CLOUDFLARE

报告

2024 年应用安全趋势

目录

摘要

目录

Web 应用是现代生活的核心。对政府而言，它们是向公众传达信息和提供基本服务的重要途径。对企业来说，它们是收入、效率和客户洞察的来源。

然而，移动关键数据、流程和基础设施的应用和应用编程接口 (API) 也代表着一个不断扩大的攻击面。未受保护的应用遭到利用可能导致业务中断、财务损失和关键基础设施崩溃。

开发人员需要快速交付新功能，例如由大型语言模型 (LLM) 和生成式 AI 驱动的能力，放大了这个问题。

Cloudflare 由世界上最大的网络之一驱动，平均每秒处理超过 5700 万个 HTTP 请求，每天阻止 2090 亿次网络威胁。这一流量的体量、速度和多样性为本《**2024 年应用安全趋势》报告中探讨的洞察提供了信息。**

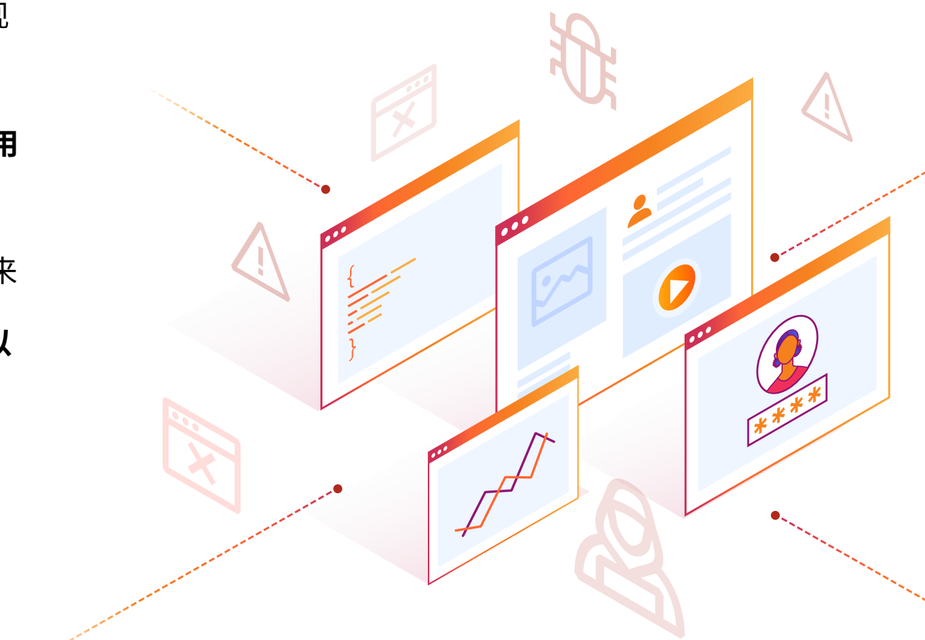
例如，DDoS 攻击的速度和数量不断增加，表明**僵尸网络越来越多被用于发动 DDoS 攻击，效率也越来越高。**而 DDoS 攻击是针对 Web 应用的第一大攻击类型。您的团队是否具备适当的能力，以检测和阻止由数十万、甚至数百万台机器组成的恶意僵尸网络发送的流量？

此外，某些行业**面临更大比例的机器人流量。**其他行业发现自己成为**大量 DDoS 攻击的目标。**您能以多快的速度响应这些威胁，以避免财务损失和声誉损害？

Cloudflare 还发现，截至 2024 年 5 月，**企业和组织平均使用 47.1 个第三方脚本。**您的组织是否无意中使最终用户暴露于供应链风险中？

随着新的应用风险超出专门应用安全团队的资源范围，越来越多组织意识到需要采取不同的方法。Gartner® 预测 **“到 2027 年，30% 的网络安全功能将重新设计应用安全性，以供非网络专家直接使用，并由应用所有者负责。”**

不管您的组织如何处理应用安全问题，我们都希望这份报告可以指导您在哪些地方优先考虑未来的应用安全控制——而不会抑制数字创新。



应用安全领域的关键发现

数据收集期间：除非尾注中另有说明，否则本报告评估的时间范围为 2023 年 4 月 1 日至 2024 年 3 月 31 日的 12 个月期间。

头号攻击

分布式拒绝服务 (DDoS) 攻击仍然是针对 Web 应用的最常见攻击类型之一，在 Cloudflare 缓解的所有应用层流量中占 **37.1**。[1]

CVE 快速武器化

一个新 zero-day 漏洞的概念验证 (PoC) 发布**仅 22 分钟**后，Cloudflare 就观察到尝试利用。[2]

对第三方代码的信任

Enterprise 和组织**平均使用 47.1 个第三方脚本**——其 Web 应用平均向第三方资源进行 **49.6 个出站连接**。[3]

93% 的机器人可能是恶意的

约三分之一 (31.2%) 的流量来自机器人，其中**大多数 (93%) 未经验证**并可能存在恶意。[4]

过时的 API 安全方法

传统的 Web 应用防火墙 (WAF) 规则最常用于保护 API 流量[5]；然而，传统的 WAF 负面安全模型方法**不足以**抵御现代 API 威胁。

Cookie 同意风险

企业网站**平均使用 11.5 个 HTTP cookie**，中位数为 5 个。[6]这些 HTTP Cookie 可能会使最终用户面临隐私风险，应用的所有者有责任监控和最小化这些风险。

范围和报告方法

目录

总体而言，Cloudflare 在数据收集期间缓解了所有 Web 应用流量的 6.8%。[7] “缓解”流量定义为任何被 Cloudflare 阻止或质询的流量（完整技术定义请参阅术语表）。具体的威胁类型和相关缓解技术取决于许多因素，例如应用的潜在安全漏洞、受害者业务的性质以及攻击者的目标。

2023-2024 年期间针对 Web 应用和 API 的攻击部分例子：

- Anonymous Sudan 组织出于政治动机，在全球范围内对银行、大学、医院、机场、社交媒体平台、政府机构和其他机构发动了 DDoS 攻击。
- Cloudflare 观察到一次创纪录的 DDoS 攻击，其利用了 HTTP/2 协议的一个漏洞，由一个僵尸网络发起，其中仅有 2 万台机器，它们不断更换 IP 地址以逃避缓解措施。
- T-Mobile 于 2023 初披露，一个被利用的 API 导致 3700 万个客户账户信息泄露。

换句话说：此类攻击的多样性使 Web 应用安全成为一个广泛的学科，但仍需要专门的工具来阻止专门的攻击。

为了涵盖如此广泛的范围，本报告基于 Cloudflare 全球网络上的聚合流量模式（2023 年 4 月 1 日至 2024 年 3 月 31 日期间），包括以下服务：

- 使用各种安全措施过滤 Web 应用和互联网之间的 HTTP 流量，以阻止广泛的实时攻击 *（Web 应用防火墙）*
- 缓解针对域名系统 (DNS) 服务器的 DDoS 攻击 *（高级 DDoS 防护）*
- 充当接受、转换、路由和管理所有 API 调用的中介 *(API Gateway)*
- 监控 Web 应用在客户端浏览器加载并使最终用户面临风险的第三方依赖 *(Page Shield)*
- 识别机器人活动、机器人信誉、机器人来源和其他机器人行为 *（机器人管理）*
- 阻止用户、机器人或应用过度使用或滥用 Web 资产 *（速率限制）*

以上来自 Cloudflare 网络的数据和威胁情报得到第三方来源的补充，读者可以使用内联链接访问这些来源。

缓解流量的趋势

与前一个 12 个月期间相比，2023 年第二季度至 2024 年第一季度，**Cloudflare 缓解的应用层流量和第 7 层 (L7) DDoS 攻击比例有所上升 (6.8% vs 6%)**。[8]

WAF 产品缓解也成为第一大缓解技术——取代了此前 DDoS 防护的地位。

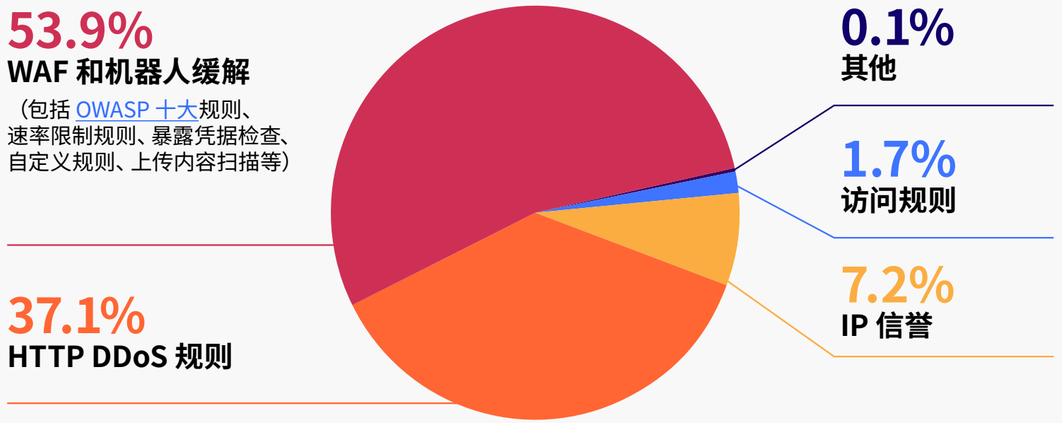
缓解技术排名之所以发生变化，可能是因为更多企业使用 WAF 规则来阻止暴力攻击或凭据填充，并防止应用泄露敏感数据，或者使用 Cloudflare 的机器学习在披露前阻止 zero-day 漏洞利用企图。

WAF 规则还包括**自定义规则，**这有助于实施组织策略并执行其他自定义缓解措施。

部分自定义规则的常见用例包括：

- 允许来自搜索引擎机器人的流量
- 仅允许来自特定国家/地区的流量
- 质询恶意机器人
- 配置令牌身份验证
- 要求特定 Cookie

图 1：Cloudflare 产品组别缓解的流量[9]



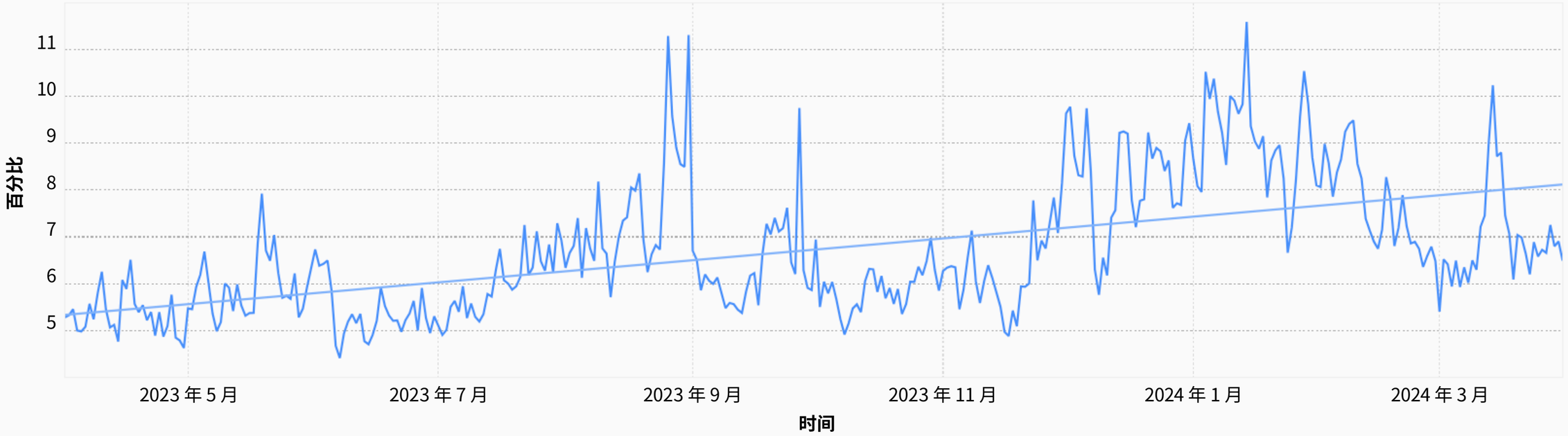
有关这些缓解类型的定义请参阅术语表。

数据快照：缓解流量随时间变化的情况

目录

在截至 2024 年 3 月 31 日的 12 个月内，Cloudflare 观察到缓解流量（也就是攻击流量）总体上有所增加。我们还发现今年的攻击流量在 2024 年 1 月出现激增但寒假期间的峰值低于预期。

图 2：2023 年第二季度至 2024 年第一季度 Cloudflare 全球网络缓解的 HTTP 流量百分比[10]



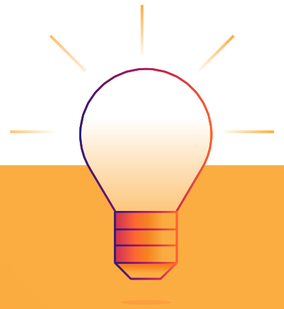
商业考量和建议

目录

流量有增无减，这是因为企业继续现代化传统应用或发布新应用以：

- 为全球分布的数据和用户提高应用性能
- 将传统应用迁移到云、混合或多云环境
- 通过 AI 驱动的洞察、建议和信息增强用户体验
- 现代化后台流程和功能
- 从各种不同的工具中构建开发管道，以便开发人员专注于编码

由业务驱动的应用开发不能放缓；因此，阻止、质询和限制（即缓解）恶意或无用 Web 应用流量的需求将可能出现增长。



建议

为了帮助降低与扩展基础设施以服务应用增长相关的成本，企业应该**考虑在边缘提供应用内容和缓解攻击。**（根据一组 Cloudflare 客户自行报告，其通过在边缘提供和缓解流量平均节省了大约 30% 的基础设施成本。）[11]

zero-day 趋势

zero-day 漏洞利用（也称为 zero-day 威胁）正在增加，已披露 CVE 的武器化也在加快。

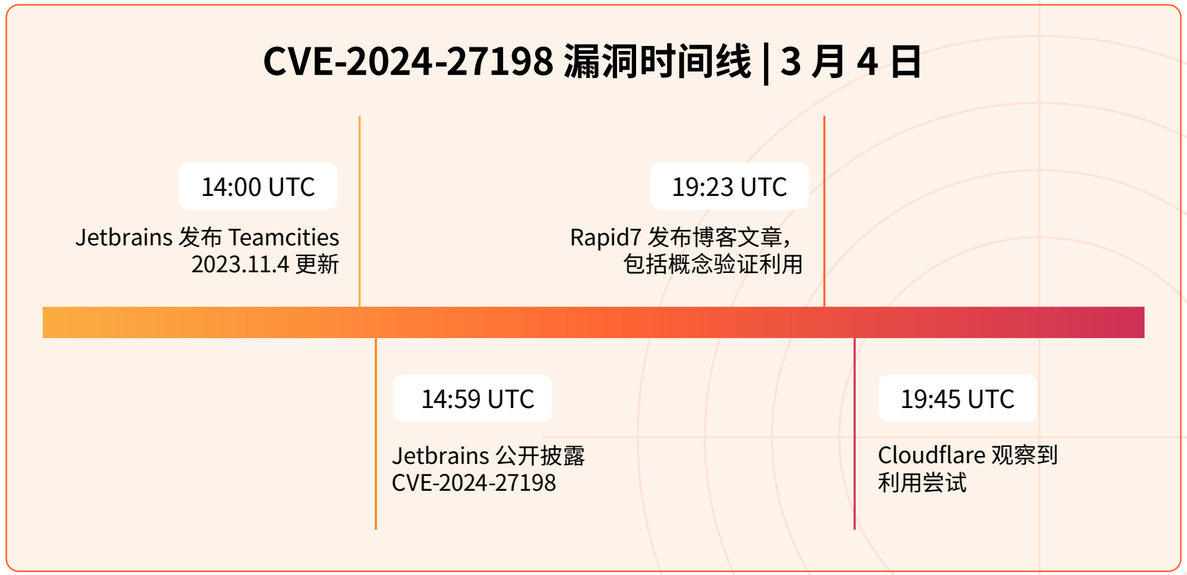
- 2023 年，**97 个 zero-day** 漏洞在实际网络环境中遭到利用
- 2022 年至 2023 年期间披露的 CVE 数量增加了 15%
- 2023 年，超过 5000 个严重漏洞被披露，但针对高危 Web 应用漏洞发布补丁的平均时间为 35 天

从针对客户的 CVE 利用尝试来看，Cloudflare 主要观察到**扫描活动**，其次是**命令注入**，以及一些针对线上存在 PoC（例如 Apache、Coldfusion、MobileIron）的**漏洞利用尝试**。[1][2]

CVE 利用尝试活动的这一趋势表明，攻击者首先瞄准最容易的目标，而鉴于围绕老漏洞的持续活动，在某些情况下可能取得成功。

已披露 CVE 漏洞被利用的速度通常快于人类创建 WAF 规则或创建和部署补丁以缓解攻击的速度。

例如，Cloudflare 在 3 月 4 日 19:45 UTC 观察到对 CVE-2024-27198 的利用尝试时，**距离概念验证代码发布仅 22 分钟。**



商业考量和建议

目录

根据定义，zero-day 是指还没有相应补丁可用的漏洞。漏洞披露后，安全专家和攻击者之间就会展开一场保护和利用应用之间的竞赛。

在新型攻击手段造成问题前越快发现和予以缓解，内部团队就有越多时间来修补和解决相应漏洞。然而，有时 CVE 补丁可能要等好几个小时（甚至几天或几个月）才发布。

建议

资源紧张的组织应该**优先处理高风险和正在被利用的漏洞，并使用提供自动规则更新的 Web 应用防火墙 (WAF) 部署**，以保护那些无法及时修补的应用。

WAF 机器学习 (ML) 模型使得更容易在某些 zero-day 利用被公布和漏洞被披露之前予以阻止。

例如，对于 2023 年 6 月首次披露的一些 Sitecore CVE，最初未被 Cloudflare 托管规则识别——但它们被我们基于机器学习的分类器在“零时间”内正确检测和分类。Cloudflare 还在漏洞被公开披露之前就阻止了 Ivanti Connect Secure 漏洞。

DDoS 攻击趋势

目录

图 3：不同时间段内的应用层 DDoS 攻击体量[13]
全球 - 数据日期范围从 2023-04-01 到 2024-03-31

DDoS 攻击仍然是针对 Web 应用的最常见攻击类型，**在缓解应用流量中占 37.1**（参见图 1）。[9]

我们在 2024 年 2 月和 3 月观察到容量耗尽攻击大幅增加。[13] 仅在 2024年第一季度，Cloudflare 的自动防御系统就缓解了 450 万次 DDoS 攻击，相当于 Cloudflare 在 2023 年缓解 DDoS 攻击总数的 32%。

具体而言，应用层 HTTP DDoS 攻击同比增长 93%，**环比增长 51%。[14]**

例如，2024 年 3 月 7 日瑞典加入北约后，Cloudflare 观察到针对瑞典的 DDoS 攻击增加了 466%。这与 2023 年芬兰加入北约时观察到的 DDoS 模式一致。[15] **DDoS 攻击本身的规模也在增长，如下页所示。**

数据快照: 最大规模的 HTTP DDoS 攻击

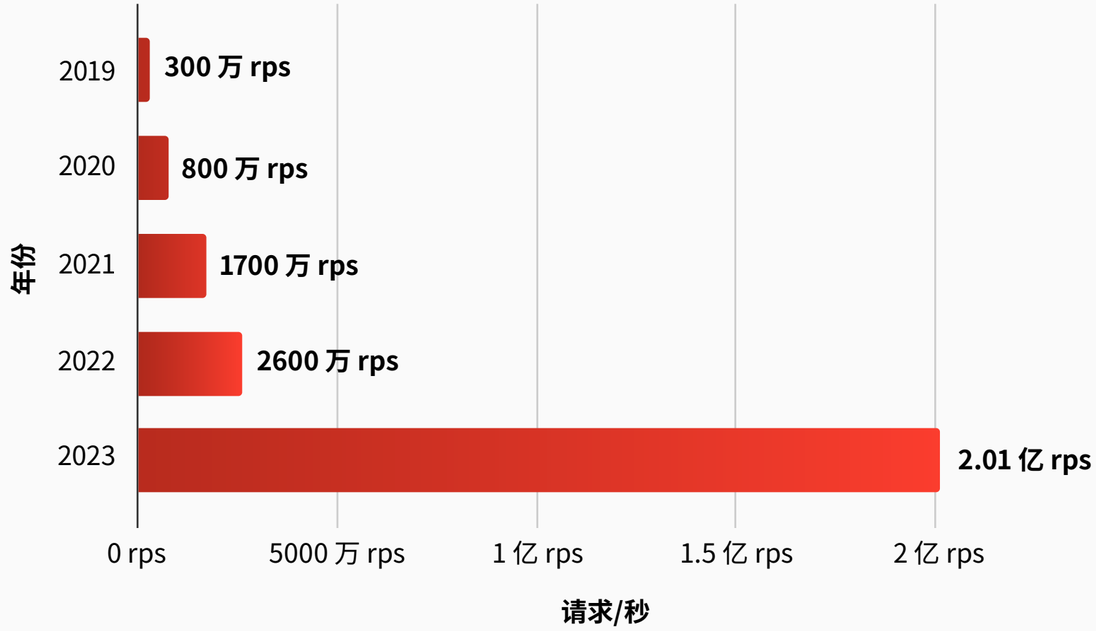
目录

2023 年，Cloudflare 缓解了一次**超大容量的 DDoS 攻击，其峰值达到每秒 2.01 亿个请求 (rps)**——三倍于以往观察到的最大攻击。[16]

在“HTTP/2 Rapid Reset”攻击中，威胁行为者利用了 HTTP/2 协议中的一个 zero-day 漏洞。HTTP/2 协议对互联网和所有网站的工作至关重要。

这一漏洞利用有可能使几乎所有支持 HTTP/2 的服务器或应用瘫痪，凸显了利用漏洞发动的 DDoS 攻击对未受保护的企业有多大威胁。

图 4: Cloudflare 观察到的最大 HTTP DDoS 攻击 (按年)



来源: Cloudflare 2023 年第四季度 DDoS 威胁趋势报告[17]

商业考量和建议

目录

HTTP/2 Rapid Reset 和其他大型 DDoS 攻击表明，目前 DDoS 攻击由僵尸网络更高效地发动。

例如，网络犯罪团伙在暗网上以低廉的价格提供 DDoS 即服务，甚至提供 “订阅和节省” 套餐及支持档次。

截至 2023 年，许多提供 DDoS 即服务的网站对持续一小时的 DDoS 攻击收费低至 10 美元，而使用其僵尸网络一整天收费 35-170 美元。

鉴于发动 DDoS 攻击变得如此简单，以下行业的企业应特别警惕并维持高级 DDoS 防护。

图 5：受到最多 L7 DDoS 攻击的行业（基于占总体互联网流量的比例）[18]

1	游戏/泛娱乐
2	IT 和互联网
3	加密货币
4	计算机软件
5	营销和广告
6	电信
7	零售
8	成人娱乐
9	银行、金融服务和保险
10	制造业

商业考量和建议（续）

目录

对于由公共云提供的 DDoS 保护，云服务提供商通常位于组织的应用和基础设施前，将所有流量引导到一个清洗中心进行“清洗”。仅合法流量会发回给客户。

这个操作可以“按需”或“始终开启”方式激活。但是通常存在以下限制：

- 按需云清洗依赖于人工干预，增加了缓解响应时间。提供商也可能按攻击流量的字节数收费，成本随时间推移而增加。
- 许多始终开启的 DDoS 供应商依赖远程清洗中心，这可能会导致明显的延迟。

建议

要实现基于云的 DDoS 防御的全部优势，请寻找具备如下能力、可扩展和“始终开启”的服务：

- 尽可能靠近攻击源的地方自动吸收恶意流量，以减少终端用户延迟和业务停机时间
- 不计量、无限制的 DDoS 攻击缓解，不会因攻击流量激增而额外收费
- 针对所有 DDoS 攻击类型的集中式自主保护

机器人流量趋势

平均而言，Cloudflare 处理的所有应用流量中，机器人占三分之一（31.2%）。[19] 这一比例在过去三年中保持相对稳定（徘徊在 30% 左右）。

“机器人流量”一词可能带有贬义，但实际上机器人流量不一定是好是坏；它完全取决于机器人的用途。一些机器人是“善意的”，执行所需的服务，例如客户服务聊天机器人和授权的搜索引擎爬虫。但一些机器人滥用在线产品或服务，需要予以阻止。

不同的应用所有者可能对他们认为的“恶意”机器人有不同的标准。例如，一些组织可能希望阻止竞争对手为降低价格而部署的内容抓取机器人，而一个不销售产品或服务的组织则可能不那么关心内容抓取活动。Cloudflare 将已知、善意的机器人归类为“经验证机器人”。

然而，我们发现的机器人中，绝大多数 (93%) 是未经验证的机器人，并且可能是恶意的。[20]

未经验证的机器人通常是为破坏性和有害目的而创建的，例如囤积库存、发动 DDoS 攻击或试图通过暴力破解或凭据填充方式接管帐户。（已验证机器人是已知安全的机器人，例如搜索引擎爬虫）。

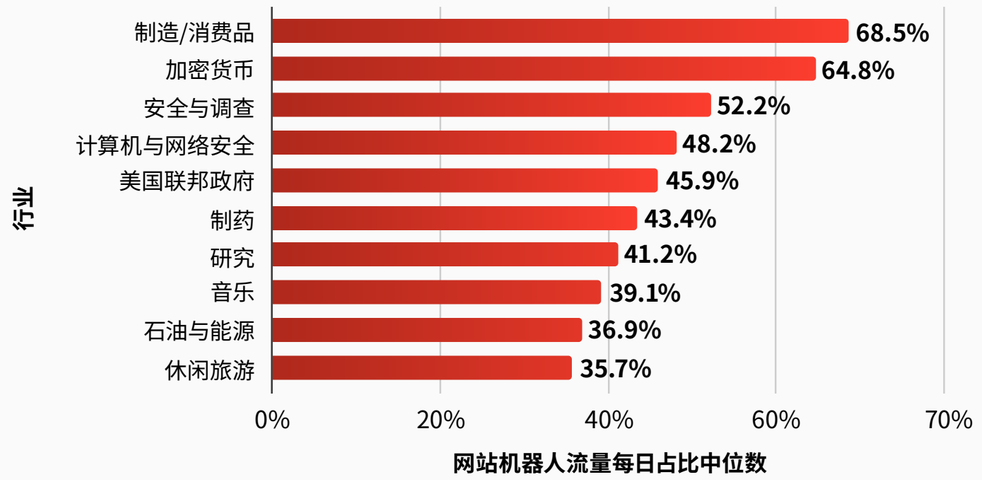
恶意机器人——如不加以阻止——可能会导致严重的问题：

- **性能影响：**过多的机器人流量会给 Web 服务器带来沉重的负担，减慢或拒绝对合法用户的服务。
- **业务中断：**机器人可以快速从网站抓取或下载内容，传播垃圾内容或囤积线上商店库存
- **数据盗窃和账户接管：**机器人可以窃取信用卡数据、登录凭据并接管账户

数据快照：具有高机器人流量的行业

利用机器人的攻击者主要关注那些可能为他们带来高额财务收益的行业。

图 6：机器人流量每日占比中位数最高的行业[21]

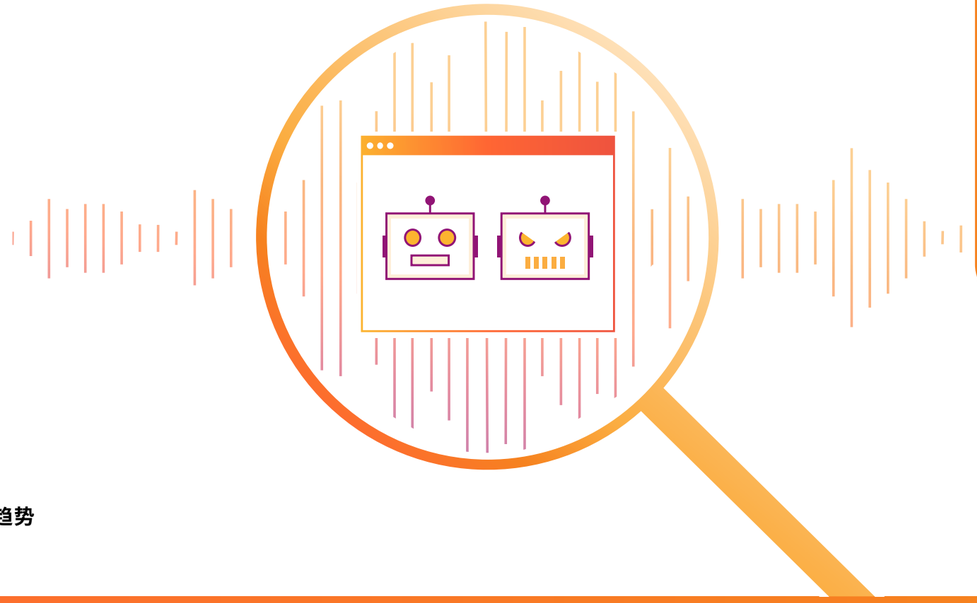


商业考量和建议

目录

如上图所示，在分析哪些行业面临最大的机器人问题时，我们发现**制造和消费品企业网站处理的所有流量中有惊人的 68.5%** 来自机器人。[21]

我们的发现证实了消费品行业零售商观察到的情况（例如，在人类还未来得及将鞋子或游戏主机放入购物车之前，库存囤积机器人就已经将货品抢购一空），损害了品牌信任。另一方面，在线销售实物商品较少的行业，例如保险或酒店业，所处理的机器人流量比例更接近互联网平均水平——31.2%。[21]



建议

如果您所在的行业往往会面临更多机器人流量，请考虑**增加对机器人管理的投资**，以先发制人地阻止凭据填充、内容抓取、垃圾内容、库存囤积和来自恶意机器人的其他威胁。

寻找具备以下功能的机器人管理服务：

- 通过对海量多样化的数据应用行为分析、机器学习和指纹识别技术，规模化**准确识别机器人**
- 与企业的其他 Web 应用安全和性能服务（例如 WAF、CDN、DDoS）**轻松集成**
- **允许好的机器人**（例如属于搜索引擎的机器人）继续到达您的网站，同时将恶意流量拒之门外

客户端风险

大多数组织的 Web 应用依赖于来自第三方提供商的不同程序或代码片段（通常为 JavaScript 形式）。使用第三方脚本可加速现代 Web 应用的开发，并允许组织更快地将功能推向市场，而无需自行构建所有新的应用功能。

数据快照：第三方脚本和 Cookie 使用情况

事实上，Cloudflare 的典型企业客户平均使用 **47.1 个第三方脚本，中位数为 20.0 个第三方脚本**。[22] 由于 SaaS 提供商通常有数千个子域，平均值远高于中位数。**以下是 Cloudflare 客户最常使用的一些第三方脚本：** [23]

- Google (Tag Manager, Analytics, Ads, Translate, reCAPTCHA, YouTube)
- Meta (Facebook Pixel, Instagram)
- Cloudflare (Web Analytics)
- jsDelivr
- New Relic
- Appcues
- Microsoft (Clarity, Bing, LinkedIn)
- jQuery
- WordPress
- Pinterest
- UNPKG
- 抖音
- Hotjar

第三方软件依赖虽然有用，但它们通常由最终用户的浏览器直接加载（即在客户端加载），使组织及其客户面临风险，因为组织无法直接控制其安全措施。例如，在零售领域，根据 Verizon 的 2024 年数据泄露调查报告，18% 的数据泄露事件源自 Magecart 式攻击。

平均而言，每个网站有 **49.6 个到 JavaScript 函数及其目的地的连接，中位数为 15.0 个。**[24] 这些连接中的每一个也构成潜在的客户端安全风险。

以下是 Cloudflare 客户最常用的一些第三方连接： [25]

- Google (Analytics, Ads)
- Microsoft (Clarity, Bing, LinkedIn)
- Meta (Facebook Pixel)
- Hotjar
- Kaspersky
- Sentry
- Criteo
- tawk.to
- OneTrust
- New Relic
- 贝宝

平均而言，我们客户的**网站使用了 11.5 个 Cookie，中位数为 5 个。仅一个组织就使用了 131 个 Cookie**。[26] 与浏览器加载的第三方脚本和连接类似，Cookie 也带来客户端风险和合规风险。具体来说，Cookie 可能会使网站访客面临安全风险，例如 Cookie 篡改，即攻击者修改客户端 Cookie 以执行会话劫持等攻击，以实现账户接管或欺诈。

虽然第三方脚本和 Cookie 将继续存在，但 Web 应用所有者日益要对这些脚本可能使其最终用户面临的风险负责——更不用说合规责任后果了。

商业考量和建议

目录

攻击者可以通过各种方式获得修改网站所用 JavaScript 组件代码的权限，例如使用被盗的账户凭据或利用 zero-day 或未修补的漏洞。然后，他们利用这一特权访问权限对每个使用该 JavaScript 代码的网站发起下游攻击。

根据 PCI DSS 4.0（将于 2025 年 3 月生效）的新要求，拥有支付页面的组织需要监控第三方脚本攻击，并保护其最终用户免受浏览器供应链攻击。

如果一个组织未能满足用户的隐私期望，Cookie 也会带来也客户端和合规风险（例如前述的 Cookie 篡改）。

例如，GDPR 的《电子隐私指令》要求网站所有者明确说明正在使用的 Cookie 及其目的（而且，在某些情况下，将这些 Cookie 存储到用户的浏览器中之前获取用户的同意）。

建议

与客户端脚本一样，网站管理员、开发人员或合规团队成员并不总是知道其网站正在使用哪些 Cookie。

因此，**寻找一种服务来自动消除第三方脚本风险**，并提供一个**完整的单一仪表板视图来显示**您的网站正在使用的所有第一方 Cookie。

影子 API 风险

消费者和最终用户期待动态的 Web 和移动体验——而这些体验是由 API 驱动的。对于企业来说，API 提供了竞争优势——更强的业务智能、更快的云部署、整合新的 AI 能力，等等。

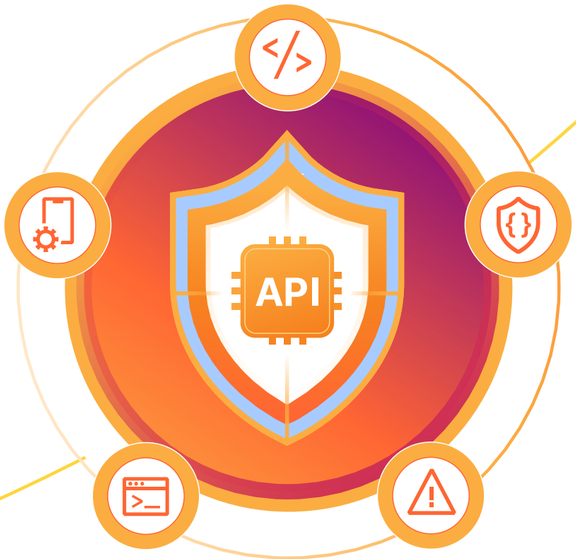
然而，API 目前在 Cloudflare 处理的**动态互联网流量占比超过一半 (58%)**[27]，由于允许外部方访问应用，带来了新的风险。

然而，对许多人来说，API 安全已经落后于 API 部署的快节奏：机器人操作者可以直接攻击例如账户创建、表单填写和付款等工作流程背后的 API，以窃取凭据和其他信息；AI 模型的 API 也容易遭受攻击。

但是您无法保护看不到的东西。**而且许多组织缺乏准确的 API 清单**，即便他们相信自己可以正确识别 API 流量。

通过使用我们的专有机器学习模型（它不仅扫描已知的 API 调用，还扫描所有 HTTP 请求，以识别可能未被考虑的API流量），**我们发现组织拥有的公共 API 端点比他们知道的多 33%。**（这个数字是中位数，它是通过比较通过基于机器学习的发现和根据客户提供的会话标识符检测到的 API 端点的数量计算得出的。）[28]

这表明近三分之一的 API 是“影子 API”——可能没有得到适当的盘点和保护



商业考量和建议

目录

Web 应用和 API 经常一起工作，例如一个电子商务网站使用 API 来处理支付。然而，API 的独特属性构成了独特的攻击面：

	交互对象	数据格式	请求和响应结构	典型威胁
Web 应用	人对系统	灵活（例如 JavaScript、HTML、CSS）	灵活，并返回视图	DDoS、恶意机器人、OWASP 十大 Web 应用风险
现代 API	系统对系统	结构化和机器可读（例如 JSON）	由 API 模式定义，仅返回数据	滥用、数据泄露、恶意机器人、OWASP 十大 API 风险

尽管 API 与 Web 应用相比构成不同的安全挑战，但我们发现，通过某种第 7 层安全机制防御的 API 流量中，有 66.6% 主要是通过传统的消极安全 WAF 规则来保护，而不是使用积极安全模型的专门 API 规则。[29]

传统的 WAF 消极安全模型方法可能无法检测所有针对 API 的攻击流量，特别是端点枚举或身份验证劫持等特定于 API 的攻击。用于保护 API 端点的任何 WAF 应具有现代的 API 专用功能，可以执行积极的安全模型。

建议

随着企业通过 API 提供更多服务，它们应该利用专为 API 安全和管理而设计的工具增强 Web 应用安全工具（例如 WAF 和 DDoS）。高级 API 安全使用无监督机器学习，帮助企业：

- **发现影子 API：** 持续扫描企业环境中的每个公共 API，甚至是那些不受管理或未受保护的 API
- **防止数据泄露：** 通过持续扫描响应有效负载的敏感数据来阻止数据泄漏
- **创建积极的安全模型：** 通过仅接受符合 OpenAPI 模式的流量来保护 API，同时阻止格式错误的请求和 HTTP 异常

总结

目录

数据很清楚：保护组织的应用和 API 以防范新风险的复杂性继续增加：

- 应用层 HTTP DDoS 攻击的数量和规模正在增长，而且由僵尸网络更高效地发动
- 大多数机器人都是不受信任或未经验证的，这可能会对 Web 应用的安全和性能产生负面影响
- 攻击者正在更快地将披露的 CVE 武器化；在一个例子中，是 PoC 发布后的 22 分钟内
- 如果企业对第三方脚本和 Cookie 的依赖度更高，则可能面临更高的软件供应链攻击、隐私问题和合规违反风险

企业通常拥有一套互相脱节、拼凑而成的传统和单点安全产品，导致难以连接和保护其 SaaS 应用、Web 应用和其他 IT 基础设施。IT 泛滥使攻击者更容易发现和利用漏洞。

Web 应用和 API 威胁的广泛性需要专门的方法来阻止专门的攻击。然而，**一种整合的、一流方法有助于确保更好的安全性、无延迟的连接和业务增长。**

Cloudflare 如何提供协助

为了减少复杂性，同时保护不断增加的攻击面，**Cloudflare 将针对用户、应用、API 和网络的保护统一到全球连通云上。**

全球连通云将一个统一的安全网络放置在 Web 应用和 API 前面。它：

- 使用强大的规则集、暴露凭据检查和其他安全措施实时**阻止广泛的攻击**
- **防止攻击者**发现并利用 IP 地址、配置和 IT 资产
- **将 Web 浏览转移到边缘**（而不是端点），为用户和设备隔离基于 Web 的威胁
- **检测基于浏览器的攻击**，包括以脆弱的 JavaScript 依赖和其他第三方脚本为目标的客户端攻击

Cloudflare 全球连通云可扩展以保护任何地方的人员、应用和网络

约 20%
的 Web 资产受到 Cloudflare 保护

320+ 城市
位于 120+ 国家/地区

2090 亿+
次威胁/日被阻止

了解更多

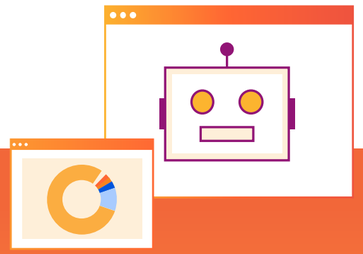
目录

我们的一体化应用安全产品组合基于一个庞大网络的骨干网构建，帮助企业全面掌控自身的安全态势。

主要服务包括：

Cloudflare Web 应用防火墙 (WAF) 提供全面的安全可见性，针对 OWASP 攻击和新兴漏洞的分层保护，通过机器学习检测规避和新型攻击，阻止账户接管，检测数据丢失等。

Cloudflare DDoS Web 保护从我们的全球网络边缘自动执行智能 DDoS 缓解，可在 3 秒内缓解大多数攻击。所有计划都提供无限的 DDoS 攻击缓解，攻击相关流量激增无额外收费。



Cloudflare 机器人管理使用机器学习、行为分析和指纹识别对机器人进行准确分类。阻止凭据填充、内容抓取、库存囤积、DDoS 和其他恶意机器人活动。

Cloudflare API Gateway 自动发现、验证和保护您的 API 端点。阻止常见的 API 攻击，包括 zero-day 漏洞、身份验证滥用、数据丢失、DDoS 和其他业务逻辑攻击。

进一步了解 Cloudflare 的应用安全和性能解决方案。

目录

Cloudflare 主要术语表

注意：本报告中的数据仅根据在 Cloudflare 网络中跟踪的流量计算得出，不一定代表整个互联网的 HTTP 流量模式。

自定义规则：允许您通过对一个区域发送的请求进行过滤来控制入站流量。根据您定义的规则，可以对入站请求执行诸如阻止或托管质询等操作。

HTTP DDoS 攻击规则：一组预先配置的规则，用于在 Cloudflare 全球网络的第 7 层（应用层）匹配已知的 DDoS 攻击手段。这些规则匹配已知的攻击模式和工具，可疑模式，协议违反，导致大量源错误的请求，到达源服务器/缓存的过多流量，以及应用层的其他攻击手段。

访问规则：使用 IP 访问规则，根据访问者的 IP 地址、国家或自治系统编号 (ASN) 对流量进行允许、阻止和质询操作。IP 访问规则通常用于阻止或质询疑似恶意流量。IP 访问规则的另一个常见用途是，允许定期访问您网站的服务，例如 API、网络爬虫和支付提供商。

IP 信誉：此威胁评分衡量 Cloudflare 服务中的 IP 信誉。这个分数是根据 Project Honey Pot、外部公共 IP 信息以及来自我们的 WAF 托管规则和 DDoS 的内部威胁情报计算的。

托管规则：允许您部署预配置的托管规则集，提供对常见攻击的即时防御。

缓解流量：指 Cloudflare 平台应用了“终止”操作的任何最终用户 HTTP 或 HTTPS 请求。这包括以下操作：BLOCK、CHALLENGE、JS_CHALLENGE 和 MANAGED_CHALLENGE。

- 这不包括应用了以下操作的请求：LOG、SKIP、ALLOW。从 2023 年开始，Cloudflare DDoS 缓解系统应用了 CONNECTION_CLOSE 和 FORCE_CONNECTION_CLOSE 操作的请求也被排除在外，因为这些操作只会拖慢连接的启动。它们在请求中所占比例相对较小。
- Cloudflare 改进了有关 CHALLENGE 类型操作的计算，以确保只有未解决的质询才被算为已缓解。有关操作的详细说明请参阅 Cloudflare 开发人员文档。

速率限制规则：允许您为匹配一个表达式的请求定义速率限制，以及达到这些速率限制时要执行的操作。

上传内容扫描：在 Cloudflare WAF 中启用时，内容扫描尝试检测内容对象，例如上传的文件，并扫描其中的恶意特征，如恶意软件。扫描结果以及额外的元数据暴露为可供 WAF 自定义规则使用的字段，使您能够实施精细化的缓解规则。

尾注

目录

1. 通过查看 2023 年 4 月 1 日至 2024 年 3 月 31日期间缓解的应用流量，我们分析哪些应用安全规则被用于缓解流量。WAF 缓解的流量最多，但 WAF 规则可以阻止许多不同类型的攻击，包括容量耗尽攻击、凭据填充攻击、恶意内容上传等（这些攻击可以通过数百种不同规则来检测）。Web 应用触发的第二大最常见规则集是 DDoS 规则集，该规则集仅识别 DDoS 攻击。
2. Jetbrains 于 2024 年 3 月 4 日 14:59 披露 CVE-2024-27198。几小时后，Rapid7 在 19:23 UTC 发布对 CVE-2024-2178 的概念验证分析。Cloudflare 在 19:45 UTC 观察到对该漏洞的尝试利用。
3. 我们查看了截至 2024 年 5 月从 Page Shield 产品提取的聚合客户网站数据，针对包含 resource_type = 'script' 和 resource_type = 'connection' 的主机，以确定我们客户的每个主机名上的第三方脚本和连接的平均数量。我们排除了数据集中的异常值，因此连接和脚本的数量是通过查看数据集的 99.5% 来确定的。
4. 我们研究了 Cloudflare 反向代理后面所有网站在报告收集期（2023 年 4 月 1 日至 2024 年 3 月 31 日）内的所有 HTTP 流量，并按人类流量和自动流量进行排序，以了解机器人与人类流量各自所占比例。为了获得经验证的机器人流量与未经验证的机器人流量之间的比例，我们将机器人流量与 Cloudflare 维护的已知“好”机器人也就是“经验证”的机器人）列表进行对比。
5. 为了找到这些数据，我们分析了 2023 年 4 月 1 日至 2024 年 3 月 31 日期间由 Cloudflare 保护的公共 API 端点触发的应用安全规则。然后，我们将触发的规则划分到与它们的产品相对应的更大的组别中。这有助于我们了解攻击者最常尝试的策略。
6. 在 2023 年 4 月 1 日至 2024 年 3 月 31 日的收集期间，我们分析了来自 URL Scanner 项目的数据，查看在数据收集期间接收到最高流量的前 5000 名。我们选择分析前 5000 个域的 Cookie，而不是 Cloudflare 后面的所有 URL，以展示最能反映本报告企业受众的数据。
7. 我们分析了从 2023 年 4 月 1 日至 2024 年 3 月 31 日期间发给 Cloudflare 代理背后的所有应用的 HTTP 请求，并根据缓解或未缓解进行分类（有关“缓解流量”的定义，请参阅“术语表”）。
8. 我们将 2023 年 4 月 1 日至 2024 年 3 月 31 日期间缓解的应用流量百分比与我们的报告《2023 年应用安全状况》中的数据进行了比较。
9. 本图表研究在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间汇总的数据，涵盖所有由 Cloudflare 作为反向代理并部署了至少一个应用安全规则的应用，以确定哪些安全规则被最频繁地触发。然后，我们将触发的规则划分到与它们的产品相对应的更大的组别中。这有助于我们了解攻击者最常尝试的策略。
10. 本图表研究在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间汇总的数据，涵盖所有由 Cloudflare 作为反向代理并部署了至少一个应用安全规则的应用，以确定哪些安全规则被最频繁地触发。这有助于我们了解攻击者最常尝试的策略。
11. 这些数据来源于案例研究访谈中的客户反馈，特别是来自 DTLR/Villa 和 Open Access College 的公开案例研究，以及 Cloudflare 通过 TechValidate 软件进行的客户投资回报调查的 23 份答卷。
12. 我们研究了导致每个 WAF 托管规则（用于阻止针对常见和新兴漏洞的利用）发布后的 30 天内触发该规则的攻击尝试活动，以避免今年早些时候发布的托管规则所占权重过高。我们检查了 2023 年 4 月 1 日至 2024 年 3 月 31 日期间发布的 WAF 托管规则及其相关的漏洞利用企图活动。
13. 本图显示了 2023 年 4 月 1 日至 2024 年 3 月 31 日收集期间缓解的 HTTP 流量，放大到这一年期间与 DDoS 规则相关的缓解流量。
14. 来源：Cloudflare 的 2024 年第一季度 DDoS 威胁报告。
15. 来源：Cloudflare 的 2024 年第一季度 DDoS 威胁报告。
16. 这些数据来自 Cloudflare 对被称为“Rapid Reset”的 HTTP/2 漏洞以及随后发生的超大规模攻击浪潮的发现和分析。

尾注

目录

17. 来源：Cloudflare 2023 年第三季度 DDoS 威胁报告。
18. 本图表对 HTTP DDoS 攻击按行业分类，然后按照在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间互联网上所有 DDoS 流量中所占比例从大到小排序。
19. 我们研究了 Cloudflare 反向代理后面所有网站在报告收集期（2023 年 4 月 1 日至 2024 年 3 月 31 日）内的所有 HTTP 流量，并按人类流量和自动流量进行排序，以了解机器人与人类流量各自所占比例。
20. 为了获得经验证的机器人流量与未经验证的机器人流量之间的比例，我们将 2023 年 4 月 1 日至 2024 年 3 月 31 日期间的机器人流量与 Cloudflare 维护的已知“好”机器人（也就是“经验证”的机器人）列表进行对比。
21. 我们查看 2023 年 4 月 1 日至 2024 年 3 月 31 日期间的机器人流量，并按行业分类，然后将每个行业的机器人流量与人类流量进行比较，以确定哪些行业拥有最高比例的机器人流量。
22. 我们查看了截至 2024 年 5 月从 Page Shield 产品提取的聚合客户网站数据，针对包含 resource_type = 'script' 和 resource_type = 'connection' 的主机，以确定我们客户的每个主机名上的第三方脚本和连接的平均数量。我们排除了数据集中的异常值，因此连接和脚本的数量是通过查看数据集的 99.5% 来确定的。
23. 根据 Radar 年度回顾报告（2023 年 1 月 1 日 - 2023 年 12 月 31 日）以及报告期间（2023 年 4 月 1 日 - 2024 年 3 月 31 日）从 Cloudflare Page Shield 产品提取的数据，我们编制了客户 Web 应用中最常用第三方脚本的列表。
24. 我们查看了截至 2024 年 5 月从 Page Shield 产品提取的聚合客户网站数据，针对包含 resource_type = 'script' 和 resource_type = 'connection' 的主机，以确定我们客户的每个主机名上的第三方脚本和连接的平均数量。我们排除了数据集中的异常值，因此连接和脚本的数量是通过查看数据集的 99.5% 来确定的。
25. 利用 2024 年 5 月从 Cloudflare Page Shield 产品获取的数据，我们汇总了客户 Web 应用中最常用第三方连接的列表。
26. 基于 2023 年底的 Cloudflare Radar 排名前 5,000 个域。我们选择分析前 5000 个域的 Cookie，而不是 Cloudflare 背后的所有 URL，以显示最能反映本报告企业受众的数据。 Radar 的域排名数据集旨在根据全球各地人们如何使用互联网来识别最受欢迎的域，而不追踪个人的互联网使用情况。
27. 2023 年 4 月 1 日至 2024 年 3 月 31 日期间，具有成功响应（200 状态码）的 API 流量占 Cloudflare 动态 HTTP 流量的 58%（中位数）。动态内容是根据用户特定因素而变化的内容，例如访问时间、位置和设备。
28. 对于 REST API 端点，Cloudflare API Gateway 产品中的 API 发现工具通过机器学习在所有客户的域/区域中找到的端点比我们通过客户提供的会话标识符发现的数量（中位数，每个账户）多出 33%。
29. 我们研究了 2023 年 4 月 1 日至 2024 年 3 月 31 日期间到公共 API 的缓解流量，并分析哪些产品和规则集被最频繁地实施和触发。

CLOUDFLARE

目录

电话：010 8524 1783
电邮：enterprise@cloudflare.com
网站：cloudflare.com/zh-cn

REV:BDES-5907.2024JUN20