CC攻击是什么？怎么防御此CC攻击？

产品名称	CC攻击是什么？怎么防御此CC攻击？
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	
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

防护CC攻击找【152-1719-5017黄小姐】CC攻击防御、CC攻击防护、防御CC、WEB防护、WEF防护、入侵防御等为各类型攻击的防御

CC攻击的原理：

CC攻击的原理就是攻击者控制某些主机不停地发大量数据包给对方服务器造成服务器资源耗尽，一直到宕机崩溃。CC主要是用来消耗服务器资源的，每个人都有这样的体验：当一个网页访问的人数特别多的时候，打开网页就慢了，CC就是模拟多个用户(多少线程就是多少用户)不停地进行访问那些需要大量数据操作(就是需要大量CPU时间)的页面，造成服务器资源的浪费，CPU长时间处于饱满状态，永远都有处理不完的连接直至就网络拥塞，正常的访问被中止。

CC攻击的种类：

CC攻击的种类有三种，直接攻击，代理攻击，僵尸网络攻击，直接攻击主要针对有重要缺陷的WEB应用程序，一般说来是程序写的有问题的时候才会出现这种情况，比较少见。僵尸网络攻击有点类似于DDOS攻击了，从WEB应用程序层面上已经无法防御，所以代理攻击是CC攻击者一般会操作一批代理服务器，比方说100个代理，然后每个代理同时发出10个请求，这样WEB服务器同时收到1000个并发请求的，并且在发出请求后，立刻断掉与代理的连接，避免代理返回的数据将本身的带宽堵死，而不能发动再次请求，这时WEB服务器会将响应这些请求的进程进行队列，数据库服务器也同样如此，这样一来，正常请求将会被排在很后被处理，就象本来你去食堂吃饭时，一般只有不到十个人在排队，前面却插了一千个人，那么轮到你的机会就很小很小了，这时就出现页面打开极其缓慢或者白屏。

防御者：

1.应对当前系统了如指掌，如系统醉高负载、醉高数据处理能力，以及系统防御体系的强项与弱点

2.历史日志的保存、分析

3.对当前系统进行严格安全审计

4.上报公安相关部分，努力追溯攻击者

5.网站，能静态，就一定不要动态，可采取定时从主数据库生成静态页面的方式，对需要访问主数据库的服务使用验证机制。

6.防御者应能从全局的角度，迅速及时地发现系统正在处于什么程度的攻击、何种攻击，在平时，应该建立起攻击应急策略，规范化操作，免得在急中犯下低级错误

简易CC攻击防御策略

确定Web服务器正在或者曾经遭受CC攻击，那如何进行有效的防范呢?

(1).取消域名绑定

一般cc攻击都是针对网站的域名进行攻击，比如我们的网站域名是“ www.abc.com ”，那么攻击者就在攻击工具中设定攻击对象为该域名然后实施攻击。对于这样的攻击我们的措施是取消这个域名的绑定，让CC攻击失去目标。

(2).域名欺骗解析

如果发现针对域名的CC攻击，我们可以把被攻击的域名解析到127.0.0.1这个地址上。我们知道127.0.0.1是本地回环IP是用来进行网络测试的，如果把被攻击的域名解析到这个IP上，就可以实现攻击者自己攻击自己的目的，这样他再多的肉鸡或者代理也会宕机，让其自作自受。

(3).更改Web端口

一般情况下Web服务器通过80端口对外提供服务，因此攻击者实施攻击就以默认的80端口进行攻击，所以，我们可以修改Web端口达到防CC攻击的目的。运行IIS管理器，定位到相应站点，打开站点“ 属性 ”面板，在“ 网站标识 ”下有个TCP端口默认为80，我们修改为其他的端口就可以了。

(4).屏蔽IP

我们通过命令或在查看日志发现了CC攻击的源IP，就可以在防火墙中设置屏蔽该IP对Web站点的访问，从而达到防范攻击的目的。