Antiy Labs

Virus Detection Based on the Packet Flow

Seak@antiy.net

Foreword

- Worms and other network viruses are more and more common and VXers have become more familiar with hacking techniques, as a result, network security technology and anti-virus technology are more and more integrated.
- Developers hope to extend the anti-virus capabilities of firewalls, IDS and GAP products. Though they can be combined with the file-level detection of traditional anti-virus vendors, there are still some problems.
- This presentation attempts to explore the integration point of network security technology and anti-virus technology - virus detection based on network packet flow.

1. A Comparison of Two Detection Methods’ Granularity

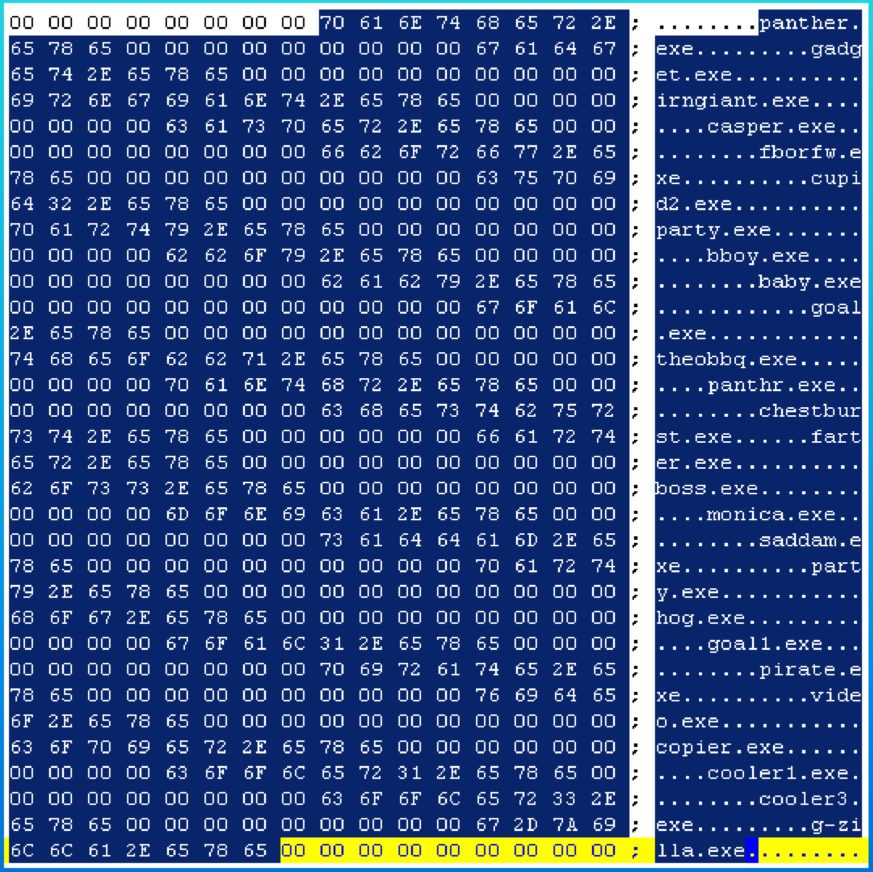
- We will take the extremely coarse anti-virus rules of snort as an example.
- In the latest snort virus.rules, up to 24 rules are used to detect the worm named NewApt, which accounts for 28% of all VX rules

Coarse File Name Detection

```
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\"";
```

Low Detection Granularity



```
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.........
```

After analysis, we found that there are 26 Worm.NewApt attachment files, not 24.

Rules from C&D are correct. We hope to improve Code&Disassemblers besides Capture&Decode.

Flaws of Attachment File Name Detection

- It can do nothing to worms that randomly choose attachment file names or extract local file names.
- When a normal attachment file triggers a false alarm, users will panic. In addition, renaming the file name is the easiest way to modify worms.

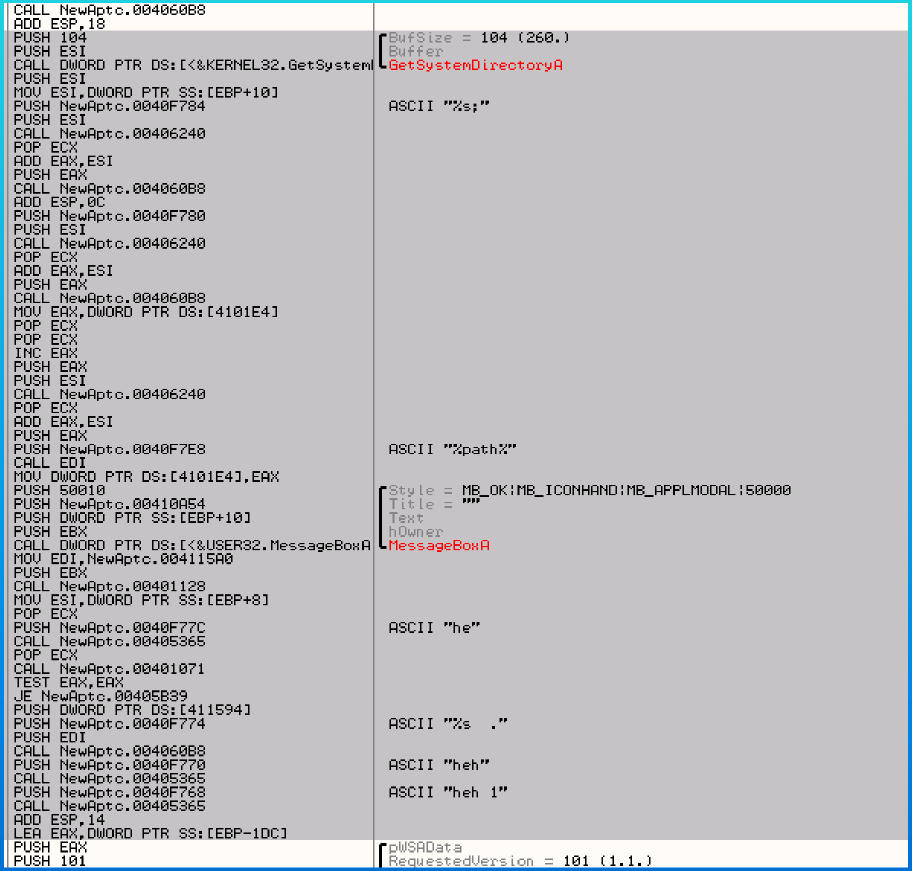
High-Granularity Detection

- From the perspective of file system-based virus analysis, I-worm.NewApt can be totally detected by the following signature string: | 680401000056FF152CC04000568B 75106884F7400056E8CC0800005903C650 E83B07000083C40C6880F7400056E8B50 800005903C650……|

Problem 1 Differences on Network Detection and File detection

- Worms spread via network encoded with base64, not as binary files. The following is the corresponding base64 code of the virus signature code. GgEAQAAVv8VLMBAAFaLdRBohPdAAFbozAgAAFkDxlDoOwcAAIPEDGiA90AAVui1CAAAWQPGUOgkBwAAoeQBQQBZWUBQVuidCAAAWQPGUGjo90AA/9ej5AFBA……
- A new problem comes up: how to process |0d 0a|?

Problem 2 Requirements of the Signature Code



```
CALL NewAptc.004060B8
ADD ESP,18
PUSH 104                                  [BufSize = 104 (260.)
PUSH ESI                                  |Buffer
CALL DWORD PTR DS:[<&KERNEL32.GetSystemI  LGetSystemDirectoryA
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   LMessageBoxA
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.)
```

It can’t be arbitrarily chosen. Instead, it should correctly detect without false positives.

- •Length requirement
- •Complexity requirement
- •Other requirements

Problem 3 How to Meet Multi-Layer Needs

- IDS rules are the starting point of problem 3.
- Can we prevent malware from entering the intranet?
- Can we extend anti-virus capabilities to firewalls and Gap products？
- Can we build a virus monitoring mechanism, or even directly cut off worm spread in backbone networks ?

Preparations for Independent Virus Analysis

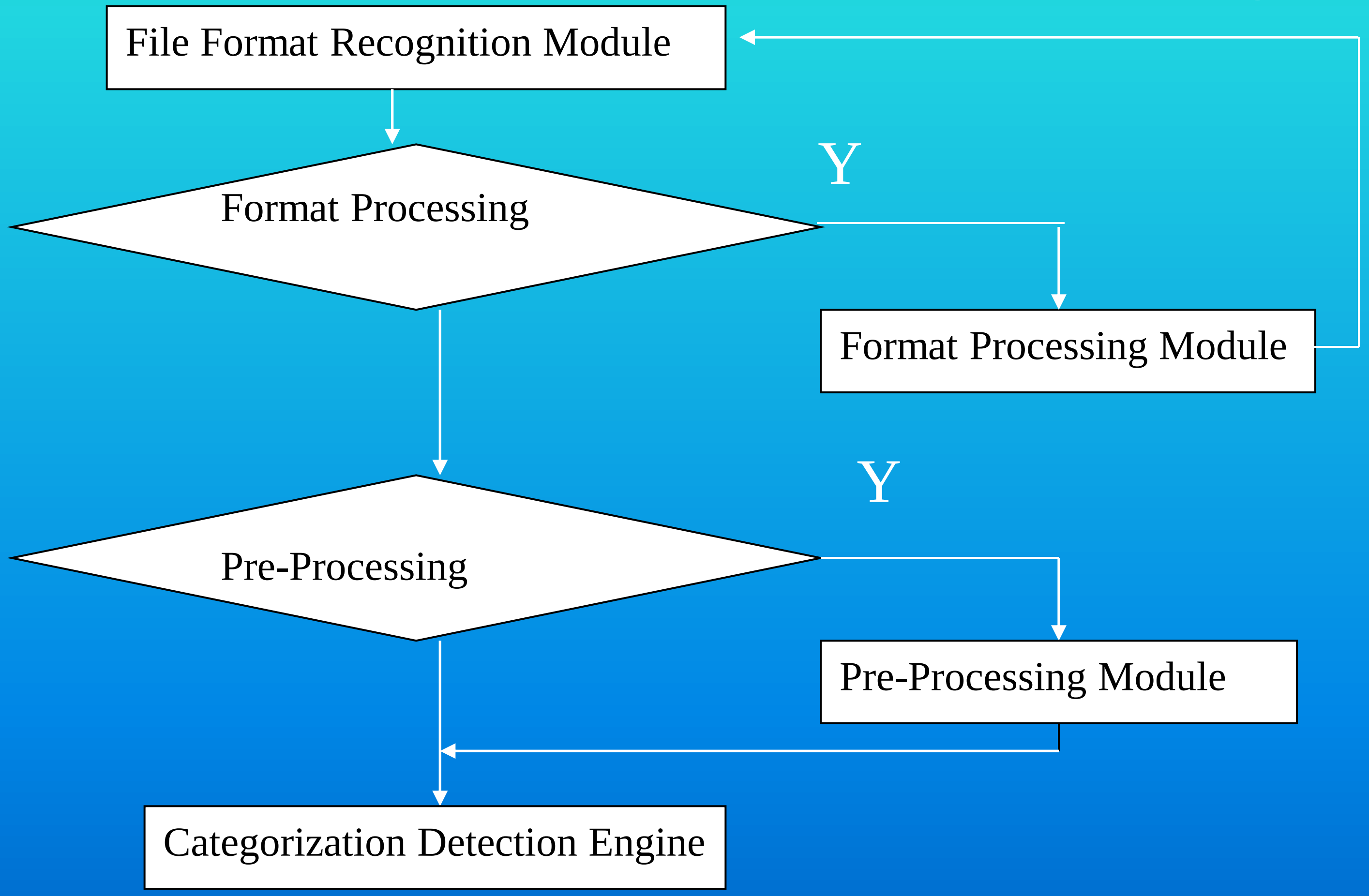
- It is a piece of cake for network security pros to analyze worms and extract signatures. But we should note that a series of tasks needs to be done：

- Build a virus capture network, and get new virus samples as soon as possible
- Build a complete sample database
- Build a signature analysis mechanism, and avoid omission and false positives
- Warning: For firewall or IDS development departments, it is far too wasteful to build a Virus CERT

2 . Combing File-Level Antivirus Technologies

- Anti-virus technology requires experience, so there are certain thresholds. For this reason, combining the technologies of traditional antivirus vendors is a good choice.
- Some b-grade antivirus vendors also turn to providing an AV SDK for other network security vendors and service providers.
- On the other hand, more antivirus vendors are actively expanding their network security product line, in order to build a complete solution.

Description of Traditional Antivirus Technologies



File Format Recognition Module

Format Processing

Y

Format Processing Module

Y

Pre-Processing

Pre-Processing Module

Categorization Detection Engine

Integration with Traditional Antivirus Technologies

- Traditional antivirus technologies are based on files. They are used to build a gateway server based file system or application-layer proxy.
- Case-in-point: the antivirus system of hotmail
- The antivirus gateway of Trend Micro

Advantages of Integration with traditional Antivirus Technologies

- Good for integration with application-level gateways
- Various known viruses can be detected
- Support for compressed formats

Problems of Traditional Antivirus Network-Level Applications

- They must restore specific files, leading to a series of problems:
- High resource consumption and low efficiency
- Can’t process Malware such as Stuxnet II and Code Red
- Can’t respond to and process network-level situations in real-time
- Protocols such as UDP can’t restore to files without high cost
- Can we build a virus detection mechanism on the flow level or the packet level?

3. Virus Detection Based on the Flow and Packet

- Virus analysis technologies
- Network transmission forms
- We developed a usable Virus Catcher SDK

Detection on the Flow-Level and Packet-Level

	Virus Catcher Steam	Virus Catcher Packet	Virus Catcher File
Binary Virus Detection Module	√	√	√
Email Worm Detection Module	√	√	√
URL Detection Module	√	√	
Script Detection Module	√		√

Comparison on Packet-Level and File-Level Detection

Transmission of scan objects

```
struct se_data
{
    unsigned long src_ip,dst_ip; //source IP, target IP
    unsigned short src_port,dst_port; //source port, target port
    unsigned long protocol; //protocol type（used by response processing module）
    unsigned char * data; //data to be scanned
    unsigned long len; //length of data to be scanned
};
```

Comparison on Packet-Level and File-Level Detection

Processing methods:

```
int vise_response（unsigned long vi_id,//Virus code
          unsigned long src_ip,      //source IP
          unsigned short src_port,  //source port
          unsigned long dst_ip,  //target IP
          unsigned short dst_port,  //target port
          unsigned long protocol）；  //network protocol （specific
    protocol）
```

Not Simple Technology Mixing

- Packet-level detection ≠ traditional virus database +high-speed matching algorithm
- Why can’t current antivirus systems be used for packet-level detection?
- Detection mechanism of file-level antivirus software:
  File formats, preprocessing, virtual machine, signature code
  |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|

Problems Solved

- High-speed matching: 2Gbps
- Signature codes are cut
- High-speed pre-processing
- High-quality signature codes
- Transparent processing

Unsolved Problems

- Complex metamorphic viruses
- Encrypted Macro viruses
- Compressed formats

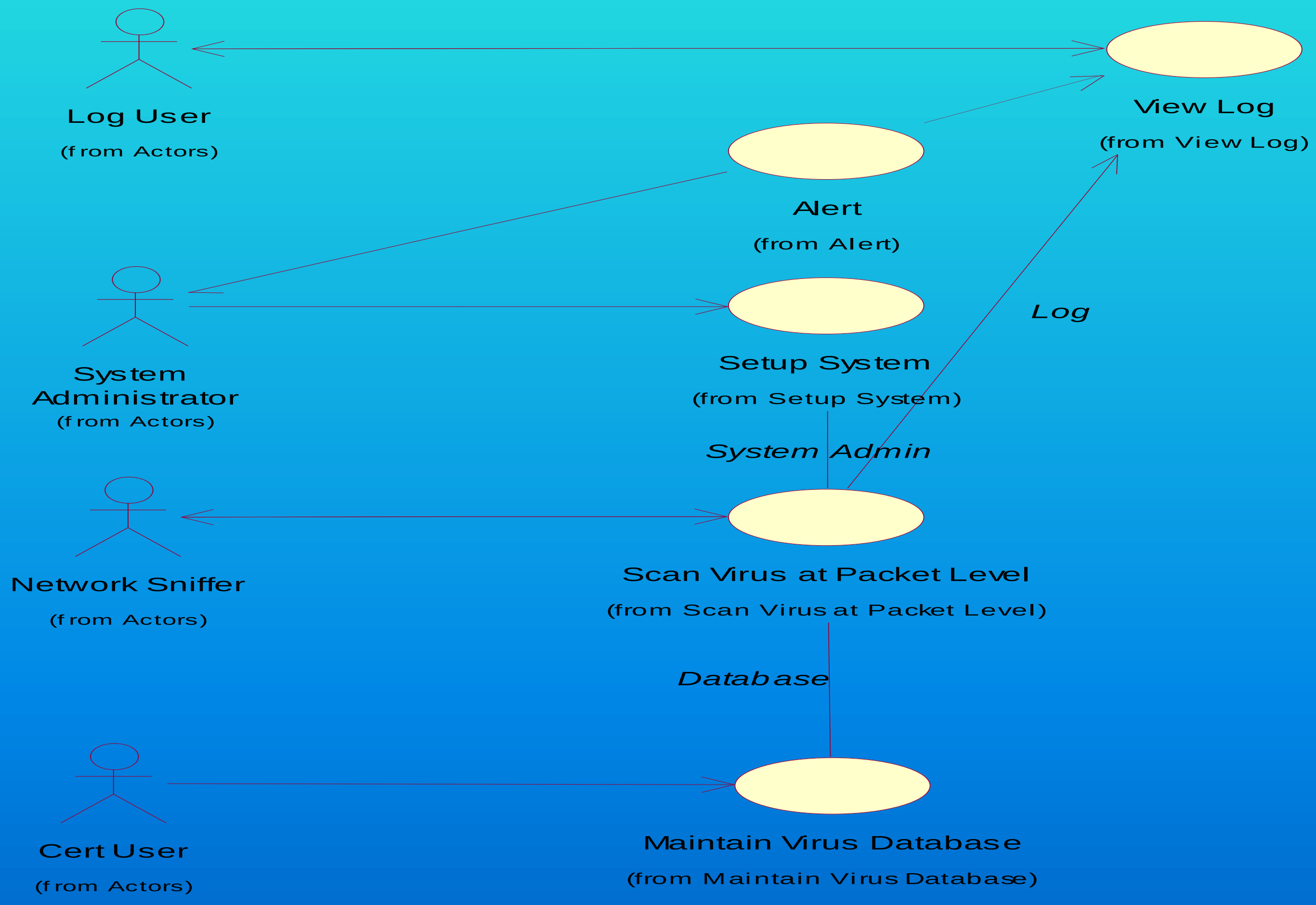
Technical Conclusion

- Reliable virus processing focuses on the system and the file level
- Packet-level detection can’t solve all virus problems, so it can’t replace traditional antivirus products
- Technologies are not always complete, but they can still be used to solve practical issues
- Antivirus technologies will never be complete, but they sure can help us a lot

Technical Application

- Antivirus modules in firewalls and GAP products
- More reliable IDS Worm rule set
- Independent backbone network anti-virus module

Examples


Log User
(from Actors)
View Log
(from View Log)
Alert
(from Alert)
System Administrator
(from Actors)
Setup System
(from Setup System)
Log
System Admin
Network Sniffer
(from Actors)
Scan Virus at Packet Level
(from Scan Virus at Packet Level)
Database
Cert User
(from Actors)
Maintain Virus Database
(from Maintain Virus Database)

Application Purposes

- Used in packet detection and gateway/firewall antivirus systems to prevent malware from spreading.
- Protect users who are not aware enough of malware damages
- Virus monitoring on backbone networks

Related Download Sites

- Nothing has been uploaded. If you are interested, you can leave me your email.

Contact Information

- Email: Seak@antiy.net