



# How to Analyse Virus Log

Simon Wang

Product Technical Consultant



# 1 日志导出

Log>Virus Logs>OfficeScan Clients>Export to CSV

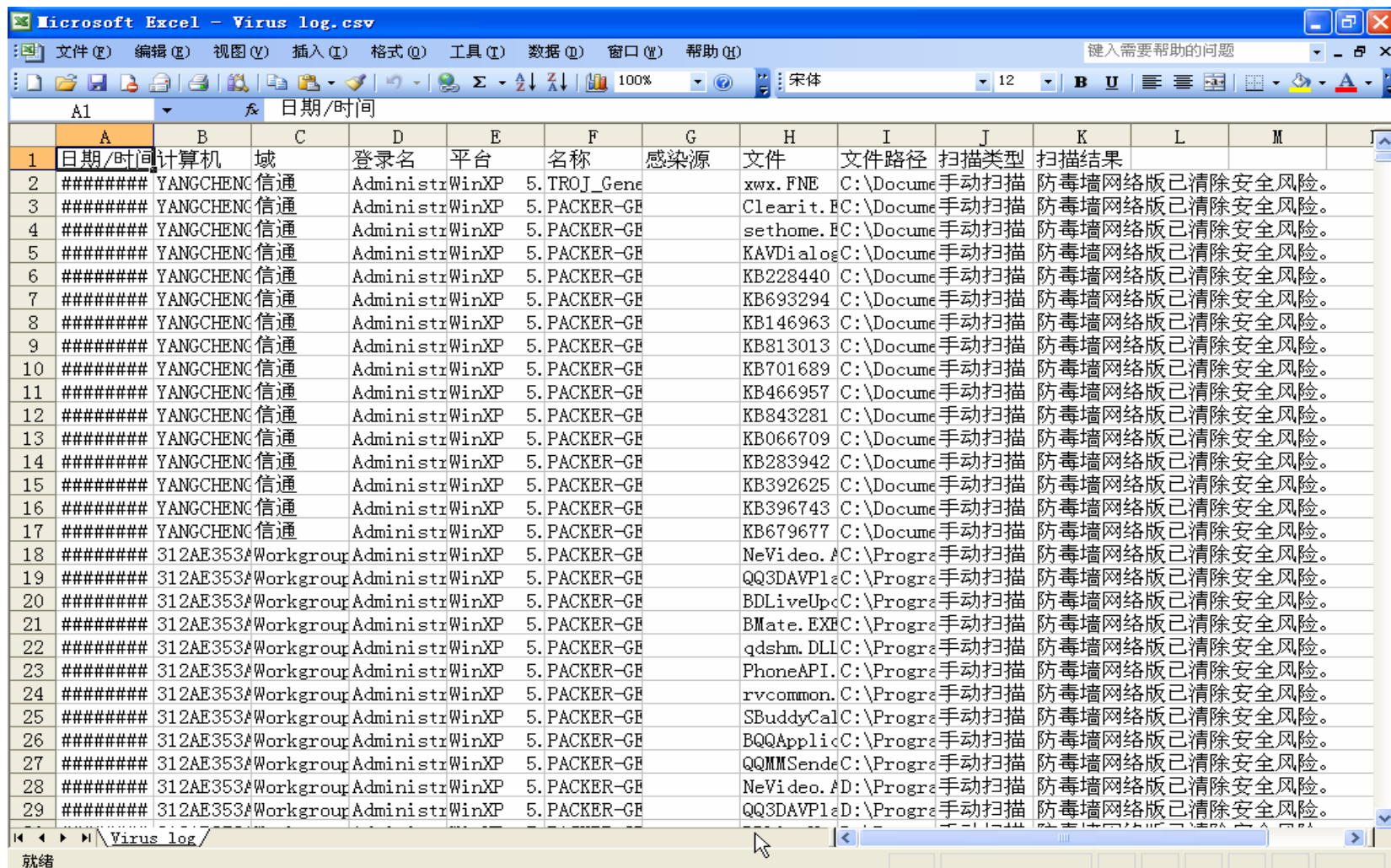
**View Virus Logs**

**Time:**  Select a time period: Last 7 days  Specify a range:  
From    
To

**Scan Types:**  Manual Scan  
 Real-time Scan  
 Scheduled Scan  
 Scan Now  
 Damage Cleanup Services

**Sort by:** Date and time

## 2 通过Excel打开



Microsoft Excel - Virus log.csv

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 数据(D) 窗口(W) 帮助(H) 键入需要帮助的问题

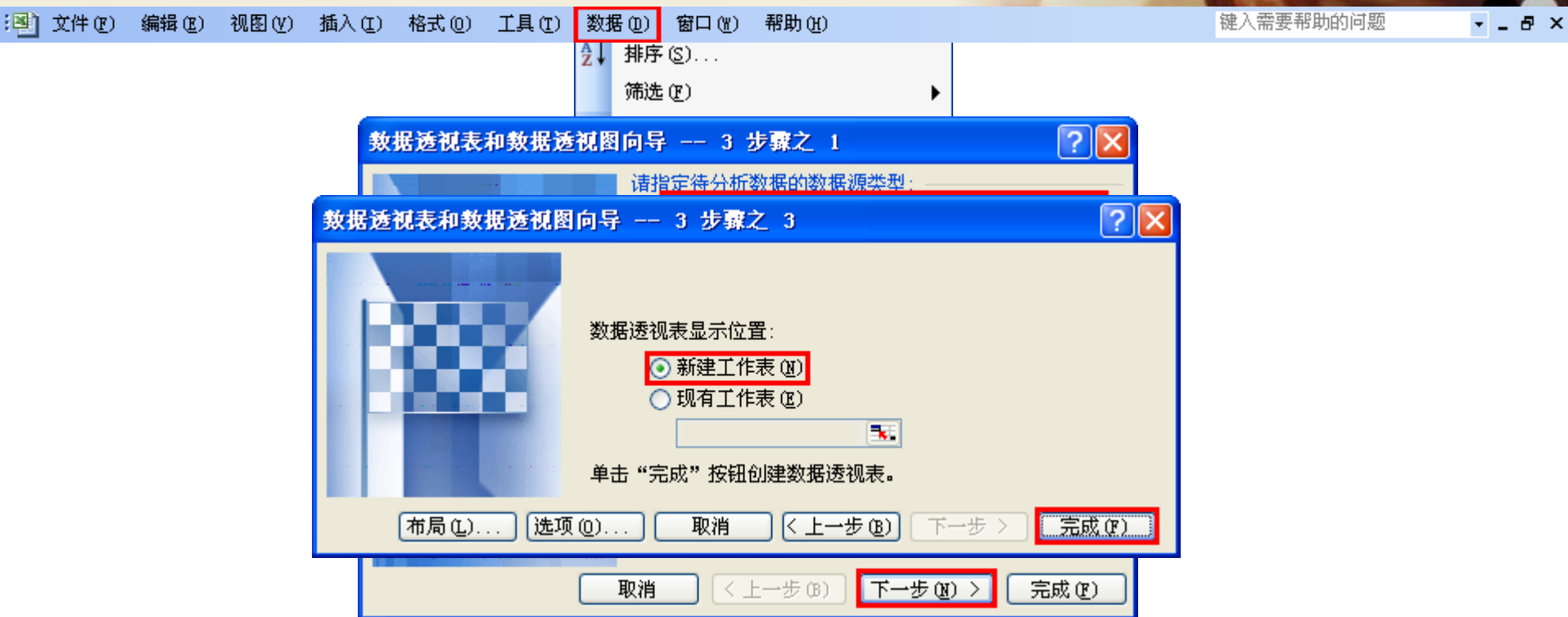
宋体 12 B U

日期/时间

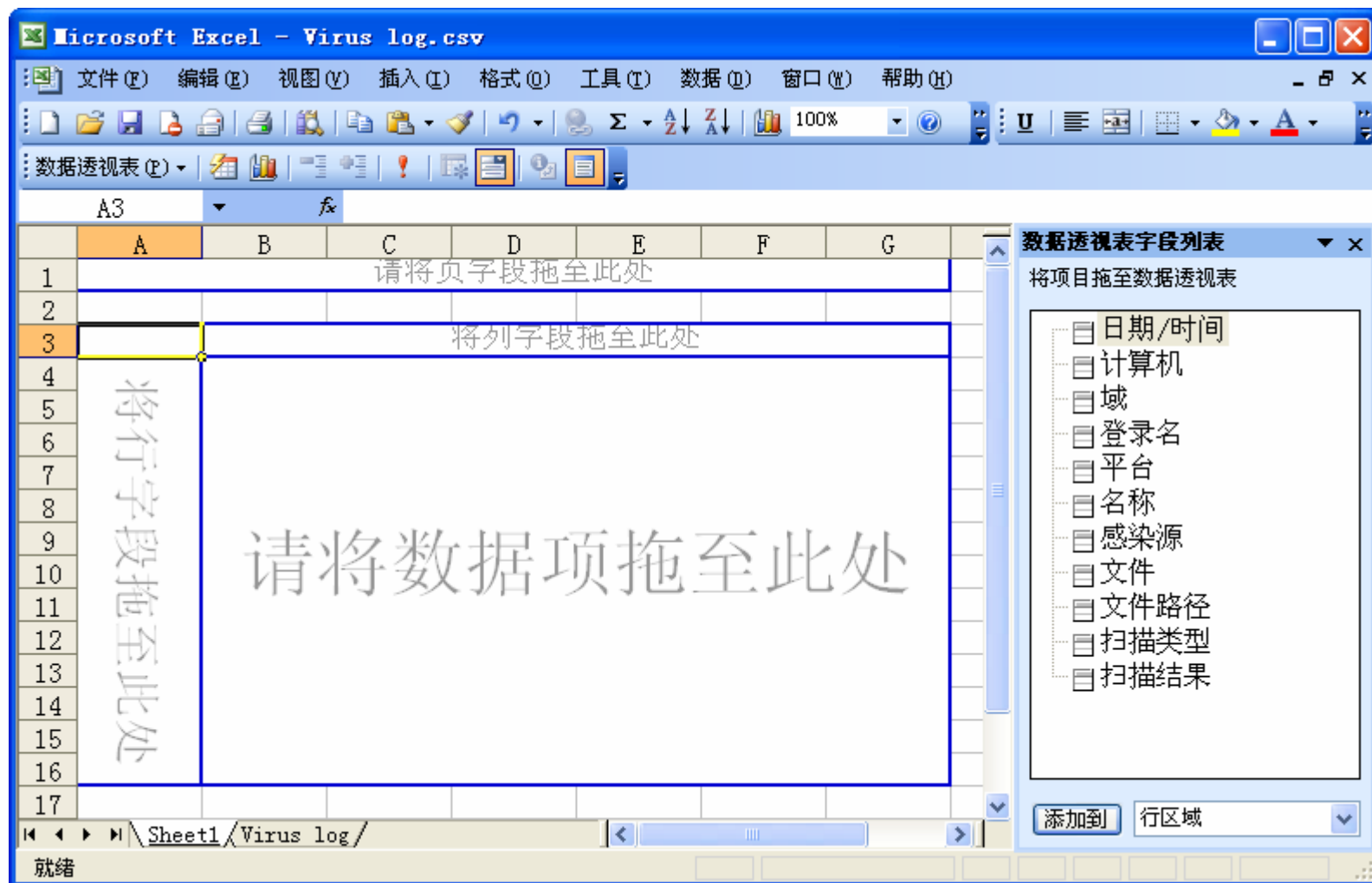
A1	A	B	C	D	E	F	G	H	I	J	K	L	M
1	日期/时间	计算机	域	登录名	平台	名称	感染源	文件	文件路径	扫描类型	扫描结果		
2	#####	YANGCHENG	信通	Administr	WinXP	5. TROJ_Gene		xwx.FNE	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
3	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		Clearit.FC	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
4	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		sethome.FC	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
5	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KAVDialogC	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
6	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB228440	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
7	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB693294	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
8	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB146963	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
9	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB813013	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
10	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB701689	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
11	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB466957	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
12	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB843281	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
13	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB066709	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
14	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB283942	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
15	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB392625	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
16	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB396743	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
17	#####	YANGCHENG	信通	Administr	WinXP	5. PACKER-GE		KB679677	C:\Docume	手动扫描	防毒墙网络版已清除安全风险。		
18	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		NeVideo.AC	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
19	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		QQ3DAVPl	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
20	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		BDLiveUp	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
21	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		BMate.EXE	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
22	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		qdshm.DLL	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
23	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		PhoneAPI	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
24	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		rvcommon	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
25	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		SBuddyCal	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
26	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		BQQApplic	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
27	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		QQMMSend	C:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
28	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		NeVideo.A	D:\Progre	手动扫描	防毒墙网络版已清除安全风险。		
29	#####	312AE353A	Workgroup	Administr	WinXP	5. PACKER-GE		QQ3DAVPl	D:\Progre	手动扫描	防毒墙网络版已清除安全风险。		

就绪

# 3 数据处理



## 4 报表生成



Microsoft Excel - Virus log.csv

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 数据(D) 窗口(W) 帮助(H)

数据透视图表(P)

A3

1 请将页字段拖至此处

2

3 将列字段拖至此处

4 将行字段拖至此处

5

6

7

8

9 请将数据项拖至此处

10

11

12

13

14

15

16

17

就绪

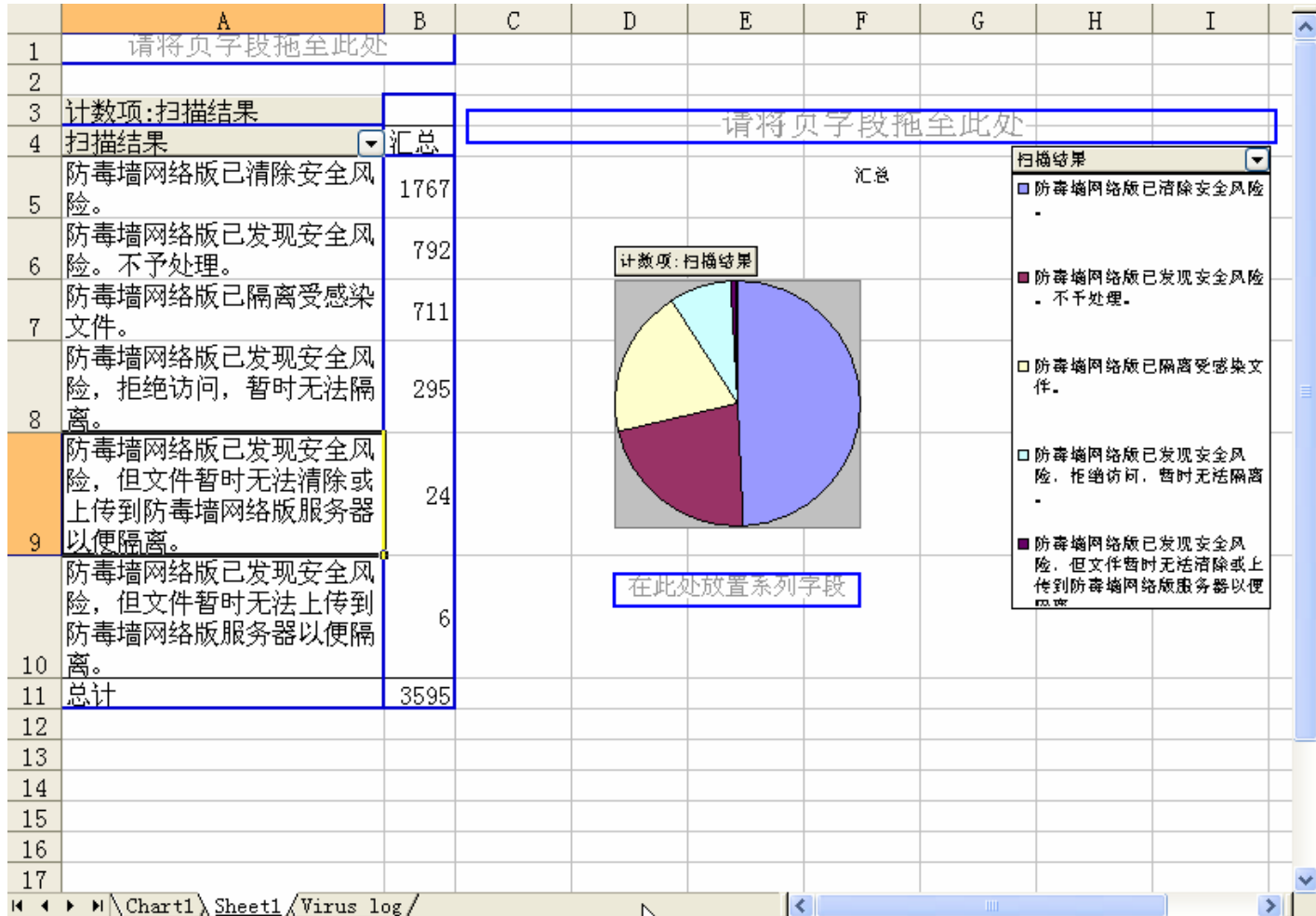
数据透视表字段列表

将项目拖至数据透视图表

- 日期/时间
- 计算机
- 域
- 登录名
- 平台
- 名称
- 感染源
- 文件
- 文件路径
- 扫描类型
- 扫描结果

添加到 行区域

# Case 1 整体情况汇总



# Case 2 计算机感染情况

	A	B	C	D	E	F
3	计数项:扫描结果					
4	扫描结果	计算机	名称	文件路径	文件	汇总
5	防毒墙网络版已隔离受感染文件。	1C90C65B00674FD	ADW_BORAN.FE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\	cx_ad1086.exe	1
6			ADW_CDNUF.K	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\	setup168.exe	1
7			ADW_PIGSEARCH.AF	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\	tdsetup.exe	1
8		237EF5C01331483	ADW_PIGSEARCH.A	C:\Program Files\wsearch\	Mouse1.dll.tmp (Mouse1.dll)	1
9					Search.exe.tmp (Search.exe)	1
10					SearchM.dll.tmp (SearchM.dll)	1
11		312AE353AB18499	ADW_BORAN.AM	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\	up_15.tmp	1
12					up_1F.tmp	1
13					up_4.tmp	2
14					up_5.tmp	1
15					up_5C.tmp	1
16					up_6.tmp	1
17					up_8.tmp	1
18					433D1BEDB3FE4B4	ADW_CNSMIN.G
19		63AF441AF2614AE	ADW_CNSMIN.G	C:\System Volume Information\restore{4A868894-65BC-436D-BE76-14D2EF42B7AA}\RP298\	A0047034.DLL	1
20		85E34F16446643D	ADW_AGENT.JXF	C:\WINDOWS\system32\	hotunist.exe	1
21			ADW_CNSMIN.G	C:\PROGRA~1\3721\	alliveex.DLL	1
				C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\		1

# Case 3 病毒感染情况

	A	B	C	D	E	F
3	计数项:扫描结果					
4	扫描结果	名称	计算机	文件路径	文件	汇总
5	防毒墙网络版已隔离受感染文件。	ADW_ADMEDIA.AF	WINXP-SP2	C:\DOCUME~1\Admin\LOCALS~1\Temp\	xp4.tmp	1
6		ADW_ADMEDIA.AG	WINXP-SP2	C:\DOCUME~1\Admin\LOCALS~1\Temp\	xpE.tmp	1
7		ADW_AGENT.FAN	MY-TOMATO	C:\	~del.tmp	1
8		ADW_AGENT.JXF	85E34F16446643D	C:\WINDOWS\system32\	hotunist.exe	1
9		ADW_BAIDU.E	WEIQIAOSUO	C:\WINDOWS\system32\	znmq_bd.exe	1
10		ADW_BDSEARCH.AN	MY-TOMATO	C:\WINDOWS\system32\drivers\	Albus.SYS	9
11		ADW_BDSEARCH.BR	LENOVO-41102E88	C:\DOCUME~1\Owner\LOCALS~1\Temp\116\	cdnprot.sys	1
12			NONMI-3V05YA2NH	C:\System Volume Information\_restore {D212AEF0-87C2-4DF0-BB9A-19C5A1565882} \RP162\	A0021375.sys	1
13				C:\System Volume Information\_restore {D212AEF0-87C2-4DF0-BB9A-19C5A1565882} \RP163\	A0022363.sys	1
14				C:\System Volume Information\_restore {D212AEF0-87C2-4DF0-BB9A-19C5A1565882} \RP166\	A0022513.sys	1
15				C:\System Volume Information\_restore {D212AEF0-87C2-4DF0-BB9A-19C5A1565882} \RP168\	A0023626.sys	1
16		ADW_BORAN.AM		312AE353AB18499	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\	up_15.tmp
17					up_1F.tmp	1
18					up_4.tmp	2
19					up_5.tmp	1
20					up_5C.tmp	1
21					up_6.tmp	1