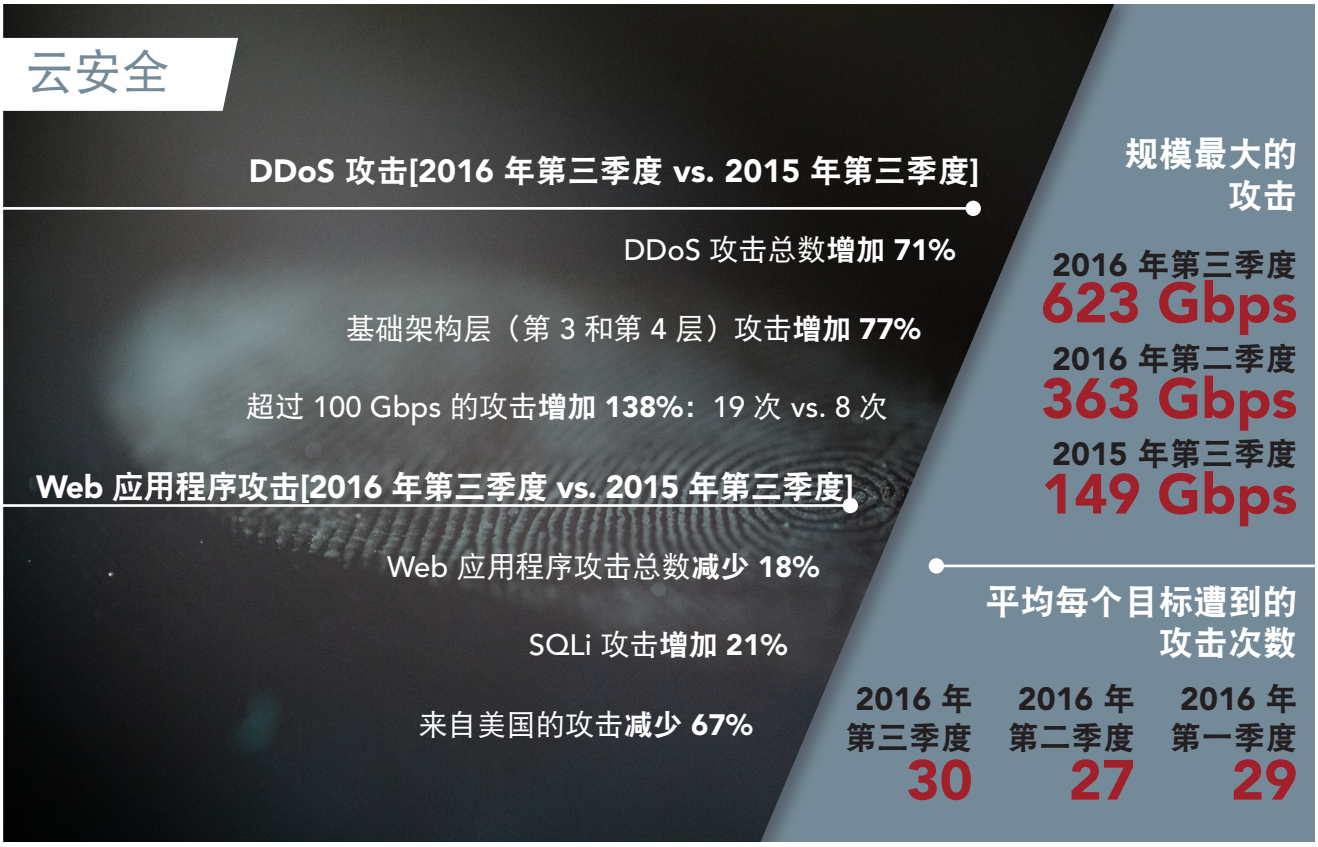
Akamai 的[互联网现状]/安全

2016 年第三季度执行摘要

关于摘要/全球领先的内容交付网络 (***CDN***) 提供商 Akamai 利用其遍布全球的智能平台 (Intelligent Platform™)，每天处理数万亿计的互联网交互活动。这让 Akamai 能够收集与宽带连接、云安全性和媒体交付有关的指标的海量数据。*互联网现状*计划旨在利用该数据，支持企业和政府机构更好地制定明智的战略决策。每个季度，Akamai 都会利用此数据发布以宽带连接和云安全性为重点的*互联网现状*计划报告。



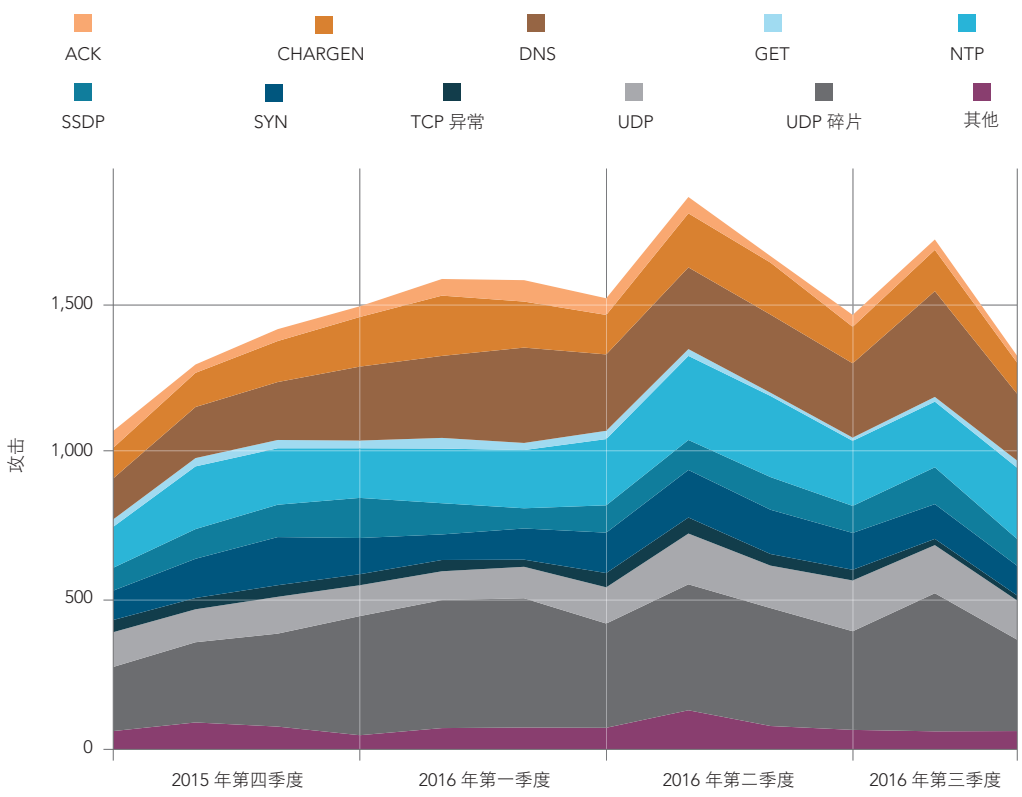
云安全 / *2016 年第三季度互联网现状/安全报告*将路由网络上的分布式拒绝服务 (DDoS) 攻击数据和来自 Akamai Intelligent Platform™ 的 Web 应用程序和 DDoS 攻击数据相结合。

DDoS 更新/ 该季度中最大规模的攻击数量几乎翻倍。两次 DDoS 攻击的规模达到 623 Gbps 和 555 Gbps 的新高，明显高于之前 363 Gbps 的纪录。这两次破纪录的攻击均针对网络安全作者和博主 Brian Krebs (www.krebsonsecurity.com)，近期发表作品之后，他成为 Mirai 僵尸网络的首要攻击目标。555 Gbps 攻击使用 ACK 泛洪和 NTP 反射攻击，但是 623 Gbps 攻击中的流量来源却不同寻常：一个基于恶意软件、名为 Mirai 的僵尸网络，由受感染的物联网 (IoT) 设备提供支持。

Mirai 僵尸网络的扩散方式类似于蠕虫，使用远程登录以及默认的用户名和密码感染设备，被感染的设备然后会接收攻击指令，同时扫描更多存在漏洞的设备。攻击方式包括 UDP、GRE、ACK、SYN、DNS、Valve Engine 和 HTTP 泛洪攻击。

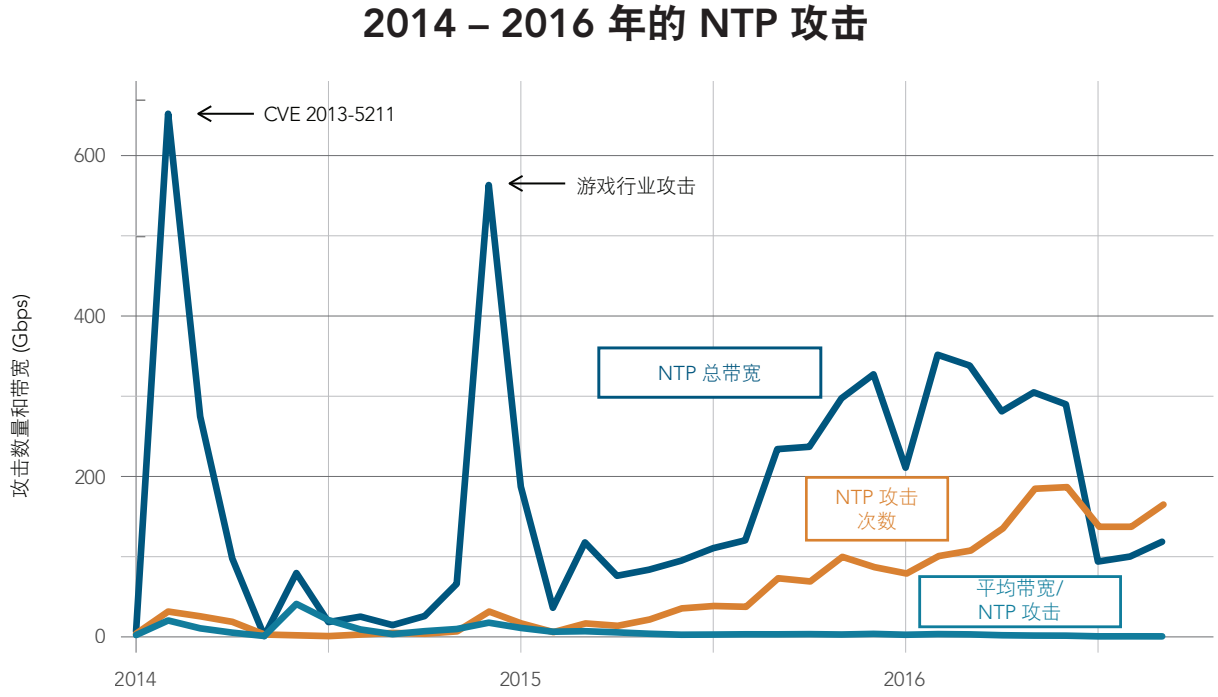
第一季度，峰值达到 100 Gbps 以上的攻击数量登顶，而第三季度再次发生了 19 次大型攻击。虽然本季度的攻击总数下降 8%，但是大型攻击的数量和规模均有增加。在 19 次大型攻击中，13 次攻击以媒体和娱乐行业为目标，4 次攻击以游戏行业为目标，2 次攻击以软件和科技行业为目标。

路由网络上的 DDoS 攻击总数达到 4,556，比去年第三季度上升 71%，但是比上一季度下降 8%。攻击总数下降诚然令人欣慰，但是这一趋势未必能够持久。长期以来，寒假期间 DDoS 攻击数量都有上升趋势，况且现在恶意攻击者还有了新工具，物联网推动的僵尸网络可能被再次利用。



虽然 8 月份的攻击数量猛增，但是第三季度的攻击总数少于 2016 年第二季度。

上一季度报告的 NTP 攻击比 2015 年第二季度增加了 276%。我们对本季度的分析显示，尽管攻击数量高，但是因为可用于恶意用途的未打补丁的 NTP 服务器数量持续减少，所以每次攻击所产生的流量大幅降低。在 2014 年假日季，NTP 泛洪攻击的平均流量超过 40 Gbps，而本季度的 NTP 攻击平均流量很少超过每秒 700 兆比特 (Mbps) – 带宽下降 98%。

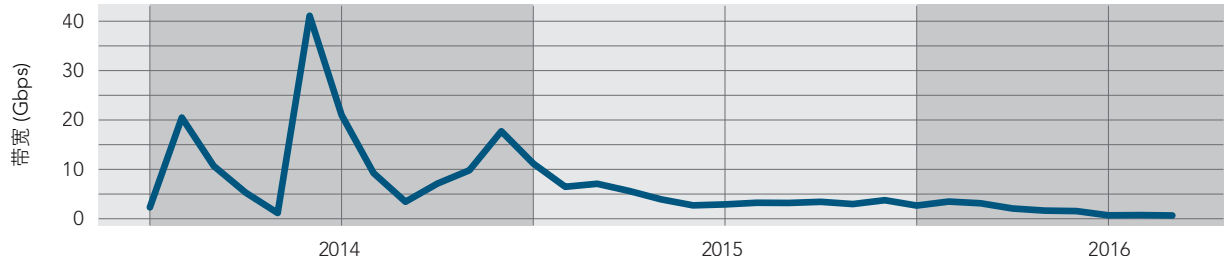


NTP monlist 漏洞的发布造成 NTP 攻击流量剧增，导致游戏公司在 2014 年 12 月遭受集中攻击

尽管 Mirai 僵尸网络在第三季度大量使用通用路由封装 (GRE) 泛洪攻击，但是在整个攻击环境中 GRE 所占比例仍然较小。不过，由于最近的攻击的曝光，GRE 泛洪攻击的普遍程度也有可能增加。不同于反射攻击，GRE 泛洪攻击高度依赖僵尸网络节点的性能，并且不支持放大攻击流量。

本季度数据标志着中国成为最大的 DDoS 攻击来源国已有一年。在第三季度中，30% 的 DDoS 攻击流量来自中国。但积极的一面是，来自中国的流量的比例下降了 56%，从而使攻击总数减少了 8%。美国、英国、法国和巴西均位列前五大攻击来源国。

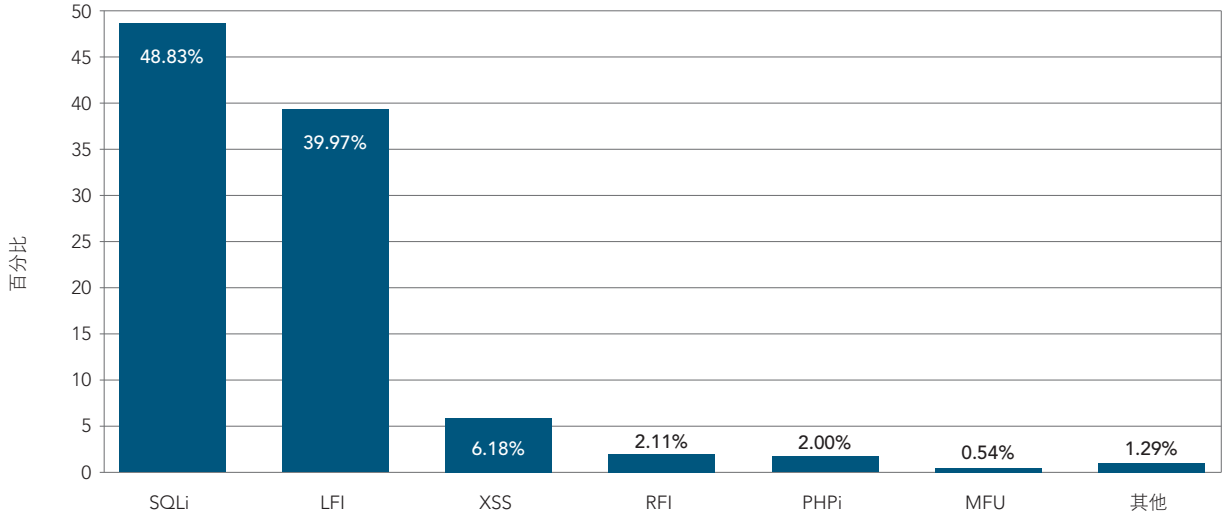
每个目标在本季度遭受的 DDoS 攻击平均数量增加至 30 次，这表明在第一次攻击之后，该组织非常有可能遭受另一次攻击——甚至有些组织几乎受到连续攻击。被列为头号目标的组织每天均遭受三到五次攻击。对于这些组织，每天发生数次短时间中断可能对其企业声誉造成严重的不良影响。



截至 2016 年 6 月，NTP 反射攻击带宽的减少程度导致僵尸网络所有者开始转换至其他协议

Web 应用程序攻击统计 / 尽管来自美国的 Web 应用程序攻击减少了 13%，但是美国仍高居攻击流量最大来源国榜首。上一季度高居首位的巴西已下降至第四位，仅次于荷兰和俄罗斯。荷兰以 18% 的攻击比例，出乎意料地成为第二大来源国。攻击者经常使用代理服务器来隐蔽 Web 应用程序攻击的来源。这些国家是所观察到的最后一个跃点的 IP 地址的来源。

美国仍然是 20% 的 Web 应用程序攻击的来源国，而 66% 的攻击以其为目标。



在观察到的 Web 攻击中，SQLi 占近 50%

三个向量占到本季度全部 Web 应用程序攻击的 95%：SQL 注入 (SQLi)、本地文件包含 (LFI) 和跨站点脚本攻击 (XSS)。远程文件包含 (RFI)、PHP 注入 (PHPi) 和恶意文件上传 (MFU) 各占 2% 或以下。

出于好奇，我们研究了大型体育赛事和 Web 应用程序攻击数量之间的关系。我们发现，在欧洲足球冠军联赛期间，与之后一个月相比，来自法国和葡萄牙的攻击分别减少了 68% 和 95%。在里约夏季奥运会期间也呈现了同样的趋势。在举办奥运会的 17 天时间里，来自巴西的攻击从一个月前同期的 730 万次减少到仅 100 万次。这是个有意思的现象，但是我们建议您在此类活动期间继续开启防火墙。

资源 / 访问 Akamai 提供的 2016 年第三季度网络安全资源：

1. Kaiten/STD 路由器 DDoS 恶意软件威胁报告
2. SSHowDowN 威胁报告：利用物联网设备发起大规模攻击活动

[互联网现状] / 安全性

互联网现状/安全团队

Martin McKeay，高级安全倡导者，资深编辑
Jose Arteaga，Akamai 安全智能响应团队
Amanda Fakhreddine，编辑
Dave Lewis，安全倡导者
Larry Cashdollar，Akamai 安全智能响应团队
Chad Seaman，Akamai 安全智能响应团队
Jon Thompson，自定义分析
Ryan Barnett，威胁研究部门
Ezra Caltum，威胁研究部门

设计

创意指导 Shawn Doughty
艺术指导/设计 Brendan O'Hara

联系方式

SOTIsecurity@akamai.com
Twitter：*@akamai_soti / @akamai*
www.akamai.com/StateOfTheInternet

下载完整报告

[互联网现状] / 安全性报告
2016 年第三季度

Akamai FASTER FORWARD

作为内容交付网络 (CDN) 服务的全球领军者，Akamai 竭力为客户营造高速、可靠、安全的互联网。公司先进的 Web 性能、移动性能、云安全性和媒体交付解决方案正在彻底改变企业在任何地点、任何设备上优化消费者、企业和娱乐体验的方式。要了解 Akamai 解决方案及其互联网专家团队如何帮助企业加快发展，请访问 ***https://www.akamai.com/cn/zh/*** 或 ***blogs.akamai.com***，或者扫描下方二维码，关注我们的微信公众号。

Akamai 总部位于美国马萨诸塞州的坎布里奇市，并且在世界各地 57 多个分支机构开展业务。我们卓越的服务和体贴的客户关怀使各企业能够为其全球客户提供无可比拟的互联网体验。所有分支机构的地址、电话号码和联系信息均列在 ***https://www.akamai.com/cn/zh/locations.jsp***。