

Cloudflare 试图强迫我们在 24 小时内支付 12 万美元，随后关闭了我们的网站

Cloudflare took down our website after trying to force us to pay 120k\$ within 24h



罗宾·德夫ROBIN DEV

2024 年 5 月 26 日MAY 26, 2024



146146



8181



66

分享Share

总结：

多年来，我们一直在使用 *Cloudflare* 商业计划（每月 250 美元）。他们突然联系我们，要求我们在 24 小时内预付 12 万美元购买一年的企业版，否则他们将删除我们所有的域名。虽然这让我们的业务量有所提升，但我们还是与他们进行了 3 次销售电话，试图弄清楚发生了什么以及如何在一周内达成合理的合同。当我们告诉他们我们也在与 *Fastly* 谈判时，他们突然“清除”了我们所有的域名，导致我们的核心业务长时间停机，我们不得不彻夜难眠地从 CF 迁移，客户信任度不可挽回地丧失，我们的内部系统持续停机数周。

背景故事

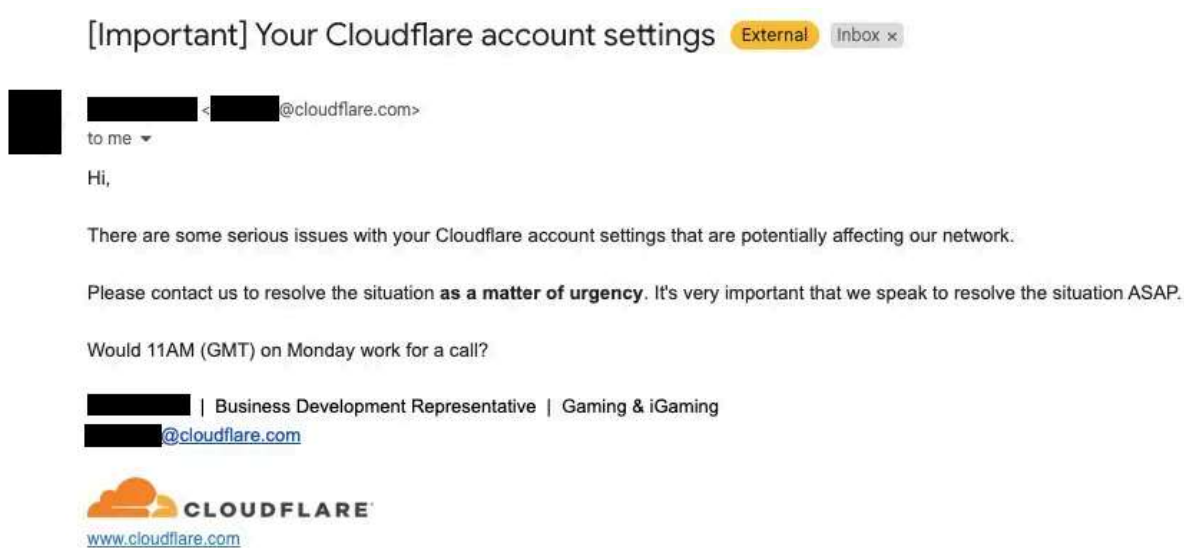
我是一家相当大的在线赌场的系统操作工程师。（我认为这篇文章与你是否认为一般的赌场是合乎道德的无关，我只是为了背景而提到它。）我们每月有大约 400 万活跃用户。自 2018 年以来，我们一直是 Cloudflare 的满意客户，使用“商业”计划，该计划具有一些不错的功能，每月 250 美元可享受“无限”流量。

现在，不可否认的是，对于我们通过 Cloudflare 推送的流量而言，250 美元可能相当低。我们主要将 CF 用于 CDN（缓存所有静态内容）和 DDOS 保护，它在这方面表现相当不错。它易于使用，您通常无需过多考虑。

我读过 Hacker News 上的几篇文章，其中提到 Cloudflare 曾联系过你，并积极要求你升级到“企业版”并享受自定义定价。但我没想到事情会变得这么糟糕。

2024 年 4 月 19 日

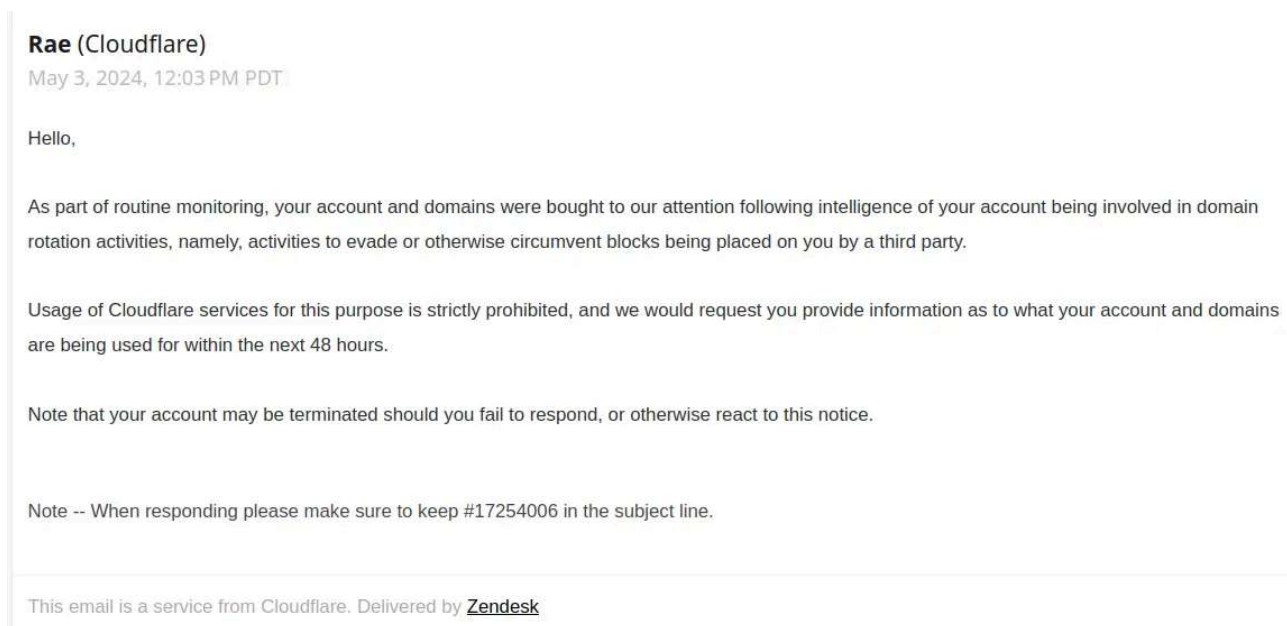
今年 4 月，我们收到了 Cloudflare 发来的这封电子邮件：



这听起来像是我们的网站出了问题。我们安排与他们的“业务开发”部门通话。结果会议是与他们的销售团队进行的，他们根本没有任何“严重问题”需要报告。他们问我们是否愿意考虑 Enterprise。我们礼貌地拒绝了，对电子邮件的语气有点困惑。

2024 年 5 月 3 日

两周后，我们收到另一封电子邮件：



现在需要对他们所说的内容进行一些背景介绍。我们确实有多个域名，它们主要充当我们主域名的镜像。我们拥有这些域名有几个原因。一是因为我们是一家赌场，所以

我们需要遵守许多国家/地区的不同监管要求。例如，许多游戏仅在某些国家/地区可用。有些国家/地区我们会完全屏蔽。然后，我们有几个不同的域名可以删除某些游戏组或站点功能 - 例如我们的社交功能（聊天、用户小费/互动）或我们的体育博彩。另一个原因是我们使用它们来定位不同的全球用户组和附属机构并长期跟踪转化。这也意味着，如果某个国家/地区的 DNS 阻止了我们的主要域名，则辅助域名可能仍然可用。正如他们上面所写，这可以说被视为违反了 Cloudflare TOS。

无论如何，我们 **95%** 以上的流量都是通过自成立以来一直未变的主域接收的，我们很乐意以任何方式解决这个问题，包括从 Cloudflare 中删除任何受影响的二级域。

我们向他们发送了有关我们域名的信息，并试图从他们那里获得有关该问题的更多信息以及我们应该让团队中的哪位成员参与其中，但除了通话日期外，他们拒绝向我们提供任何信息。

2024 年 5 月 7 日

因此，我们又安排了一次通话，这次是与他们的“信任与安全”团队通话。但结果发现，我们实际上又在与销售人员进行交谈。

他们说他们可以为我們提供一份每月 1 万美元的超值合同，其中包含各种出色的功能。我们试图弄清楚这与 TOS 问题究竟有何关联，以及如何解决这种情况。我们询问他们哪些域名受到“轮换”问题的影响。他们没有给我们答案。我们询问我们实际上必须获得哪些企业功能。

他们除了每月 1 万美元的全套服务外，不提供任何其他服务，这样问题就能神奇地解决了。他们对任何其他解决方案都不感兴趣。

他们说我们只有 24 小时的时间来签署合同，因为他们必须“回到信任与安全”部门。我们要求按月付款。他们说我们需要签署年度承诺并预付全年费用。这感觉像是敲诈勒索。在明天之前向我们支付 12 万美元，否则我们会毁了你的生意。

通话结束后，他们向我们发送了以下信息：

As discussed, please find below a summary of the solution needed for your use case as well as the preliminary quote.

Cloudflare Enterprise Plan with:

1. [BYOIP](#) (you can lease IPs and we will onboard and advertise them on your behalf)
2. [SSL4S](#) (helps you to add/change hostnames/mirrors with 3 sec. propagation and without the need to set up DNS/ CDN/DDoS/WAF/SSL configurations) - this can be done via API too

The **Enterprise Plan** includes the following services:

- Advanced **DDoS / WAF / CDN / DNS / Certificates** fully managed
- **Argo Smart Routing** - optimised content delivery via fastest routes (up to 70% latency improvement)
- **Advanced Cache control** (ie. Custom Cache Keys, Cache Purge by Tag and more)
- **Image Resizing** (1m images served per month, included)
- **Workers** (10m included)
- **Zero Trust Access** - 50 seats
- **Raw logs** - detailed HTTP request logs to debug, identify configuration adjustments and create analytics - up to 150 attributes for each request. Additionally direct integration with SIEM tools like Splunk, DataDog, ELS, Azure, GCP, AWS or any S3 compatible storage
- **Site Analytics** resolution (down to 1 minute scope for the last 30 minutes)
- **Priority Support** 24/7/365 via telephone, chat, email
- Assigned Account Manager and Solutions Engineer, Access to Success team for consultation
- Advanced/ proactive notifications on the status of your Cloudflare environment - support for Webhooks and Slack
- **Role Based access** - grant access to Cloudflare based on member's access rights. Additionally full audit log on the activity

BYOIP (leasing companies): These are some options where you can lease IPs, you can of course use any other provider:

Larus <https://www.larus.net/ip-leasing>

Bandwidth Technologies <https://www.bandwidth.co.uk/connectivity/ipv4-leasing>

IPXO <https://www.ipxo.com/lease-ips/>

IPV4Market Group <https://ipv4marketgroup.com/broker-services/ip-leasing/>

Commercials: \$9.940/ month (with default annual payment), including:

- Enterprise Plan (as per above) - based on 80 TB/ 6B requests
- Your main domains & hostnames for rotation - 2 Top Level Domains & 15 mirror domains
- BYOIP support and onboarding

Happy to walk this through and discuss further technical details tomorrow.

As we have a very short window to report back to the Trust and Safety team, please let me know if you can make time **tomorrow at 13:00 CET**.

请注意，电子邮件暗示可以按月付款。当我们要求澄清时，我们被告知必须预付全年费用。

他们提到的大多数功能我们都不需要。我理解他们要求我们做 **BYOIP** 是为了免除他们对我们域名的责任，但其余的都是我们不需要或纯粹“好有”的东西。

我们设法争取到了一周的时间，将问题上报给我们的 CEO 和 CTO，并让他们直接与 Cloudflare 进行沟通。

但他们仍然不关心该问题的其他解决方案，并拒绝向我们提供任何其他合同选项。在网上查找数字很困难，但如果你仔细看看（与此帖子比较：<https://news.ycombinator.com/item?id=29333160> 和此帖子 <https://news.ycombinator.com/item?id=31336515>）80TB 流量的合理价格可能是每月 150-2000 美元。请注意，80TB 是他们试图向我们出售的数字，我不知道这是否准确，因为他们删除了我们对历史分析的所有访问权限。

在此期间，我们还研究了替代方案，并设置了一个测试域并与 Fastly 进行通话，因为他们似乎是一个合理的竞争对手。

2024 年 5 月 16 日

在另一通试图协商合理合同的电话中，我们的首席执行官告诉 Cloudflare 销售部门，我们也在与竞争对手谈判。我本以为这是显而易见的，当收到 12 万美元的发票时，谁不会寻找替代方案呢？但通话几小时后，发生了以下事情：

Date ▾	Action	User	Domain
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	
May 16, 2024	Purge	Cloudflare	

Cloudflare 突然删除了我们所有的域名。我们所有的 DNS 记录、缓存设置、速率限制、白名单都消失了。我们的公共网站、收到的电子邮件（包括来自客户的支持电子邮件）和内部基础设施、Cloudflare Access 上的身份验证配置都瘫痪了。

他们还向我们发送了这封电子邮件：

[Cloudflare]: Your Cloudflare account has been suspended

ExternalInbox x



Cloudflare

<noreply@notify.cloudflare.com>

to me ▾

1

Hello,

The Cloudflare account associated with this email address has been suspended for a possible Terms of Service violation. Cloudflare's Terms of Service are available at <https://www.cloudflare.com/terms/>.

This account suspension does not impact, disable, or remove your current services. This does block the addition of new domains to your Cloudflare account while this matter is under review.

If you have any questions regarding this suspension please contact Cloudflare's Trust & Safety team at abusereply@cloudflare.com to discuss this action.

Thanks,

The Cloudflare Team

电子邮件说“这[...]不会影响当前服务”，所以我们疯狂地给他们写了一张支持单，但没有得到任何回复。所以我们打电话给我们的 SysOps 团队，开始将我们的主要网站迁移到 Fastly。几个小时后，我们就完成了基本工作，但即便如此，“NS”DNS 条目更改显然需要相当长的时间才能传播到所有地方，从 1 小时到 48 小时不等。我们仍在从后果中恢复。

在某个时候，Cloudflare 对我们的票做出了这样的回复：



Hello there,

Thanks for contacting Cloudflare Technical Support.

We've escalated this request onto our Trust and Safety Team for review. Trust and Safety will reach out to you soon, and will help to address your request.

Please note that your request with Technical Support has been closed as our Trust and Safety team will need to follow up directly.

If you need any other **technical support** assistance, please follow the instructions on our [Support Portal](#).

This ticket will now be marked as closed.

Best Regards,



“信任与安全”从未联系我们，我们的帐户仍处于锁定状态。

当 Cloudflare 联系您时我的建议

首先，恭喜！你的生意一定很成功。CF 到底是如何决定“要求”你转向 Enterprise 的？

或许...

- ...你每月的流量达到 10TB
- ...他们的熔岩灯进入了特定的星体排列
- ...一位销售代表意识到他们还没有达到季度配额

最后，谁知道呢？Cloudflare 完全不知道他们何时会强迫您使用自定义计费，但当他们开始“紧急”需要与您交谈时，您可能不会离开，直到您与他们签订一份丰厚的自定义合同。他们没有公开任何有关流量限制或企业定价的信息是有原因的。他们的销售团队会利用任何事情（例如拥有多个域）作为推动力，强迫您的整个帐户使用企业版，无论它是否可以通过简单的方式修复。

- 他们给您的价格完全基于他们认为您可能会支付的价格，而不是基于任何可衡量的指标或功能集。
 - 我们尝试询问如果流量减少，价格会受到怎样的影响，但他们拒绝透露任何信息，只说包含 80TB（我们有大量使用 IP 白名单的回调流量，因此实际上

不需要经过 CDN，只是由于包含无限流量，我们从未花时间对其进行优化）。

- 我们试图说我们不需要其中包含的 14 项功能中的任何一项，他们说无论我们是否想要，所有这些令人惊叹的功能都已包含在内。
- 在 Hacker News 帖子（上面的链接）中发现的数字表明，相同服务的价格至少相差一个数量级。
- 我们试图说我们的不同域（例如内部域）并不都需要企业，但他们说整个帐户都是企业。
- 如果他们认为你不靠谱（也许你有其他选择？），他们会给你一个不合理的期限，并强迫你提前支付一年的费用。
- 他们会用任何借口作为您突然“需要”企业版的理由，即使您对企业版的功能集感到满意。
 - 我们的业务并非唯一受到 CF 激进销售策略威胁的公司：
 - <https://news.ycombinator.com/item?id=34235237>
 - <https://news.ycombinator.com/item?id=34639212>
 - <https://news.ycombinator.com/item?id=31573854>
 - <https://news.ycombinator.com/item?id=31336515>
- 仅仅因为您每月支付 250 美元，就不要指望他们会以任何礼节或（非销售）方式回复支持邮件。如果您希望 CF 在销售之外回复您，唯一的方法显然是给他们负面报道。
- 准备在 24 小时内离开 Cloudflare。
 - 永远不要直接在 CF 上注册域名。如果你这样做，他们就会屏蔽你，我不知道你如何在合理的时间内找回你的域名。幸运的是，我们只有 NS 指向 CF，因此大多数用户大约需要 3-24 小时的停机时间。
 - 不要在 CF 上使用任何自定义缓存规则。CF 默认会忽略大多数/所有标准 HTTP 缓存标头（任意一组扩展除外），并鼓励您在 CF 上创建自定义规则。相反，将 CF 设置为“Cache: Always”（这实际上并不意味着总是）和“Respect Origin Headers”。这样，规则将适用于其他缓存代理。
 - 不要使用任何专有的 Cloudflare 产品，例如 Zero Access 或 Workers。我们在内部产品中大量使用 Zero Access 进行身份验证，现在我们必须从头开始重建所有这些基础设施，并且停机时间很长。仅在与第三方标准兼容的情况下使用其技术。

- 备份 Cloudflare 上的配置。重新创建所有这些配置（包括各种发送电子邮件服务（SPF、DKIM 等）、站点验证 DNS 条目、IP 列表、速率限制规则等）是一件出乎意料的大麻烦。
- 确保你了解 CF 的商业模式对你的影响：要么你正在依赖 Cloudflare（免费/商业计划的客户），要么 Cloudflare 正在依赖你（不透明的企业定价）。没有中间地带，在某个时候需要切换。
- 并且：考虑一下您是否需要 Cloudflare。
 - CF 仅管理过（对我们来说）相当大的 DDOS 攻击。如果您有一些更易受攻击的攻击面（例如，未缓存的未经身份验证的 API 请求会占用 100 毫秒的 CPU 时间，因此每秒仅 10-100 个请求就会耗尽您的核心），Cloudflare 甚至不会检测到它。特别是因为所有半专业的“DDOS 攻击即服务”团体似乎都专门针对 Cloudflare 支持的服务，包括“攻击模式”解决方法等。



146 个赞146 Likes · 6 重新堆叠6 Restacks

关于此帖的讨论Discussion about this post

评论Comments

重新堆叠Restacks



写评论...

**宝马云SREBMWCloudSRE** 5月29日May 29

我们宝马公司就遇到过这种情况。法律部门威胁要起诉，要求赔偿数百万美元，但奇怪的是，一切都恢复了，没有任何反馈。This happened to us at BMW. Legal threatened to sue for millions in business and strangely everything was restored with NO FEEDBACK.

赞(22)LIKE (22) 回复REPLY 分享SHARE ...

**噢AW** 5月27日May 27

你好，我们也遇到过同样的事情，BYOIP，信任和安全团队，但这是销售，我们可以讨论如何不使用 cloudflare 吗？Hi, we've had the exact same thing happen to us, the

BYOIP, the trust and safety team but it was sales, we can talk and discuss about how to NOT use cloudflare?

 赞(16)LIKE (16)  回复REPLY  分享SHARE ...

1 条回复1 reply

另外 79 条评论...79 more comments...