# 遇到黑客攻击我们网站服务器，我们要怎么防御？

| | |
|---|---|
| 产品名称 | 遇到黑客攻击我们网站服务器，我们要怎么防御？ |
| 公司名称 | 广州数据猫网络科技有限公司 |
| 价格 | .00/个 |
| 规格参数 | 机房:江苏/佛山等<br>租赁周期:年/月<br>套餐:200G/300G等 |
| 公司地址 | 广州市天河区灵英东路3号 |
| 联系电话 | 17701938714 15625004753 |

# 产品详情

防御DDOS，找梁经理199-2742-9680 V电，帮你解决。DDOS防御CC流量攻击，防御DDOS,防御CC攻击，DDOS防御，DDOS防御CC攻击，CC防御，DDOS防御流量攻击，专业防御DDOS攻击

怎样去防御黑客攻击，可以采用以下以下方式：

1、设置复杂密码定期更换

现在的黑客也有可能使用这样暴力破解的方法来破解超级账户的密码，从而对服务器实行攻击。如果你要要预防超级管理员密码被暴力破解再复杂的密码也有被破解的风险，所以建议超级管理员的密码设置复杂同时定期修改。

2、选择高防服务器预防DDOS攻击

现在DDOS攻击是服务器常见的一种攻击，它的攻击方式有很多，常见的是通过服务请求来占用服务资源，比如带宽CPU内存等从而导致用户无法得到服务响应，甚至瘫痪。如何预防DDOS攻击的有效的方法是选择设有机房硬防的机房，硬件防火墙能够有效预防DDOS攻击和黑客攻击。硬件防火墙有很好的防御效果，并且对CC攻击有一定的防护作用

3、系统漏洞补丁及时更新

系统漏洞也是黑客主要的入侵途径之一，黑客经常会通过系统漏洞或者是.程序的各种漏洞等对服务器实行攻击。每个网站的系统、或者程序或多或少都会存有一些漏洞，这个不可以避免，或系统本身就存在的漏洞，或系统管理员写代码的时候错误导致的漏洞，所有应该及时给服务器系统打更新补丁

，及时升级程序新版本修复漏洞的发生，及时对代码进行审计。

4、关闭端口，只开放必须的端口

服务器的端口是攻击的比较重要的入口，就是服务器对外的一扇窗户，服务器上已经开放的端口是那些黑客的利用对象，他们通过这些开放端口对服务器进行攻击。相对比较有效的预防方法是关闭一些不必要端口，然后修改重要端口。对外少开放一个端口，他们就少一个入侵途径，如果你开放一个服务就意味着对外开放多一个端口，那么在关闭端口的同时也要关闭一些不必要的服务。此外，修改一些比较重要端口同时可以加大黑客的进攻难度，那么这样也能有效地保护我们的服务器。

近年来，DDoS攻击已经危及不同的行业，金融、游戏行业尤其严重。黑客喜欢追逐金钱。因此，像荷兰银行那样资金充裕的金融部门更容易受到攻击。攻击使金融系统无法访问。原因可能是通常的赎金和敲诈勒索，更值得关注的是声誉受损和经济损失。更糟糕的是，商业竞争可能与此类攻击有关。随着网上银行的普遍使用以及电子货币市场的蓬勃发展，此类涉及天文数字损失的事件将DDoS攻击的流行带到国际关注的最前沿

那么，黑客有哪些常用来攻击服务器的手段呢?

1、重新发送攻击

重新发送攻击就是指黑客收集特定的IP数据包篡改其数据，然后再将这些IP数据包一一重新发送，从而欺骗接收数据的目标计算机，实现攻击，破坏服务器安全。

2、伪造信息进攻

伪造信息进攻就是指黑客通过发送到伪造的路由器信息，构造源计算机和目标计算机之间的虚报途径，从而获取这些数据包中的银行账户密码等个人敏感信息。

3、数据驱动攻击

数据驱动攻击是指黑客向目标计算机发送或复制的表面上看来无害的特殊程序，被执行时所发起的攻击。该攻击可以让黑客在目标计算机上修改与网络安全有关的文件，从而使黑客在下一次更容易入侵该目标计算机。数据驱动攻击主要包括缓冲区溢出攻击、格式化字符串攻击、输入验证攻击、同步漏洞攻击、信任漏洞攻击等。

4、对协议弱点攻击

在局域网中，IP地址的源路径选项允许IP数据包自己选择一条通往目标计算机的路径。当黑客试图连接位于防火墙后面的一台不可达到的计算机X时，他只需要在送出的请求报文中设置IP地址源路径选项，使得报文的某一个目的地址指向防火墙，但是zui终地址却指向计算机X。

当报文到达防火墙时被允许通过，因为它指向的是防火墙而不是计算机X。防火墙的IP层处理该报文的源路径被改变，并发送到内部网上，报文就这样到达了不可到达的计算机X，从而实现了针对信息协议弱点攻击。