TippingPoint IPS防御网络钓鱼攻击配置

潘猛 2007-03-20 发表

TippingPoint IPS防御网络钓鱼攻击配置

1. 对网络钓鱼攻击的防御

TP过滤器通过识别钓鱼攻击过程中的各个阶段的不同活动来阻断钓鱼攻击：

u 安装钓鱼网站WEB服务器

TP过滤器保护钓鱼者攻击WEB服务器,这些服务器被钓鱼者攻击,并用来显示与合法金融机构WEB相同的欺骗性的页面

u 发送大批量钓鱼邮件

TP过滤器阻断钓鱼垃圾邮件的传输

u 受害用户连接误导的URL地址

TP过滤器过滤器阻断受害者对钓鱼活动的响应,例如,阻断受害者对钓鱼网址的连接

u 钓鱼网页的显示

TP过滤器阻止钓鱼站点页面的显示

u 受害用户向钓鱼网站提交数据信息

TP过滤器阻止用户向钓鱼网站传输个人信息和金融信息

A缺省情况下，Phish类过滤器都是未启用的.

2. 防御网络钓鱼攻击配置

1) 选择“IPS >> Filter”在“Search”栏目中输入“phish”,搜索结果如图：

图表 1 Phish Edit

2) 编辑网络钓鱼攻击过滤器,设置响应动作为Block + Notify,对网络钓鱼攻击进行阻断

图表 2 Phish Edit