



降速的发动机 ——安全设备第三方AV引擎开发者的反思

安天实验室 江海客（肖新光）

seak@antiy.com

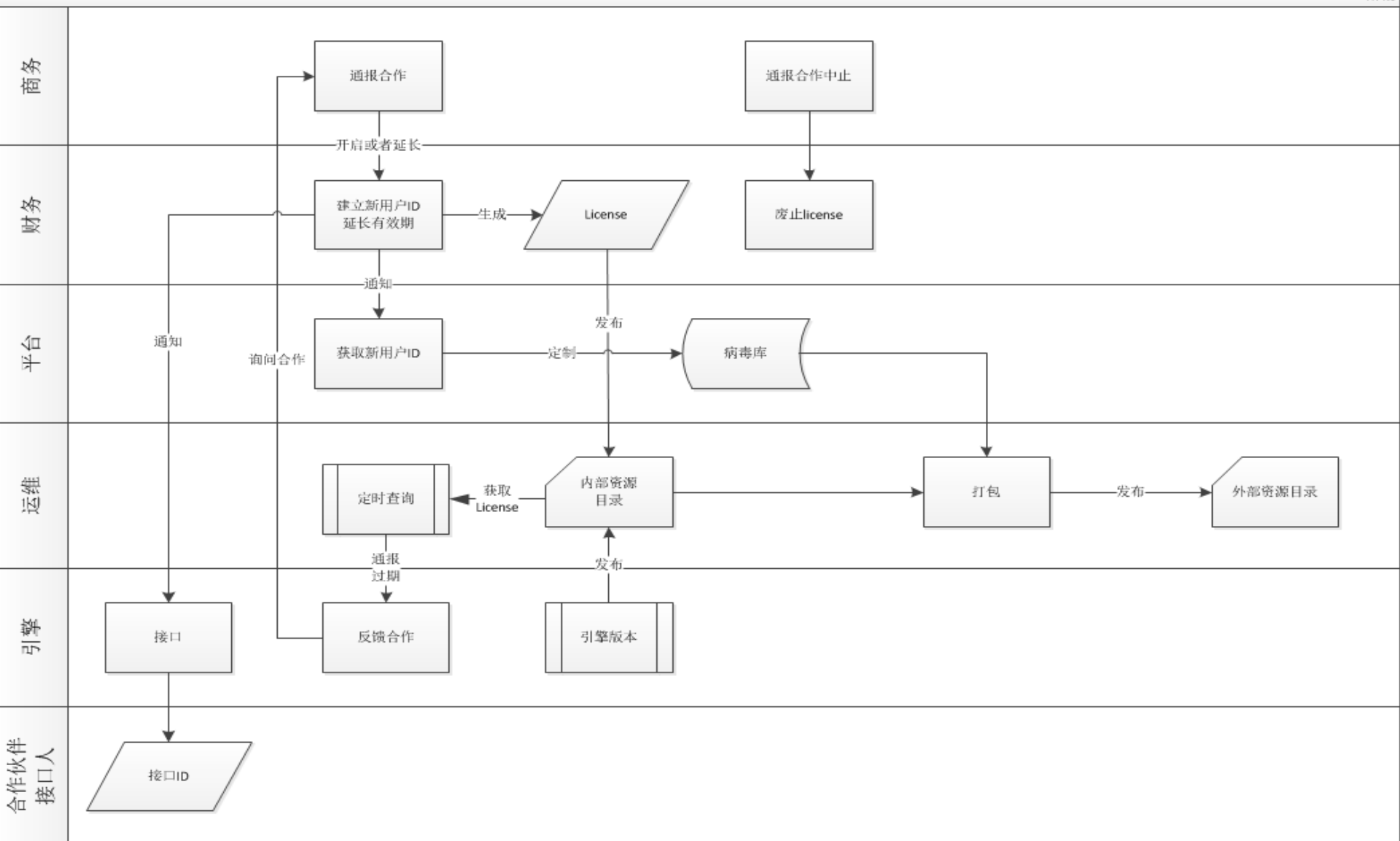
传统里面潜藏着多少危机

引子：终止一个十年流程的原因...

一个已经执行了十年的流程

安天AVL引擎用户流程(旧.已经废止)

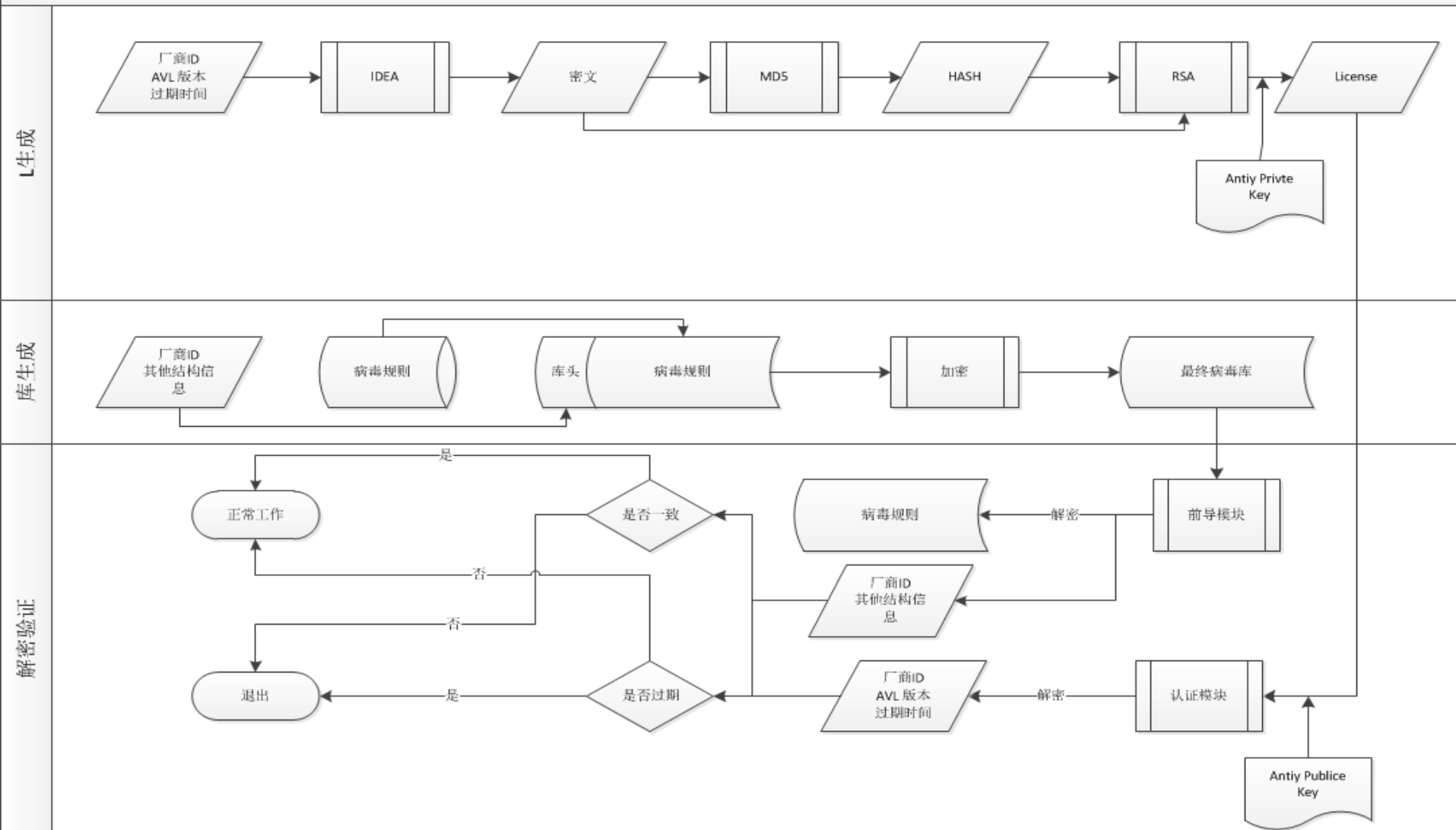
阶段



流程的风险.....

安天引擎License认证和病毒库加密机制示意图

阶段



反病毒引擎供应商并不考虑客户应该使用怎样的引擎，而是告诉客户应该这样使用引擎。

我们做了这些事

“最简单”的调用接口

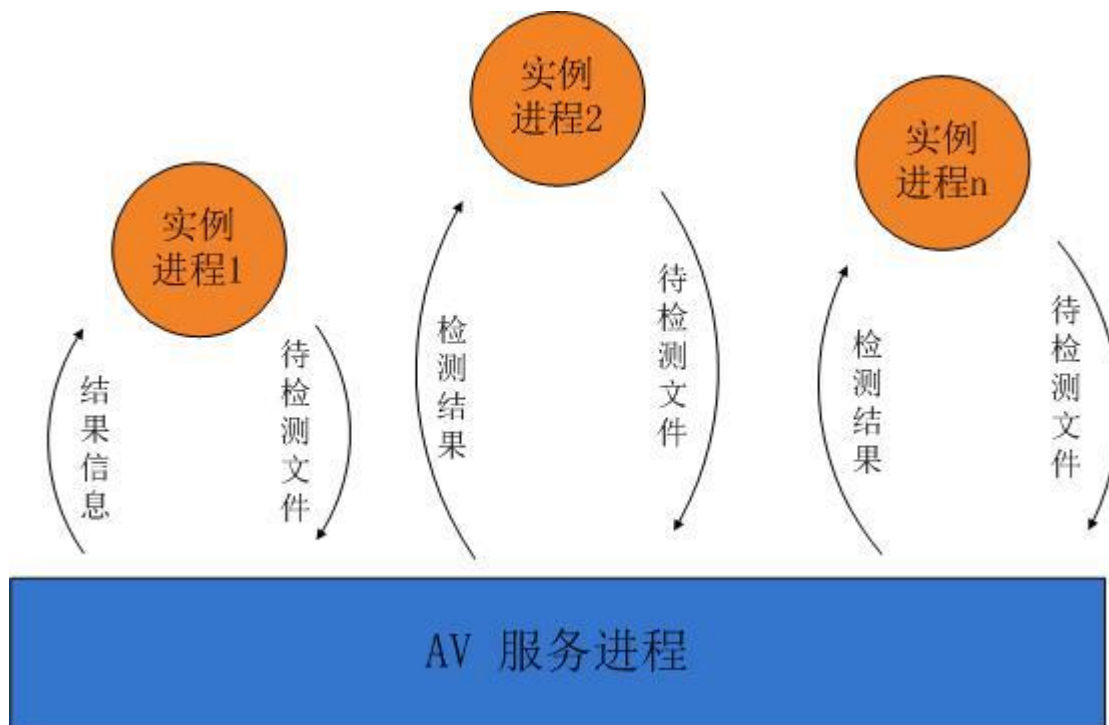
◎ 我们的引擎接口简单，只要传递文件句柄！

```
int scan_file(  
    __IN__ const char          *file_name,  
    __OUT__ const char        **vir_name,  
    __IN__ unsigned long      *scanned,  
    __IN__ const struct engine_handle *engine,  
    __IN__ unsigned int       options);  
  
HRESULT avScanHandle(  
    /*[in]*/ HANDLE hFile,  
    /*[in]*/ const OPTIONS *options, // 0 - default options  
    /*[in]*/ DWORD dwClientValue,  
    /*[out]*/ RESULT *pResult, // 0 - asynchronous call  
    /*[out]*/ DWORD *pdwScanID  
);
```

- ◎ 早期的AV引擎，多数以文件句柄为参数，这是因为，这是主机反病毒引擎的原始接口。
- ◎ 但对网络来说，避免发生磁盘IO是绝对的原则，因此意味着必须采用内存临时文件。

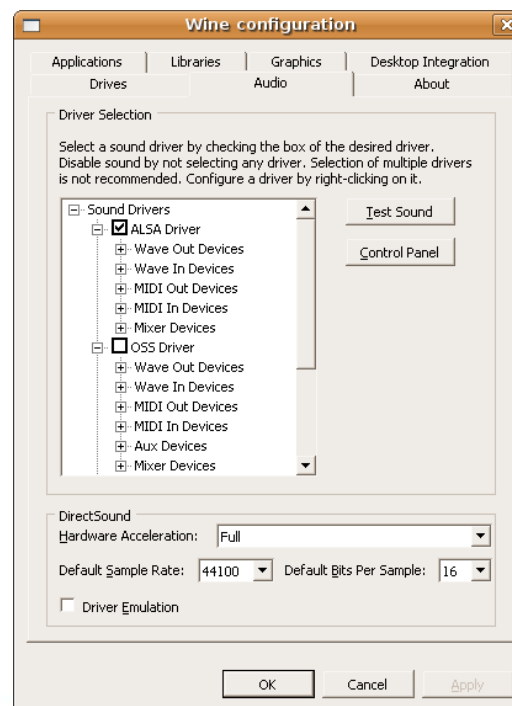
“最先进”的COM架构

- ◎ 没有参数和行命令接口的引擎，封装了一个AV“服务”，采用进程间通讯机制，但仍需传递文件位置。并采用进程间通讯位置传回。



“最科学的”异构平台一致性

- ⊙ 由于不希望承担向Linux移植的成本，使用了一个Windows仿真器。
- ⊙ 一致性的几种实现方式
 - 代码通用
 - 库通用
 - 全二进制通用



反病毒引擎的能力与反病毒厂商的自身能力并不是一致的。

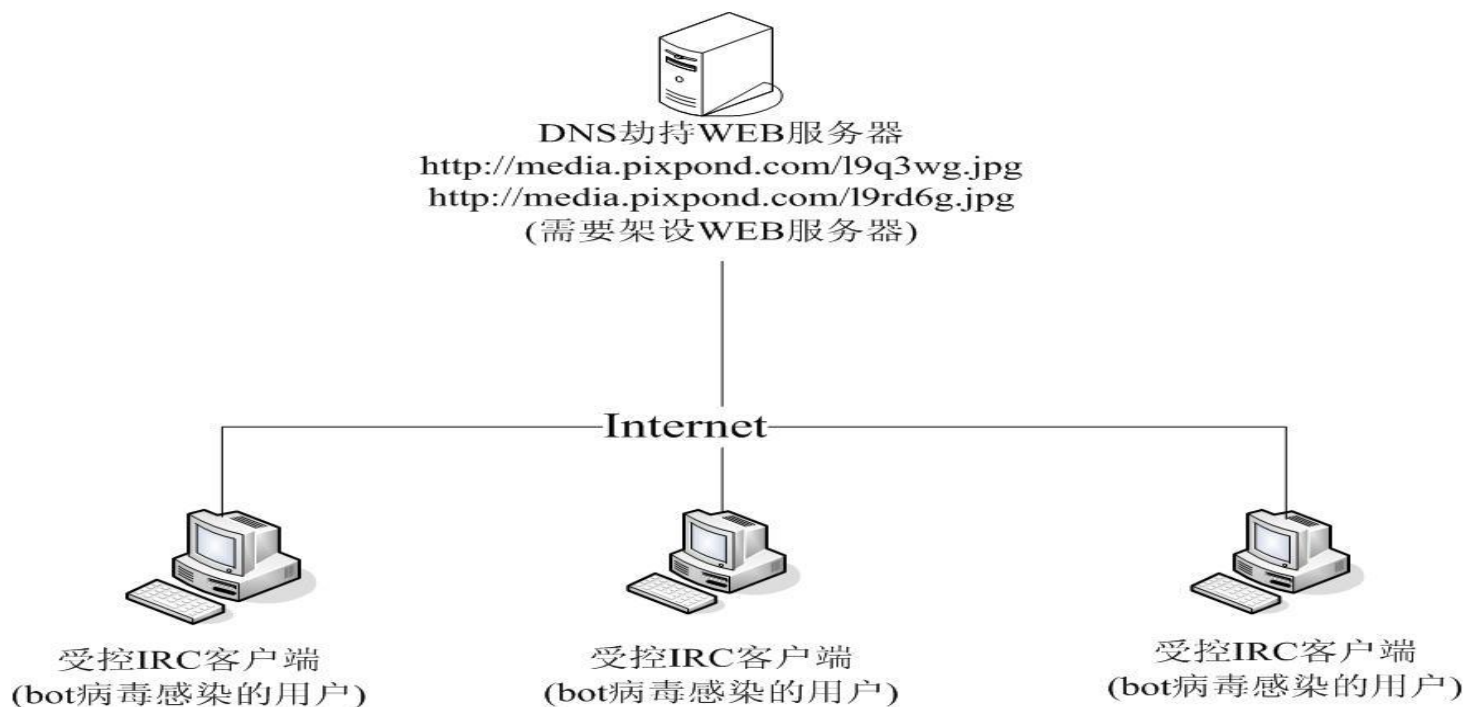
我们仿佛为你做了这些事

广告色情件检测

- ◎ 我们可以为防火墙和其他安全设备提供病毒、蠕虫、木马、后门、黑客工具、**广告件、色情件**等各种恶意代码的过滤功能。——AVL SDK 2.0宣传。
-

Botnet的检测

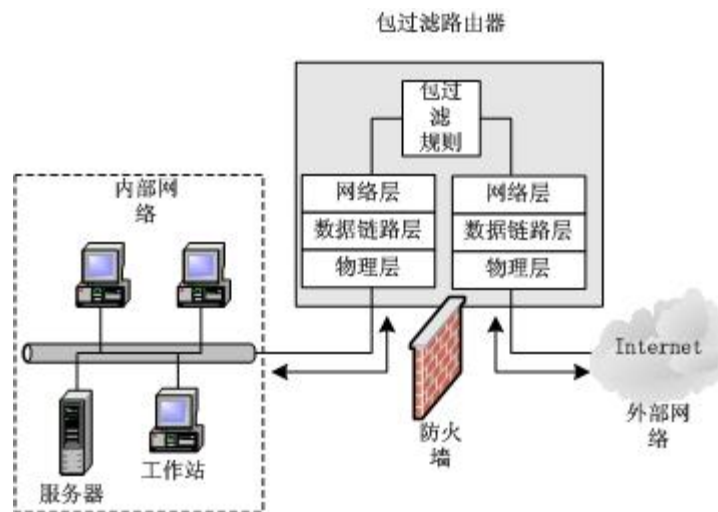
◎ 我们可以检测34个僵尸家族的大量变种——AVL SDK 2.2说明书（2008年）



示意图

包过滤

- ◎ 高速的、流行的，明文规则
- ◎ 支持GPU优化。



高质量的规则剪裁

- ◎ 高质量规则的故事。
- ◎ 所谓1/4高质量的规则，不是通过网络事件遴选的，而是主机统计，但实际上主机上的高频样本，不见得是通过网络感染的。



开放的规则和引擎

- ◎ 可以开放源码和规则的反病毒引擎，带有500万条流行规则。
- ◎ 采用全文HASH检测，提供明文规则。
- ◎ 为什么云可以，设备不行。
- ◎ 流行统计会有效么？
- ◎ 云端变形的时代。

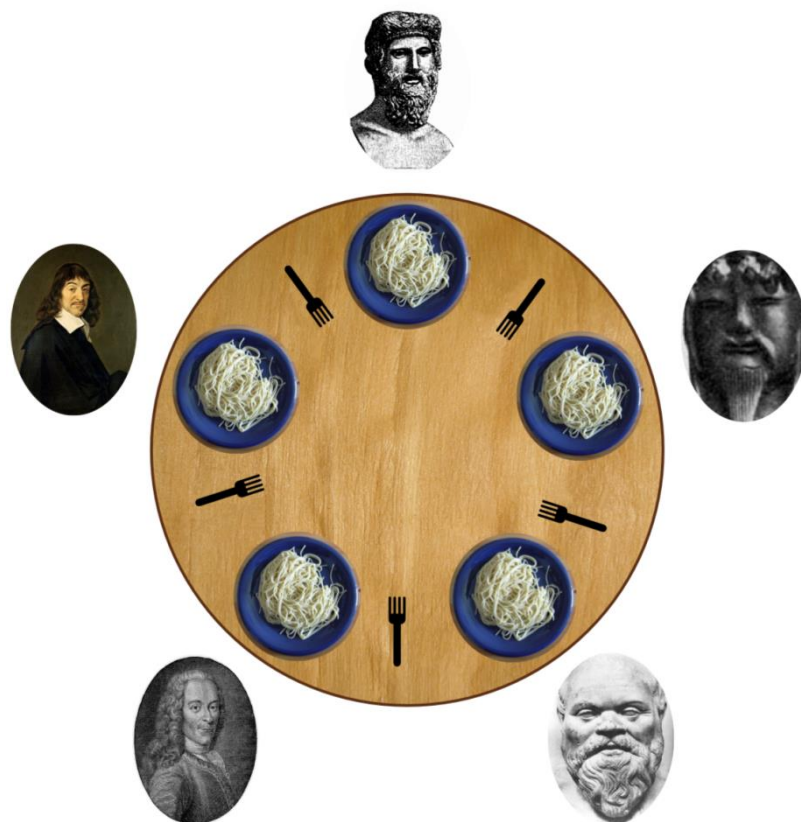


我们不是不能做这些事，但我们为什么拒绝。

我们拒绝做了哪些事

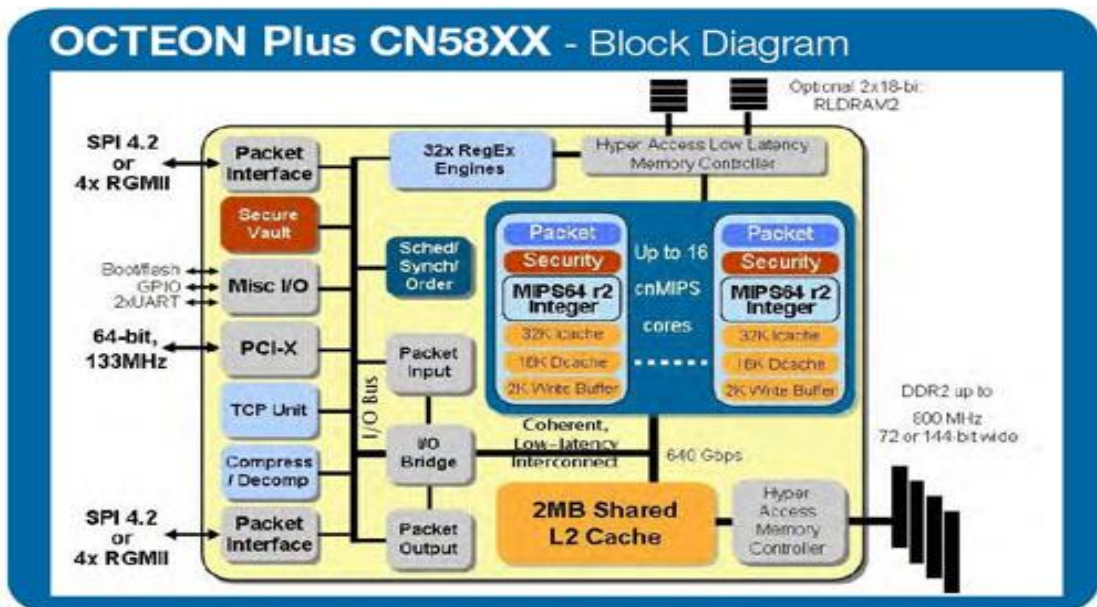
多线程支持

- ⊙ 由于引擎框架的设计问题，大量的全局变量应用，无可避免的产生了多线程间竞争的问题
- ⊙ 一但需要支持多线程，意味着整体框架的改动，反病毒厂商不愿承受整体重构的压力
- ⊙ 反病毒厂商告诉用户无法支持多线程



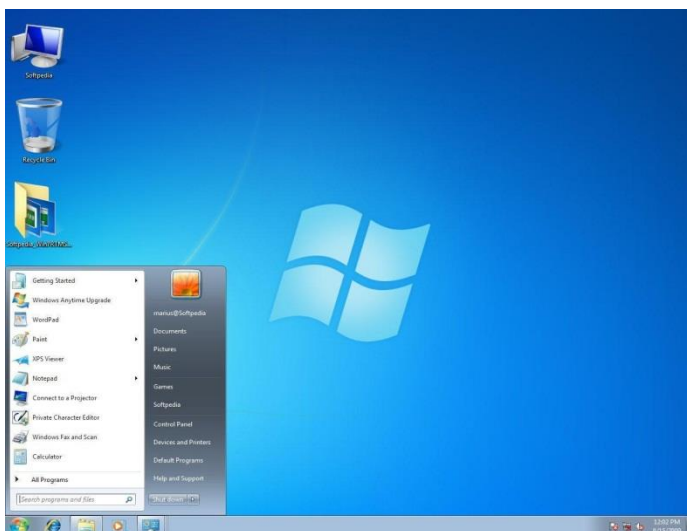
Cavium移植

- ◎ 基于MIPS体系架构的改动，巨大工作量
- ◎ 基于X86架构写的ASM
- ◎ 字节序的问题
- ◎ 多核运行
- ◎ 裸核无操作系统

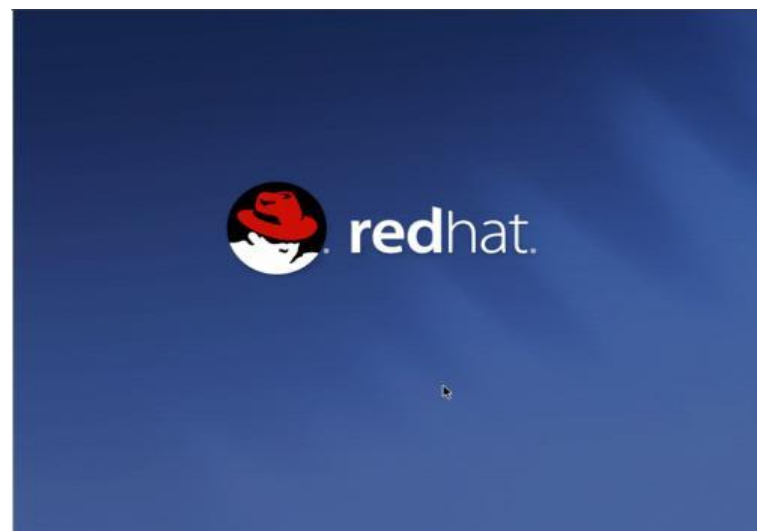


脱壳功能

- ◎引擎中使用了大量的平台相关的API，例如WINDOS平台中的函数，导致了无法移植到非WINDOS的平台中



VS



反病毒引擎会给你的设备带来麻烦，是的，是这样的。

我们给你找了这些麻烦

邮件病毒的处理

◎直路设备对于检测到的病毒可以采用阻断处理，对于邮件蠕虫可以采用反馈式、或者追加式补发邮件告知用户——《AVL SDK 2.0产品说明（2004）》

	Smtplib 检测				POP3 检测			
	收件人为构造	收件人为非构造	发件人为真	发件人为假	收件人为构造	收件人为非构造	发件人为真	发件人为假
反馈式			有效	无效			有效	无效
追加式	无效	有效			有效	有效		

木马下载阻断

◎看看下面的阻断日志

http://attachments.gfan.com/attachments2/day_111204/111204151032200157526a06ce.rar	Exploit.Linux.Lotoor.ag
http://attachments.gfan.com/attachments2/day_120505/12050514590b28e492c83458f8.rar	Exploit.Linux.Lotoor.ak
http://attachments.gfan.com/attachments2/day_120611/12061112040d7bac7cae47272c.rar	Exploit.Linux.Lotoor.an
http://attachments.gfan.com/attachments2/day_111205/1112052046e807afcc122f4201.rar	Exploit.Linux.Lotoor.an
http://js.9553.com/soft/Kingroot_android_v2.1_20120731.rar	Exploit.Linux.Lotoor.aw

反病毒厂商与用户信息的不对称性问题。

我知道你不知道我知道的事

你知道么？

◎你们知道这些名字的含义么？

– Agent、Jorik、Genome

◎你知道这两个前缀的区别么

– Trojan-PSW

– Trojan-PWS

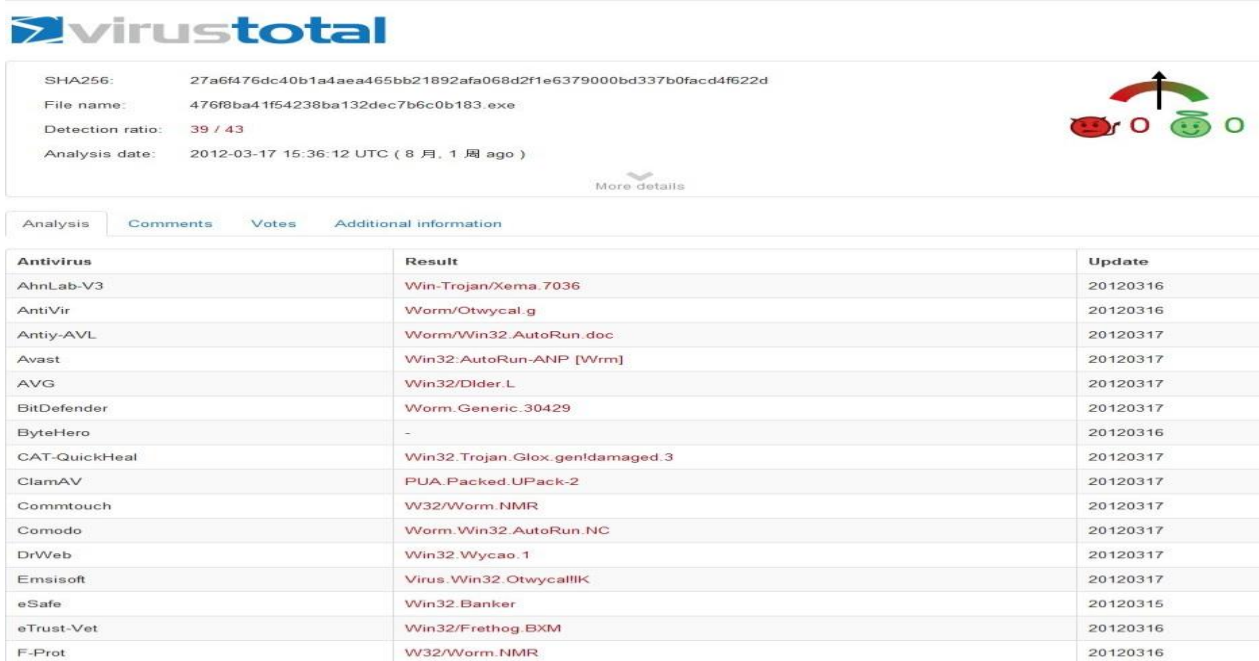
◎你知道这两个名字的区别么？

– Trojan.Win32.IRCbot.aa

– Trojan.Win32.Jorik.IRCbot.aa

关于对照扫描

- ⊙ 最庞大的多引擎对照扫描系统一定不是vt，而是位于各个反病毒引擎厂商。
- ⊙ 但除了少数分析报告上的对照命名，你看不到更多结果。



The screenshot shows the VirusTotal analysis page for a file. The file name is 476f8ba41f54238ba132dec7b6c0b183.exe, and the detection ratio is 39 / 43. The analysis date is 2012-03-17 15:36:12 UTC (8月, 1周 ago). The analysis results table is as follows:

Antivirus	Result	Update
AhnLab-V3	Win-Trojan/Xema.7036	20120316
AntiVir	Worm/Otwycal.g	20120316
Antiy-AVL	Worm/Win32.AutoRun.doc	20120317
Avast	Win32:AutoRun-ANP [Wrm]	20120317
AVG	Win32/Dlder.L	20120317
BitDefender	Worm.Generic.30429	20120317
ByteHero	-	20120316
CAT-QuickHeal	Win32.Trojan.Glox.genfdamaged.3	20120317
ClamAV	PUA.Packed.UPack-2	20120317
Commtouch	W32/Worm.NMR	20120317
Comodo	Worm.Win32.AutoRun.NC	20120317
DrWeb	Win32.Wycao.1	20120317
Emsisoft	Virus.Win32.OtwycallIK	20120317
eSafe	Win32.Banker	20120315
eTrust-Vet	Win32/Frethog.BXM	20120316
F-Prot	W32/Worm.NMR	20120316

关于行为分析

◎ 你可能使用过Shadow Server之类的在线分析，但你们用过AV引擎提供者的在线分析么？难道我们不分析病毒么？

基本信息
检测模块判定
详细结果
静态启发
衍生文件

基本信息(BASEINFO)

Format Name:
BinExecute/Microsoft.PE[X86]
Format ID: 22
Pack Name:
Packer_Compression/Dwing.UPACK[v0.3x]
Pack ID: 1225

详细结果

模块名称	模块缩写	病毒ID	病毒名称
最终检测结果	MALWARE	1204130	Trojan/Win32.OnLineGames.qzh[GameThief]
感染式病毒检测	INFECT	-	-
通用特征检测	ATBM	2242724	Trojan/Win32.WOW.gjc[GameThief]
木马检测	ATROJAN	1204130	Trojan/Win32.OnLineGames.qzh[GameThief]
格式混淆检测	AEXPLOIT	-	-
脚本检测	ASCRIPIT	-	-
静态启发式检测	VCSII	3357027	VCS/Environment DigitalFN.a
木马检测S	ATROJANS	-	-

基本信息

■ 基本信息

分析系统版本号: v0.3.2
 分析开始时间: 2012-09-03 15:51:59
 分析结束时间: 2012-09-03 15:55:13
 耗用时间: 193 seconds
 文件名: SEASD7E15A73CA339494B4DD4D369A87.AC86B974.exe
 文件大小: 98752
 文件类型: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
 CRC32: AC86B974
 MD5: 5ea5d7e15a73ca339494b4dd4d369a87
 SHA1: 349ca66d73b77a42f85bd04e6037f7e22543ce
 SHA256: 7b27fae775b9060e9b316ba538d2a1f4294315ae7979b23870136167c9d46e80
 SHA512: 76bde6c9d47a1db9471d88ec8a11fb456cdccad5929077c105f8691c3a9434073c42e29b723d4d49f1e4fe04f090d98ed5019f1c670b1ad25fd20e8756065b
 Sddeep:
 PEID Signatures:
 恶意性判断: Yes

危险行为

■ 行为判断

行为名称	具体行为
Malware:	YES
CopySelf:	{u'Process: u'5EA5D7E15A73CA339494B4DD4D369A87.AC86B974.exe', u'Pid: 1192, u'Module: u'0x004350A6@5EA5D7E15A73CA339494B4DD4D369A87.AC86B974.exe', u'Details: (u'lpNewFileName: u'c:\\bymiudcohv', u'dwCopyFlags: u'0x00000000', u'lpData: u'0x00000000', u'lpProgressRoutine: u'0x00000000', u'lpExistingFileName: u'c:\\5ea5d7e15a73ca339494b4dd4d369a87.ac86b974.exe'), u'ApiName: u'CopyFileExW', u'Time: 1346658752, u'Tid: 240, u'Result: 0}
DeleteSelf:	{u'Process: u'bymiudcohv', u'Pid: 1296, u'Module: u'0x004350A6@bymiudcohv', u'Details: (u'lpFileName: u'c:\\5ea5d7e15a73ca339494b4dd4d369a87.ac86b974.exe'), u'ApiName: u'DeleteFileW', u'Time: 1346658769, u'Tid: 1204, u'Result: 87}
SuspiciousProcessName:	{u'Process: u'5EA5D7E15A73CA339494B4DD4D369A87.AC86B974.exe', u'Pid: 1192, u'Module: u'0x004350A6@5EA5D7E15A73CA339494B4DD4D369A87.AC86B974.exe', u'Details: (u'lpCommandLine: u'\"C:\\5EA5D7E15A73CA339494B4DD4D369A87.AC86B974.exe\" a -scl\\5ea5d7e15a73ca339494b4dd4d369a87.ac86b974.exe', u'ProcessId: u'1296', u'lpEnvironment: u'0x00000000', u'lpCurrentDirectory: u'NULL', u'lpApplicationName: u'c:\\bymiudcohv', u'ProcessHandle: u'0x0000005C', u'lpInheritHandles: u'0x00000000', u'dwCreationFlags: u'0x00000020', u'ApiName: u'CreateProcessInternalW', u'Time: 1346658755, u'Tid: 240, u'Result: 0}

发现自己、改造自己

提纲回顾

- ◎ 引子：从终止一个执行十年的流程开始……
 - ◎ 我们做了这些事
 - ◎ 我们仿佛做了这些事
 - ◎ 我们拒绝做这些事
 - ◎ 我们做了找麻烦的事
 - ◎ 我知道你不知道我知道的事
 - ◎ 尾声：发现这样的自己
-

发现这样的自己



改造自己：让昨天告诉明天





感谢大家的关注！

求点击：<http://www.antiy.net>

求批判：<http://www.virusview.net>

求关注：<http://weibo.com/seak>