思科 2016
年中网络安全报告

目录

执行摘要和主要研究结果

防御者必须减少攻击者的行动时间。
这是挫败攻击者的关键。

目前，攻击者的行动时间毫无限制。他们的攻击活动通常利用组织和最终用户可能（本应）有所了解且已经处理的已知漏洞，可在几天、几个月甚至更长时间内保持活动状态并且不被发现。与此同时，防御者竭力了解威胁活动并缩短已知威胁和新威胁的检测时间 (TTD)。他们取得了长足进步，但是要真正破坏攻击者铺设攻击基础并进行具有高冲击强度且有利可图的攻击的能力，仍任重道远。

《思科® 2016 年年中网络安全报告》提供来自思科安全研究部门的研究、见解和观点，为安全专业人员带来我们在上一份安全报告中介绍的趋势的最新信息，另外还研究了可能影响今年下半年的安全形势的新情况。

我们对影子经济的最新发展情况的全面观察证实，攻击者对创造收入的关注有增无减。勒索软件已成为特别有效的摇钱树，企业用户似乎已成为某些勒索软件操纵者的首选目标。本报告讨论的许多威胁和安全趋势都与勒索软件相关，从用于发起攻击活动和隐藏攻击者活动的技术，到我们对这一强大威胁的下一代演变情况的预期，不一而足。

在本报告中，我们探讨了组织为了改善其防御能力，能够且应该采取的行动。思科研究人员的建议包括：

- **制定并测试在遭受勒索软件攻击后能够帮助快速恢复正常业务运营的事件响应计划**
- **不盲目信任 HTTPS 连接和 SSL 证书**
- **快速采取行动，修补已发布的软件和系统（包括作为关键互联网基础设施组件的路由器和交换机）漏洞**
- **对用户进行有关恶意浏览器感染威胁的教育**
- **了解什么才是真正可行的威胁情报**

在本报告中，我们涵盖四个主要的主题领域：

I. 网络犯罪趋势聚焦：勒索软件

思科安全研究人员已将其焦点放在勒索软件上，研究可能导致此类恶意软件攻击大幅蔓延的种种创新。另外，还根据之前观察到的趋势，提供了勒索软件的演变预测。此外，我们还考虑了未修补的系统和过时设备中的漏洞是如何为恶意攻击实施者提供行动时间的。勒索软件操纵者现在正在瞄准企业用户。因此，组织应该确保将关键数据备份到受保护场所，并建立在发生攻击后能够帮助他们尽快恢复正常业务运营的可行计划。

II. 行动时间

本部分研究为攻击者提供时间和机会进行威胁创新并开展攻击活动的客户端攻击媒介。涉及加密和授权的漏洞的增加，标志着威胁实施者现在正在伺机攻击安全连接。本部分探讨了漏洞攻击包和攻击媒介的发展趋势，例如服务器漏洞对于试图接触更广数据集的网络犯罪分子的吸引力。另外，还研究了“恶意广告即服务”的兴起及其给防御者造成的难题，以及由此引起的谁应保护网络用户的问题。

III. 保护时间

在本部分，思科安全研究人员探讨了攻击者活动与安全解决方案之间的时间差。例如，虽然供应商缩短了从公布公共漏洞到提供补丁的时间，但是用户在实施这些补丁时却存在滞后。本部分还包括思科在不断努力缩短其中值检测时间 (TTD) 方面的最新成果以及攻击者和防御者之间持续展开“军备竞赛”的影响。思科研究人员还详细介绍了 HTTPS 在恶意攻击活动中的使用不断增加，以及恶意攻击实施者使用传输层安全 (TLS) 来加密其通信的情况。

IV. 全球视野和安全建议

本部分研究了与安全相关的当前地缘政治趋势，包括政府越来越关注紧跟技术变革步伐以了解威胁、控制数据或访问数据所面临的各种挑战。本部分还提供了帮助防御者减少网络攻击者行动时间的建议。此外，还解释了危害表现 (IOC) 与威胁情报之间的重要区别。

主要研究结果

- 勒索软件目前在恶意软件市场中占据主体地位。虽然它不是一个新威胁，但它已逐渐发展成为有史以来最有利可图的恶意软件类型 — 而企业现在正在成为某些勒索软件操纵者的首选目标。2016年上半年，针对个人和企业用户的勒索软件攻击变得更加普遍和猛烈。新趋势：通过更快、更有效的传播方法，最大限度地扩大恶意软件活动的影响，提高攻击者创造巨额收入的概率。
- 漏洞攻击包是打造勒索软件这一突出威胁的罪魁祸首，还将继续利用 Adobe Flash 存在的漏洞。以普遍使用的 Nuclear 漏洞攻击包为例，思科研究人员最近开展的研究发现，Flash 占成功漏洞攻击的 80%。
- 企业应用软件 JBoss 的漏洞为攻击者提供了新的媒介，攻击者可利用该媒介来发起勒索软件等攻击活动。思科研究表明，与 JBoss 相关的入侵已导致服务器遭到严重损害，使其易受攻击。
- 从 2015 年 9 月到 2016 年 3 月，思科安全研究人员观察到与恶意活动相关的 HTTPS 流量增长了五倍。此类网络流量的增加很大程度上可归因于恶意广告注入器和广告软件。威胁实施者越来越多地使用 HTTPS 加密流量，以掩盖他们在网络上的活动，并增加他们的行动时间。
- 思科研究发现，即使主要软件供应商几乎在漏洞公布的同时就提供了补丁，但是仍然有很多用户没有及时下载和安装这些补丁。这些补丁的提供和实际实施之间的时间差为攻击者提供了充足的时间来发动攻击。
- 为了吸引人们注意由于组织没有适当维护老化的基础设施或修补易受攻击的操作系统而造成的安全风险，思科研究人员研究了一组思科设备样本，以确定在基本基础设施上运行的已知漏洞的存在时间。我们发现这些设备中有 23% 存在始于2011年的漏洞；近16%存在首次发布于2009年的漏洞。
- 少量、但是数量不断增长的恶意软件样本显示，恶意攻击实施者正在使用传输层安全（TLS，一种用于提供网络流量加密的协议）来隐藏他们的活动。这是导致安全专业人员担忧的一个原因，因为它使深度数据包检测这一安全工具失去效力。机器学习方法与创新数据视图的结合，提供了有关该趋势的更高质量的信息。
- 从 2015 年 12 月到 2016 年 4 月，思科将其中值 TTD 降低到大约 13 小时，远低于目前让人难以接受的行业估计值 100-200 天。在这段时期内观察到的 TTD 增减变化有助于凸显攻击者与防御者之间持续进行的白热化“军备竞赛”：攻击者不断发动猛烈的新威胁攻击，而安全供应商则必须快速识别。

简介

防御者对系统的保护无法匹敌攻击者的攻击。虽然防御者已经改进了对抗网络犯罪分子的策略和工具，但是攻击者仍然有太多不受限制的时间来采取行动。

问题就在于缺乏可视性，这使得用户对攻击毫无防备。安全专业人员依赖的是单点解决方案和“分类”方法，试图到处阻止攻击，而不是整体把握安全挑战，这更有助于攻击者发挥优势。

攻击者有充足的时间，可以识别并利用已经部署但是缺乏维护甚至长时间为人遗忘的基础设施、系统和设备中的漏洞。他们可以在网络中建立据点，然后逐步渗透。他们还可以发起基于服务器的攻击活动，这些活动能够为其提供更大的行动空间以开展攻击，并且实现更大的投资回报。

“如果防御者能够缩短修补漏洞和升级基础设施所需的时间，从而自主改进工具，攻击者就会浮出水面，防御者因而能够限制甚至杜绝攻击者的行动。”

尽管攻击者有时间优势，但他们的行动方式却有限。他们进去网络的方式不外乎那么几种。如果防御者能够缩短修补漏洞和升级基础设施所需的时间，从而改进手中的工具，攻击者就会浮出水面，防御者因而能够限制甚至杜绝攻击者的行动。防御者还可以全面了解安全格局：是否存在攻击者，他们如何获得进入权，以及哪些系统成功（或未能）识别出恶意活动。

遗憾的是，防御者似乎已经焦头烂额，无力履行为网络提供多层面保护的职责，这也是他们默认采取分类方法的原因。这种思维模式使得攻击者能够集中全部优势（充足的行动时间充足且防御者未能封锁最容易的攻击途径）来加强其攻击活动。正因如此，攻击者能够攻破防御并获利，从而成就了勒索软件这一“完美风暴”，而且勒索软件还在蓬勃发展，并且变得更加难以击败（请参阅“勒索软件：一个持久力毋容置疑的巨大收入来源”，**第 7 页**）。

网络犯罪趋势聚焦：勒索软件

网络犯罪趋势聚焦：勒索软件

勒索软件目前在恶意软件市场中占据主体地位。虽然它不是一个新威胁，但它已逐渐发展成为有史以来最具盈利能力的恶意软件类型。2016 年上半年，针对个人和企业用户的勒索软件攻击变得更加普遍和猛烈。

最近，针对多家企业（包括医疗保健行业的几个组织）进行的勒索软件攻击取得成功，这很可能会促使许多攻击者计划在未来实施类似的攻击活动。网络和服务器端漏洞使攻击者有机会悄无声息地实施可能影响整个行业的勒索软件攻击活动。

勒索软件：一个持久力毋容置疑的巨大收入来源

勒索软件存在多种变体，其中很多都是特定于语言的的，所有变体都有很好的恢复能力。这个领域的创新者，也就是众所周知的恶意软件品牌（如 CryptoLocker 和 CryptoWall）的创造者，在开始使用具有良好加密能力的文件加密后，使其恶意软件的效力达到全新的水平。目前，大多数已知的勒索软件都无法轻易被解密，受害者别无选择，在大多数情况下只能支付索价。

攻击者通常收取的是比特币。这种加密货币无意中又促进了勒索软件行业的繁荣，因为比特币地址用户可以匿名。安全研究人员的另一个难题是，几乎所有勒索软件交易都是通过 Tor（一个互联网匿名程序）进行的。比特币还可以分割为更小的单位，使攻击者能够将一个比特币分给整个团队，非常方便但又基本上无法追踪。

勒索软件的新媒介

电子邮件和恶意广告是勒索软件攻击活动的主要媒介。然而，有些威胁实施者现在开始利用网络和服务器端漏洞。

今年早些时候，一项似乎是以医疗保健行业为目标的大范围攻击活动采用了 Samas/Samsam/MSIL.B/C（“SamSam”）勒索软件变体，该变体是通过被入侵的服务器分发的。威胁实施者利用这些服务器在网络中逐步渗透，并入侵更多机器，然后进行勒索。

攻击者使用了 JexBoss（一个用于测试和攻击 JBoss 应用服务器的开源工具）在组织的网络中建立据点。一旦获得网络访问权，他们就继续使用 SamSam 勒索软件系列加密多个 Microsoft Windows 系统。

“我们预期下一波勒索软件将变得更加普遍而有弹性。组织和最终用户现在就应做好准备：备份关键数据并确认这些备份不会受到入侵。”

在许多方面，SamSam 攻击不可避免，因为许多组织运行的 JBoss 服务器都没有修补漏洞。（请参阅“JBoss：基础设施中的漏洞为攻击者提供行动时间”，**第 18 页**。）在 2016 年 4 月的一项调查中，思科发现至少 2100 台 JBoss 服务器已遭入侵，随时可能为恶意攻击实施者所利用。当时所有组织都收到通知，要求他们中断服务器的网络连接，并立即升级。

易受攻击的互联网基础设施是一个普遍问题，我们完全可以预料，会有更多的威胁实施者利用这个渠道，悄无声息地实施恶意软件活动，不仅针对企业，还有整个行业。（请参阅“老化的基础设施：勒索软件的增加使修补长期存在的漏洞成为势在必行的紧急任务”，**第 30 页**。）

另一个新问题：数据完整性

受到勒索软件攻击的用户和企业处境尴尬，不得不相信攻击者。虽然支付赎金似乎是最简单（也是唯一）的办法，但是，遭受勒索的用户需意识到，他们的文件可能无法解密甚至可能丢失。一些勒索软件的早期版本存在缺陷，即使支付了赎金，文件仍会丢失。

此外，还存在攻击者可能故意篡改他们控制的文件的风险。根据加密文件的类型（ 例如，医疗记录或工程设计），数据篡改或失窃的后果可能非常严重。

还有一个问题是重新感染的可能性，目前已经出现勒索软件对同一机器上的相同用户攻击两次的例子。有时候，第二次攻击的赎金金额有所减少，实质上类似于为用户提供优先客户折扣。攻击者也会反其道而行：如果用户在支付第一次索价时犹豫不决，攻击者第二次就会索要更高的赎金。

勒索软件已变得极为有效，并且非常有利可图。毫无疑问，将会有更多攻击者依靠它作为主要的快钱来源。当然，企业为攻击者提供了索要高额赎金的机会，其数额远高于攻击者预期个人最终用户愿意支付的数额。成为勒索软件攻击目标的组织或行业所遭受的潜在破坏和损失也显然要大很多。

我们预期下一波勒索软件将变得更加普遍而有弹性。（请参阅“勒索软件的演变：自我传播”，**第 9 页**。）组织和最终用户现在就应做好准备：备份关键数据，确认这些备份不会受到入侵。事实上，他们还必须确保在遭到攻击后，其备份数据能够快速恢复。对于企业，数据恢复可能是一项艰巨的工作；因此，主动出击，确定潜在的瓶颈至关重要。组织还应确认其互联网基础设施和系统中的已知漏洞已得到修补。

有关 SamSam 攻击活动和 JBoss 漏洞的详细信息，请参阅以下思科 Talos 博客文章：

“SamSam：医生会来看你的，不过是在他支付赎金之后”

“广泛存在的 JBoss 后门带来重大威胁隐患”

勒索软件的演变：自我传播

SamSam 攻击标示着攻击重点所发生的转变，即从攻击个人最终用户转向感染整个网络（请参阅**第 16 页**）。SamSam 的传播方法虽然简单，却很有效。考虑到 SamSam 的成功，攻击者还会推出更快、更有效的传播方法，以最大限度地扩大其影响并提高收到赎金的概率，这只是一个时间问题。

根据迄今为止观察到的趋势和进展，思科安全研究人员预计，自我传播勒索软件将是该领域创新者的下一步棋，因此敦促用户现在就采取措施做好应对准备。今年早些时候，攻击者利用 JBoss 后门发起针对医疗保健行业组织的勒索软件攻击活动，这是一个强烈的信号，说明攻击者一旦有充足的行动时间，就会寻找新的方法来侵害网络和用户，包括利用早该修补的旧漏洞。

自我传播型恶意软件并不是新事物，实际上，它已经以蠕虫和僵尸网络的形式存在了几十年的时间。这些威胁有很多，仍然普遍存在，并且不断得逞。自我传播恶意软件的特点包括：

- **利用广泛部署的产品中的漏洞。**过去大多数成功的蠕虫都使用互联网上部署的产品的漏洞。
- **复制到所有可用驱动器。**某些种类的恶意软件会枚举本地和远程驱动器（包括网络驱动器和 USB 驱动器），并将自身复制到这些驱动器中，以进行传播或驻留。这使得离线系统以及无法通过公共互联网访问的系统也会受到感染。
- **文件感染。**以文件为感染目标的恶意软件会将自身附加到文件前面或者后面。具体来说，恶意软件会附加在未受 Windows SFC 或 SFP（系统文件检查器或系统文件保护器）保护的可执行文件上。有些蠕虫病毒还可以自行粘附到非可执行文件上，并且通过其进行传播。
- **有限暴力破解攻击活动。**过去很少有蠕虫尝试过此方法。
- **弹性指挥和控制。**有些蠕虫会考虑通常用于中断指挥和控制基础设施的操作，并实施预防措施来规避这些中断。许多蠕虫没有指挥和控制基础设施。它们所使用的只是一个简单的默认操作，以便尽快地进行传播。
- **使用其他后门。**一些恶意软件制作者意识到其他的感染可能已经在系统上留下了后门，可以直接利用这些后门来传播自己的恶意软件。

“根据迄今为止观察到的趋势和进展，思科安全研究人员预计，自我传播勒索软件将是此领域的创新者要采取的下一步，因此敦促用户现在就采取措施做好应对准备。”

巨额赎金框架

我们对勒索软件创新者技术的观察表明，开发下一代勒索软件的攻击者很可能倾向于使用采用模块化设计的软件，在很多流行的开源渗透测试套件中都能找到这种架构。采用此种方法，他们可以根据需要使用某些功能。模块化设计提高了效率，并使威胁实施者能够在某个方法被发现或者无效的情况下改变策略。

我们猜测，下一代勒索软件框架（我们将其称作巨额赎金框架）将包含如下核心功能：

- 对用户文件的标准位置进行加密，以及提供自定义的目录和文件类型，允许按目标进行自定义
- 标记哪些系统和文件已加密
- 提供使用比特币付款的指示
- 允许攻击者设定赎金的数额，并指定双重期限：一个是提高支付金额的期限；另一个是删除加密数据的密钥的期限

该框架还将支持不同的模块，这使得攻击者可以根据不同的环境定制恶意软件，并且在能够使用漏洞时，改变方法从而更大肆地进行传播。此类模块的示例包括：

AUTORUN.INF/USB 大容量存储传播

本模块将搜索受感染的系统，以查找本地和远程的映射驱动器。然后它将自我复制到这些驱动器的特定位置，并对文件属性进行设置，从而使人们更难以发现和删除这些复制文件。随后，它会将“autorun.inf”文件写入这些驱动器中，从而使之后与该驱动器连接的所有计算机都运行这些感染程序。

身份验证基础设施漏洞攻击

本模块将利用作为很多公司网络组件的常见身份验证基础设施中已知的漏洞进行攻击。然后，可以利用凭证访问其他系统，有时甚至以管理员的身份进行访问。

指挥和控制以及报告感染

为了降低被发现的风险，下一代勒索软件可以通过配置使其丧失指挥和控制的功能。本模块将向指挥和控制域传送一个附有 GUID（全局唯一标识符）的标志，以尝试通过通用协议和服务（如 HTTP、HTTPS 或 DNS）访问该域，从而能够传送该数据。然后，该域可以收集这些 GUID，以统计出目标网络里受感染和加密的系统的数量。攻击者可以使用此类信息确定其攻击活动的效力。

速度限制器

本模块可以确保勒索软件“友善”地对待系统资源，从而使用户不太可能发现有勒索软件正在运行。它将限制 CPU 的使用率，并减缓网络的使用率，以确保尽可能微妙地执行操作。

RFC 1918 目标地址限制器

如果主机有一个 RFC 1918 地址，所设计的植入程序将只攻击和植入目标主机；这些地址被内部网络使用。

通过周密构建的架构和谨慎的密码管理，可以使未来的自我传播勒索软件的逐步渗透变得更加困难有关应对下一代勒索软件挑战的防御措施的更多信息，请参阅“安全建议”（**第 52 页**）。

有关勒索软件演变以及企业可以对此领域的下一代威胁做些什么准备的详细信息，请参阅思科 Talos 博客文章：

“勒索软件：过去、现在和未来”

漏洞

漏洞为恶意攻击实施者提供行动时间，而他们利用这个优势在防御者修补漏洞之前发起攻击活动。通过漏洞攻击包、勒索软件甚至社交引擎垃圾邮件，攻击者依靠未修补的系统和过时的设备实现其目标。

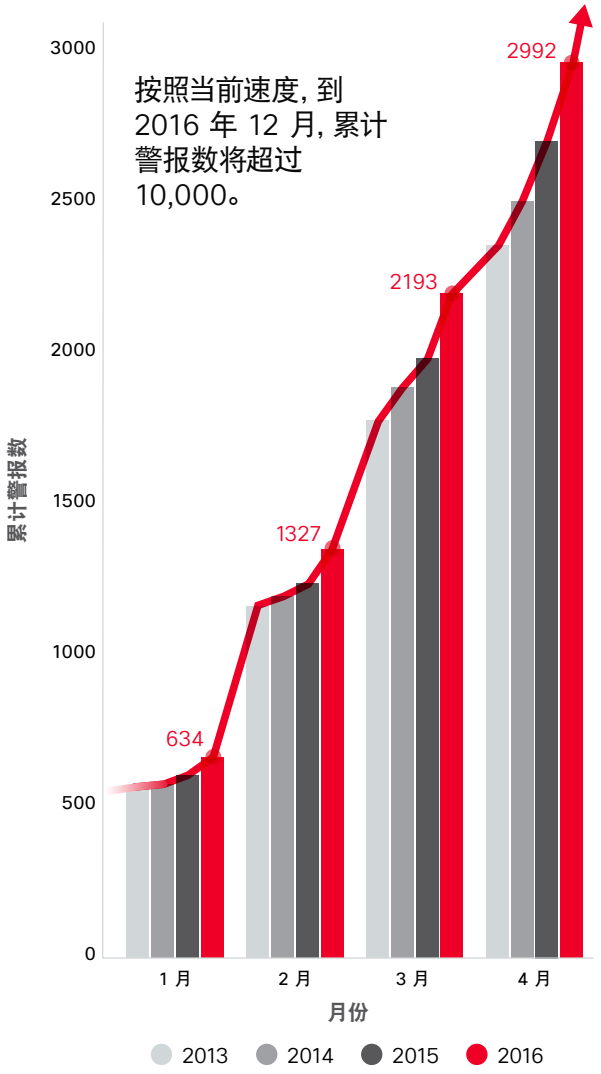
漏洞既是攻击者攻击的入口，也是防御者保护其组织的突破口。如果防御者能够修补漏洞，不让攻击者有机可乘，则可以降低这种威胁。如果防御者对漏洞听之任之，不予修补，攻击者就会将其作为发起攻击活动的垫脚石。

得益于安全开发生命周期 (SDL) 实践，供应商现在更加关注漏洞的识别和披露。但是，如**第 15 页**所述，攻击者也密切关注补丁，对其进行反向工程，以确定进行了哪些修补，并根据了解的内容开发新的攻击方法。

2016 年前四个月的年度累计警报数与去年同期总数相比，略有增加，这很有可能归功于 Microsoft 和 Apple 等供应商的重大软件更新；代码审核的增加；代码审查工具的改进；以及上述 SDL 实践（图 1）。所有这些趋势都有助于产品漏洞识别的增加。

防御者对其流程进行改进和创新，以消除漏洞披露与修补之间的时间差，但是，攻击者也在利用其技能再次拉开这些时间差，发动数量更加庞大、更加复杂且能够削弱防御者响应能力的的攻击。防御者必须识别并杜绝攻击者的行动。应对已披露的漏洞并实施稳健的修补管理制度，是实现该目标的核心所在。

图 1. 年度累计警报总数



来源：思科安全研究部门

分享

“防御者对其流程进行改进和创新，以消除漏洞披露与修补之间的时间差，但是，攻击者也在利用其技能再次拉开这些时间差，发动数量更加庞大、更加复杂且能够削弱防御者响应能力的的攻击。”

对安全连接的安全错觉

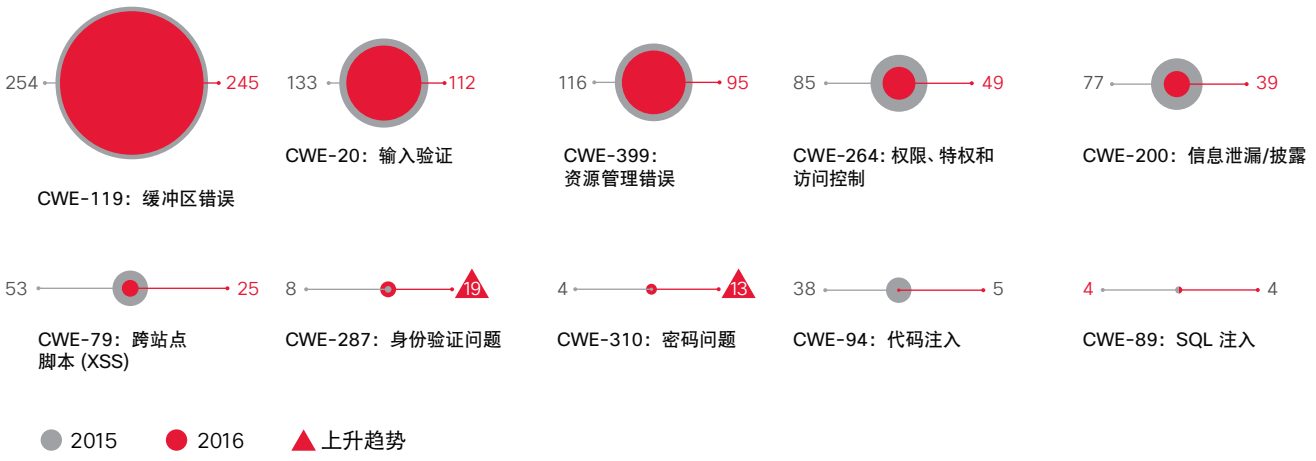
安全连接，例如 HTTPS 连接和 SSL 证书创建的连接，应该能让用户对自己的在线活动有安全感。但是，最近涉及加密和授权的漏洞警报的增加不禁让人担忧，攻击者要破坏安全连接将会更加容易。结果：连接的安全性存疑。

如以下常见缺陷列表 (CWE)（图 2）所示，身份验证问题和加密问题自 2014 年和 2015 年以来呈上升趋势。仅仅从 2015 年 12 月至 2016 年 3 月，就识别了 19 个身份验证问题和 13 个加密问题，接近上一年的总数。

加密的使用增多是一个积极的发展势头，因为它有助于保护信息安全，防止信息遭窥探。但是，加密也存在固有风险：加密会导致更多复杂问题，而且加密需要多种工具，用户会期望加密能保障隐私而事实却并非如此，这些都会带来新的漏洞。如果加密操作不当，则将无法提供保护。

建立安全连接需要复杂的流程和工具链。除了证书，该链可能不可靠。在连接的中间有各种设备，例如 VPN 网关，这不一定是安全的。此外，表示安全连接的网站可能已受到入侵。最重要的是，对于带有“锁定”图标的 URL（不注意的话会认为这是安全活动的指示），也不能认为其是安全或受到安全保护的。

图 2. 身份验证和加密问题的增多，12 月 - 3 月



来源：思科安全研究部门

行动时间

行动时间

勒索软件攻击活动在增多，最近的攻击活动的范围在扩大，这些都表明攻击者因行动时间不受限制而获益良多。这使得他们能够悄无声息地为攻击活动奠定基础，在准备就绪后发动攻击，并最终成功获得收入。

为了隐藏其活动，他们会使用加密货币、ToR、HTTPS 加密流量和传输层安全 (TLS)。同时，通过快速行动，对补丁进行反向工程，并利用难以管理的漏洞披露，漏洞攻击包制作者进一步获得成功。除此之外，恶意广告新手法为网络攻击者提供了一种高效且难以跟踪的方法来增加遭入侵站点的流量，这样一来，他们就可以感染用户的计算机，最终发动勒索软件攻击。

攻击媒介：客户端

长期以来，攻击者更喜欢客户端，因为它有更高的用户参与度，而用户一直是一个薄弱环节。此外，客户端为攻击者提供了多种方法来获取行动空间。选择的范围非常广。

但是，使用 PDF 等媒介的攻击数量经过几年的增长，似乎已趋于稳定。与此同时，有迹象表明，攻击者正在服务器端寻找新的机会。在服务器端，他们可以逐步渗透网络并积累更多优势。

PDF 和 JAVA 攻击呈下降趋势

PDF 和 Java 作为攻击媒介的流行程度继续下降。在 2016 年 1 月，Oracle 宣布将终结其 Java 浏览器插件，因为浏览器供应商正在实施计划停止对这些插件的支持。[1] Oracle 转而专注于其无插件 Java Web Start 技术。

Java 浏览器插件的终结意味着使用其作为攻击媒介的做法还将减少，但安全研究人员会密切观察攻击者是否会改进旧的威胁来利用 Java 的新化身。安全专业人员和企业应考虑阻止 Java（需要 Java 的站点除外）。

[1] “转向无插件 Web。”Java 平台小组，2016 年 1 月：**https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free**。

虽然 PDF 漏洞利用也在下降，它们仍然存在于电子邮件中 – 例如，说服电子邮件收件人点击已被损坏的附件。垃圾邮件制作者会使用这种策略搭配显示时事新闻或大型赛事的主题行（请参阅**第 19 页**关于垃圾邮件的更多信息）。

漏洞攻击包开发人员仍在利用 Flash，但是除此之外的在线 Flash 内容正在缓慢而稳步地减少。然而，许多在线应用，例如使用富媒体内容或交互式广告的应用，仍然高度依赖 Flash 来正常工作。

替代应用，例如 HTML5 正在被缓慢地接受，但是过渡是逐步的过程，因此仍然要依赖 Flash。只要 Flash 存在，它就仍然会被用作攻击媒介。

主要的漏洞攻击包继续利用 FLASH

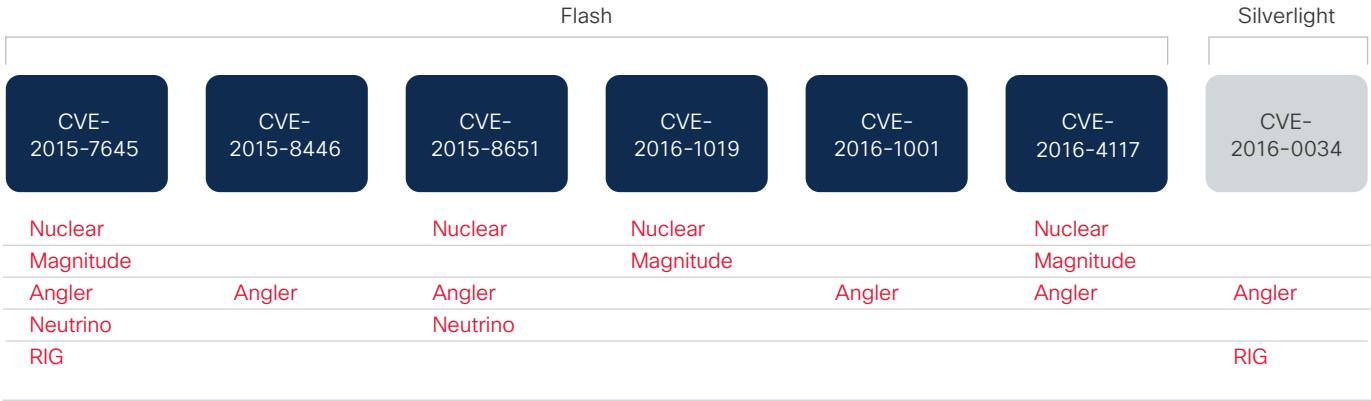
漏洞攻击包是打造勒索软件这一突出威胁的罪魁祸首，还将继续利用 Adobe Flash 漏洞。以普遍使用的 Nuclear 漏洞攻击包为例，思科研究人员最近开展的研究发现，Flash 占成功漏洞攻击的 80%。[2]

面对频出的漏洞，Adobe 不断发布补丁；但是攻击者的动作同样迅速。一旦 Adobe 发布 Flash 更新以修补漏洞，漏洞攻击包制作者就开始对补丁进行反向工程，以了解修补了哪些漏洞。在一周内，漏洞攻击包制作者就能够识别 Flash 漏洞，并利用这些漏洞制造武器用于实施远程代码。

我们建议用户和管理员禁用或删除不必要的浏览器插件，以降低遭受威胁的风险，或者至少在更新发布之后立即升级 Flash。

为了帮助强调安装补丁的积极影响，图 3 显示了利用最近的 Flash 和 Microsoft Silverlight 漏洞的各种漏洞攻击包。通过安装所有这些漏洞的可用补丁，用户可以显著削弱漏洞攻击包提供的勒索软件的影响。

图 3. 漏洞攻击包利用的漏洞



来源：思科安全研究部门

分享

[2] “威胁聚焦：漏洞攻击包跨国攻击 150 多个国家/地区。”思科 Talos 博客，2016 年 4 月 20 日：**http://blog.talosintel.com/2016/04/nuclear-exposed.html**。

漏洞攻击包使用 Tor 隐藏通信

漏洞攻击包制作者一直在寻找规避安全防御的方法，并且在这一方面极富创造力。我们最近观察到的一个例子涉及到 Nuclear 漏洞攻击包。一般情况下，该攻击包投放的是勒索软件变体，但我们却观察到其提供 Tor（一个用于匿名通信的软件）变体。这种策略似乎是一种使最终恶意负载匿名的方法，从而使防御者难以跟踪该活动。

通常，当漏洞攻击包投放某个恶意文件时，可通过监控产生的指挥和控制流量（也就是当恶意软件“联系总部”时），检测该恶意文件。但是，在思科观察到的 Nuclear 漏洞攻击包负载投放的示例中，首先投放的是一个 Tor 可执行文件，然后再通过 Tor 发出通信请求。由于 Tor 是一个“结束时退出”加密路由协议，安全专业人员看不到恶意软件对该协议做了什么。

通过漏洞攻击包传送的勒索软件已成为其制作者的绝佳摇钱树。（请参阅“勒索软件：一个持久力毋容置疑的巨大收入来源”，**第 7 页**。）因此，勒索软件开发者寻求新的方法来增强其恶意软件的有效性，并与其他漏洞攻击包竞争，是很合乎逻辑的。对 Nuclear 漏洞攻击包利用 Tor 的观察还发现了恶意软件开发者做出的另一个巧妙的改进。

有关 Nuclear 漏洞攻击包利用 Tor 的更多信息，请阅读此思科 **Talos 博客文章**。

攻击者发现基于服务器的攻击活动的价值

攻击者发动攻击活动是为了获得高价值，换言之，是为了高额回报。向客户端或最终用户输送恶意软件或漏洞攻击包行之有效，但是也会削弱攻击的影响：在客户端攻击期间，恶意攻击实施者能够积累的带宽和能力都受到限制。

但是，现在攻击者发现，发动利用服务器端的攻击活动，他们能够获得更多回报。JBoss 是一个企业应用平台，最近被用于获取网络访问权，以散播 SamSam（一个勒索软件变体）（请参阅**第 7 页**）。在思科研究人员观察的案例中，攻击者使用了 JexBoss（一个用于测试和利用 JBoss 应用服务器漏洞的开源工具）在医疗保健组织的网络中建立据点。一旦攻击者进入网络，他们就能够使用 SamSam 来加密 Windows 文件。

利用服务器中的漏洞传播勒索软件的做法，为这种本已十分猖獗的威胁打开了新的维度。思科研究人员对互联网上的机器进行了扫描，发现有机器已被入侵，随时可能收到勒索软件负载。此外，思科还发现有 2000 个后门已被安装在 1600 个 IP 地址中。这些后门有许多存在于使用学校通用图书馆管理系统的系统中。思科联系了相关软件开发商，他们迅速行动，发布了必要的补丁。

通过利用服务器端的漏洞，攻击者获得了更为宽广的舞台，而且要遏制他们的攻击活动所造成的损失，要费时费力得多。客户端应用（例如 Web 浏览器）越来越多地通过自动更新进行修补，因而不那么容易受到攻击。

而另一方面，服务器端应用却长期过时，这是因为修补和升级都有赖于 IT 人员通常非常有限的工作时间，而且升级这些系统难免会影响运营。此外，网络周界存在较多漏洞，这使得攻击者能够访问以前依赖周界提供防御的服务器。

如图 4 所示，许多主要基础设施供应商的产品在客户端和服务器应用上都存在漏洞。

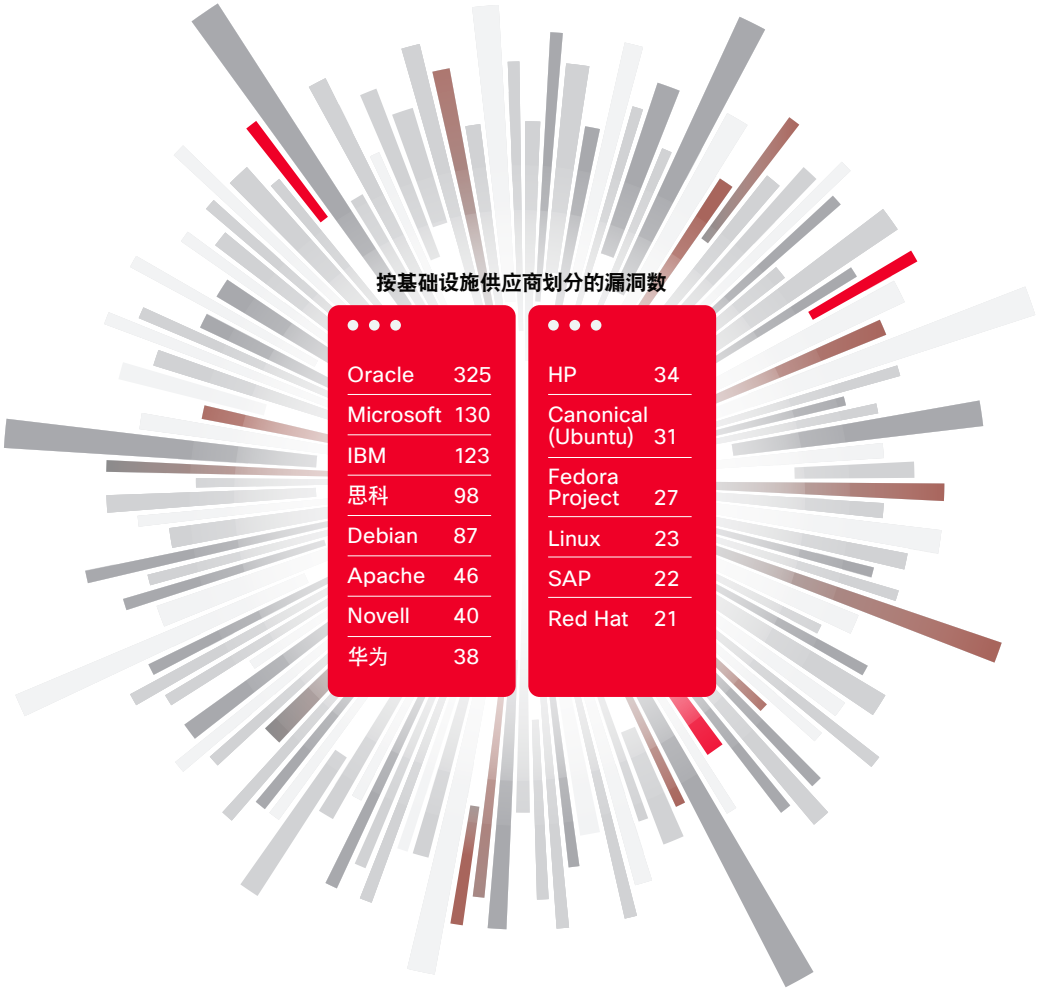
要了解有关服务器解决方案中漏洞的危险性的更多信息，请阅读思科 Talos 博客文章：

“广泛存在的 JBoss 后门带来重大威胁隐患”

“SamSam：医生会来看你的，不过是在他支付赎金之后”

分享

图 4. 按基础设施供应商划分的漏洞数，2016 年 1 月 1 日–3 月 30 日



来源：思科安全研究部门

JBOSS：基础设施中的漏洞为攻击者提供行动时间

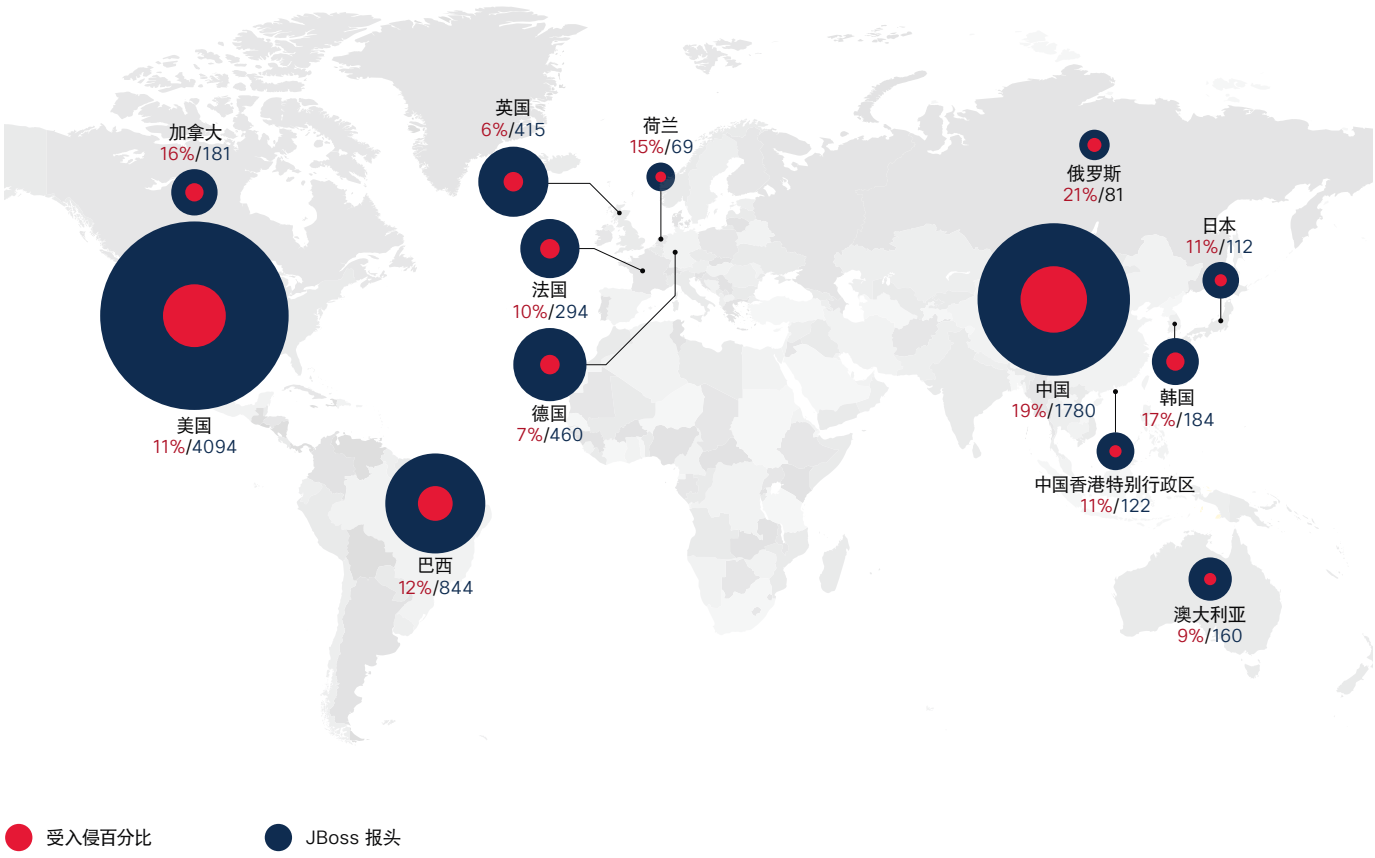
勒索软件制作者在通过企业应用软件 JBoss 发动的攻击活动中占了上风。从最近涉及医疗保健组织的勒索软件攻击活动（**第 7 页**）中可以看出，JBoss 中的漏洞使得恶意攻击实施者能够进入网络，并且有时间收集数据或发动启动恶意软件。利用 JBoss 实施的入侵提供了更多证据，证明网络维护不良会为犯罪分子提供这些网络的访问权，而这些访问是可以阻止的。

思科研究人员发现，与 JBoss 相关的漏洞已导致服务器遭到严重损害，使其易受攻击。对互联网进行扫描时：

- 我们寻找在 HTTP 报头或页面内容中报告 JBoss 安装的服务器。
- 然后我们搜索了主机上是否存在众多不同的后门、Web 外壳或其他 .jsp 入侵。

图 5 显示了疑似已遭入侵的服务器的百分比与显示存在 JBoss 安装的服务器的数量之比较。例如在美国，观察到的 Web 外壳有 11% 显示出遭入侵迹象。

图 5. Web 外壳的存在表示遭受 JBoss 入侵



来源：思科安全研究部门

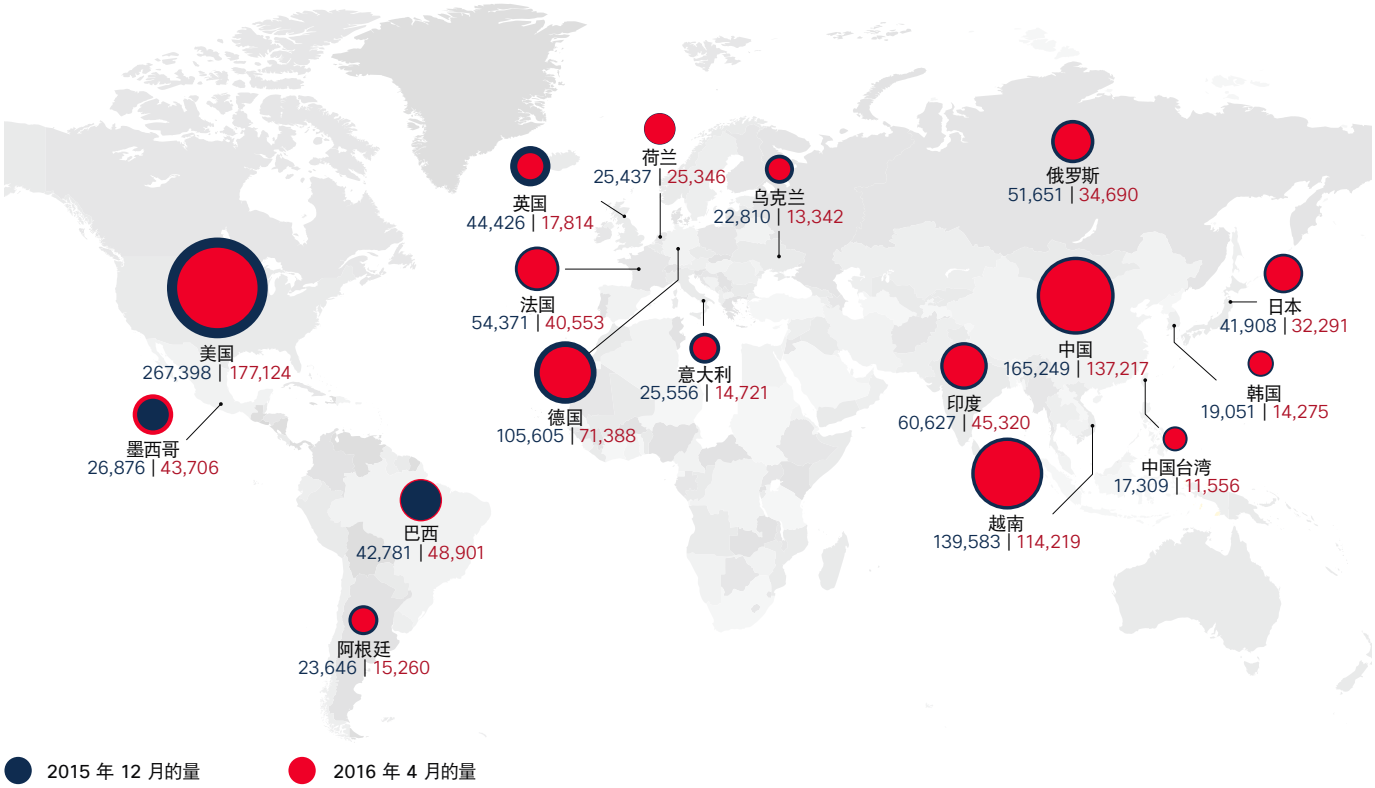
全球垃圾邮件数量保持相对稳定

为了测算全球的垃圾邮件流量，思科从其电子邮件设备收集样本，以反映编写在电子邮件设备和网关中的策略决策（例如被阻止或标记为未知的电子邮件）的影响。垃圾邮件经常被用作攻击媒介，尤其是被勒索软件所利用。

根据思科对邮件流量的研究，从 2015 年 12 月至 2016 年 5 月，垃圾邮件数量保持平稳（图 6）。来自巴西的垃圾邮件流量在 2016 年 1 月和 3 月表现出垃圾邮件峰值。这些增加可能是由当时的垃圾邮件僵尸网络活动所致。

正如关于地区网络阻止活动部分所述（请参阅**第 47 页**），攻击者经常变换其开展活动的国家和主机提供商，因为他们希望找到适合发起攻击活动的环境。垃圾邮件发送者利用在可信赖的主机中拥有和配置的僵尸网络机器。他们会利用这些机器，直到被检测系统发现，再转移到另一个僵尸网络。

图 6. 各国家/地区的垃圾邮件数量，2015 年 12 月 – 2016 年 5 月



来源：思科安全研究部门

分享

图 7. 垃圾邮件中广泛使用的社会工程主题

版本数量	URL	消息摘要	语言	上次公布日期 (GMT)
95	RuleID4626	发票, 付款	德语、英语	3.18.16
82	RuleID4400KVR	采购订单	英语	2.1.16
64	RuleID4626 (续)	发票, 付款, 发货确认	英语、德语、西班牙语	1.28.16
62	RuleID4961KVR	付款, 转账, 订单, 发货	英语	3.25.16
58	RuleID4961KVR	报价请求, 产品订单	英语、德语、多种语言	1.25.16
52	RuleID5118KVR	产品订单, 付款	德语、英语	3.17.16
49	RuleID858KVR	货运报价, 付款	英语	3.14.16
47	RuleID4961	转账, 发货, 发票	英语、德语、西班牙语	2.22.16
44	RuleID4627 和 RuleID4627KVR	航空旅行电子机票	英语	3.29.16
30	RuleID8337KVR	订单, 付款, 报价	英语	1.21.16

来源: 思科安全研究部门

垃圾邮件制作者会继续通过聪明的社会工程说服用户点击邮件中的附件（例如携带恶意软件的 PDF — 参阅**第 15 页**）或链接。如图 7 所示，垃圾邮件制作者会创建声称包含关于账单和发票、差旅安排或业务报价的重要信息的附件或链接。垃圾邮件发送者还会以其他语言来制作其他版本的邮件，以诱骗更多受害者。

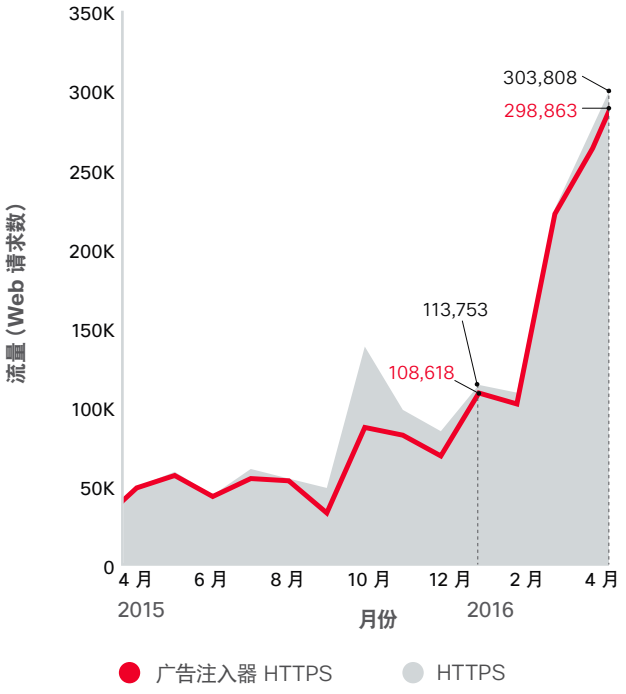
回归黑名单？攻击者对 HTTPS 的采用使防御者的调查复杂化

当广告注入器通过 HTTPS 加密的流量传播恶意广告时，用户和安全团队无法依靠通过 URL 发送的信息识别潜在威胁。攻击者很清楚这一点，所以他们使用的 HTTPS 加密流量迅猛增长，以此来掩盖他们在网络上的活动，并增加他们的行动时间。

从 2015 年 9 月到 2016 年 3 月，思科安全研究人员观察到与恶意活动相关的 HTTPS 流量增长了五倍。为了确定这种利用 HTTPS 的趋势，我们对八种威胁类别的 80 个恶意攻击活动进行了超过 16 个月的跟踪。根据我们的研究，HTTPS 流量的增加主要归因于广告注入器和广告软件（图 8）。

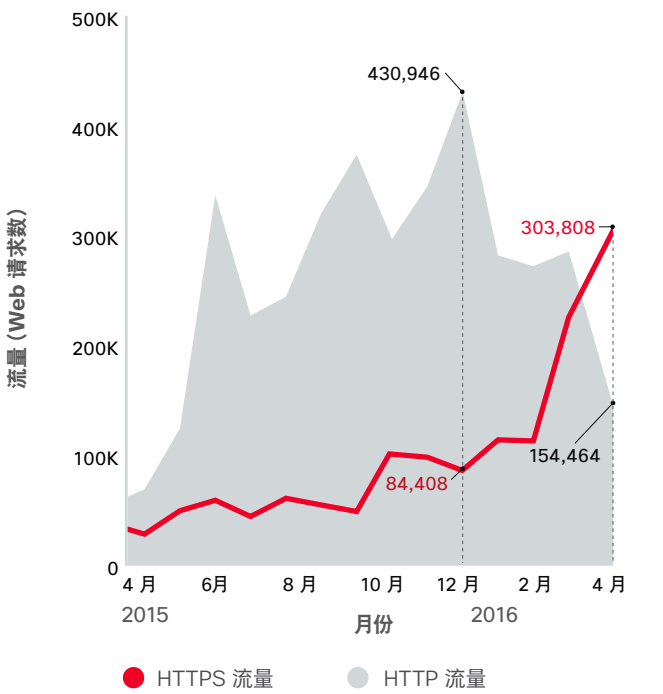
我们还发现，从 2015 年 12 月至 2016 年 4 月，与广告注入器相关的 HTTPS 流量增长了 300%（图 9）。

图 8. 广告注入器是导致 HTTPS 增加的主要源头



来源：思科安全研究部门

图 9. 广告注入器的 HTTPS 流量在 4 个月内增长了 300%



来源：思科安全研究部门

恶意广告注入器是广告软件感染的主要组成部分（图 10）。网络犯罪分子利用这些浏览器扩展将恶意广告注入到网页中，使用户接触展示广告和弹出窗口，而这些广告和弹出窗口能够促进勒索软件和其他恶意软件活动。恶意广告和恶意广告注入器占据了广告生态系统的一部分，在这个系统中，合法行为和恶意活动难以区分。

广告注入器和广告软件感染不容忽视。今年，思科安全研究人员发现了通过广告软件传送的新版本 DNSChanger 特洛伊木马。这一情况表明，广告注入器和广告软件感染会给用户和公司带来更大的危险。[3]

我们还发现攻击者的恶意软件向 HTTPS 转变的迹象。这个转变的速度低于我们观察到的广告注入器的转变速度。这很可能是因为攻击者始终以收入最大化为目标，因而只有在必要时才变更基础设施。

讽刺的是，网络犯罪分子推迟对这些基础设施的更新与合法商界的趋势不谋而合。这个趋势就是，许多组织都推迟修补其互联网基础设施中的已知漏洞（通常长达数年），因为担心为了进行升级而断开设备和软件的网络连接会影响收入。（请参阅“老化的基础设施：勒索软件的增加使修补长期存在的漏洞成为势在必行的紧急任务”，**第 30 页**）。修补大量受感染主机的挑战毫无疑问也会鼓励攻击者保持其旧技术的有效使用。

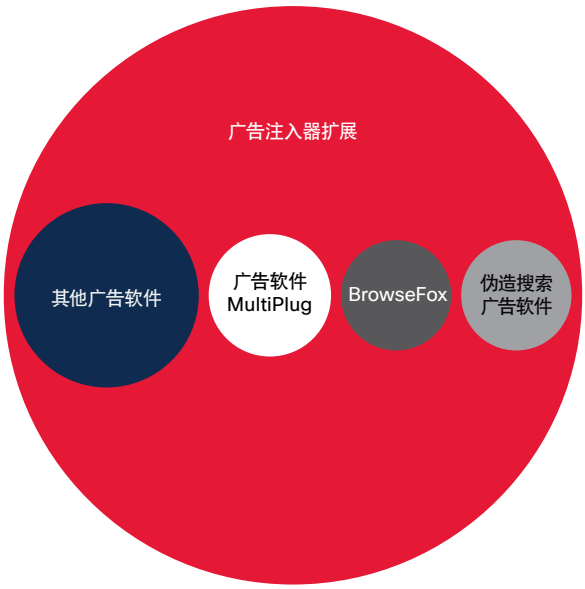
我们进行了为期 16 个月的分析，发现以下恶意软件系列增加了 HTTPS 的使用：

- Gamarue/Andromeda，多用途僵尸网络
- Necurs，信息窃取僵尸网络
- Miuref/Boaxxe，点击欺诈僵尸网络
- Ramdo/Redyms，点击欺诈僵尸网络
- 数据外泄特洛伊木马

与恶意活动相关的 HTTPS 加密流量的增长令人烦忧，因为它为跟踪和调查恶意软件活动的安全研究人员带来了巨大挑战。防御者用于识别 HTTP 流量中的威胁的技术，例如基于 URL 模式的基于签名的 IDS 检测，在不添加 SSL 检查功能的情况下无法应用于 HTTPS 流量。在许多情况下，安全研究人员从单个域名或 IP 地址着手调查。

威胁分类也变得困难，因为威胁通常常共享基础设施。我们建议防御者采用的退守策略是使用黑名单（所有已知恶意软件的列表），但是这种方法容易出错，并且不够精细，难以达到效果。这种策略也需要花费大量时间，因为分析人员需要对威胁进行手动研究和分类。

图 10. 广告注入器：在广告软件感染中观察到的主要组件



来源：思科安全研究部门

[3] “与广告软件在网设备相关的 DNSChanger 爆发。”思科安全博客，2016 年 2 月：**http://blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base**。

恶意广告即服务：高效感染是问题的实质

广告代理有意或无意地成为网络上恶意广告的传播渠道，实质上支持了攻击者的新业务模式：“恶意广告即服务”。威胁实施者在热门合法网站上购买广告空间，作为提供恶意广告的一个途径。这为防御者带来新挑战，并且产生了谁应该负责保护用户免受恶意广告困扰的问题。

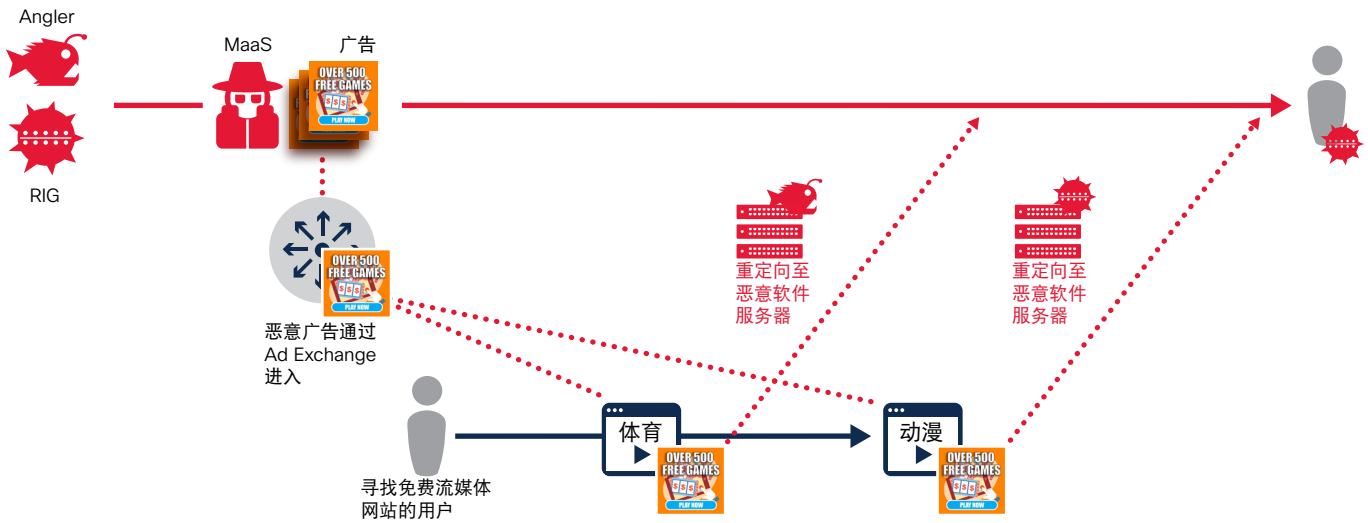
通过购买合法的广告空间，攻击者可以轻松地在不相关站点上散播威胁。由于广告仅短时间弹出，防御者很少有或根本没有时间识别威胁的存在。此外，因为广告代理使用浏览器类型和版本等信息来确定目标用户，攻击者可以更容易地对精细层面（包括语言）上的特定用户群发起漏洞攻击。

恶意广告即服务的趋势类似于域名抢注。域名抢注者通过出售或使用用户可能会联想到合法企业和知名品牌的域名获利。通过引导这些域的流量，他们在输送威胁中没有直接发挥作用，但是却促进了恶意软件的散播。

启动广告拦截器是避免遭受恶意广告（特别是我们已经发现的不需要用户交互就能够感染机器和传输负载的新型恶意广告）的一个明智的策略。但是，一些领先的在线内容提供商（其收入严重依赖于数字化广告）要求用户禁用广告拦截器以查看网站上的其他内容。这显然为用户带来风险，并且使安全团队陷入困境。安全团队现在必须考虑是否阻止提供来自广告交易平台的广告的站点。

分享

图 11. 恶意广告即服务 (MaaS) 如何运作



来源：思科安全研究部门

多层重定向

思科研究人员发现威胁实施者通过购买广告空间来传送恶意广告。这些恶意广告要么直接感染用户计算机，要么将用户重定向到传播恶意软件负载的其他位置。在许多情况下，存在多层重定向。在有些情况下，用户甚至不需要与恶意广告交互，其计算机都会被感染；一切都发生在后台，远离屏幕。

在 2015 年 10 月首次出现的恶意广告即服务的攻击活动中，用户被重定向到传播不同负载的多个不同漏洞攻击包，包括 Angler 和 RIG。这些负载有许多是 TeslaCrypt 和 CryptoWall 等勒索软件的变体。用户被一个模仿赌博网站的恶意广告欺骗。在广告背后的代码中隐藏了指向 JavaScript 的链接。该链接把用户带到 Angler 登陆页面，但是还有其他的重定向，包括 iFrames。

这种传播恶意广告的新方法的出现再一次表明，影子经济产业化的程度越来越高。思科研究人员预计，随着越来越多的网络犯罪分子寻求高效方法，通过合法站点感染大量网络用户并躲避检测，恶意广告即服务这一趋势将不断增强。在帮助攻击者开展勒索软件攻击活动中，恶意广告发挥着核心作用，而勒索软件攻击活动正在快速成为攻击者的首选攻击方法，因为它们可能会带来高额利润。（请参阅“勒索软件：一个持久力毋容置疑的巨大收入来源”，**第 7 页**。）

有关恶意广告即服务发展趋势的详细信息，请参阅思科 Talos 博客文章：

“威胁聚焦：隐藏在博彩广告背后的恶意软件”

“思科研究人员预计，随着越来越多的网络犯罪分子寻求高效方法，通过合法站点感染大量网络用户并躲避检测，恶意广告即服务这一趋势将不断增强。”

网络攻击方法：设置勒索软件以取得成功

2016年上半年网络攻击方法的一些发展趋势与恶意软件的爆炸性增长相关。以居于图 12 中列表之首的可疑 Windows 二进制文件为例，网络攻击者利用这些文件来传播间谍软件和广告软件等威胁。这些工具使他们能够在网络基础设施中建立据点，从而能够发起勒索软件等攻击。

Facebook 诈骗（社会工程）、特洛伊木马和 iFrames 仍然是获取用户计算机和组织网络初始访问权的常用工具。

正如我们的上一次网络安全报告中所述，Facebook 诈骗是我们在 2015 年下半年观察到的首要网络攻击方法。Windows 二进制文件位居该列表的第四位。JavaScript 恶意软件在我们之前的前 10 位攻击方法中占据三位，目前却甚至排不到前 10 位。

但是，JavaScript 恶意软件绝不会消失。事实上，这种恶意软件是促成今年许多勒索软件攻击活动的关键组件。

图 13 中的列表是不太常见但是可能位于感染链更深层次的恶意软件的集合。

图 13 所示图谱的长尾巴显示了一个存在勒索软件签名、特洛伊木马和植入程序的示例。随着攻击者越来越多地使用勒索软件，我们看到勒索软件的基础设施组件的频率高于信息窃取恶意软件。

图 12. 观察到最常用的恶意软件

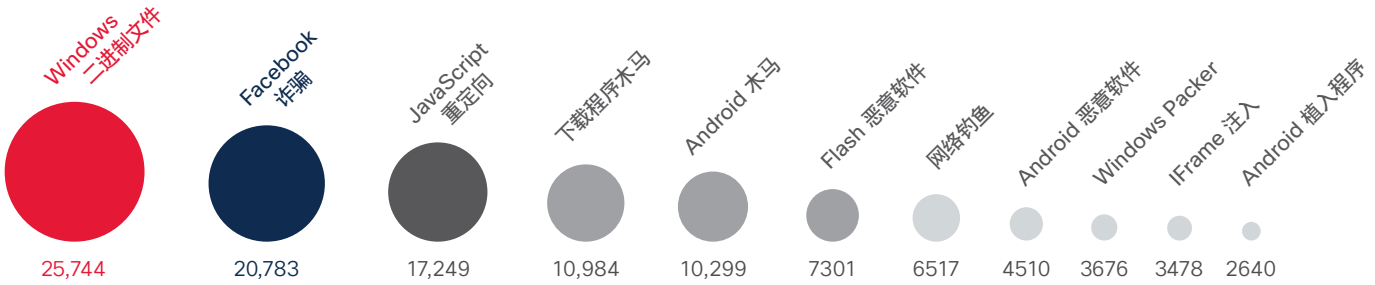
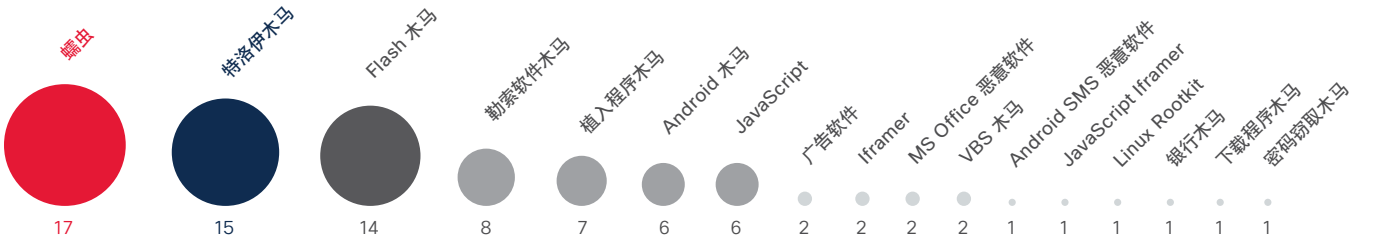


图 13. 观察到的少量使用恶意软件的示例



来源：思科安全研究部门

保护时间

保护时间

虽然防御者一直在创新，数字经济依赖的基础设施仍然很脆弱，并且依赖于不充分的安全做法。如今，由于大多数组织中网络浏览器、应用和基础设施的混杂，攻击者有大量的入口通道。

这些欠缺防护的设备和软件向攻击者开放了行动空间，安全专业人员必须关闭这些空间。减少攻击者不受限制的行动空间，并且使攻击者的行踪暴露，是安全人员的首要任务。

修补时间：补丁和升级的提供与实施之间的时间滞后造成安全漏洞

近年来，主要供应商变得越来越主动，在漏洞和攻击活动披露之后提供补丁所需的时间越来越短，并且更加积极地与发现这些漏洞的安全研究人员协作。事实上，根据思科对数以千计的通用漏洞披露 (CVE) 进行的研究，主要终端软件供应商从公开披露漏洞到提供补丁之间的时间中值为零天。换句话说，通常在公开披露漏洞的同时，就提供了补丁，所以供应商在实行协调的披露做法。

然而，根据思科的研究，尽管补丁的提供迅速，但是仍然有很多用户没有及时下载和安装这些补丁。这些补丁的提供和实际实施之间的时间差为攻击者提供了发动攻击的机会 — 也就是提供了在一个本来可以利用简单的软件补丁阻止其进入的网络中实施行动的时间。恶意攻击实施者甚至能够在漏洞被公开披露之前就开始利用漏洞。因此，关闭补丁的提供与安装之间的窗口对于防御至关重要。

为了帮助关闭该窗口，供应商对其产品采用了各种形式的自动更新功能。这些功能包括定期检查并提供用户通知，以及选择加入和选择退出日益难以禁用的后台更新。

根据自动更新策略，用户可以选择延迟更新，直到后续方便的时间再进行更新，有时候还可以干脆跳过更新。通过研究思科客户使用的终端上浏览器软件的安装情况，我们可以看到自动更新的价值。我们对实施了强大的选择退出策略的 Google Chrome 浏览器的安装情况进行研究发现，大多数用户（随着自动更新策略力度的加强，用户群的 60% 到 85%）运行的是该软件的最新版本，这足以证明自动更新的价值。

在最坏的情况下，也有 75% 到 80% 的用户使用最新版本或次新版本的浏览器（图 14）。Google 使运行其旧版本浏览器变得越来越难：需要管理员访问权才能关闭自动更新，并且不允许从其自己的网站或其他网站下载旧版本的浏览器。

自动更新策略对于用户运行什么版本有重大影响，而不仅仅影响自动更新的存在。思科调查的所有软件都具有某种类型的自动更新机制，从用户通知弹出窗口到无提示的自动操作，不一而足，除非用户费尽心思主动禁用该过程。策略越严格，期望的行为越容易变为现实。

图 14. 按版本划分的 Chrome 安装（前 50% 的用户）

注：本部分中的修补时间图表显示对排名前 50% 的人群进行研究得出的结果。通过突出该人群的简单多数，可以更容易地发现更新是否发挥预期作用，或者是否还存在其他阻碍客户群保护的普遍屏障。

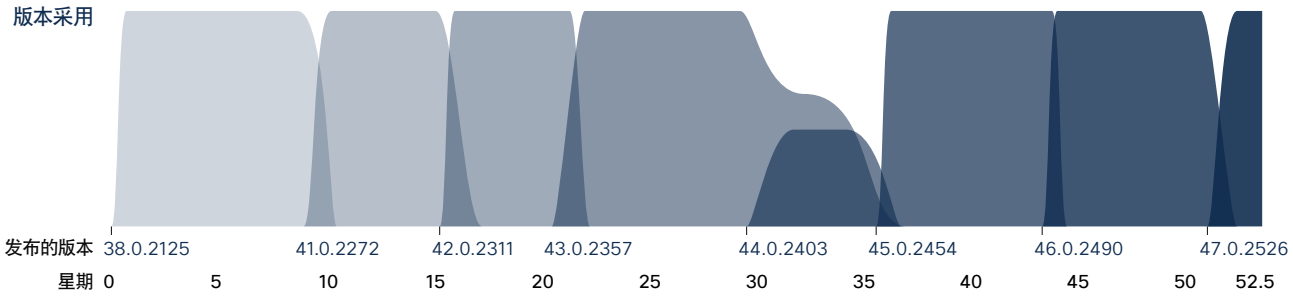


图 15. 按版本划分的 Java 安装（前 50% 的用户）

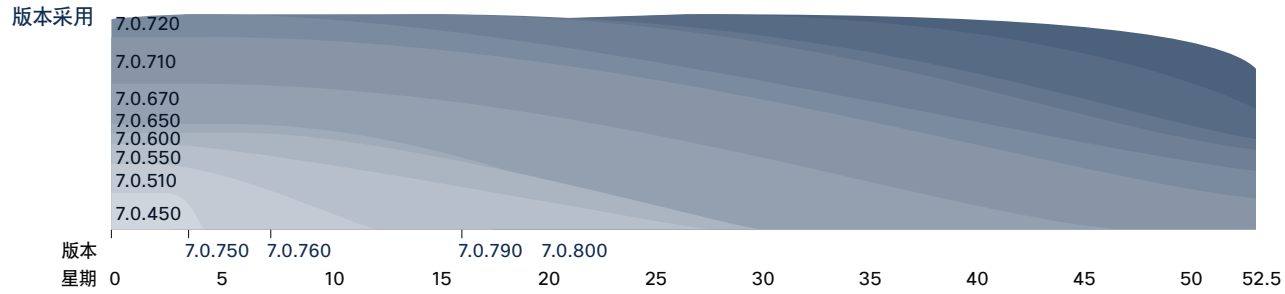
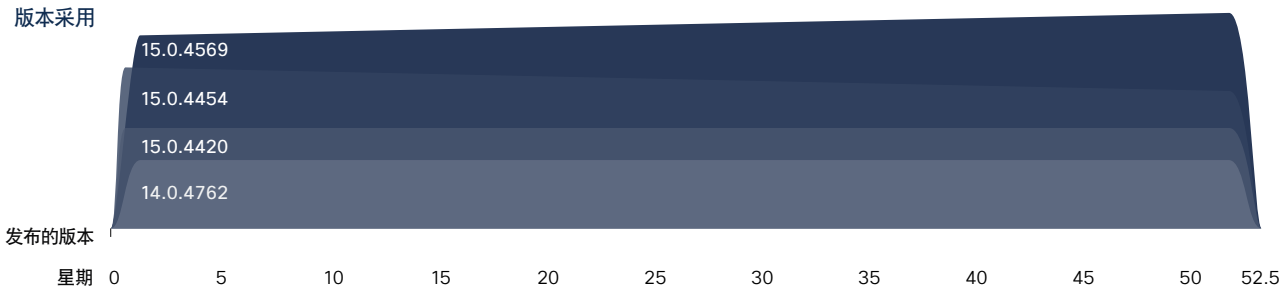


图 16. 按版本划分的 Microsoft Office 安装（前 50% 的用户）



来源：思科安全研究部门

分享

当我们从调查浏览器转向调查软件时，我们可以看到缺乏自动更新策略所带来的影响。在研究思科客户使用的终端上的 Java 软件安装情况时（图 15，在前一页显示），思科研究人员还发现了危害表现 (IOC)：调查的系统中有三分之一运行 Java SE 6，该版本已被 Oracle 逐步淘汰；最新版本是 SE 10。（在这项为期 1 年的调查中，开始时的实际百分比为 33%，到结束时则为 23%。）

此外，许多安装了最新版本 Java 的用户的系统中可能仍然保留着主要的旧版本，用于支持其他软件，或者可能只是没有删除这些旧版本。这意味着系统中仍然存在带有已知漏洞并处于易受攻击状态的版本。用户的其他防御，例如入侵防御系统，可提供一些保护，但是无法提供保证。事实上，如果终端上的防御缺乏其他保护，则风险甚至更高。

在调查 Microsoft Office 的安装情况时（图 16，显示在前一页），我们看到该软件套件的企业管理所面临的挑战。虽然存在薄弱的自动更新行为，但是大量用户群体使用的都是既定版本，并且一直使用该版本。当升级涉及许可证或 IT 支持成本，或者用户担心功能变更会改变与安全修补相同的数据包中提供的产能工具的行为时，这些因素可能会增加补丁所面临的挑战。

在分析的时间段内，存在四个主要的 Office 版本，但是最新版本的发布并没有看到有意义的采用。大量采用的三个版本所占的百分比大致为 28-52-20，与一年前相比，迁移量略有上升。主要版本升级涉及到许可事件，而次要版本更新则是常规软件维护生命周期的一部分。我们本来预计会看到一个主要版本的大多数用户都会运行最新版的服务包，但是研究最新版本（Office2013/版本15x）时却发现，我们划分的三个主要安全更新点几乎平分秋色。

最重要因素：许多大供应商都履行了自己的安全职责，及时发布通知、修补程序和分发漏洞补丁。然而，最终用户却没有这么重视修补工作，因此，他们在削弱自己及其业务的安全性。

除了快速发布补丁外，安全专业人员还应检查使用自动更新功能作为及时修补的有用工具的情况。有些系统比其他系统更易于应用自动更新，这是正常的。例如，浏览器更新是终端最轻量的更新，而企业应用和服务器端基础设施则更加难以更新，并且可能会导致业务连续性问题。因此，不太可能经常对其进行处理。安全专业人员必须按重要顺序进行更新和修补，使安全网络免受已知威胁和明显的威胁。

使挑战进一步增强的是，安全措施发布经常与功能发布混合在一起，这可能导致用户避免更新，因为更新会改变他们目前使用的功能。混合发布增加了供应商的支持负担和复杂性。

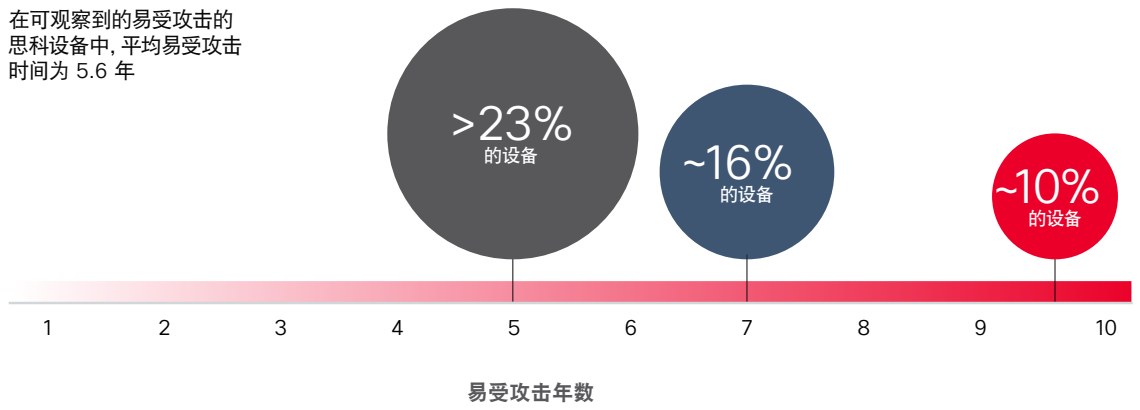
老化的基础设施：勒索软件的增加使修补长期存在的漏洞成为势在必行的紧急任务

2015年，为吸引人们注意由于组织没有适当维护老化的基础设施或修补易受攻击的操作系统而造成的安全风险，思科对互联网和客户环境中的115,000台思科设备进行了分析。[4]我们发现这115,000台思科设备中，106,000台（92%)运行的软件存在已知漏洞。

为制定本报告，我们当时打算研究一组思科设备样本，以确定在基本基础设施（路由器和交换机）上运行的已知漏洞存在的时间。我们的样本包括互联网上的 103,121 台思科设备（2002 年至 2016 年期间存在已知 CVE 的可观察安装）。平均每台设备上存在 28 个已知漏洞。

此样本中的设备存在已知漏洞的平均时间为 5.6 年。这些设备有超过 23% 存在始于 2011 年的漏洞。近 16% 存在首次发布于 2009 年的漏洞。并且有近 10% 存在超过 10 年的已知漏洞（图 17）。

图 17. 按已知漏洞的存在时间划分的运行已知漏洞的设备百分比

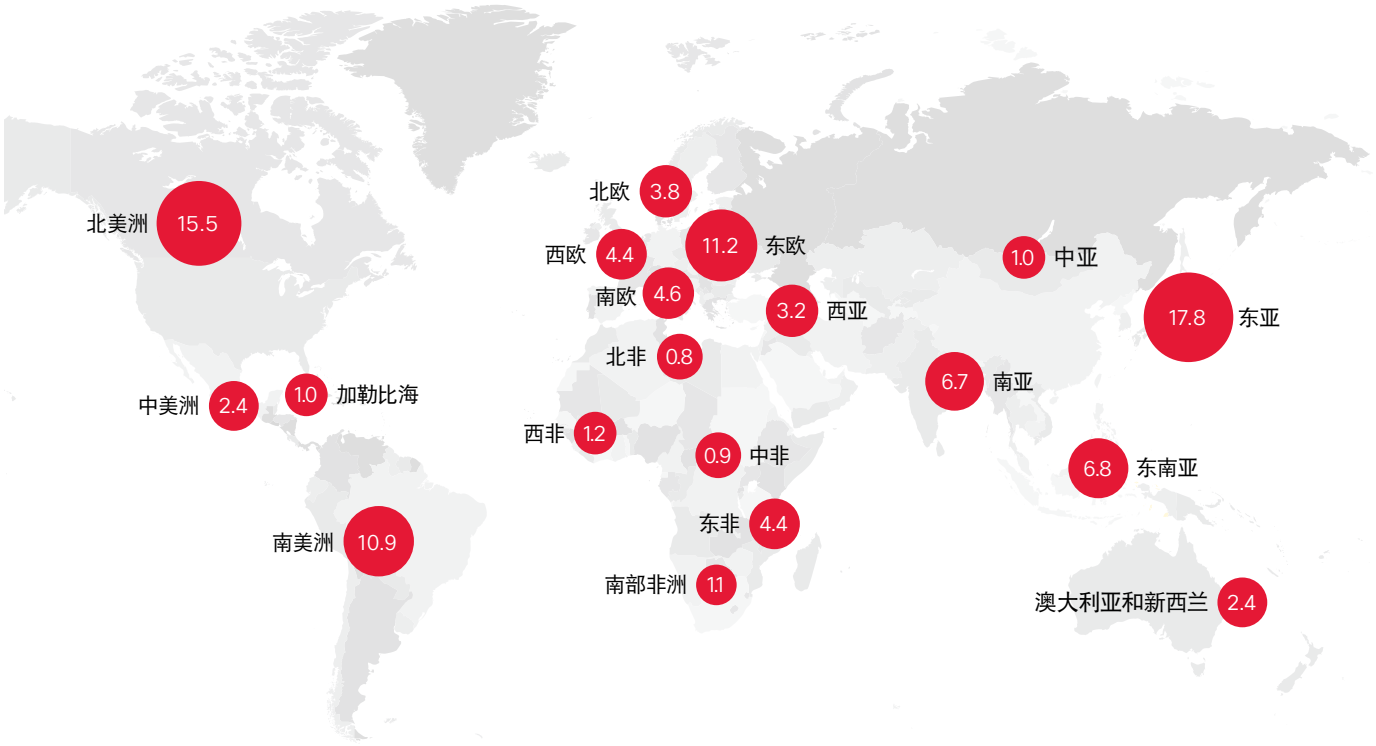


来源：思科安全研究部门

分享

[4]思科通过扫描互联网然后“从外向内”（从互联网视角到企业内部）检查设备来确定 1 天抽样的 115,000 台设备。有关该分析过程的详细信息，请参阅《思科 2016 年度安全报告》，网址如下：**cisco.com/go/msr2015**。

图 18. 按地区划分的易受攻击的思科设备百分比



来源: 思科安全研究部门

根据思科研究人员的研究，易受攻击的思科设备的最高比例出现在东亚 (17.8%) 和北美 (15.5%)。（请参见图 18。）

分享

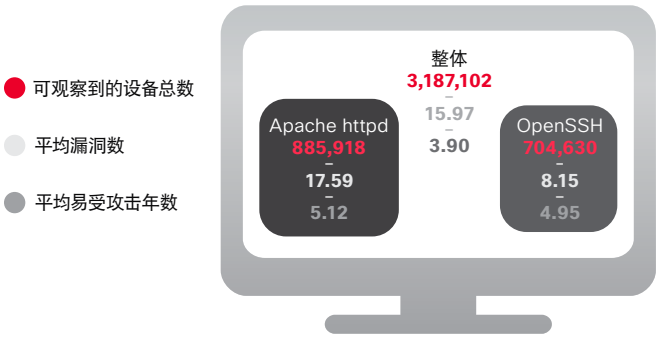
比较点：易受攻击的软件基础设施

思科研究人员调查了流行的软件基础设施中的漏洞，以确定组织是否更加勤勉地修补这些产品中的已知漏洞（图 19）。我们的样本包含 300 多万可观察的有漏洞安装，涉及众多产品，但大多数是 Apache httpd (885,918) 或 OpenSSH (704,630)。这些软件产品的平均已知漏洞数量接近 16 个。

根据我们的研究，使用 Web 服务器软件的组织运行已知漏洞的平均时间为 3.9 年。

至于地区结果，我们发现安装易受攻击软件数量最多的是北美、西欧和东欧（图 20）。

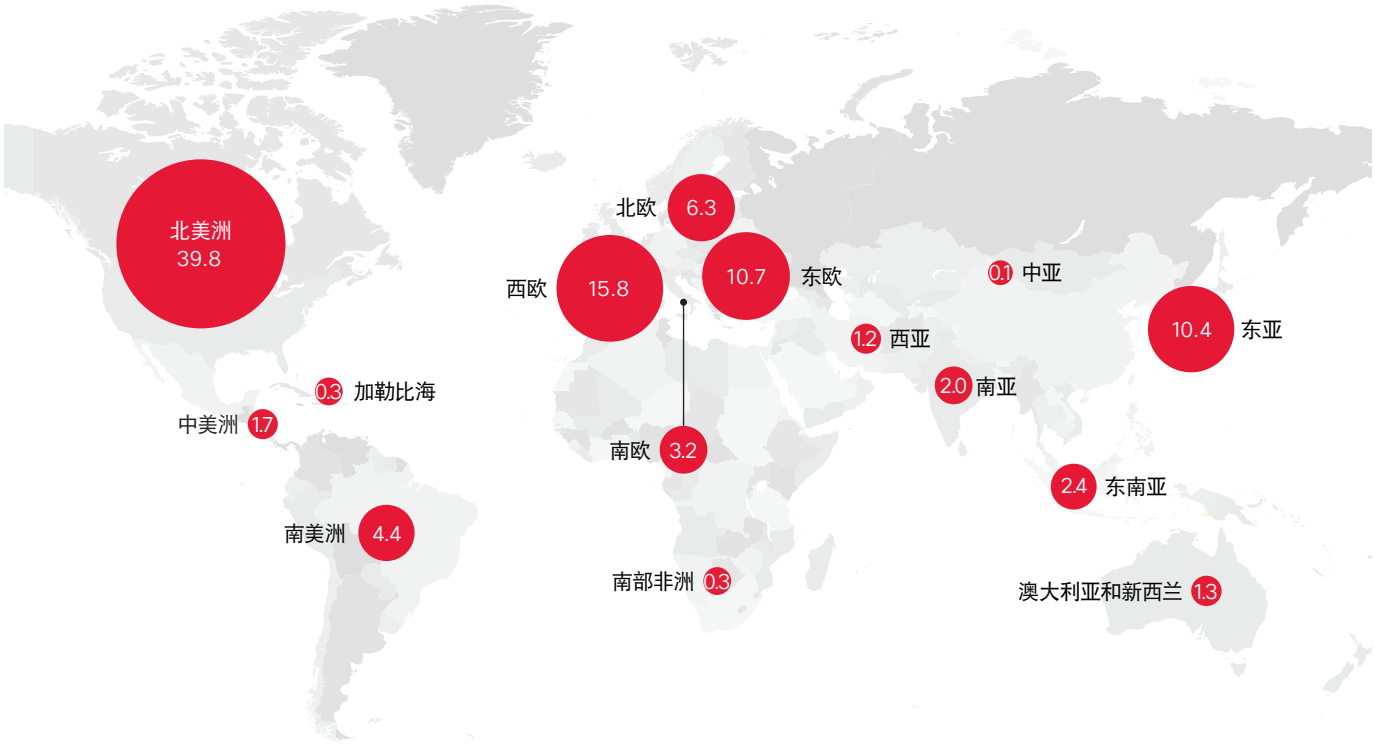
图 19. 按产品划分的易受攻击的软件安装数量



来源：思科安全研究部门

分享

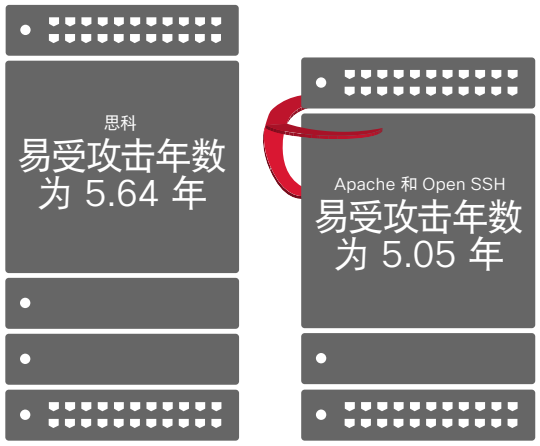
图 20. 按地区划分的易受攻击的软件安装百分比



来源：思科安全研究部门

我们对思科、Apache 和 OpenSSH 产品的分析发现，组织没有积极解决任一组产品中的已知漏洞（图21）。有些组织嫌麻烦不想升级，只是等着更换基础设施，或者他们也可能发现自己等待的时间太长，以至于无法升级自己的产品，因为这些产品不再受支持。无论是哪种情况，我们发现产品存在已知漏洞的平均时间大约为 5 年。

图 21. 软件卫生概述：思科与 Apache 及 OpenSSH 对比



来源：思科安全研究部门

分享

不再拖延：立即行动

虽然组织进行网络基础设施升级可能需要耗费大量时间和金钱，但是不进行必要的更新就会为攻击者提供更好的攻击机会。SamSam 勒索软件攻击活动（请参阅**第 7 页**）已经证明攻击者可以利用互联网基础设施中长期存在的已知漏洞发动具有高度针对性的攻击，使不警惕的组织陷入瘫痪并付出巨大代价。（请参阅“JBoss：基础设施中的漏洞为攻击者提供行动时间”，**第 18 页**。）

组织尤其要谨记：我们的分析中包含的所有产品安装，外部具备适当工具和专业知识的人员都能观察到。这些人当中就包括威胁攻击者。

全球的组织必须按重要顺序解决老化的基础设施和系统的问题。这不仅仅是要修补放任不管的旧漏洞，还要评估已部署的基础设施和系统的整体强度和网络弹性。很多组织都到了必须面对以下现实的时候：必须放弃不再受支持并且无法升级以应对当今安全挑战的产品。

有迹象表明，发展中国家在这些方面的步伐滞后，如图 22 和 23 所示。

图 22. 按地区划分的思科设备处于易受攻击状态的平均年数

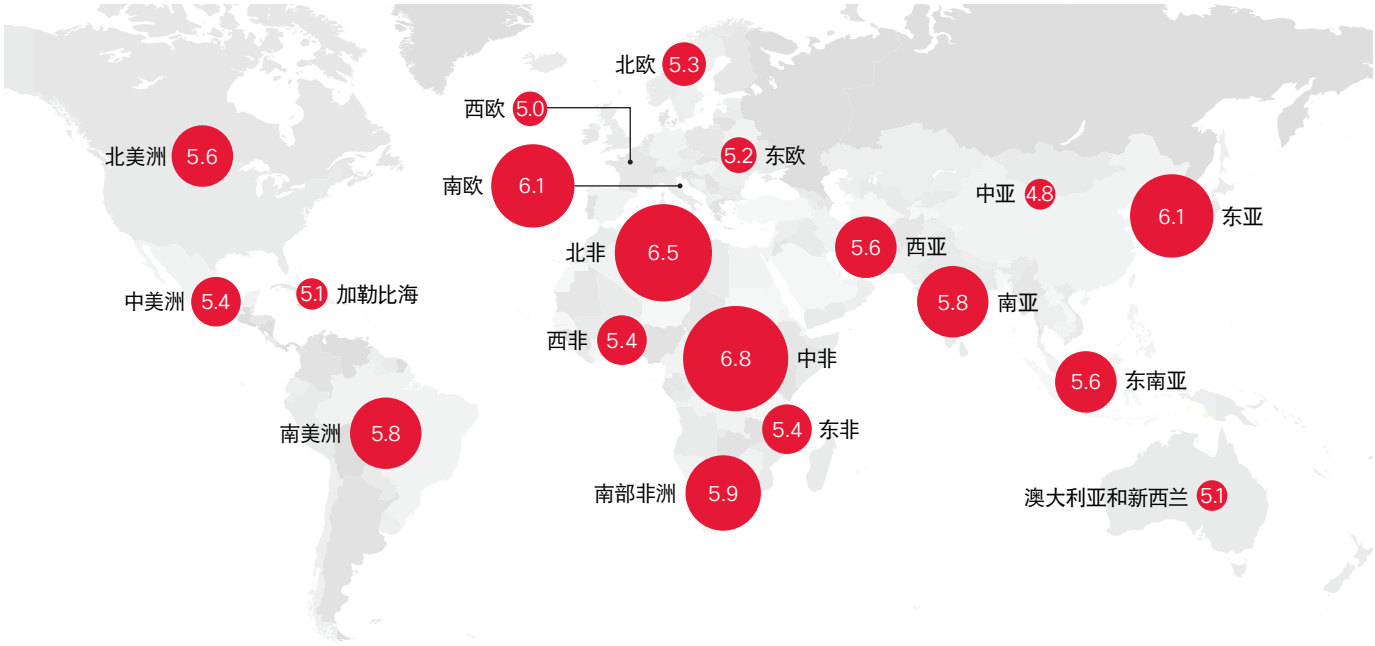
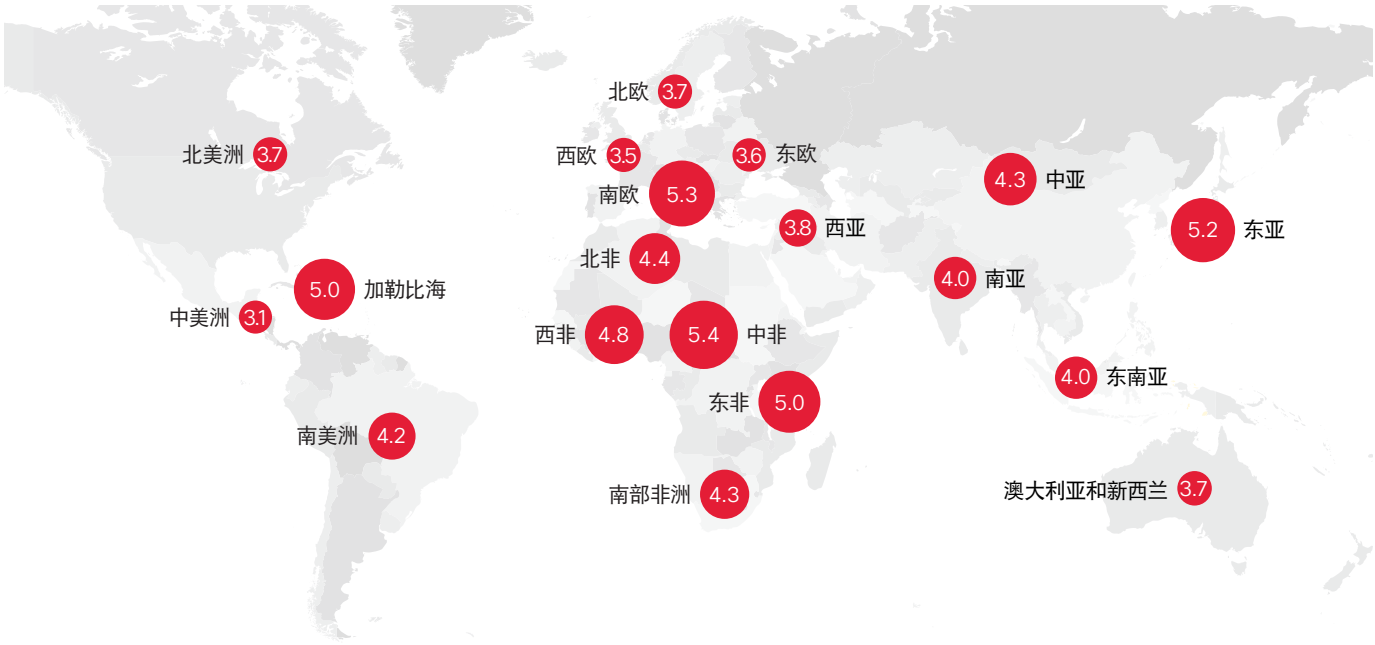


图 23. 按地区划分的各种类型的服务器软件处于易受攻击状态的平均年数



来源：思科安全研究部门

脆弱而不安全的基础设施无法支持新兴的下一代数字化经济。为了真正实现数字化和物联网将会带来的效益，组织需要解决第一次数字化浪潮的安全问题。

造成这些问题的部分原因是对于将安全性嵌入互联网基础设施的这一需求缺乏远见。在互联网早期，没有人知道基础设施将成为攻击者的目标。但是造成老化基础设施安全问题的原因也可能仅仅是由于组织虽然知道已知漏洞的修补程序，却一直拖延。他们不是勇于面对暂时断开关键基础设施的网络连接进行升级所带来的预期风险，而是将赌注压在希望自己不会成为攻击者目标的这种微乎其微的机会上。

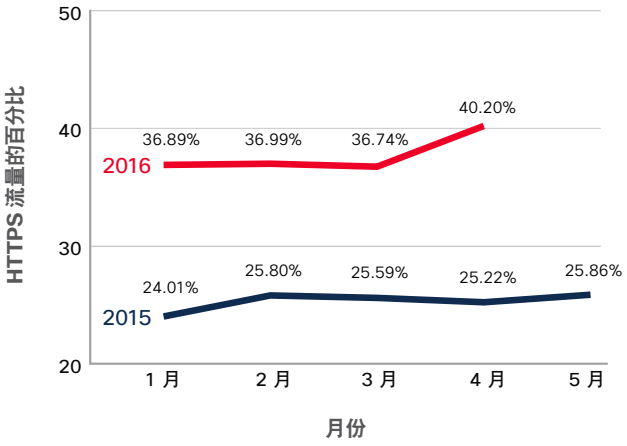
“脆弱而不安全的基础设施无法支持新兴的下一代数字化经济。为了真正实现数字化和物联网将会带来的效益，组织需要解决第一次数字化浪潮的安全问题。”

加密：到目前为止，2016 年的 HTTPS 流量保持稳定 …

正如我们上一次安全报告中所述，加密已经成为致力于保护敏感数据和客户隐私的组织偏好使用的工具。在 2015 年出现逐步但是显著的总体增长后，2016 年 1 月至 4 月的 HTTPS 请求量保持相对稳定。

从 2015 年加密的使用增加的情况来判断，安全行业专家预计加密的使用将继续增长，虽然 2016 年到目前为止的流量仅显示出小幅增长（图 24）。

图 24. 到目前为止，2016 年的加密 HTTPS 流量保持相对稳定



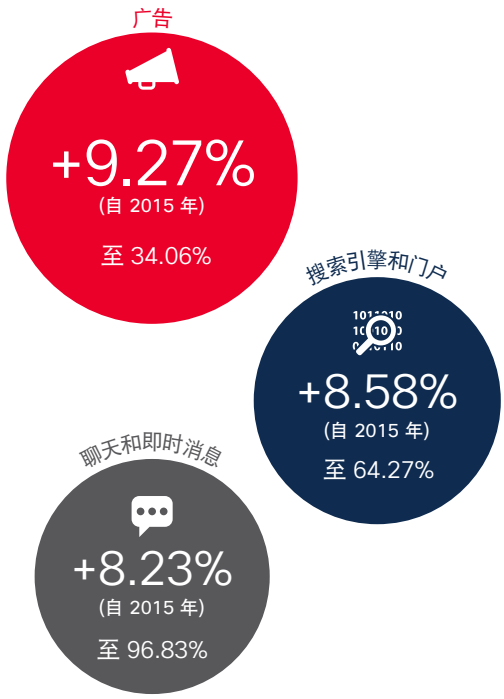
来源：思科安全研究部门

2016 年前四个月，广告领域的 HTTPS 流量出现增长（请参阅图 25）。增长的原因很可能是由于该行业希望保护用户隐私，破坏恶意活动。但是，这种流量的增长也可能反映出恶意活动开发者对 HTTPS 的使用增多：广告注入器（广告软件感染的主要组成部分）已成为利用 HTTPS 进行的恶意活动数量增加的主要来源。

使用 HTTPS 的前三个应用为组织电子邮件、聊天和即时消息以及基于 Web 的电子邮件，如图 26 所示。

通常来说，合法组织对于加密的稳步使用对用户而言是好消息，但是对于安全专业人员而言并不是什么好消息。犯罪分子也认识到加密对于隐藏其活动不被防御者发现的价值。利用加密，恶意攻击实施者有更多时间可以不受干扰地继续他们的活动（请参阅**第 22 页**了解关于恶意软件制作者使用 HTTPS 的详细信息）。由于无法了解被加密流量隐藏的危害表现 (IOC)，单点解决方案的效力会降低，防御者也更加难以在恶意活动造成持久损害之前有所发觉。

图 25. HTTPS 恶意软件流量增加 2015 年 1 月 – 2016 年 4 月



来源：思科安全研究部门

图 26. 使用 HTTPS 的热门应用

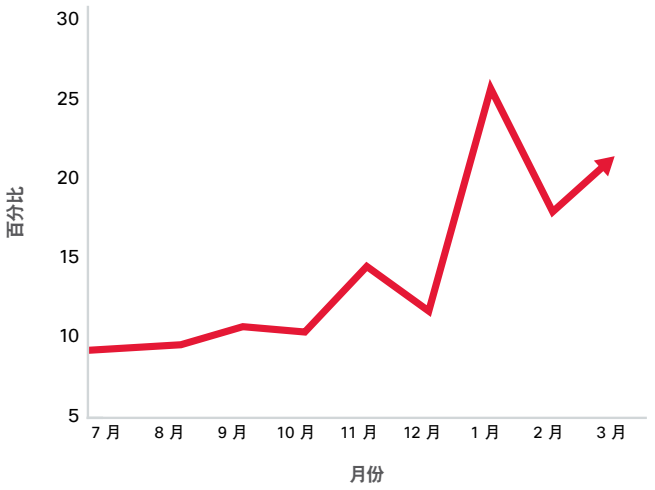
类别（1 月至 4 月）	平均百分比HTTPS
组织电子邮件	97.88%
聊天和即时消息	96.83%
基于网络的邮件	96.31%
在线存储和备份	95.70%
互联网电话服务	95.07%
职业社交网络	90.78%
社交网络	81.15%
文件传输服务	67.63%
流视频	64.71%
搜索引擎和门户	64.27%
照片搜索/图像	61.90%
网页转换	54.60%
SaaS 和 B2B	54.36%

来源：思科安全研究部门

TLS 加密负载，但不隐藏恶意软件行为

在不断追求更长时间地开展行动而不被发现的过程中，恶意软件制作者和使用者通常选择一般用于合法用途的技术工具。攻击者偏好的一个新选择可能是传输层安全 (TLS)。这是用于提供网络流量加密的主要协议。通过观察未加密的 TLS 报头，思科研究人员发现，少量、但是数量不断增长的恶意软件样本开始使用 TLS 进行受保护的通信。这是导致安全专业人员担忧的一个原因，因为它使深度数据包检测这一安全工具失去效力。

图 27. 使用 TLS 的恶意软件样本的百分比



来源：思科安全研究部门

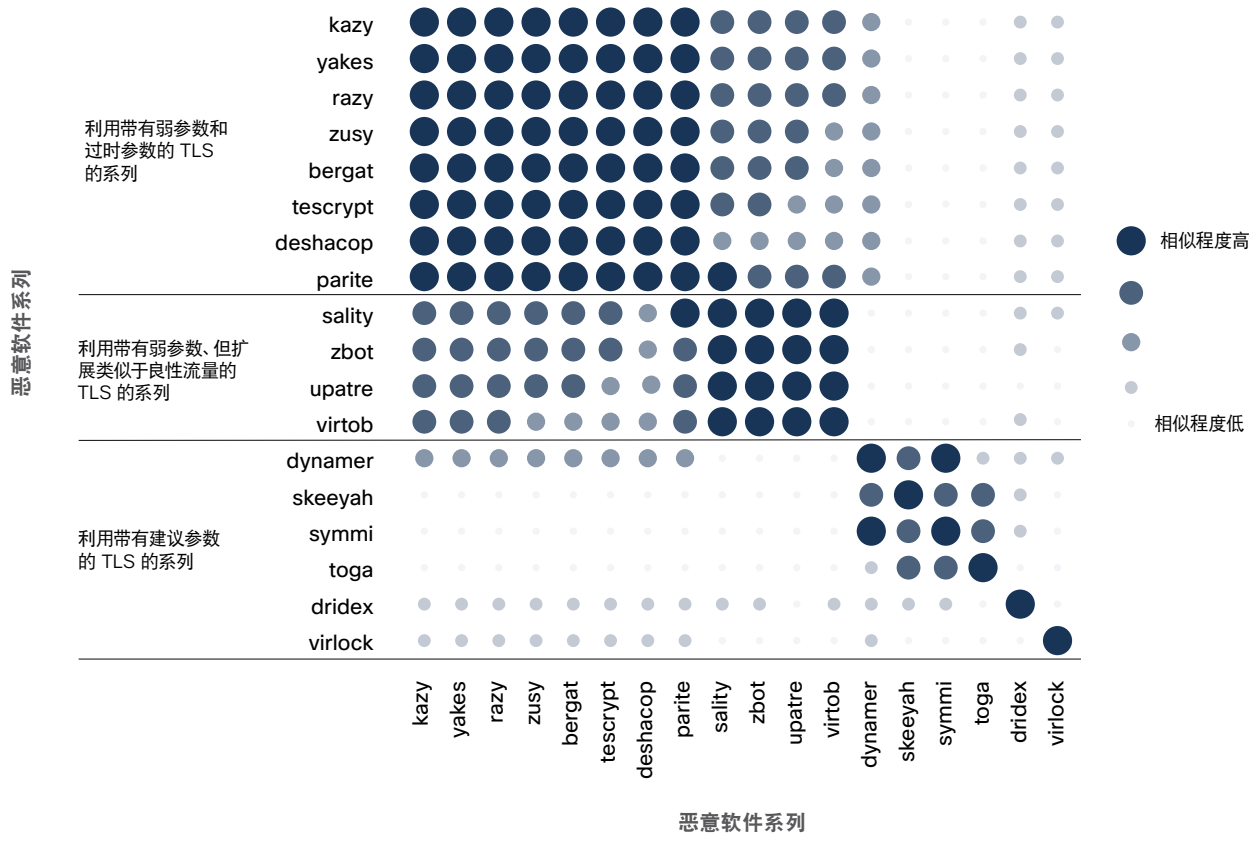
根据思科研究人员的研究，多达 60% 的网络流量使用 TLS 进行加密。在研究人员研究的恶意软件样本中，约 10% 的恶意软件使用了 TLS。这个百分比也许看起来很低，但是研究人员认为这个数字会随着良性流量中总体的加密使用量增加而增加。他们观察到，2015 年 7 月到 2016 年 3 月之间，恶意加密流量出现增长（图 27）。

知道恶意攻击实施者可能加大使用 TLS 后，安全专业人员如何才能提高对于使用此策略的恶意软件的检测？恶意软件对于 TLS 的使用显然与良性流量不同。对于大多数恶意软件系列，可以利用这一特点高度准确地对恶意流量模式进行分类。

研究人员发现，与良性网络流量中使用的加密参数相比，恶意软件制作者使用的加密参数通常较旧。恶意软件使用的较旧密码套件也许可以提供指示，表明该流量是恶意的。良性应用更有可能使用最新的 TLS 最佳做法，这很可能是因为这样做可以通过提供更高的安全性而使他们的产品脱颖而出。

而另一方面，恶意软件使用者会选择较旧的加密库，因为这些加密库经过验证，在许多运行环境中都能正常工作而不会导致错误。举例来说，可能破坏恶意软件加密的一种错误是，当主机上不存在恶意软件可执行文件预计会存在的库时，该可执行文件无法运行。

图 28. 恶意软件系列在 TLS 参数比较方面的相似性



来源: 思科安全研究部门

为了发现恶意软件系列使用 TLS 的模式，研究人员研究了 18 个恶意软件系列，数以千计的独特恶意软件样本，以及数以万计的加密网络流量。他们通过几种方法识别出恶意软件系列：

- 利用带有建议参数的 TLS 的系列，例如 Skeeyah 恶意软件
- 利用带有弱参数、但扩展类似于良性流量的 TLS 的系列，例如 Sality
- 利用带有弱参数和过时参数的 TLS 的系列，例如 tescrypt

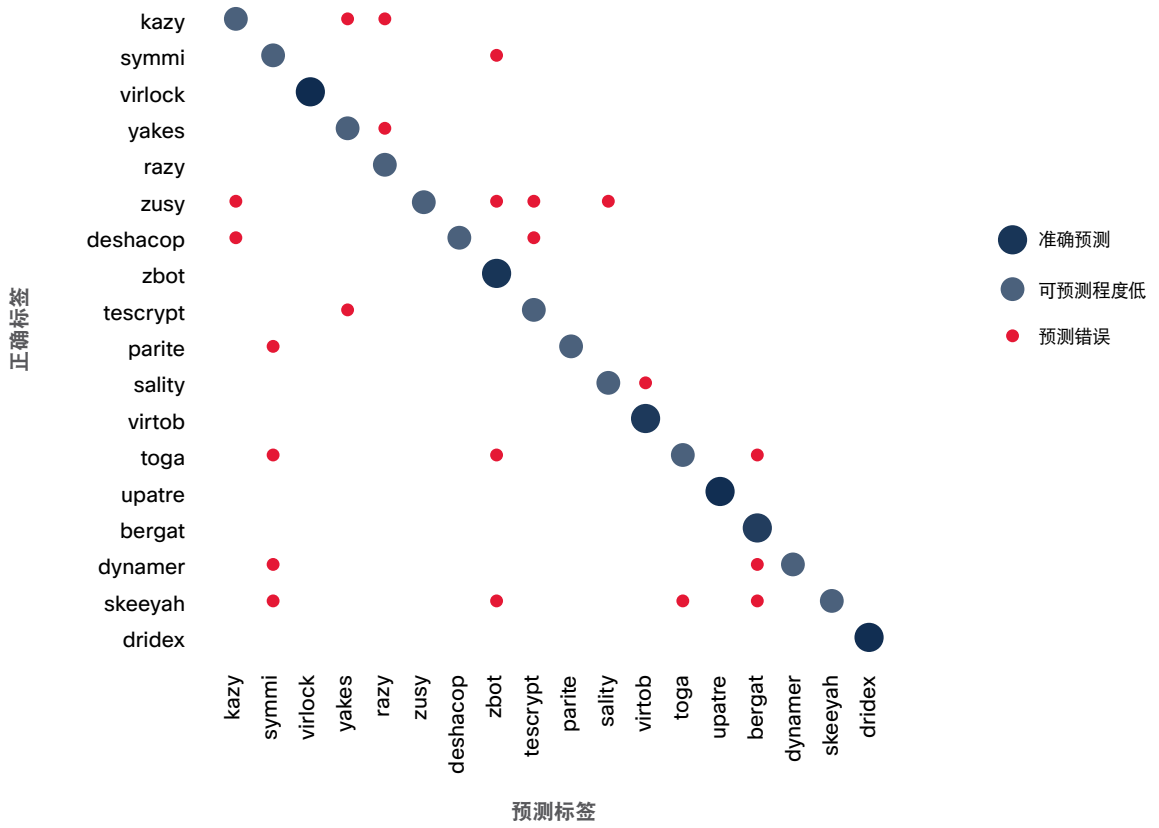
如图 28 所示，研究人员可以证明，一些恶意软件系列使用 TLS 加密的方式有相似性。

混淆矩阵（图 29）显示了区分不同恶意软件系列的容易程度。预测标签可能匹配正确标签（以大圆圈表示），而不正确预测（以小圆圈表示）则不太可能匹配。

不出意料，积极改进 TLS 使用方法的恶意软件系列更加难以分类。但是，研究人员发现，如果运用有关接受检查流量的特定领域知识，例如 TLS 证书是否为自签名，就能够更加准确地识别模式。例如，他们可以准确地将网络通信归因于特定的恶意软件系列，即使受限于单个加密流，准确度也能高达 86.8%。这证实了综合威胁防御（更确切地说，采用单纯的分类方法结合机器学习技术）的必要性和优势。机器学习方法与创新数据视图的结合，可为安全专业人员提供更优质的信息。

将恶意软件样本准确地归入已知恶意软件系列的能力对于安全专业人员而言很有价值。此类归属可以让事件响应人员在开始进行恶意软件样本的反向工程之前，就知道他们所处理的威胁的类型。此外，研究加密流量也可以帮助事件响应团队更好地规划时间，例如，分配更多资源来处理最为严重的恶意软件感染。

图 29. 混淆矩阵：区分各种恶意软件系列



来源：思科安全研究部门

检测时间趋势凸显白热化的“军备竞赛”

思科将“检测时间”或 TTD 定义为从发生入侵到发现威胁之间的这段时间窗。我们使用从全球部署的思科安全产品收集的选择性安全遥感勘测数据来确定这个时间窗口。利用我们的全球可视性和持续分析模型，对于在发现时没有分类的所有恶意代码，我们都能够测出从恶意代码开始在终端上运行到它被确定为威胁之间的时间。

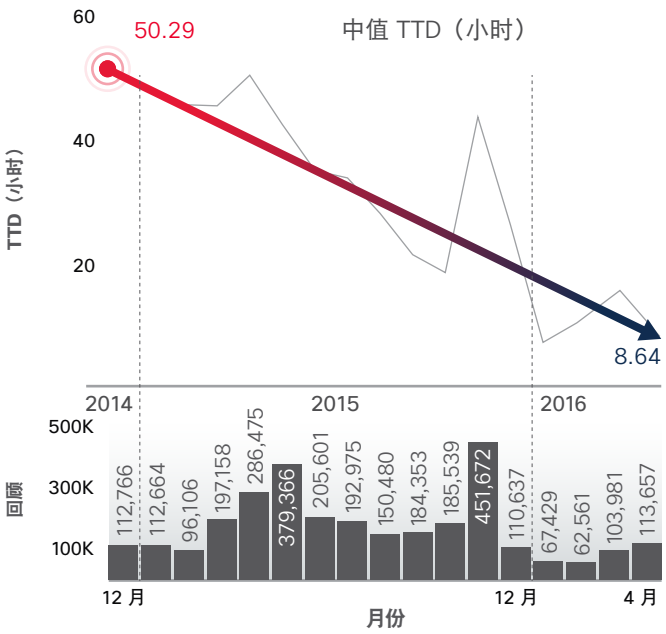
从 2014 年年底开始，我们跟踪了在缩窄 TTD 窗口方面取得的进展。一年前，我们报告的 TTD 中值大约为两天（50 小时）。[5]到 2015 年 10 月，思科将 TTD 中值大幅降低到 17 个小时。

2015 年 12 月到 2016 年 4 月期间，TTD 中值甚至更低：约 13 小时。该数字是观察的时间段内五个中值的加权平均值。

我们的 TTD 中值远低于 100-200 天的行业估计值，我们还将继续增强检测众多威胁的能力。图 30 显示了思科从 2014 年 12 月到 2016 年 4 月实现的 TTD 缩短的整体情况。

在图 30 中，TTD 中值的稳步下降趋势非常明显。曲线上也存在数次显著的高峰和低谷。它们是攻击者和防御者之间“军备竞赛”的证明。

图 30. 按月显示的 TTD 中值，2014 年 12 月 - 2016 年 4 月



来源：思科安全研究部门

分享

“我们的 TTD 中值远低于 100-200 天的行业估计值，我们还将继续增强检测众多威胁的能力。”

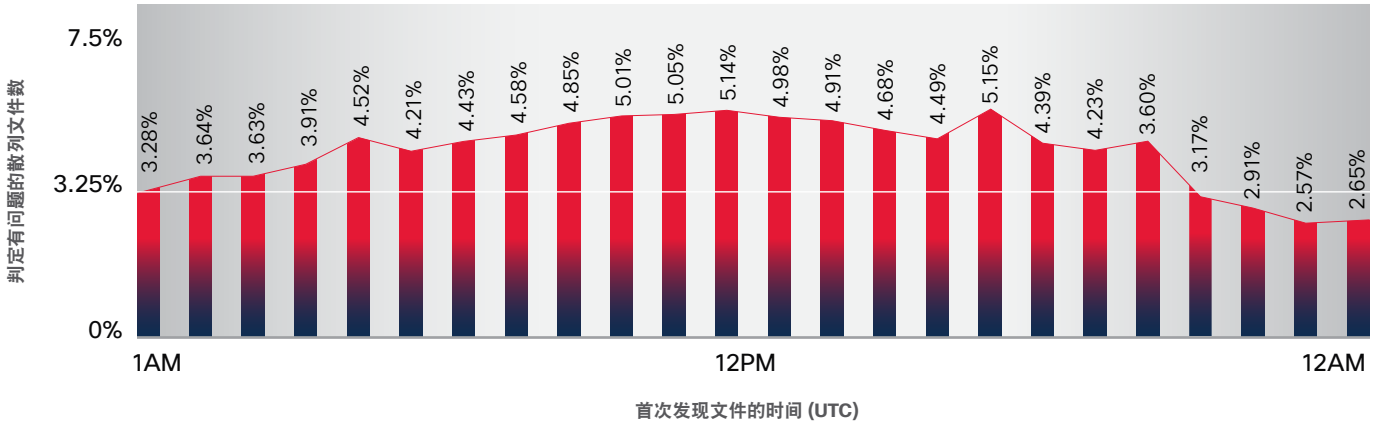
[5] 思科 2015 年年中安全报告，网址如下：**cisco.com/go/msr2015**。

攻击者不断创建隐秘技术以避开检测。安全供应商则通过更好的集成和威胁检测予以应对。然后，他们将其确定的 IOC 集成到自动检测技术中，并为该数据添加情景，使其成为对客户可行的威胁情报。（请参阅**第 53 页**上的“危害表现不是威胁情报”。）

TTD 的显著下降表示思科在对抗攻击者时获得优势的时间段，获得优势指检测威胁的速度快于攻击者开发和投入使用新技术的速度。峰值表示攻击者利用创新（需要分析人员进行研究或利用其他情报来源才能检测到）反击的时间段，从而使 TTD 中值上升。

攻击者与防御者之间的军备竞赛从未停止。攻击者不断发动猛烈的新威胁攻击，而安全供应商则必须快速识别。图 31 显示了在观察期间（2015年12月至2016年4月）典型的一天中发现的被判定有问题的散列文件数。总体上，一天中被判定有问题的文件比率相当一致。

图 31. 按一天中的小时划分的被判定有问题的散列文件



来源：思科安全研究部门

分享

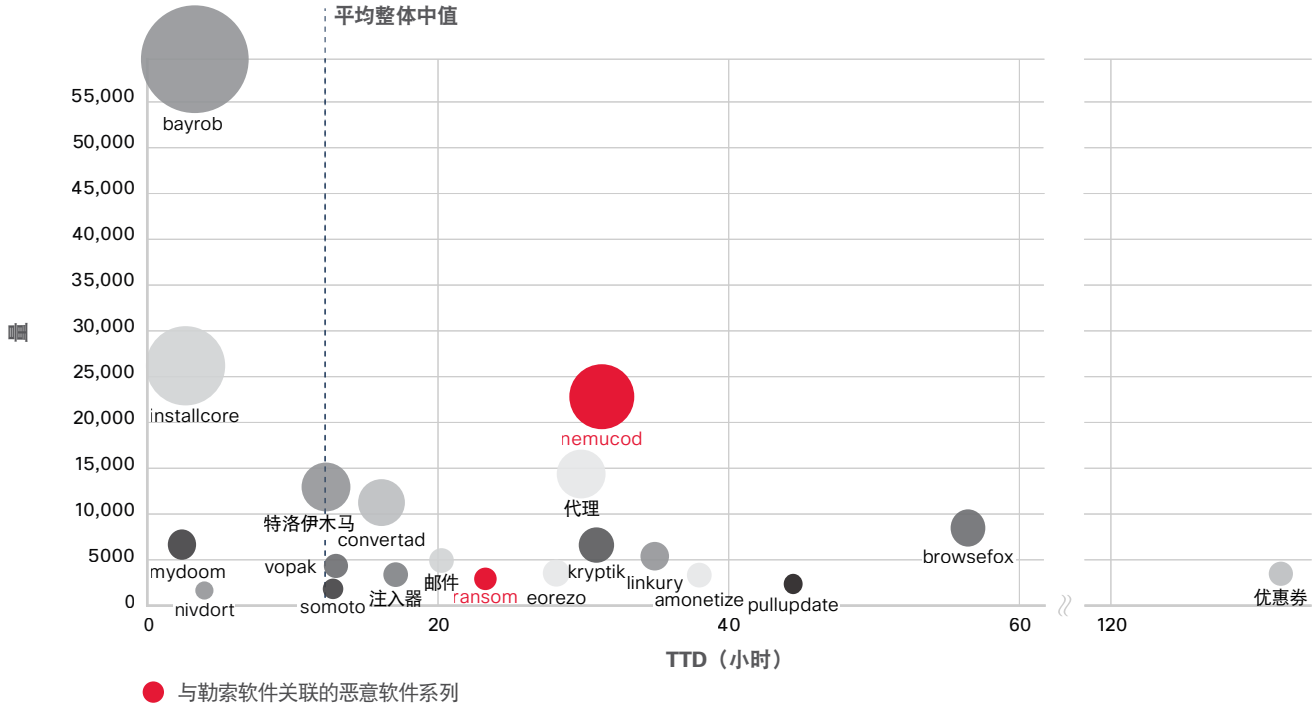
“TTD 的显著下降表示思科在对抗攻击者时获得优势的时间段，获得优势指检测威胁的速度快于攻击者开发和投入使用新技术的速度。”

勒索软件激增：造成最近 TTD 中值波动的一个因素

正如我们的上一次网络安全报告中所述，这种影子经济的产业化以及商业恶意软件的更广泛使用是促使我们自 2014 年起坚定不移地显著缩短 TTD 的重要因素。产业化的威胁散播迅速，使其更加易于检测。

在 2016 年前五个月，思科在 TTD 中值（约 13 小时）处或附近检测到的恶意软件系列属于较老但仍然普遍存在的威胁。这种威胁的两个范例是 Bayrob（僵尸网络恶意软件，2007 年开始出现，并且在今年年初重新兴起）和 Mydoom（一种通过电子邮件散播的计算机蠕虫，在 2004 年首次发现，会影响 Microsoft Windows）。知名的恶意广告软件 InstallCore 也很盛行，可能是由于其在帮助散发勒索软件中起的作用（图 32）。

图 32. 排名靠前的恶意软件系列的 TTD 中值（检测数量排名前 20 的系列）



来源：思科安全研究部门

分享

过去一年勒索软件的激增是导致某些恶意软件系列使用增加，因而检测到的次数增多的一个因素。

与勒索软件有关联的几个恶意软件系列的 TTD 趋于高于中值，因为自动化技术（例如试探式扫描和沙盒）无法提供早期检测，分析人员需要花时间研究这些威胁。

图 33 显示了思科在 2016 年 1-4 月检测到的排名居前的恶意软件系列的逐月趋势。突出显示的名称是与勒索软件相关的恶意软件系列示例。攻击者对于某些恶意软件系列的使用的增加或减少导致 TTD 中值出现波动。需要思科分析人员进行研究才能检测的威胁使 TTD 中值从 2016 年 2 月的仅仅 9 个多小时上升到 2016 年 3 月的超过 14 小时。

图 34 突出了防御者在努力缩短 TTD 时面临的挑战，以及组织采用综合威胁防御的必要性。能够早于 TTD 中值检测到的威胁是通过沙盒等自动化技术识别的。新兴和更复杂的威胁则需要利用内部或第三方调查和情报，因此需要更长的时间才能检测出。

恶意软件活动变幻无常，但有一点是不变的：攻击者和防御者之间的对抗关系。攻击者必须不断创造出可以躲避检测的威胁，以便增加其行动时间。而防御者必须通过持续搜索新型和新兴恶意软件，将其发现的 IOC 集成到自动化检测技术中，并将其研究结果转换为实际的威胁情报，以此应对攻击者的行动。

在未来几个月内，思科将致力于不断降低 TTD 中值。我们建议其他组织测出自己的 TTD 中值，以便开始跟踪改善情况，并帮助降低目前让人难以接受的 100–200 天的行业估计值。

更好的 TTD 和 TTP（修补时间）做法和加密的使用，加上主动解决基础设施老化的问题，都有助于减少攻击者不受限制的行动空间。具体来说，TTD 和 TTP 可作为关键的性能指标，使防御者能够专注于在哪些方面以及如何提高自己的能力，以检测攻击者的状态，并限制攻击者改变战术和逃过识别的能力。

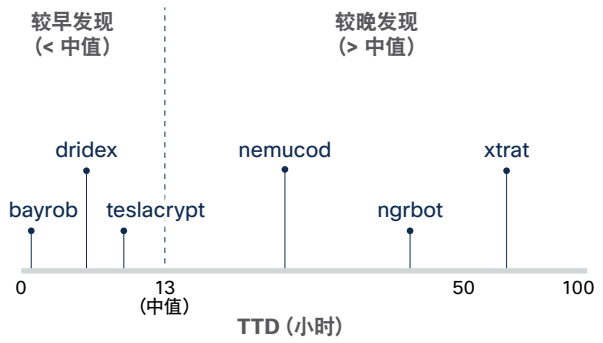
图 33. 按月划分的前 10 位被检测到的恶意软件系列

	1 月	2 月	3 月	4 月
1.	bayrob	下载程序	下载程序	bayrob
2.	下载程序	installcore	nemucod	下载程序
3.	installcore	convertad	代理	installcore
4.	代理	msil	installcore	nemucod
5.	convertad	browsefox	convertad	代理
6.	勒索	linkury	mydoom	convertad
7.	linkury	nemucod	msil	fareit
8.	kryptik	代理	browsefox	msil
9.	browsefox	kryptik	kryptik	特洛伊木马
10.	msil	mydoom	vilsel	heur

● 与勒索软件关联的恶意软件系列

来源：思科安全研究部门

图 34. 恶意软件系列检测较早和较晚的示例，基于 13 小时的 TTD 中值



来源：思科安全研究部门

事件响应：削弱组织安全性的做法

安全媒体经常报道有关网络入侵、勒索软件攻击和精心设计的恶意软件的新闻，还会报道这些事件造成的影响，如业务关闭和品牌声誉受损。但是，对于可能遭受此类攻击，很多组织似乎仍大感意外。这些组织认为他们的威胁检测和事件响应机制稳固，实际上却可能漏洞百出。

通常情况下，这些组织采用的安全技术和做法可能落后于当前产品十几年。所以真正发生攻击时，通才型安全专业人员可能很快就疲于应付可能需要专业技能的事件响应需求。

思科就安全准备情况咨询了各种规模的组织，经常会发现他们缺乏有助于强化安全的最佳做法。思科团队还发现，恶意攻击实施者找出了这些薄弱环节，并借此侵入网路。

例如，进行合并和收购 (M&A) 交易的公司可能没有对合作伙伴业务风险状态进行足够的尽职调查。他们可能会在交易完成后才发现新组合业务的缺点，此时进行补救，为时已晚，或者更加困难，因为网络现在已经交织在一起。在开始 M&A 交易之前，首席信息安全官 (CISO) 应充分评估安全保护情况。至少，他们应该在直接转换之前确保相应网络中不存在可疑活动迹象。

> “报告自己以前从未遭受入侵的组织不会真正了解自己的网络活动。任何成熟的组织都会遇到某种程度的商业恶意软件活动和防御系统遭攻击的情况。”

和不好的做法（例如设置弱密码或频繁使用管理员权限）一样，评估不当的网络也可能会导致恶意攻击实施者在网络中停留更长的时间。组织没有准备好对抗复杂威胁的另一个标志是，不了解过去有什么影响过其网络。报告自己以前从未遭受入侵的组织不会真正了解自己的网络活动。任何成熟的组织都会遇到某种程度的商业恶意软件活动和防御系统遭攻击的情况。

思科还观察到，对于自身对攻击者的吸引力，组织没有自知之明。医疗保健等行业近年来对恶意攻击实施者的吸引力有所增强，这是因为它们拥有宝贵的数据，同时长期以来安全防范相对薄弱（请参阅**第 45 页**）。此外，思科还注意到，攻击者将其注意力转移到易受攻击的机构（例如学校），因为他们知道这些机构的安全防御可能微乎其微。有关能够支持有效事件响应的最佳做法，请参阅**第 52 页**上的“安全建议”。

医疗保健行业的勒索软件攻击为所有组织上了一堂安全卫生课

今年，医疗保健行业遭受了数次勒索软件攻击。在对遭受勒索软件攻击的医疗保健垂直行业的思科客户进行的分析中，我们发现了一些使这些组织遭受感染的风险加大的企业漏洞。具体包括：

- 共享密码和“权限过高”的帐户
- 可能导致已泄露密码被检测到的不充分安全日志记录
- 带有 **OWASP** 前 10 位漏洞的 Web 应用
- 未修补的操作系统和应用

思科研究人员还发现，一家医院中的所有 PC 通常运行易受攻击的相同版本的软件，例如 Windows XP、Adobe Flash 播放器或 Java 。值得注意的是，我们调查的医疗工作站最近遭受的勒索软件感染中，大部分都可以追溯到临床人员从缺少 Flash 播放器补丁的工作站进行的网络浏览行为。

缺乏确保及时安装安全补丁的正式流程，也是我们的医疗保健客户的一个常见问题。

此外，大多数被勒索软件盯上的医疗服务提供商都没有制定事件响应计划，这严重削弱了他们有效应对攻击的能力。

另外，几乎没有医疗保健组织具备专门的安全团队。IT 资产维护通常由一名或多名缺乏安全专业知识的通才型 IT 人员负责。

我们建议面临类似安全挑战的企业至少要采取以下措施来改善其整体安全状态：[6]

- 进行基本的系统强化，以抵抗恶意软件和黑客攻击
- 评估组织的 IT 形势：网络中有哪些设备，数量多少？这些设备位于何处？
- 对用户开展威胁和最佳做法教育
- 制定事件响应计划
- 积极监控网络的被入侵迹象

此外，必须解决已知的安全漏洞。JBoss 服务器上长期存在的漏洞使最近 SamSam 攻击活动背后的威胁实施者能够逐步渗透互联网基础设施，以锁定医疗保健网络（请参阅 **第 7 页**）。思科研究人员预计，考虑到互联网上数量众多的易受攻击设备和软件，攻击者只会越来越多地瞄准基础设施，以支持勒索软件攻击活动。（有关更多信息，请参阅“老化的基础设施：勒索软件的增加使修补长期存在的漏洞成为势在必行的紧急任务”，**第 30 页**。）

各行各业的组织都能够从医疗保健行业的恶意软件经历中学到许多教训。他们应考虑采取措施，确保负责安全管理的技术人员拥有有效开展工作所需的工具、资源和政策。

[6] 注：进行安全改进时，组织应考虑他们必须遵守的所有监管合规性要求或其他行业相关指令，因为这些要求可能会影响组织如何具体处理安全工作的某些方面，例如数据保护和数据隐私。

全球视野和安全建议

全球视野和安全建议

恶意软件来自世界各个角落，攻击者在必要时会迅速变换行动基地的地区位置。对于认为自己不会成为攻击者目标的组织，毫无疑问的一点是：没有哪个垂直行业可以在攻击中独善其身。试图依靠 IOC 而不是真实威胁情报来提高其威胁检测和事件响应能力的组织，实际上并不能改善其安全状态。

与此同时，在日益复杂的威胁形势中，企业也面临着另一个不确定性：政府日益关注对数据的控制或访问需求，由此产生相互冲突的信号、法规和要求。这些关注最终可能会限制国际商务、安全技术和可信赖的公私合作关系并与其发生冲突。

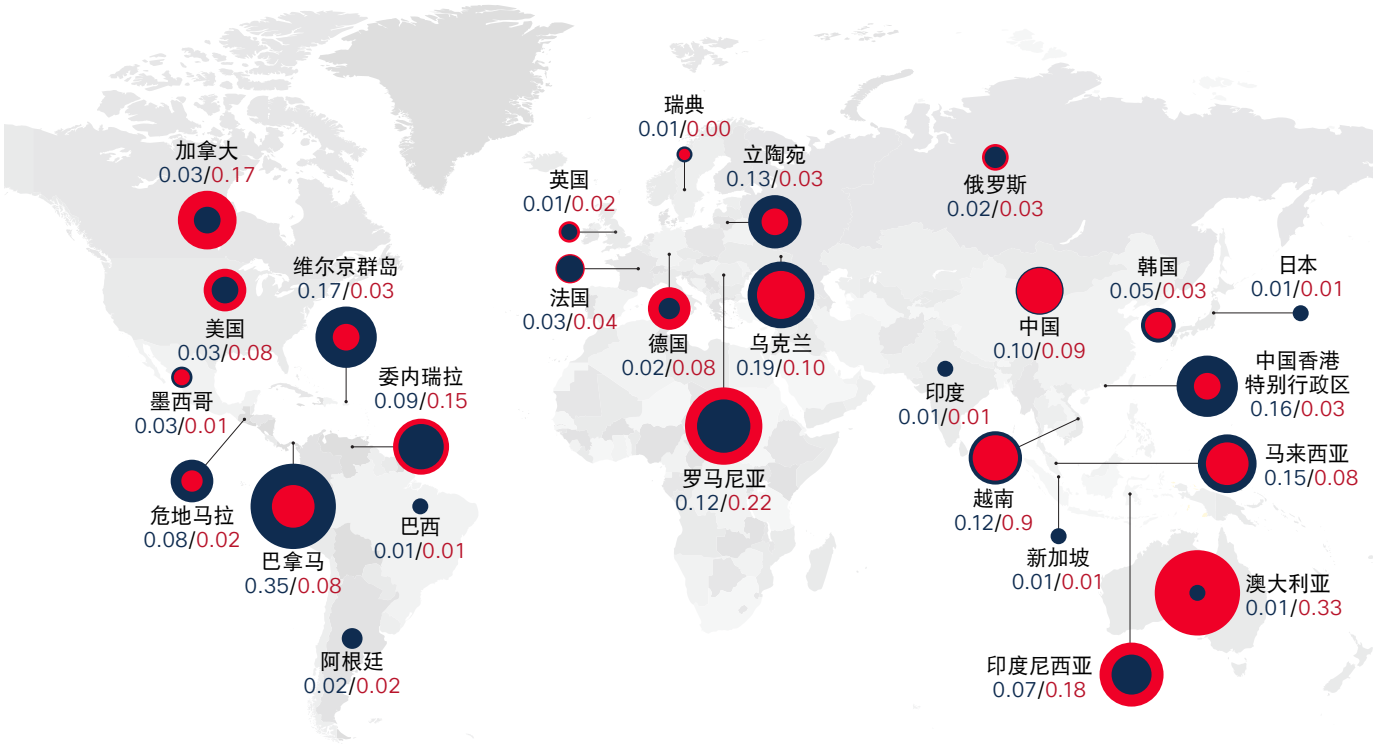
网络阻止活动的地区概况

通过研究总体互联网流量和阻止活动，思科研究人员得以洞悉恶意软件的来源。在美洲，加拿大似乎是美国以外受阻止流量的最大来源。

在欧洲、中东和非洲地区，按照受阻止流量占总流量的比例计算，乌克兰和罗马尼亚是受阻止流量的最大来源；在亚太地区，澳大利亚居于首位（请参阅下一页的图 35）。

由于各种原因（例如容易被黑客入侵的服务器的可获得性），攻击者会变换其行动基地的地区位置。

图 35. 按国家或地区划分的网络威胁阻止情况



来源: 思科安全研究部门

分享

和对垂直行业的调查一样（**第 49 页**），最重要的是没有哪个国家或地区可以免遭恶意流量攻击。应该将恶意软件视为全球问题。当然，有些地区和国家表现出更高比例的阻止活动，这是因为攻击者已经发现能够利用的基础设施漏洞。

此外，2015 年 12 月和 2016 年 1 月观察到的澳大利亚恶意软件活动峰值将导致各个国家及其受阻止流量的权重发生显著变化。

恶意软件对垂直行业造成的风险：没有哪个行业是安全的

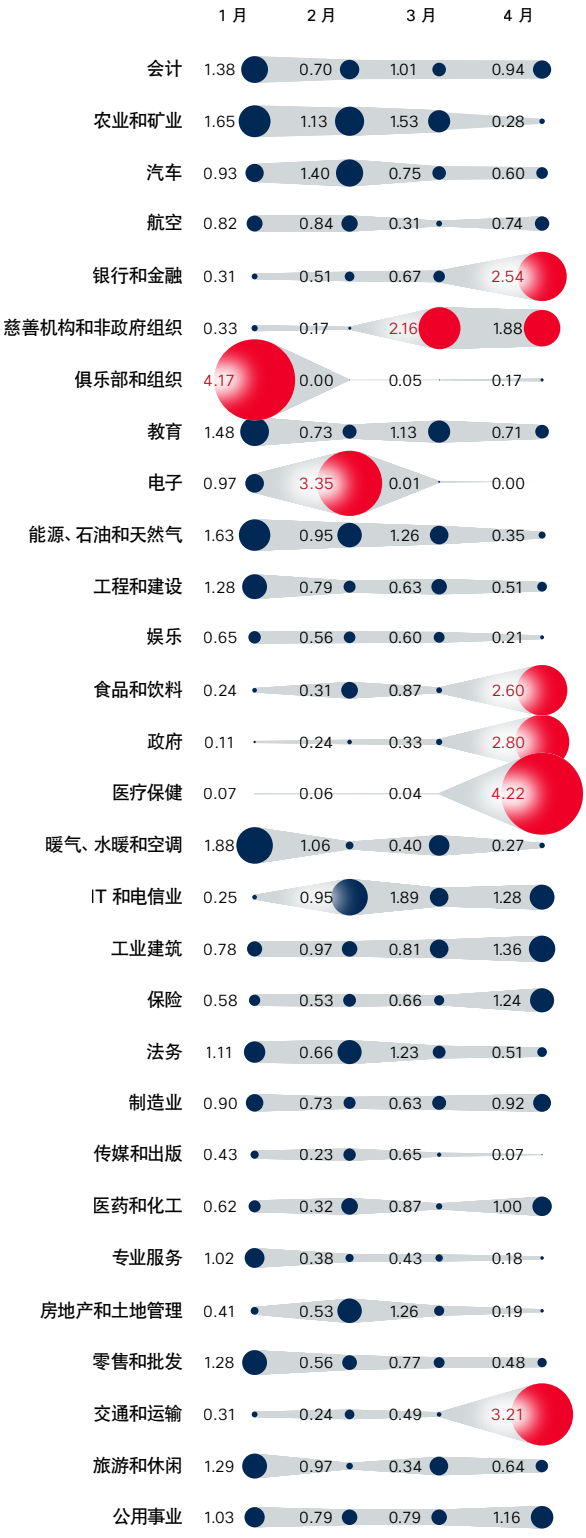
要向认为自己所在的行业对于网络攻击者没有吸引力的安全专业人员传达的信息：这是盲目自信。思科对各行业的攻击流量（“阻止率”）和“正常”或预期流量进行的定期研究发现，显然没有哪个垂直行业可以免遭恶意软件攻击。在想方设法获得攻击活动空间和时间的攻击者面前，所有行业都可能成为受害者。

虽然新闻报道称医疗保健行业是攻击者偏好的行业（请参阅**第 7 页**），但是思科数据表明，在 2016 年的最初几个月内，其他行业显示出成比例的大量恶意软件。例如，俱乐部和组织、慈善机构和非政府组织以及电子商务行业都出现了最高的阻止率。

这项阻止率研究的要点是每个行业都存在风险。虽然数据显示不同行业偶尔会出现阻止流量峰值，但是攻击者的注意力显然是随着他们发现的网络入侵机会而在各个行业间转移。一旦他们实现自己的目标，就立即转向具有最佳投资回报的任何行业目标。推动攻击活动的是机会，而不是行业。

图 36 显示了 29 种主要行业及其相关阻止活动，以占常规网络流量的比率表示。比率为 1.0 意味着阻止活动的数量与观察到的数据流量相称。任何高于 1.0 的比率则表示阻止率高于预期，任何低于 1.0 的比率表示阻止率低于预期。

图 36. 每月的垂直行业阻止率，2016 年 1 月 – 4 月



来源：思科安全研究部门

地缘政治最新动态：政府和企业应对数据保护困境

地缘政治环境中的网络安全继续使技术供应商、电信和其他全球公司在复杂而通常相互矛盾的监管世界中周旋。在这种形势下，安全问题的竞争元素 — 一方面是政府和企业，另一方面则是隐私和安全 — 展开较量。

不管是涉及公民个人数据的保护还是涉及物理基础设施（例如国家电网和供水系统）的完整性，数据安全都已成为政府的当务之急。政府还希望能够在需要时访问数据，例如通过合法拦截。

政府知道他们已失去对技术和数据访问的控制，并且在着手重新建立一部分控制。恐怖袭击和全球经济的缓慢增长使这种需求得到增强，迫使当选官员证明他们有能力保护公民和商业企业：

- **爱德华·斯诺登泄密事件余波未平，有关个人权利与国家权利的争论促使人们重新思考《安全港协议》等协议。新的《欧美隐私盾牌》协定规定美国公司要承担更大的义务保护欧洲公民的个人数据不受政府访问。**
- **欧盟 (EU) 的移民危机以及最近发生在巴黎、布鲁塞尔、土耳其、美国以及其他地方的恐怖袭击，引发了有关执法机构访问加密私人通信的争论。了解了全球范围内对这一问题的关注，人们密切关注美国联邦调查局 (FBI) 与苹果公司之间关于解锁恐怖分子使用的 iPhone 的对峙也就不难理解。**
- **政府和私营安全公司也更加愿意对国家发起的间谍和窃取活动采取行动。利用国际金融网络 SWIFT（环球银行金融电信协会）对银行进行的攻击被指由朝鲜发起；德国政府最近将其联邦议院受到的攻击的源头指向莫斯科。**

世界各地的政府正在考虑采取措施，希望借此掌握更高程度的技术控制权，以便对抗恐怖主义和网络犯罪等威胁。在这个过程中，他们承担发现新漏洞的风险，并且在某些情况下，他们保留利用这些漏洞的权利。他们不一定会与技术供应商分享所有这些信息，从而引起一个不可避免的问题：谁应承担披露漏洞的责任？当提到公众对于不断增强的政府干预的反应时，商业企业通常位于最前线。

尽管全球化的步伐很快，但是对于广泛的网络安全问题或相关问题（例如透明度、责任、数据保护和加密），却没有全球统一的解决方案。为全球互联网建立“交通规则”的工作在继续，但是划分优先事项所存在的分歧将使企业继续在政治化的、有法律风险的环境中开展业务。

“尽管全球化的步伐很快，但是对于广泛的网络安全问题或相关问题（例如透明度、责任、数据保护和加密），却没有全球统一的解决方案。”

不断演变的监管形势

全球电信和技术供应商必须紧跟每个国家的法规步伐，遵守每个主权国家的法规，同时还要符合自己国家的法律体制和公众期望。但是，考虑到不同国家正在推行的众多类型的立法，这注定是一条艰难的道路。

以英国为例，政府的《调查权力法案》试图在本年底将英国安全服务部门的监管权力全部集中在一项立法中。英国议会目前正在就该法案展开辩论。政治家、企业和人权组织已经指出了该法案中的一些有争议的措施，包括称为“按需解密”的条款，该条款要求技术供应商和电信运营商在英国安全服务部门要求时可能要解除加密。

其他国家/地区则正在采取进一步的措施，并设法加速完成这些措施。例如：

- **欧盟自己的《网络和信息安全指令》将在今年夏天最终确定。**
- **法国正在推动议会通过一项反恐法案。该法案规定，对公司管理层拒绝配合恐怖主义调查的公司处以巨额罚款，并建议将管理层判处监禁。该法案的支持者希望该法案在法国延长的紧急状态（在 11 月份巴黎遭遇袭击后启动）到期之前成为法律。**
- **匈牙利政府讨论了将使加密软件成为非法活动的法律法规。**
- **俄罗斯和中国对恐怖主义的日益关注促使其采取措施来扩大对国内技术网络的控制。**

由于这些措施要求严格，且有可能导致法律后果，这些措施成为电信和技术供应商极为关心的问题。

复杂性降低我们所有人的安全性

这种监管日益复杂的局面对商业企业而言具有挑战性。最终，复杂性会降低我们所有人的安全性，而攻击者可以并且会利用这方面的分歧。

- **一直以来，美国的情况都比较特殊，因为到目前为止，许多对政府有用的数据都存储在美国的服务器上。这种情况将不复存在。德国、俄罗斯和中国等国家正在采取行动，制定数据本地化法律，建立监管平台。**
- **美国也在谨慎考虑甚至比英国的《调查权力法案》更进一步的立法。该项立法将要求任何生产软件或硬件或维护应用商店的公司以政府可以阅读的形式提供数据，并且内置“反向工程”技术能力，以移交可识别的数据。**

由于缺少一套全球计划，政府与私营部门之间亟需就网络安全问题建立更好的沟通和理解。用于交换数据请求的更有效的系统是实现这个目标的一个良好开端。政府和商业企业之间的信息共享也至关重要，虽然还有误解需要设法消除。

例如，企业坚持认为，强制技术供应商提供数据“后门”也许可以带来短期安全效益，但是最终可能会破坏消费者的信任。反过来，这还会损害构成其经济支柱的公司。

对于公共和私营部门而言，数据保护都是个难题。诸如《欧美隐私盾牌》之类的协议旨在促进数据的国际流动，以便进行分析，并让消费者相信，数据流能够安全传输，不会对其和数据造成风险。消费者是否愿意接受这些措施仍然有待观察。

“由于缺少一套全球计划，政府与私营部门之间亟需就网络安全问题建立更好的沟通和理解。”

安全建议

随着下一代勒索软件的发展，组织需要部署“第一道防线”，阻碍勒索软件的逐步渗透和传播，并减少攻击者的行动时间。第一道防线除了基本的最佳做法，例如修补易受攻击的互联网基础设施和系统（请参阅**第 22 页**和**第 29 页**）和完善密码管理（**第 44 页**），还包括网络分段。

组织可以使用网络分段来阻止或减慢自我传播威胁的逐步渗透，并对其进行遏制。组织应考虑实施适用于分段网络的多个组件，包括：

- 用于在逻辑上分隔数据访问的 VLAN 和子网，包括在工作站层级的分隔
- 专用防火墙和网关分段
- 具有已配置入口和出口过滤的基于主机的防火墙
- 应用白名单和黑名单
- 基于角色的网络共享权限（最小权限）
- 适当的凭证管理

最后一道防线：备份恢复

对于现在以及将来都不想向已经利用勒索软件将其数据加密的攻击者支付“巨额赎金”的组织来说，备份恢复是其最后一道防线（**第 10 页**）。然而，能否在最大限度地避免数据丢失和服务中断的情况下从勒索软件攻击中恢复，取决于系统备份和灾难恢复站点是否遭到破坏。

如果在勒索软件攻击中，本地备份被删除、撤除或被攻击者使用其他方式导致不可用，如果想不支付赎金而恢复服务，非现场备份通常是组织的唯一希望。备份发送至非现场的频率将决定有多少数据（如有）将不可访问或丢失。

不要忽略浏览器感染威胁

当广告注入器通过 HTTPS 加密流量传播恶意广告时，防御者无法立即识别出威胁（请参阅**第 21 页**）。由于攻击者越来越多地使用 HTTPS 加密流量来隐藏他们的活动，安全团队不能再将浏览器感染视为对其组织及用户的低严重级别威胁，这一点尤为迫切。

一个看似良性的浏览器感染可以迅速成为一个大问题。有证据表明，恶意广告注入器已成为攻击者为更高风险的攻击铺设基础的重要工具。

提高浏览器感染监控的优先级，将更有利于组织迅速识别这些威胁并进行补救。行为分析工具和协作威胁情报是防御者补救此类威胁的关键资源。教育用户将弹窗广告和骚扰广告增多的情况告知安全团队，这对于防御也至关重要。

设置定期修补生命周期

所有行业的各种规模的组织都需要摒弃“逐项核对”的做法。这种方法不足以应对当今的威胁。要保持“安全第一”的立场，除了对安全防御的财政投入外，还需要采用综合威胁防御。

例如，安全专业人员应使用可用工具定期检查是否存在意外的系统或管理员帐户。他们还应记录和分析所有网络通信是否存在恶意流量，并检查此类可疑流量的 IOC。领导层应为安全专业人员提供开展这些深入研究所需的工具。

此外，他们应该通过设置定期修补生命周期，将最新的补丁提供给威胁实施者可能寻找并利用其漏洞的操作系统和常用软件，确保环境保持最新状态。

危害表现不是威胁情报

IOC 是威胁情报的描述语言 — 威胁活动的构建基块。然而，尽管此数据对于开展调查的防御者非常有价值，但 IOC 不是威胁情报。

组织可能会花费数百万美元购买当作威胁情报出售的 IOC 列表。然后由其安全团队利用该数据，并想办法将其与业务关联。这个过程会耗费大量资源，耽误安全从业人员进行更高优先级的活动。在某些情况下，依赖 IOC 可能会让人误以为组织可能是安全的，不会受到攻击者的攻击，攻击者更关注其他组织的安全状态。

那么，什么是威胁情报？威胁情报是指通过理解产生该数据的情景，已经转化为切实可行的信息的数据。威胁智能还附带针对性的“接下来如何利用这些数据告诉我们的信息”。没有企业级应用的数据仅仅是数据，就像海滩上的沙子。

为了确保投资的是真正的威胁情报并从中获益，组织应该寻找将 IOC、包含与组织相关影响的情景以及指示结合在一起的安全供应商。他们在该过程中谨慎地加入人的因素，并将这些见解融入他们的安全工具，为依赖威胁情报的安全团队提供自动化威胁情报。

区分 IOC 和威胁情报至关重要。威胁情报能够帮助防御者了解攻击的整体情况，并提高其检测能力和事件响应能力。

“区分 IOC 和威胁情报至关重要。威胁情报能够帮助防御者了解攻击的整体情况，并提高其检测能力和事件响应能力。”

结论

当今的攻击普遍胜过防御者的响应能力。只要攻击者拥有不受限制的时间来开展行动，寻求创新，他们的成功几乎就是确凿无疑的。但是，如果组织能够限制攻击者为攻击做准备和开展攻击的时间和机会，就可以迫使攻击者在压力之下作出决策，使其更容易被发现，从而将其挫败。

通过迫使攻击者不断改进他们的威胁，扭转对抗攻击者的局面，是减少攻击者行动时间的一个策略。不管他们尝试多少方法来躲避检测和掩盖踪迹，他们需要改变的越多，就越有可能留下线索，最终被识别出来。

因此，这是势在必行的。如果防御者不知道自己检测威胁的能力如何，他们就无法改进。应将 TTD 和 TTP（修补时间）视为关键性能指标；这样一来，安全团队就能够专注于研究限制攻击者的技术，并迫使攻击者改变策略。

在帮助减少威胁实施者的行动时间方面，组织和最终用户一直以来都发挥着重要作用。对企业而言，现在是改进安全做法的前所未遇的绝佳时机，同时，这也是比以往任何时候都要迫切的需求。

升级老化的基础设施和系统，以及修补已知漏洞，将削弱网络犯罪分子利用这些资产开展攻击活动的能力。实施 SamSam 勒索软件攻击的攻击者为影子经济开辟了一片充斥着旧漏洞的新沃土。他们可以利用这些漏洞侵害用户，并获得前所未有的高额利润。（请参阅“勒索软件：一个持久力毋容置疑的巨大收入来源”，**第 7 页**。）

许多组织的互联网基础设施已经到达了临界点。他们希望简化和更新设备及软件，以降低成本并建立能够帮助他们在新兴的下一代数字化经济中取得成功的强大 IT 基础。这是他们在自己的整个网络中强化安全、实现可视性的关键时刻，也是帮助缩短攻击者目前拥有的不受限制的行动时间的关键时刻。

“许多组织的互联网基础设施已经到达了临界点… 这是他们在自己的整个网络中强化安全、实现可视性的关键时刻，也是帮助缩短攻击者目前拥有的不受限制的行动时间的关键时刻。”

关于思科

思科提供符合当前实际需求的智能网络安全解决方案和业界最全面的高级威胁防范解决方案组合，这些方案覆盖了最广泛的攻击媒介。思科的以防御威胁为中心且运营化的安全方案可以降低复杂性并减少零散片断，同时可在攻击的整个过程中（攻击前、攻击中和攻击后）提供无与伦比的可视性、一致的可控性和先进的威胁防范。

借助从海量设备和传感器、公共和私人来源及思科开源社区处取得的遥感勘测数据，来自思科综合安全智能 (CSI) 生态系统的威胁研究人员将行业领先的威胁智能汇聚到了一起。这相当于每日提取数十亿的网页请求和数以百万计的电子邮件、恶意软件样本和网络入侵数据。

我们先进的基础设施和系统利用这些遥感勘测数据，帮助机器学习系统和研究人员跟踪跨网络、数据中心、端点、移动设备、虚拟系统、网络、邮件以及来自云的威胁，以找出威胁的产生根源和爆发范围。我们将由此产生的情报转化为对我们产品和服务的实时保护，并立即交付到全球各地的思科客户手中。

要详细了解思科的以威胁为中心的安全方法，请访问 **www.cisco.com/go/security**。

思科《2016 年年中网络安全报告》撰稿人

TALOS 安全情报和研究小组

Talos 是思科的威胁情报组织，这个由安全专家组成的精英团队专门为思科客户、产品和服务提供卓越的保护。Talos 由领先的威胁研究人员组成，在成熟系统的支持下，为检测、分析和防御已知和新兴威胁的思科产品创建威胁情报。Talos 维护 Snort.org、ClamAV、SenderBase.org 和 SpamCop 的官方规则集，是向思科 CSI 生态系统提供威胁信息的主要团队。

安全和信任组织

思科安全和信任组织致力于实现思科对董事会和各国领导人最关心的两个最重要问题的承诺。该组织的核心任务包括保护思科的公共和私人客户，在思科的所有产品与服务组合中实现和确保思科的安全开发生命周期以及信任系统工作，并保护思科企业免受不断发展的网络威胁的攻击。思科采用整体方法来全面增强安全与信任，将人员、策略、流程和技术等环节全部包括在内。安全和信任组织重点围绕信息安全、信任工程、数据保护与隐私、云安全、透明与验证，以及高级安全研究与政府等领域，努力推动实现卓越运营。有关更多信息，请访问 **http://trust.cisco.com**。

全球政府事务

思科为众多不同级别的政府机构提供支持，帮助其形成支持技术产业并有助于政府实现各项目标的公共政策和法规。全球政府事务团队负责开发和影响支持技术的公共政策和法规。通过与行业利益相关者以及相关合作伙伴合作，该团队与政府领导建立各种关系，对影响思科业务和整体 ICT 采用的政策施加影响，以帮助形成全球、全国和地方级别的政策决策。政府事务团队由前任官员、国会议员、监管者、美国高级政府官员和政府事务专业人员组成，帮助思科提倡及保护技术在全球的使用。

感知威胁分析

思科感知威胁分析是通过对网络流量数据的统计分析，发现在受保护网络内运行的漏洞、恶意软件和其他安全威胁的一种基于云的服务。它通过使用行为分析和异常检测，来识别恶意软件感染的症状或数据泄露，从而应对基于外围的防御的漏洞。感知威胁分析依靠高级统计建模和机器学习来独立识别新威胁，从其所发现的内容中学习，并随着时间推移而适应。

INTELLISHIELD 团队

IntelliShield 团队执行漏洞和威胁研究、分析、整合，以及将来自思科安全研究和运营组织的数据与信息和外部来源关联，提供 IntelliShield 安全智能服务，其支持多种思科产品和服务。

LANCOPE

Lancope 是思科旗下公司，作为网络可视性和安全情报的领先提供商，致力于保护企业抵御当今的主要威胁。通过分析 NetFlow、IPFIX 和其他类型的网络遥感勘测，Lancope 的 StealthWatch® 系统提供情景感知安全分析，以快速检测从 APT 和 DDoS 到零日恶意软件与内部威胁的各种攻击。Lancope 将对整个企业网络的持续单边监控与用户、设备和应用感知相结合，加速事件响应，改善调查分析并有效降低企业风险。

主动威胁分析团队

思科主动威胁分析 (ATA) 团队利用先进的大数据技术，帮助组织抵御已知的入侵、零日漏洞攻击和高级的持续性威胁。这种全面管理服务通过我们的安全专家和我们的全球安全运营中心网络提供。一周七天，一天 24 小时提供不间断的警戒和按需分析功能。

安全研究和运营组织 (SR&O)

安全研究和运营组织 (SR&O) 负责所有思科产品与服务的威胁与漏洞管理，下属成员包括行业领先的产品安全事件响应团队 (PSIRT)。SR&O 通过 Cisco Live 和 Black Hat 等活动以及通过与思科及整个行业的合作伙伴进行协作，帮助客户了解不断发展的威胁形势。此外，SR&O 努力通过创新提供各种新服务。例如，思科定制威胁情报 (CTI) 服务可以识别现有安全基础设施未检出或未缓解的感染指标。

高级安全研究和管理 (ASRG)

高级安全研究和管理 (ASRG) 为思科的长期安全愿景提供方向和指导。为实现这一目标，ASRG 在关键安全领域（例如高级加密和安全分析）开展内部研究。ASRG 还与大学研究人员合作，并向其提供资金，以帮助解决长期问题。

思科安全事件响应服务 (CSIRS)

思科安全事件响应服务 (CSIRS) 团队由世界级的事件响应人员组成。这些人员负责在思科客户经历事件之前、期间和之后为客户提供协助。CSIRS 利用一流的人员、企业级安全解决方案、最先进的响应技术以及从多年来对抗攻击者的经历中总结出的最佳做法，确保我们的客户在面对任何攻击时，都能够更加主动地防范、快速作出响应并从中恢复。

下载图表

本报告中的所有图表都可以通过以下网址下载：
www.cisco.com/go/mcr2016graphics.com

更新和修正

要查看对本报告中信息的更新和修正，请访问：
www.cisco.com/go/mcr2016errata.com

美洲总部
Cisco Systems, Inc.
加州圣荷西

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

欧洲总部
Cisco Systems International BV
荷兰

思科在全球设有 200 多个办事处。思科网站上列有各办事处的地址、电话和传真，网址为：**www.cisco.com/go/offices**。

发布时间：2016 年 7 月