中国安天实验室

基于网络流和包的病毒检测

肖新光

Xfocus
焦点峰会
2002

前言

- 蠕虫和其他网络病毒的日益蔓延和流行，VXER对黑客技术的利用日趋成熟，网络安全技术和反病毒技术的融合趋势日趋明显。
- 开发者希望扩展firewall、IDS和GAP产品的反病毒能力，与传统的反病毒厂商的文件级别的检测技术结合是一个解决思路，但也面临一些问题。
- 本专题试图探讨，网络安全技术与反病毒技术的一个结合点——基于流和包的病毒检测。

一、两种检测粒度的比较

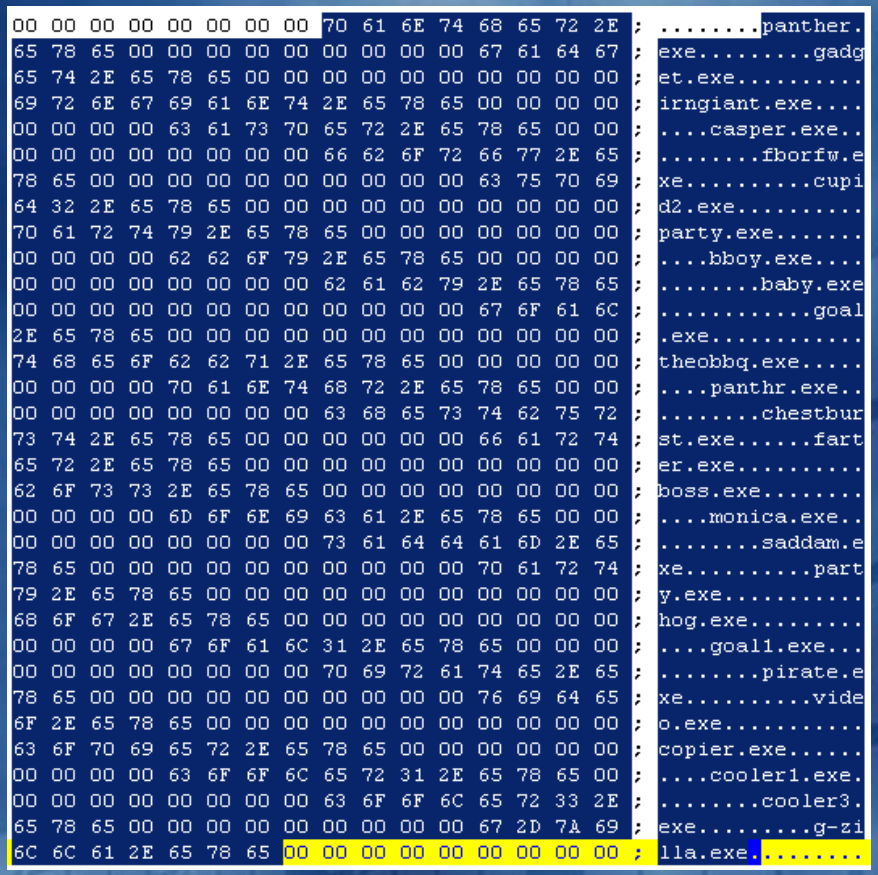
- snort中及其粗糙的反病毒规则作为我们今天批判的靶子…
- 最新的snort在其virus.rules中，用了多达24条规则来检测名为NewApt的蠕虫，占了全部VX规则的28%。

粗糙的文件名检测法

```
content: "filename=\"THEOBBQ.EXE\"";
content: "filename=\"COOLER3.EXE\"";
content: "filename=\"PARTY.EXE\"";
content: "filename=\"HOG.EXE\"";
content: "filename=\"GOAL1.EXE\"";
content: "filename=\"PIRATE.EXE\"";
content: "filename=\"VIDEO.EXE\"";
content: "filename=\"BABY.EXE\"";
content: "filename=\"COOLER1.EXE\"";
content: "filename=\"BOSS.EXE\"";
content: "filename=\"G-ZILLA.EXE\"";
content: "filename=\"COYPER..EXE\"";
```

```
content: "filename=\"GADGET.EXE\"";
content: "filename=\"IRNGLANT.EXE\"";
content: "filename=\"CASPER.EXE\"";
content: "filename=\"FBORFW.EXE\"";
content: "filename=\"SADDAM.EXE\"";
content: "filename=\"BBOY.EXE\"";
content: "filename=\"MONICA.EXE\"";
content: "filename=\"GOAL.EXE\"";
content: "filename=\"PANTHER.EXE\"";
content: "filename=\"CHESTBURST.EXE\"";
content: "filename=\"FARTER.EXE\"";
content: "filename=\"CUPID2.EXE\"";
```

粗检测粒度的表现



```
00 00 00 00 00 00 00 00 70 61 6E 74 68 65 72 2E ; ........panther.
65 78 65 00 00 00 00 00 00 00 00 00 67 61 64 67 ; exe.........gadg
65 74 2E 65 78 65 00 00 00 00 00 00 00 00 00 00 ; et.exe..........
69 72 6E 67 69 61 6E 74 2E 65 78 65 00 00 00 00 ; irngiant.exe....
00 00 00 00 63 61 73 70 65 72 2E 65 78 65 00 00 ; ....casper.exe..
00 00 00 00 00 00 00 00 66 62 6F 72 66 77 2E 65 ; ........fborfw.e
78 65 00 00 00 00 00 00 00 00 00 00 63 75 70 69 ; xe..........cupi
64 32 2E 65 78 65 00 00 00 00 00 00 00 00 00 00 ; d2.exe..........
70 61 72 74 79 2E 65 78 65 00 00 00 00 00 00 00 ; party.exe.......
00 00 00 00 62 62 6F 79 2E 65 78 65 00 00 00 00 ; ....bboy.exe....
00 00 00 00 00 00 00 00 62 61 62 79 2E 65 78 65 ; ........baby.exe
00 00 00 00 00 00 00 00 00 00 00 00 67 6F 61 6C ; ............goal
2E 65 78 65 00 00 00 00 00 00 00 00 00 00 00 00 ; .exe............
74 68 65 6F 62 62 71 2E 65 78 65 00 00 00 00 00 ; theobbq.exe.....
00 00 00 00 70 61 6E 74 68 72 2E 65 78 65 00 00 ; ....panthr.exe..
00 00 00 00 00 00 00 00 63 68 65 73 74 62 75 72 ; ........chestbur
73 74 2E 65 78 65 00 00 00 00 00 00 66 61 72 74 ; st.exe......fart
65 72 2E 65 78 65 00 00 00 00 00 00 00 00 00 00 ; er.exe..........
62 6F 73 73 2E 65 78 65 00 00 00 00 00 00 00 00 ; boss.exe........
00 00 00 00 6D 6F 6E 69 63 61 2E 65 78 65 00 00 ; ....monica.exe..
00 00 00 00 00 00 00 00 73 61 64 64 61 6D 2E 65 ; ........saddam.e
78 65 00 00 00 00 00 00 00 00 00 00 70 61 72 74 ; xe..........part
79 2E 65 78 65 00 00 00 00 00 00 00 00 00 00 00 ; y.exe...........
68 6F 67 2E 65 78 65 00 00 00 00 00 00 00 00 00 ; hog.exe.........
00 00 00 00 67 6F 61 6C 31 2E 65 78 65 00 00 00 ; ....goal1.exe...
00 00 00 00 00 00 00 00 70 69 72 61 74 65 2E 65 ; ........pirate.e
78 65 00 00 00 00 00 00 00 00 00 00 76 69 64 65 ; xe..........vide
6F 2E 65 78 65 00 00 00 00 00 00 00 00 00 00 00 ; o.exe...........
63 6F 70 69 65 72 2E 65 78 65 00 00 00 00 00 00 ; copier.exe......
00 00 00 00 63 6F 6F 6C 65 72 31 2E 65 78 65 00 ; ....cooler1.exe.
00 00 00 00 00 00 00 00 63 6F 6F 6C 65 72 33 2E ; ........cooler3.
65 78 65 00 00 00 00 00 00 00 00 00 67 2D 7A 69 ; exe.........g-zi
6C 6C 61 2E 65 78 65 00 00 00 00 00 00 00 00 00 ; lla.exe.........
```

通过对病毒的分析来看，Worm.NewApt附件文件清单是26个，而不是24个。

Rule(s) from C&D没有错误，但Capture&Decode之外，希望能补充进，Code&Disassemblers

附件文件名检测方式弊端

- 对于那些随机选择附件名文件名或者提取本机文件的文件名作为自身名字的蠕虫无能为力。
- 一个同名的正常附件，带来误报造成用户的恐慌。同时，修改文件名对于修改蠕虫是最容易的。

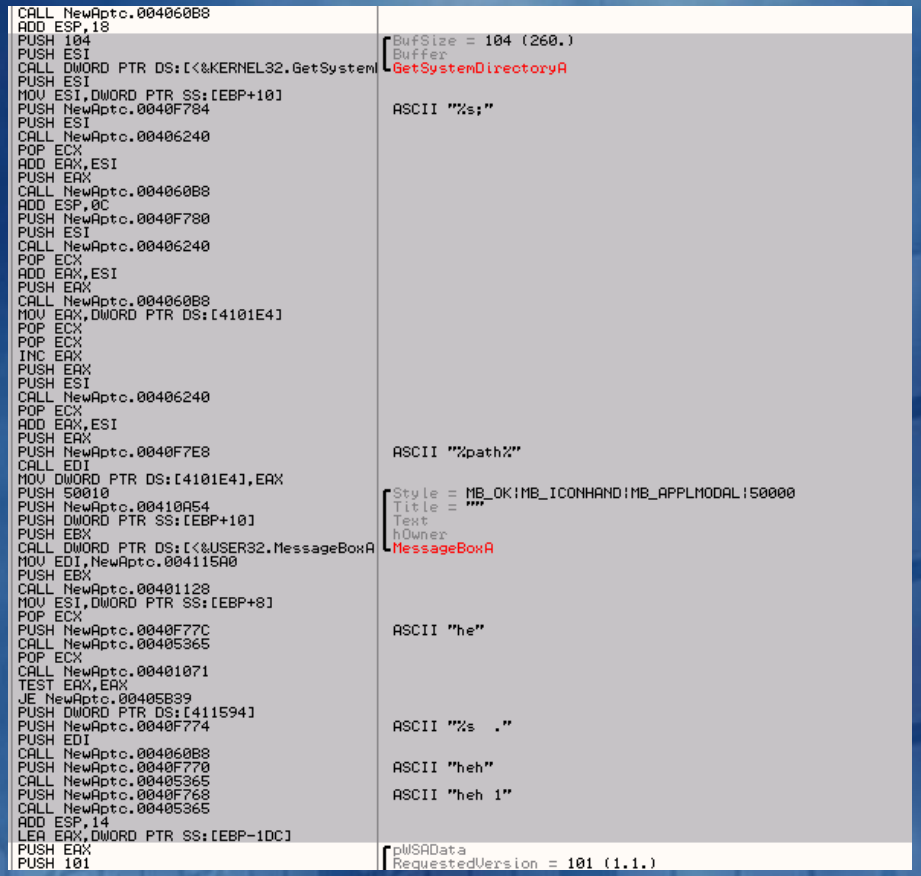
细粒度检测

- 站在基于文件系统的病毒分析来看，I-worm.NewApt完全可以靠文件体中如下的特征串来检测：|680401000056FF152CC04000568B75106884F7400056E8CC0800005903C650E83B07000083C40C6880F7400056E8B508000005903C650……|

问题（一）网络检测与文件检测的不同

- 蠕虫在网络传输中的形态，不是2进制文件，而是经过编码后的，下面就是病毒特征码所对应的base64编码：
  GgEAQAAVv8VLMBAAFaLdRBohPdAAFbozAgAAFkDxlDoOwcAAIPEDGiA90AAVui1CAAAWQPGUOgkBwAAoeQBQQBZWUBQVuidCAAAWQPGUGjo90AA/9ej5AFBA……
- 同时新的问题产生：|0d 0a|如何处理？

问题（二）特征码质量



```
CALL NewAptc.004060B8
ADD ESP,18
PUSH 104                                  ; BufSize = 104 (260.)
PUSH ESI                                  ; Buffer
CALL DWORD PTR DS:[<&KERNEL32.GetSystemI  ; GetSystemDirectoryA
PUSH ESI
MOV ESI,DWORD PTR SS:[EBP+10]
PUSH NewAptc.0040F784                     ; ASCII "%s;"
PUSH ESI
CALL NewAptc.00406240
POP ECX
ADD EAX,ESI
PUSH EAX
CALL NewAptc.004060B8
ADD ESP,0C
PUSH NewAptc.0040F780
PUSH ESI
CALL NewAptc.00406240
POP ECX
ADD EAX,ESI
PUSH EAX
CALL NewAptc.004060B8
MOV EAX,DWORD PTR DS:[4101E4]
POP ECX
POP ECX
INC EAX
PUSH EAX
PUSH ESI
CALL NewAptc.00406240
POP ECX
ADD EAX,ESI
PUSH EAX
PUSH NewAptc.0040F7E8                     ; ASCII "%path%"
CALL EDI
MOV DWORD PTR DS:[4101E4],EAX
PUSH 50010                                ; Style = MB_OK|MB_ICONHAND|MB_APPLMODAL|50000
PUSH NewAptc.00410A54                     ; Title = ""
PUSH DWORD PTR SS:[EBP+10]                ; Text
PUSH EBX                                  ; hOwner
CALL DWORD PTR DS:[<&USER32.MessageBoxA]  ; MessageBoxA
MOV EDI,NewAptc.004115A0
PUSH EBX
CALL NewAptc.00401128
MOV ESI,DWORD PTR SS:[EBP+8]
POP ECX
PUSH NewAptc.0040F77C                     ; ASCII "he"
CALL NewAptc.00405365
POP ECX
CALL NewAptc.00401071
TEST EAX,EAX
JE NewAptc.00405B39
PUSH DWORD PTR DS:[411594]
PUSH NewAptc.0040F774                     ; ASCII "%s  ."
PUSH EDI
CALL NewAptc.004060B8
PUSH NewAptc.0040F770                     ; ASCII "heh"
CALL NewAptc.00405365
PUSH NewAptc.0040F768                     ; ASCII "heh 1"
CALL NewAptc.00405365
ADD ESP,14
LEA EAX,DWORD PTR SS:[EBP-1DC]
PUSH EAX                                  ; pWSAData
PUSH 101                                  ; RequestedVersion = 101 (1.1.)
```

特征码不能任意选取，而要求能够准确无误报的实现检测。

- 长度要求
- 复杂度要求
- 其他要求

问题（三）如何面对更多层面的需求

- IDS的规则问题只是我们问题的出发点。
- 能否实现御毒于内网之外
- Firewall、Gap能否扩充反病毒能力
- 骨干网络能否建立病毒疫情监控机制，甚至直接切断蠕虫传播

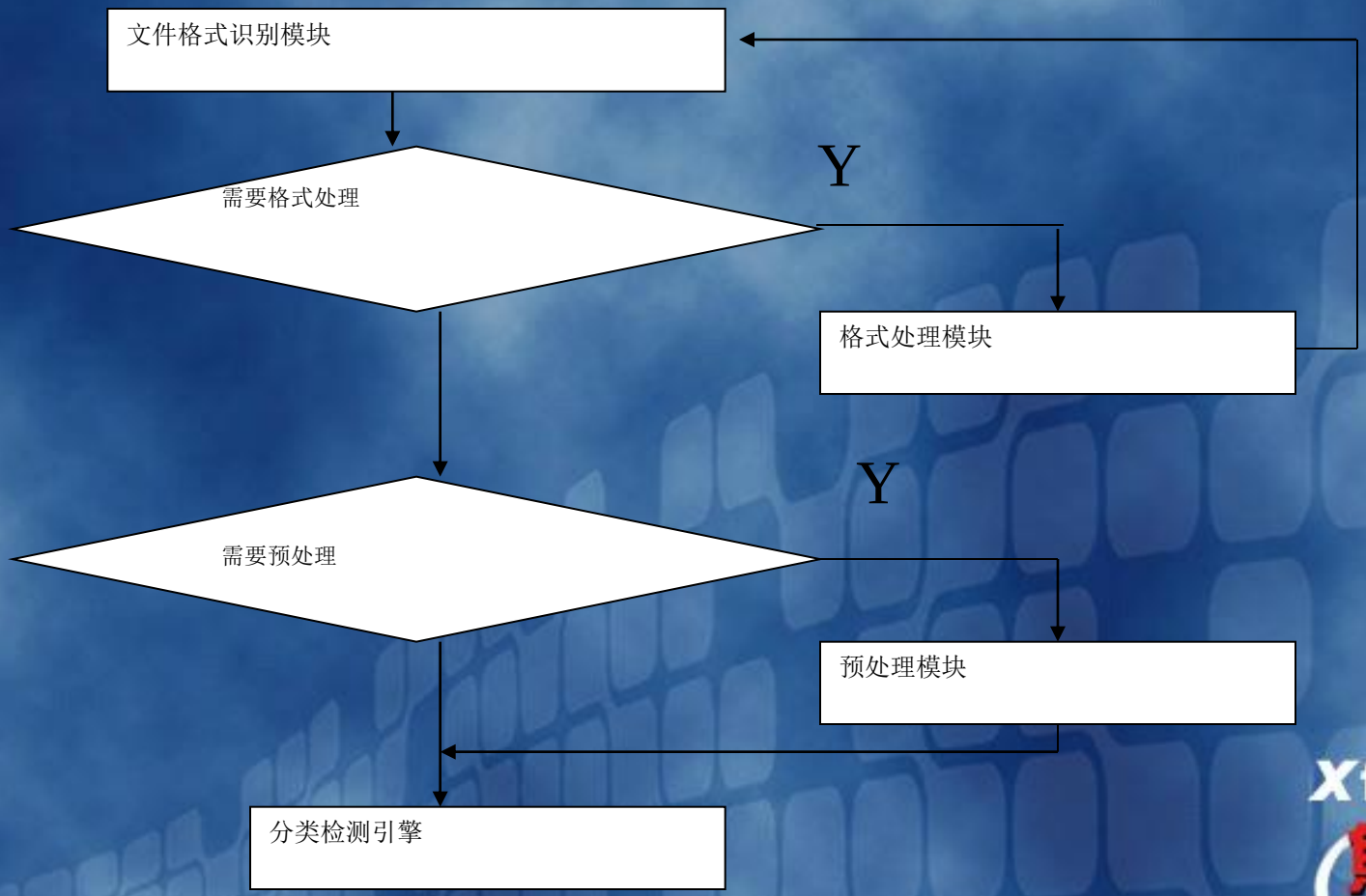
独立病毒分析的准备工作

- 对于网络安全企业的高手们来说，剖析几个蠕虫，提取特征码，没有问题，但要注意这是系统的工作：
- 建立自己的病毒捕获网络，第一时间获得新病毒样本；
- 建立完善的样本库
- 建立自己的特征码分析体制，保证特征码的科学性，避免漏报和误报的可能。
- 警告：对于firewall或者IDS开发部门来说，维持一个专门的Virus Cert小组可能是得不偿失的。

第二章、结合文件级别反病毒技术

- 反病毒技术是一个积累性技术。有一定难以逾越的基础，因此，结合传统反病毒企业的技术是安全厂商的一种选择。
- 一些二线反病毒厂商也把向其他网络安全安全厂商、其他厂商和服务商和提供AV SDK作为新的热点。
- 另一方面，更多的反病毒厂商正在积极扩展自己的网络安全产品线，从而构筑全面地解决方案。

传统的反病毒技术说明



结合传统的反病毒技术

- 传统的反病毒技术是基于文件对象的，适合搭建机遇应用网关服务器的文件系统或者独立构造应用层代理的情况。
- 案例：hotmail的反病毒系统。
- 趋势反病毒网关

结合传统反病毒技术的优势

- 最好的与应用层网关结合
- 全面、彻底的检测各种类型的已知病毒
- 对包裹格式的良好支持。

传统反病毒技术的网络级别应用面临的问题

- 必须还原出具体文件导致一系列的问题产生。
- 极大的资源占用，很低的效率。
- 不能处理类似IIS-Worm.CodeRed之类的情况。
- 不能实时地实现网络级别响应处理
- UDP协议等难以还原到文件、或者还原代价很大的情况
- 能否在流级别直至包级别直接搭建病毒检测体制?

三、基于流和包的病毒检测

- 从病毒分析技术入手
- 从网络传输形态的角度
- 为了证明该思路是成熟的，我们制作了一个可使用的SDK——Virus Catcher。

流级别和包级别的不同检测层次

	Virus Catcher Steam	Virus Catcher Packet	Virus Catcher File
2进制病毒检测模块	√	√	√
邮件蠕虫病毒检测模块	√	√	√
url检测模块	√	√	
脚本病毒检测模块	√		√

比较包级别检测与文件级别检测（一）

扫描对象的传递

```
struct se_data
{
   unsigned long src_ip,dst_ip; //源IP、目的IP
   unsigned short src_port,dst_port; //源端口、目的端口
   unsigned long protocol; //协议类型（由响应处理模块使用）
   unsigned char * data; //待扫描数据
   unsigned long len; //待扫描数据的长度
};
```

比较包级别检测与文件级别检测（二）

处理方式：

```
int vise_response(unsigned long vi_id,//病毒编码
        unsigned long src_ip,     //源IP
        unsigned short src_port,  //源端口
        unsigned long dst_ip,  //目的IP
        unsigned short dst_port,  //目的端口
        unsigned long protocol); //网络协议（具体协议定义，由
    前端设备制订）
```

并非简单的技术叠加

- 包级别检测不是简单的传统病毒特征码库+高速内容匹配算法
- 为什么现有反病毒体系不适合作包级别的检测
- 进一步谈文件级别反病毒软件的检测机理
- 文件类型、预处理、虚拟机、特征码风格

|B3 03 B4 38 81 03 F3 B4 38 81 8C C8 B7 38 81 8C DB B5 38 81 39 C3 B4 38 81 74 11 B4 |

->|B303B4 ?1 03F3B4 ?1 8CC8B7 ?1 8CDBB5 ?1 39C3B4 ?1 7411B4|

已经解决的问题

- 高速匹配的问题：2Gbit/S
- 特征码被边界截断的问题：
- 高速预处理问题：
- 更高质量的特征码问题：由于没有文件格式处理和文件预处理模块，误报概率大大增加，对特征码提取质量的要求大大提高。
- 透明处理的问题。

不能解决的问题

- 编写可靠的变形病毒
- 加密的宏病毒
- 包裹格式

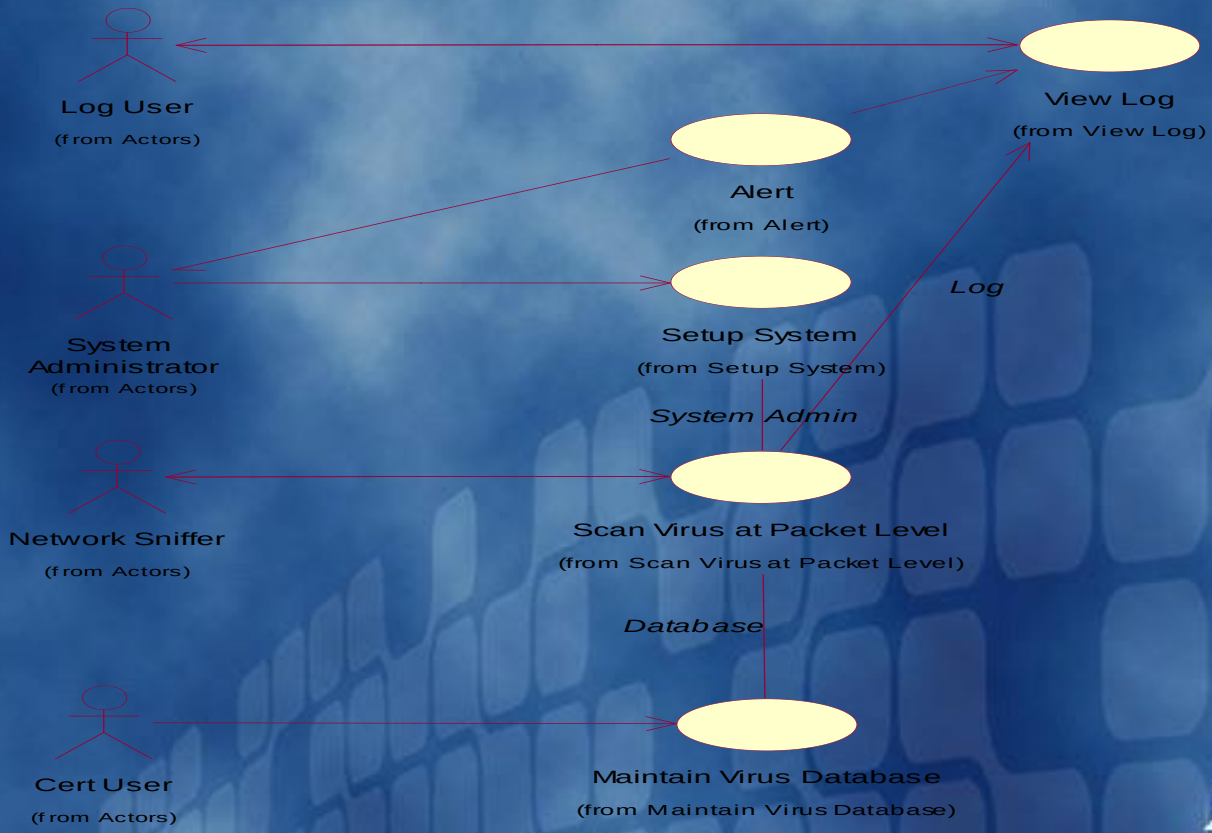
技术定位结论

- 病毒的可靠处理环节是要在实体系统和文件级别上，这依然是毋庸置疑的。
- 包级别检测不能解决所有病毒问题，其定位不应是替代传统反病毒产品。
- 技术并不因为不完备而无价值，技术的价值在于有否合理应用，解决实际问题。
- 反病毒技术在任何层次上都是不完备技术，聊胜于无。

技术的应用点

- Firewall、GAP的反病毒模块
- 更加可靠的IDS Worm规则集
- 独立的骨干网络病毒模块

实例



应用目的

- 基于高速的包检测和响应处理的网关/防火墙级别反病毒系统，遏制恶性病毒的网络传播，构建屏障，降低最终用户的压力。
- 在最终用户的安全防范水平和意识的不可确定性的基础上，增加一层确定性更好的网管屏障。
- 基于主干网络的病毒监控。

相关下载地址

- 还没有上传，感兴趣的兄弟留Mail我发过去。

谢谢

- 肖新光(江海客)
- 电子邮件： Seak@antiy.net
- 通讯地址：哈尔滨898邮政信箱
- 邮政编码：150080