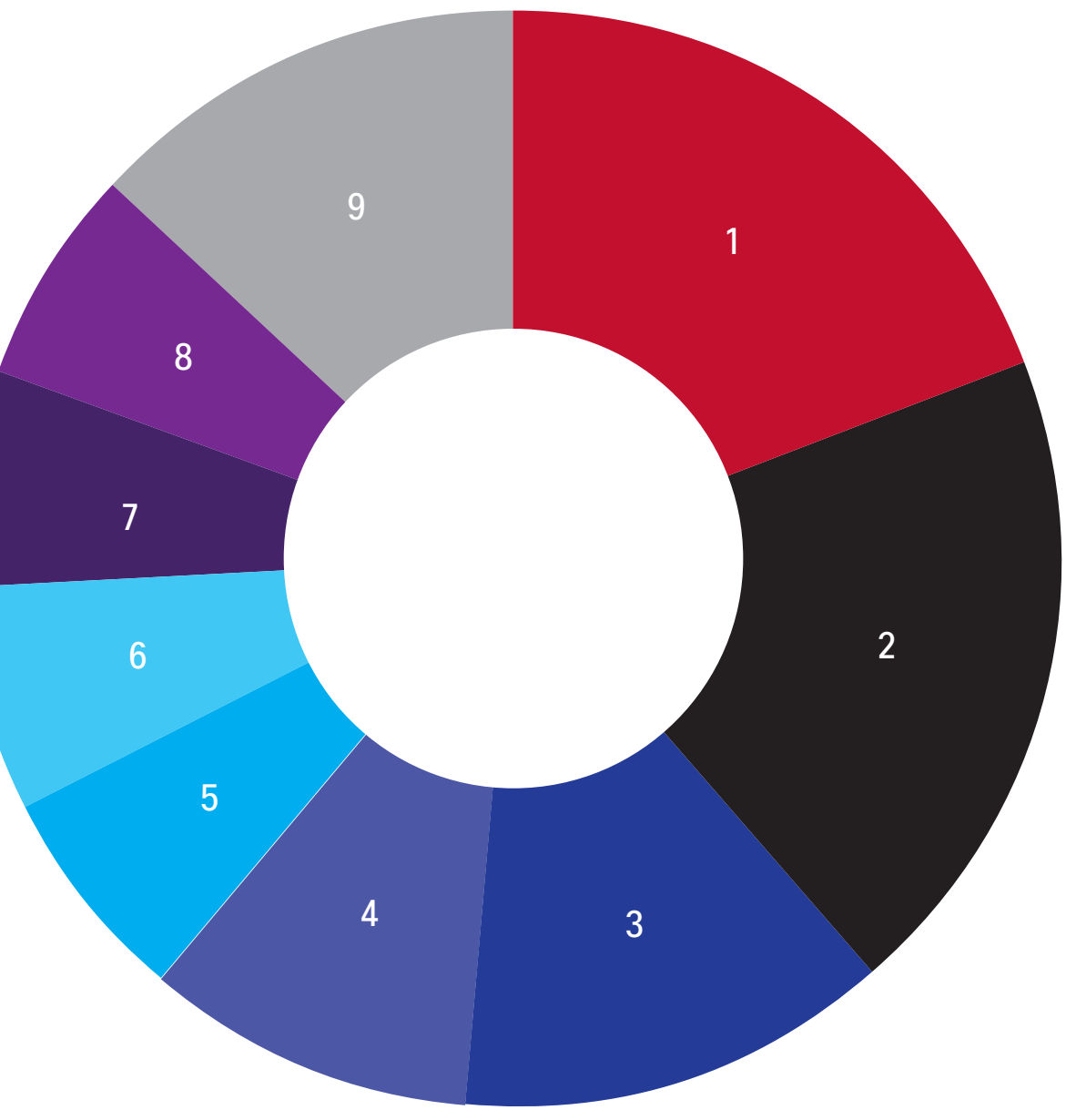
CWE-59：链接跟随

CWE-16：配置

CWE：信息不足

CWE：其他

CWE-189：数字错误



垃圾邮件总量呈下降趋势，但恶意垃圾邮件仍具威胁

2013年，全球垃圾邮件总量呈下降趋势。虽然垃圾邮件总数有所减少，但是恶意垃圾邮件所占比例仍保持恒定不变。

垃圾邮件发送者使用速度工具，滥用电子邮件用户的信任，当新事件或趋势降低接受者对垃圾邮件骗局抵抗力时，发送大量垃圾邮件。

2013 年 4 月 15 日波士顿马拉松爆炸案发生之后，4 月 16 日和 17 日接连发生两次大规模垃圾邮件市场活动，其旨在吸引渴望得知爆炸案影响新闻的电子邮件用户查看。思科安全研究人员在波士顿马拉松爆炸案发生后的数小时内，最先检测到成百上千的波士顿爆炸案相关域名注册行动。[11]

垃圾邮件制造者利用人们对了解更多重大事件信息的渴望行骗。

垃圾邮件市场活动的邮件主题是与爆炸案有关的信以为真的新闻，同时邮件包含的链接声称通往炸弹爆炸视频，或知名媒体资源的新闻。这些链接将接受者引导至包含真正新闻或视频链接的网页，但也包含旨在使访客电脑感染病毒的恶意 IFRAME。在高峰时段，与波士顿马拉松爆炸案相关的垃圾邮件占到 2013 年 4 月 17 日全球垃圾邮件总量的 40%。

图 6 显示的是一个伪装成 CNN 来源邮件的僵尸网络垃圾邮件市场活动。[12] 图 7 显示的是波士顿马拉松爆炸案垃圾邮件的源 HTML。最后一个 IFRAME (模糊) 是恶意网站的 IFRAME。[13]

由于突发新闻垃圾邮件时效性极强，电子邮件用户更容易相信垃圾邮件是合法的。垃圾邮件发送者捕食人们在重大事件发生后渴望了解更多信息的急切心情。当垃圾邮件发送者发送在线用户想要的内容之后，更容易诱骗在线用户如其所愿采取行动，如点击受到病毒感染的链接。此外，亦更容易防止在线用户怀疑邮件存在问题。

图 6

波士顿马拉松爆炸案垃圾邮件

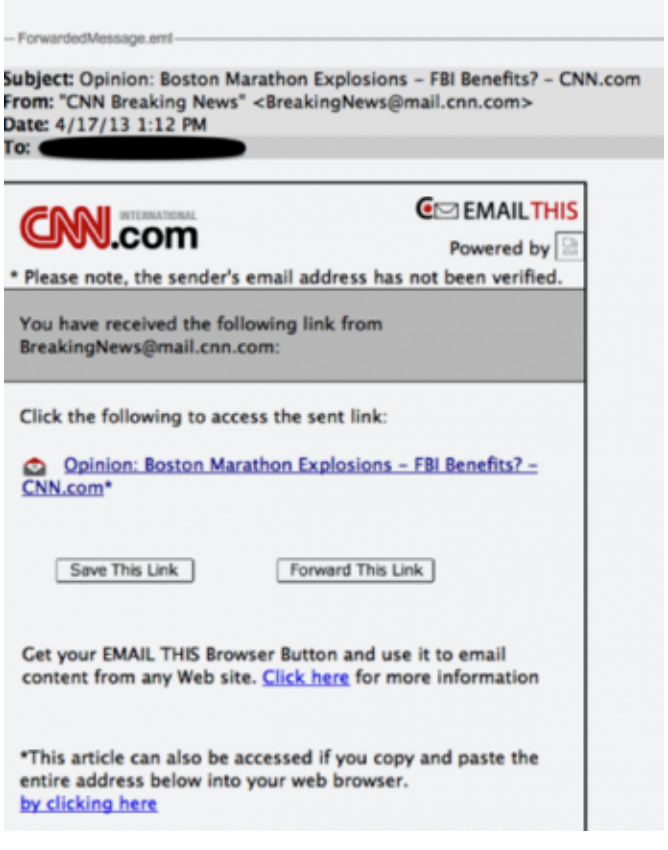
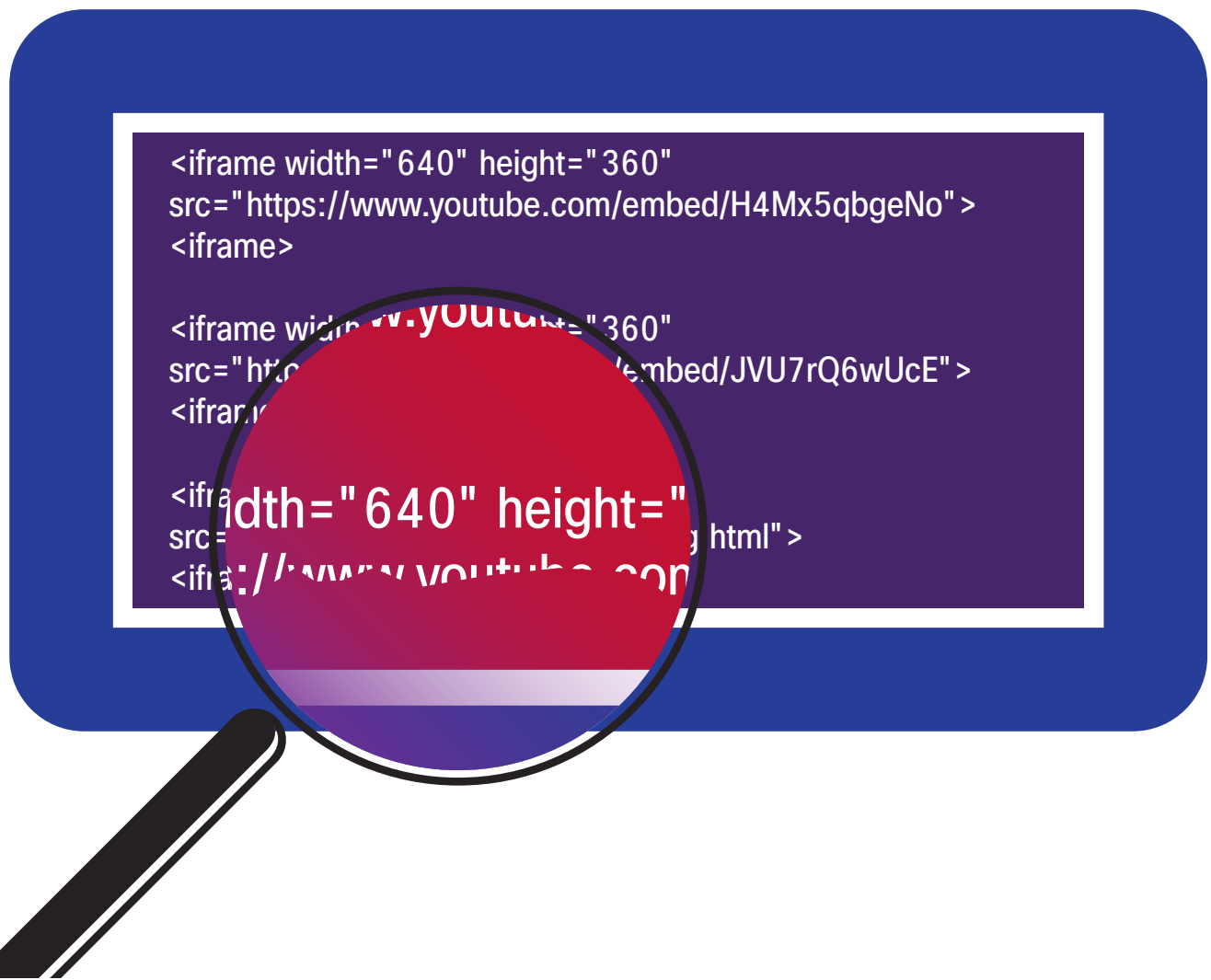


图 7

波士顿爆炸案垃圾邮件的源 HTML



垃圾邮件数量分布图

思科研究分析和通讯 (TRAC)/SIO 采集的数据显示，虽然各国情况有所不同 (图 9)，但是全球垃圾邮件总量呈下降趋势 (图 8)。

图 8

2013 年全球垃圾邮件总量

来源：思科 TRAC/SIO

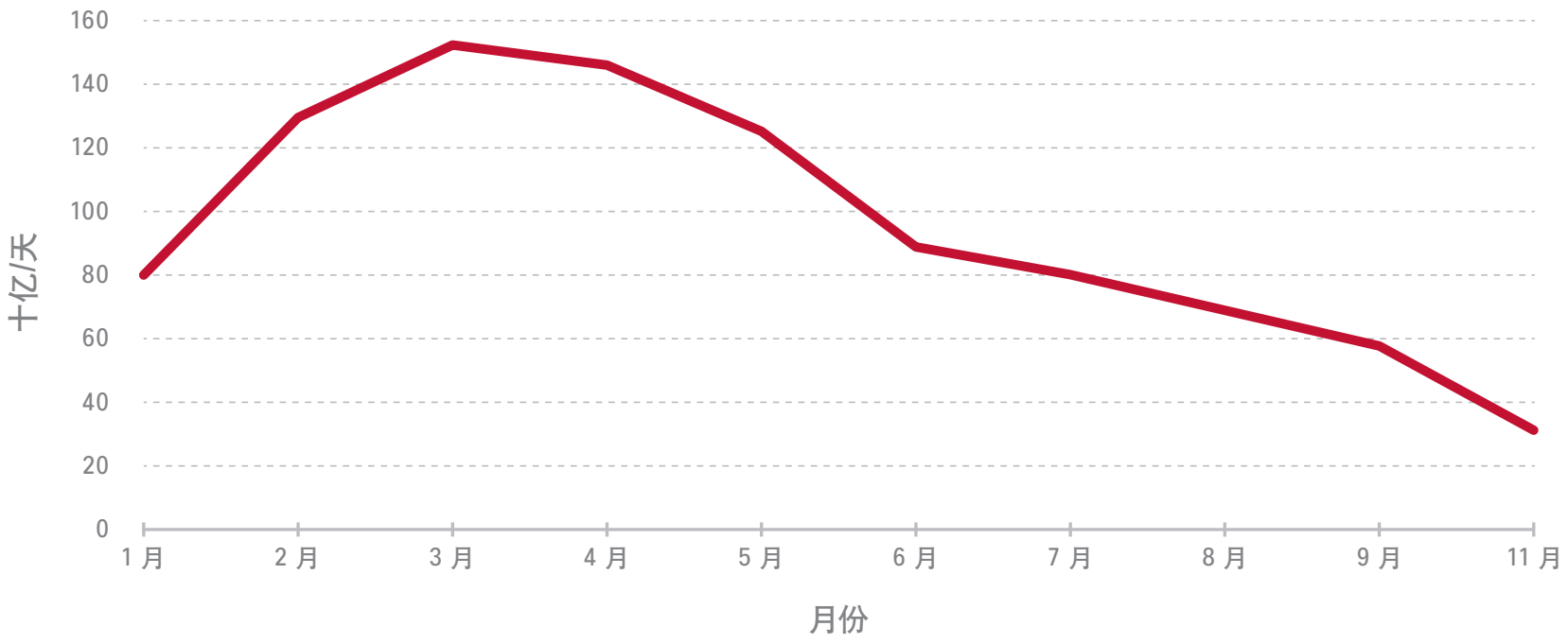


图 9

2013 年总量趋势

来源：思科 TRAC/SIO

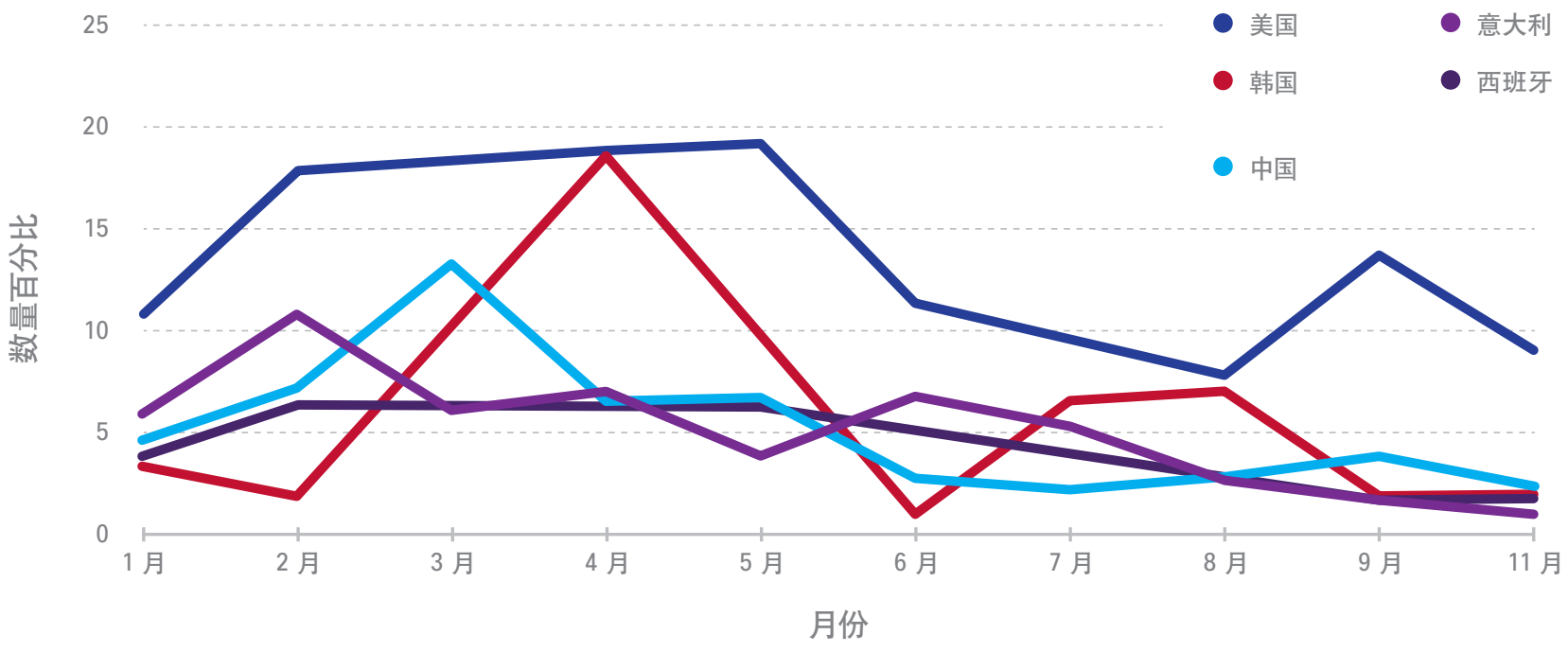


图 10

全球垃圾邮件热门主题

1.
银行存款/付款通知
有关存款、转帐、付款、退回支票和欺诈警报的通知。

2.
在线购买产品
产品订单确认、请求采购订单、报价、试用。

3.
附件照片
恶意附件照片。

4.
货运通知
发票、送货或取货、跟踪。

5.
在线交友
在线交友网站。

6.
纳税
税务资料、退税、报表、
债务信息、网上税务申报。

7.
Facebook
帐户状态、更新、通知、安全软件。

8.
礼品卡或优惠券
各种商店（最常见的是 Apple）的提醒。

9.
PayPal
帐户更新、确认、付款通知，付款纠纷。

Web 攻击: Java 居首

思科采集的数据显示, 在所有危害网络安全的所有基于 Web 的威胁中, Java 编程语言的漏洞继续成为最经常利用的对象。

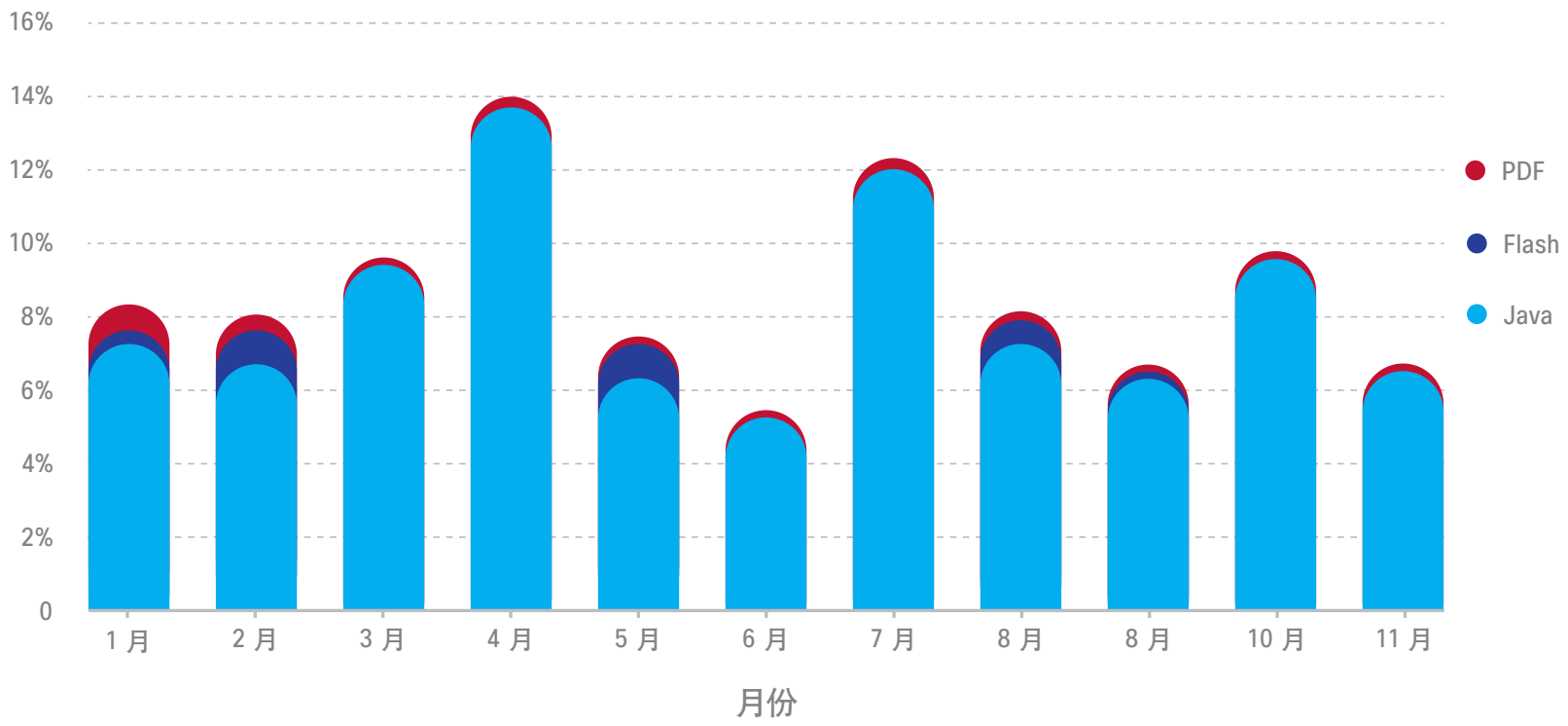
Java 攻击远超 Flash 或 Adobe PDF 文件所检测到的攻击, 其也是受欢迎的犯罪活动载体 (图 11) 。

Sourcefire 已被思科收购, 其采集的数据也显示, 在 Sourcefire FireAMP 高级恶意软件分析和保护解决方案监测的入侵指标 (IoC) 内, Java 攻击占据绝大多数份额 (91%) (图 12) 。FireAMP 检测到端点实时存在的入侵行为, 然后记录导致入侵的软件的类型。

图 11

2013 年借助 PDF、Flash 和 Java 实施的恶意攻击

来源: 思科云 Web 安全报告



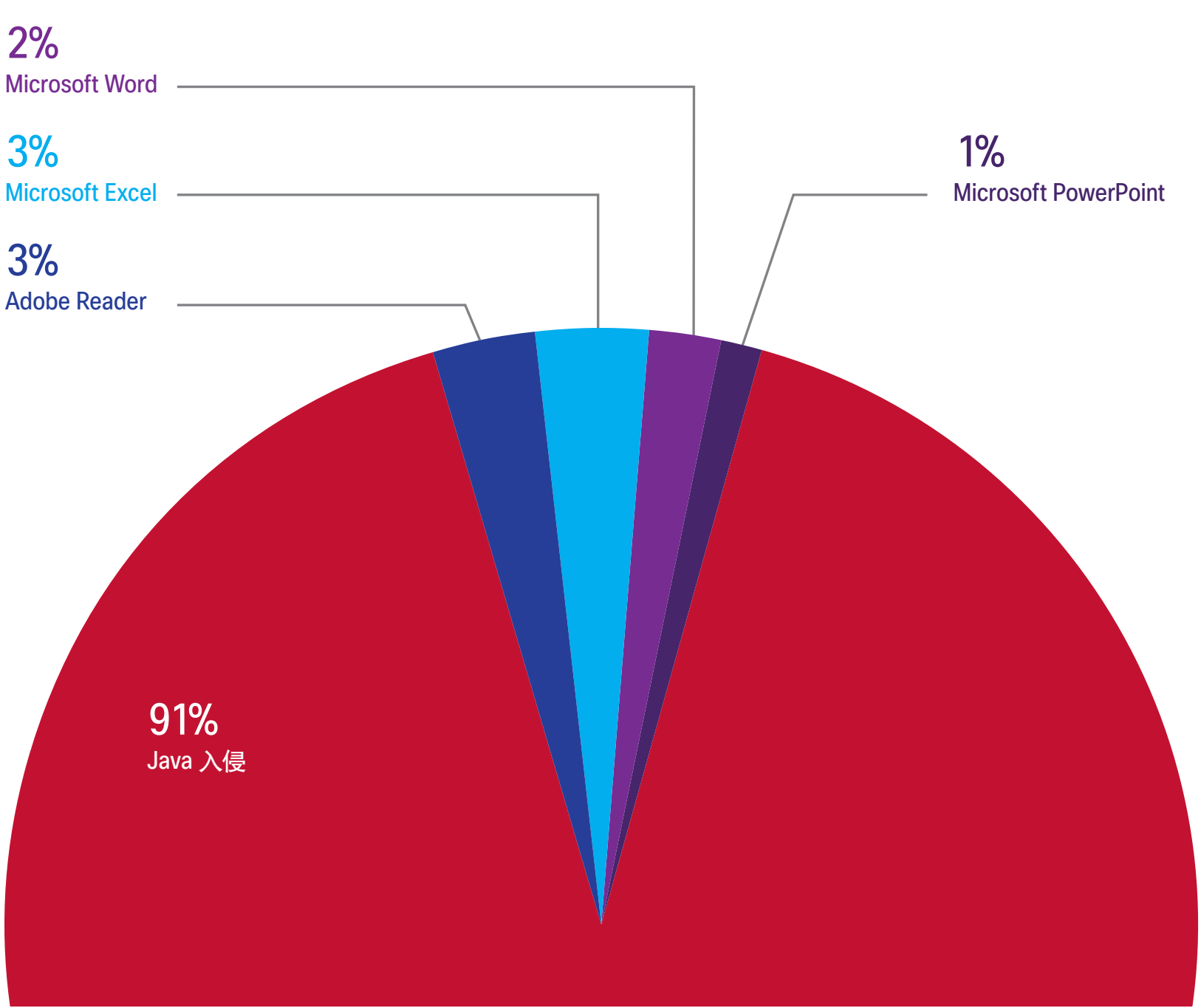
对于 Java 攻击等维修，安全从业人员面临的最重要问题是恶意软件如何进入他们的网络环境，以及在何处集中精力增强安全措施，以最大程度减少受感染风险。个人行为可能看似并无恶意，但紧随事件链之后，即会清楚显示恶意软件详情。事件链接是指对连接恶意攻击实施者为绕过外围网络安全防御并侵袭网络而采取的路径的相关数据进行回顾性分析的能力。

IoC 本身可以证明，前往特定网站是安全的。反过来，启用 Java 可能是安全的，启用一个可执行文件也可能是安全的。但是，如果用户访问植入 IFRAME 的网站，然后启用 Java ，Java 随后下载一个可执行文件，并且该文件执行恶意攻击操作，则企业面临安全性风险。

图 12

入侵指标类型分布图

来源：Sourcefire （FireAMP 解决方案）



由于 Java 普遍存在，因此其也成为网络犯罪分子最喜爱的工具之一，并使 Java 入侵成为 2013 年迄今最恶意的“事件链”活动。正如“关于 Java”网页所述，美国 97% 的企业桌面系统运行 Java，89% 的桌面电脑运行 Java。[14]

Java 提供的攻击面非常大，大到网络犯罪分子不可能忽视。他们往往会创建按序利用漏洞进行攻击的解决方案—例如，他们首先尝试使用最容易或最知名的漏洞破坏网络，或窃取数据，然后再转而使用其他方法。在大多数情况下，Java 是网络犯罪分子的首选，因为它能带来最佳投资回报。

缓解 Java 问题

虽然基于 Java 的攻击司空见惯，并且其漏洞难以完全修补，但是仍有许多方法可以减少其危害：

- 如果可行，禁用浏览器网络的 Java 功能可以防止网络犯罪分子发送 Java 攻击。
- 诸如许多安全解决方案内置的思科 NetFlow 等遥测工具可以监控 Java 相关流量，可使安全专业人员更好地了解威胁源。
- 全面的补丁管理可以修补许多安全漏洞。
- 可在文件进入网络之后继续跟踪和分析文件的端点监控和分析工具可以追溯检测，并阻止先以安全面貌通过但随后展现恶意攻击行为的威胁。
- 可以使用 IoC 生成可能被破解设备的优先级排序列表，以使恶意软件智能 (即使看似良性的事件) 相互关联，并确定无现有反病毒签名，未受病毒感染。

升级至最新版本的 Java 也有助于规避漏洞。思科 TRAC/SIO 的研究显示，90% 的思科客户使用最新版本的 Java 7 Runtime Environment。从安全角度来看，这非常好，因为该版本很可能提供更大的漏洞防范保护。

但是，思科 TRAC/SIO 的研究还显示，使用思科解决方案中 76% 的企业同时使用 Java 6 Runtime Environment 和 Java 7。Java 6 是旧版本，已经到达其使用寿命终点，不再获得技术支持。由于不同应用程序可能以来不同版本的 Java 来执行 Java 编码，因此企业往往同时使用两种版本的 Java Runtime Environment。但是，思科的调查显示，超过四分之三的受访企业使用使用寿命终结的解决方案，并且其拥有从未公开发布补丁进行修补的漏洞，因此网络犯罪分子拥有足够的机会来利用这些漏洞。

2013 年 4 月，Java Web 恶意软件交会次数达到顶峰，占到全年总量的 14%。2013 年 5 月和 6 月的交会次数为全年最低，分别约占全年总量的 6% 和 5% (图 13) 。

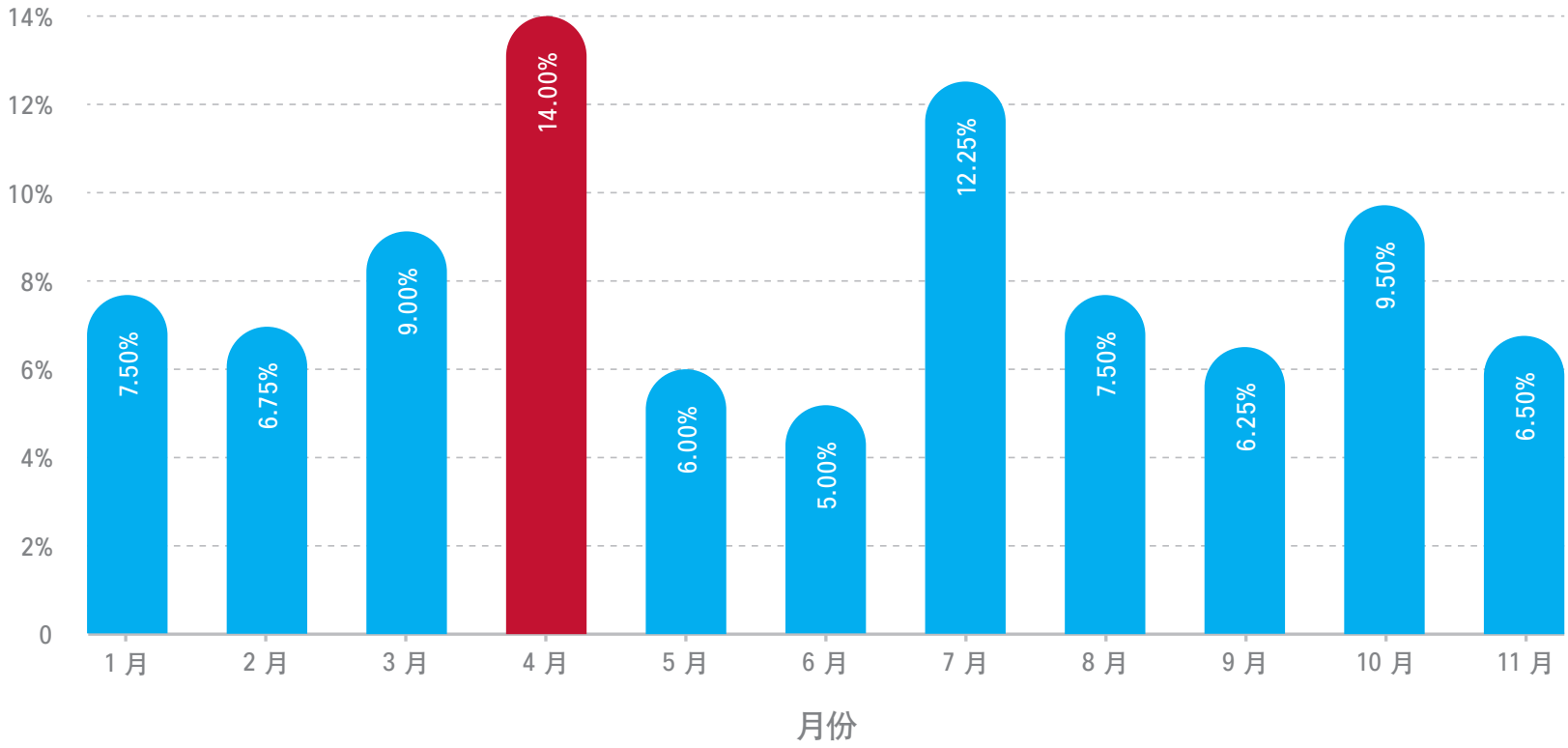
（今年初，甲骨文宣布其不再发布 Java SE 6 更新至其公共下载网站，虽然现有 Java SE 6 更新可以前往甲骨文技术网络 (Oracle Technology Network) 的 Java Archive 下载。

如果安全专业人员利用其有限的时间打击网络攻击，并决定将大部分注意力投向 Java，那么他们会正确配置资源。

图 13

2013 年 Java Web 恶意软件交会

来源：思科 TRAC/SIO



BYOD 和移动性：设备成熟惠及网络犯罪

网络犯罪分子及其目标面临共同的挑战：两者均试图弄清如何最充分地利用自带设备 (BYOD) 和移动性趋势，以获取商业优势。

两件事情看似帮助网络犯罪分子占得上风：第一件事情是移动平台的成熟。思科安全专家指出，如同传统桌面和笔记本电脑那样运行的智能手机、平板电脑和其他设备越多，为其设计恶意软件即越容易。

第二件事情是移动应用程序的用量日益增长。当用户下载移动应用程序时，他们实质上是将轻量级客户端安装到端点上，并下载编码。另一项挑战：许多用户定期下载移动应用程序，而从未考虑安全问题。

与此同时，当今的安全团队正在努力解决“任何到任何问题”：如何确保用户安全地在任意地点使用任何设备访问任何应用程序或资源。[15] BYOD 趋势仅会使这些努力变得复杂。很难管理所有这些类型的设备，尤其是在信息技术预算有限的情况下。在 BYOD 环境内，CISO 需要特别肯定数据室得到严格控制。

许多用户经常下载手机应用程序，从不考虑安全问题。

移动性提供入侵用户和数据的新方法。思科研究人员发现，恶意攻击实施者使用无线信道窃听并获取权限访问通过这些信道交换的数据。移动性还使企业面临众多安全问题，包括知识产权和其他敏感数据的丢失，如果雇员的设备丢失或被盗，并且其设备安全保障措施不足。

思科安全专家指出，制定移动设备管理的正式计划，以帮助确保任何设备在安全无虞的前提下访问网络，这是提高企业安全性的一项有效解决方案。最起码，应要求使用个人身份识别码 (PIN) 锁闭程序进行用户身份验证，安全团队应能在设备丢失或被盗的情况下远程关闭或彻底清理设备。

移动设备恶意软件趋势：2013

以下为思科 TRAC/SIO 和 Sourcefire（思科新收购的子公司）在 2013 年进行的移动设备恶意软件趋势研究。

针对特定设备的移动设备恶意软件数仅占 2013 年 Web 恶意软件交会总数的 1.2%。虽然比例不高，但是这仍值得注意，因为移动设备恶意软件显然是恶意软件开发者探索的顺理成章的新兴领域。

手机恶意软件以特定的设备为目标，2013 年只占所有网络恶意软件活动的 1.2%。

思科 TRAC/SIO 研究人员指出，当移动设备恶意软件蓄意入侵特定设备时，所有交会中的 99% 针对 Android 设备。在 2013 年，针对启用 Java Micro Edition (J2ME) 功能的设备的木马程序居第二位，占所哟移动设备恶意软件交会总数的 0.84%。

但是，并非所有移动设备恶意软件均被设计为针对特定设备。许多交会涉及网络钓鱼、likejacking 或其他社交工程诡计，或强制重定向到其他意料之外的网站。思科 TRAC/SIO 进行的用户代理人程序分析揭示，Android 用户遭遇所有形式的 Web 恶意软件的交会率最高，达 71%，其次为 Apple iPhone 用户，其遭遇所有 Web 恶意软件的交会率是 14% (图 14) 。

思科 TRAC/SIO 研究人员还观察到 2013 年通过入侵 Android 设备赚钱的网络攻击行为证据，包括启用广告软件和中小型企业 (SME) 相关的间谍软件。

思科 TRAC/SIO 进行的研究显示，Andr/Qdplugin-A 是最经常遇到的移动设备恶意软件，比例高达 43.8%。典型的交会是通过非官方应用程序市场分销的重新打包的合法应用程序副本 (图 15) 。

图 14

移动设备 Web 恶意软件交会分布图

来源：思科云 Web 安全报告

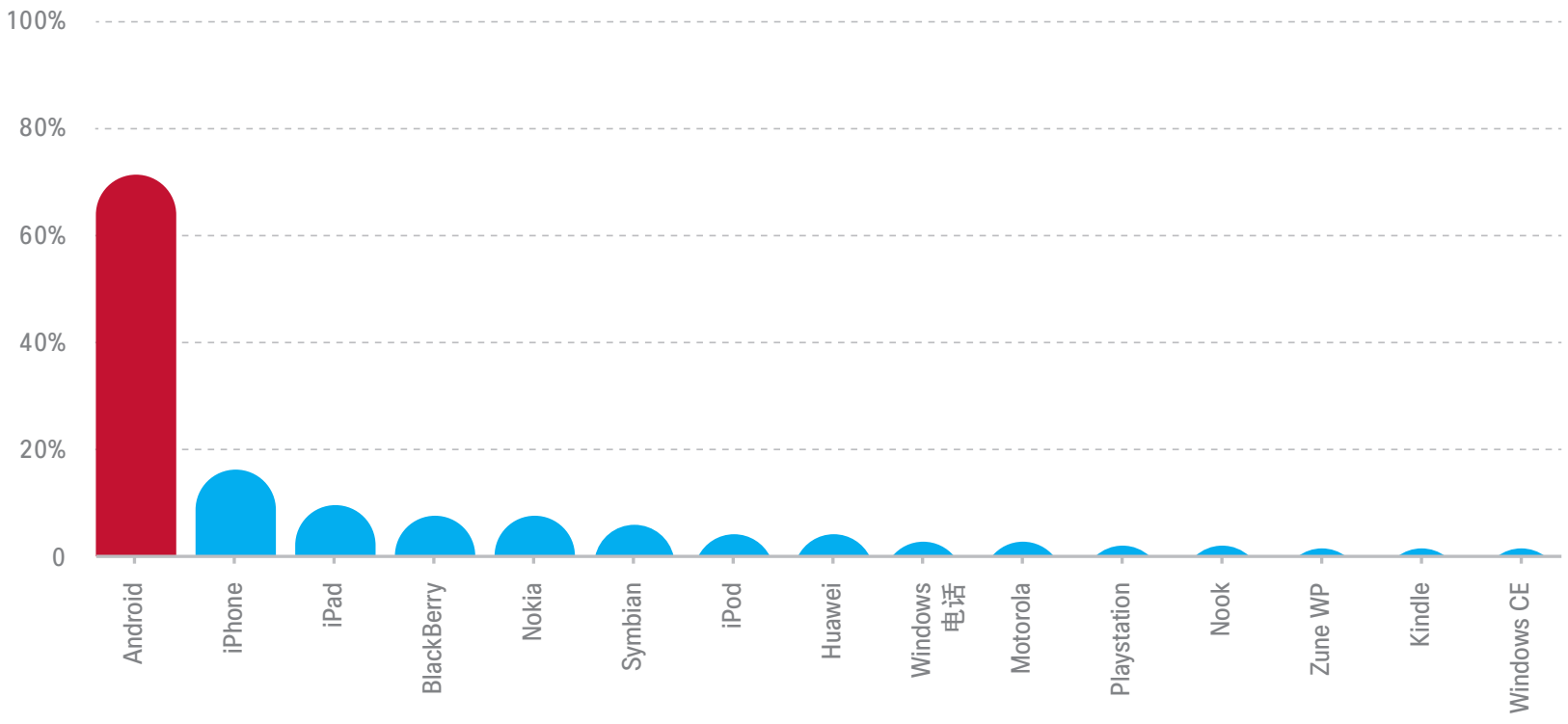


图 15

2013 年十大移动设备恶意软件交会

来源：思科云 Web 安全报告

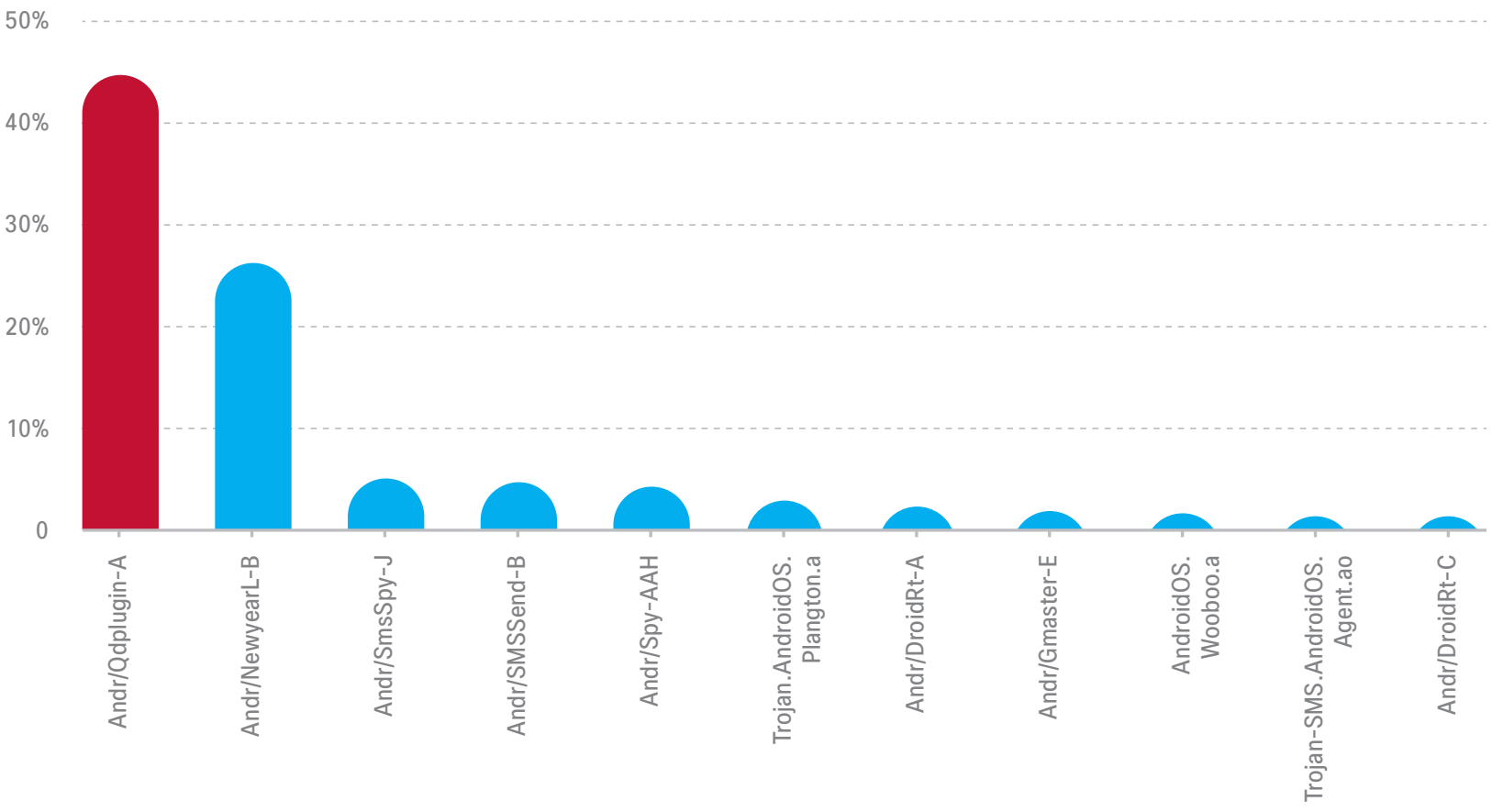
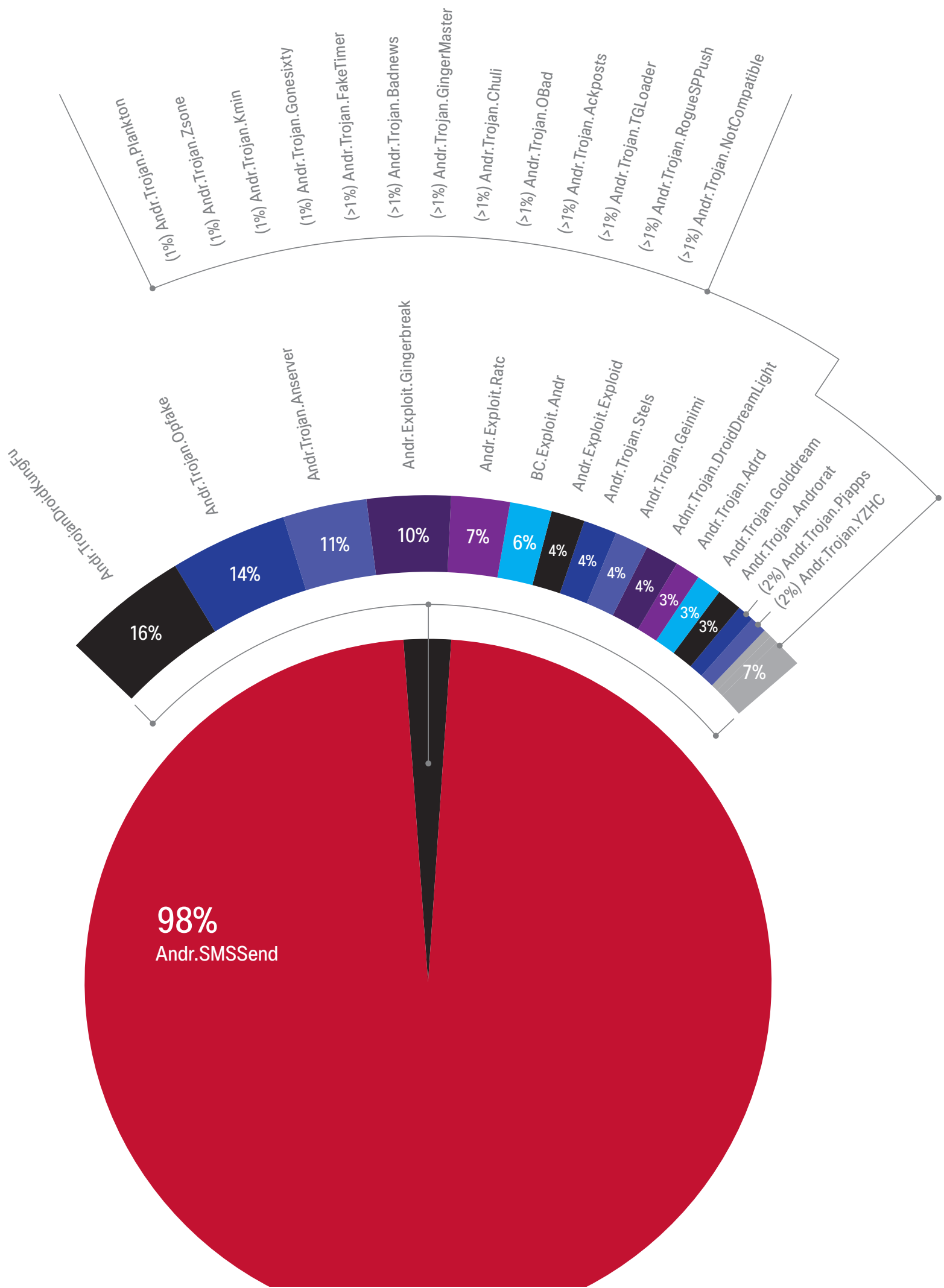


图 16

2013 年排名靠前的 Android 恶意软件家族

备注：SMSSend 占到所有 Android 恶意软件的 98%；剩余 2% 按比例显示。来源：Sourcefire



针对性攻击：驱逐持续且到处渗透的“访客”的挑战

针对性攻击很可能已经侵入您的网络。

一旦嵌入网络，它们往往会留守，暗中窃取数据，或使用网络资源进行“数据透视”，然后攻击其他实体（欲知数据透视详情，请参阅第 18 页）。损害远超数据盗取或业务终端：合作伙伴和客户之间的信任会消失，如果未及时从网络驱逐这些攻击。

针对性攻击威胁到知识产权、客户数据和政府敏感信息。针对性攻击的创造者使用精密复杂的工具规避企业的安全基础结构。罪犯竭尽全力，使用导致“入侵指标”（或 IoC）几乎察觉不到的方法，以确保这些漏洞未被发现。他们获得权限进入网络并执行其任务的系统性方法涉及“攻击链”—通向或经过攻击阶段的事件链。

罪犯竭尽全力确保漏洞不被发现。

一旦这些针对性攻击在网络内找到藏身之处，它们即会有效执行任务，通常在未被察觉的情况下执行任务。

图 17

攻击链

要了解当今威胁阵列，并有效防护网络，信息技术安全专业人员需要向攻击者那样思考问题。更深入了解恶意攻击实施者用来执行其任务的系统方法之后，企业可以找到方法来增强其防御能力。攻击链即简化版本的“网络杀伤链”，是指通往和经过攻击阶段的事件。

1. 调查

全面了解环境：网络、终端、移动和虚拟，包括已部署的安全防护技术。

2. 创作

创建有针对性的情景感知恶意软件。

3. 测试

确保恶意软件按照预期运作，以便它能避过部署的安全工具。

4. 执行

在扩展的网络中游荡——由于具有环境感知能力，因此可避过检测，并横向移动，直至到达目标。

5. 完成任务

收集数据，导致中断或造成破坏。

恶意软件快照：观察到的 2013 年度趋势

思科安全专家持续研究并分析恶意软件流量和其他已发现的威胁，获得未来可能的网络犯罪行为的洞察，并协助检测威胁。

图 18

排名靠前的恶意软件类别

本图显示了排名靠前的恶意软件类别。木马程序是最常见的恶意软件，紧随其后的是广告软件。来源：Sourcefire（ClamAV 和 FireAMP 解决方案）

图 19

排名靠前的 Windows 恶意软件家族

本图显示了排名靠前的 Windows 恶意软件家族。最大的恶意软件家族 Trojan.Onlinegames 主要包括密码窃取程序。Sourcefire 的 ClamAV 反病毒解决方案检测到该恶意软件。来源：Sourcefire（ClamAV 解决方案）

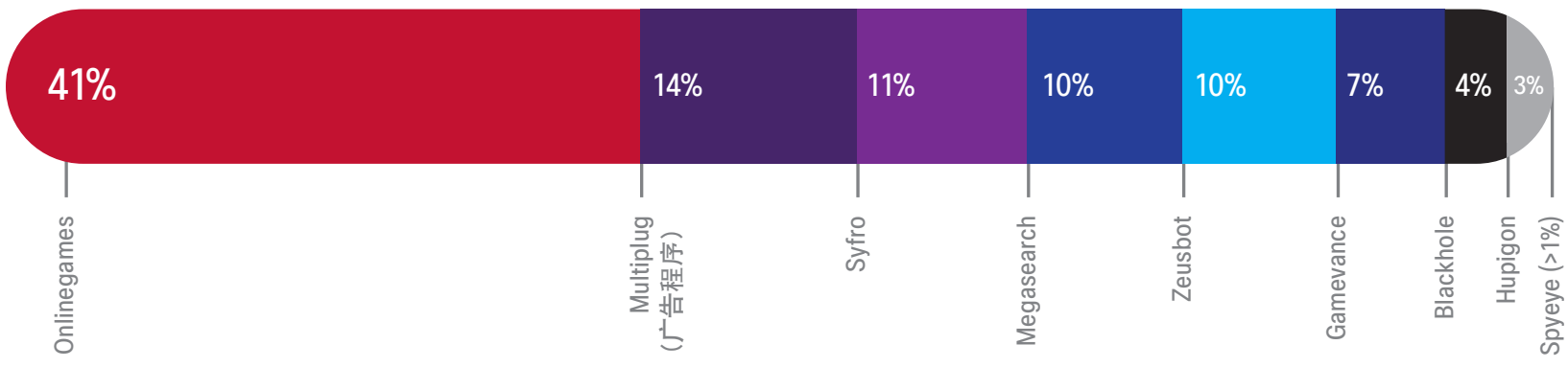


图 20

2013 年十大 Web 恶意软件主机类别

本图显示了思科 TRAC/SIO 研究发现的最经常使用的恶意软件主机。来源：思科云 Web 安全报告

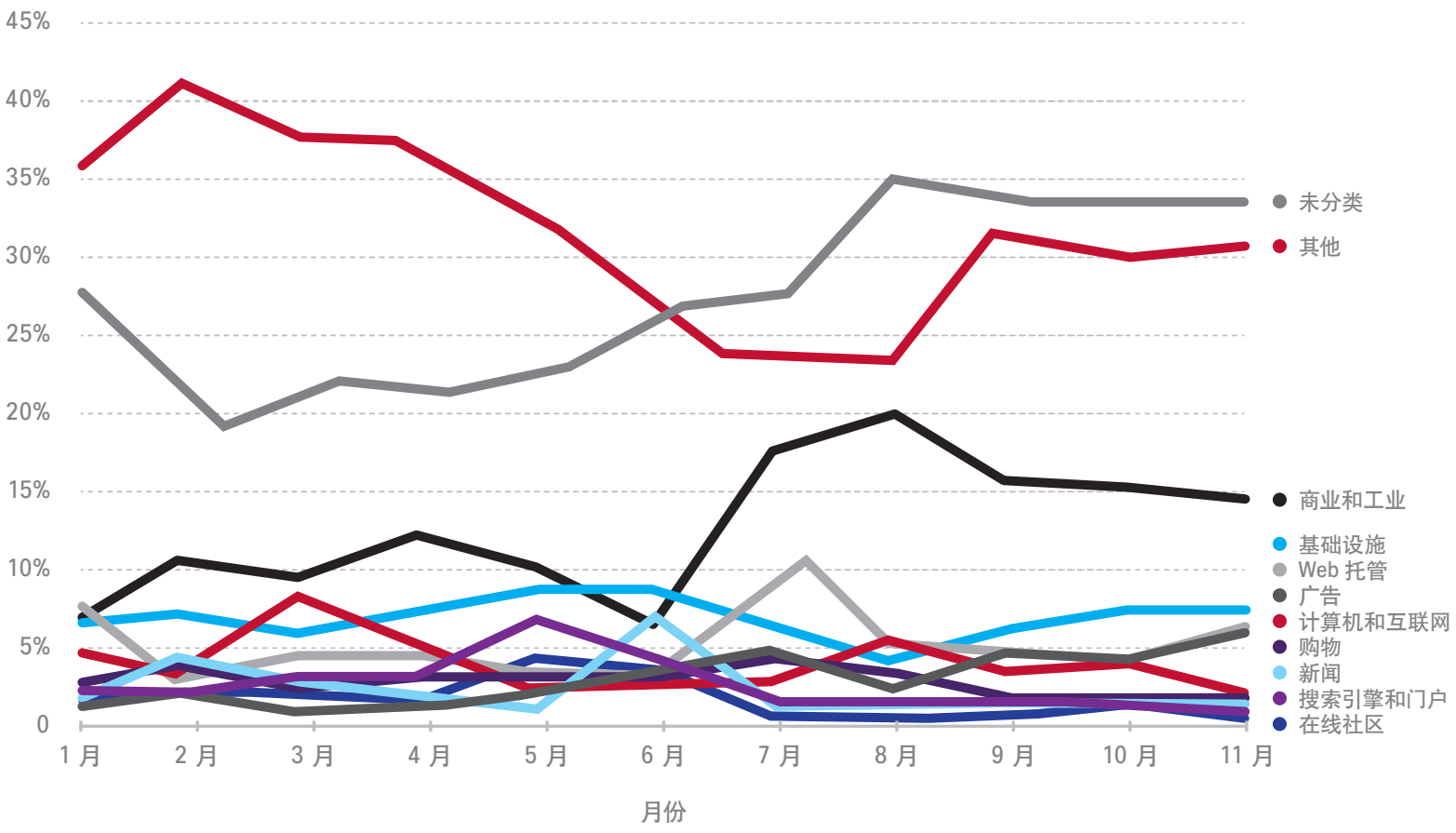
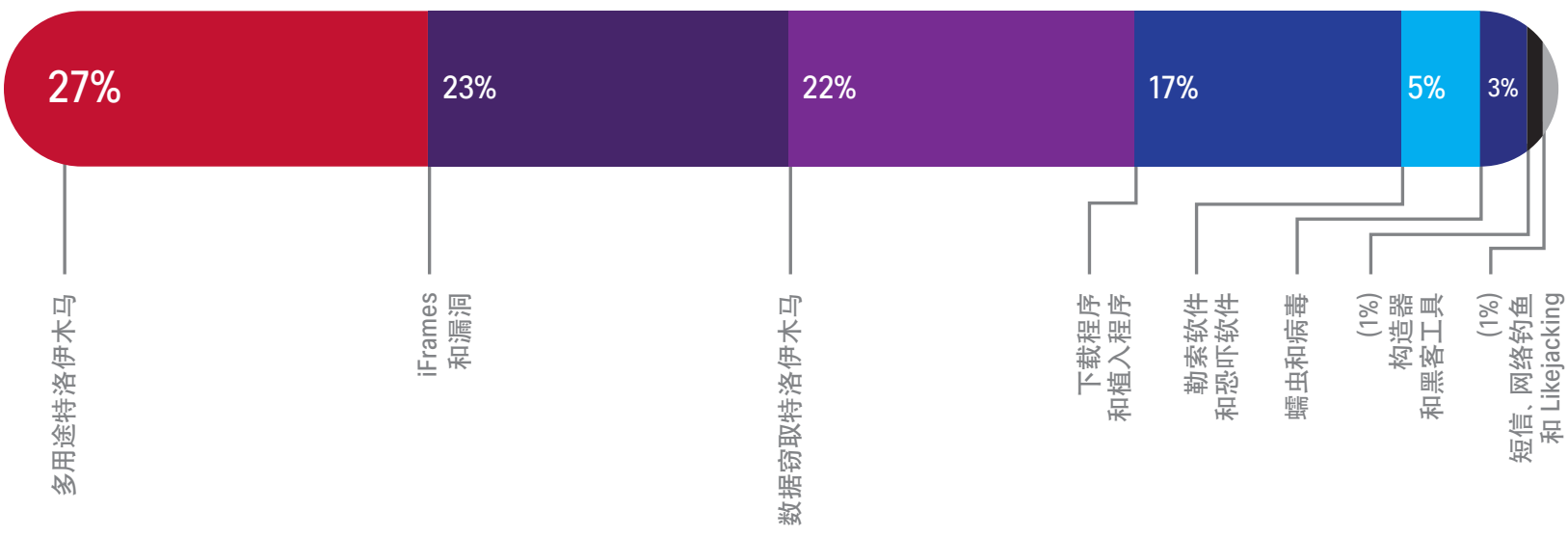


图 21

2013 年按总交会数占比划分的恶意软件类别

来源：思科 TRAC/SIO



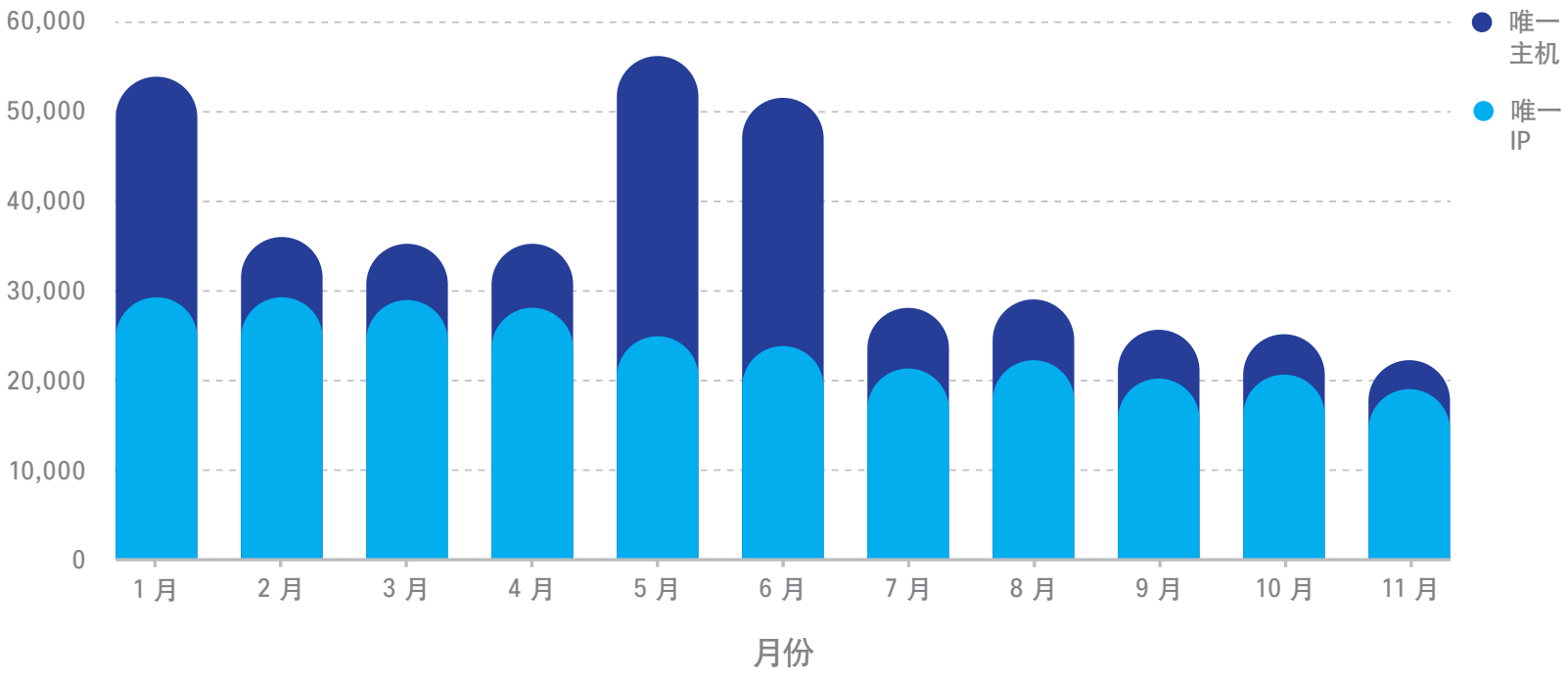
2013 年间思科 TRAC/SIO 进行的研究显示，多功能木马程序是最经常遇到的 Web 恶意软件，占交会总数的 27%。诸如 iframes 等恶意脚本为排名第二的最经常遇到的恶意软件类别，占交会总数的 23%。诸如密码窃取程序和后门等数据窃取木马程序占 Web 恶意软件交会数的 22%，下载程序和植入程序木马程序排名第四，占交会总数的 17% (参阅图 21) 。

独特恶意软件主机和 IP 地址总数呈现稳步下降趋势，2013 年 1 月至 9 月，降低 30%，这表明恶意软件向更少的主机和 IP 地址集中发动攻击 (图 22) 。(备注：一个 IP 地址可以用作多域名的网站。) 随着主机数量下降，但恶意软件数量保持稳定，这些主机的价值和声誉变得更高，因为出色的主机可以帮助网络犯罪分子实现其既定目标。

图 22

2013 年独特的恶意软件主机和 IP 地址

来源：思科云 Web 安全报告



水坑并非目标企业的绿洲

恶意攻击实施者向特定行业纵向市场内的企业植入恶意软件的方法之一是使用“水坑式”攻击。如同大型捕食动物观察猎物，寻求针对特定群体发动攻击的网络犯罪分子（如航空业从业人员）会监控该群体经常访问哪些网站，然后使用恶意软件感染其中一个或多个网站，然后坐下来静候并希望目标群体内至少有一名用户访问该网站，进而受到攻击。

水坑式攻击本质上是一种信任攻击，因为其使用了合法网站。它也是一种形势的鱼叉式网络钓鱼。虽然鱼叉式网络钓鱼瞄准特定个人，但是水坑旨在攻击拥有共同利益的人群。水坑式攻击并不挑剔目标对象：访问被感染网站的任何人均处于被攻击危险之中。

4 月底，托管美国劳工部网站核能相关内容的特定网页发动了 水坑式攻击。[16] 自 2013 年 5 月初开始，思科 TRAC/SIO 研究人员观察到集中在能源和石油部门领域的其他几个网站发动了另一波水坑式攻击。两波攻击所使用的特定攻击手段等诸多相似之处表明两波攻击很可能存在关联。思科 TRAC/SIO 的研究还显示，许多网站使用同一网页设计师和托管服务提供商。这可能意味着，初始攻击源于该托管服务提供商被网络钓鱼攻击或窃取的凭据。[17]

接下一页

主要目标：行业纵向市场

思科 TRAC/SIO 的研究显示，高利润纵向市场（如制药和化工行业，以及电子制造业）内的企业遭遇 Web 恶意软件交会的比率较高。

由于特定纵向市场的商品和服务价值上下波动，其遭遇 Web 恶意软件交会的比率随之上下波动。

思科 TRAC/SIO 研究人员观察到农业和采矿业遭遇的恶意软件交会数显著增加，而在以往，这两大行业的风险相对较低。他们将该行业的恶意软件交会数增长归因于网络犯罪分子抓住贵金属资源减少和与天气相关的食品供应中断等趋势。

此外，电子行业的恶意软件交会数继续增长。思科安全专家指出，瞄准该纵向市场的恶意软件通常旨在帮助恶意攻击实施者获取权限访问知识产权，他们反过来利用这些知识产权获得竞争优势，或将这些知识产权销售给出价最高的人。

为确定行业特定的恶意软件交会比率，思科 TRAC/SIO 研究人员比较了通过思科云 Web 安全访问代理服务器的所有企业的交会比率中位数和特定行业内通过思科云 Web 安全访问代理服务器的所有企业的交会比率中位数。如果某个行业的交会比率高于 100%，则表明其面临异常高的 Web 恶意软件交会风险，如果比率低于 100%，则表明其风险较低。例如，如果一家企业的

接上一页

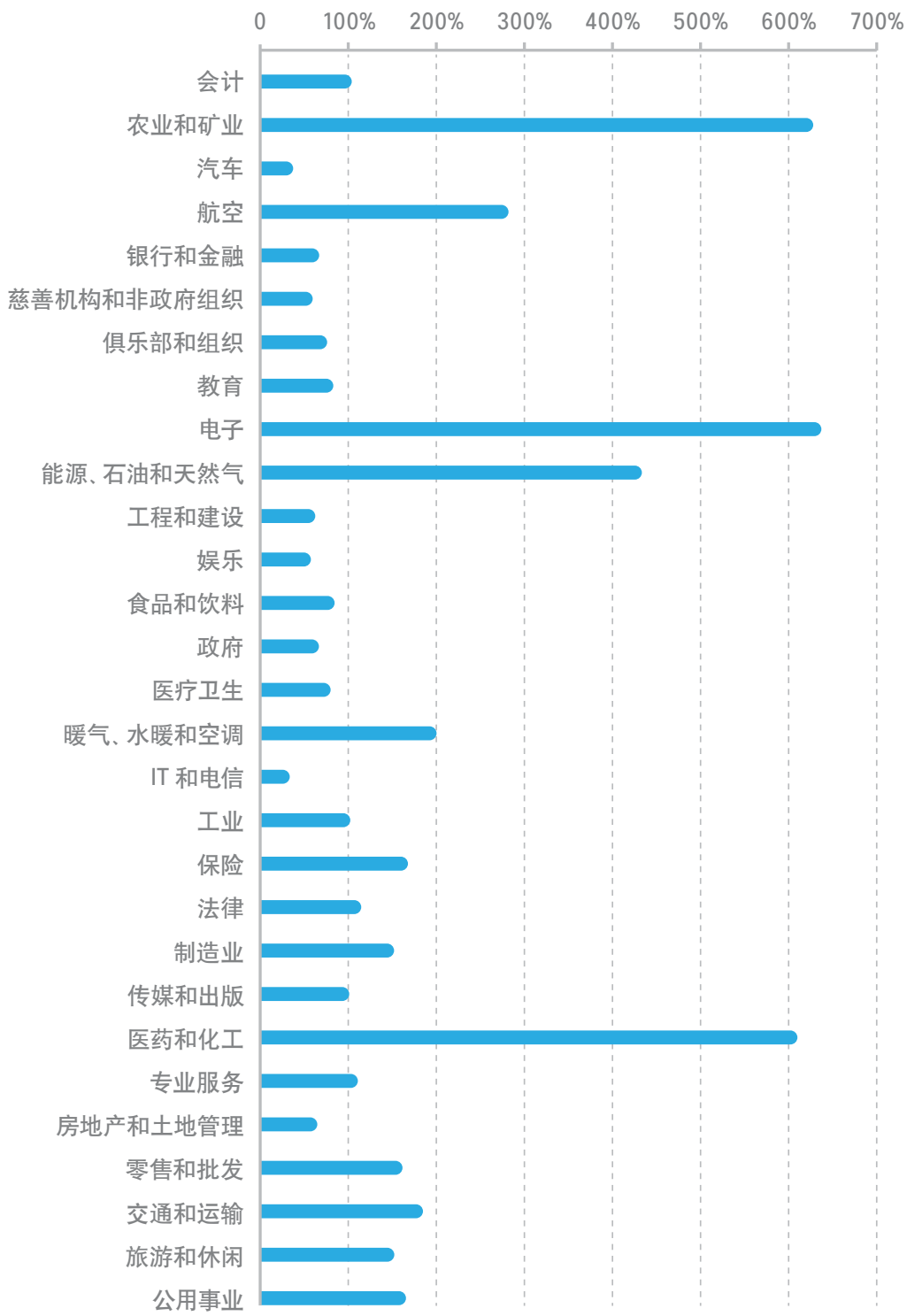
保护用户免受这些攻击涉及为机器和网络浏览器及时安装全部补丁，以最大程序减少网络攻击者可以利用的漏洞数量。确保对网络流量进行恶意软件过滤和检查，然后再将其发送到用户的浏览器，亦是必不可少的一项步骤。

交会比率高达 170%，则表明其面临的风险高出中位数 70%。相反，如果一家企业的交会比率为 70%，则表明其面临的风险低于中位数 30% (图 23) 。

图 23

2013 年行业风险和 Web 恶意软件交会

来源：思科云 Web 安全报告



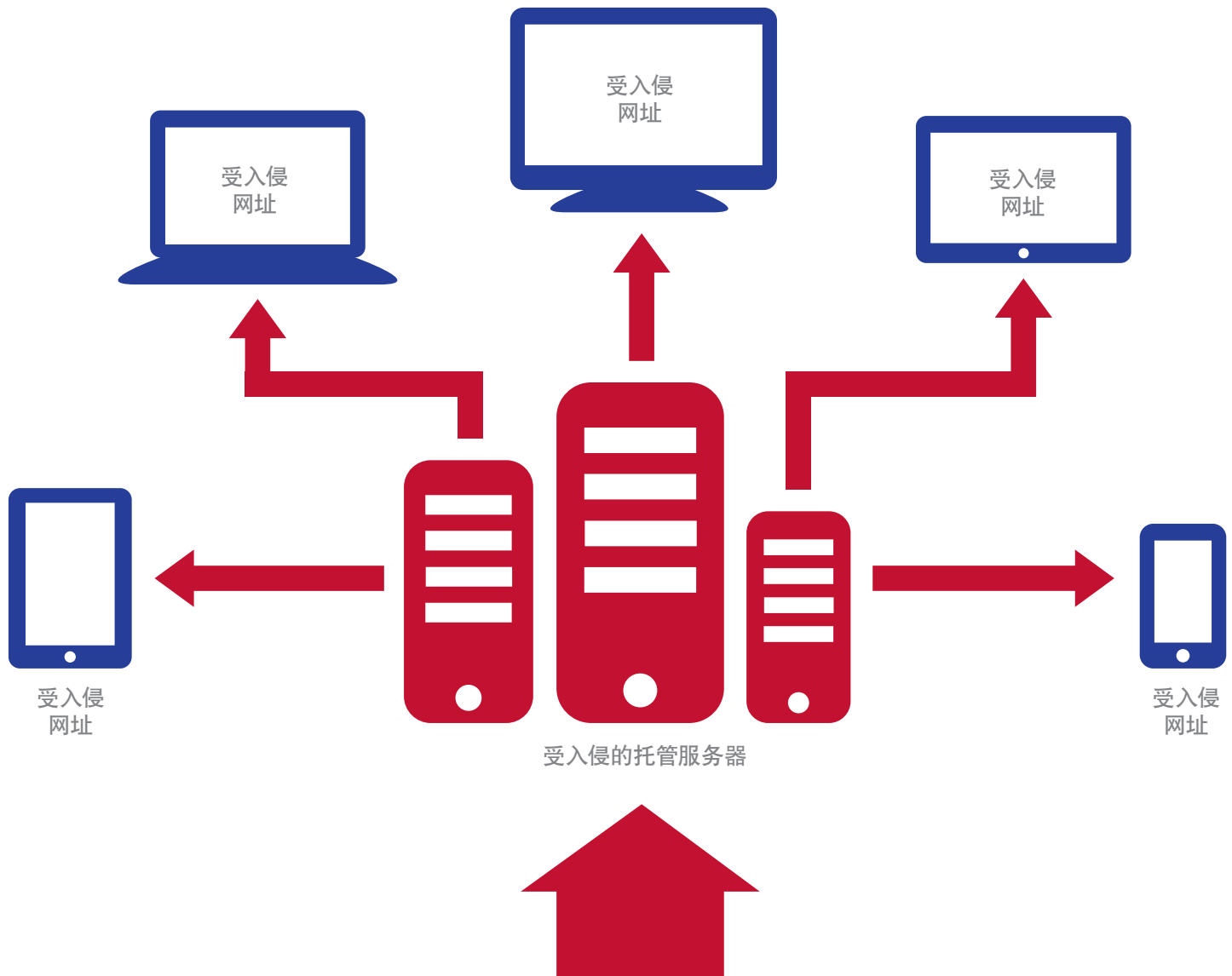
脆弱生态系统断裂

网络犯罪分子认识到，利用互联网基础结构的力量所能产生的利益远大于仅获取权限存取个人电脑。

恶意软件攻击的最新花样是获取权限访问网络托管服务器、域名服务器和数据中心，其目标是利用它们提供的卓越处理能力和带宽。利用此方法，网络攻击可以触及更多不知情的电脑用户，并对目标企业产生更大的影响，不论其目标是发表政治声明，削弱竞争对手，或产生收入。

图 24

高效感染策略



从本质上说，这种针对互联网基础结构发送攻击的趋势意味着 Web 本身的基础不可信任。用来最终获取托管服务器根访问权限的方法多种多样，并且包括诸如管理工作站的木马程序（旨在窃取服务器登录凭据）、服务器使用的第三方管理工具的漏洞和暴力登录尝试等策略（参阅第 53 页）。服务器软件本身的未知漏洞也可能被网络犯罪分子用来发动侵袭攻击。

被入侵的托管服务器会使全球成千上万的网站和网站所有者感染病毒（图 24）。

被入侵服务器托管的网站可用作重定向器（感染链的媒介）和恶意软件资源库。许多被入侵网站并非仅从几个恶意域名加载恶意软件（多对少关系），现已变成多对多关系（妨碍拆卸努力）。

域名服务器是此类新型攻击的主要对象，其使用的确切方法仍在调查。除个人网站和托管服务器之外，指标还包括某些托管服务提供商的域名服务器也正收到入侵。思科安全研究人员指出，这种针对互联网基础结构发动攻击的趋势正在改变威胁环境，因为它可使网络犯罪分子控制 Web 根基的重要部分。

“网络犯罪已变得如此有利可图和极具商业气息，它需要功能强大的基础结构确保自己在经济上应付自如”，思科威胁情报总监 Gavin Reid 说道。“入侵托管服务器和数据中心不仅可使攻击者获取权限使用大量带宽，而且可以获得这些资源持续正常运行的利益”。

> “网络犯罪能够带来丰厚的利润并已经高度商业化，因此需要强大的基础设施使其进行下去。”
>
> 思科的威胁情报主管 Gavin Reid 说。

连接点：DarkLeech 和 Linux/CDorked

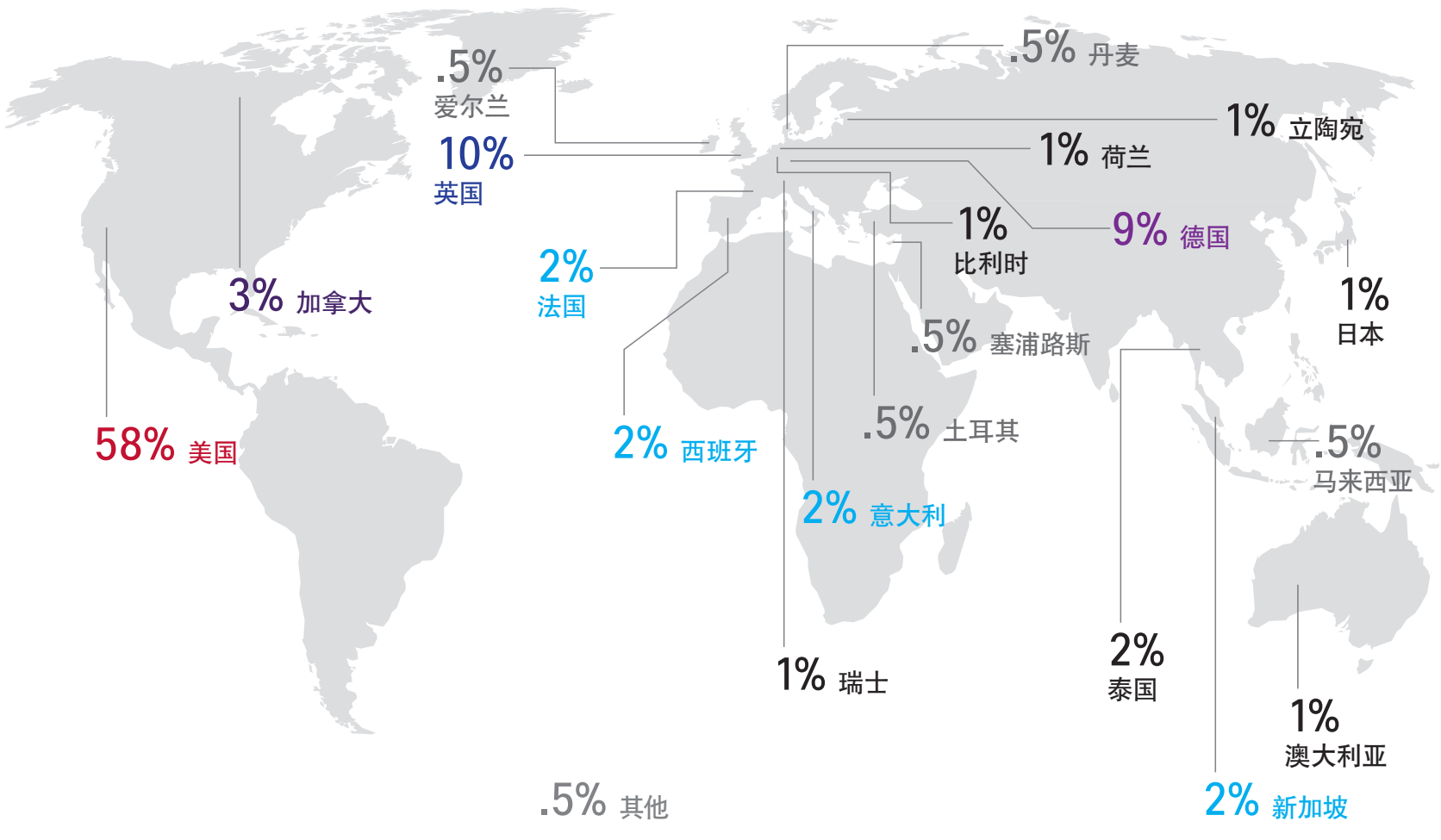
思科报告的 2013 年 DarkLeech 攻击活动 [18] 如何入侵强调托管服务器并将其用作更大规模攻击活动的跳板。据估计，DarkLeech 攻击在短期内入侵世界各地至少 20,000[19] 个使用 Apache HTTP 服务器软件的合法网站。被 Secure Shell 后台程序 (SSHD) 后门感染的网站可使远程攻击者上传和配置恶意 Apache 模块。入侵可使攻击者在被托管网站实时动态植入 iframes (HTML 元素)，通过 Blackhole 攻击软件包手段发送攻击代码和其他恶意内容。

由于 DarkLeech iframe 仅在访问网站时植入，因此感染迹象可能不是很明显。此外，为避免攻击检测，网络犯罪分子使用复杂的条件性标准阵列，例如仅在访问者从搜索引擎结果页访问网站时植入 iframe，当访问者的 IP 地址与网站所有者或托管服务提供商相同时不植入 iframe，仅每隔 24 小时向个人访问者植入一次 iframe。

图 25

2013 年受到 DarkLeech 攻击的服务器国家分布图

来源：思科 TRAC/SIO



思科 TRAC/SIO 调查显示，DarkLeech 攻击在全球各地均有发生；托管服务提供商数量最多的国家的病毒感染率当然最高。

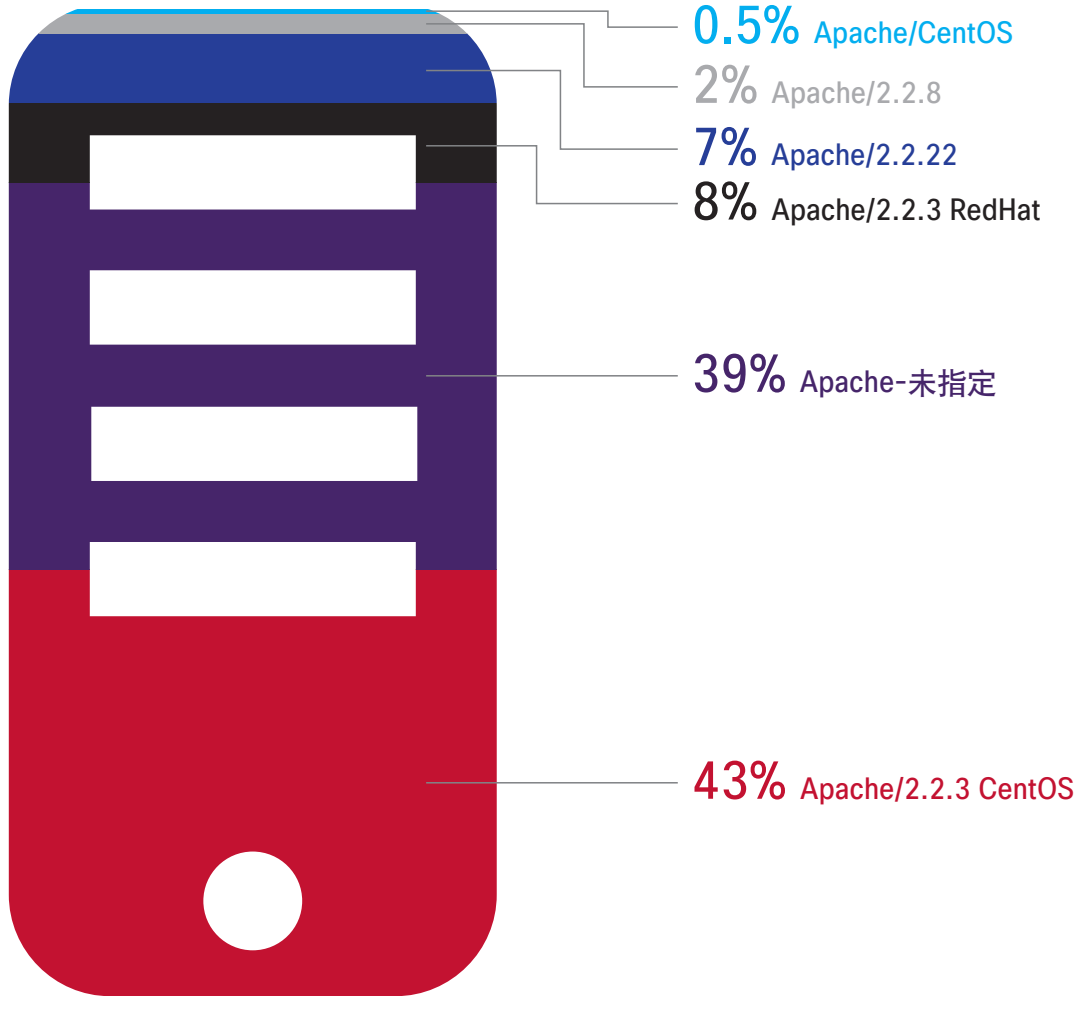
思科 SIO/TRAC 研究人员查询成千上万的被入侵服务器，以查明被感染入服务器软件版本的分布情况。

2013 年 4 月，思科检查到另一个恶意后面感染成百上千台运行 Apache HTTP 服务器软件的服务器。Linux/CDorked[20] 取代 cPanel 安装版本的 Apache 上的 HTTPD 二进制。此外，还发现针对 Nginx 和 Lighttpd 的相似后门。如同 DarkLeech 选择性使用攻击方法，CDorked 还使用条件性标准向受感染服务器托管的网站动态植入 iframe。浏览受感染网站的任何访问者然后收到另一个恶意网站发送的恶意内容，犯罪软件程序包尝试进一步入侵用户的个人电脑。[21]

图 26

受到 DarkLeech 攻击的服务器的响应

来源：思科 TRAC/SIO



Linux/CDorked 的独特功能是其在平均 24 小时内循环访问网站域名。仅极少数被入侵网站的使用时间会长于 24 小时。即使恶意软件域名被揭发，攻击者早已转移攻击对象。此外，对于 Linux/CDorked，攻击者经常更换托管服务提供商（大约每两周更换），循环访问被入侵主机，以避免被检测到。这些相同托管服务提供商被入侵的域名服务器可使恶意攻击实施者在主机间随意转换，但在过渡期间不会失去对域名的控制权。一旦更换到新主机，攻击者开始新域名循环周期，往往使用误植[22] 域名，企图使其在不经意观察者看来是合法的。

CDorked 和 DarkLeech 似乎是更大更复杂策略的一部分。

思科 TRAC/SIO 针对 CDorked 流量模式的分析结果表明其强烈建议连接DarkLeech。CDorked使用的特殊编码引用者URL专门表示DarkLeech的流量。但这并非是恶意软件最新奇的攻击花样：CDorked 和 DarkLeech 似乎只是更大、更复杂的攻击策略的一部分。

“这些攻击的复杂性表明网络犯罪分子已经牢牢控制住成千上万的网站和多个托管服务器，包括这些主机使用的域名服务器”，思科威胁情报总监 Gavin Reid 说道。“结合最近针对网站的大量暴力登录攻击，我们似乎正在见证趋势转变，使用 Web 基础体系构建仅可被描述为超大且极为强大的僵尸网络。使用此 überbot 发送垃圾邮件，传播恶意软件，并发动前所未见的大规模 DDoS 攻击”。

通常是针对性攻击征兆且可在所有企业网络中检测到的恶意流量

思科进行的威胁情报趋势研究结果表明，所有企业网站均可见恶意流量。这意味着，有证据表明富有经验的网络犯罪分子或其他积极参与者已渗透进这些网站，并可能长时间作业而未被发现。

所有企业均应假定其已被黑客入侵，或至少同意其成为攻击对象，但对何时受到攻击以及攻击持续多长时间有所疑问。

在最近实施的审查源于企业网络内部域名服务 (DNS) 查找项目的过程中，思科威胁情报专家发现，在所有情况下，有证据表明企业网络已被滥用或入侵 (图 27)。例如，思科分析的企业网络全都有流量流向托管恶意软件的网站，92% 的企业网络显示有流量流向无内容的网页，这些网页通常托管恶意攻击活动。96% 的企业网络有流量流向被劫持的服务器。

思科还检测到企业网络内有流量流向军事或政府网站 (企业通常与两者均无业务网络)，以及高风险地理区域的网站，如受到美国贸易禁运制裁的国家。思科还观察到，由于此类网站通常在公共或政府组织享有较高声誉，因此这些网站被网络攻击者使用。流向这些网站的流量可能并非入侵的明确迹象，但是对于平常与政府或军方无业务往来的企业，此类流量可能表明其网络正受到入侵，以致网络犯罪分子可以使用这些网络侵入政府或军事网站和网络。

尽管竭尽全力确保其网络免受恶意威胁，但是思科在 2013 年调查的所有企业的网络均存在可疑流量。通过 DNS 查找确定的流量可以提供显著 IoC，值得想要其网络制止这些极难检测到的攻击威胁的企业进一步开展调查。它是增加通常极难找到的犯罪行动的可见性的方法。

图 27

恶意流量无处不在

思科安全研究特点：

位元占用新花样和制止攻击的新方法

网络蟑螂—注册与特色商标相同或极为相似的域名的行为—是网络犯罪分子长期以来一直使用的工具。“位元占用”即为注册与原始域名仅有一个二进制数字差异的行为，最近已成为将互联网流量重定向至托管恶意软件或骗局的网站的另一种方法。

位元占用是一种形式的网络蟑螂，其针对计算机内存的位元错误。但凡内存读取的一个或多个位元不同于以前写入的状态时，即发生内存错误。这些内存错误发生的原因非常多，包括宇宙射线（即每秒每平米有 10,000 高能粒子撞击地球），在建议环境参数之外使用设备，工艺缺陷，甚至是低产率核爆炸。

通过更改单个位元，诸如“twitter.com”等域名可以变成位元占用域名“twitte2.com”。攻击者只需注册位元占用域名，等候发生内存错误，然后拦截互联网流量。

安全研究人员认为，最频繁解析的域名最有可能发生位元占用攻击，因为这些域名最有可能在发生位元错误时出现在内存中。但是，思科最近进行的研究预测，以前未被认为“受欢迎”到足以攻击的域名实际会产生有用数量的位元占用流量。这是因为每台设备的内存数量和连接到互联网的设备数量均不断增多；据思科估计，至 2020 年，将有 370 台“智能物品”连接到互联网。[23]

位元占用攻击载体

思科 TRAC/SIO 已找到新的位元占用攻击载体，包括：

- **子域分隔符位元占用：**根据公认的域名标签语法，域名内唯一有效的字符为 A-Z、a-z、0-9 和连字符。但是，检查位元占用域名时，限定搜索这些字符忽略了在域名内同样有效的重要字符：点号。一项新位元占用技术依赖于导致字母“n”（二进制 01101110）变成点号“.”（二进制 00101110）的位元错误，反之亦然。
- **“n”跳至“.”的子域名分隔符：**即上述技术的变异体，如果二级域名包含字母“n”，并且字母“n”后面有两个或多个字符，这是潜在的位元占用。例如，“windowsupdate.com”可能变成“dowsupdate.com”。
- **URL 分隔符位元占用：**流行的域名上下文位于 URL 内。在典型的 URL 内，诸如“/”等正斜杠字符用作分隔符，将方案与主机名和 URL 路径隔离开来。正斜杠字符（二进制 00101111）可通过一个位元跳转变成字母“o”（二进制 01101111，反之亦然。

接下一页

接上一页

防止位元占用攻击：创建位元占用 RPZ

安全专业人员通常使用以下两种缓解技术来防止位元占用攻击，但这两种技术均非最佳选择：

- **使用错误纠正（ECC）内存：**全球已安装的所有设备必须同时升级，以使其成为有效解决方案。
- **注册位元占用域名以使第三方无极可乘：**这并非总是可行，因为许多流行的位元占用域名已被注册。这也代价高昂，具体取决于域名的长度。

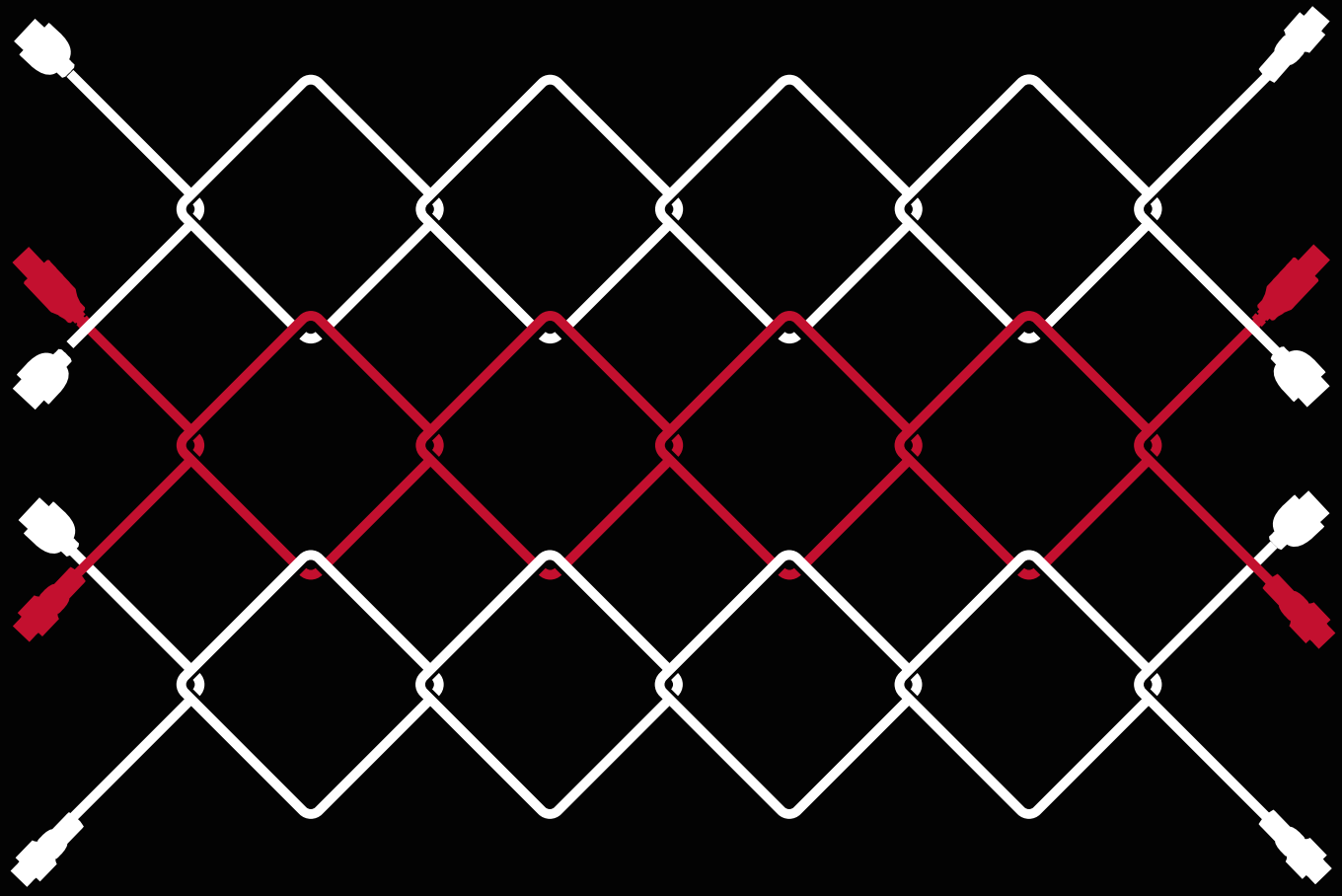
好消息是这些缓解技术并非安全专业人员用来保护用户免受意外误用互联网流量的唯一技术。只要采用数量足够多，新的缓解指数几乎可以完全消除位元占用攻击问题。

例如，自 BIND 版本 9.8.1 发布以来，响应政策区域 (RPZ) 已成为配置选项之一，早期版本的 BIND 的补丁存在。（BIND 是广泛使用的互联网 DNS 软件。）RPZ 是本机区域文件，通过说出域名并不存在 (NXDOMAIN)，重定向用户至“防火墙防御地区”（关闭平台），或其他可能性，可使 DNS 解析程序响应特定 DNS 请求。

要减轻 DNS 解析程序用户的单个位元错误的影响，解析程序管理器可以创建 RPZ，以保护经常解析或仅内部使用的域名免于位元占用。例如，可以设置 RPZ，向 DNS 解析程序发送这些域名的位元占用变量的任何请求都将获得 NXDOMAIN 响应，并悄无声息地纠正位元错误，无需对发生位元错误的客户端进行纠正。[24]

行业

思科 SIO 调查员深入讨论超出思科遥测范围的行业趋势。



暴力登录尝试受青睐的危害网站战术

虽然暴力登录尝试绝不是网络犯罪分子的新策略，但其使用量在 2013 年上半年增加了三倍。

在调查过程中，研究人员与思科 TRAC/SIO 发现了用于馈送这种行为的数据中枢。它包括 890 万种可能的用户名和密码组合，其中包括了强密码，而不只是“password123”这类易于破解的密码。被盗的用户凭据有助于保持这些组合的列表，而其他人希望它得到妥善保存。

图 28

暴力登录尝试工作原理

最近的暴力登录尝试主要以广泛使用的内容管理系统 (CMS) 平台为目标，例如 WordPress 和 Joomla。成功暴力登陆以获得对 CMS 未经授权的访问使攻击者能够上传 PHP (超文本预处理器) 后门程序和其它恶意脚本以破坏网站。在一些情况下，破坏可以使攻击者找到通往主机服务器的路径，然后将其强占 (图 28)。

鉴于全球有超过 6700 万 WordPress 站点——而且出版商正在使用该平台创建博客站点、新闻网站、公司网站、杂志、社交网络、体育网站等等——许多网络犯罪分子注重通过 CMS 获取访问权限就不足为奇了。[25] Drupal 这一迅速增长的 CMS 平台今年也成了攻击的目标，例如，在五月份，用户被建议更改密码，因为有人通过安装在 Drupal.org 服务器基础结构上的第三方软件[对 Drupal] 进行了未经授权的访问。[26]

许多网络犯罪都把目标集中在通过 CMS 获得访问权。

但这些系统成为理想的攻击目标不仅仅因为其流行。许多这样的网站——尽管处于活动状态——但基本上已经被拥有者抛弃。就像数百万遭到抛弃的博客和处于闲置状态的已购买域名一样，许多这些网站现在很可能由网络犯罪分子控制。由于全球新兴互联网市场有越来越多的人开设博客或网站然后弃之不顾，思科安全专家预测这一问题只会越来越严重。

插件的广泛使用也是那些希望未经授权访问 WordPress 和 Joomla 平台的网络恶徒们的福音，这些插件本来是为了增强 CMS 系统的承载视频、动画和游戏的功能。思科研究人员在2013观察到的许多 CMS 破坏都可追溯到用 PHP 网络脚本语言编写的插件，这些插件设计拙劣，没有考虑安全问题。

DNS 放大

缓解技术

思科安全专家指出，通过 DNS 放大发动的攻击在 2014 年仍是一大问题。开放解析程序项目 (openresolverproject.org) 发布报告指出，截至 2013 年 10 月，互联网内有 2800 万开放解析程序构成“重大威胁”。(考虑到 300 Gbps 的 Spamhaus DDoS 攻击仅仅 30,000 次开放解析程序。)

如果解析程序是开放的，这意味着它在发送响应时并未进行过滤。DNS 使用无状态的 UDP 协议，这意味着会代表其他当事方发送请求。该当事方随后接收放大数量的流量。这正是确定开放解析程序—并采取步骤关闭它们—安全行业在今后一段时间内必须处理的重要事宜的原因所在。

企业可以使用多种方式来减少通过 DNS 放大发动攻击的机会，包括实施互联网工程任务组的最佳实践 (BCP) 38 来避免成为攻击源。该最佳实践建议上游 IP 连接提供商过滤进入其网络的下游客户数据包，并摒弃其内部源地址未分配给该客户的任何数据包。[30] 该最佳实践由思科共同撰写，内含 uRPF 部署及实施指南。[31]

接下一页

DDoS 攻击：老瓶换新酒

分布式拒绝服务 (DDoS) 攻击——可扰乱进出目标网站的流量并能够使 ISP (互联网服务提供商) 瘫痪——在数量和严重程度上均不断增加。

因为 DDoS 攻击长久以来被认为是网络犯罪技术方面的“旧新闻”，很多企业相信他们采取的安全措施可以提供充分的保护。但 2012 年和 2013 年发生的大规模 DDoS 攻击动摇了这种信心，其中包括针对多家金融机构的燕子行动 (Operation Ababil)，该行动可能具有政治动机。[27]

“DDoS 攻击是公共和私营部门的组织在 2014 年最应该担忧的安全问题。”思科高级副总裁兼首席安全官 John N. Stewart 说道。“预计未来攻击活动会更加广泛并且持续更长时间。各组织，尤其是在已经成为攻击主要目标的行业中从事经营或拥有利益的组织，例如金融服务和能源行业，必须问问自己能否灵活应对，DDoS 攻击？”

一种新的手法：一些 DDoS 攻击可能被用于掩盖其他的不法活动，例如在攻击活动之前、之中或之后进行电汇欺诈。(请参阅第 57 页“黑色首尔”。) 这些攻击可以让银行工作人员应接不暇，阻碍向客户发送转账通知，以及阻碍客户报告欺诈行为。等某个机构从攻击中恢复过来后，其将无法挽回受到的经济损失。2012 年 12 月 24 日就发生了一起针对加利福尼亚地区金融机构网站的此类攻击，“攻击帮助分散了银行官员的注意力，使他们未发现一起窃取该银行某位客户网络账户的行为，造成了超过 900,000 美元损失。[28]

接上一页

另一种缓解技术是配置所有权威 DNS 服务器，以限制其响应速率。用作企业域名的权威域名服务器通常向所有请求开放。可以开启 DNS 响应速率限制 (DNS RRL) 功能，以防止 DNS 服务器回答同一实体太多次提出的相同问题，并保护企业免被用作 DDoS 攻击的媒介。启用 DNS 服务器的 DNS RRL 功能，服务器管理员可以使用此方法限制攻击者进行放大攻击时使用服务的有效性。DNS 响应速率限制是一个较新的功能，并非所有 DNS 服务器都支持此功能，仅流行的 DNS 服务器 ISC BIND 支持此功能。

此外，所有递归 DNS 服务器需要使用访问控制列表 (ACL) 进行配置，因此它们仅响应其自己网络上主机发送的查询。管理不善的 ACL 是 DNS 攻击的主要因素，尤其是拥有大量可用带宽的大型服务器。此项技术还有助于减少服务器成为 DDoS 攻击媒介的机会。

“由于安全行业讨论是否允许权威域名服务器禁用那些最终成为 DDoS 攻击媒介的实体的服务，因此企业应部署上述简单的缓解技术”，思科威胁情报总监 Gavin Reid 说道。

接下一页

主机服务器攻破技术的迅速深化只会使网络犯罪分子更容易发起 DDoS 攻击并窃取目标组织的信息 (请参阅第 43 页“在脆弱的生态系统中骨折”)。通过强占一部分互联网基础结构，恶意攻击者可以利用大量带宽进行定位以发起任意数量的强力攻击。这种事已经发生：2013 年 8 月，中国政府报告说，其有史以来受到的最大规模的 DDoS 攻击使中国互联网瘫痪将近四个小时。[29]

即使是垃圾邮件发送者也使用 DDoS 攻击对妨碍他们获取利益的组织发起反击。2013 年 3 月，跟踪垃圾邮件发送者并创建了 Spamhaus 黑名单——一个可疑 IP 地址目录——的非营利组织 Spamhaus 成为 DDoS 攻击的目标，使其网站暂时关闭并减缓了全球互联网流量。据称，攻击者与总部位于荷兰的 CyberBunker 以及 STOPhaus 存在关联，前者是一家托管服务提供商，其使用条款比较宽松，后者则公开表示不喜欢 Spamhaus 的活动。有人在广泛使用 Spamhaus 服务将 CyberBunker 列入黑名单后发起了这起 DDos 攻击。这明显是可疑的垃圾邮件发送者的报复，他们试图通过 DDoS 攻击使 Spamhaus 宕机。

DDoS 事件利用 DNS 放大攻击，它利用了开放 DNS 解析器对超出其 IP 范围的查询也作出响应。通过伪装为攻击目标的源地址向开放解析器发送非常小的蓄意形成的查询，攻击者可以激发解析器对攻击目标的极大响应。在最初试图使 Spamhaus 宕机失败后，攻击者对 Spamhaus 的 1 级和其他上游提供商进行了 DNS 放大攻击。

接上一页

欲了解 DNS 最佳实践详情，请参阅“DNS最佳实践、网络保护和攻击识别”：http://www.cisco.com/web/about/security/intelligence/dns-bcp.html。

黑色首尔

正如“DDoS 攻击：老瓶换新酒”中所述，网络犯罪分子的新攻击目标和主机服务器攻破技术的迅速发展只会使发起 DDoS 攻击和窃取组织的信息更加容易。

思科安全研究人员警告说，未来 DDoS 攻击很可能会造成重大破坏和损害——包括因窃取导致经济损失。

2013 年 3 月的“黑色首尔”针对性攻击使用了“雨刮器”恶意软件，该软件旨在销毁数万 PC 和服务器硬盘上的数据。这场攻击针对的是韩国的金融机构和媒体公司，其将有效载荷设定在同一时间激活。然而，雨刮器恶意软件似乎只是攻击的一个方面。该恶意软件在同一时间被触发，韩国网络提供商 LG U+ 的网站遭到污损，其他目标组织的网络则开始发生故障——功能因雨刷器恶意软件而无法复制。[32]

一些人认为这场攻击是朝鲜为了扰乱韩国经济而发动网络战的结果，或者是其他民族国家的破坏行为。但黑色首尔攻击以掩盖经济收益为目的的可能性是存在的。[33]

安全研究人员仍在试图了解这些攻击——以及追查谁应该对攻击负责——但证据表明，策划黑色首尔攻击的动机最早可追溯到 2011 年。那一年，美国 联邦调查局 (FBI) 首次对某种银行木马程序的出现发出警告，这种程序旨在掩盖从受害者账户电汇出诈骗资金。[34] 然后在 2012 年，RSA 安全公司报告了一类新的网络犯罪分子，他们构建复杂的木马活动，可以在预定日期发起攻击，并试图“在被安全系统拦截前尽可能多地从受害者账户汇出现金。”[35] 然后在 2012 年圣诞前夜，网络窃贼使用 DDos 攻击掩护他们盗窃加利福尼亚一家地区金融机构的行为。[36]

思科 TRAC/SIO 调查员表示，针对媒体组织和金融机构的黑色首尔攻击使用了一种恶意二进制，那是一种银行木马程序，专门以几家韩国银行的客户为目标。这一事实以及黑色首尔攻击发动前网络犯罪趋势的大事记表明，这场攻击可能由网络窃贼发动，为的是制造某种假象。

勒索软件

纵观 2013 年，攻击者越来越多地放弃通过僵尸网络感染个人计算机的传统方式。这种转变其中一部分包括更多地使用勒索软件作为来自受害网站、恶意邮件和木马下载程序的最终恶意软件有效载荷。勒索软件是恶意软件的一种，可以在指定费用支付前阻止受感染系统正常运行。

勒索软件为攻击者提供了一条难以跟踪但简单易行的直接收入来源，而不需要使用传统僵尸网络提供的那些中介租赁服务。攻击者模拟因失业和经济衰退导致独资企业大量增加的合法当地经济体，但网络犯罪分子的动机则是因关闭导致僵尸网络可用性和可访问攻击套件的丧失。

在整个 2013 年，越来越多的攻击者从传统的僵尸网络感染转移到个人电脑。

在 2013 年秋季，一种被称为 CryptoLocker 的新型勒索软件开始使用 RSA 2048 位密钥配对与 AES-256的组合加密受害者的文件。CryptoLocker会将文件移出本地计算机以包括任何可写映射驱动器上的匹配文件类型。加密过程完成后，受害者将看到一系列对话框，其中提供了支付赎金的详细说明 (图29) 。受害者还会看到一个要求其在特定时间内 (30到100小时) 支付赎金的计时器。对话框还会进一步警告说，如果赎金未在规定时间内支付，则命令和控制服务器上的私钥将被删除，此后文件将无法解密。

CryptoLocker的使用量在十月中旬出现飙升，这有可能是对这些框架所谓的作者被逮捕后丧失黑洞和酷攻击套件作出的回应。

图 29

CryptoLocker 勒索赎金说明

安全人才短缺和解决方案差距

[网络犯罪分子使用的技术和策略的复杂性——以及他们不断尝试破坏网络安全并窃取数据——已经超出了 IT 和安全专业人员处理威胁的能力。大多数组织没有人手或系统来对其网络一直实施监控并确定网络被渗透的方式。]

安全人才短缺使这一问题变得更加严重：即使预算充足，首席信息安全官也很难招到具备最新安全技能的人才。据估计，到 2014 年时全球安全专业人才短缺将超过一百万。具备数据科学技能的安全专业人员也处于供不应求状态——了解和分析安全数据可以帮助改善业务目标的实现情况。（请参阅第 68 页的附录，“安全组织需要数据科学家：安全从业人员数据分析工具导论”）

CISO 努力雇用具有最新的安全技能的人员。

作为新周边的云

正如首席信息安全官对思科安全专家所说的 (见第 18 页)，将越来越多的关键业务数据转移到云中是日益严峻安全问题。

思科工程部副总裁 Michael Fuhrman 说，云计算革命与二十世纪九十年代基于 Web 的解决方案的崛起类似。

Fuhrman 说："这是企业使用新技术的根本性转变——与此同时，我们也看到犯罪分子发动网络攻击的兴起。""今天，根本性的转变来自云计算。企业不仅将许多关键应用程序托管在云端，而且还使用云计算来消耗和分析关键业务信息。"

云计算的增加是不可否认的，也是无法阻止的。

云计算的崛起是不可否认且不可阻挡的。思科预计，云计算网络流量到 2017 年时将增长三倍以上。[37]

在2014年及此后，安全专家预计可看到整个企业周边迁移到云端。这些网络边缘近年来一直处于变得远非定义明确的过程中。但将这么多应用程序和数据托管在云端，企业正在迅速丧失了解进出企业边界的人和物的能力，也不了解用户正在采取什么行动。

向云计算转变改变了游戏规则，因为它重新定义了数据的存储、移动和访问，而且为攻击者提供了更多机会。

对云服务供应商如何保护他们的产品不受安全攻击缺乏了解增加了人们将数据控制权移交云端的担忧。企业往往不会仔细询问云服务供应商的服务水平协议中包含的内容，或者供应商升级安全软件或修补漏洞的频率。

企业需要确保云服务供应商使用了最先进的工具和策略来阻止攻击，或者及时发现并制止在进行的攻击。对于信息安全团队而言，决定迁往云端往往归结为一个问题："我应该寻求供应商提供哪些控制措施才能放心让供应商管理并保护我的数据？"

另一方面，云服务提供商在努力确定和实施一套可管理的控制措施，以符合国际法规日益增多的要求，这是应对日益严峻的安全环境所必须的。

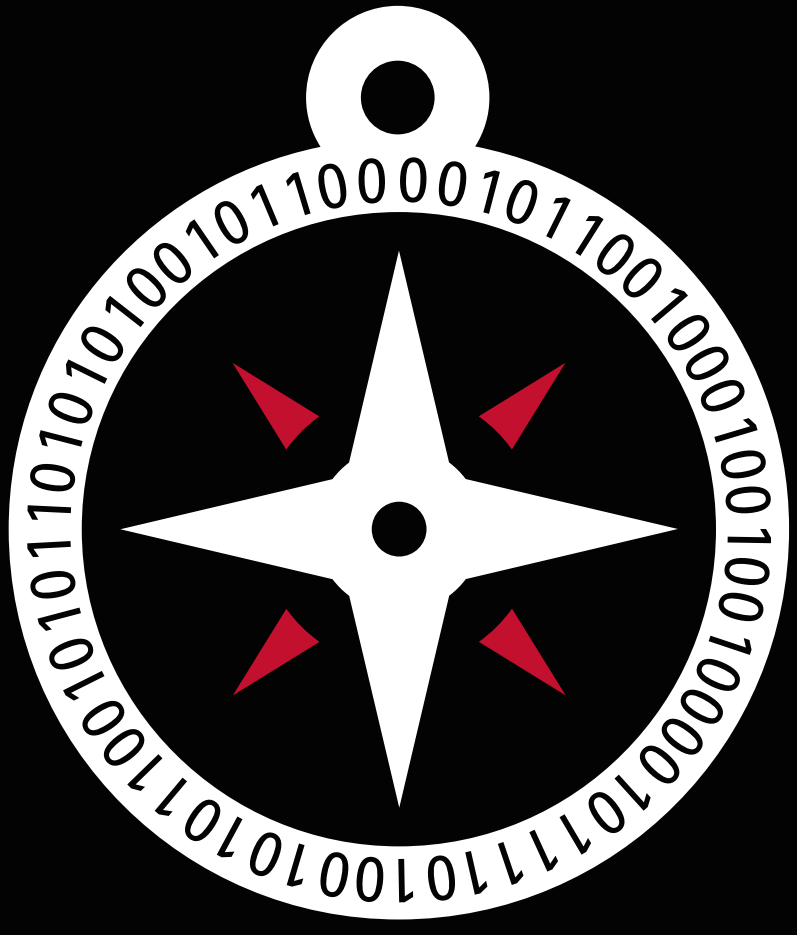
"当我们选择供应商提供安全和关键基础结构时，我们常常根据技术资质和信誉决定购买。"思科高级副总裁兼首席安全官 John N. Stewart 说道。"最近，供应商的流程和不断发展的安全措施也是越来越重要的因素。"

巧的是，使云成为威胁的因素——例如网络周边之外的位置以及越来越多地使用云计算处理关键业务数据——可使企业作出更准确且近乎实时的安全决策。随着更多的流量流经云端，同样依赖云计算的安全解决方案可以快速、轻易地分析这些流量，并从中获得补充信息。此外，对于小型或预算有限的组织，保护和管理良好的云服务可提供比企业自己的服务器和防火墙更多的安全保障。

> "我们在选择安全和关键基础设施的供应商时，我们通常根据技术条件和声誉进行购买。最近，供应商的流程与不断发展的安全方法也成为越来越重要的因素。"
>
> John N. Stewart，思科高级副总裁兼首席安全官

建议

越来越多的组织正在努力实施采用了新技术的有效策略来支持其巩固安全愿景，简化其架构和操作，并且增强其安全团队。



2014 年目标：验证可信度并提高能见度

如今，在一个与网络或设备相关的信任水平必须经过动态评估的环境中，组织面临各种支离破碎的的安全模型，这些模型存在执行不一致、威胁情报孤立化且需要管理供应商和产品扩散的问题。

组织、数据和恶意攻击者发动的高级攻击之间的联系对于单一设备而言过于复杂，难以应对。而且大多数组织缺少具有专业知识和经验的安全人员帮助他们调整自己的安全模型以应对挑战——和迎接机遇——由云计算、移动计算和其他受技术进步推动的开展业务的新方式带来的机遇。

在过去一年中，各种类型组织均努力理解如何拥抱创新而不至于创建新的安全漏洞或扩大已知的漏洞。2013 年也将信任问题推上了台面。所有类型的用户如今不论是在工作中还是在个人生活中都更可能对他们日常依赖的技术的可信度提出质疑。因此，技术供应商帮助向客户保证安全是其制造流程中的首要关切比以往任何时候都更加重要——并且要时刻准备支持这些保证。

思科首席安全官 John N. Stewart 说：“我们正处于信任至关重要的市场转型过程中，流程和技术必须是产品设计的组成要素，以使供应商满足应对当今威胁的需求。一家公司的承诺是不够的。公司需要通过认证的产品、集成开发流程、创新技术和行业内受尊敬的地位得到确证。组织还必须使验证他们所使用技术产品以及产品供应商的可信度成为持续的首要关切。”

提高安全经营与业务目标之间的一致性也是增强企业安全的重要措施。在资源有限和预算不足的情况下，这种一致性可以帮助组织中的首席信息安全官和其他安全高管确定主要风险和适当的缓解措施。此过程其中一部分就是接受并非所有企业资源在任何时候都能得到完全保护这一事实。思科威胁情报主任 Gavin Reid 说："从网络安全角度就什么最重要达成协议。""比起希望找到解决一切问题的神奇药丸，这种方法更有成效。"

为了应对当今面临的安全挑战，组织需要全面检查他们的安全模型并了解攻击连续性的全貌：

- 攻击发生前：要保卫自己的网络，组织必须对设备、操作系统、服务、应用程序、用户和其他方面有所了解。此外，他们还必须实施访问控制，执行安全策略，并且阻止应用程序及对关键资产的总体访问。然而，安全策略和控制措施只是整个安全宏图的一小部分。这些措施可以帮助减少攻击面，但攻击者总会找到某些漏洞，然后加以利用以实现其目标。
- 攻击过程中：组织必须使用可以在任何威胁可能出现的地方运行的解决方案来应对各种各样的攻击媒介——在网络上、在断点上、来自手机设备以及在虚拟环境中。部署有效的解决方案后，安全专家将能更好地阻止威胁并帮助保卫系统环境。
- 攻击结束后：肯定的是，许多攻击都会成功。这意味着组织需要实施正式的计划，使他们能够确定攻击造成损害范围、补救措施并且尽快恢复正常运营。

> 思科安全集团的首席安全架构师 Marty Roesch 说："攻击者和他们的工具经过发展已经可以避开传统防御。实际上，攻击者能否攻破系统不再是问题，问题是他们何时攻破。""在攻击发生之前、之中和之后，需要采取可见性驱动且专注于威胁的安全措施以保护用户度过连续的攻击。"

服务如何有助于应对安全挑战

随着攻击面的扩大、攻击模型的日益扩散和复杂化以及网络复杂性的日益增加，更多的组织正在努力采用新技术、简化其架构和操作并加强其团队来巩固其安全愿景。

正如第 60 页讨论的，安全人才的缺乏使这些问题变得更加复杂。此外，安全行业的创新速度比企业采用并实施这些新工具的速度要快。

寻找合适的人才以有效地应对不断变化的安全环境是一项挑战。引进互补的外部资源不仅可以帮助降低成本，也使企业可以腾出资源以专注于更优先的事项。

加强链条中的薄弱环节

防范威胁对于维护网络安全当然至关重要。这是为什么当更多的网络犯罪分子将攻击重点从入侵个人计算机转到破坏互联网基础结构时，思科的安全专家建议 ISP 和主机公司发挥更积极的作用帮助保护互联网的完整性。

确定难以检测的威胁，例如 DarkLeech 和 Linux/CDorked（参见第 45 页）需要主机提供商有更多“人员响应”。这样的响应包括来自用户的全面调查报告并予以严肃对待。提供商还需要建立更好的控制措施，以确保其能够验证他们的服务器操作系统安装的完整性。思科调查人员说，由于 CDorked 这样的隐蔽恶意软件，如果未实施适当控制以验证安装的完整性，则安全团队将无法知晓二进制是否被替代。

个人用户的系统当然容易遭到破坏，但链条中某些环节的弱化在用户遭到威胁很久以前就开始了。现在，攻击更多的时候发生在链条的中间环节，这就是为什么提供商需要更好地了解以互联网基础结构为目标的潜在威胁。

附录

安全组织需要数据科学家

安全从业人员数据分析工具导论

首席安全官 (CSO) 团队正在收集前所未有的大量数据和情报，而且在这些数据中捕获的情报具有极大的使用价值。分析安全相关的数据提供了了解攻击者活动的线索并使人从中洞悉挫败攻击的可行方案。

数据分析对于安全从业人员并不新鲜。安全从业人员同时也期望记录将会生成并得到标注。渗透测试员在做完评估后创建调查记录。操作系统设计人员施用审计子系统。应用程序开发人员设计可以生成日志的应用程序。

不论记录的称谓是什么，有一件事是肯定的：安全从业人员掌握了大量数据——而分析数据可能会有重要发现。

虽然数据分析本身并非新鲜事物，但安全环境的演变已经对数据分析过程产生了影响：

- 所生成数据的绝对数量是惊人的。
- 需要进行特定数据分析的频率在不断增加。
- 标准化报告虽然有帮助，但这是不够的。

安全从业人员拥有大量的数据，对这些数据进行分析可以获得重要的发现。

幸运的是，安全从业人员进行数据分析的门槛即使在这种更复杂的环境中也比较低——而且数据分析工具生态系统非常丰富。以下是安全从业人员可以用于开始进行数据分析的一些免费工具的概览。

使用 Wireshark 和 Scapy 分析流量

Wireshark 和 Scapy.是两个出色的流量分析工具。Wireshark 不需要介绍。Scapy 是一个基于 Python 的工具，可用作 Python 模块或以交互方式定制或检查流量。

Wireshark 包含丰富的命令行工具套件和协议解码器，是必不可少的工具。例如，使用 Wireshark 的 tcp.stream 显示过滤字段，可以将多个 TCP 流中包含的 pcap 文件分解成较小的文件，每个小文件都包含属于单一 TCP 流的所有数据包。

图 1 所示的命令可以打印 traffic_sample.pcap 中前五个 TCP 数据包的 TCP 流索引。

图 A1

解压 tcp.stream 索引的 tshark 命令

```
tshark -r traffic_sample.pcap -T fields -e tcp.stream tcp | head -n 5
```

tshark 是 Wireshark 的命令行工具之一。

tcp.stream 表示 TCP 显示过滤器流索引字段。

知道索引后，人们可以编写脚本将 traffic_sample.pcap 分割成单个 pcap 文件：

```
$ cat ~/bin/uniq_stream.sh
#!/bin/bash

function getfile_name() {

                orig_name=$1
                stream=$2
                file_name="$(echo $orig_name | cut -d'.' -f1)"
                file_name+="-${stream}.pcap"

                echo "${file_name}"

                return 0
}

streams=$(tshark -r ${1} -T fields -e tcp.stream | sort -un | tr '\n' ' ')

for x in ${streams}
do
                file_name=$(getfile_name ${1} ${x})
                echo "Creating ${file_name}..."
                tshark -r ${1} -w $file_name tcp.stream eq ${x}
done
$
```

该脚本会为 traffic_sample.pcap 中的 147 个 TCP 流分别创建一个 pcap 文件。现在是更容易进行进一步分析每个TCP流。请注意，来自 traffic_sample.pcap 的非 TCP 数据包将不会包括在任何新的 pcap 文件中：

```
$ /bin/uniq_stream.sh traffic_sample.pcap
Creating traffic_sample-1.pcap...
Creating traffic_sample-2.pcap...
...
...
Creating traffic_sample-146.pcap...
Creating traffic_sample-147.pcap...
```

Scapy 有其自身的优势。由于其是用 Python 语言开发的，可以使用 Python 语言的所有功能和其它 Python 工具。以下代码片段演示了 Scapy 如何利用运算符重载，以便快速和直观地定制流量：

```
# scapy
>>> dns_query = IP()/UDP()/DNS()
>>> from socket import gethostbyname,gethostname
>>> dns_query[IP].src = gethostbyname(gethostname())
>>> dns_query[IP].dst = “8.8.8.8”
>>> import random
>>> random.seed()
>>> dns_query[UDP].sport = random.randint(0, 2**16)
>>> dns_query[DNS].id = random.randint(0, 2**16)
>>> dns_query[DNS].qdcount = 1
>>> dns_query[DNS].qd = DNSQR(qname=“www.cisco.com”)
>>> scapy.sendrecv.sr1(dns_query)
>>> response = scapy.sendrecv.sr1(dns_query)
Begin emission:
.....Finished to send 1 packets.
.*
Received 14 packets, got 1 answers, remaining 0 packets
>>> response[DNS].ar[DNSRR].rdata
‘64.102.255.44’
>>>
```

这段代码例显示了构建数据包和分析实时流量的方式。然而，Scapy 用来分析 pcap 文件也一样容易。

CSV 数据分析

逗号分隔值 (CSV) 是进行数据交换的流行格式。许多工具 (包括 tshark) 允许用户将数据导出为 CSV 格式。通常，安全从业人员可以使用 Excel 等电子表格程序来分析 CSV 数据。他们也可以使用 grep、cut、sed、awk、uniq 和 sort 等命令行工具。

考虑使用 csvkit 作为替代。Csvkit 提供了若干实用程序，使其可以更容易地处理来自命令行的 CSV 数据。请检查以下 CSV 文件，注意要查找 src 列中包含 tty.example.org 主机的所有行有多容易：

```
$ head -n 3 tcp_data.csv
src,srcport,dst,dstport
“tty.example.org”,“51816”,”vex.example.org”,”443”
“vex.example.org”,”443”,”tty.example.org”,”51816”

$ csvgrep -n tcp_data.csv
                1: src
                2: srcport
                3: dst
                4: dstport

$ csvgrep -c 1 -r ‘tty\.example\.org’ tcp_data.csv | head -n 5
src,srcport,dst,dstport
tty.example.org,51816,vex.example.org,443
tty.example.org,51816,vex.example.org,443
tty.example.org,51427,paz.example.org,5222
tty.example.org,51767,bid.example.org,80
```

Csvkit 包含一系列实用程序。Csvstat 会自动计算各种统计数据，尤其实用。例如，它可以很容易地计算出频率最高的前五个 src 主机：

```
$ csvstat -c 1 tcp_data.csv
  1. src
  <type ‘unicode’>
  Nulls: False
  Unique values: 55
  5 most frequent values:
                tty.example.org:        2866
                lad.example.org:        1242
                bin.example.org:        531
                trw.example.org:        443
                met.example.org:        363
Max length: 15

Row count 6896
```

Matplotlib、Pandas、IPython 和其它

可以使用的基于 Python 的数据分析和可视化的工具非常丰富。SciPy 网站是发现这些工具的一个好地方 (http://www.scipy.org) 。Matplotlib、pandas 和 IPython 工具包特别令人感兴趣：

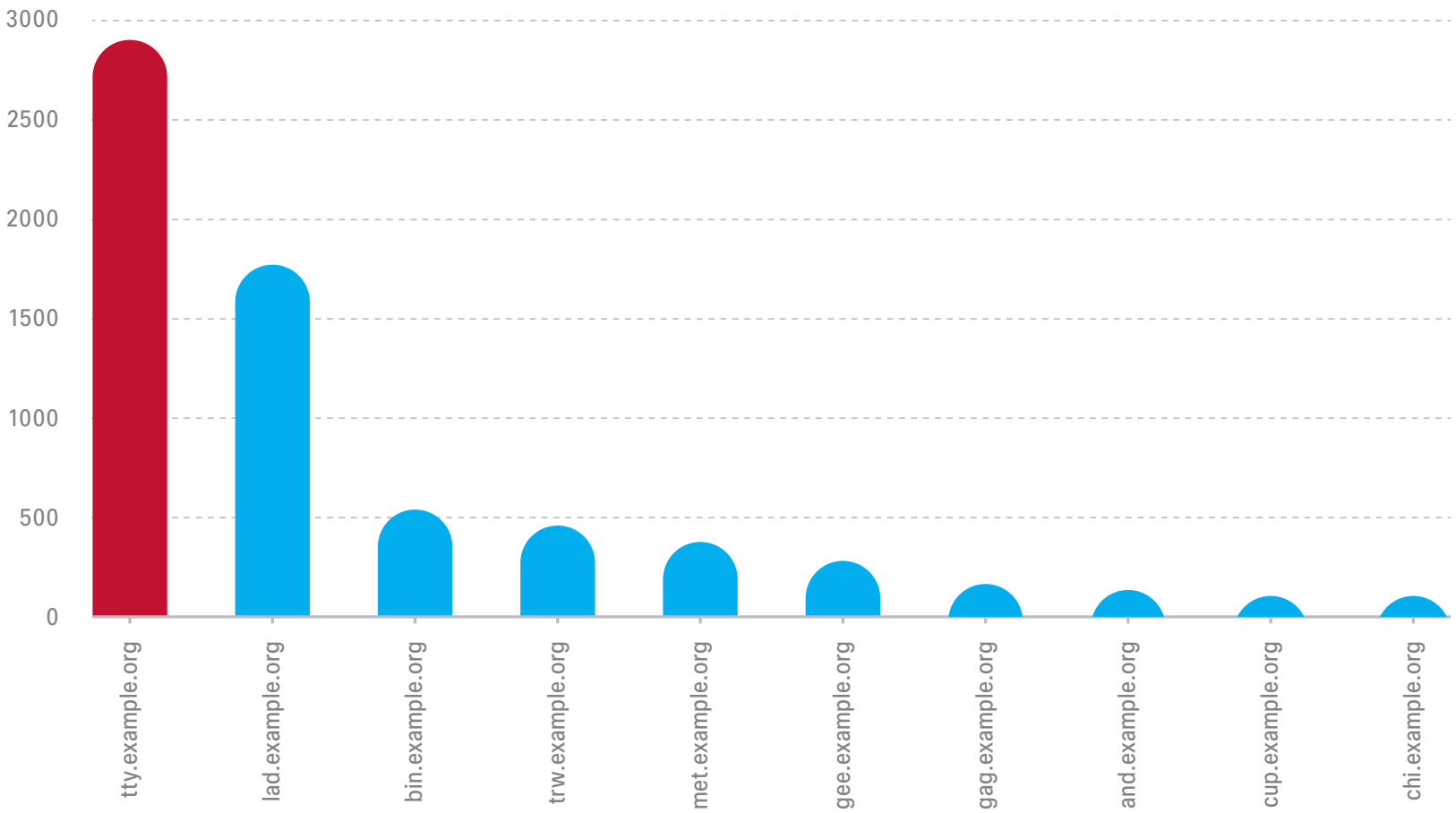
- Matplotlib 具有方便、灵活和可视化特征。
- Pandas 提供了操作和检查原始数据的工具。
- IPython 为 Python 解释器带来的功能可方便交互式数据分析。

以下代码展示了安全从业人员可以如何使用这三个工具绘制 tcp_data.csv 中前几大 src 主机的图表。

```
In [3]: df = read_csv("/Users/shiva/tmp/data_analysis/tcp_data.csv")
In [4]: df
Out[4]:
<class 'pandas.core.frame.DataFrame'>
Int64Index: 6896 entries, 0 to 6895
Data columns (total 4 columns):
src 6896 non-null values
srcport 6896 non-null values
dst 6896 non-null values
dstport 6896 non-null values
dtypes: int64(2), object(2)
In [5]: df['src'].value_counts()[0:10]
Out[5]:
tty.example.org 2866
lad.example.org 1242
bin.example.org 531
trw.example.org 443
met.example.org 363
gee.example.org 240
gag.example.org 126
and.example.org 107
cup.example.org 95
chi.example.org 93
dtype: int64
In [6]: df['src'].value_counts()[0:10].plot(kind="bar")
Out[6]: <matplotlib.axes.AxesSubplot at 0x8479c30>
```

图 A2

使用绘图 () 生成的图表



pandas 的好处就在于其允许用户浏览数据的方式。例如，要查找 tty.example.org 为每个与其通信的 dst 和 dstport 组合连接的独特 srcport 的数量非常容易：

```
In [229]: tty_df = df[df.src == “tty.example.org”]
In [230]: num_ports = lambda x: len(set(x))
In [231]: pivot_table(tty_df, rows=[‘dst’,‘dstport’], values=‘srcport’, aggfunc=num_ports)
Out[231]:
dst dstport
add.example.org 80 2
ala.example.org 80 3
and.example.org 80 1
auk.example.org 80 2
bid.example.org 80 1
…
```

开始分析数据

前几页的例子只是沧海一粟，并未展示所述工具的全部功能。但安全从业人员用它们来执行有意义的数据分析足足有余。

首席安全官们需要让他们的安全从业人员戴上数据科学家的帽子。深入挖掘可用的数据将可了解到其他方式无法提供的信息。随着时间推移，对于需要浏览数据哪些部分的直觉将培养起来。一些组织甚至可能发现他们可以受益于在团队中安排专门人员担任数据科学家。

关于思科 SIO

Cisco SIO

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。

思科采用思科安全智能运营中心 (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、基于云的安全生态系统，它使用超过 75 兆兆位由已部署思科电邮、网络、防火墙和入侵防御系统 (IPS) 解决方案提供的实时数据源。

Cisco SIO 对数据进行分析和处理，然后自动对威胁进行分类并使用 200 多种参数创建规则。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。

传统的安全措施不足以防御最新一代的恶意软件。

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：www.cisco.com/go/sio。

尾注

1 有关任意对任意评估的更多信息，请参考 *Cisco 2013 年度安全性报告*的“设备、云和应用程序”部分：https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf。

2 同上

3 *不再需要“咬嚼中心”：引入信息安全零信任模型*，作者 John Kindervag、Forrester，2012 年 11 月 12 日

4 “Timeline of Edward Snowden’s Revelations,” *Al Jazeera America*: http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html.

5 “NSA collecting phone records of millions of Verizon customers daily,” 作者：Glenn Greenwald, *The Guardian* 2013 年 6 月 5 日：http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

6 GCHQ：政府通信总部，一家英国情报局。

7 “NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say,” 作者：Barton Gellman 和 Ashkan Soltani，2013 年 10 月 30 日*华盛顿邮报*：http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

8 有关更多信息，请参考“Cisco Secure Development Life cycle (CSDL)”：http://www.cisco.com/web/about/security/cspo/csdl/index.html.

9 同上

10 思科将“万物互联”定义为“下一波互联网的显著增长，将经历人、过程、数据与事情的大汇合。”

11 “紧随波斯顿悲剧之后，大量的垃圾邮件和恶意软件活动将大行其道，”*思科安全性博客*，2013 年 4 月 17 日：http://blogs.cisco.com/security/massive-spam-and-malware-campaign-following-the-boston-tragedy/.

12 同上

13 同上

14 Java 网站“关于”页面：http://www.java.com/en/about/.

15 要了解更多关于“任意对任意评估”的信息，请参考*Cisco 2013 年度安全性报告*：http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf。

16 “采用了可能的高级侦测能力的劳工部水坑攻击确认为 0-Day 攻击，”作者：Craig Williams，*思科安全性博客*，2013 年 5 月 4 日：http://blogs.cisco.com/security/department-of-labor-watering-hole-attack-confirmed-to-be-0-day-with-possible-advanced-reconnaissance-capabilities/.

17 “水坑攻击以能源领域为目标”，作者：Emmanuel Tacheau，*思科安全性博客*，2013 年 9 月 18 日：http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/.

18 “Apache DarkLeech 妥协，”作者：Mary Landesman，*思科安全性博客*，2013 年 4 月 2 日：http://blogs.cisco.com/security/apache-DarkLeech-compromises/.

19 “正在进行的以 Apache 为攻击目标的恶意软件攻击袭击了 20,000 网站，”作者：Dan Goodin,*Ars Technica* 2013 年 4 月 2 日 http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/.

20 “Linux/CDorked常见问答，”作者：MaryLandesman，*思科安全性网站*，2013年5月1日：http://blogs.cisco.com/security/linuxcdorked-faqs/.

21 “DarkLeech Apache 大肆攻击，” 作者：Matthew J. Schwartz，*信息周刊*，2013 年 4 月 30 日 http://www.informationweek.com/security/attacks/DarkLeech-apache-attacks-intensify/240153922.

22 域名误植是指注册与著名域名中的一个字符不同的域名的行为。

23 “由于 IoE，下个十年看起来非常“疯狂”，作者：Dave Evans，*思科平台博客*，2013 年 2 月 12 日 http://blogs.cisco.com/news/thanks-to-ioe-the-next-decade-looks-positively-nutty/.

[24] 有关域名抢注缓解策略的更多信息，请参见思科白皮书 *Examining the Bitsquatting Attack Surface*，2013：http://blogs.cisco.com/wp-content/uploads/Schultz-Examining_the_Bitsquatting_Attack_Surface-whitepaper.pdf.

[25] “WordPress Sites in the World” 和 “A Look at Activity Across WordPress.com,” WordPress.com: http://en.wordpress.com/stats/.

[26] “重要安全更新：重设您的 Drupal.org 密码，” Drupal.org，2013-5-29：https://drupal.org/news/130529SecurityUpdate.

[27] 有关燕子行动活动模式及载荷的更详细报告，请参考 “Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions”：http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[28] “DDoS Attack on Bank Hid $900,000 Cyberheist,” by Brian Krebs, *KrebsonSecurity* 博客，2013 年 2 月19 日：http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[29] “中国互联网周末遭遇攻击，” 作者：Paul Mozer，*中国实时报道*，WSJ.com，2013 年 8 月 26 日：http://blogs.wsj.com/chinarealtime/2013/08/26/chinese-internet-hit-by-attack-over-weekend/.

[30] 来源：Wikipedia: “入站过滤”： http://en.wikipedia.org/wiki/Ingress_filtering.

[31] “了解逆向路径转发，” 思科网站：http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html.

[32] “Your Hard Drive Will Self-Destruct at 2 p.m.: Inside the South Korean Cyberattack,” 作者：Sean Gallagher，*Ars Technica*，2013 年 3 月20 日： http://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/.

[33] “关于 DarkSeoul 的思考：数据共享与针对性攻击者，” 作者：Seth Hanford，*思科安全性网站*，2013 年 3 月 27 日 3 月 27 日：http://blogs.cisco.com/tag/darkseoul/.

[34] 同上

[35] “网络黑客寻求僵尸主控机发动针对美国银行的大规模特洛伊木马 攻击，” 作者：Mor Ahuvia，RSA，2012 年 10 月 4 日：https://blogs.rsa.com/cyber-gang-seeks-botmasters-to-wage-massive-wave-of-trojan-attacks-against-u-s-banks/.

[36] “DDoS Bank 银行攻击隐藏 90 万美元的网络盗窃案，” 作者：Brian Krebs，*KrebsonSecurity* 博客，2013 年 2 月19 日 http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[37] “思科项目数据中心云流量到2017年将翻番，至顶网，2013年10月15日：http://www.zdnet.com/cisco-projects-data-center-cloud-traffic-to-triple-by-2017-7000021985/.

美洲总部
Cisco Systems, Inc.
San Jose, CA

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International
荷兰
阿姆斯特丹

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。