CLOUDFLARE

Cloudflare DDoS 威胁报告

2023 年第二季度

内容

摘要

欢迎阅读 Cloudflare 针对 2023 年 4 月至 6 月推出的季度分布式拒绝服务 (DDoS) 报告。本报告根据 2023 年第二季度在 Cloudflare 全球网络中观察到的 DDoS 威胁形势，提供相关深入分析和趋势。

2023 年第二季度的特点是在多个方面发动了精心策划、量身定制和持续不断的 DDoS 攻击浪潮。

在 HTTP 层，我们检测到亲俄黑客组织 REvil、Killnet 和 Anonymous Sudan 对西方互联网网站的攻击行动非常活跃，并且低流量、高度随机化的 DDoS 攻击数量有所增加。在过去的一个季度里，基于 DNS 的 DDoS 攻击已经成为最常见的 DDoS 攻击手段——32% 的 DDoS 攻击针对 DNS 协议。在 UDP 层，我们观察到有利用我们在 2022 年 3 月披露的 zero-day 漏洞 (CVE-2022-26143, TP240PhoneHome) 进行的攻击。

除了具体的攻击活动之外，我们还对应用程序和网络层攻击趋势以及行业和地区变化进行了细分。最后，我们将介绍如何主动加强安全性，以便在不断发展的 DDoS 威胁环境中确保服务的连续性。

本报告的交互式版本可在 Cloudflare Radar 上查看。

报告要点

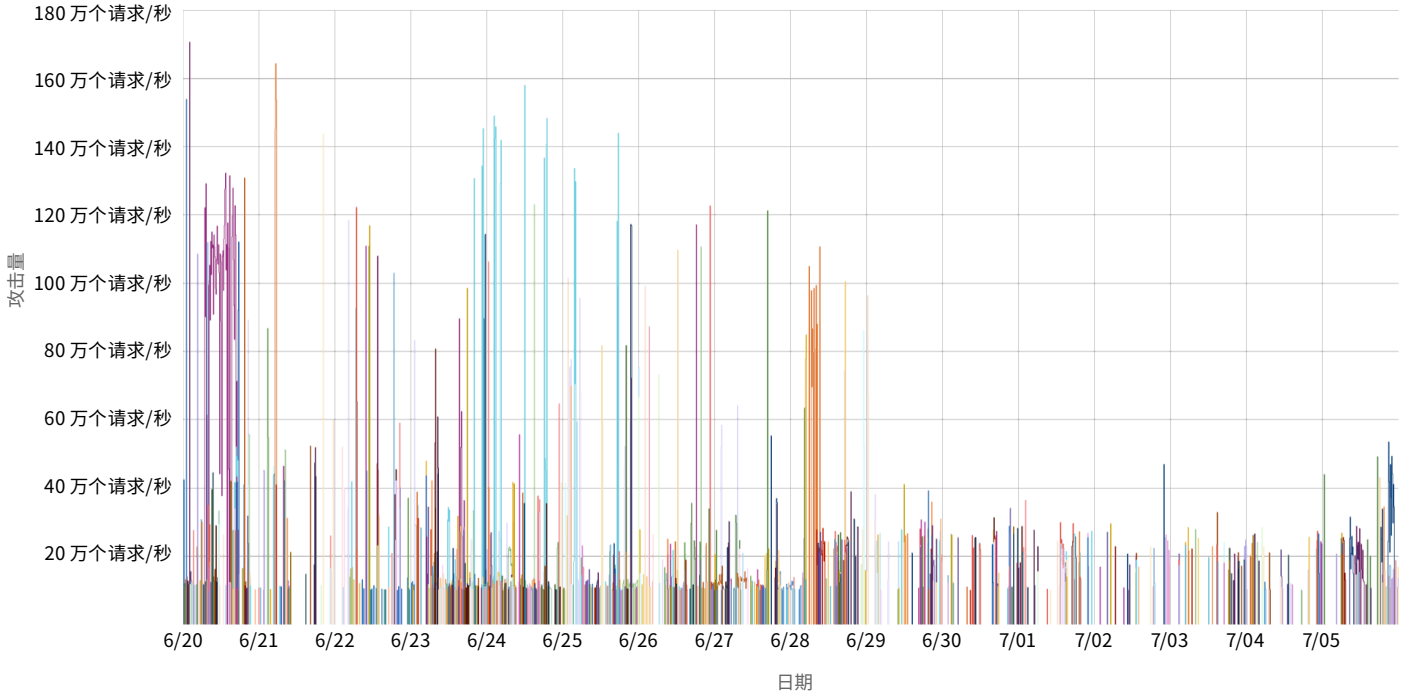
被称为“Darknet Parliament”（暗网议会）的黑客联盟正在行动

6 月 14 日，黑客组织 Killnet、以及再次活跃的 REvil 和 Anonymous Sudan 宣布会联合起来组成“Darknet Parliament”（暗网议会）。

他们宣称会对西方金融体系实施“大规模”网络攻击，目标包括西方的银行、美国联邦储备系统和 SWIFT 网络（环球银行金融电信协会）。

在本季度，暗网议会对受 cloudflare 保护的网站发起了多达 10,000 次 DDoS 攻击。然而，根据我们在这次活动中已经发现的针对我们客户的攻击，银行和金融服务网站仅是第九大受攻击最多的行业。我们的系统一直在自动检测和缓解与此活动相关的攻击。

在 2023 年第二季度，Killnet、REvil 和 Anonymous Sudan 对各行业发起了 10,000 次攻击



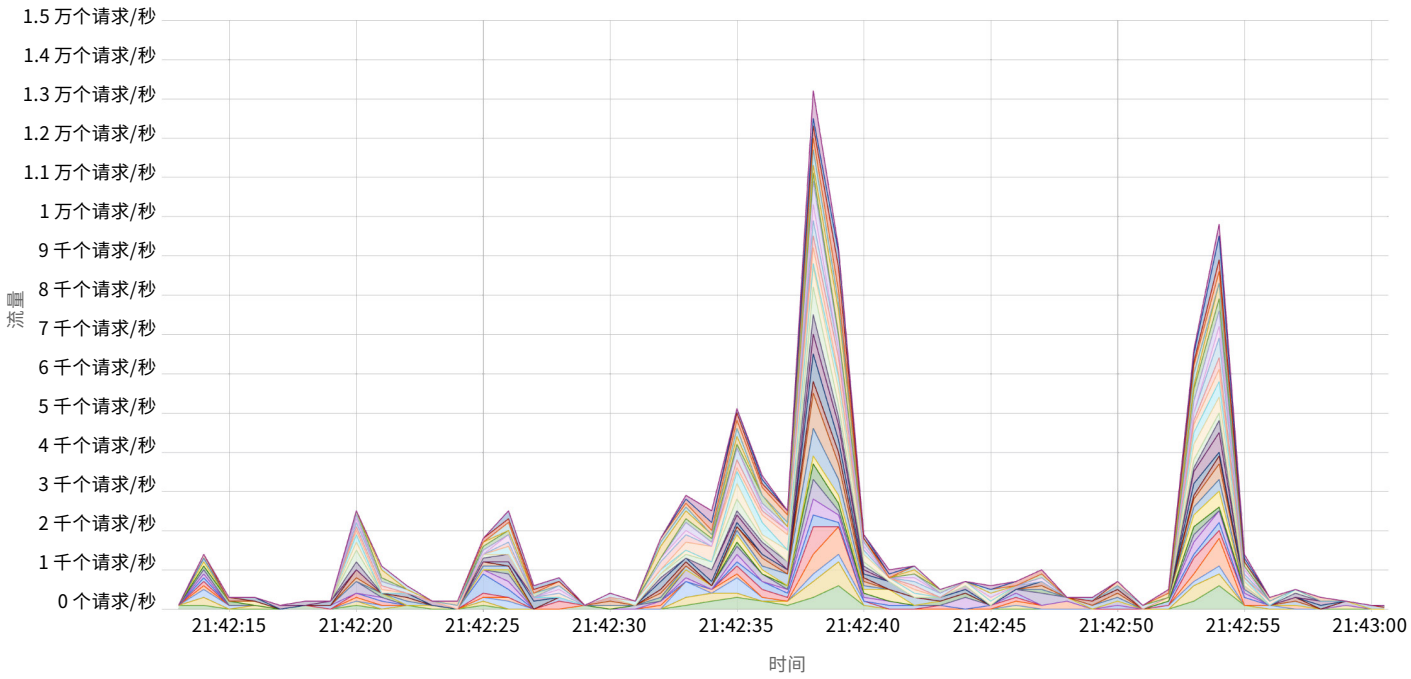
低流量、高度随机化的 HTTP DDoS 攻击

HTTP DDoS 攻击是通过超文本传输协议 (HTTP) 发动的 DDoS 攻击。其目标是 HTTP 互联网资产，如网站和 API 网关。在过去的几个月里，我们观察到低容量、高度随机化的 HTTP DDoS 攻击有所增加。这种策略过去主要是资金雄厚的政府黑客在使用。

这些攻击背后的威胁行为者似乎通过非常准确地灵活模仿用户的浏览器行为，特意设计攻击来攻克缓解系统。在某些情况下，他们在用户代理和 JA3 指纹等各种属性中引入了高度的随机化。

以下为此类攻击的一个示例。每种不同的颜色代表一个不同的随机化特征。

低容量、高度随机化的 HTTP DDoS 攻击随时间发生的 HTTP 流量变化



DNS 洗钱 DDoS 攻击

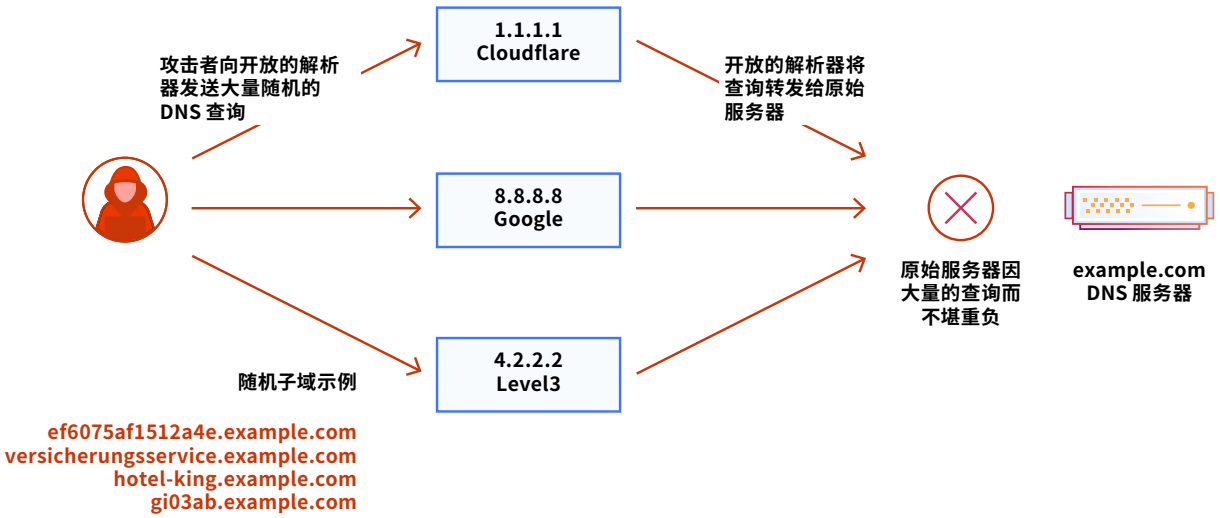
在过去的一个季度里，基于 DNS 的 DDoS 攻击已经成为最常见的 DDoS 攻击手段——32% 的 DDoS 攻击针对 DNS 协议。域名系统 (DNS) 相当于互联网的电话簿。DNS 帮助将对人类友好的网站地址（例如 www.cloudflare.com）转换为对机器友好的 IP 地址（例如 104.16.124.96）。通过中断 DNS 服务器，攻击者可以影响机器连接到网站的能力，并以此来让用户无法访问网站。

一种令人担忧且增长迅速的攻击是 DNS 洗钱攻击。这种攻击可能会给运行自有权威 DNS 服务器的组织带来严峻的挑战。DNS 洗钱攻击是通过信誉良好的递归 DNS 解析器将不良的恶意流量伪装成好的合法流量的过程。这就类似于让“赃款”合法的洗钱过程。

在 DNS 洗钱攻击中，威胁参与者将查询由受害者 DNS 服务器管理的域的子域。定义子域的前缀是随机的，在这种攻击中使用的次数绝不会超过一次或两次。由于这种随机性，递归 DNS 服务器将永远不会有缓存的响应，需要将查询转发到受害者的权威 DNS 服务器。然后，权威 DNS 服务器受到大量查询的轰炸，直到无法提供合法查询，甚至完全崩溃。

最近遭受这种攻击的受害者中包括一家亚洲大型金融机构和一家北美 DNS 提供商。来源包括信誉良好的递归 DNS 服务器，如 Google 的 8.8.8.8 和 Clouflare 的 1.1.1.1。受攻击的域是有效的，且必须为合法查询提供服务。因此，DNS 管理员无法封锁攻击来源，也不能阻止前往受攻击域的所有查询。区分合法查询与恶意查询相当困难。

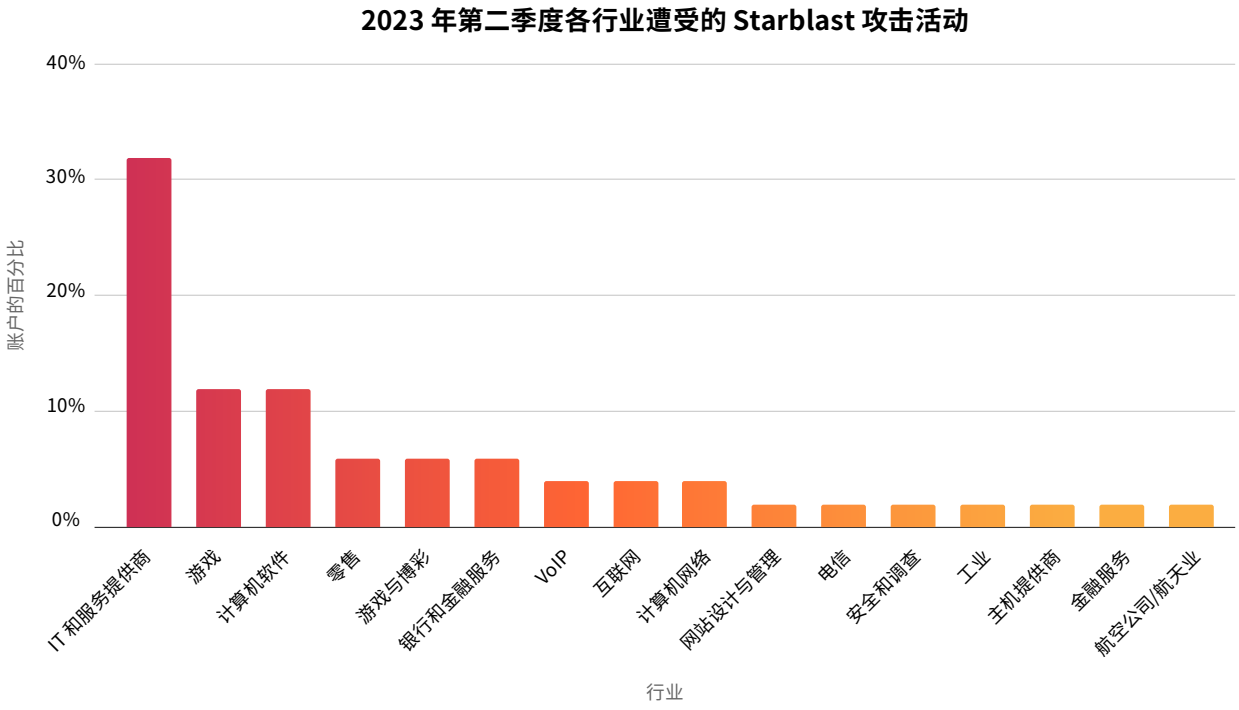
DNS 洗钱 DDoS 攻击的攻击链



“Startblast”：利用 Mitel 漏洞进行 DDoS 攻击

在 UDP 层，我们观察到有攻击利用了我们在 2022 年 3 月披露的 zero-day 漏洞 (CVE-2022-26143, TP240PhoneHome)。我们与 InfoSec 社区的成员一起，在 Mitel MiCollab 商务电话系统中发现了这一漏洞，它会使系统暴露于 UDP 放大 DDoS 攻击。

活动名称 “Startblast” 源自同名的调试命令，该命令对利用此漏洞至关重要。我们发现大多数攻击都是针对 IT 和服务提供商，而非游戏行业。在过去的一个季度中，这种攻击类型在网络层 DDoS 攻击中增长最为迅猛。



高性能僵尸网络的持续崛起

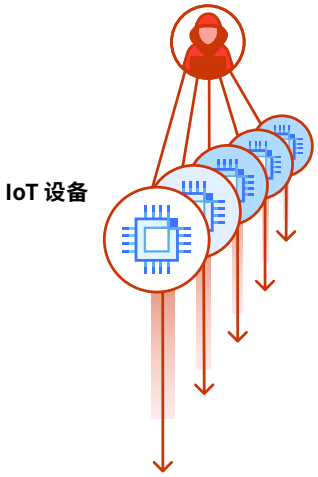
正如 Cloudflare 的 2023 年第一季度 DDoS 趋势报告中所述，我们将继续见证僵尸网络 DNA 的演变。基于虚拟机的 DDoS 僵尸网络时代已经到来，随之而来的是超大容量的 DDoS 攻击。这些僵尸网络由虚拟机 (VM) 或虚拟专用服务器 (VPS) 组成，而不是物联网 (IoT) 设备，这使其攻击能力强大得多，高达 5000 倍。

Cloudflare 正在与知名的云计算提供商积极合作，共同打击这些新型僵尸网络。我们已经看到初步成果：这些僵尸网络的重要组成部分已经丧失作用。自 2023 年第二季度以来，我们尚未看到进一步的超大容量攻击（达到 2023 年第一季度和之前的规模）。

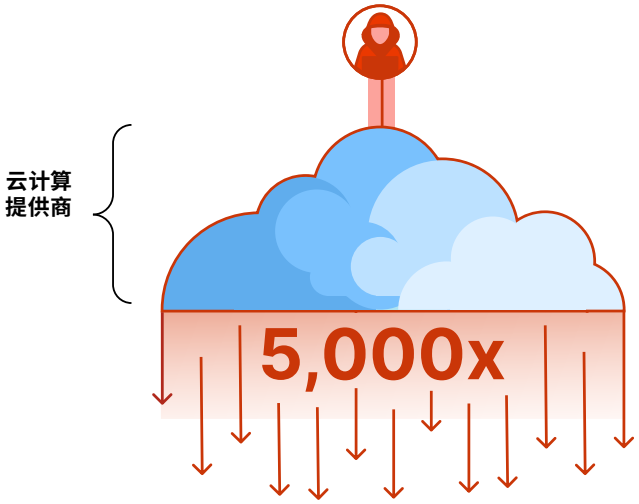
我们的目标是实现自动化并进一步扩大这种合作。我们要求云计算提供商、托管提供商和其他一般服务提供商加入 Cloudflare 的 Botnet Threat Feed。

这对提供商是免费的，并且我们不会将数据出售给第三方。这可以了解来自提供商自有网络的攻击，有助于我们合力瓦解僵尸网络。

基于 IoT 的僵尸网络攻击



基于 VPS 的僵尸网络攻击



主要 DDoS 趋势——2023 年第二季度

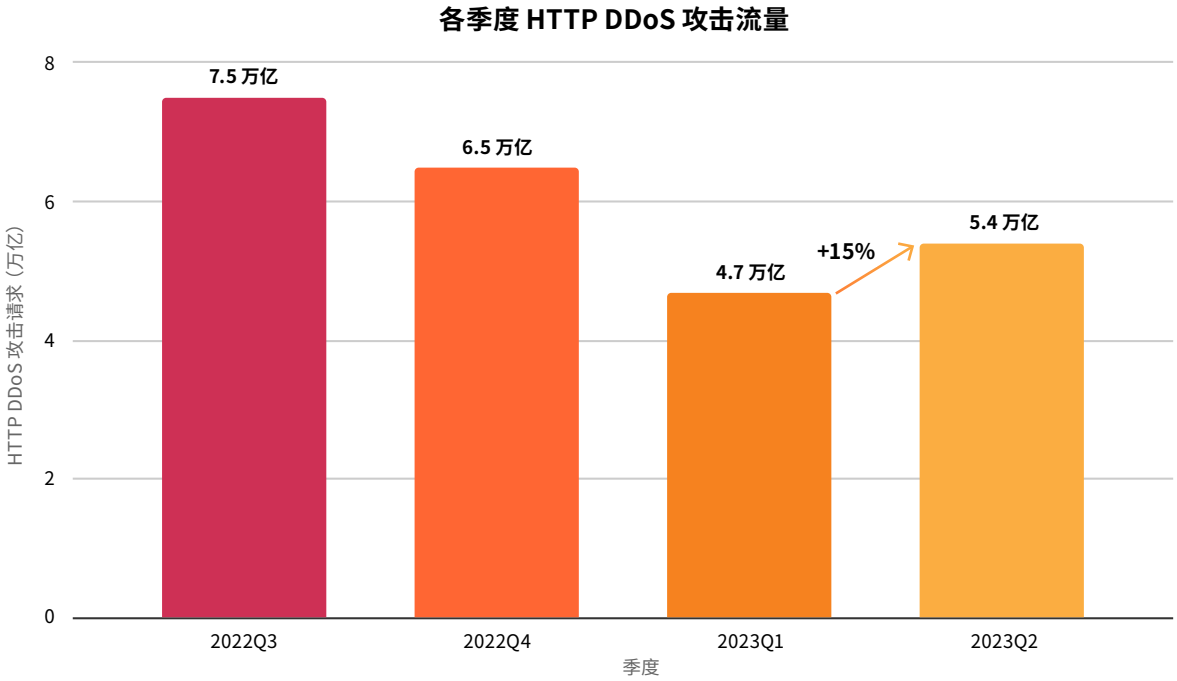
报告的以下部分将介绍有关攻击目标的主要趋势。

整体流量变化

与去年同期相比，2023 年前 6 个月应用程序层和网络层 DDoS 攻击分别下降了 35% 和 14%。Cloudflare 也希望能够继续保持这种逐年下降的趋势，因为 Cloudflare 和信息安全社区会让网络犯罪分子更加困难和痛苦。

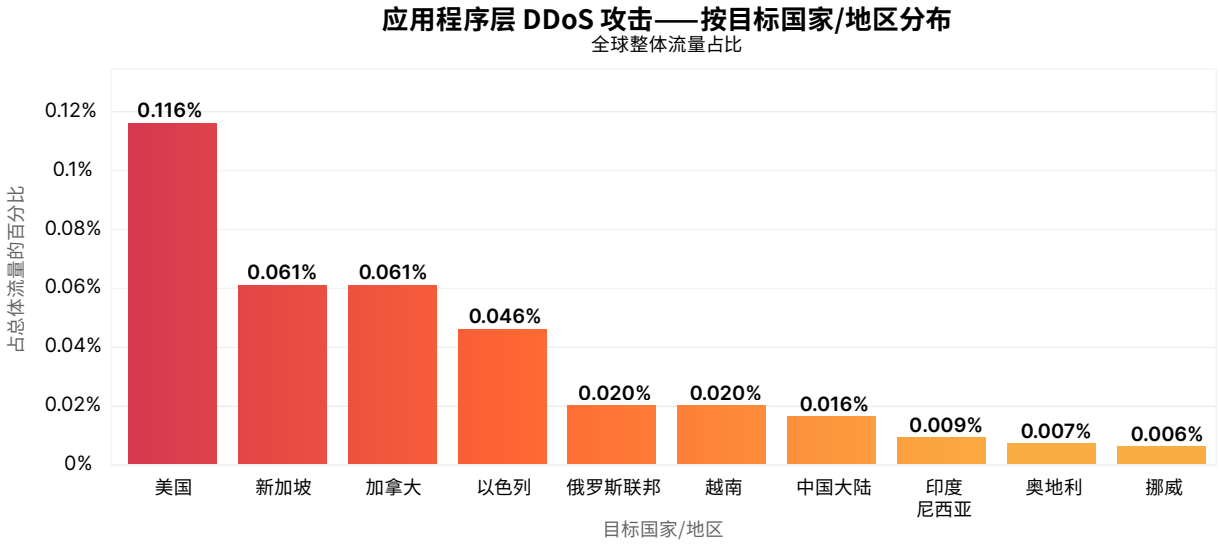
值得注意的是，我们确实看到 2023 年第二季度的应用程序层 DDoS 攻击比去年同期增加了 15%。我们需时刻严阵以待！

总体而言，HTTP DDoS 攻击同比下降了35%，但环比增长了 15%。此外，与上一季度相比，本季度网络层 DDoS 攻击减少了约 14%。



受攻击最多的国家/地区

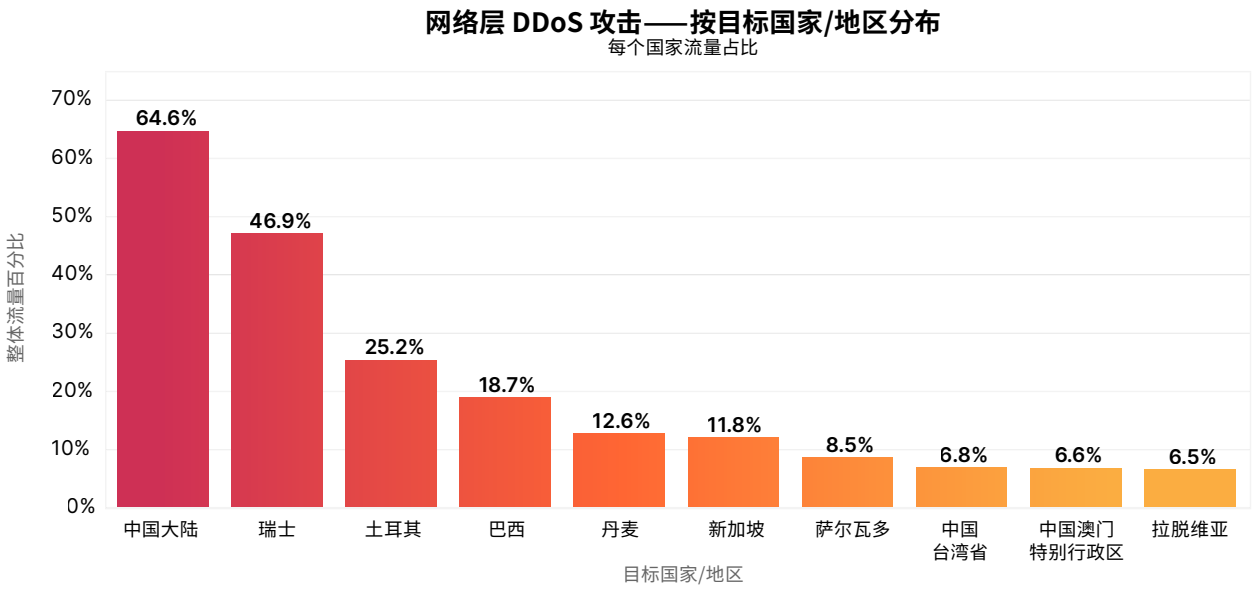
上个季度，我们报告了以色列是受应用程序层 DDoS 攻击最多的国家。本季度，美国的网站重新占据首位，新加坡和加拿大的网站分别位居第二和第三。针对以色列网站的攻击减少了 33%，使其排名下降到第四位。



⚠ **应用程序层 DDoS 攻击增加 2 倍**
美国受到的应用程序层 DDoS 攻击是第二名国家的两倍

⚠ **超过 10%**
在巴勒斯坦与圣基茨和尼维斯的全部应用程序层流量中，DDoS 攻击流量占比超过 10%

在网络层，中国再次成为网络层 DDoS 攻击最多的国家。在 2023 年第二个季度，前往中国网络的流量中，三分之二的字节携带 DDoS 攻击流量。而且我们已经看到，在多个季度中，流向中国的恶意流量份额都如此之高。2023 年第一季度中，芬兰网络中 83% 的字节携带 DDoS 攻击流量的独特态势在第二季度已经平息。芬兰已经退出了遭受 DDoS 攻击最多的前十个国家和地区之列。

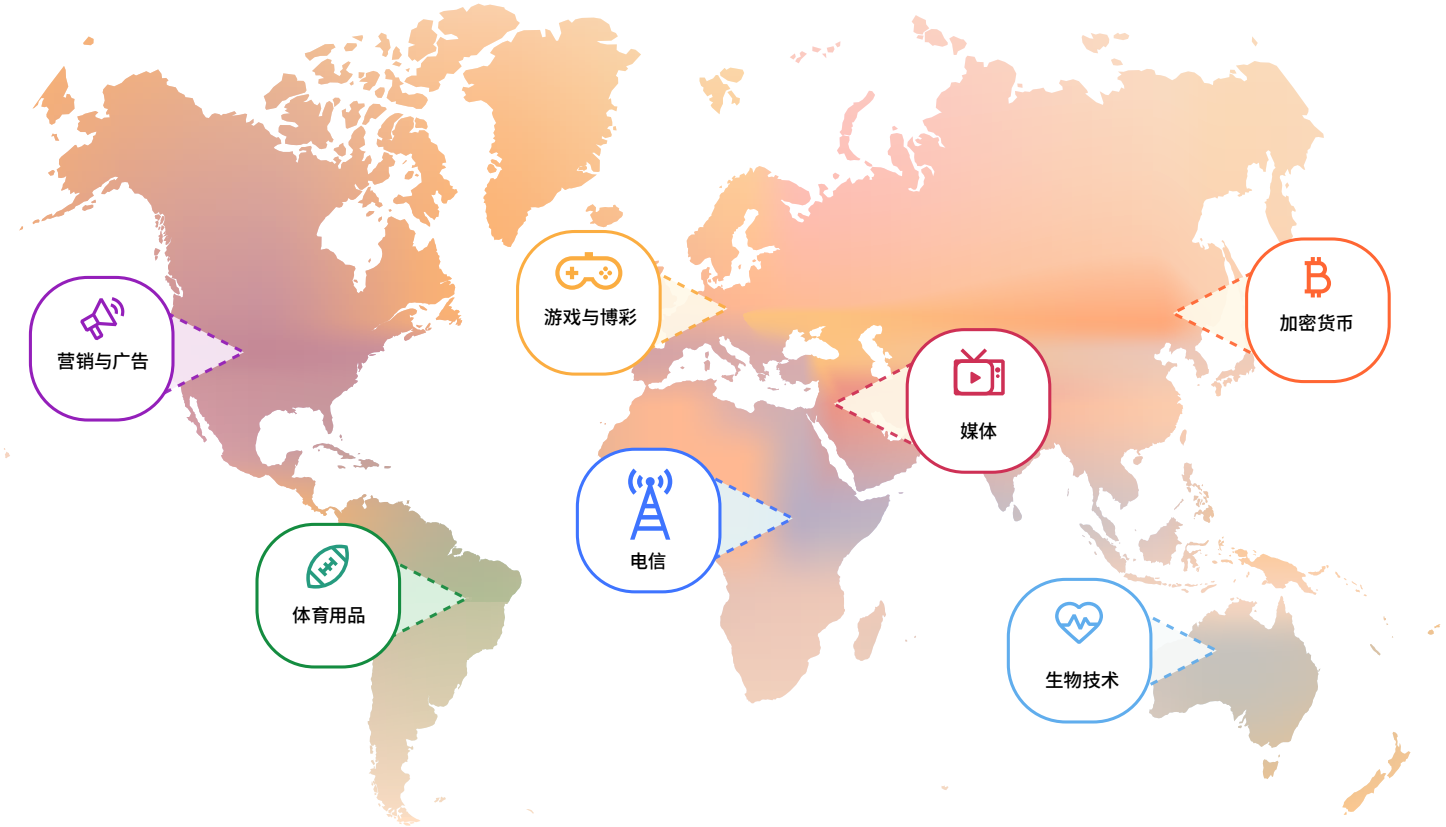


DDoS 攻击的行业和地区差异

在 2023 年第二季度中，加密货币网站成为 HTTP DDoS 攻击流量最大的目标。前往加密货币网站的 HTTP 请求中，每 1 万个就有 6 个属于这些攻击。这比上一季度增长了 600%。

游戏和博彩网站排名第二，与 2023 年第一季度相比，该行业在 2023 年第二季度的攻击份额增长了 19%。市场营销和广告网站紧随其后，排名第三，攻击流量占比变化甚微。

不幸的是，非营利组织正在面临着大量攻击。事实上，非营利组织的 HTTP 流量中有 12% 是 DDoS 攻击，在各行业中，流量份额高居第二位。作为 Galileo 计划的一部分，Cloudflare 为 111 个国家的 2271 个非营利组织提供保护，而今年已是该计划的第九周年。在过去的几个月里，平均每天有 6770 万起针对非营利组织的网络攻击。



按地区分的攻击主要目标行业

建议和关键要点

最佳实践	优化 Cloudflare 使用
更新或制定拒绝服务应对方案	您是否在安全作业中纳入了 Cloudflare 警报和威胁情报? 您是否知道在发生攻击时如何联系到所有必要的合作者? 他们是否接受过应对计划相关的培训?
部署威胁情报和内嵌的自动化 DDoS 缓解解决方案。	使用多种检测技术应对本报告中列出的攻击趋势: 1. 动态无状态指纹识别 2. 基于机器学习的分类 3. 异常流量检测 4. 流量分析和具状态缓解 5. 关于当前 DDoS 活动和趋势的威胁情报
更新您的基础结构以便灵活地适应您的流量状况。 **提高网络和应用程序性能，从而避免瓶颈。**	确保 DDoS 缓解工具的容量足够大，能够处理有记录以来最大攻击两倍大小的攻击，以及合法流量最大速率两倍大小的流量。 当受到攻击时，自动减少 HTTP/2 多路复用上限，从而启用 WAF 利用数字 Waiting Room 优化缓存，使用内容分发网络 (CDN) 和基于云的负载平衡解决方案更好地管理负载。
使用积极的安全模型：确保需要的流量能够可靠地进入。	确保业务关键型和正在使用的端口开放 对 API 流量使用模式验证和 API 网关
利用威胁情报和人工智能提前应对新兴威胁	可以在防火墙和速率限制规则中使用的机器人评分

Cloudflare 致力于为各种规模的组织提供更简便且免费的方式，以保护他们免受最大、最复杂的 DDoS 攻击侵害。2017 年以来，我们向所有客户免费提供不计量和无限的 DDoS 防护，开创了先河。

欢迎观看 DDoS 趋势网络研讨会，以进一步了解新兴 DDoS 威胁及如何防御。

010 8524 1783 | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-4839.2023AUG28