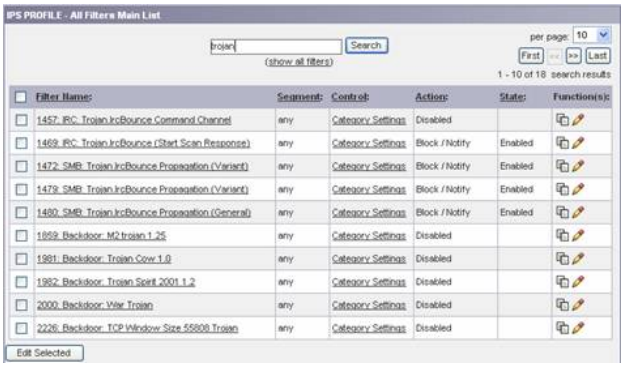
TippingPoint IPS 防御木马攻击配置

潘猛 2007-03-20 发表

TippingPoint IPS 防御木马攻击配置

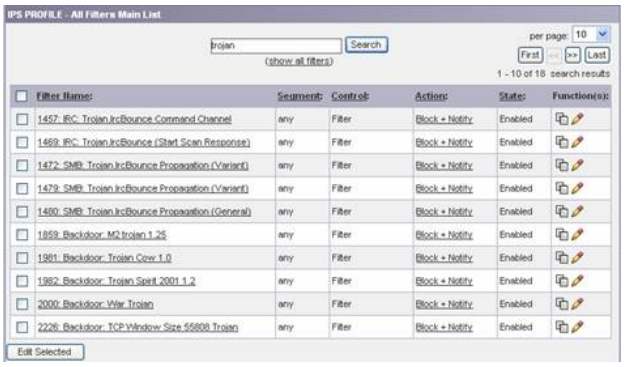
一　选择“IPS >> Filter”在“Search”栏目中输入“Trojan”,搜索结果如图:

A缺省情况下，木马后门类过滤器部分开启.



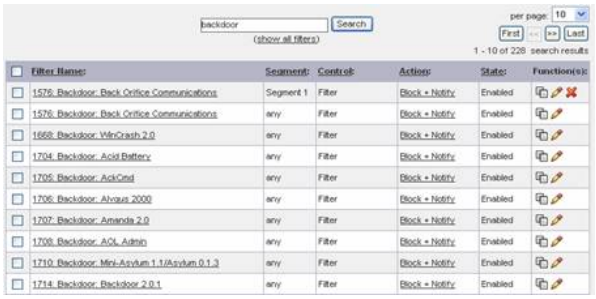
图表 1 Trojan Edit

二　编辑特洛依木马攻击过滤器,设置响应动作为“Block + Notify”,对特洛依木马进行阻断:



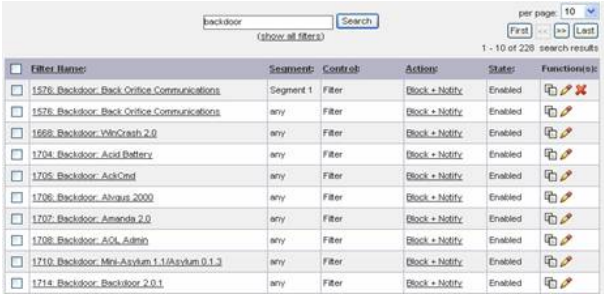
图表 2 Trojan Edit

三　选择“IPS >> Filter”在“Search”栏目中输入“Backdoor”,TP包含200多条关于后门攻击的过滤器,搜索结果如图:



图表 3 Backdoor Edit

四　编辑后门攻击过滤器,设置响应动作为“Block + Notify”,对后门进行阻断:



图表 4 Backdoor Edit