系统应用现状及维护说明

——TDA

2011 年 9 月初创建

文档修订记录

文档修订日期	所修订的章节编号（可说明修订原因）	编辑人员
2011 年 9 月 8 日	文档初创	
2011 年 9 月 14 日	更新 IP 地址信息和线路信息	
2011 年 11 月 14 日		

目 录

1. 系统维护信息

1.1 系统访问方式

TDS 是趋势科技威胁发现系统的简称，主要由威胁发现设备，威胁日志收集分析以及威胁报表服务器组成。XX 证券部署的 TDS 系统 IP 配置以及管理登陆方式如下所示：

名称	IP 地址	管理方式	用户名密码
办公网 TDA 发现设备			
业务网 TDA 发现设备			
因特网 TDA 发现设备			
日志收集服务器			
控制台服务器 TMSP2.6 SP1			

1.2 服务厂商信息

建设维护厂商	姓名	角色	联系方式
趋势科技		工程师	
		商务	

1.3 软件资产信息

系统组件名称	软件版本	服务器位置	资产管理 IP
TDA 探针（办公终端区）		A2-16	
TDA 探针（广域网内联区）		A2-16	
TDA 探针（业务终端区）		A2-16	
TMSP			
Log Server			

1.4 硬件资产信息

1.4.1 办公终端区（测试设备）

硬件资产型号	
设备数量	1 台
资产管理 IP	

设备序列号	
机房机柜位置	7 层 A2-16
SPAN	
License 授权	2 个电口做采集，1 个电口做管理，连至“全局系统管理中心”

1.4.2 广域网内联网区

硬件资产型号	
设备数量	1 台
资产管理 IP	
设备序列号	
机房机柜位置	7 层 A2-16
SPAN	
License 授权	2 个电口做采集，1 个电口做管理，连至“全局系统管理中心”

1.4.3 业务终端区

硬件资产型号	
设备数量	1 台
资产管理 IP	
设备序列号	
机房机柜位置	7 层 A2-16
SPAN	
License 授权	2 个光口做采集，1 个电口做管理，连至“全局系统管理中心”

1.4.4 全局系统管理中心-TMSP

硬件资产型号	TMSP
设备数量	1 台
资产管理 IP	
设备序列号	
机房机柜位置	7 层 A2-16
SPAN	
License 授权	1 个电口做管理，连至“全局系统管理中心”

1.4.5 全局系统管理中心-Log Server

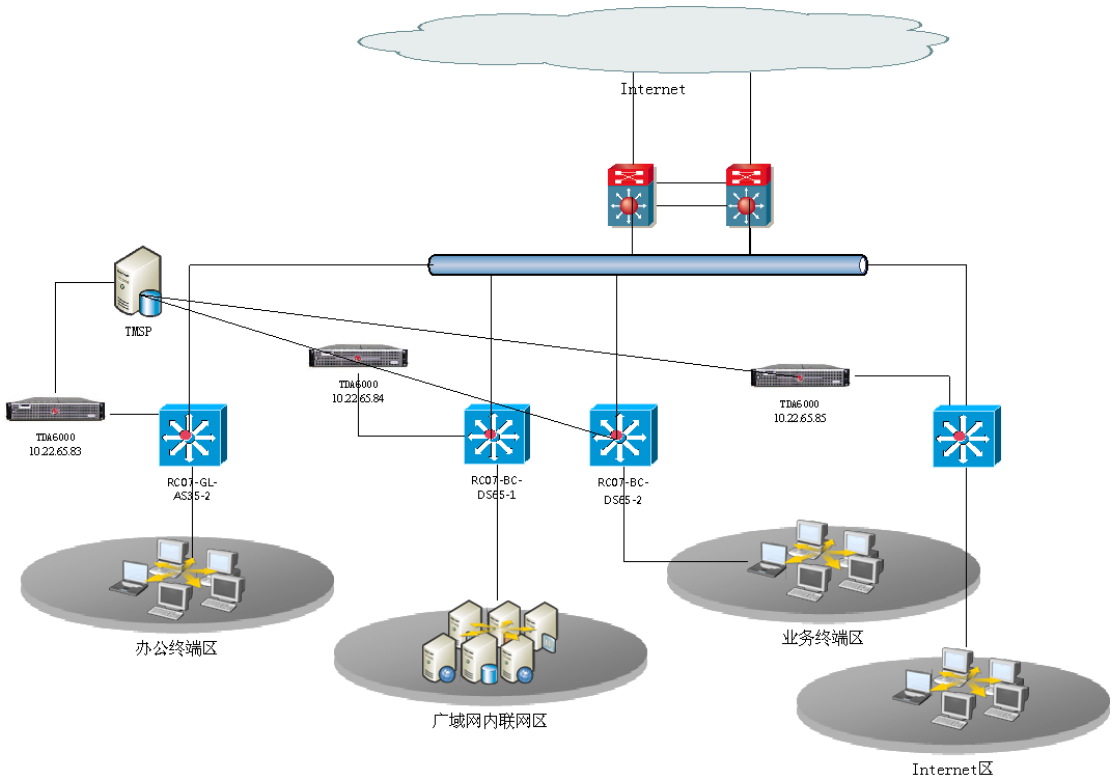
硬件资产型号	Log Server
设备数量	1 台
资产管理 IP	
设备序列号	
机房机柜位置	
SPAN	
License 授权	1 个电口做管理，连至“全局系统管理中心”

2. 物理连线

交换机名称	端口	跳线类型	设备名称	设备 IP	所在机柜	起始位置	端口
RC07-BC-DS65-1	G7/6	RJ45	办公终端 TDA	10.22.65.83	A2-16	25	
RC07-BC-DS65-2	G7/6	RJ45					
RC07-GL-AS35-1	G0/31	RJ45					
RC07-YT-AS35-1	G0/7	RJ45	因特网 TDA	10.22.65.85	A2-16	28	
RC07-YT-AS35-2	G0/7	RJ45					
RC07-GL-AS35-2	G0/29	RJ45					
RC07-JY-CS65-1	G1/8	LC 光纤	业务终端、广域网内联 TDA	10.22.65.84	A2-16	31	
RC07-JY-CS65-2	G1/8	LC 光纤					
RC07-GL-AS35-2	G0/31	RJ45					

起始位置重新确定一下。

3. 系统架构



XX 证券 TDS 系统拓扑示意图

4. 例行类维护工作

4.1 维护工作计划

以下是本系统涉及的所有例行维护工作，并以列表方式摘要执行计划。

	日例行	周例行	月例行
系统健康性检查		每周三	
问题设备处理	每周一至周五		

4.2 维护工作原则

针对 TDS 日报邮件逐条分析“建议”中的事件，然后对有问题的主机确认是否安装有防病毒客户端；如果装了，再到 officescan 中确认是否有病毒日志，事件是否对应（TDS 的检测范围较 osce 更宽）；如果未装，提示终端安装。

TDS 系统会根据对镜像过来的流量进行分析，找出有问题的设备，并通过 TMSP 日报通知管理员。由于发现的问题会比较多，因此请在处理 TDS 系统报表时遵循以下原则：

问题设备类型优先级：服务器区> 业务区>办公区

风险漏洞优先级：漏洞类风险>蠕虫>bot>DNS 解析>垃圾邮件>下载>其它

优先处理  叹号图标的客户端，这些客户端在过去的 3 天内连续发现高风险事件。

同时由于目前公司内部客户端通过代理服务器上网，从 Interent 上下载到的一些病毒文件在 TDA 上显示的源头会是代理服务器，因此在日报报警中，有时会出现代理服务器病毒排名较高的情况，对于此种情况可将代理服务器滤掉。

4.3 维护处理流程：

4.3.1 设备定位：

TDS 日报指出的问题设备的 IP 地址以及风险类型信息，当确认为处理优先级之后，需要对设备进行定位。

定位顺序为：

首先在防病毒平台上查找该 IP，确认其是否安装杀毒软件；

然后通过北信源 VRV 系统定位到具体人员姓名；

最后如果依然找不到，则联系中信证券管理员协助定位。

4.3.2 现场问题处理：

在现场进行问题处理，采用方法为：

首先检查设备是否安装防病毒软件，如未安装，则安装防病毒软件；

其次检查防病毒软件是否有病毒信息，如存在病毒记录，且病毒信息与 TDS 检测到的现象可匹配，则按照病毒特征采用相关处理方法；

如没有病毒记录，采用小工具进行问题处理（小工具有 Sysclaen，闪电杀毒手，windows 清理助手等，对于生产系统，请不要使用此类工具）；

最后使用信息收集工具 SIC 收集信息提交后台进行分析。

4.3.3 问题跟踪：

对于已经处理过的设备，在今后两天的日报中，着重检查其是否还被 TDS 系统检测。

4.3.4 配合使用的专杀工具：

1、闪电杀毒手：

2、Windows 清理助手：

3、SIC 日志收集工具。

详细使用方法参考附件内容。

4.4 TDS 事件处理举例：

1、 TDS 系统给管理员发送 TDA 日报通知邮件，基本信息如下：

发件人： antivirus
发送时间： 2011-11-09 10:30:09
收件人： antivirus
抄送：
主题： Threat_Discovery_Service_Daily_Report_2011/11/08_for_中信证券

事件描述： TDS Daily Report
对象/信息：

亲爱的用户，您好！
昨日贵单位的TDA设备主要检测到以下威胁，具体详情请参考附件PDF文档，谢谢！

威胁行为	影响	检测次数	主要受影响客户机			处理建议	备注
			组	IP地址	主机名		
Malicious Bot	连接恶意网站下载病毒	14	中信证券办公	10.24.22.11	zg-lchen6.[redacted]o.com	闪电杀毒手清毒，阻断BOT服务器	该主机建立了BOT感染的TCP协议通讯信息。
			Default		zg-lchen6.ci[redacted].com		
			中信证券办公	10.24.8.181	meng-bootcamp.c[redacted].com		

TDA 的日报邮件正文的主要部分为一个风险威胁统计表，其默认按检测次数排序，如下表所示：

威胁行为	影响	检测次数	主要受影响客户机			处理建议	备注
			组	IP 地址	主机名		
Malicious Bot	连接恶意网站下载病毒	14	xx 证券办公	10.24.22.11	zg-lchen6.xx.com	闪电杀毒手清毒，阻断 BOT 服务器	该主机建立了 BOT 感染的 TCP 协议通讯信息。
			Default		zg-lchen6.xx.com		
			xx 证券办公	10.24.8.181	meng-bootcamp.xx.com		
			Default		meng-bootcamp.xx.com		
虚假随机域名查询	组建僵尸计算机网络	10	Default	10.24.15.5	zongban-zhangling6.xx.com	使用闪电杀毒手和 downad 专杀工具清毒	随机查询虚假域名
			Default	10.24.9.36	it-weixu3.xx.com		
			Default	10.24.18.3	pc-201105031610		
			Default	10.24.22.58	zg-gangwang.xx.com		
			Default	10.24.10.77	lenovo-m4600		
Vundo 木马		2	xx 证券办公	10.24.8.145	it-limenghang8.xx.com		该主机建立了 Vundo 木马的 HTTP 协议请求

							信息。
发送恶意电子邮件	传播病毒和垃圾邮件	1	xx 证券服务器	10.23.175.243	10.23.175.243	闪电杀毒手清毒	该主机发送了多封含已知恶意文件的电子邮件附件的邮件。
恶意软件感染	影响系统运行，网络性能，下载新病毒	1	xx 证券服务器	10.23.161.114	10.23.161.114	使用闪电杀毒手杀毒	ADW_CDNHELPER.CK
Downad/ Conficker 蠕虫	攻击网络	1	xx 证券服务器	10.23.171.117	th-zhangzhan3.xx.com	参考 Downad 解决方法	这台客户机正在使用 Waledac bot 相关加密 P2P 协议
MS08-067_SERVER_SERVICE_PATH_CANONICALIZATION_EXPLOIT	传播病毒	1	xx 证券服务器	10.23.171.117	th-zhangzhan3.xx.com	安装系统补丁，使用闪电杀毒手和 downad 专杀工具清毒	这台主机正通过系统漏洞攻击网络内的其他主机

以上表格中列举了 TDA 发现有问题的计算机信息，由于涉及的 IP 与问题计算机较多，不可能一一处理。因此需要按照优先级及影响程度进行处理。

2、 判断需有限处理的设备：

从以上表格我们可做以下判断：

1、 以上列举的 IP 涉及 10.23 和 10.24 网段，10.23 属于服务器网段，因此该网段设备处理优先级较高，因此 10.23.171.117、10.23.161.114、10.23.175.243 这 3 台设备处理优先级较高；

2、 从风险判断，Downad/Conficker 蠕虫和 MS08-067_SERVER_SERVICE_PATH_CANONICALIZATION_EXPLOIT 属于漏洞风险及扫描性蠕虫，因此其风险级别最高。

3、 经确认 10.23.161.114 为代理服务器 IP，因此其从处理清单中去除。

4、 Malicious Bot 涉及到的 2 个 IP 亦为办公网 IP，处理优先级往下排。

5、 虚假域名查询涉及到的几个 IP 为办公区域，处理优先级再往下排

综上所述，该日报，管理员当日处理设备的优先级顺序如下：

最高优先级：10.23.171.117（th-zhangzhan3.xx.com），该设备由于未安装补丁，在尝试攻击其他计算机，需要在当天定位，并进行处理；

第二优先级：10.23.175.243，该设备在发送恶意电子邮件，需要确认其是否为邮件服务器，如为邮件服务器，也可参考代理服务器处理方式，将其排除。

第三优先级：Malicious Bot 涉及到的两个 IP，10.24.22.11 和 10.24.8.181，建议检查是否安装有防病毒软件，并收集 SIC 日志给后台分析一下，确认是否有新病毒。

第四优先级：虚假随机域名查询涉及到的几个 IP 地址；

最低优先级：以该日报内容为例，其他涉及 IP 可暂缓处理。

最高优先级涉及到的设备，请在当天处理完毕，第二优先级则建议在两到三天内进行处理，第三优先级涉及设备建议在一周内至少找一到两台进行处理，摸清处理此类计算机的方法。

3、 问题处理流程：

确认处理优先级之后，则进入问题处理流程，整个问题处理流程建议如下所示：

1、 设备定位：TDS 日报指出的问题设备的 IP 地址以及风险类型信息，当确认为处理优先级之后，需要对设备进行定位。定位顺序为：首先在防病毒平台上查找该 IP，确认其是否安装杀毒软件；如找不到，则通过北信源 VRV 系统定位到具体人员姓名；如依然找不到，则联系 xx 证券管理员协助定位；

2、 现场问题处理：在现场进行问题处理，采用方法为：首先检查设备是否安装防病毒软件，如未安装，则安装防病毒软件；检查防病毒软件是否有病毒信息，如存在病毒记录，且病毒信息与 TDS 检测到的现象可匹配，则按照病毒特征采用相关处理方法；如没有病毒记录，采用小工具进行问题处理（小工具有闪电杀毒手，windows 清理助手等，对于生产系统，请不要使用此类工具）；最后使用信息收集工具 SIC 收集信息提交后台进行分析。

3、 问题跟踪：对于已经处理过的设备，在今后的日报中，检查其是否还被 TDS 系统检测。

5. 常用配置指导

TDS 在上线安装完毕之后，需要进行一些简单配置，以便其检测信息能够更好的被解读和使用。主要涉及以下几个方面：

1、 设定受监控的网络：

TDA 默认会把 3 个私有网段（10.0.0.0/8，172.16.0.0-172.31.255.255，192.168.0.0/16）加入可信站点 default，但是在使用过程中，建议根据企业的实际情况对监控的网络进行调整。如下所示：

2、 增加已注册的服务信息，对于一些服务器（如 DNS 服务器，Proxy 服务器，邮件服务器）建议添加这些服务器的信息，如下所示：

3、 增加潜在风险检测例外：对于一些服务器如代理服务器，邮件服务器，DNS 服务器，其本身存在一些转发性质，可能会被检测到有风险行为，建议将其加入潜在风险检测例外。

4、 检查更新配置：定期检查更新，确认设备正常更新。

6. FAQ 及问题跟踪

为了持续积累该系统的问题处理经验，本章节请维护人员定期更新。要求客观、准确地描述当

前问题现象，复现方式，以及最终处理措施；对于当前尚未完全解决的问题也请标注出准确状态和跟进人员。

编辑本章节时，请注意采用二级标题摘要问题名称。对于严重问题请在二级标题中标注“严重-”字样。

7. 附件

7.1 闪电杀毒手工具使用说明：


闪电杀毒手产品使用手册.doc

7.2 Windows 清理助手使用说明

7.3 SIC 工具使用手册


SIC使用手册.doc