## TippingPoint IPS 防御木马攻击配置

— 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.

broan per page 11 (show al filters) 1-10 of 18 search 1-10 of 18 search						
	Filter Name:	Segment:	Control:	Action:	State:	Function(s)
	1457: IRC: Trojan & Bounce Command Channel	any	Category Settings	Disabled		60
	1469. RC: Troian IrcBounce (Start Scan Response)	any	Category Settings	Block / Notify	Enabled	60
	1472. SMB: Trojan IrcBounce Propagation (Variant)	any	Cetegory Settings	Block / Notify	Enabled	60
	1479: SMB Trojan IrcBounce Propagation (Variant)	any	Category Settings	Block / Notity	Enabled	60
	1480, SMB: Trojan IrcBounce Propagation (General)	any	Category Settings	Block / Notify	Enabled	60
	1859. Backdoor: M2 troian 1.25	any	Cetegory Settings	Disabled		B /
	1981: Backdoor: Trojan Cow 1.0	any	Colegory Settings	Disabled		00
	1982. Backdoor: Trojan Spirit 2001 1.2	any	Category Settings	Disabled		60
	2000. Backdoor: War Troian	any	Category Settings	Disabled		60
	2226: Backdoor: TCP Window Size 55808 Troian	any	Category Settings	Disabled		00

## 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:

broian		Search		pe	page: 10 👻
	(show all filter	υ		First I Last 1 - 10 of 18 search results	
Filter Barne:	Segment:	Control:	Action:	State:	Function(s):
1457: IRC: Troian IrcBounce Command Channel	any	Filter	Block + Notity	Enabled	60
1469. IRC: Trojan IrcBounce (Start Scan Response)	any	Filter	Block + Notity	Enabled	00
1472 SMB: Troisn IccBounce Propagation (Variant)	any	Fitter	Block + Notify	Enabled	00
1479: SMB: Troisn IncBounce Propagation (Variant)	any	Filter	Block + Notity	Enabled	60
1480: SMB: Trojan IrcBounce Propagation (General)	any	Filter	Block + Notify	Enabled	00
1859. Backdoor: M2 troien 1.25	any	Filter	Block + Notity	Enabled	00
1981. Backdoor: Troian Cow 1.0	any	Fitter	Block + Notify	Enabled	۳b /
1982 Backdoor: Trojan Spirit 2001 1.2	any	Filter	Block + Notify	Enabled	00
2000: Backdoor: War Troian	any	Filter	Block + Notify	Enabled	60
2226 Backdoor: TCP Window Size 55808 Trojan	any	Filter	Block + Notify	Enabled	00

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:

backdoor	(show all filter	Search D		per page: 10 V First V III V Last 1 - 10 of 228 search result		
Fifter Hame:	Seament:	Control	Actions	State:	Function(s):	
1576. Backdoor: Back Orifice Communications	Segment 1	Filter	Block + Notify	Enabled	602	
1576: Backdoor: Back Orifice Communications	arvy	Filter	Elock + Notify	Enabled	60	
1668. Backdoor. WinCrash 2.0	eny	Filter	Block + Notify	Enabled	00	
1704. Backdoor: Acid Battery	arry	Filter	Block + Notify	Enabled	00	
1705: Backdoor: AckOnd	eny	Filter	Block + Notity	Enabled	60	
1705: Backdoor: Alvaus 2000	ary	Fiter	Block + Notify	Enabled	600	
1707. Backdoor: Amanda 2.0	atry	Filter	Block + Notify	Enabled	600	
1708, Backdoor, AOL Admin	arry	Fitter	Block + Notity	Enabled	00	
1710. Backdoor. Mini-Asylum 1.1/Asylum 0.1.3	any	Filter	Block + Notify	Enabled	00	
1714. Backdoor: Backdoor 2.0.1	any	Filter	Block + Notity	Enabled	00	

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:

backdoor	(show all filter	Search		per page: 10 ¥ First >> Last	
Eilter Hame:	Seament	Control	Actions	State:	Function(s):
1576: Backdoor: Back Onlice Communications	Segment 1	Fiter	Block + Notity	Enabled	602
1576: Backdoor: Back Onlice Communications	any	Fiter	Block + Notify	Enabled	00
1668. Backdoor, WinCrash 2.0	any	Filter	Block + Notify	Enabled	60
1704. Backdoor: Acid Battery	any	Fiter	Block + Notify	Enabled	100
1705: Backdoor: AckCred	any	Filter	Block + Notify	Enabled	00
1706. Backdoor: Alvaus 2000	eny.	Fitter	Block + Notify	Enabled	80
1707: Backdoor: Amanda 2.0	any	Fitor	Block + Notify	Enabled	600
1708. Backdoor: AOL Admin	any	Filter	Block + Notify	Enabled	60
1710. Backdoor: Mini-Asylum 1.1/Asylum 0.1.3	(N <sup>1</sup> Y)	Fiter	Block + Notify	Enabled	60
1714. Backdoor, Backdoor 2.0.1	any	Fiter	Block + Notity	Enabled	00

图表 4 Backdoor Edit