(知) TippingPoint对间谍软件防御的典型配置

赵彪　2006-11-09 发表

TippingPoint对间谍软件防御的典型配置

一、 组网需求：
验证TippingPoint对间谍软件的防御功能。

二、 组网图

TippingPoint 1200：TOS Version：2.2.4.6519，Digital Vaccine：2.2.0.5720；
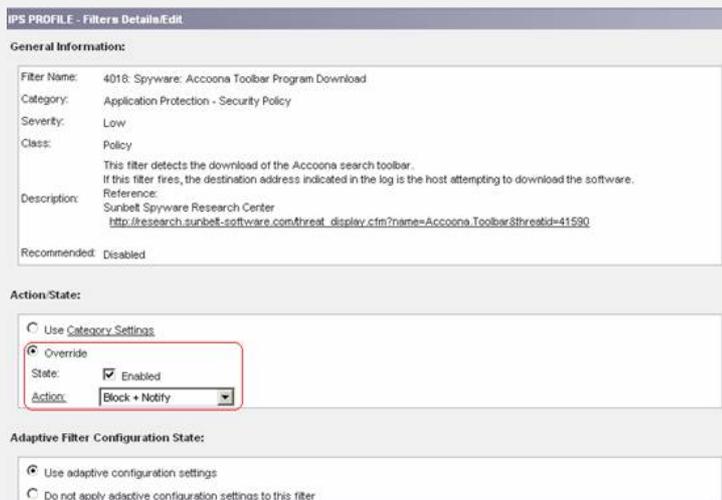PC： Windows XP，IE；
Server： 互联网上一台Web服务器。

三、 配置步骤

步骤1： "IPS"->"Filters"，查找"Spyware"过滤器：

步骤2： 选中过滤器"4018"并编辑其属性：

步骤3： 保存设置，查看状态：

	SpyWare	Search		per page: 10 ▾	
	(show all filters)			First | << | >> | Last	
				116 - 125 of 136 search results	

☐ **Filter Name:**	**Segment:**	**Control:**	**Action:**	**State:**	**Function(s):**
☐ 3915: Spyware: Look2Me Information Transfer	any	Category Settings	Disabled		🗐 ✏
☐ 3916: Spyware: Virtumonde Information Transfer	any	Category Settings	Disabled		🗐 ✏
☐ 3971: Spyware: 180Solutions/Zango Program Download	any	Category Settings	Disabled		🗐 ✏
☐ 4018: Spyware: Accoona Toolbar Program Download	any	Filter	Block + Notify	Enabled	🗐 ✏
☐ 4067: Spyware: BestOffers Program Download	any	Category Settings	Disabled		🗐 ✏
☐ 4068: Spyware: BestOffers Information Transfer	any	Category Settings	Disabled		🗐 ✏
☐ 4069: Spyware: BestOffers Pop-up Advertisement	any	Category Settings	Disabled		🗐 ✏
☐ 4082: Spyware: Malicious Anti-Spyware Program Download	any	Category Settings	Disabled		🗐 ✏
☐ 4083: Spyware: Malicious Anti-Spyware Program Download	any	Category Settings	Disabled		🗐 ✏
☐ 4104: Spyware: Starware Program Download	any	Category Settings	Disabled		🗐 ✏

Edit Selected				per page: 10 ▾	
	SpyWare	Search		First | << | >> | Last	
	(show all filters)			116 - 125 of 136 search results	

步骤4： 在PC上访问www.accoona.com，下载accoona工具条软件，发现下载不成功。

步骤5： 查看Block日志中有记录。

四、 配置关键点

默认间谍软件防范功能的过滤器没有启用。