

## China Pattern 部署手册

版本: 3.6

日期: 2008.04.18

一. Pattern King计划及China Pattern介绍 .....	1
二. Officescan部署China Pattern .....	2
2.1 Officescan部署China Pattern的方法 .....	2
2.2 Officescan部署China Pattern后的Rollback的方法 .....	4
三. 部署China Pattern专用引擎(含Intellitraps(智能扫描)技术).....	6
3.1 Intellitraps介绍 .....	6
3.2 在部署IntelliTrap引擎前的必要设置 (务必进行).....	6
3.3 如何部署Intellitraps扫描引擎 .....	6
3.4 如何确认升级完成.....	7
3.5 如何确认IntelliTrap(智能扫描)扫描结果.....	7
四. 如何处理IntelliTrap的检测 .....	8
4.1 用户确认为误报(用户认为是正常加壳程序).....	8
4.2 如果用户无法确认是否误报, 很可能为未知病毒.....	10
4.3 趋势科技Packer-Gen. xxx可疑文件收集工具.....	10
五. DCE 5.3 提高病毒清除率 .....	10
5.1 DCE 5.3 介绍 .....	10
5.2 DCE5.3 部署的步骤 .....	10
六. 其他产品部署China Pattern方法 .....	11
七. 趋势科技厂商资源 .....	12

## 一. Pattern King 计划及 China Pattern 介绍

### Pattern King 计划:

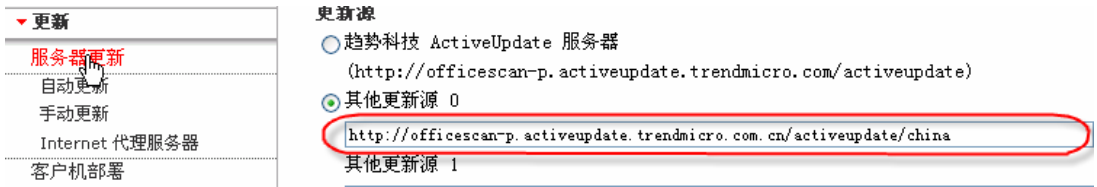

趋势科技于 2006 年 9 月开始推出的 Pattern King 计划, 内容是根据中国区流行病毒的特点, 专门制作的**中国区病毒码(以下统称为 China Pattern)**. China Pattern 是在全球病毒码(同步更新)的基础上, 加入加入了针对本地流行病毒的病毒库, 启用了智能扫描技术(IntelliTrap), 和启发式通用检测(Generic Rule)技术, 配合先进的 DCE5 损害清除引擎, 可以将检测到的已知和未知病毒实时清除掉, 全面提升了趋势科技防毒产品的病毒检测率和查杀率, 受到用户的广泛欢迎.

### 中国区病毒码的优势:

1. China Pattern 基于全球病毒码, 并随全球病毒码同步更新.
2. China Pattern 额外加入了针对本地流行病毒的病毒库, 累积达 5 万多, 并且不断增长中.
3. China Pattern 启用了智能扫描技术(IntelliTrap), 对蠕虫(worm)和加壳过的(Packer)恶意软件等有很高的检测率, 并防范未知病毒.
4. China Pattern 启用了启发式通用检测(Generic Rule)技术来检测同一家族的不同病毒变种, 有效提高检测率, 并防范未知病毒.
5. 配合先进的 DCE5 损害清除引擎, 可以将检测到的已知和未知病毒实时清除掉, 提高了查杀率.
6. China Pattern 的性能:  
到目前为止(版本号:4.554.60) 只比全球病毒码文件(30.2 MB) 大 1M 左右.  
目前没有用户报因为中国区病毒码导致的性能问题
7. China Pattern 已经从 2006.9 推出到现在已快达一年之久, 性能稳定.
8. China Pattern 已经推广到全国, 现在有 90%的客户正在使用 China Pattern, 受到用户广泛欢迎.

## 二. Officescan 部署 China Pattern

### 2.1 Officescan 部署 China Pattern 的方法

产品	OfficeScan 7.0/7.3													
方法	更改 pattern 更新源													
URL	<a href="http://officescan-p.activeupdate.trendmicro.com.cn/activeupdate/china">http://officescan-p.activeupdate.trendmicro.com.cn/activeupdate/china</a>													
修改方法	<p><b>自动更新:</b> OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 自动更新 (Automatic Update) → 更新源 (Update Source) → 其他更新源 (Other Update Source), 填入上述的 URL。</p> <p><b>手动更新:</b> OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 手动更新 (Manually Update) → 更新源 (Update Source) → 其他更新源 (Other Update Source), 填入上述的 URL。</p> 													
验证方法	<p>点击 OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 手动更新 (Manual Update) → 更新 (Update), 出现病毒码版本号 x.yyy.60 (注意最后是.60 结尾, 也有可能是.70 或.80 结尾)</p> <p><b>可用更新</b></p> <table border="1" data-bbox="319 1377 1300 1512"> <tr> <td><input checked="" type="checkbox"/> 病毒码</td> <td>3.601.60</td> </tr> <tr> <td><input checked="" type="checkbox"/> 通用防火墙驱动程序</td> <td>1.2.1029</td> </tr> </table> <p>立即更新    &lt; 返回</p> <p>更新成功后同样显示:</p>  <table border="1" data-bbox="311 1691 1396 1825"> <thead> <tr> <th>组件</th> <th>版本</th> <th>上次更新时间</th> </tr> </thead> <tbody> <tr> <td><b>防病毒</b></td> <td></td> <td></td> </tr> <tr> <td>病毒码</td> <td>3.601.60</td> <td>2006-7-25 11:08:58</td> </tr> </tbody> </table>	<input checked="" type="checkbox"/> 病毒码	3.601.60	<input checked="" type="checkbox"/> 通用防火墙驱动程序	1.2.1029	组件	版本	上次更新时间	<b>防病毒</b>			病毒码	3.601.60	2006-7-25 11:08:58
<input checked="" type="checkbox"/> 病毒码	3.601.60													
<input checked="" type="checkbox"/> 通用防火墙驱动程序	1.2.1029													
组件	版本	上次更新时间												
<b>防病毒</b>														
病毒码	3.601.60	2006-7-25 11:08:58												
备注	<p>注意: 如果只需要测试部分电脑, 请把部分电脑的更新源指向到 <a href="http://officescan-p.activeupdate.trendmicro.com.cn/activeupdate/china">http://officescan-p.activeupdate.trendmicro.com.cn/activeupdate/china</a> 如图:</p>													

## 更新源 ?

可以选择某些客户机使之从该防毒墙网络版服务器以外的源进行更新。替代的更新源可以是一个远程代理或一台 ActiveUpdate 服务器。

- 标准更新源 (从防毒墙网络版服务器更新)
- 定制的更新源
- 如果所有定制源均不可用或未找到, 则从防毒墙网络版服务器更新

### 定制的更新源列表

		添加		编辑		删除		移动	
顺序	客户机 IP:	从	到	更新源					
<input type="checkbox"/>	1	10.28.132.58	10.28.132.68	http://officescan-p.activeupdate.trendmicro.com.cn/activeupdate/china					

在发送通知后, 新设置将对客户机生效。

通知所有客户机

## 2.2 Officescan 部署 China Pattern 后的 Rollback 的方法

恢复方法

**情况一：初次尝试 China Virus Pattern 后，想立刻退回使用 Global Virus Pattern.**  
操作步骤：

1. 打开控制台，点击更新>还原，选择病毒码文件还原的“还原服务器和客户机”按钮，如图：

### 还原

病毒码文件	
当前版本：	3.729.60
上次更新时间：	2006-9-7 14:15:52
先前版本：	3.725.50
上次更新时间：	2006-9-6 0:05:27

单击还服务器和客户机可用先前的版本替换最近的  
还原到先前版本

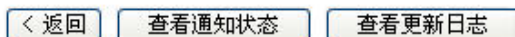


此时，会出现客户机树页面，选择需要回退的客户机，并点击“通知”按钮。  
以下画面，提示还原成功：

### 复原

客户机已收到复原该组件的通知。

复原后，病毒码和扫描引擎的预设部署（客户机预设更新）将不予执行，直到服务器通知客户机进行更新或在自动部署中定义的事件触发了部署。



2. 将病毒码更新源，修改为趋势全球更新服务器

#### 自动更新：

OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 自动更新 (Automatic Update) → 更新源 (Update Source) → 趋势科技 ActiveUpdate 服务器

#### 手动更新：

OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 手动更新 (Manually Update) → 更新源 (Update Source) → 趋势科技 ActiveUpdate 服务器。

**情况二：China Virus Pattern 已经使用了一段时间，想立刻退回使用 Global Virus Pattern**

操作步骤：

1. 打开控制台，点击更新>还原，选择病毒码文件还原的“还原服务器和客户机”按钮，如图：

## 还原

### 病毒码文件

当前版本:	3.729.60
上次更新时间:	2006-9-7 14:15:52
先前版本:	3.725.50
上次更新时间:	2006-9-6 0:05:27

单击还服务器和客户机可用先前的版本替换最近的  
还原到先前版本

还原服务器和客户机

与服务器同步

此时，会出现客户机树页面，选择需要回退的客户机，并点击“通知”按钮。  
以下画面，提示还原成功：

## 复原



客户机已收到复原该组件的通知。

复原后，病毒码和扫描引擎的预设部署（客户机预设更新）将不予执行，直到服务器通知客户机进行更新或在自动部署中定义的事件触发了部署。

< 返回

查看通知状态

查看更新日志

2. 将病毒码更新源，修改为趋势全球更新服务器

### 自动更新：

OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 自动更新 (Automatic Update) → 更新源 (Update Source) → 趋势科技 ActiveUpdate 服务器

### 手动更新：

OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 手动更新 (Manually Update) → 更新源 (Update Source) → 趋势科技 ActiveUpdate 服务器。

3. 执行手动更新：

点击 OfficeScan 管理控制台 → 更新 (Update) → 服务器更新 (Server Update) → 手动更新 (Manual Update) → 更新 (Update)

### 三. 部署 China Pattern 专用引擎(含 Intellitrapp(智能扫描)技术)

#### 3.1 Intellitrapp 介绍

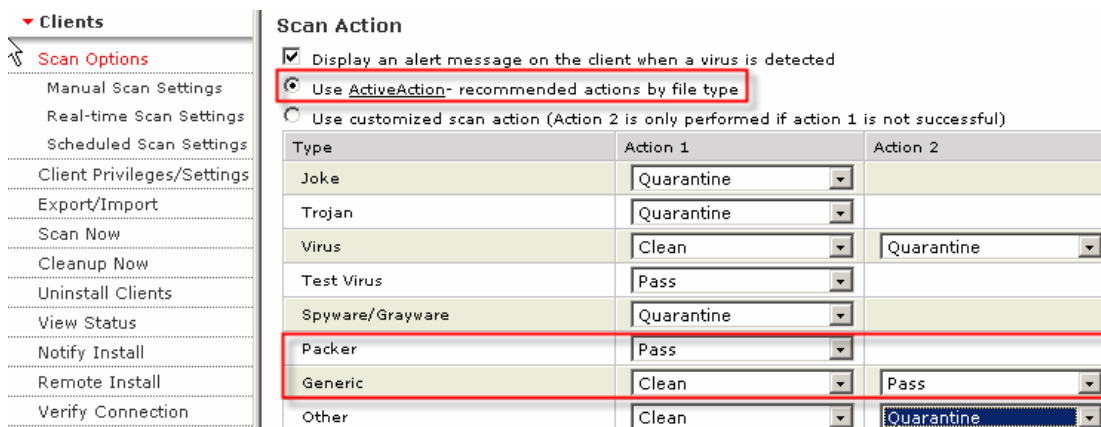
1. Intellitrapp 针对网络中存在的病毒特点, 在识别 bot 类程序以及特殊文件结构上进行了增强, 可提高对未知病毒的识别率。

2. Intellitrapp 技术配合它的黑白名单以及不断加强的 unpack 技术, 可以有效的增强查毒能力。

以下提到的 intellitrapp 引擎即是指 China Pattern 专用引擎。

#### 3.2 在部署 IntelliTrap 引擎前的必要设置 (务必进行)

在客户使用 China Pattern 的 IntelliTrap 技术初期, 为了将启发式扫描的误判风险降到最低, 趋势科技建议您对 IntelliTrap 的检测类型 Packer 和 Generic 扫描动作做以下的设置:



**Scan Action**

Display an alert message on the client when a virus is detected

Use ActiveAction- recommended actions by file type

Use customized scan action (Action 2 is only performed if action 1 is not successful)

Type	Action 1	Action 2
Joke	Quarantine	
Trojan	Quarantine	
Virus	Clean	Quarantine
Test Virus	Pass	
Spyware/Grayware	Quarantine	
Packer	Pass	
Generic	Clean	Pass
Other	Clean	Quarantine

#### 注意:

1. 必须把**手动扫描, 实时扫描, 预设扫描**的设置设在 ActiveAction 上
2. 或者使用定制扫描, 但是必须
  - a. 把 Packer 设置在 Pass 上,
  - b. 然后把 Generic 的 Action1 设置为 Clean, Action2 设置为 Pass。

#### 3.3 如何部署 Intellitrapp 扫描引擎

启用 Intellitrapp 智能扫描技术, 需要将 Officescan 的病毒扫描引擎 vsapi 升级到 8.511.1002.

方法: 把更新服务器指向新的更新源

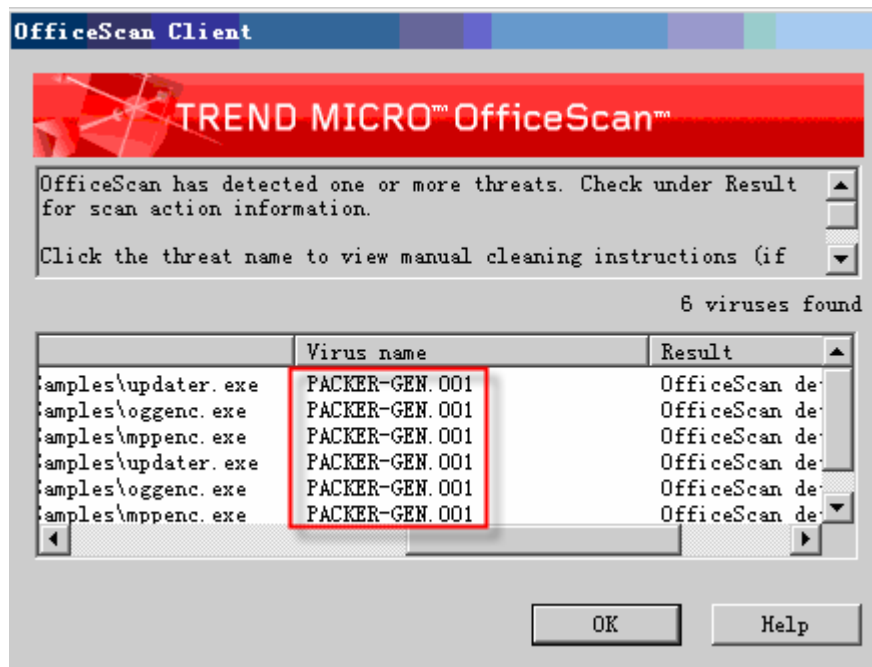
<http://officescan-p.activeupdate.trendmicro.com.cn/activeupdate/china>

### 3.4 如何确认升级完成

组件	最新版本	最新	过时	更新百分比
Windows NT/2000/XP/Server 2003 版的客户机程序	7.3	1	0	100%
基于 x64 体系结构的 Windows XP/Server 2003 版的客户机程序	7.3	0	0	0%
基于 IA64 体系结构的 Windows XP/Server 2003 版的客户机程序	7.3	0	0	0%
Windows 95/98/ME 版的客户机程序	7.3	0	0	0%
病毒码	4.802.60	1	0	100%
Windows NT/2000/XP/Server 2003 版的扫描引擎	8.511.1002	1	0	100%
基于 x64 体系结构的 Windows XP/Server 2003 版的扫描引擎	8.500.1002	0	0	0%
基于 IA64 体系结构的 Windows XP/Server 2003 版的扫描引擎	8.500.1002	0	0	0%
Windows 95/98/ME 版的扫描引擎	8.320.1003	0	0	0%

### 3.5 如何确认 IntelliTrap(智能扫描)扫描结果

若 IntelliTrap(智能扫描)扫描到 packer 文件, 会报 packer-gen.00X (x=1~6)的检测名



#### 四. 如何处理 IntelliTrap 的检测

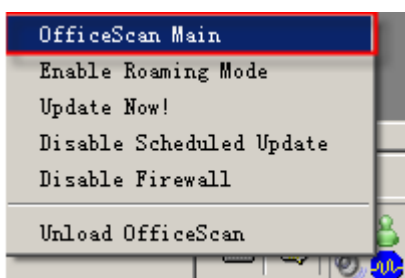
##### 4.1 用户确认为误报(用户认为是正常加壳程序)

###### 1) 用户先自行消除误报事件(临时):

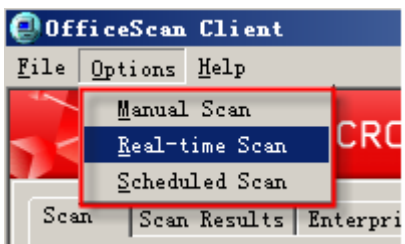
方法: 用户可以采用“设置例外列表”的方式对该类文件(或所在目录)特殊处理:

把文件或者目录加入到 Officescan 例外列表的操作说明如下:

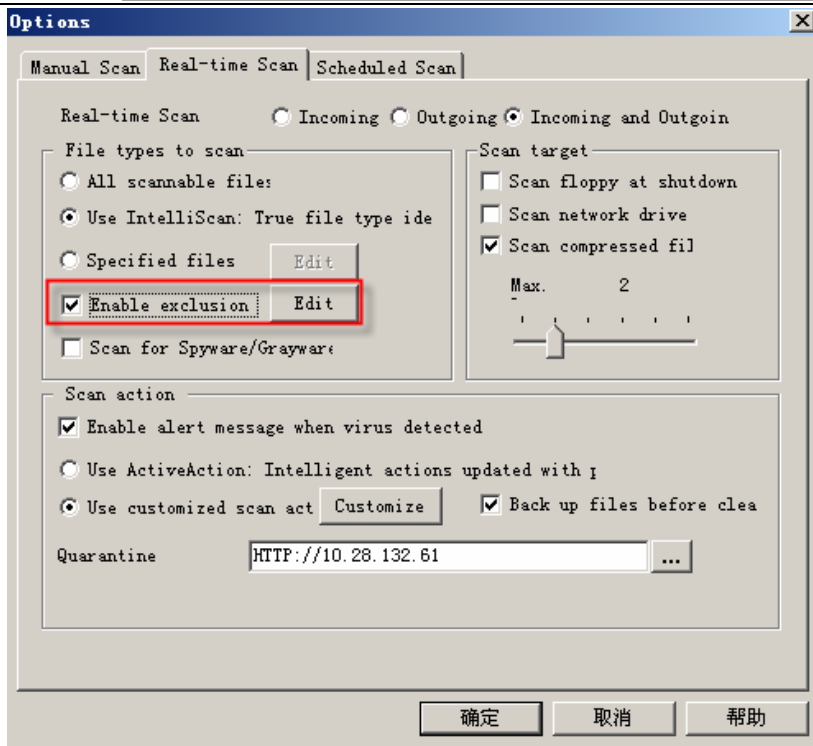
打开 Officescan 客户端主画面:



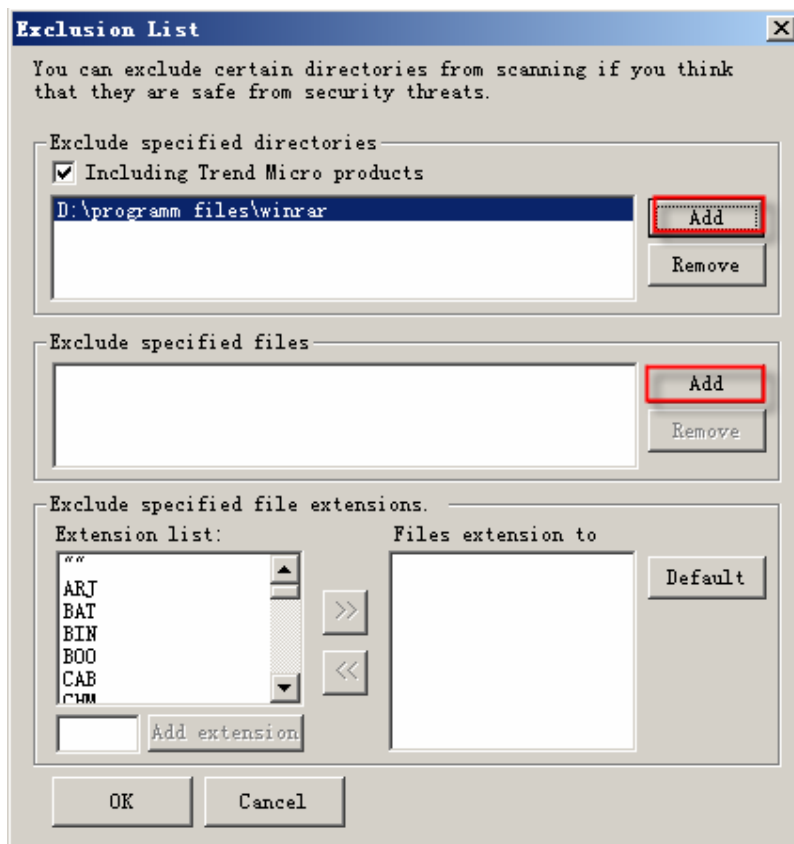
请在 Real-time Scan, Manual Scan 和 Scheduled Scan 中做以下设置:



选择例外列表:



加入例外目录或者例外的文件名称：



具体设置的方法可以参考管理员手册或者帮助手册。

## 2) 用户提交该误报文件(或文件集)到趋势科技,制作 WhitePattern

对于误报文件趋势科技有一整套处理流程和联系窗口:

请用户收集您系统中误报文件,打包加密(密码: virus)压缩成 zip 后提交到趋势科技 China Pattern 专用邮箱:

[China\\_Pattern@trendmicro.com.cn](mailto:China_Pattern@trendmicro.com.cn)

注意: 邮件主题请注明”确认 FA”字样+”XXX 公司”,这样可以加速处理流程.

## 4.2 如果用户无法确认是否误报,很可能为未知病毒

请使用趋势科技开发的 PackerCollector 自动收集 packer(见后).

并将收集到的 Packer zip 包提交到趋势科技 China Pattern 专用邮箱:

[China\\_Pattern@trendmicro.com.cn](mailto:China_Pattern@trendmicro.com.cn)

注意: 邮件主题请注明”未知 Packer”字样+”XXX 公司”,这样可以加速处理流程.

## 4.3 趋势科技 Packer-Gen. xxx 可疑文件收集工具

工具介绍:

Packer-Gen. xxx (001-006) 是 China Pattern 查出来的可疑病毒,考虑到用户收集时候比较麻烦,需要到每个目录去复制收集。目前趋势科技有制作一个收集 Packer-Gen. xxx 的小工具,这个工具可以自动收集所有的可疑文件。具体说明请参考压缩包中的 Readme。

请到以下地址下载 Packer 收集工具,收集完成请发送到 [China\\_Pattern@trendmicro.com.cn](mailto:China_Pattern@trendmicro.com.cn),我们会及时处理。

Packer 收集工具:

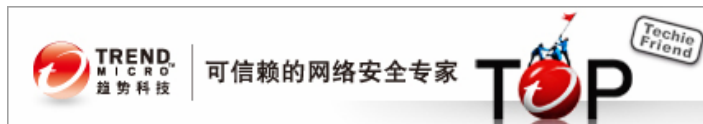
[http://support.trendmicro.com.cn/Anti-Virus/China-Pattern/Pk\\_tools/PackerCollectionTool/](http://support.trendmicro.com.cn/Anti-Virus/China-Pattern/Pk_tools/PackerCollectionTool/)

# 五. DCE 5.3 提高病毒清除率

## 5.1 DCE 5.3 介绍

DCE (Damage Cleanup Engine) 5.3 是趋势科技用来清除病毒的工具, DCE 5.3 在原来 DCE 3.98 的基础上,对于无法清除、无法隔离的病毒使用了先进的技术,从而可以提高清除病毒的能力。

## 5.2 DCE 5.3 部署的步骤



安装 Hotfix 即可支持 DCE5.3, 然后把升级地址指向 China Pattern AU, 就会更新到 DCE5.3。  
对于 Officescan 不同的版本, 需要安装不同的 Hotfix:

### Officescan7.0 必须安装 hotfix 1286 以支持 DCE5.3

#### A) 简体中文版:

[http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE 5.0 hotfix/OSCE7.0/osce 70 win\\_sc\\_hfb1286.exe](http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE%205.0%20hotfix/OSCE7.0/osce_70_win_sc_hfb1286.exe)

#### B) 英文版:

[http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE 5.0 hotfix/OSCE7.0/osce 70 win\\_en\\_hfb1286.exe](http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE%205.0%20hotfix/OSCE7.0/osce_70_win_en_hfb1286.exe)

### Officescan7.3 必须安装 hotfix 1120 以支持 DCE5.3

#### A) 简体中文版:

[http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE 5.0 hotfix/OSCE7.3/osce 73 win\\_sc\\_hfb1120.exe](http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE%205.0%20hotfix/OSCE7.3/osce_73_win_sc_hfb1120.exe)

#### B) 英文版:

[http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE 5.0 hotfix/OSCE7.3/osce 73 win\\_en\\_hfb1120.exe](http://support.trendmicro.com.cn/TM-Product/Beta/pk2006/DCE%205.0%20hotfix/OSCE7.3/osce_73_win_en_hfb1120.exe)

指向 China Pattern AU

<http://officescan-p.activeupdate.trendmicro.com/activeupdate/apac>

### 确认更新到 DCE5.3

损害清除模板	874	1	0	100%
间谍软件/灰色软件清除特征码	266	1	0	100%
损害清除引擎	5.3.1103	1	0	100%
通用防火墙驱动程序	1.2.1020	1	0	100%
网络病毒特征码	.....	.	.	.....

## 六. 其他产品部署 China Pattern 方法

其他产品要部署 China Pattern 需要把各个产品的更新 URL 指向到以下更新站点:

**TMCM:** <http://cm-p.activeupdate.trendmicro.com.cn/activeupdate/china>

**CSS/CSM3.0:** <http://csm-p.activeupdate.trendmicro.com.cn/activeupdate/china>

**CSS/CSM3.5:** <http://csm3-p.activeupdate.trendmicro.com.cn/activeupdate/china>

**IGSA1.0/1.5:** <http://igsa-p.activeupdate.trendmicro.com.cn/activeupdate/china>

**IWSA3.1 :** <http://iwsa31-p.activeupdate.trendmicro.com.cn/activeupdate/china>

**SMD3.0:** <http://smln-p.activeupdate.trendmicro.com.cn/activeupdate/china>

**SMEX7 :** <http://smex-p.activeupdate.trendmicro.com.cn/activeupdate/china>

**SPNT :** <http://serverprotect-p.activeupdate.trendmicro.com.cn/activeupdate/china>

## 七. 趋势科技厂商资源

- ◆ 800 免费售后热线:800-820-8839
- ◆ 售后电子邮件地址:service@trendmicro.com.cn
- ◆ China Pattern 收集到的 Packer 或 FA 样本处理专用邮箱:  
[China\\_Pattern@trendmicro.com.cn](mailto:China_Pattern@trendmicro.com.cn) (注意:对于其他av案件,不予处理)
- ◆ 趋势科技中文网站: www.trendmicro.com.cn
- ◆ 病毒查询:www.trendmicro.com.cn/vinfo
- ◆ 中文版资料及软件下载: ftp.trendmicro.com.cn

附注: 打 800 电话或者发邮件到 Service 邮箱时请注明自己是 China Pattern 用户或者请注明自己的病毒码版本。