



APT的线索、关联与样本集 度量

安天实验室 肖新光（江海客）



报告提纲

Contents



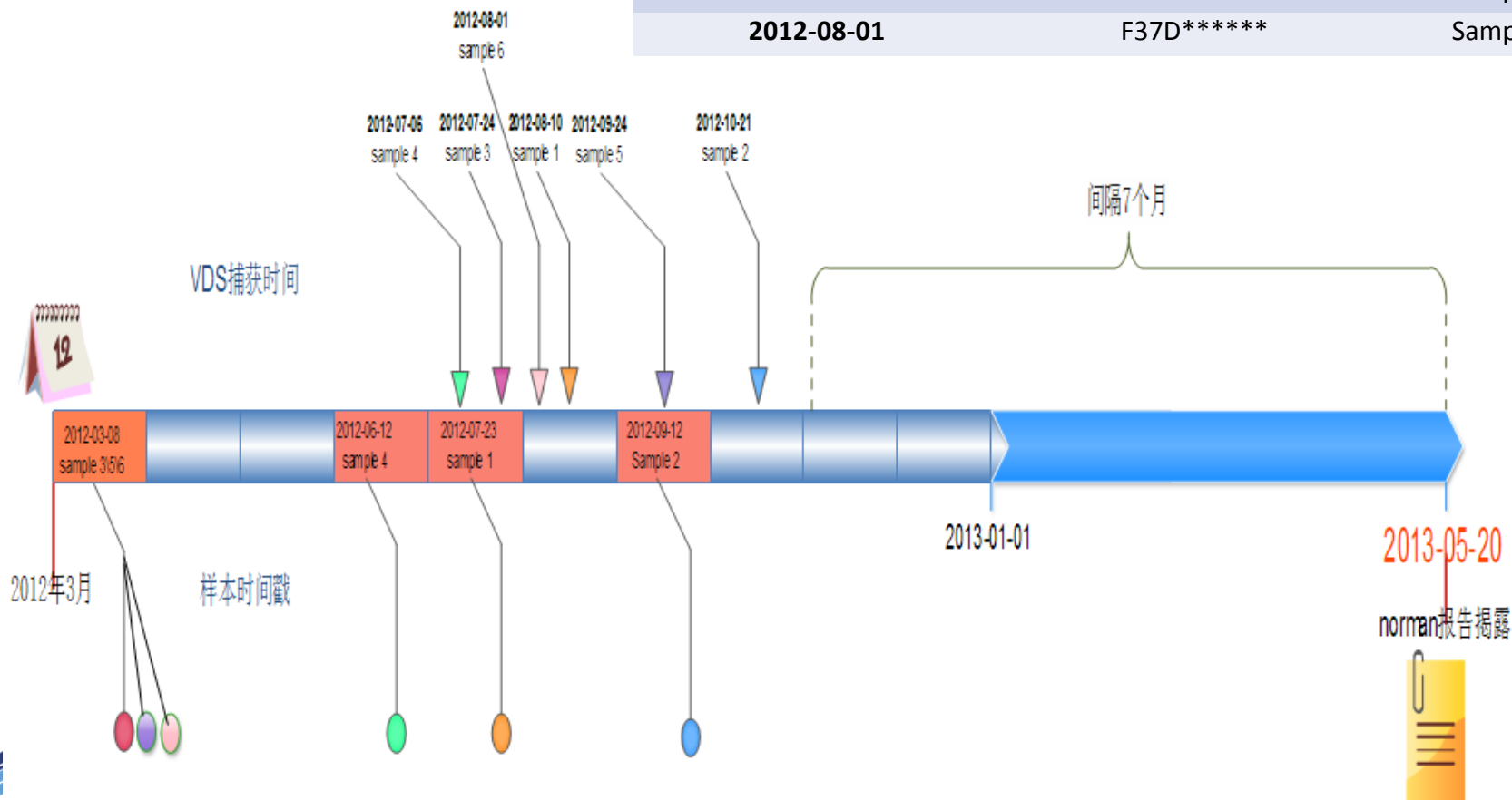


线索

- 从Hangover事件说起。

<http://blogs.norman.com/2013/security-research/the-hangover-report>

捕获时间	样本hash列表	代号
2012-08-10	0D46*****	Sample 1
2012-10-21	734E*****	Sample 2
2012-07-24	9A20*****	Sample 3
2012-07-06	CE00*****	Sample 4
2012-09-24	DE81*****	Sample 5
2012-08-01	F37D*****	Sample 6

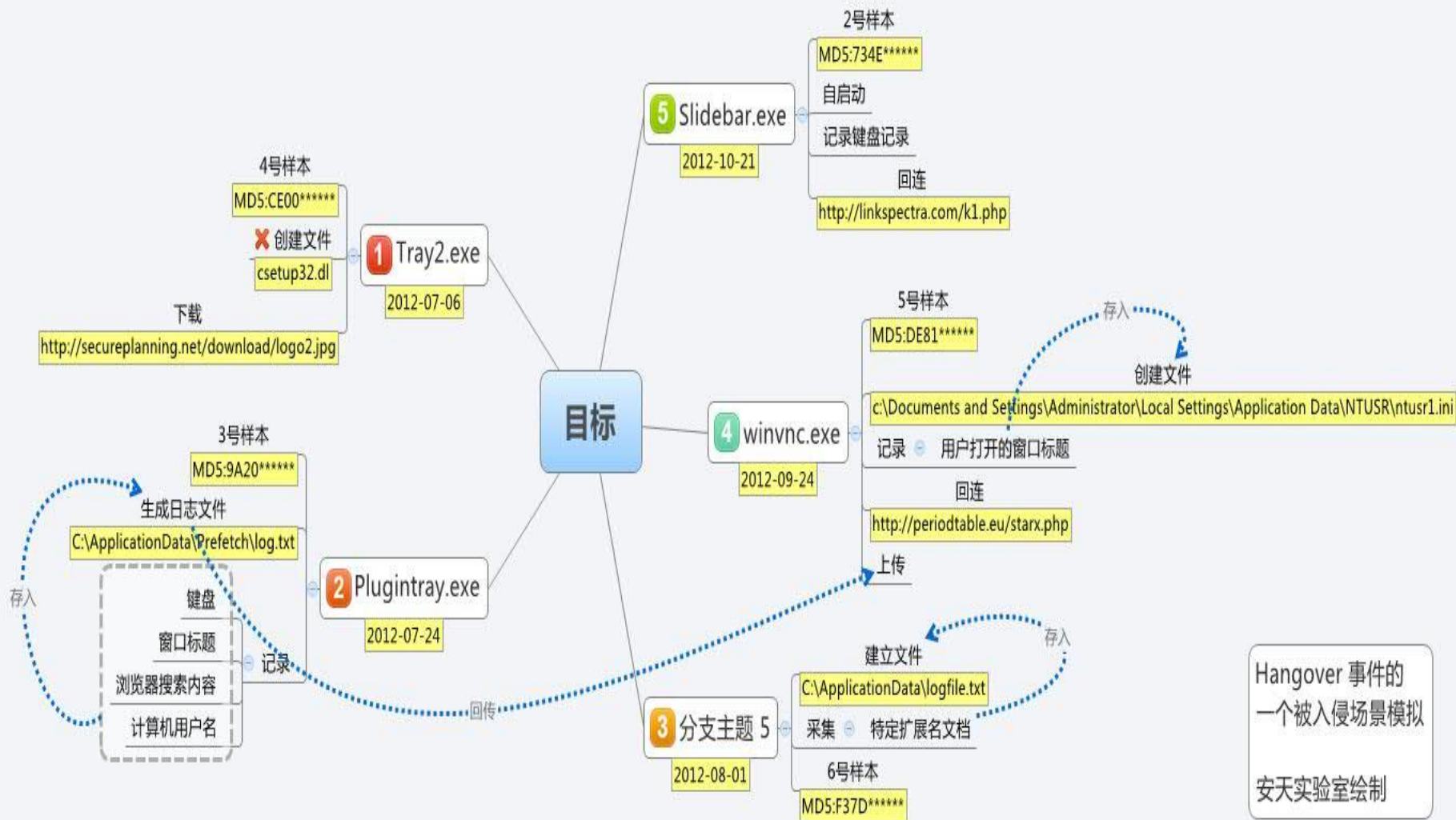




样本情况

6

	壳	编译器	主要行为	回连地址
Sample 1	无	Microsoft Visual Basic 5.0 / 6.0	释放的VBScript脚本,脚本执行后连接远程服务器zolipas.info。(域名失效)。	http://zolipas.info/advd
Sample 2	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后将 以下文件设置为Run自启 C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sidebar.exe, 记录键盘信息并上传。	http://linkspectra.com/k1.php
Sample 3	UPX 0.89.6 - 1.02 / 1.05 - 1.24	Dev-C++ 4.9.9.2	运行后在C:\ApplicationData\Prefetch\目录下生成log.txt文件,不断的记录键盘、窗口标题、浏览器搜索内容、计算机用户名等信息。	
Sample 4	UPX 0.89.6 - 1.02 / 1.05 - 1.24	Microsoft Visual C++ 7.0	运行后试图创建csetup32.dll,但未成功。链接域名secureplanning.net欲下载其他恶意代码(URL失效)。	http://secureplanning.net/download/logo2.jpg
Sample 5	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后在 c:\Documents and Settings\Administrator\Local Settings\Application Data\NTUSR\目录下创建文件ntusr1.ini,记录用户打开的窗口标题。不断地上传样本3记录的信息log.txt	http://periodtable.eu/starx.php
Sample 6	无	Dev-C++ 4.9.9.2	样本运行后在C:\ApplicationData\目录下释放logFile.txt文件,收集各种相关扩展名文档名称。	





样本不同时间点的第三方检测情况对比

8

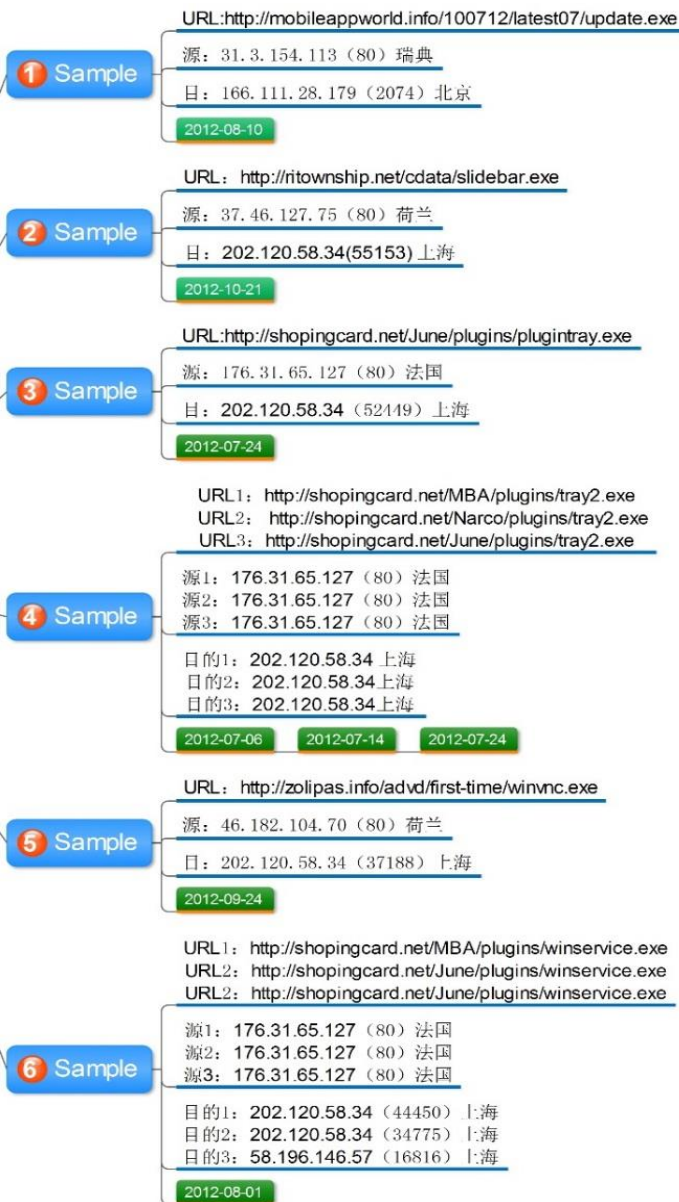
Sample	卡巴	BitDefender	微软	江民	小红伞	McAfee	金山	瑞星	Norton	命中率
Sample 1										0/9
Sample 2	✓	✓		✓	✓					4/9
Sample 3		✓						✓	✓	3/9
Sample 4										0/9
Sample 5	✓									1/9
Sample 6										0/9
以上是样本捕获时入库对照扫描结果										
Sample 1	✓	✓	✓		✓					4/9
Sample 2	✓	✓	✓	✓	✓				✓	6/9
Sample 3	✓	✓	✓	✓	✓				✓	6/9
Sample 4	✓	✓		✓	✓				✓	5/9
Sample 5	✓	✓			✓					3/9
Sample 6	✓	✓	✓	✓	✓			✓	✓	7/9
以上是 2013 年 08 月 20 日对应样本对照扫描结果										



最新的对照命名情况

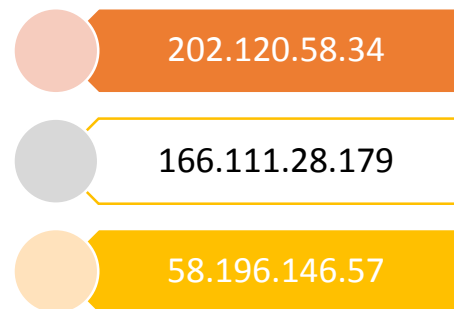
9

	Sample1	Sample2	Sample3	Sample4	Sample5	Sample6
卡巴	Trojan-Downloader. Win32. VB.bkrb	Trojan-Spy. Win32. KeyLogger.actw	Trojan-Spy. Win32. KeyLogger.absi	Trojan.Win32. Agent.sryd	Trojan- Spy.Win32. KeyLogger.acqh	Trojan.Win32. Agent2.fhog
McAfee	未识别	未识别	未识别	未识别	未识别	未识别
Norton	未识别	Infostealer	Trojan.ADH	Trojan.Gen.2	未识别	Trojan.Gen
瑞星	未识别	未识别	未识别	未识别	未识别	Trojan.Win32.Gen eric.12DC27CD
江民	未识别	Backdoor/Agent. t.doyw	TrojanSpy.KeyL ogger.cwwy	Trojan/Agent.gn xm	未识别	Trojan/Agent.gkpg
小红伞	TR/Zoli.A	TR/Agent.7432 8.1	TR/Agent.2126 5	TR/Spy.21504.3 51	WORM/Agent. 22813	TR/Offend.KD.532 260
微软	TrojanDownloader: Win32/Adodb.A	TrojanSpy:Win 32/Keylogger.C B	Trojan:Win32/ Sulunch	未识别	未识别	Trojan:Win32/Sulu nch
BitDefender	Trojan.Generic.KDV. 735533	Trojan.Spy.Keyl ogger.WY	Trojan.Generic. 7642155	Gen:Trojan.Heu r.RP.bmGfa05AQ Rai	IRC- Worm.Generic. 22813	Trojan.Generic.KD. 532260



瑞典
荷兰
荷兰
法国

涉及到4个域名



上海
北京
上海

捕获到3个目的IP



样本来源：shoppingcard.net 法国

- 文档载荷
- PE载荷
- ▲ 网页/脚本载荷
- 载荷投放轨迹
- 心跳与回传

SHOW



记录与其他URL库的对比

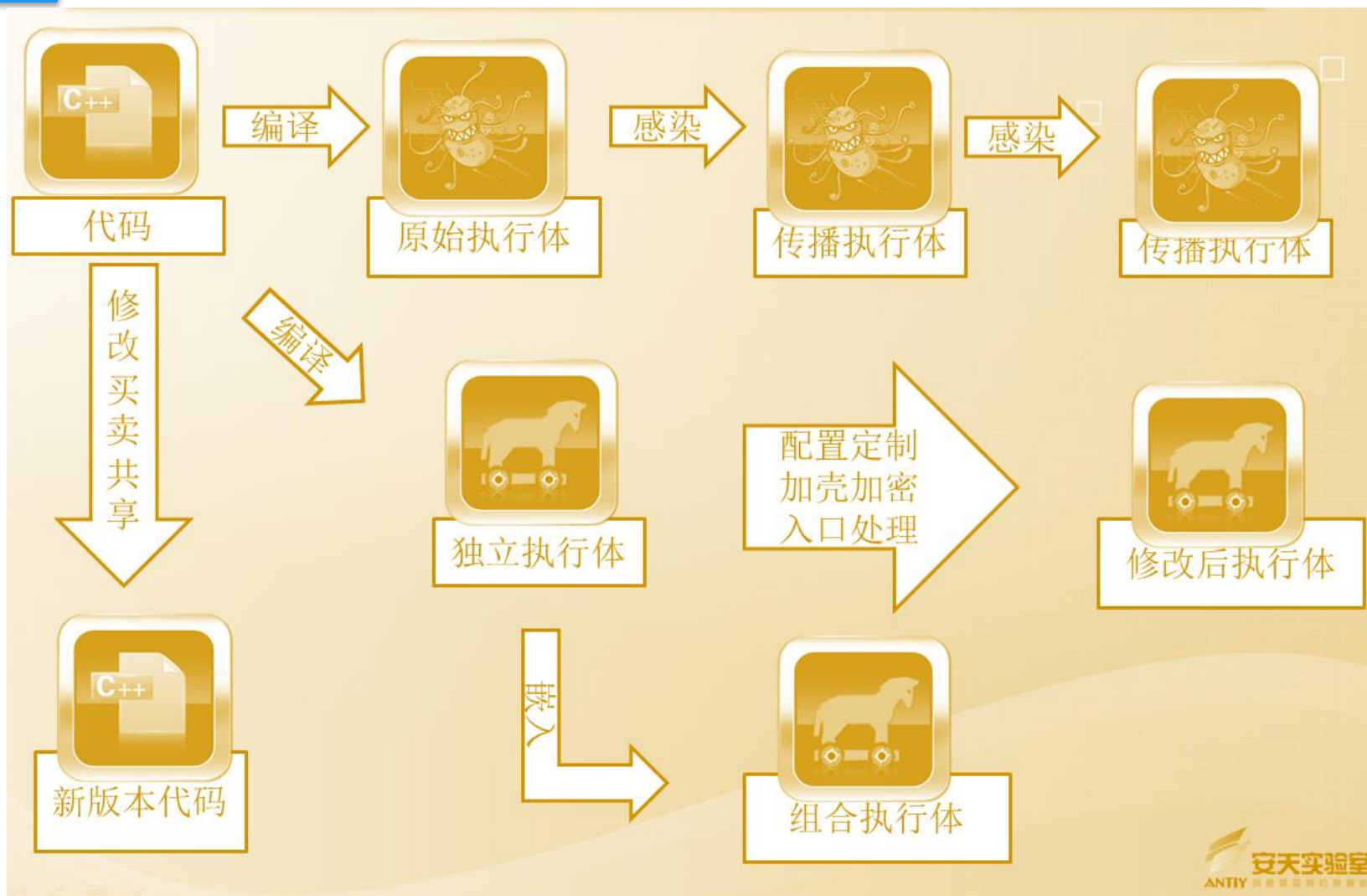
12

时间	源URL	目标IP	目标位置	与其他URL资源库比对
2012/7/6	http://shopingcard.net/MBA/plugins/tray2.exe	202.120.58.34	上海交大闵行校区	未发现
2012/7/14	http://shopingcard.net/Narco/plugins/tray2.exe	202.120.58.34	上海交大闵行校区	未发现
2012/7/23	http://shopingcard.net/MBA/plugins/winservice.exe	202.120.58.34	上海交大闵行校区	未发现
2012/7/24	http://shopingcard.net/June/plugins/plugintray.exe	202.120.58.34	上海交大闵行校区	未发现
2012/7/24	http://shopingcard.net/June/plugins/tray2.ex	202.120.58.34	上海交大闵行校区	晚6小时
2012/7/25	http://shopingcard.net/June/plugins/winservice.exe	202.120.58.34	上海交大闵行校区	晚1天
2012/8/1	http://shopingcard.net/June/plugins/winservice.exe	58.196.146.57	上海交大	晚1天
2012/8/10	http://mobileappworld.info/100712/latest07/update.exe	166.111.28.179	清华大学化学系	未发现
2012/9/24	http://zolipas.info/advd/first-time/winvnc.exe	202.120.58.34	上海交大闵行校区	未发现
2012/10/21	http://ritownship.net/cdata/sliderbar.exe	202.120.58.34	上海交大闵行校区	晚31天



关联

- 在没有更多事件的情况下，我们只能找到更多样本，并期待从样本找到更多事件。



- 序列相似
- 图相似

```

00404663 var_18= dword ptr -18h
00404663 var_14= dword ptr -14h
00404663 var_10= dword ptr -10h
00404663
00404663 push     ebx
00404664 xor     ebx, ebx
00404666 cmp     dword_407240, ebx
0040466C push     esi
0040466D push     edi
0040466E jnz     short loc_404682
    
```

```

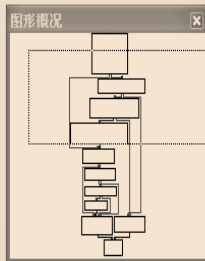
NLL
00404670 push     offset s_User32_dll ; "user32.dll"
00404675 call    dword_405060
0040467B mov     edi, eax
0040467D cmp     edi, ebx
0040467F jz      short loc_4046E8
    
```

```

NLL
00404681 mov     esi, dword_405080
00404687 push     offset s_MessageBoxA ; "MessageBoxA"
0040468C push     edi
0040468D call    esi
0040468F test    eax, eax
00404691 mov     dword_407240, eax
00404696 jz      short loc_4046E8
    
```

```

NLL
00404698 push     offset s_Getactivewind ; "GetActiveWindow"
0040469D push     edi
0040469E call    esi
004046A0 push     offset s_Getlastactive ; "GetLastActivePopup"
004046A5 push     edi
004046A6 mov     dword_407244, eax
004046AB call    esi
004046AD mov     dword_407248, eax
    
```



```

00405053
00405053 arg_0= dword ptr 8
00405053 arg_4= dword ptr 0Ch
00405053
00405053 push     ebx
00405054 xor     ebx, ebx
00405056 cmp     dword_583268, ebx
0040505C push     esi
0040505D push     edi
0040505E jnz     short loc_4050A2
    
```

```

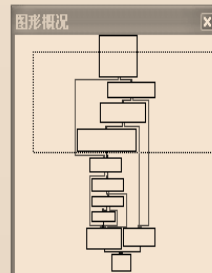
NLL
00405060 push     offset LibFileName ; "user32.dll"
00405065 call    LoadLibraryA
0040506B mov     edi, eax
0040506D cmp     edi, ebx
0040506F jz      short loc_4050D8
    
```

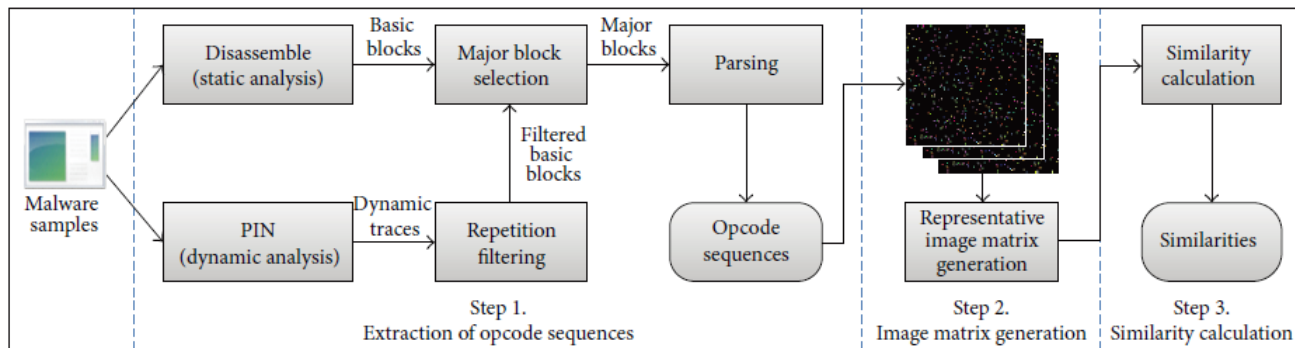
```

NLL
00405071 mov     esi, GetProcAddress
00405077 push     offset ProcName ; "MessageBoxA"
0040507C push     edi ; hModule
0040507D call    esi ; GetProcAddress
0040507F test    eax, eax
00405081 mov     dword_583268, eax
00405086 jz      short loc_4050D8
    
```

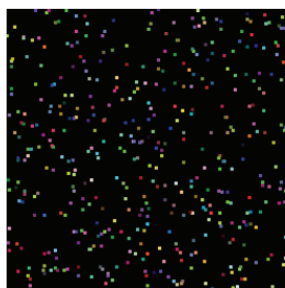
```

NLL
00405088 push     offset s_Getactivewind ; "GetActiveWindow"
0040508D push     edi ; hModule
0040508E call    esi ; GetProcAddress
00405090 push     offset s_Getlastactive ; "GetLastActivePopup"
00405095 push     edi ; hModule
00405096 mov     dword_58326C, eax
00405098 call    esi ; GetProcAddress
0040509D mov     dword_583270, eax
    
```

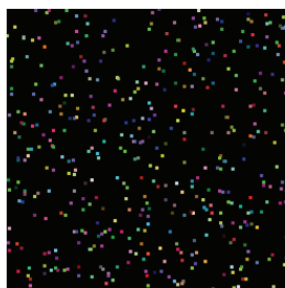




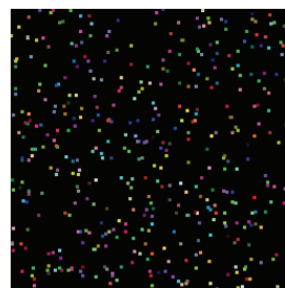
(a) Virus.Win32.HLLP.Semisoft family



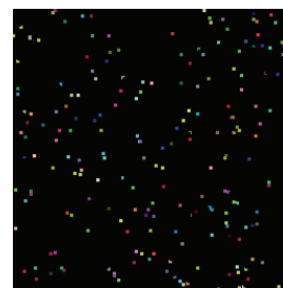
Semisoft.a



Semisoft.b

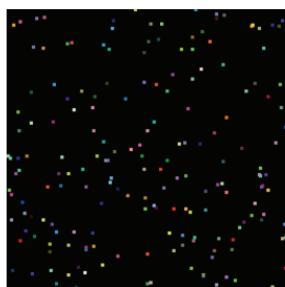


Semisoft.c

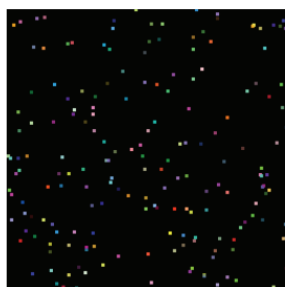


Semisoft representative

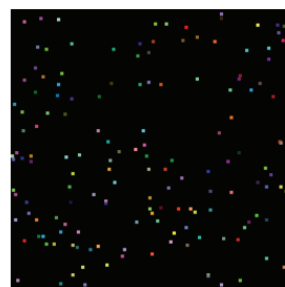
(b) Virus.Win32.HLLP.Semisoft family



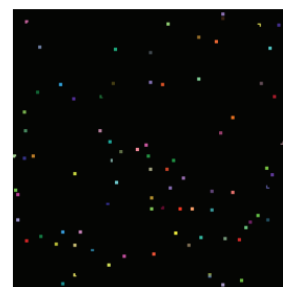
Deborm.c



Deborm.j

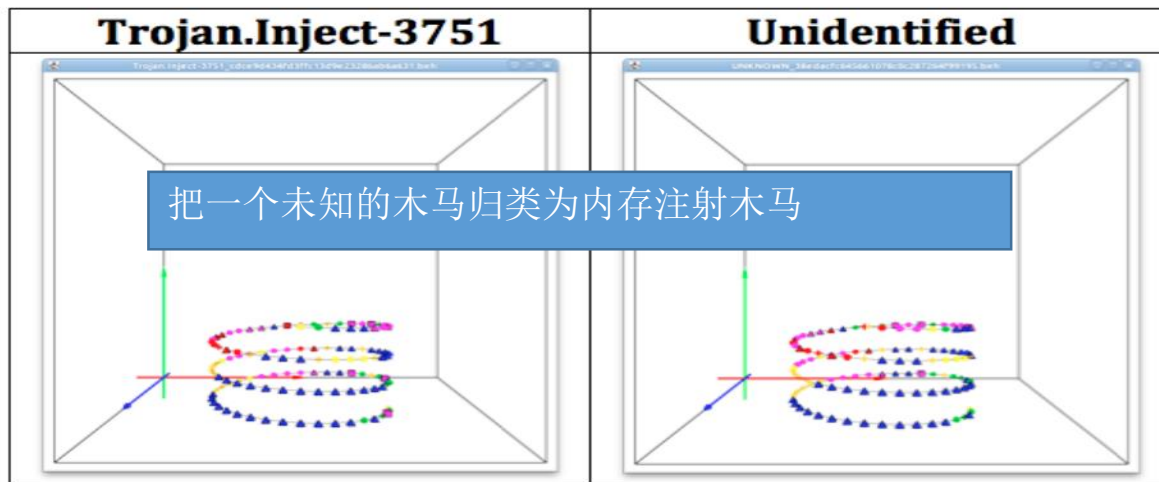
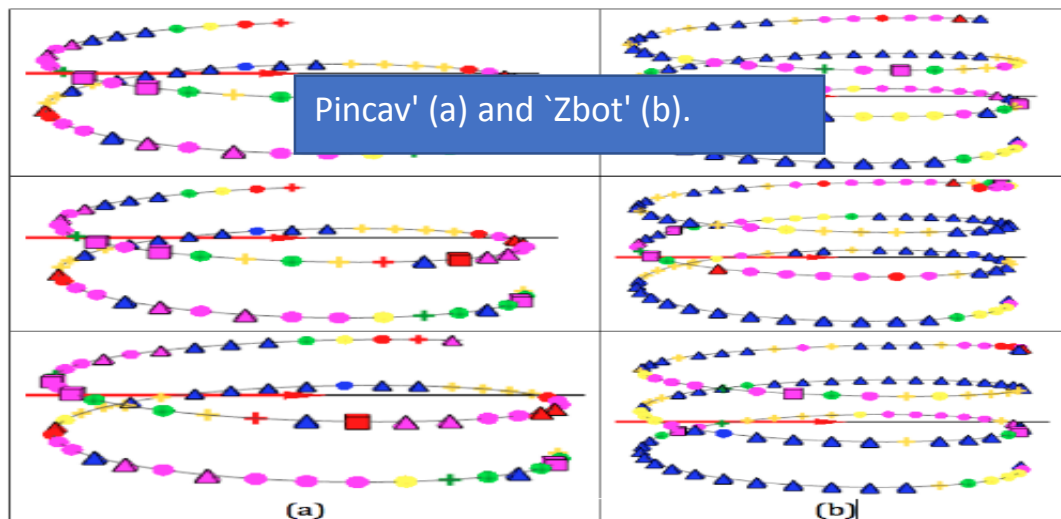


Deborm.k



Deborm representative

Action / Type	MUTEX	FILE	PROC	REG	NET
READ					
QUERY					
RECEIVE					
WRITE					
SEND					
CONNECT					
CREATE					
DISCONNECT					
DELETE					
TERMINATE					
RELEASE					



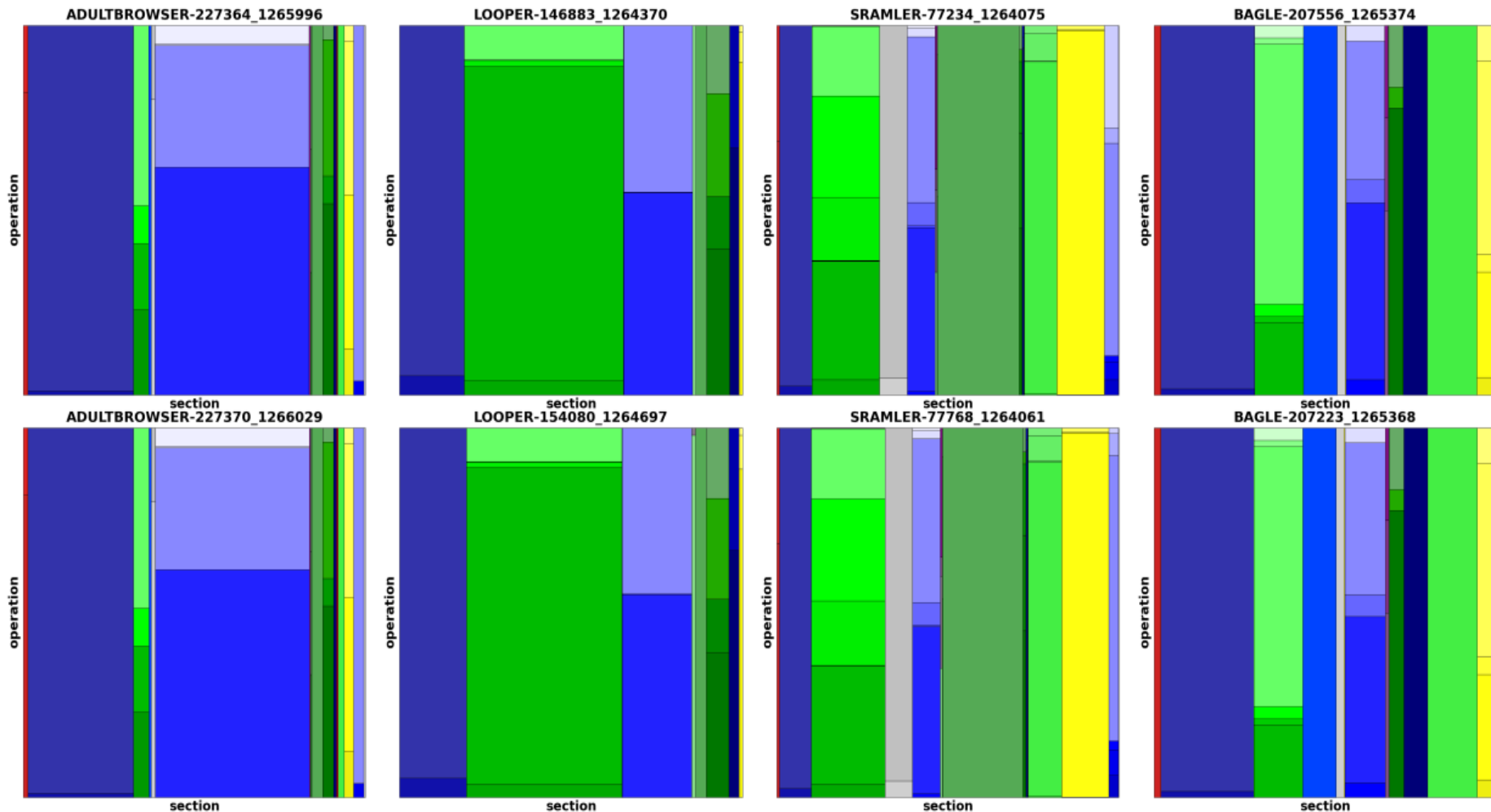


Figure 7: Selection of treemaps out of four different malware classes

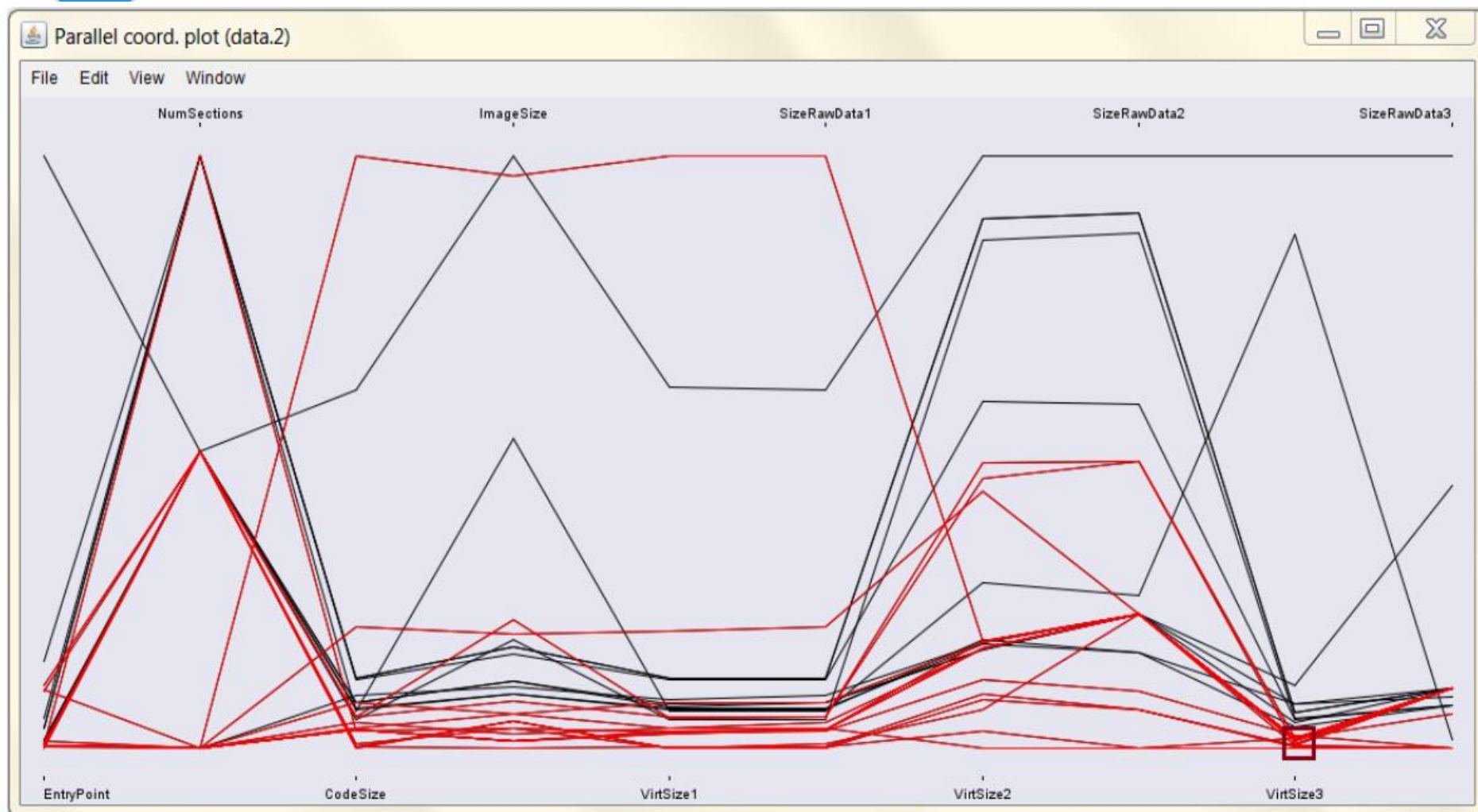


Figure 6 Interactive Parallel graph, selected files with similar Virtual Size of the third section value - Gamarue worm family

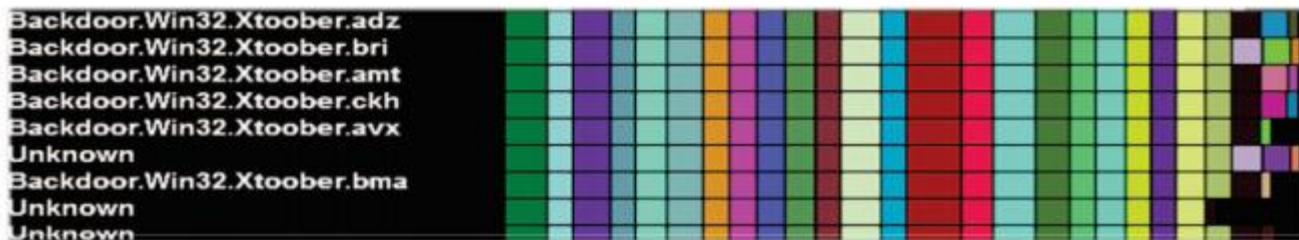


Figure 9. Visually clustering unknown malware samples with known malware samples. The unknown samples appear almost identical to the labeled samples in terms of their behavioral sequences.



Figure 10. Comparing unknown and known samples. There is clearly overlap between the two samples.

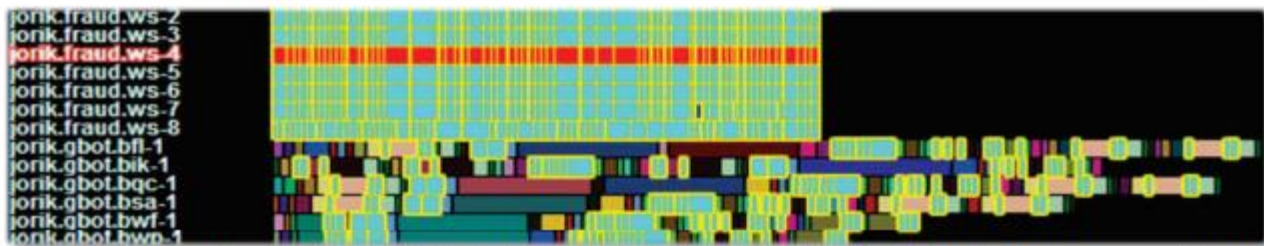


Figure 11. Comparing one sample with many. The user brushes jorik.fraud.ws-4 and it is highlighted in red. As a result, all of the sequences that other samples have in common with jorik.fraud.ws-4 are highlighted.

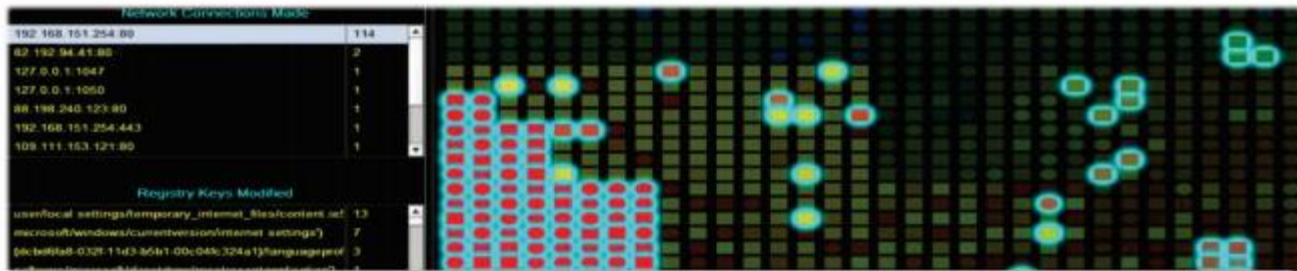
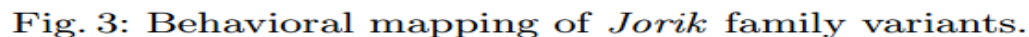
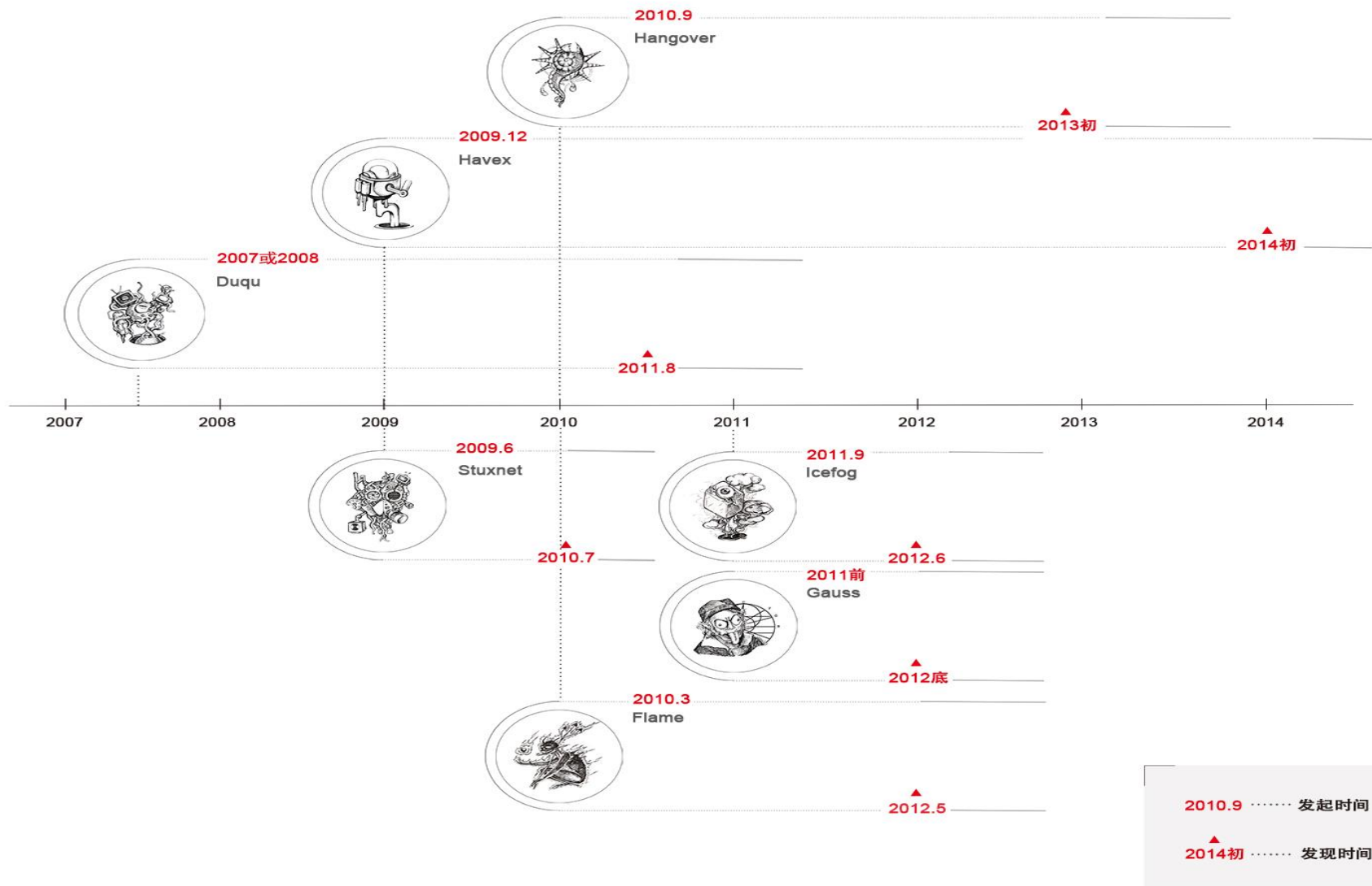
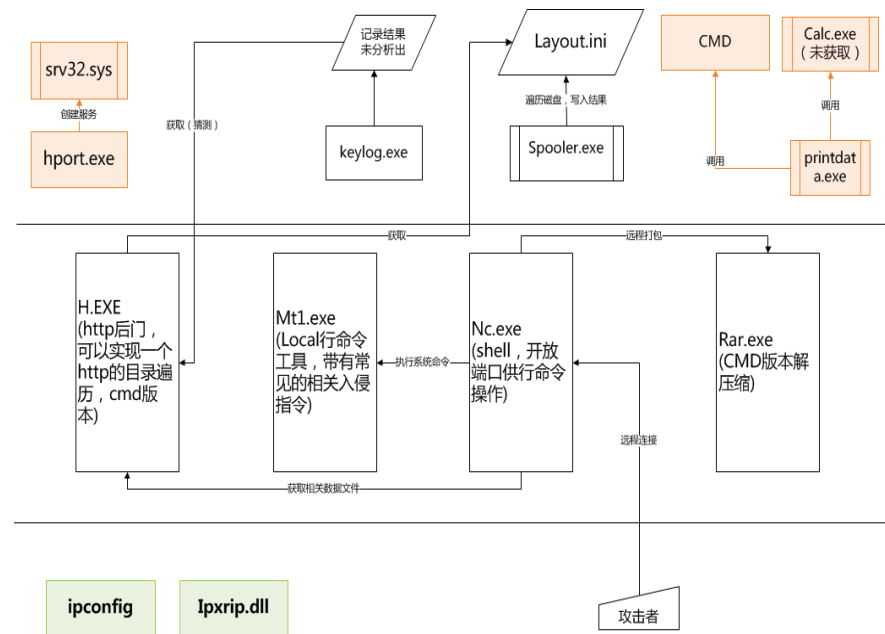
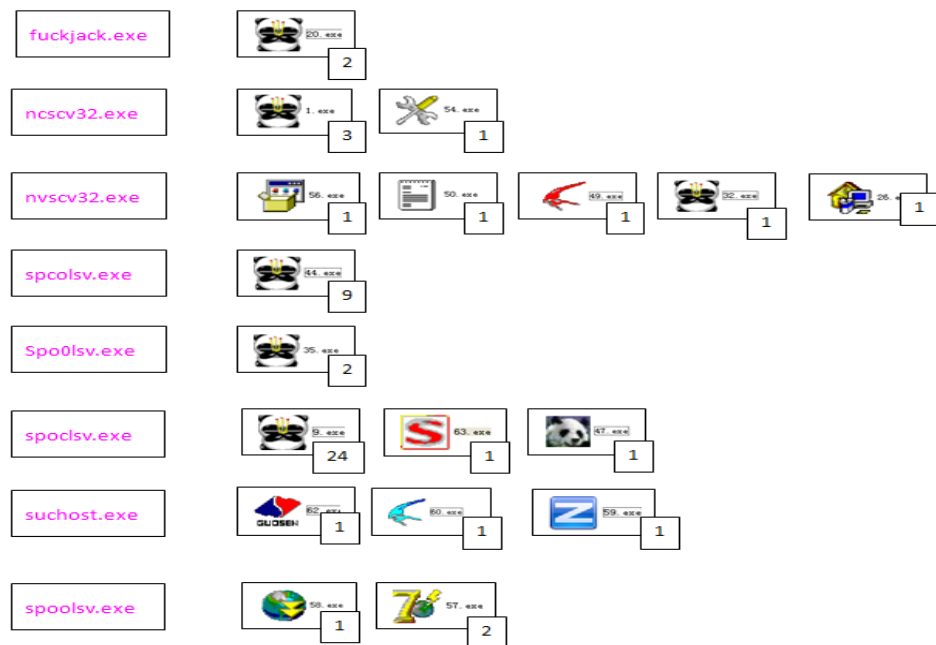


Figure 12. The user brushes an IP address and port on the left, and the samples that connect out to that IP address and port highlight on the right.







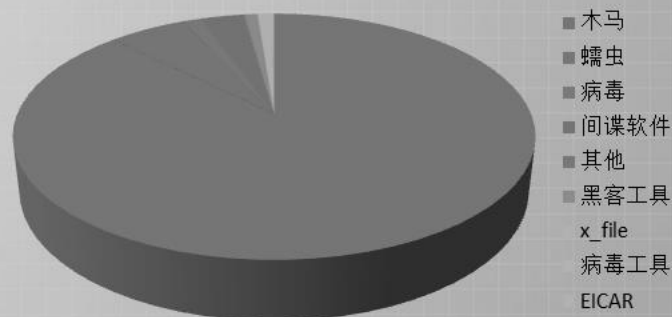
更多传统的同源性方法，基于单一执行体想象

2007所分析的一例定向攻击事件，展示了通过大量开源和免费工具建立一个场景

传统维艰

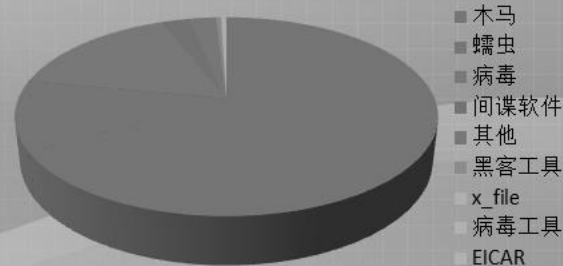
全库种类表		
名称	数量	比例%
木马	1759031	87.47%
蠕虫	114305	5.68%
病毒	28562	1.42%
间谍软件	63837	3.17%
其他	1691	0.08%
黑客工具	18889	0.94%
x_file	20917	1.04%
病毒工具	3765	0.19%
EICAR	1	0.00%
总计	2010998	100.00%

全库种类饼图

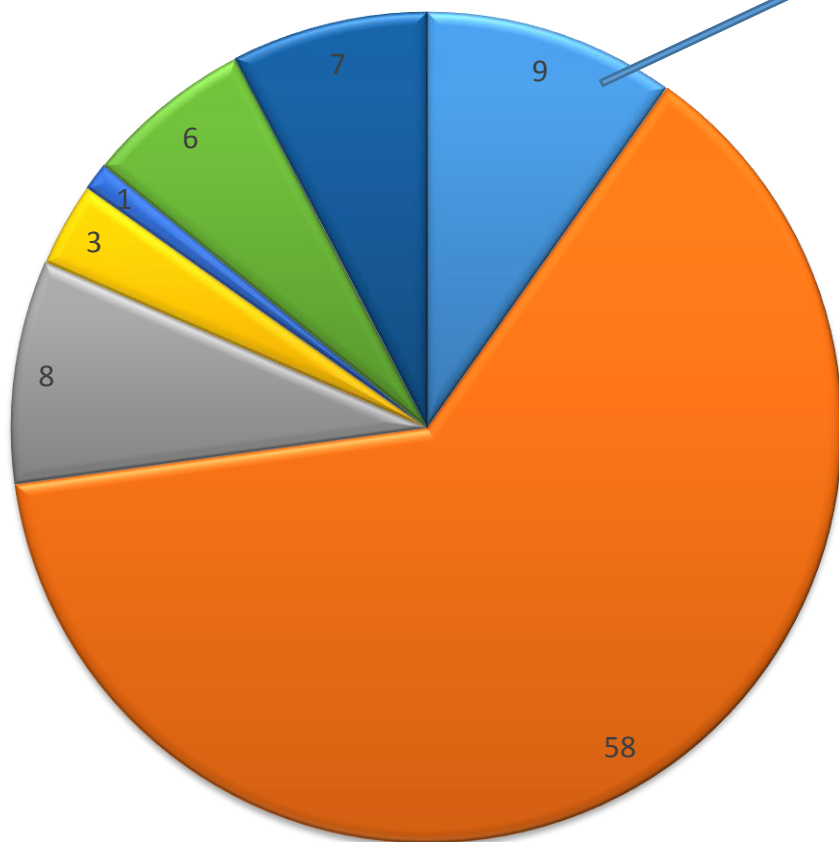


全库样本数量表		
名称	数量	比例%
木马	15533454	66.40%
蠕虫	2722270	11.64%
病毒	3748355	16.02%
间谍软件	622196	2.66%
其他	541844	2.32%
黑客工具	110117	0.47%
x_file	102636	0.44%
病毒工具	11473	0.05%
EICAR	330	0.00%
总计	23392675	100.00%

全库样本数量饼图



AVP引擎检测家族数



- ◆ HEUR:Trojan.Win32.Generic
- ◆ Trojan.Win32.Agent
- ◆ Trojan.Win32.Bublik
- ◆ Trojan.Win32.Gertr
- ◆ Trojan.Win32.Havex
- ◆ Trojan.Win32.Sysmain.b
- ◆ Trojan-Dropper.Win32.Daws.bqsi
- ◆ Trojan-Dropper.Win32.Injector
- ◆ Trojan-Spy.Win32.HavexOPC

■ havex
 ■ hangover
 ■ iceFog
 ■ Gauss
 ■ Duqu
 ■ Flame
 ■ Stuxnet



静态关联点:

- 文件名、文件大小、时间戳、壳信息、编译器信息、入口点、代码段大小、病毒名、SSDEEP...

动态关联点:

- 衍生文件名、衍生文件路径、注册表项及键值、域名、IP、URL、IP地理位置...

查询

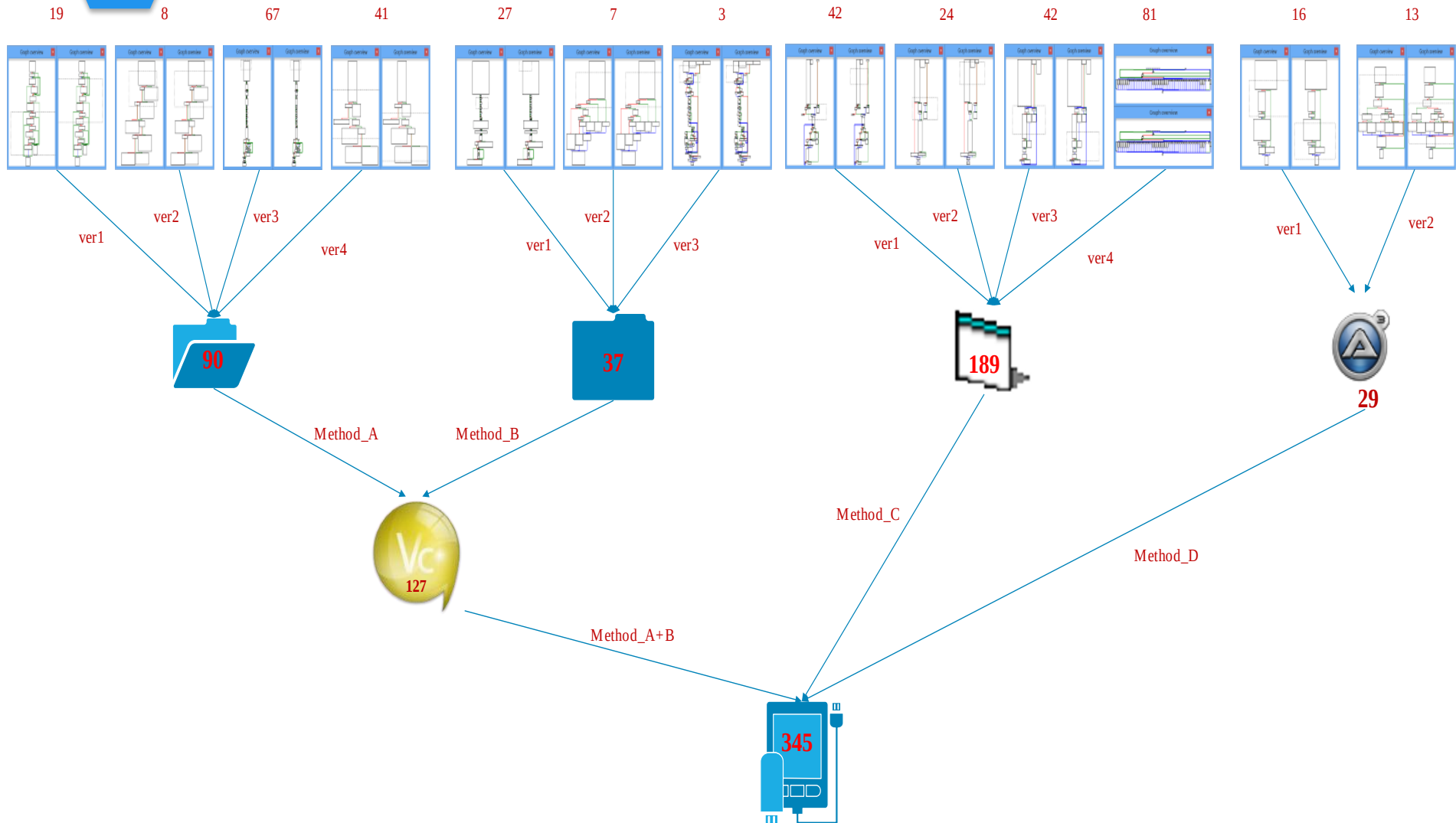
下载样本

SHOW

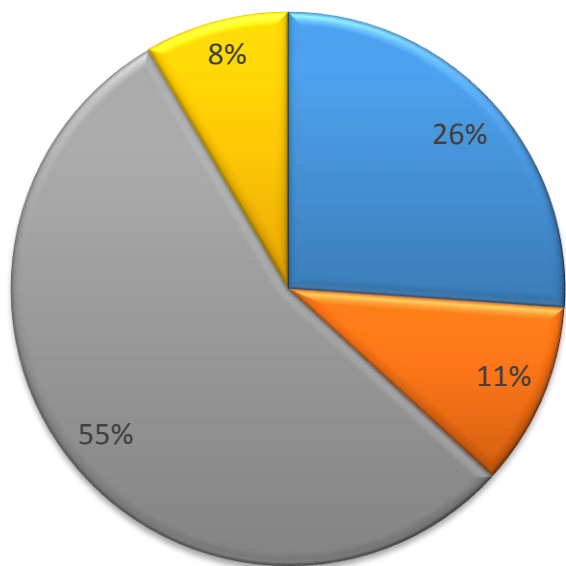


人工确认关联样本

28

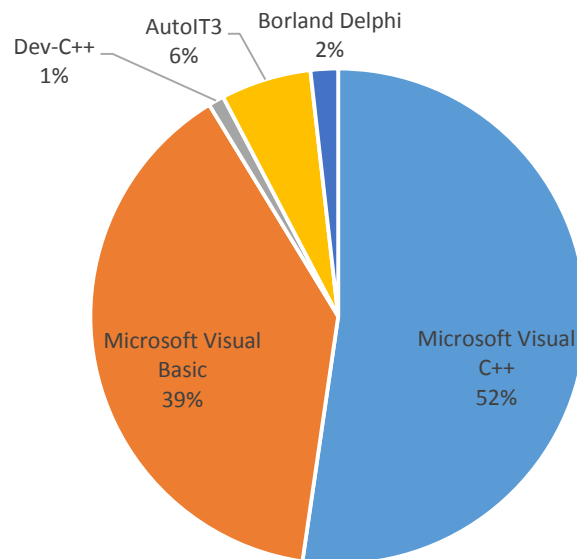


关联出的新的hangover样本



■ Method_A ■ Method_B ■ Method_C ■ Method_D

hangover编译器分布



■ Microsoft Visual C++ ■ Microsoft Visual Basic ■ Dev-C++ ■ AutoIT3 ■ Borland Delphi



从样本集看到Hangover的特点

30

- 攻击组织人员较多（人海战术）
- 编程水平参差不齐
- 无流行厂商的数字证书（窃取） 储备
- 加密算法简单
- 使用大量C&C
- 未见0day漏洞的使用

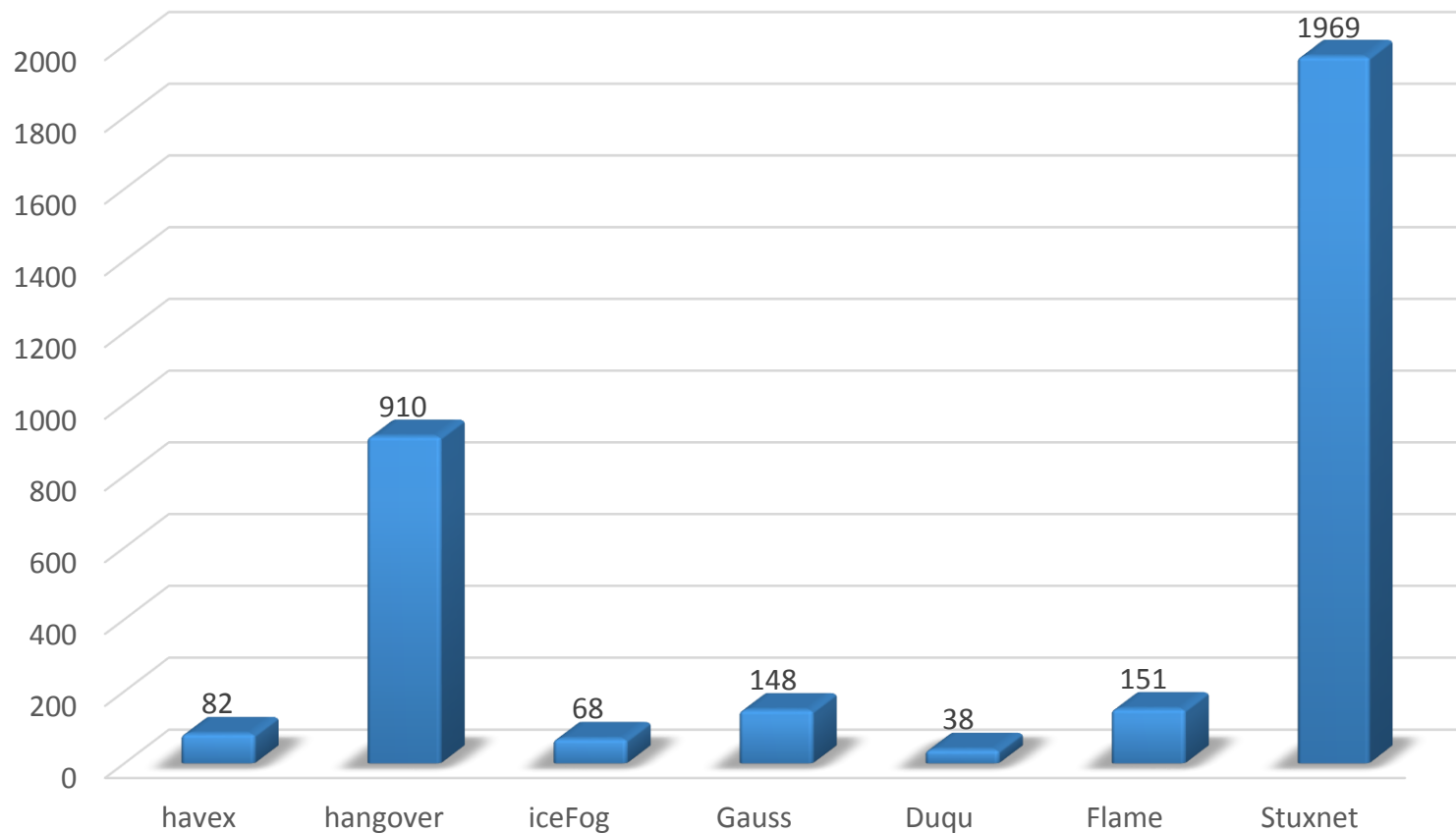


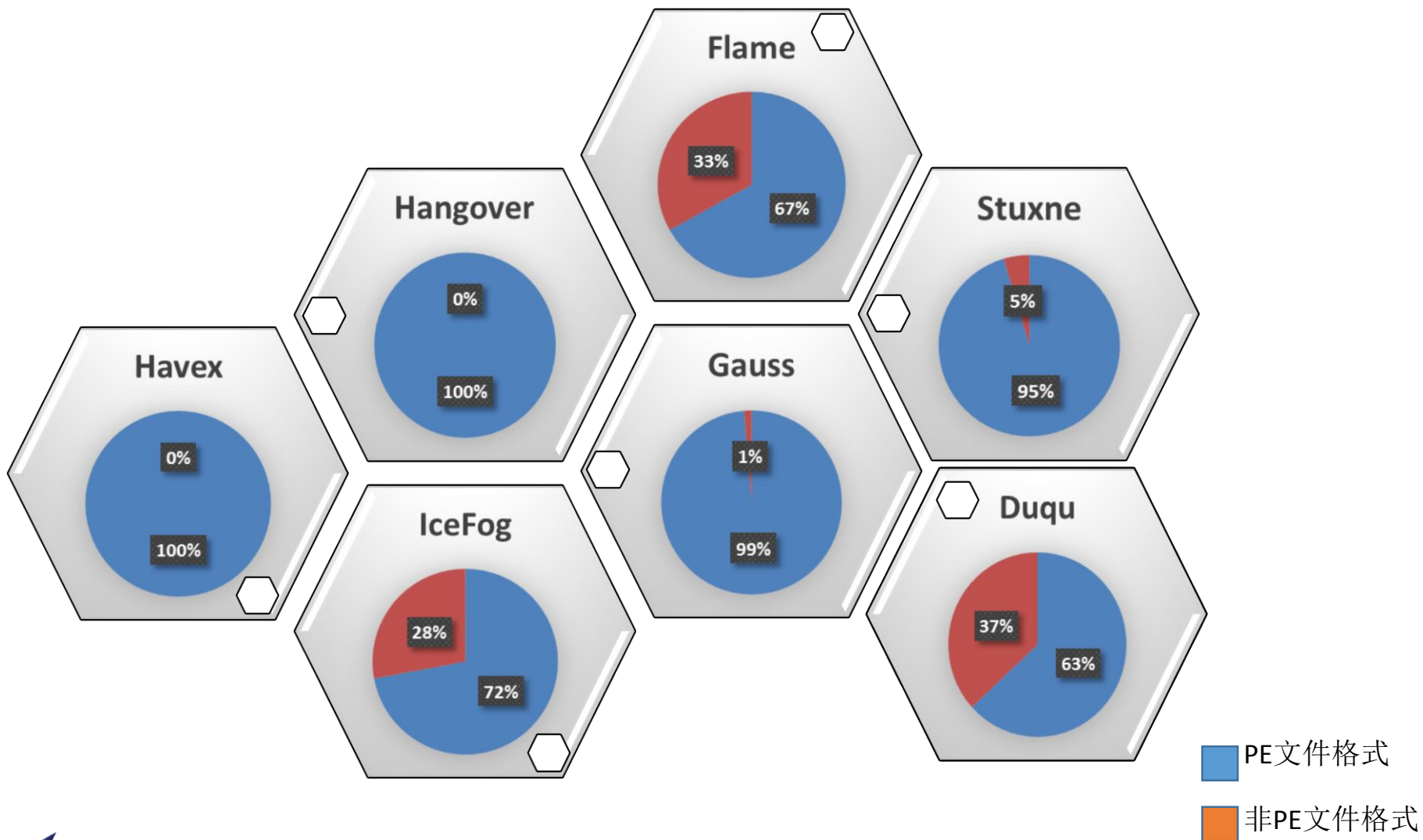
度量

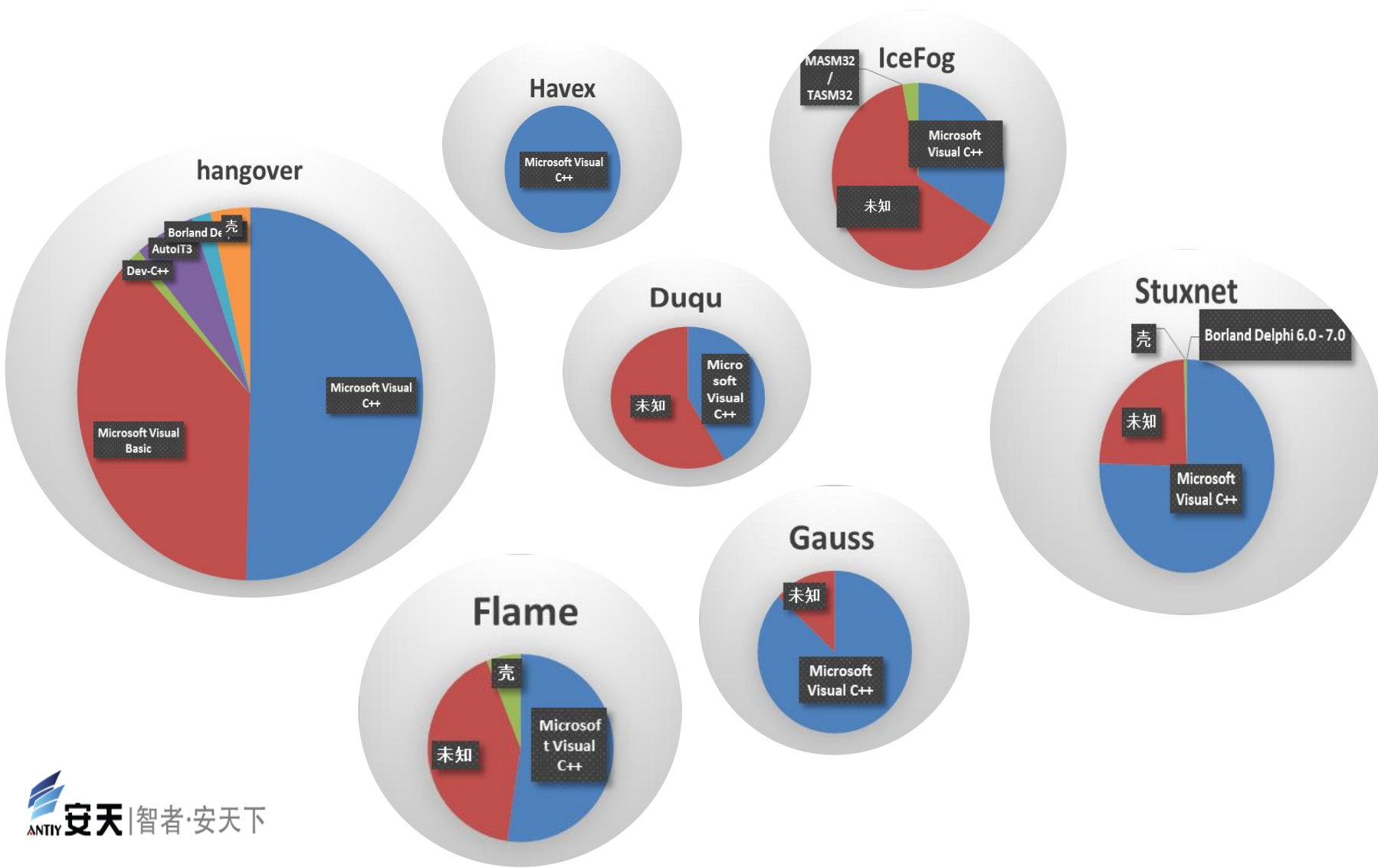
- 如何为样本集建立一些指标。



APT样本集



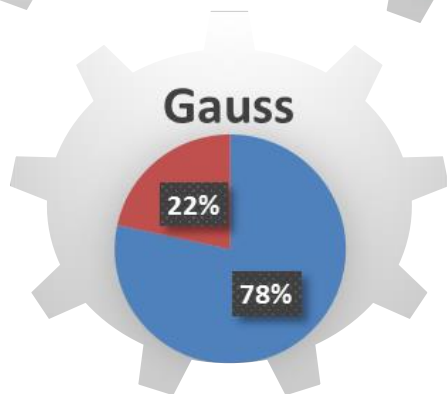
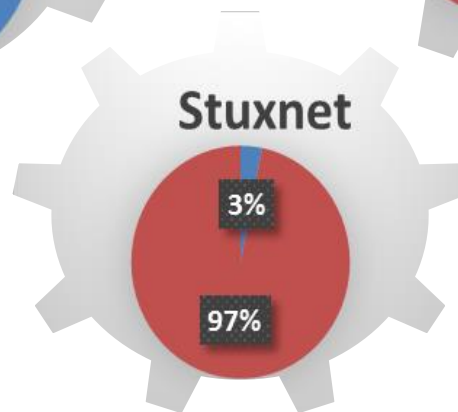
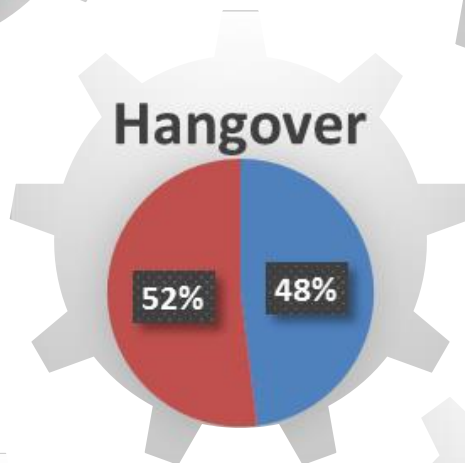
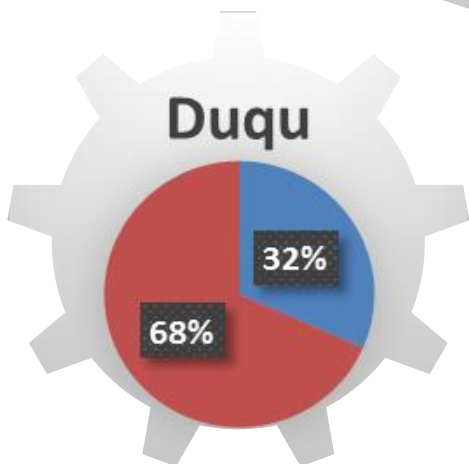
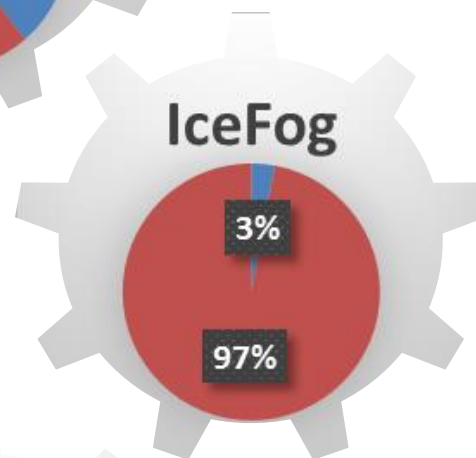
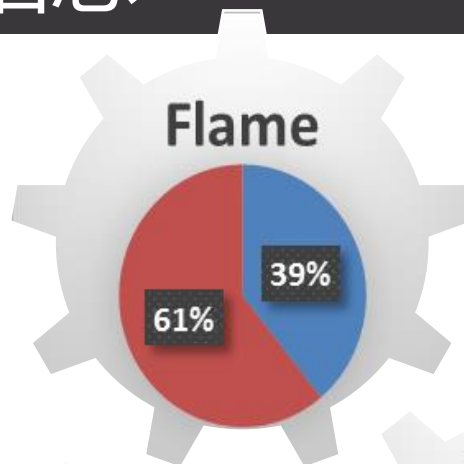
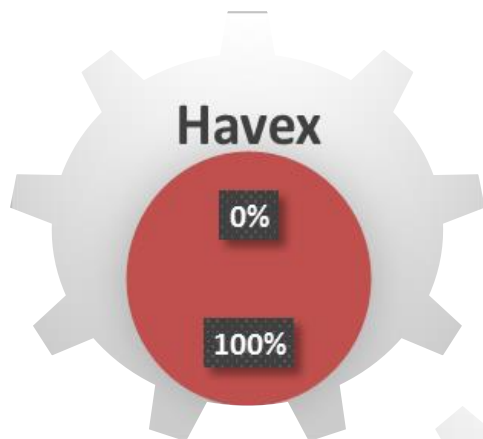




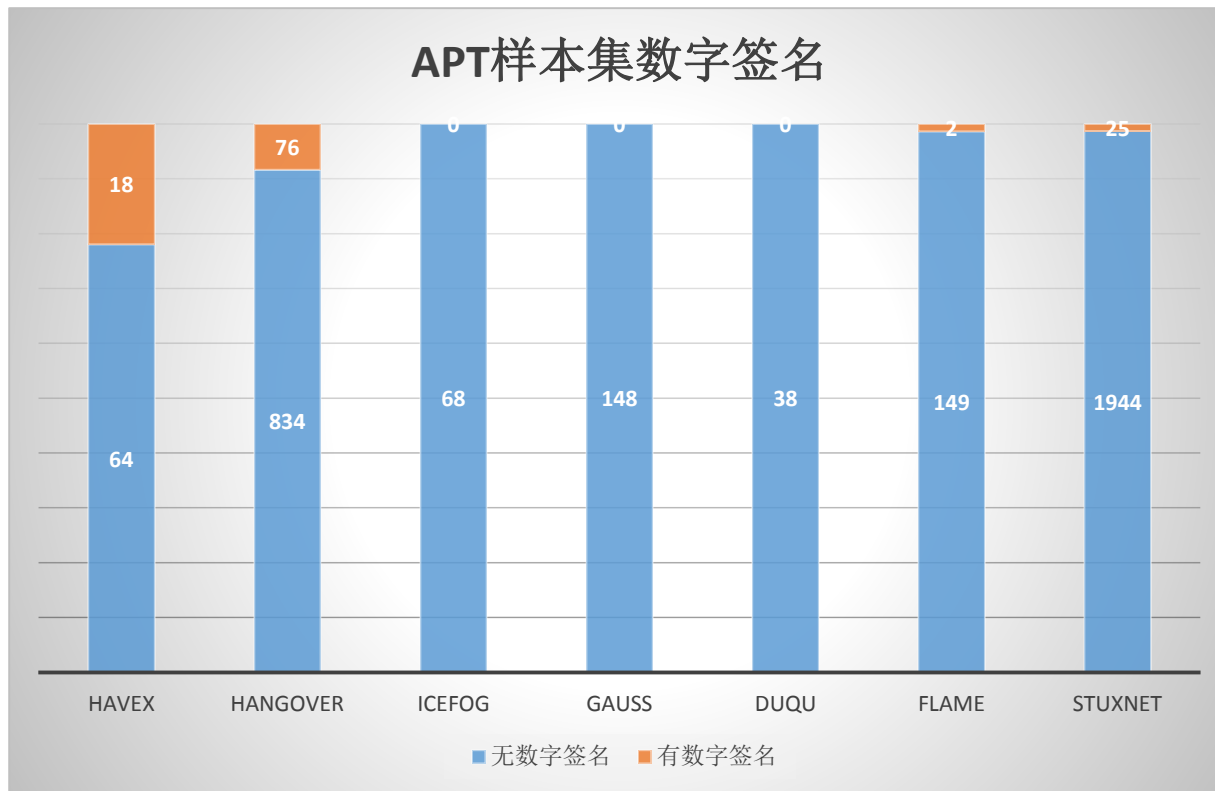


APT样本集PE版本信息

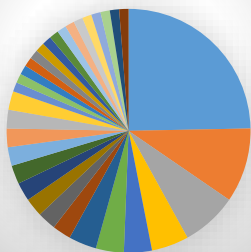
35



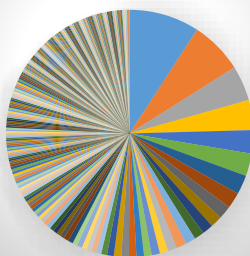
有版本信息
无版本信息



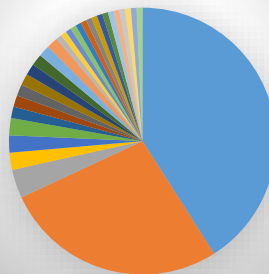
Havexs



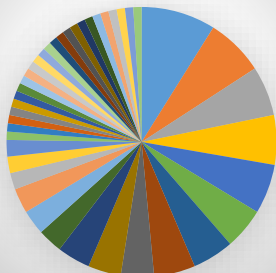
Hngover



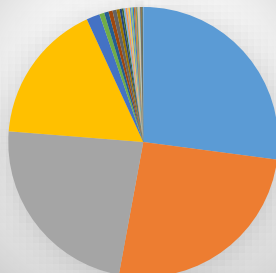
Gauss



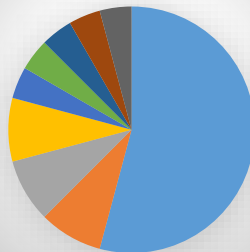
Flame



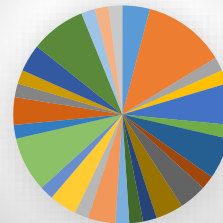
Stuxnet



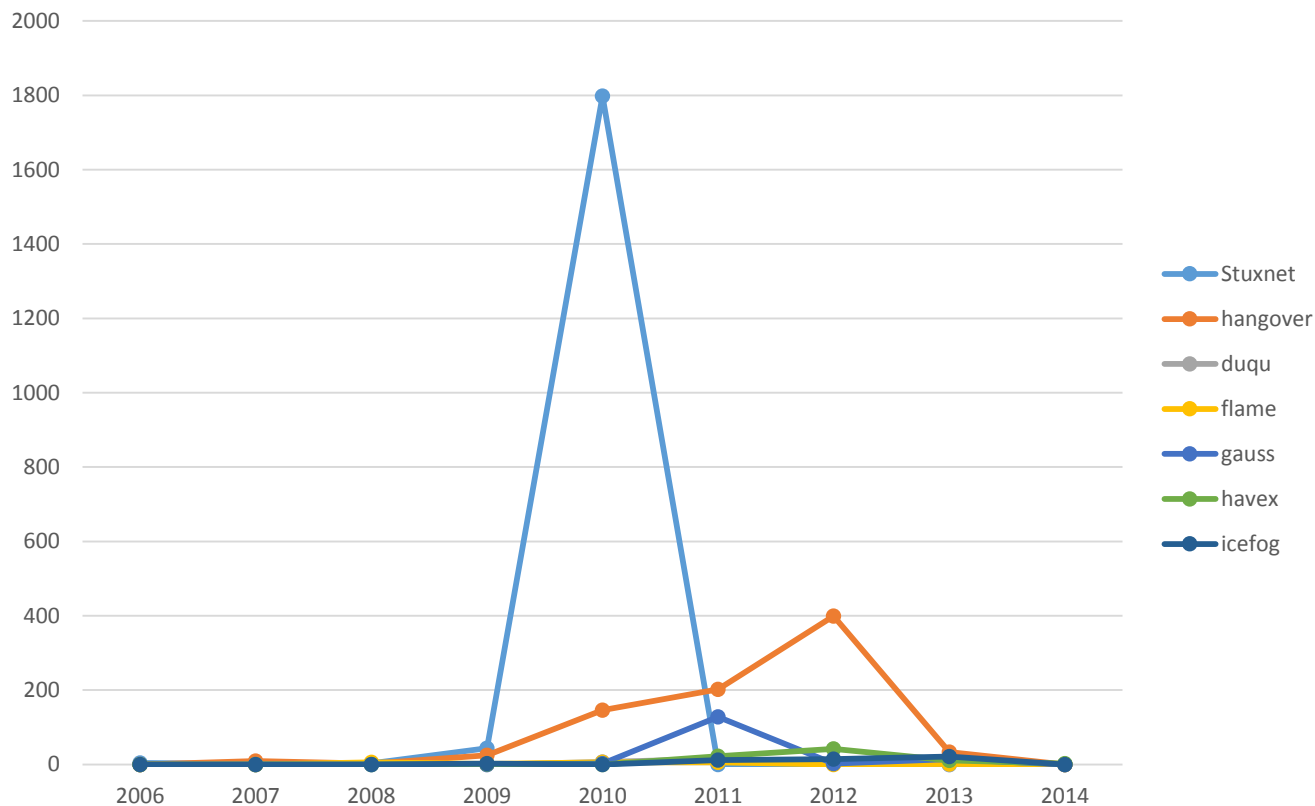
Duqu



IceFog



APT样本集PE文件时间戳







还有很多事情在继续做

40

- 每个事件集合的版本关联图谱？
- Flame、Duqu、Stuxnet的复用描述？
- 为什么Stuxnet有这样多的样本？
- 如何把更精确的计算编码工作量？

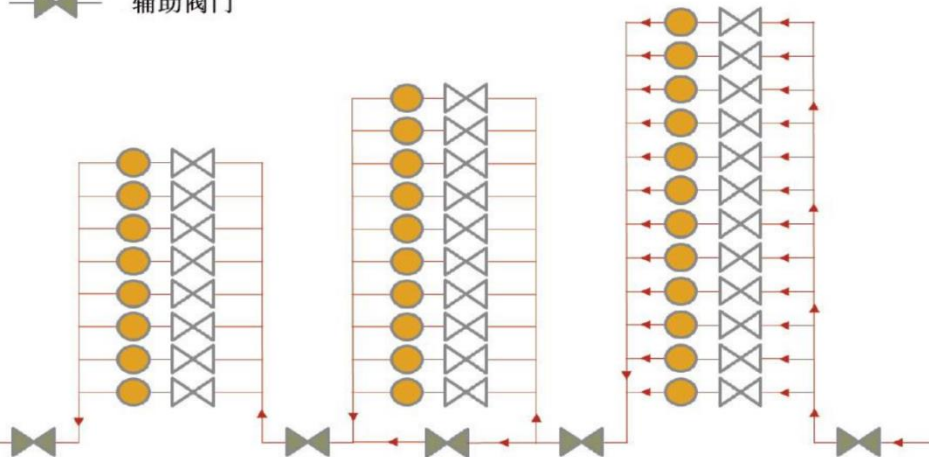
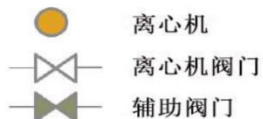


总结

- 样本集是一部分，但也只是一部分。

漏洞	0.500	1.001	1.100	1.101	描述
CVE-2010-3888			X	X	任务调度程序 EOP
CVE-2010-2743			X	X	加载键盘布局 EOP
CVE-2010-2729		X	X	X	PrintSpooler RCE
CVE-2008-4520		X	X	X	Windows 服务器服务 RPC RCE
CVE-2012-3015	X	X	X	X	Step7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC 缺省密码
CVE-2010-2568			X	X	Shortcut.Ink RCE
MS09-025		X			NtUserRegisterClassExWow /NtUserMessengerCall EOP

表 2. Stuxnet 漏洞利用的演变

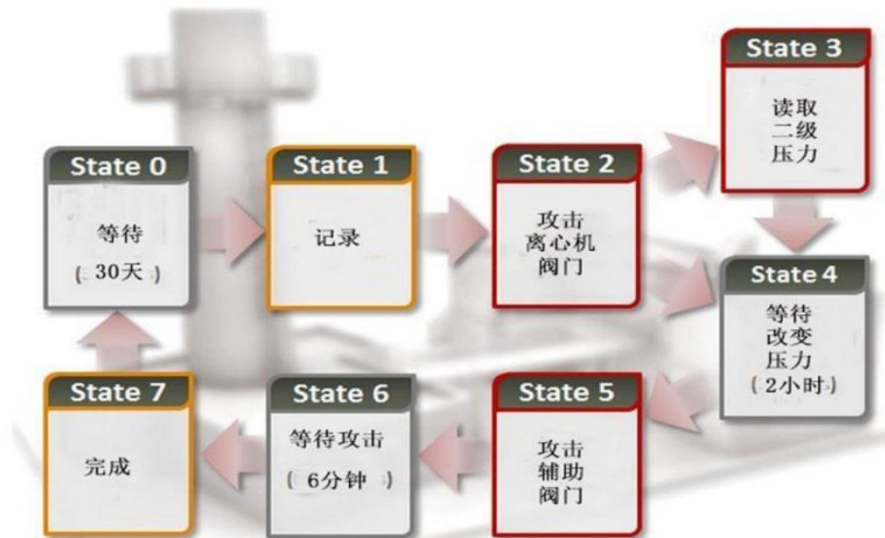


《Stuxnet 0.5 How It Evolved》

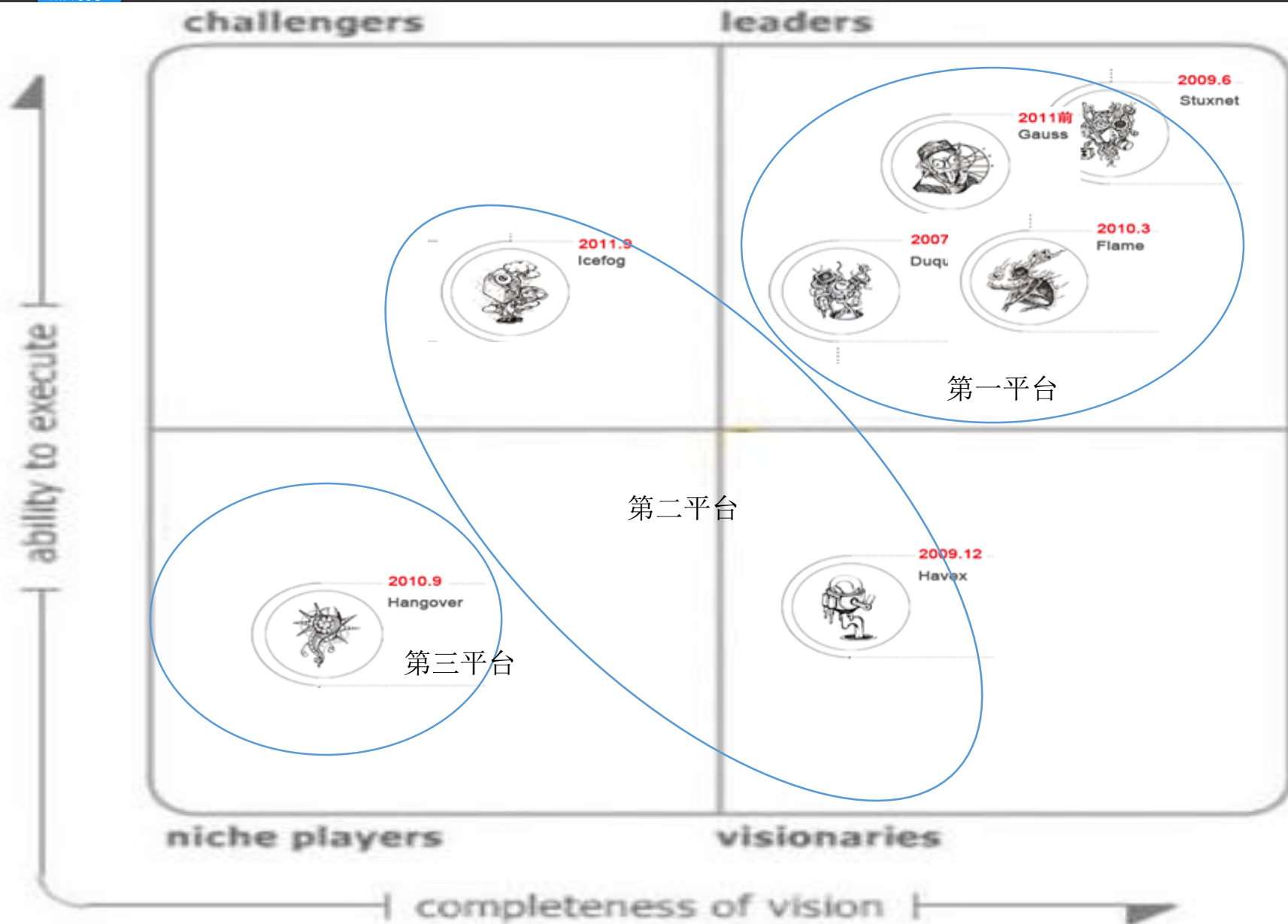
复制技术	0.500	1.001	1.100	1.101
Step 7 项目文件	X	X	X	X
利用 Step 7 项目文件的 USB	X			
利用自动运行的 USB		X		
利用 CVE-2010-2568 的 USB			X	X
网络共享		X	X	X
Windows 服务器 RPC		X	X	X
Printer Spooler		X	X	X
WinCC 服务器		X	X	X
利用 mailslots 进行 P to P 更新	X			
利用 RPC 进行 P to P 更新		X	X	X

表 3. Stuxnet 复制机制的演变

417PLC攻击代码状态流程图



《Stuxnet 0.5 The Missing Link》



- 百万军中取上将首级，如探囊取物。
- 千顷密林擒忍者真身，当信手拈来。
- 梦想尤远，人在征途

感谢交流



seak@antiy.cn



@江海客

Thank you!

