# 黑客思维

# 为什么安全性在游戏行业更加重要

游戏业是一个有着丰富攻击目标的环境。在 2020 年的新冠疫情期间，针对游戏业的攻击流量的增幅超过了其他任何行业。

玩家积极参与社交社区的活动 — 他们拥有可支配收入，并且倾向于将其用在游戏帐户和游戏体验上。

在 Akamai 和 DreamHack 对 1253 名游戏玩家开展的调查中，有一半的受访者表示曾遭受黑客攻击。每 10 名游戏玩家中就有 8 名遇到过这种情况：遭到黑客入侵的帐户被放到网上出售。对于游戏玩家而言，他们在其帐户上投入的时间和热情是不可替代的。游戏玩家对以下两个问题的担忧程度不相上下：丢失信用卡信息 (49%) 和失去帐户的访问权限 (48%)。

犯罪分子通常通过泄漏的密码列表攻击游戏帐户。网络钓鱼也是一种流行（而且仍然有效！）的攻击手段，并且针对的是安全知识薄弱且易受攻击的玩家。

目标是快速行动，并首先攻击最容易破解的帐户。这种攻击通常针对的是符合以下条件的玩家拥有的帐户：重复使用密码，且未启用多因素身份验证。

只要在 YouTube 上快速搜索一番，您就可以找到讲解如何针对特定热门游戏有效开展此类攻击的大量视频教程。

> **“...[安全性] 必定是多方共同努力的结果。游戏公司必须提供安全的解决方案，而我也必须配合并使用这些解决方案...”**
>
> **— 过去曾遭遇帐户劫持的资深玩家，Akamai/DreamHack 报告**

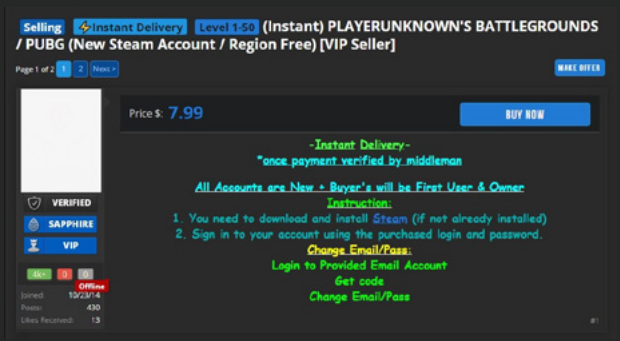
犯罪分子成功访问帐户后，他们会寻找几种不同的资源。犯罪分子会寻找个人身份信息 (PII)，这可能有助于他们横向入侵其他有价值的帐户。

他们还会寻找可以转移到其他帐户名下、进行交易或在二级市场上出售的游戏道具或游戏虚拟货币。

最终，许多犯罪分子会将整个帐户出售给某个作弊者 — 不想慢慢升级，而是想直接从更高等级开始体验游戏的玩家。

在 Akamai/DreamHack 开展的调查中，有二分之一的受访者认为，网络安全是游戏玩家和游戏公司的共同责任。

出售玩家帐户




Web 攻击持续不断。撞库攻击可能会将上周的数据泄露事件变成影响数千或数百万人的全新事件。DDoS 攻击对即时通信领域和互联世界造成了破坏。

您永远无法阻止所有攻击，但您可以做某些事情来反击和抵御攻击，比如加强现有的保护措施，保护 API 访问以及淘汰掉旧的保护措施（比如通过短信接收的一次性密码）。

要保护的并不只有游戏帐户。有些受害者早在自己的游戏个人资料遭遇入侵之前就已成为攻击目标。犯罪分子会从方方面面寻找可乘之机，包括电子邮件和社交媒体，并将那些信任网络、盲目假设一切安全的用户视为垫脚石，发起环环相扣的新攻击，入侵其他目标。

如何抵御攻击：

- 了解敌人的具体目标
- 专注于监测能力和多层安全性
- 与您的玩家（尤其是那些易受攻击的玩家）建立合作伙伴关系

## 并非所有 DDoS 抵御措施都具有同等的效力

DDoS 攻击的规模每两年翻一番，它在攻击媒介的数量和组合方面具备前所未有的复杂性。

一个游戏中发生的 DDoS 攻击不仅可以影响其他游戏，甚至可能会扰乱整个平台和生态系统。

例如，如果对一个大型多人游戏发起 DDoS 攻击并使其离线，玩家将会不断尝试登录 — 这会使身份验证服务器不堪重负并导致停机，从而关闭平台上的所有服务器。

媒体和游戏企业在努力保持接近 100% 的应用程序和网络可用性，而黑客希望发起容量耗尽攻击、协议攻击和应用程序层 DDoS 攻击，以破坏任何潜在的故障点，使最终用户无法使用面向互联网的资源和资产。

通过对受害环境、应用程序和 IP 空间进行侦查，攻击者可以确定哪些 DDoS 媒介将造成最大的损害。攻击者可利用众多攻击技术和工具来发现企业防御中存在的弱点或漏洞。

借助大型全球边缘平台，安全可靠地部署游戏、补丁和更新：

Download Delivery

点击阅读

DDoS 结果

扰乱业务运营
— 勒索攻击

扰乱其他玩家

为其他 Web
攻击提供掩护

DDoS 攻击者会以任何潜在的故障点为目标，例如：

网站

Web 应用程序和
其他企业服务

VPN 集中器（用于远
程访问公司资源）

SD-WAN
控制器

应用程序编程
接口 (API)

域名系统 (DNS)
和源站服务器

数据中心和网络
基础设施

随着企业继续扩大和保护分布在各地的工作团队的远程访问能力，DDoS 攻击的影响只会加剧。根据 Ponemon Institute 的数据，企业遭受的 DDoS 攻击的平均年度成本为 170 万美元，这一成本来源于技术支持增加、事件响应资源消耗、内部上报流程、法律成本、运营中断和员工生产力损失。

随着企业停用传统数据中心并将应用程序移至云托管环境，安全架构变得更加复杂。

许多企业都难以采用与数据中心内相同的 DDoS 防御水平来保护面向互联网的资产。更复杂的是，许多云托管 IP 不在企业的直接控制范围之内，如果没有适当的保护，它们很容易遭受成功的 DDoS 攻击。

恶意攻击者非常清楚这种向主机代管设备和公共云加速迁移的过程。不一致的安全策略和要求导致企业安全架构和态势存在缺陷，企业在分散且碎片化的云托管基础架构中进行故障排除时也面临众多困难，因此攻击者希望利用这些弱点。

持续保护的一种方法是建立出色的云安全。现代企业需要采取自适应防御机制，以保护各种面向 Web 的资产和服务（无论它们位于何处）。随着超过 93% 的企业（<1000 名员工）采用多云战略，现在是时候修复由基础架构复杂性导致的防御漏洞了。

Akamai 拥有遍布全球的大规模成熟 DDoS 缓解云。

无论您是要保护单个应用程序、整个数据中心还是权威 DNS，Akamai 在设计 DDoS 缓解措施时已将大容量、高恢复能力和快速缓解考虑在内。

我们已经抵御了全球范围内发起
的一些大规模 DDoS 攻击：

Prolexic

点击阅读

# 爱奇艺：视频流媒体，永远无需等待

在流媒体视频显示在队列中时，您是否还会看到那个旋转拨盘？对于爱奇艺的用户来说，这已经成为过去。在爱奇艺上，无需等待，即可开始播放视频。

爱奇艺是中国市场颇具创新意识的在线娱乐服务商。为了在持续满足现有客户需求的同时将业务拓展至其他国家/地区，该公司需要服务器设在其所有全球客户和内容提供商附近的内容交付网络 (CDN)。

这一创新功能背后的策划者是爱奇艺基础架构和智能内容分发事业群高级总监秦建华。

根据报告，爱奇艺每月有超过 5 亿的活跃用户。开发人员持续优化该公司基于人工智能的推荐引擎，按需更新软件。每天都会发布大量的内容。秦先生表示：“要持续发布新代码和新内容，我们需要极其高效的基础架构。

当爱奇艺开始在全球扩张时，秦先生要为中国境外的新用户寻找 CDN。集中式云环境会给流媒体视频带来太长的延迟时间。

秦先生表示：“我们之所以为全球用户选择 Akamai 的 CDN，是因为 Akamai 是延迟低、覆盖范围广的服务提供商，在全球拥有 325000 台服务器。Akamai 拥有一支本地技术支持团队，这点让我很满意。此外，Akamai 在边缘领域已拥有 20 多年的经验，而传统云服务提供商才刚刚开始向边缘转型。”

> **“更少的部署时间意味着更多的创新时间。”**
>
> **— 爱奇艺基础架构和智能内容分发事业群高级总监秦建华**

爱奇艺的开发人员喜欢自动化部署，这让他们有更多的时间开展创造性工作，如优化该公司的推荐引擎和识别热门内容趋势。秦先生表示：“从物理服务器到虚拟机再到容器，基础架构的每一项进步都会节省我们运营团队的时间，让他们能够更快地为开发人员提供支持。Akamai 进一步简化了新软件的部署工作。我们的开发人员只需点击一下，即可将新软件部署到多个云和数十万台 Akamai 边缘服务器上。更少的部署时间意味着更多的创新时间。”

始终如一地为大量观众
提供高品质在线视频：

Adaptive
Media Delivery

点击阅读

了解爱奇艺计划如何继续创新，
从而迈入元宇宙：

爱奇艺：视频流媒体，
永远无需等待

点击阅读

如果您想了解更多有关 Akamai
与我们提供的解决方案，请

联系我们