



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

打造一款诊断型个人防火墙

安天 | 技术委员会

CONTENTS

目 录

01

内核中的流量线索

获取对应进程信息以及端口列表

02

实时的诊断及多维联动

扫描感知，溯源，情报，监测，诱捕，取证

03

实际案例与插件体系

用户实践截图、代码演示

04

由现有系统架构带来的展望

Wfp,反-反沙箱，引导程序维护，链接与加载，沙丁鱼系列



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

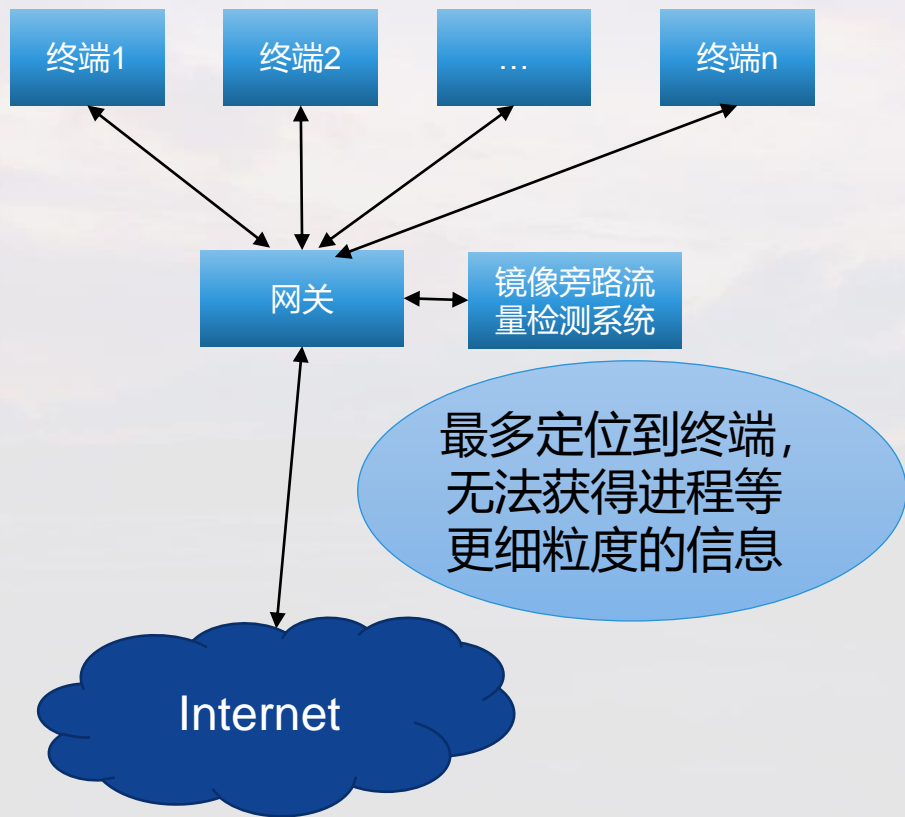
00

场景

进程联网，数据进出，
攻击载荷，取证追溯

0-场景

■ 面临的问题



哪些进程在悄悄联网，连到了哪里？发了什么内容出去？有没有人扫描我？有没有内网沦陷机在横向移动？能否捕获黑客的攻击载荷？能否顺利取证、追溯。

0-场景 围绕用户进程和流量做出设计



启用	策略	进程	Pid	标题	发送	接收	签名	路径
<input checked="" type="checkbox"/>	阻断	teamviewer_ser	5068	TeamViewer		0	TeamViewer Ger	C:\program files (x86)\teamviewer\teamviewer_s
<input checked="" type="checkbox"/>	允许	servicehub.vsde						F:\program files (x86)\microsoft visual studio\20
<input checked="" type="checkbox"/>	允许	perfwatson2.ex						F:\program files (x86)\microsoft visual studio\20
<input checked="" type="checkbox"/>	允许	devenv.exe						F:\program files (x86)\microsoft visual studio\20
<input checked="" type="checkbox"/>	允许	servicehub.ident						F:\program files (x86)\microsoft visual studio\20
<input checked="" type="checkbox"/>	允许	vmware-authd.e	4868	VMware Authori	34503	34503	VMware, Inc.	F:\program files (x86)\vmware\vmware workstat
<input checked="" type="checkbox"/>	允许	vmnat.exe	4636	VMware NAT Ser	125021	861250	VMware, Inc.	C:\windows\systemwow64\vmnat.exe
<input checked="" type="checkbox"/>	允许	vmware.exe	14252	Ubuntu 64 位 - \	12268	1794006	VMware, Inc.	F:\program files (x86)\vmware\vmware workstat
<input checked="" type="checkbox"/>	允许	usocoreworker.e	17188	USO Core Work	4911	13831	Microsoft Windo	C:\windows\system32\usocoreworker.exe
<input checked="" type="checkbox"/>	允许	settingsynchost						C:\windows\system32\settingsynchost.exe
<input checked="" type="checkbox"/>	允许	servicehub.setti						F:\program files (x86)\microsoft visual studio\20
<input checked="" type="checkbox"/>	允许	taskhostw.exe	15748	Windows 任务的	12382	56752	Microsoft Windo	C:\windows\system32\taskhostw.exe
<input checked="" type="checkbox"/>	允许	backgroundtaskd						C:\windows\system32\backgroundtaskhost.exe
<input checked="" type="checkbox"/>	允许	runtimebroker.e	16056	Runtime Broker	6224	8544	Microsoft Windo	C:\windows\system32\runtimebroker.exe
<input checked="" type="checkbox"/>	允许	sihclient.exe	9340	SIH 客户端	700	28452	Microsoft Windo	C:\windows\system32\sihclient.exe
<input checked="" type="checkbox"/>	允许	nvcontainer.exe	2624	NVIDIA Containe	5035	18334	NVIDIA Corpora	C:\program files\nvidia corporation\nvcontainer\
<input checked="" type="checkbox"/>	允许	igfxem.exe	7392	igfxEM Module	448	3268	Microsoft Windo	C:\windows\system32\driverstore\filerepository\
<input checked="" type="checkbox"/>	允许	devicecensus.ex						C:\windows\system32\devicecensus.exe

runtimebroker.exe			中文
			English
阻断	端口		
<input type="checkbox"/>	56475	TCP	
<input type="checkbox"/>	56476	TCP	
<input type="checkbox"/>	56477	TCP	
<input type="checkbox"/>	56658	TCP	

记录流量 PCAP 大小: 0

日志记录

```
10:02:48(v)[TCP] 192.168.8.166:56476->117.18.237.29:80+240
10:02:48(v)[TCP] 192.168.8.166:56476<-117.18.237.29:80+798
10:02:48(v)[TCP] 192.168.8.166:56477->204.79.197.203:80+249
10:02:48(v)[TCP] 192.168.8.166:56477<-204.79.197.203:80+2354
10:02:48(v)[TCP] 192.168.8.166:56475->13.91.100.157:443+158
10:02:48(v)[TCP] 192.168.8.166:56475<-13.91.100.157:443+326
10:02:48(v)[TCP] 192.168.8.166:56475->13.91.100.157:443+2128
10:02:48(v)[TCP] 192.168.8.166:56475->13.91.100.157:443+298
10:02:48(v)[TCP] 192.168.8.166:56475<-13.91.100.157:443+376
10:13:42(v)[TCP] 192.168.8.166:56658->13.91.100.157:443+483
10:13:42(v)[TCP] 192.168.8.166:56658<-13.91.100.157:443+145
10:13:42(v)[TCP] 192.168.8.166:56658->13.91.100.157:443+51
10:13:42(v)[TCP] 192.168.8.166:56658->13.91.100.157:443+2128
10:13:42(v)[TCP] 192.168.8.166:56658->13.91.100.157:443+298
10:13:42(v)[TCP] 192.168.8.166:56658<-13.91.100.157:443+376
```

地理位置

13.91.100.157= 美国Microsoft公司
117.18.237.29= 香港
204.79.197.203= 美国华盛顿州雷德蒙德市Microsoft公司

公共规则

允许 阻断



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

01

内核中的流量线索

获取对应进程信息以及端口列表

1-内核中的流量线索

■ 个人防火墙技术演进史

早期的各类hook
Filter Hook
Firewall Hook
...

逐渐失效、淘汰
但hook的思想永不灭

TDI
(Transport Driver Interface)

协议设备绑定
如: \Device\Tcp
不够底层, 容易bypass

1-内核中的流量线索

■ 个人防火墙技术演进史

NDIS
(Network Driver Interface
Specification)

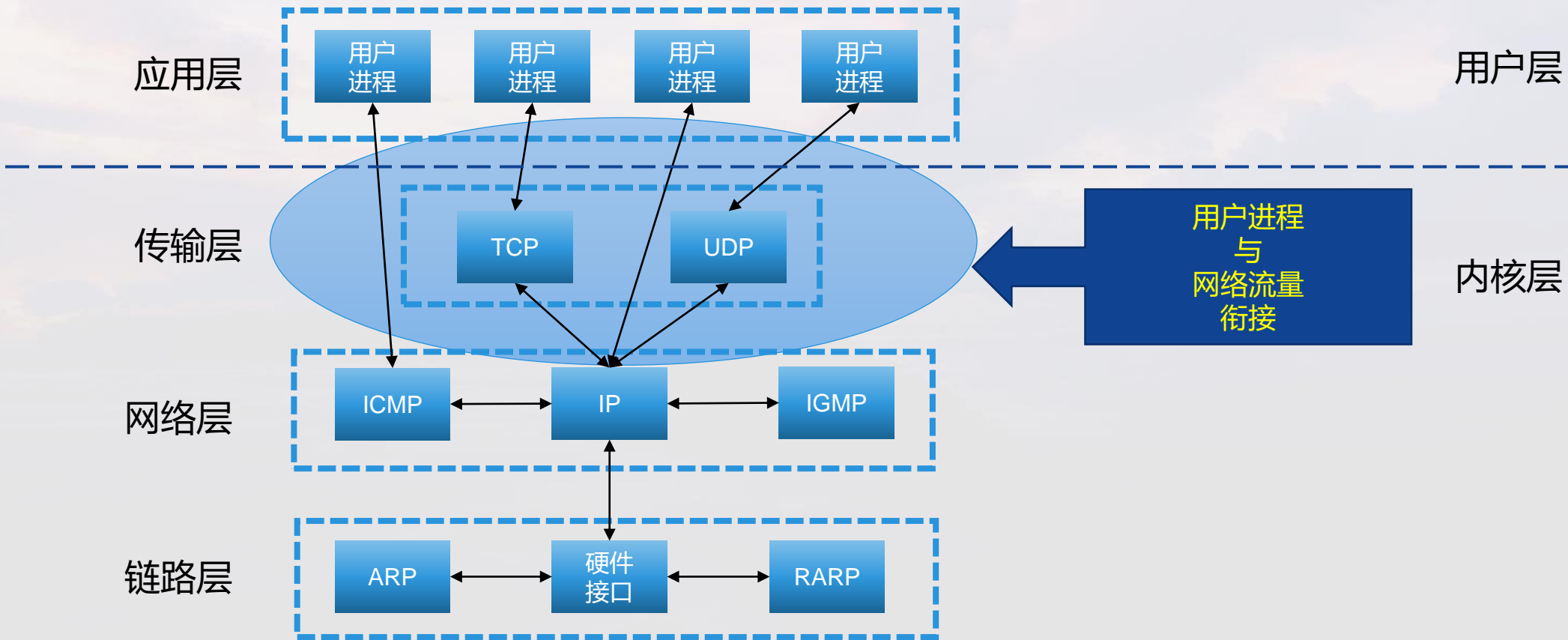
- 1.协议驱动：插入自定协议。
- 2.小端口驱动：虚拟设备。
- 3.中间层驱动：本质依然是Hook。都无法拿进程信息。如：WireShark就是用的NDIS驱动。

WFP
(Windows Filter Platform)

目前微软推荐的过滤框架，后面详细说明。

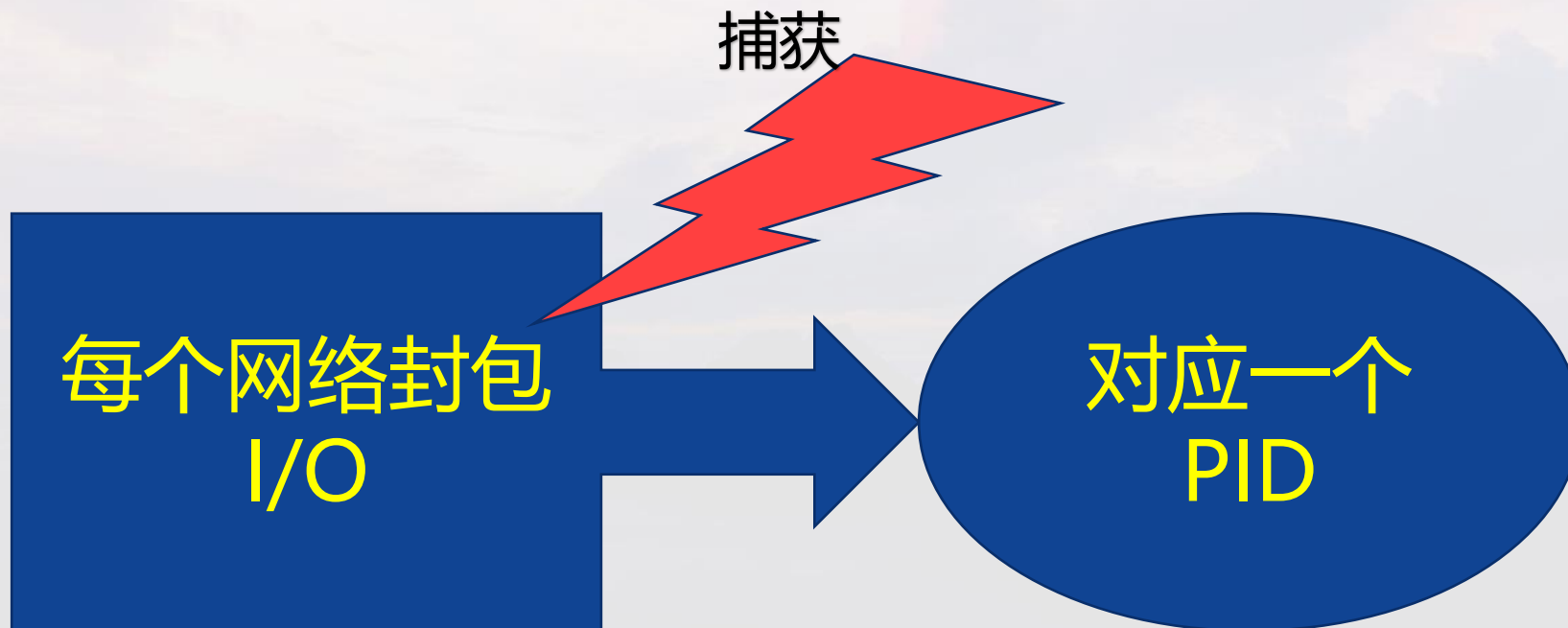
1-内核中的流量线索

■ Internet所基于的TCP/IP协议模型，各个层次在操作系统中的分布



1-内核中的流量线索

■ 合适的机制



1-内核中的流量线索

■ 再看设计，进程对应的部分端口操作

程序规则 端口规则 插件系统 应用扩展 菜单

启用	策略	进程	Pid	路径
<input checked="" type="checkbox"/>	阻断	teamviewer_service.e		C:\prograr
<input checked="" type="checkbox"/>	允许	vmnat.exe		C:\window
<input checked="" type="checkbox"/>	允许	firefox.exe	7328	C:\prograr
<input checked="" type="checkbox"/>	允许	vmware.exe		C:\prograr
<input checked="" type="checkbox"/>	允许	vmware-hostd.exe		C:\prograr
<input checked="" type="checkbox"/>	允许	perfwatson2.exe		C:\prograr
<input checked="" type="checkbox"/>	允许	devenv.exe		C:\prograr
<input checked="" type="checkbox"/>	允许	servicehub.vsdetour		C:\prograr
<input checked="" type="checkbox"/>	允许	servicehub.identityhc		C:\prograr
<input checked="" type="checkbox"/>	允许	backgrounddownload		C:\prograr

firefox.exe

阻断	端口	协议
<input type="checkbox"/>	62871	TCP
<input type="checkbox"/>	62872	TCP
<input type="checkbox"/>	62873	TCP
<input type="checkbox"/>	62874	TCP

日志

```
[v][TCP]192.168.8.166:62868->18.178.52.42:443
[v][TCP]192.168.8.166:62869->103.43.90.55:443
[v][TCP]192.168.8.166:62870->18.178.52.42:443
[v][TCP]192.168.8.166:62871->18.178.52.42:443
[v][TCP]192.168.8.166:62872->152.199.40.143:443
```

地理位置

```
52.221.148.22= 新加坡Amazon数据中?
13.57.64.215= 美国加利福尼亚州旧金山Amazon数据中心
67.195.231.24= 美国
117.18.232.12=香港
180.222.102.159=台湾省 桃园市Yahoo(TP2)数据中心
180.222.102.162=台湾省 桃园市Yahoo(TP2)数据中心
152.199.40.143= 亚太地区
```

公共规则

全部允许 全部阻断

编辑

禁止感染端口，
开放正常端口。
杀毒不停机。

1-内核中的流量线索

- 由PID引出更多维度的信息，作为检测向量，接下来就可以多维联动了

进程名

环境变量
PEB、TEB

异常
HOOK

签名证书

.....

模块列表

文件路径

堆喷
ROP
ShellCode

传参列表

远端地理
位置



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

02

实时的诊断及多维联动

扫描感知, 溯源, 情报, 监测, 诱捕, 取证

2-实时的诊断及多维联动

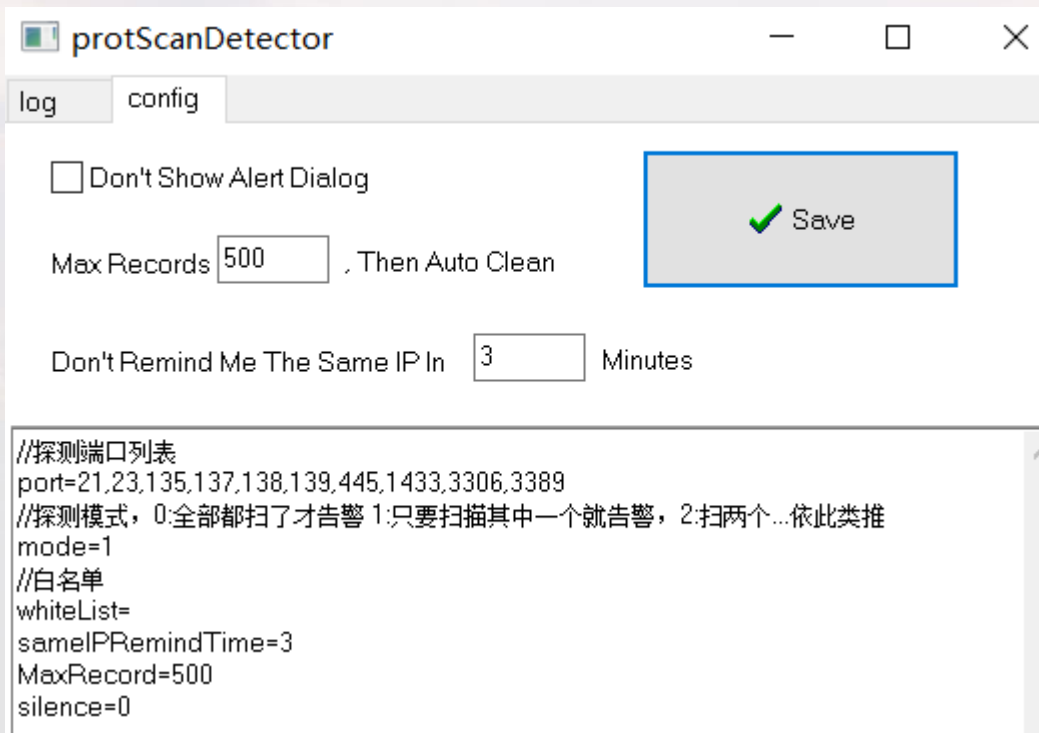


- 联动的形式：所有外部联动基于插件扩展，保持低耦合，易维护

启用	名称	作者	详细描述
<input type="checkbox"/>	logManager	Simpower	日志记录插件，同时提供全日志查询图形界面
<input type="checkbox"/>	logManger	Simpower	日志记录插件，同时提供全日志查询图形界面
<input type="checkbox"/>	advClean	Simpower	清理弹窗
<input checked="" type="checkbox"/>	geolocation	Simpower	在线获取地理位置,用的人太多会Ddos封IP，造成查询失效，需要时启用，否则禁用
<input checked="" type="checkbox"/>	PortScanDetect	Simpower	端口扫描探测插件，如果被人扫描，则告警！
<input type="checkbox"/>	pythonEngin	Simpower	支持用log.py(Python,例子是python2.7语法)脚本来获取日志并进行处理，需要安装32位python环境，
<input type="checkbox"/>	PluginTemp	Simpower	插件模板生成（C++语法）
<input type="checkbox"/>	HoneyPot	Simpower	小蜜，可以打开端口，并将端口的流量转发致安全大脑(或蜜罐)进行分析。
<input type="checkbox"/>	PASUnion	Simpower	流量分析联动插件，可以将流量信息上报至安天PAS或PTD，也可通过cfg.txt联动其他中控或分析系统
<input type="checkbox"/>	ThreatIntelligen	gzy2001	威胁情报联动
<input type="checkbox"/>	UserCounter	Simpower	用户体验计划，统计本软件功能使用频率，启用本插件可以帮助我们做好产品！

2-实时的诊断及多维联动

■ 端口扫描感知插件的图形界面 及 告警窗口



根据远端尝试接入的连接信息
(如: 敏感端口列表, 连接频率), 判断自己是否被扫描



2-实时的诊断及多维联动

■ 端口扫描感知的配置脚本设计

```
//探测端口列表  
port=21,23,135,137,138,139,445,1433,3306,3389  
//探测模式, 0:全部都扫了才告警 1:只要扫描其中一个就告警, 2:扫两个...依此类推  
mode=1  
//白名单  
whiteList=  
sameIPRemindTime=3  
MaxRecord=500  
silence=0
```

2-实时的诊断及多维联动

■ 端口扫描感知的日志记录

远端IP 扫描时间, 被扫描的本机端口
192.168.8.200=2022-01-08 19:10:24,137

.....

2-实时的诊断及多维联动

■ 蜜罐联动



通过模拟端口，将首包发送至蜜罐，用于诊断是否自己正在被攻击，通过自定义的协议建立代理，将攻击方数据透明转发至蜜罐，进行下一步的追踪捕获等

2-实时的诊断及多维联动

- 流量检测系统联动，如:ptd, pas等

配置文件: cfg.txt

```
ip=127.0.0.1  
port=8091
```

与流量检测系统的联动，使得流量检测系统能够定位到异常流量所**对应的样本**，方便取证。

- 报文标准:

- 五元组+程序路径+时间(精确到毫秒)。
- 五元组对应程序路径如果没有变动，则只发一次，如果后面对应关系有了变化，则再次发送。

这样设计的好处是尽可能减少额外流量，每个应用只需要多出几十个字节即可完成联动。

2-实时的诊断及多维联动

■ 威胁情报联动:

根据IP, c2等

■ 与赛博超脑联动:

通过获取关键网络封包(如: 首包), 并将其发送至赛博超脑, 用于分析, 并传回结果, 决定是否封锁异常进程。

.....



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

03

实际案例与插件体系

用户实践截图、代码演示

3-实际案例与插件体系

■ 某电力行业国企发现病毒并清理



来自用户的截图：任务管理器看不到该进程ID，而防火墙却看到ID11896正在联网，发送和接收数据。

The screenshot shows two windows side-by-side. The left window is the ANTIY firewall's '程序规则' (Program Rules) tab, displaying a list of rules. The right window is the Windows Task Manager, showing a list of running processes.

启用	策略	进程	Pid	标题	发送	接收	名称	PID	状态	用户名	CPU	内存活动...	UAC	虚拟化
<input checked="" type="checkbox"/>	允许	fypid.exe	11896	11896 316	4413	C:\users\alex\AppData\Local\Temp\...	Foxmail.exe	11500	正在运行	Alex	00	5,480 K	不允许	
<input checked="" type="checkbox"/>	允许	svchost.exe	2876	2876 16971	159988	C:\windows\system32\svchost.exe	chrome.exe	11892	正在运行	Alex	00	18,532 K	不允许	
<input checked="" type="checkbox"/>	允许	update.exe	6276	6276 1263	4286	C:\downloads\install\update.exe	svchost.exe	12076	正在运行	SYSTEM	00	1,152 K	不允许	
<input checked="" type="checkbox"/>	允许	pt3100sm.exe	14744	14744 11660		C:\windows\system32\pt3100sm.exe	dllhost.exe	12216	正在运行	Alex	00	1,872 K	不允许	
<input checked="" type="checkbox"/>	允许	system	4	4 1740	50469	system	TextInputHost.exe	12376	正在运行	Alex	00	13,144 K	不允许	
<input checked="" type="checkbox"/>	允许	wxwork.exe	16272	企业微信 7053	8336	C:\program files (x86)\wxwork\wxwork.exe	chrome.exe	12424	正在运行	Alex	00	8,536 K	不允许	
<input checked="" type="checkbox"/>	允许	qqqprt.exe	2820	2820 27071	180	C:\program files (x86)\tencent\qq\qqqprt.exe	SearchApp.exe	12792	已挂起	Alex	00	0 K	不允许	
<input checked="" type="checkbox"/>	允许	qqqctray.exe	9724	9724 10784	4730	C:\program files (x86)\tencent\qq\qqqctray.exe	RuntimeBroker.exe	12908	正在运行	Alex	00	22,848 K	不允许	
<input checked="" type="checkbox"/>	允许	qqcmgrupdate.exe	13924	13924 2574	198	C:\program files (x86)\tencent\qq\qqcmgrupdate.exe	WeChatApp.exe	13080	正在运行	Alex	00	63,276 K	不允许	

该用户反馈，打开国税局的网站，会自动跳到广告页面，显然是中毒了，而该公司安装的友商某擎未报毒，同时又向某讯管家和某绒反馈均未得到解决。于是拿本防火墙来试一下。

3-实际案例与插件体系

■ 某电力行业国企发现病毒并清理

```
C:\Users\Alex>taskkill /PID 11896  
错误：没有找到进程“11896”。
```

- 用户试图通过命令行结束该隐藏进程，然而却提示没有找到进程11896。

- 用户在某论坛的反馈（未得到解决）：

<http://bbs.huorong.cn/forum.php?mod=viewthread&tid=69678&highlight=%E7%96%91%E4%BC%BC&mobile=2>

3-实际案例与插件体系

■ 某电力行业国企发现病毒并清理

启用	策略	进程	Pid	标题	发送	接收	路径
<input type="checkbox"/>	允许	fypid.exe	11896	11896	316	4413	C:\users\alex\AppData\Local\Fypid\Fypid.exe
<input type="checkbox"/>	允许	svchost.exe	2876	2876	174912	185384	C:\windows\system32\svchost.exe
<input type="checkbox"/>	允许	update.exe	6276	6276	1263	4386	C:\download\update\update.exe
<input type="checkbox"/>	允许	pt3100sm.exe					

根据防火墙找到的进程所在路径，找到了该样本，并获取了该样本的签名证书。在内核中结束进程，并清理文件之后电脑恢复正常。
注意：该软件有**合法证书签名**。

文件资源管理器地址：用户 > Alex > AppData > Local > Fypicl

名称	修改日期	类型	大小
Fypicl.exe	2019-09-18 12:37	应用程序	694 KB
FyPicOverlayout.ini	2020-06-01 8:03	配置设置	1 KB

Fypicl.exe 属性

数字签名

签名者姓名	摘要算法	时间戳
浙江自贸区耀光网络科技有限公司	sha1	2019-09-11 1
浙江自贸区耀光网络科技有限公司	sha256	2019-09-11 1

3-实际案例与插件体系

某电力行业国企发现病毒并清理

启用	策略	进程	Pid	标题	发送	接收	路径
<input type="checkbox"/>	允许	fypid.exe	11896	11896	316	4413	C:\users\alex\appdata\local\fypid\fypid.exe
<input type="checkbox"/>	允许	svchost.exe	2876	2876	388627	3370246	C:\windows\system32\svchost.exe
<input type="checkbox"/>	允许	update.exe	6276	6276	1263	4286	C:\downloads\install\update.exe
<input type="checkbox"/>	允许	pt3100am.exe	14744	14744	88298		C:\windows\system32\pt3100am.exe
<input type="checkbox"/>	允许	system					
<input type="checkbox"/>	允许	wwork.exe					
<input type="checkbox"/>	允许	qqportp.exe					
<input type="checkbox"/>	允许	qqctray.exe					
<input type="checkbox"/>	允许	qqqongupdate.exe	13924	13924	2574	198	C:\program files (x86)\ Tencent\qqqong\13.6.20621.222\qru
<input type="checkbox"/>	允许	ingress.exe	12520	12520	1221		C:\program files\angfor\ingress3.0.2\ingress.exe
<input type="checkbox"/>	允许	chrome.exe	14196	23.2.1	371868	15633765	C:\program files (x86)\google\chrome\application\chrome.exe
<input type="checkbox"/>	允许	pic_2345svc.exe	3992	3992	10295	4898	C:\program files (x86)\2345soft\2345pic\protect\pic_2345svc.
<input type="checkbox"/>	允许	wrguard.exe	6128	6128	89783		C:\program files\angfor\ingress3.0.2\wrguard.exe
<input type="checkbox"/>	允许	cdgrededit.exe	16104	CDGRe	29257	30040	C:\program files\safenet\cobra docguard client\cdgrededit.e
<input type="checkbox"/>	允许	backgroundtaskhost.exe	5156	5156	47185	118637	C:\windows\system32\backgroundtaskhost.exe
<input type="checkbox"/>	允许	backgroundtransferhost.exe	8104	8104	3575	4322430	C:\windows\system32\backgroundtransferhost.exe
<input type="checkbox"/>	允许	wechat.exe	15268	微信	584733	20119440	C:\program files (x86)\tencent\wechat\wechat.exe
<input type="checkbox"/>	允许	2345picminipage.exe	9092	9092	7748	6310	C:\program files (x86)\2345soft\2345pic\protect\service\10.7

这是该用户发现的又一例，悄悄摸摸的隐藏自己，却背地里不停的联网收发数据。
截图中8104进程在任务管理器里根本看不到。

名称	PID	状态	用户名	CPU	内
dllhost.exe	6492	正在运行	NETWOR...	00	
svchost.exe	6576	正在运行	SYSTEM	00	
svchost.exe	6964	正在运行	SYSTEM	00	
RuntimeBroker.exe	6968	正在运行	Alex	00	
chrome.exe	6976	正在运行	Alex	00	
DDVDataCollector...	7364	正在运行	SYSTEM	00	
ServiceShell.exe	7488	正在运行	SYSTEM	00	
svchost.exe	7540	正在运行	Alex	00	
jhi_service.exe	7556	正在运行	SYSTEM	00	
svchost.exe	7708	正在运行	LOCAL SE...	00	
IAStorDataMgrSvc...	7868	正在运行	SYSTEM	00	
explorer.exe	7920	正在运行	Alex	01	
svchost.exe	7940	正在运行	SYSTEM	00	
svchost.exe	7980	正在运行	LOCAL SE...	00	
DDVCollectorSvcA...	8140	正在运行	SYSTEM	00	
svchost.exe	8264	正在运行	LOCAL SE...	00	
ApplicationFrameH...	8280	正在运行	Alex	00	
svchost.exe	8340	正在运行	Alex	00	
svchost.exe	8344	正在运行	SYSTEM	00	
srport.exe	8660	正在运行	SYSTEM	00	
svchost.exe	8680	正在运行	SYSTEM	00	



3-实际案例与插件体系

■ 对Python的支持

安世盾个人防火墙

程序规则 端口规则 插件系统

启用	名称	作者	详细描述
<input type="checkbox"/>	logManager	Simpower	日志记录插件，同时提供全日志查询图形界面
<input checked="" type="checkbox"/>	geolocation	Simpower	在线获取地理位置,用的人太多会Ddos封IP，造成查询失效，需要时启用，否则禁用
<input checked="" type="checkbox"/>	pythonEngin	Simpower	支持用log.py(Python)脚本来获取日志并进行处理。
<input type="checkbox"/>	PluginTemp	Simpower	插件模板生成（C++语法）
<input checked="" type="checkbox"/>	UserCounter	Simpower	用户体验计划，统计本软件功能使用频率，启用本插件可以帮助我们做好产品！

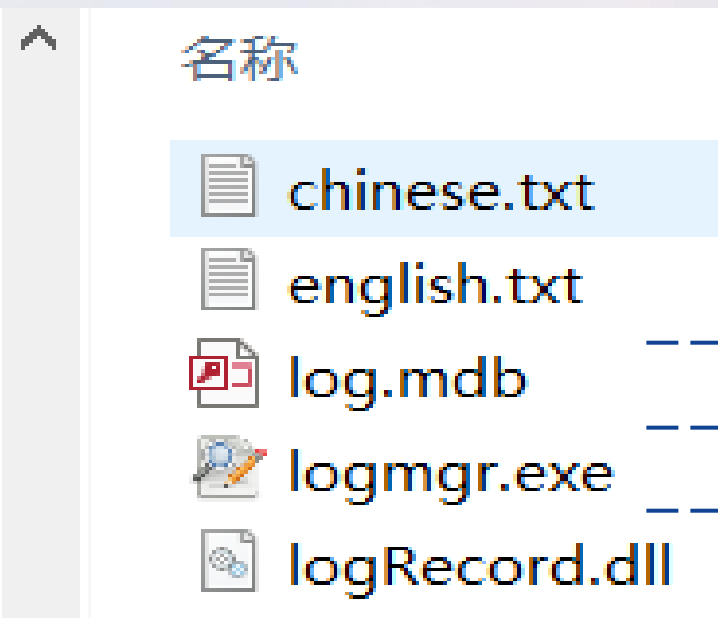
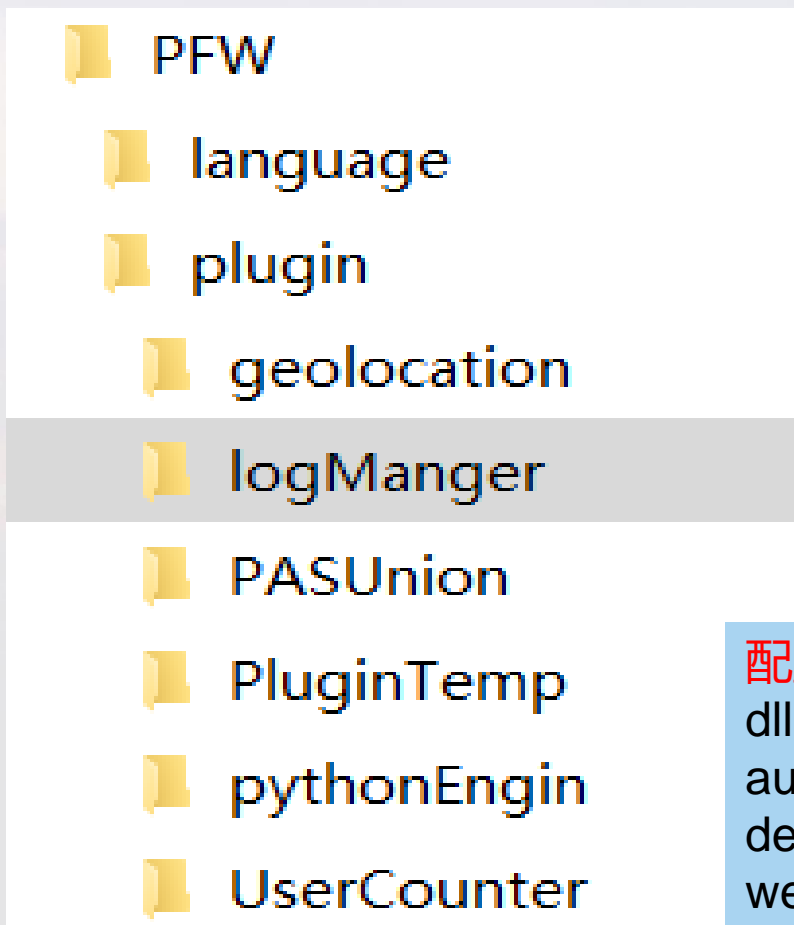
log.py - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
logstr=pfw.value
logs=json.loads(logstr)
if (logs['dip']=='127.0.0.1'):
    with open('log.txt','a') as wf:
        wf.write(logstr+"\n")
```

3-实际案例与插件体系

■ 插件的目录结构



配置文件

插件所需的其他文件

图形界面

插件主程序

```
配置文件: chinese.txt  
dll=logRecord.dll  
author=Simpower  
description=日志记录插件, 同时提供全日志查询图形界面  
weight=130 权重越大优先级越高  
gui=logmgr.exe
```


3-实际案例与插件体系

■ 插件在界面上的显示情况

配置文件: chinese.txt

```

dll=logRecord.dll
author=Simpower
description=日志记录插件, 同时提供全日志查询图形界面
weight=130
gui=logmgr.exe
    
```

IP	源端口	目的IP	目的端口	方向	进程ID
2.168.237.255	138	192.168.237.1	138	1	4
2.168.31.106	138	192.168.31.255	138	0	4
2.168.31.255	138	192.168.31.106	138	1	4
2.168.31.106	58696	202.106.196.115	53	0	2652
2.168.31.106	58731	202.106.196.115	53	0	2652
2.168.31.106	65512	202.106.196.115	53	0	2652
2.168.31.106	51637	61.182.131.251	443	0	7664
7.0.0.1	56248	239.255.255.250	1900	0	6276

■ 三个开放接口，给开发者，用户可以按需扩展

- #define DLL_EXPORT __declspec(dllexport)
- void DLL_EXPORT __stdcall init(int tid); //初始化，启用插件时调用，主线程执行
- void DLL_EXPORT __stdcall uninit(int tid); //反初始化，取消插件时调用，主线程执行
- void DLL_EXPORT __stdcall recvLog(int tid, const LPCSTR log); //接收网络日志，独立线程



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

04

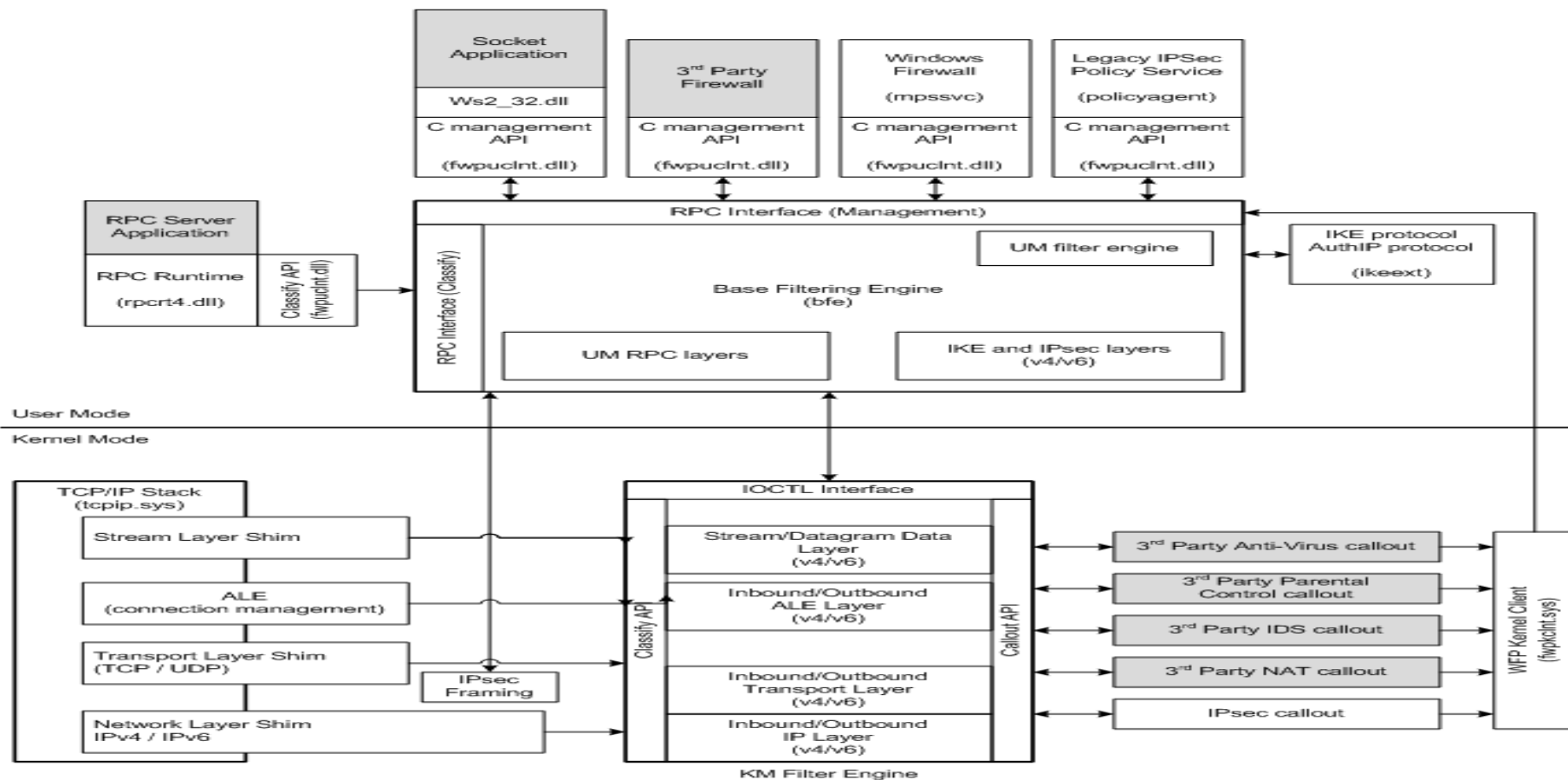
由现有系统架构带来的展望

Wfp,反-反沙箱, 引导程序维护, 链接与加载, 沙丁鱼系列

4-由现有系统架构带来的展望

■ WFP简介

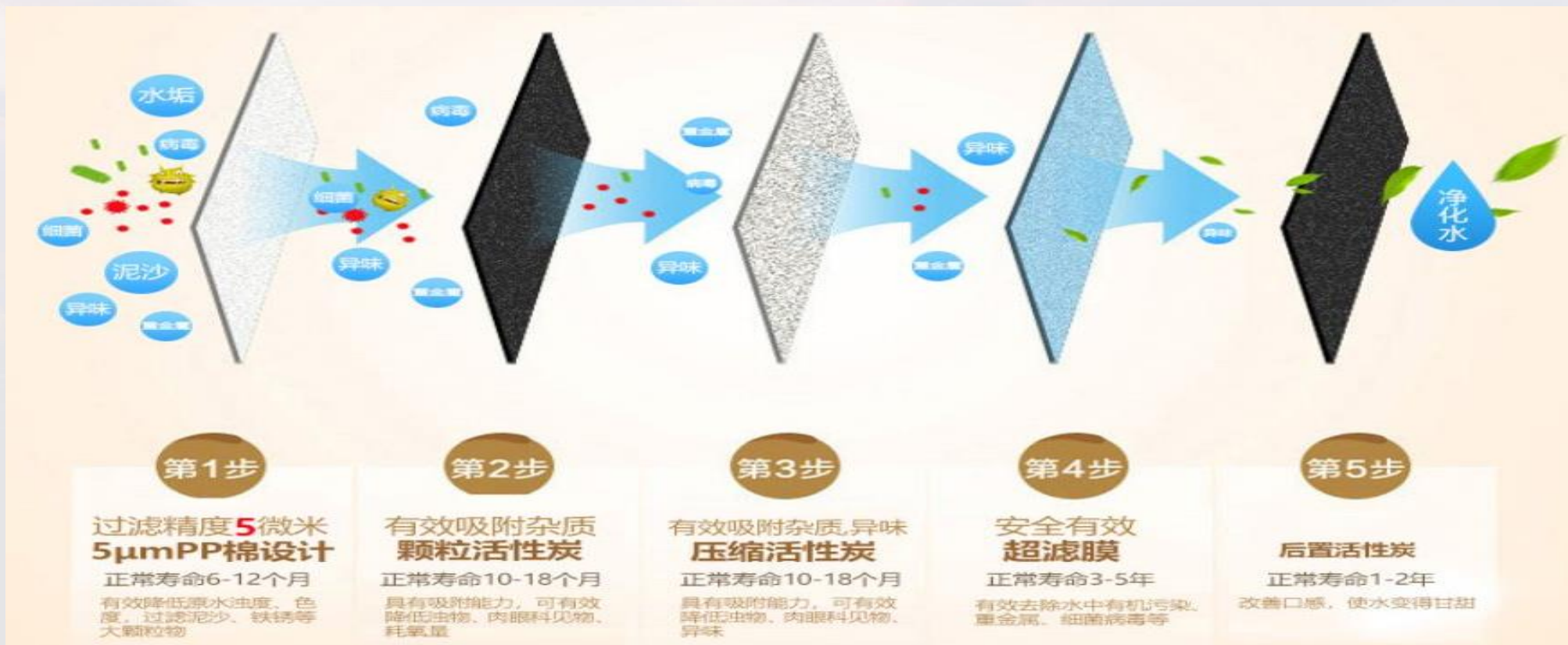
Windows Filtering Platform Architecture Overview



复杂度增加，往往带来更大攻击面

4-由现有系统架构带来的展望

- 过滤驱动的核心，shims（垫片）和 Callout（呼出接口，我觉得用注册回调函数更贴切）



4-由现有系统架构带来的展望

- 于是取其精华，统一接口，打造跨平台的内核级安全框架

好处：

- 1.摆脱现有框架(恶意代码也能用)，我们要绕到更底层，实现更深度的检测。
- 2.一套程序直接用在windows/linux/Android/鸿蒙，跨平台，低维护成本。
- 3.加固操作系统内核，贯穿引导到结束整个生命周期，对抗一些APT，rootkit，如暗云3之类的恶意代码。
- 4.关于我们操作系统缺芯少魂的问题，通过核心组件的实现，形成若干突破点之一。

4-由现有系统架构带来的展望

■ 面临的问题。

内核保护机制：

Patch guard, hyper guard等

改内核蓝屏

4-由现有系统架构带来的展望

■ 解决方法:

- ◆ 引导系统介入，一开始就取得CPU的全部资源，调优配置，可在ring -1进行监控，同时能够反-反沙箱，反-反取证。

打造引导程序链接器：vc->coff->bootloader，不同FS调整偏移

植入引导加载器：载入自定义FS，自定UEFI安全模块等

4-由现有系统架构带来的展望

■ 思考：

一些底层的東西也少有人做，比如编译器链接器，当今商用IDE所生成的可执行文件不断膨胀，一旦出问题将影响成千上万的软件。

我们的链接器将vc单独编译的多个obj链接出的文件会比自带链接出的小很多，需要进一步研究它多出来的是什么。

4-由现有系统架构带来的展望

- 沙丁鱼系列-研究过程中产生的工具 STDN.TECH下载



除了防火墙之外，一系列小工具，简单介绍

- ◆ ActionScope(取可执行文件的行为)
- ◆ certiScope(提取可执行文件中的资源证书等)
- ◆ VirtualMatrix(一系列虚拟化工具集)
- ◆ FileRescuer(恢复误删除的文件和目录等)
- ◆ MMWarpIn(直接读写物理内存，从内核投放代码到进程等)

4-由现有系统架构带来的展望

■ 沙丁鱼系列-研究过程中产生的工具 STDN.TECH下载

ActionScope(取可执行文件的行为)

ID	CNNName	Details	LEVEL	returnAddr	ACTION_DESCRIPTION	ApiName	pro
19	创建窗口	{"dwExStyle":"","lpClassName":"0x76c650e4","lpWindowNa	LEVEL_1	0x76c7a216	CREATE_WINDOW	CreateWindowExW	not
20	创建窗口	{"dwExStyle":"907644","lpClassName":"0x76c66560","lpWinc	LEVEL_1	0x76c8303f	CREATE_WINDOW	CreateWindowExW	not
21	获取系统信息(处理器版本、处理器类型等)	{"lpSystemInfo":"","905708"}	LEVEL_1	0x6c94e8dc	HOSTINFO.SYSTEMINFO	GetSystemInfo	not
22	获取系统信息(处理器版本、处理器类型等)	{"lpSystemInfo":"","899216"}	LEVEL_1	0x6c94e81d	HOSTINFO.SYSTEMINFO	GetSystemInfo	not
23	获取当前用户的界面使用的语言	""	LEVEL_0	0x0ff3a942	HOSTINFO.UI_LANGUAGE	GetUserDefaultUILanguage	not
24	获取当前用户的界面使用的语言	""	LEVEL_0	0x76f90fe8	HOSTINFO.UI_LANGUAGE	GetUserDefaultUILanguage	not
25	获取系统信息(处理器版本、处理器类型等)	{"lpSystemInfo":"","1769335772"}	LEVEL_1	0x6958df7b	HOSTINFO.SYSTEMINFO	GetSystemInfo	not
26	获取系统信息(处理器版本、处理器类型等)	{"lpSystemInfo":"","263575852"}	LEVEL_1	0x710519a2	HOSTINFO.SYSTEMINFO	GetSystemInfo	not
27	获取当前用户的界面使用的语言	""	LEVEL_0	0x76f8d3da	HOSTINFO.UI_LANGUAGE	GetUserDefaultUILanguage	not
28	堆喷射	action:heapSpray	LEVEL_5	0x0a808944	EXPLOIT.HEAPSPRAY	exploit	not
29	获取系统版本	{"lpVersionInformation":"","313306696"}	LEVEL_1	0x129b21d0	HOSTINFO.VERSION	GetVersionExW	not
30	获取系统信息(处理器版本、处理器类型等)	{"lpSystemInfo":"","310948980"}	LEVEL_1	0x53add781	HOSTINFO.SYSTEMINFO	GetSystemInfo	not
31	获取系统版本	{"lpVersionInformation":"","310949060"}	LEVEL_1	0x53add7a5	HOSTINFO.VERSION	GetVersionExW	not
32	获取系统信息(处理器版本、处理器类型等)	{"lpSystemInfo":"","310944176"}	LEVEL_1	0x53add781	HOSTINFO.SYSTEMINFO	GetSystemInfo	not
33	获取系统版本	{"lpVersionInformation":"","310944256"}	LEVEL_1	0x53add7a5	HOSTINFO.VERSION	GetVersionExW	not
34	堆喷射	action:heapSpray	LEVEL_5	0x0a80ab64	EXPLOIT.HEAPSPRAY	exploit	not
35	堆喷射	action:heapSpray	LEVEL_5	0x0a80b344	EXPLOIT.HEAPSPRAY	exploit	not
36	堆喷射	action:heapSpray	LEVEL_5	0x0a80b654	EXPLOIT.HEAPSPRAY	exploit	not
37	堆喷射	action:heapSpray	LEVEL_5	0x0a80bf14	EXPLOIT.HEAPSPRAY	exploit	not
38	获取系统版本	{"lpVersionInformation":"","310953224"}	LEVEL_1	0x0b81c9b7	HOSTINFO.VERSION	GetVersionExW	not
39	创建窗口	{"dwExStyle":"","lpClassName":"0x76c650e4","lpWindowNa	LEVEL_1	0x76c7a216	CREATE_WINDOW	CreateWindowExW	not
40	创建窗口	{"dwExStyle":"907644","lpClassName":"0x76c66560","lpWinc	LEVEL_1	0x76c8303f	CREATE_WINDOW	CreateWindowExW	not
41	创建窗口	{"dwExStyle":"","lpClassName":"0x76c650e4","lpWindowNa	LEVEL_1	0x76c7a216	CREATE_WINDOW	CreateWindowExW	not
42	创建窗口	{"dwExStyle":"907644","lpClassName":"0x76c66560","lpWinc	LEVEL_1	0x76c8303f	CREATE_WINDOW	CreateWindowExW	not

4-由现有系统架构带来的展望

■ 沙丁鱼系列-研究过程中产生的工具 STDN.TECH下载



CertiScope-G:\PFW\Oregy FW\NFCR0-x64.sys

文件(F) 视图(V) 帮助(H)

certiScope
(提取可执行文件中的资源证书等)

Offset

```
-----BEGIN CERTIFICATE-----
MIIDnTCCAoWgAwIBAgIIIFThqYHvdcx0wDQYJKoZIhvcNAQEFBQAwWzELMAkGA1UE
BhMCQ04xGTAXBgNVBAoTEFNURE4gUetJIFNlcnZpY2UxY2UxY2UxY2UxY2UxY2Ux
dGRuLnRlY2gxGTAXBgNVBAMTEFNURE4gUetJIFJPT1QgQ0EwIBcNMDAwMTAxMDAw
MDAwWhgPMjEwMDAwMDEwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
VEROIFBLSSTZXJ2aWNlMRyYwFAYDQVQLEw1wa2kuc3Rkbi50ZWNoMRkwFwYDQVQD
ExBTVEROIFBLSST09UIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCA
AQEAUVU4ZvU1voWCbkKhoET9sPYxR4IzzmwFNGCNPfVfmN81LvXqyuSW195n2Srb
o016ILKK9MbG/J5rWwt4fVsHcd1Fa8V/kDI5VcE/Ghz1hQ8On9wNB1Zq6HKhfby1
wMRxgm7DQvArq6XYsI+1Pw0gtI6Ho04eZ0Dm5J6QJ4HR0kSosJman7XpBii9Sqif
ZXJ0aDmEIpYCI5kFV7/tOKZmdKnNCfNKwZp0FjLlr0Kqg51ff5PKKYZaZdMidnHk
A+5ulqVq30Vm52wopaJ2YhfCUyX1WmlLqirU9y+cK5/fcNptism4eOfGwbaFhJTF
BPPcKanz7mR1Izkd7RRqDfkrAwIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB0G
A1UdDgQWBQMcnMlhYHbcnN+ozJdtvP29sZATAfBgNVHSMEGDAwGBQMcnMlhYH
BcnN+ozJdtvP29sZATAOBgNVHQ8BAf8EBAMCAYwDQYJKoZIhvcNAQEFBQADggEB
AIBbLBTRZC25j8KQPzvc7YicjydCurXyY5RhdB8W0euzPhWMqDUGEpskQqEqpGP
EYs65j8i2ikbNASYE1eA/445hPyjxAefjVBunc0TMAHAt0BwvtLSy9UMUSeFX6QI
4KKcOuCoc8u3DEHawVx3bV1FalA5Ija4vfLKO1EoT5T0n10x3VtK067sIXvdjg8y
q6clGpLBR3/nCenuVT3Yxlup7wHR/Rcb4XqvyhG1COaSS01zA66qbaZF1UT0tJfd
7Jc48g7pBjrpXx79cqxs4023BRPQBGu+ZQx/Yhlc8KAsIVS26e0BWy4C+CBVeQEY
C3fLiwMngb/lF6CXqUWIXMA=
-----END CERTIFICATE-----
```

InstallCertificate To Root

Export

4-由现有系统架构带来的展望

沙丁鱼系列-研究过程中产生的工具 STDN.TECH 下载

加密后的虚拟盘必须输入密码才能看内容到或安装到“我的电脑”中
 否则就是一个未知文件，机密资料不怕优盘或电脑丢失，电脑也可以随
 更拿去维修。

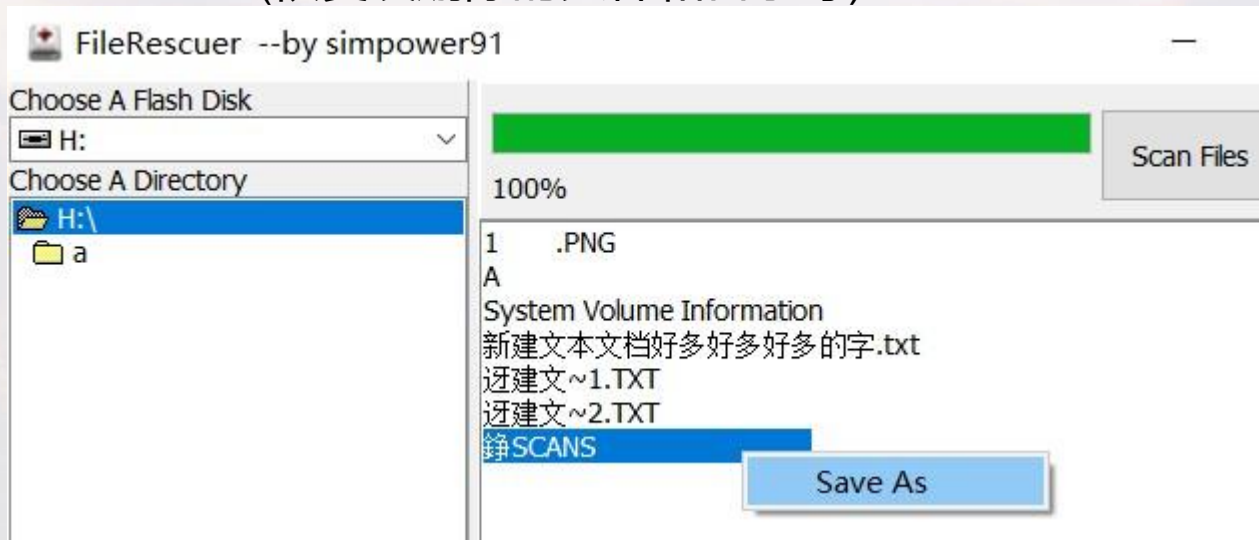
VirtualMatrix(一系列虚拟化工具集)

分区之间有一些空隙，文件系统不可见，
 可以藏rootkit进去。这个可以用于取证。

4-由现有系统架构带来的展望

- 沙丁鱼系列-研究过程中产生的工具 STDN.TECH下载

FileRescuer(恢复误删除的文件和目录等)





网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

谢谢大家



安天冬训营 wtc.antiy.cn