网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

打造一个轻量级分析工具

安天官方发布Action Scope（行为显微镜）

安天研究院

威胁框架：认知与实践

寒夜遠征

自我介绍

- 2017 安全运营中心
  - ——从事逆向工程，分析恶意代码
- 2018 网研
  - ——做追影内核开发
- 2019 研究院
  - ——研究和设计分析内核、开发Action Scope产品

问题发现与纠正

1、产品能力提升需要两个部门的协作 -- 现实，平行线，各干各，很少交流

逆向

恶意代码分析 → 报告 → 客户

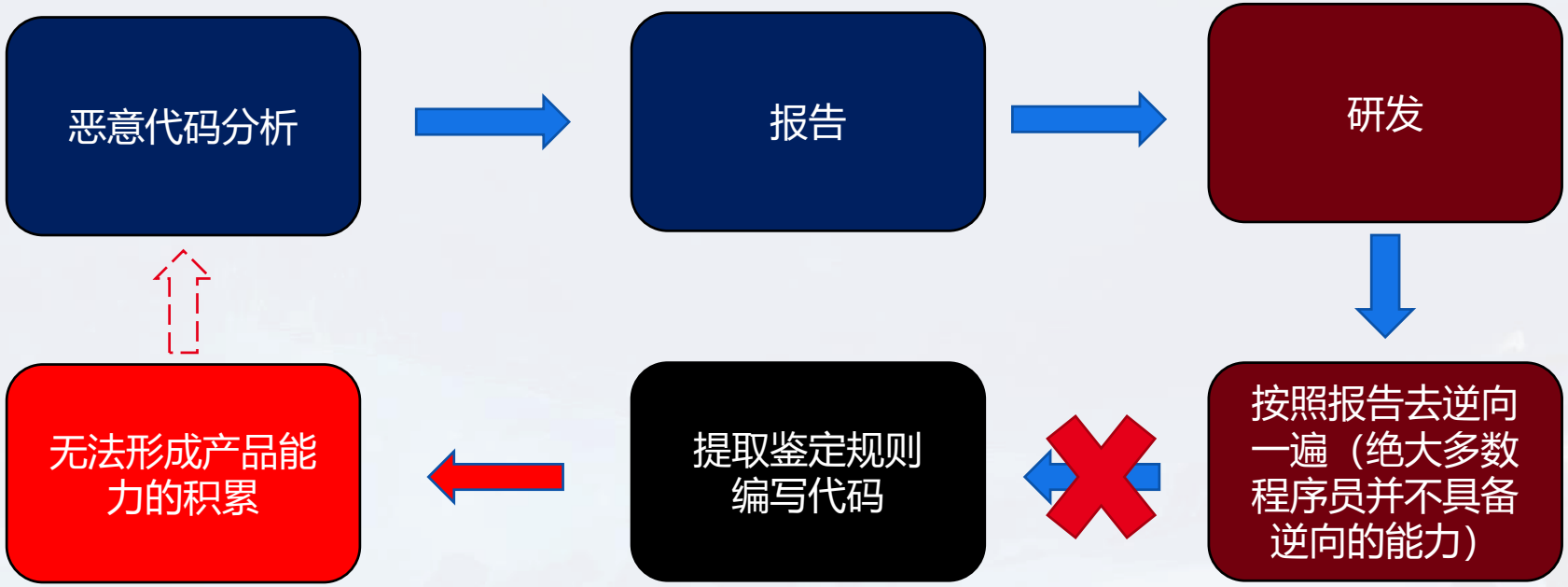
研发

写程序 → 软件产品 → 客户

问题发现与纠正

2、协作的痛点，本该形成的闭环却总是断裂 -（研发篇）

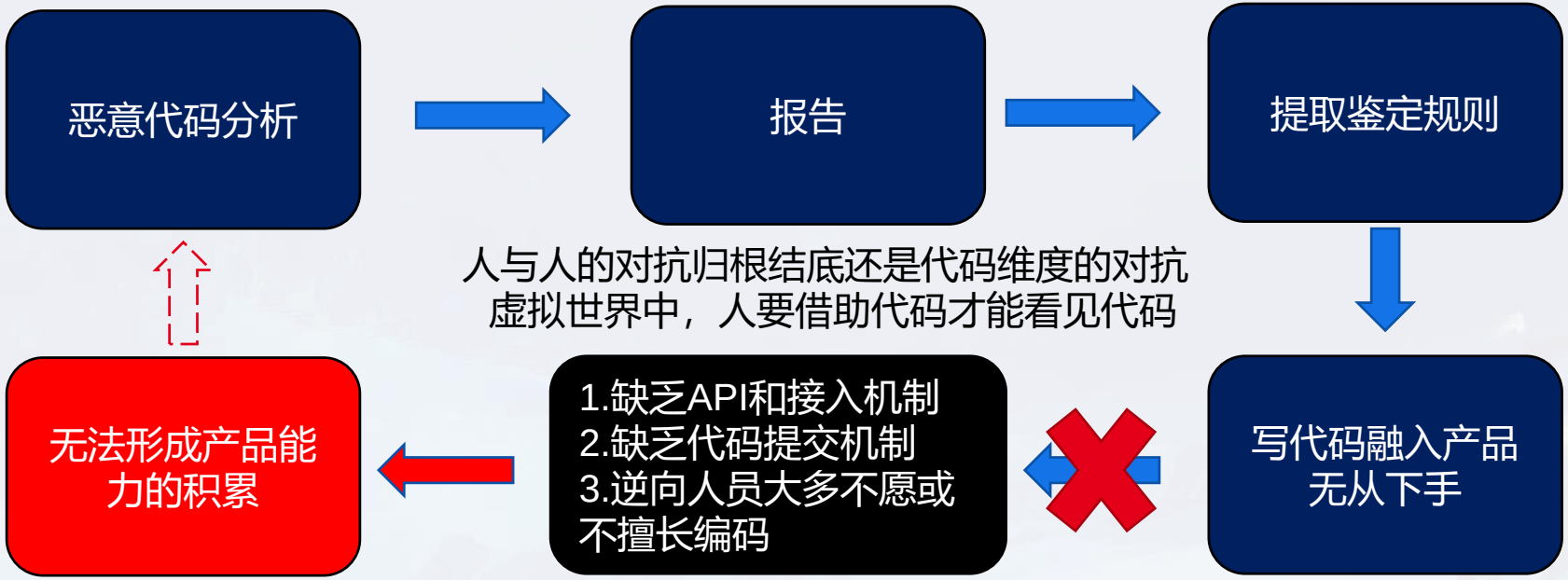
研发可以从逆向获得分析报告，却无法形成产品能力的积累，进而导致没有好的工具支援



问题发现与纠正

3、协作的痛点 -（逆向篇）

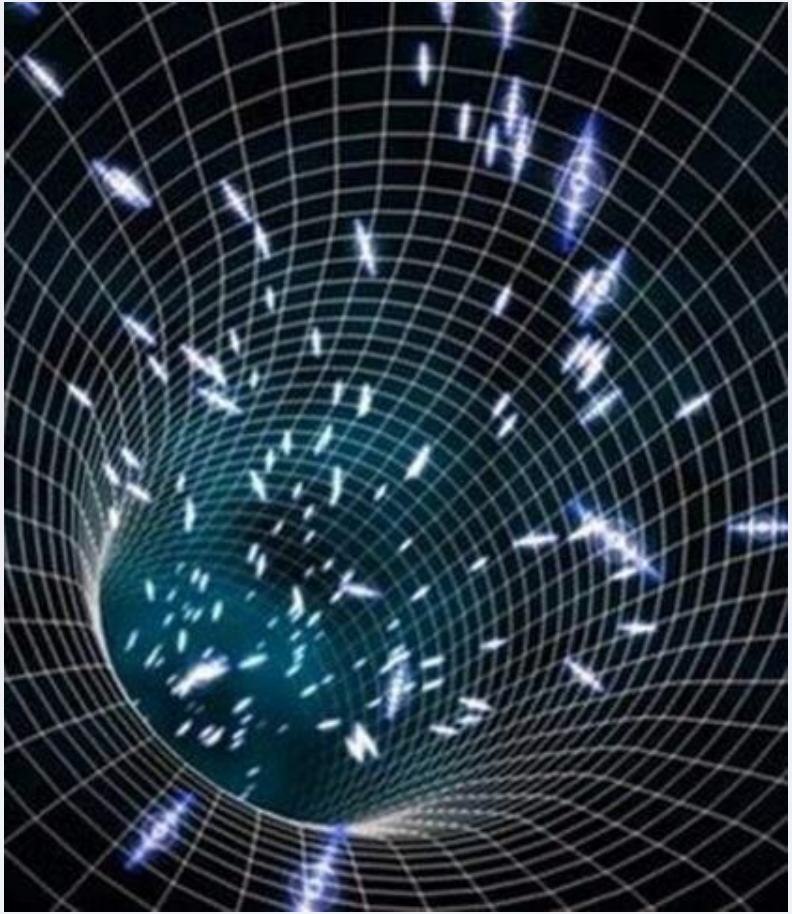
逆向需要更高效的分析工具，现实是！！！原因是。。。



人与人的对抗归根结底还是代码维度的对抗
虚拟世界中，人要借助代码才能看见代码

后面会讲解，Action Scope如何在**代码维度**解决以上问题，进而推动双方形成良好的协作闭环

Action Scope（行为显微镜）诞生



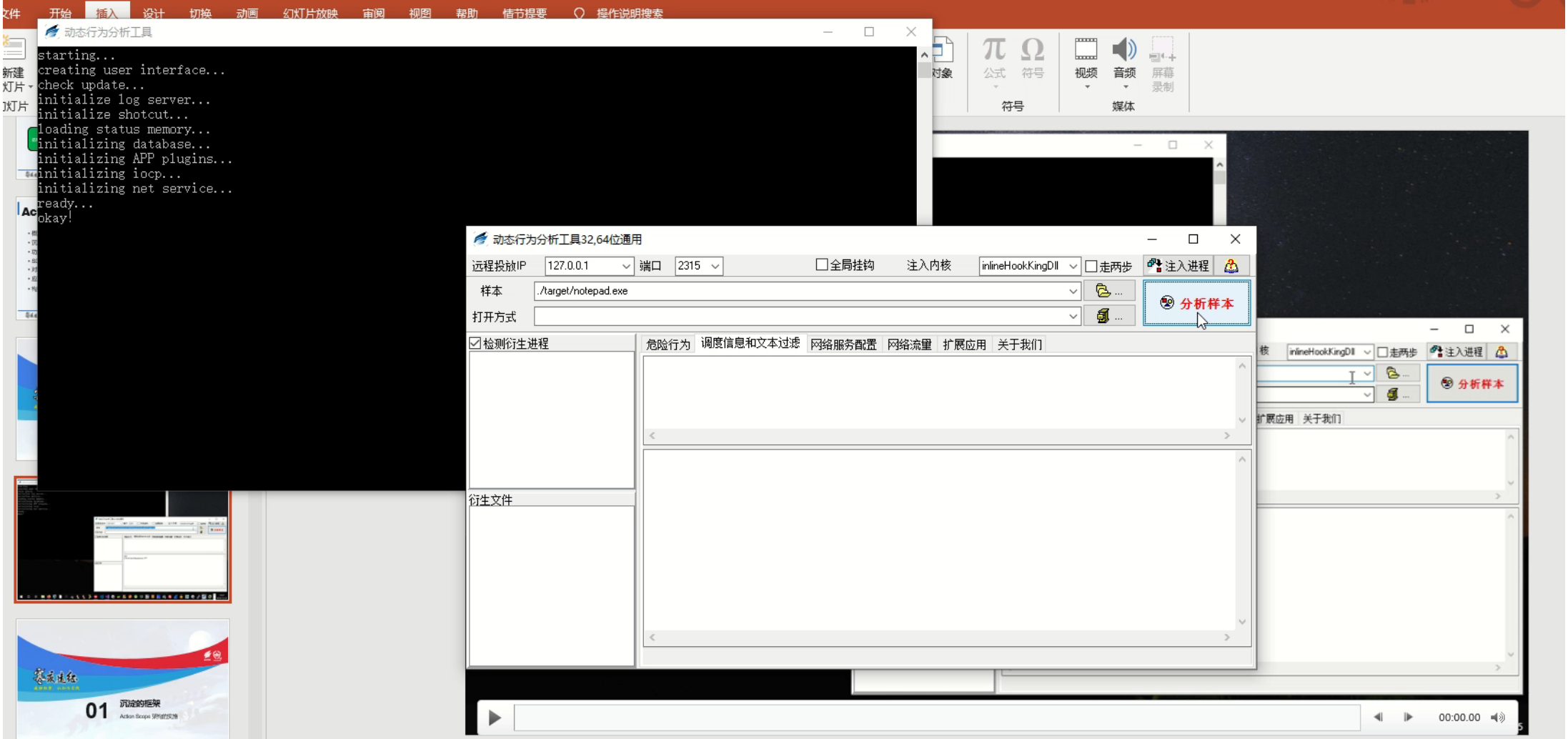
- 产品演示
- 功能及用法
- 问答环节

寒夜遠征

威胁框架：认知与实践

00 Action Scope 产品演示

- 揭示未知攻击载荷、获取每一步执行动作、模块调用、漏洞利用等…
- 轻量级，便携，易扩展



他会把样本的所有行为给抓出来，样本的一举一动全都记录下来，一边记录一遍鉴定，根据行为规则进行分级，看有没有危险的行为。

寒夜遠征

威胁框架：认知与实践

01 Action Scope功能、用法

- 一一讲解各个组件
- 不同于vt, cuckoo的黑箱&可衔接研发和逆向

构成ActionScope的组件列表（未列全...）

- 日志组件
- 钩子引擎
- API记录器**插件**
- 漏洞检测**插件**
- 反沙箱对抗**插件**
- WMI对抗**插件**
- 鉴定器
- 调度器
- 崩溃报告(dump)转储系统
- 自动升级组件
- 内核态引擎
- Python**自定义鉴定器**SDK

ActionScope 行为列表

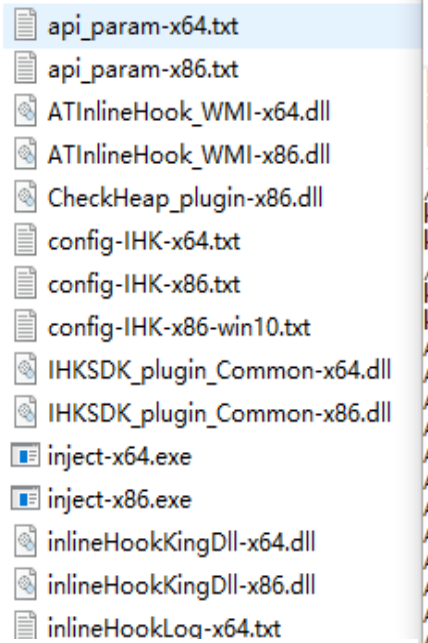
ID	CNName	Details	LEVEL	returnAddr	ACTION_DESCRIPTION	ApiName	pro
19	创建窗口	{"dwExStyle":"0","lpClassName":"0x76c650e4","lpWindowNa	LEVEL_1	0x76c7a216	CREATE_WINDOW	CreateWindowExW	not
20	创建窗口	{"dwExStyle":"907644","lpClassName":"0x76c66560","lpWinc	LEVEL_1	0x76c8303f	CREATE_WINDOW	CreateWindowExW	not
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":"0","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":"0","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

危险行为的追溯，shellCode的获取

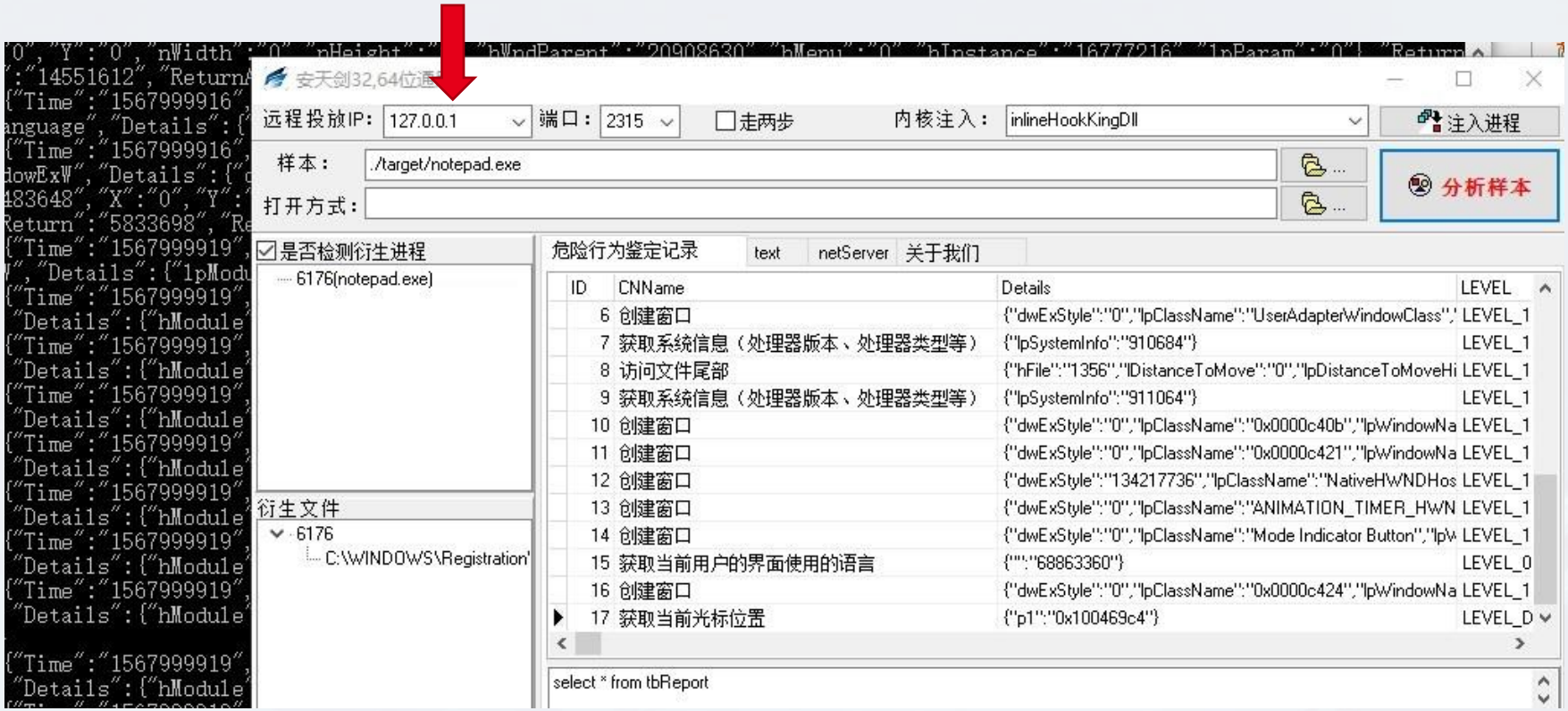
ID	CNName	Details	LEVEL	returnAddr	moduleName	ACTION_DESCRIPTION	Api
3	创建窗口	{"dwExStyle":"0","lpClassName":"CicMarshalWndClass","lpW	LEVEL_1	0x75d8a11a	MSCTF.dll	CREATE_WINDOW	Cre
4	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"913512"}	LEVEL_1	0x6fca6d85	CoreMessaging.dll	HOSTINFO.SYSTEMINFO	Ge
5	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"913504"}	LEVEL_1	0x6fc9f136	CoreMessaging.dll	HOSTINFO.SYSTEMINFO	Ge
6	创建窗口	{"dwExStyle":"0","lpClassName":"UserAdapterWindowClass","'	LEVEL_1	0x6fc9e822	CoreMessaging.dll	CREATE_WINDOW	Cre
7	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"910132"}	LEVEL_1	0x7555e99d	clbcatq.dll	HOSTINFO.SYSTEMINFO	Ge
8	访问文件尾部	{"hFile":"1360","lDistanceToMove":"0","lpDistanceToMoveHi	LEVEL_1	0x7555f210	clbcatq.dll	FILE_POS.TAIL	Sel
9	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"910512"}	LEVEL_1	0x7555be4b	clbcatq.dll	HOSTINFO.SYSTEMINFO	Ge
10	创建窗口	{"dwExStyle":"0","lpClassName":"0x0000c183","lpWindowNa	LEVEL_1	0x0f8a1785	msctfuimanager.dll	CREATE_WINDOW	Cre
11	创建窗口	{"dwExStyle":"0","lpClassName":"0x0000c359","lpWindowNa	LEVEL_1	0x0f8a1785	msctfuimanager.dll	CREATE_WINDOW	Cre
12	创建窗口	{"dwExStyle":"134217736","lpClassName":"NativeHWNDHos	LEVEL_1	0x0fb8b251	DUI70.dll	CREATE_WINDOW	Cre
13	创建窗口	{"dwExStyle":"0","lpClassName":"ANIMATION_TIMER_HWN	LEVEL_1	0x11c23671	UIAnimation.dll	CREATE_WINDOW	Cre
14	创建窗口	{"dwExStyle":"0","lpClassName":"Mode Indicator Button","lpV	LEVEL_1	0x0fb8b251	DUI70.dll	CREATE_WINDOW	Cre
15	获取当前用户的界面使用的语言		LEVEL_0	0x0fb8978a	DUI70.dll	HOSTINFO.UI_LANGUAGE	Ge
16	创建窗口	{"dwExStyle":"0","lpClassName":"0x0000c444","lpWindowNa	LEVEL_1	0x0f8a1785	msctfuimanager.dll	CREATE_WINDOW	Cre
17	获取当前光标位置	{"p1":"230123972"}	LEVEL_DISCAF	0x0db6110d	RTXOLAss.dll	GETCURSORPOS	Ge
18	获取当前用户的界面使用的语言		LEVEL_0	0x76874d82	comdlg32.dll	HOSTINFO.UI_LANGUAGE	Ge
19	创建窗口	{"dwExStyle":"0","lpClassName":"Scrollbar","lpWindowName'	LEVEL_1	0x7687a216	comdlg32.dll	CREATE_WINDOW	Cre
20	创建窗口	{"dwExStyle":"8","lpClassName":"tooltips_class32","lpWindow	LEVEL_1	0x7688303f	comdlg32.dll	CREATE_WINDOW	Cre
21	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"905932"}	LEVEL_1	0x6d04e8dc	WindowsCodecs.dll	HOSTINFO.SYSTEMINFO	Ge
22	删除文件	{"lpFileName":"C:\Users\AT\AppData\Local\Microsoft\Windo	LEVEL_0	0x6cfad6fe	thumbcache.dll	DELETE_FILE	De
23	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"899440"}	LEVEL_1	0x6d04e81d	WindowsCodecs.dll	HOSTINFO.SYSTEMINFO	Ge
24	获取当前用户的界面使用的语言		LEVEL_0	0x0ee2a942	StructuredQuery.dll	HOSTINFO.UI_LANGUAGE	Ge
25	获取当前用户的界面使用的语言		LEVEL_0	0x764671a7	windows.storage.dll	HOSTINFO.UI_LANGUAGE	Ge
26	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"901312"}	LEVEL_1	0x6cfc2ba0	thumbcache.dll	HOSTINFO.SYSTEMINFO	Ge

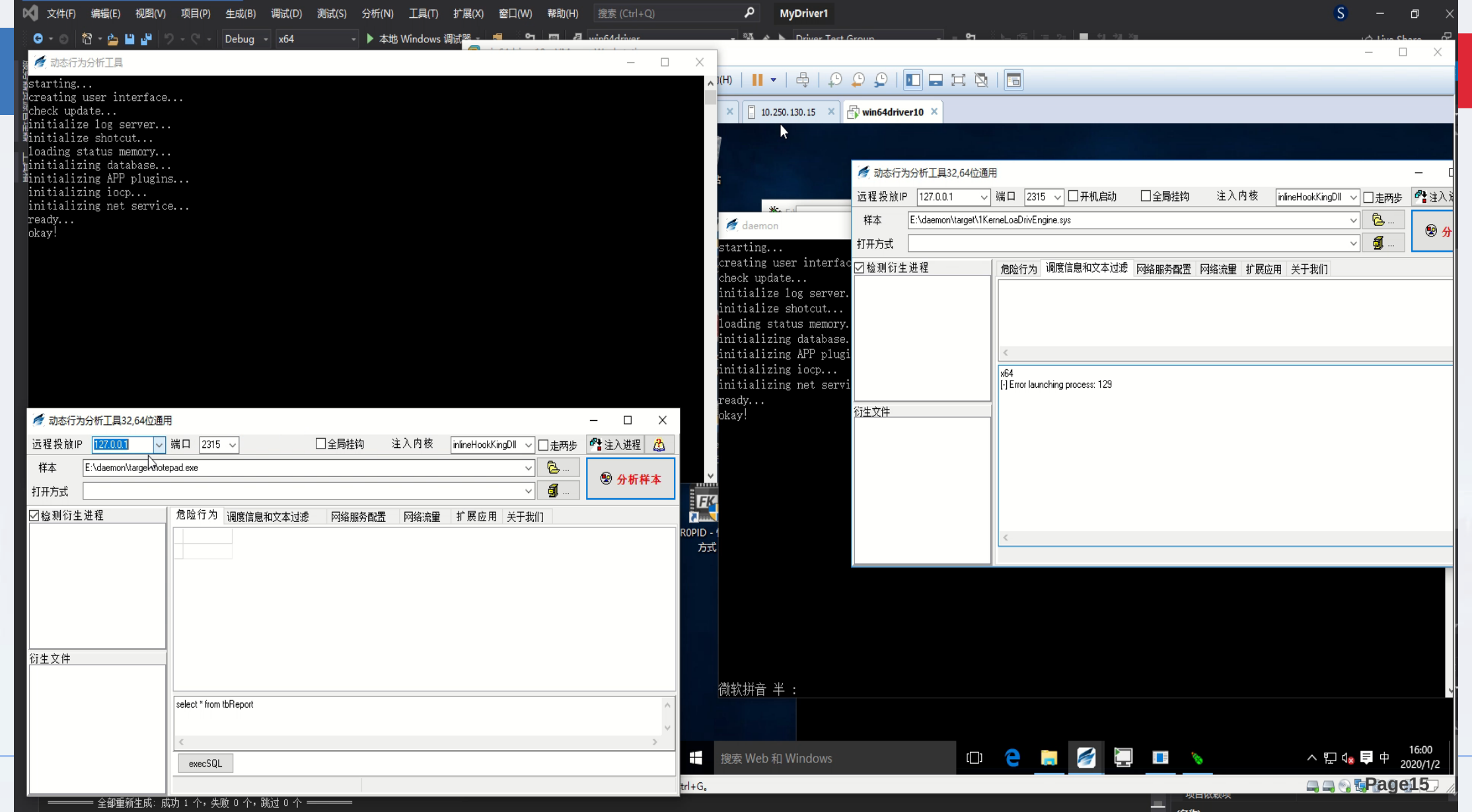
插件系统与漏洞利用检测

- 通用API记录的插件
- 检测未知漏洞利用的插件
- HeapSpray
- ROP
- shellCode



远程分析，衍生进程和文件




文件(F) 编辑(E) 视图(V) 项目(P) 生成(B) 调试(D) 测试(S) 分析(N) 工具(T) 扩展(X) 窗口(W) 帮助(H)
搜索 (Ctrl+Q)
MyDriver1
Debug
x64
本地 Windows 调试器
动态行为分析工具
starting...
creating user interface...
check update...
initialize log server...
initialize shotcut...
loading status memory...
initializing database...
initializing APP plugins...
initializing iocp...
initializing net service...
ready...
okay!
动态行为分析工具32,64位通用
远程投放IP 127.0.0.1
端口 2315
全局挂钩
注入内核 inlineHookKingDll
走两步
注入进程
样本 E:\daemon\target\notepad.exe
打开方式
分析样本
检测衍生进程
衍生文件
危险行为
调度信息和文本过滤
网络服务配置
网络流量
扩展应用
关于我们
select * from tbReport
execSQL
全部重新生成: 成功 1 个, 失败 0 个, 跳过 0 个
10.250.130.15
win64driver10
daemon
starting...
creating user interfac
check update...
initialize log server.
initialize shotcut...
loading status memory.
initializing database.
initializing APP plugi
initializing iocp...
initializing net servi
ready...
okay!
动态行为分析工具32,64位通用
远程投放IP 127.0.0.1
端口 2315
开机启动
全局挂钩
注入内核 inlineHookKingDll
走两步
样本 E:\daemon\target\1KernelLoaDrivEngine.sys
打开方式
检测衍生进程
衍生文件
危险行为
调度信息和文本过滤
网络服务配置
网络流量
扩展应用
关于我们
x64
[-] Error launching process: 129
微软拼音 半 ：
搜索 Web 和 Windows
16:00
2020/1/2

Powershell样本分析，以及wmi反虚拟机对抗

E:\daemon\daemon.exe

安天剑32,64位通用

远程投放IP: 127.0.0.1 端口: 2315 开机启动 内核注入: inlineHookKingDll 走两步

样本: E:\daemon\target\wmi_query3.ps1

打开方式: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

是否检测衍生进程

9724()

衍生文件

9724

C:\WINDOWS\Registral

C:\Users\AT\AppData\F

%AppData%\Microsoft\V

C:\Users\AT\AppData\L

C:\Users\AT\AppData\L

C:\WINDOWS\%AppDa

C:\WINDOWS\%AppDa

C:\

危险行为鉴定记录 调度信息与文本过滤 网络服务配置 关于我们

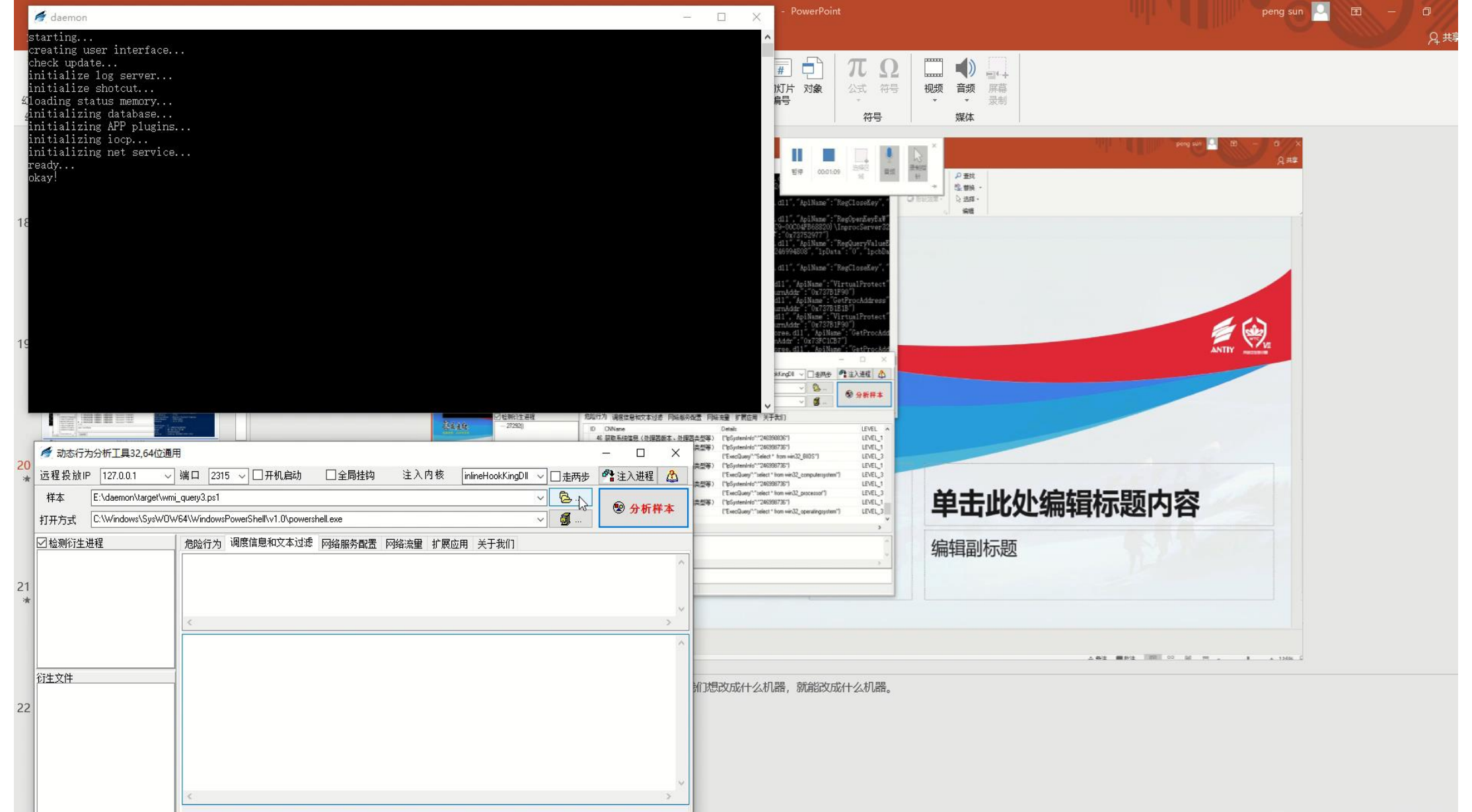
ID	CNName	Details
49	WMI SQL语句查询	{"ExecQuery":"select * from win32_computersystem"}
50	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"237887620"}
51	WMI SQL语句查询	{"ExecQuery":"select * from win32_processor"}
52	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"237887620"}
53	WMI SQL语句查询	{"ExecQuery":"select * from win32_operatingsystem"}
54	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"237887620"}
55	WMI SQL语句查询	{"ExecQuery":"select * from win32_diskdrive"}
56	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"237885472"}
57	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"237885296"}
58	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"237881588"}
59	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"237881448"}
60	获取系统信息（处理器版本、处理器类型等）	{"lpSystemInfo":"173994876"}

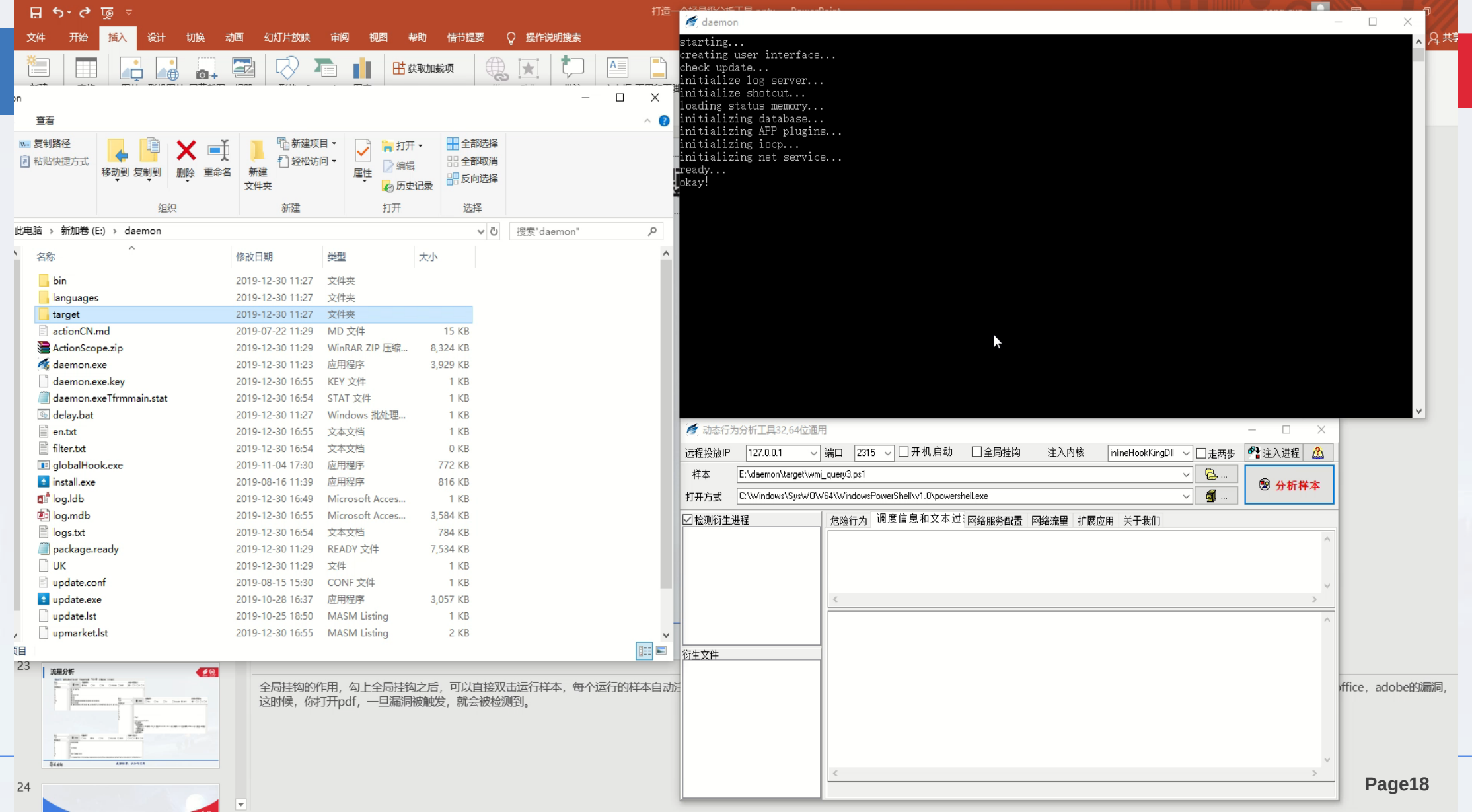
select * from tbReport

execSQL

Windows PowerShell

```
SMBIOSBIOSVersion : P85 Ver. 01.04
Manufacturer      : HP
Name              : Core(TM) i7-9500 CPU @ 3.40GHz
SerialNumber      : 9CE8013DZJ
Version           : HPQOEM - 0

Domain              : WORKGROUP
Manufacturer        : HP
Model               : HP 980 Pro G3 MT
Name                : Core(TM) i7-9500 CPU @ 3.40GHz
PrimaryOwnerName    : Hewlett-Packard Company
TotalPhysicalMemory : 9959952128

Caption           : Intel64 Family 6 Model 142 Stepping 9
DeviceID          : CPU0
Manufacturer      : HP
MaxClockSpeed     : 2712
Name              : Core(TM) i7-9500 CPU @ 3.40GHz
SocketDesignation : U3E1

SystemDirectory : C:\WINDOWS\system32
Organization    : Hewlett-Packard Company
BuildNumber     : 17763
RegisteredUser  : Hewlett-Packard Company
SerialNumber    : 9CE8013DZJ
Version         : 10.0.17763

Partitions : 6
DeviceID   : \\.\PHYSICALDRIVE0
Model      : HP 980 Pro G3 MT
Size       : 256052966400
Caption    : SanDisk SD8SN8U-256G-1006
```


daemon
starting...
creating user interface...
check update...
initialize log server...
initialize shotcut...
loading status memory...
initializing database...
initializing APP plugins...
initializing iocp...
initializing net service...
ready...
okay!
动态行为分析工具32,64位通用
远程投放IP
127.0.0.1
端口
2315
开机启动
全局挂钩
注入内核
inlineHookKingDll
走两步
注入进程
样本
E:\daemon\target\wmi_query3.ps1
打开方式
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
分析样本
检测衍生进程
危险行为
调度信息和文本过滤
网络服务配置
网络流量
扩展应用
关于我们
衍生文件
PowerPoint
peng sun
单击此处编辑标题内容
编辑副标题


daemon
starting...
creating user interface...
check update...
initialize log server...
initialize shotcut...
loading status memory...
initializing database...
initializing APP plugins...
initializing iocp...
initializing net service...
ready...
okay!
此电脑 › 新加卷 (E:) › daemon
bin 2019-12-30 11:27 文件夹
languages 2019-12-30 11:27 文件夹
target 2019-12-30 11:27 文件夹
actionCN.md 2019-07-22 11:29 MD 文件 15 KB
ActionScope.zip 2019-12-30 11:29 WinRAR ZIP 压缩... 8,324 KB
daemon.exe 2019-12-30 11:23 应用程序 3,929 KB
daemon.exe.key 2019-12-30 16:55 KEY 文件 1 KB
daemon.exeTfrmmain.stat 2019-12-30 16:54 STAT 文件 1 KB
delay.bat 2019-12-30 11:27 Windows 批处理... 1 KB
en.txt 2019-12-30 16:55 文本文档 1 KB
filter.txt 2019-12-30 16:54 文本文档 0 KB
globalHook.exe 2019-11-04 17:30 应用程序 772 KB
install.exe 2019-08-16 11:39 应用程序 816 KB
log.ldb 2019-12-30 16:49 Microsoft Acces... 1 KB
log.mdb 2019-12-30 16:55 Microsoft Acces... 3,584 KB
logs.txt 2019-12-30 16:54 文本文档 784 KB
package.ready 2019-12-30 11:29 READY 文件 7,534 KB
UK 2019-12-30 11:29 文件 1 KB
update.conf 2019-08-15 15:30 CONF 文件 1 KB
update.exe 2019-10-28 16:37 应用程序 3,057 KB
update.lst 2019-10-25 18:50 MASM Listing 1 KB
upmarket.lst 2019-12-30 16:55 MASM Listing 2 KB
动态行为分析工具32,64位通用
远程投放IP 127.0.0.1 端口 2315 开机启动 全局挂钩 注入内核 inlineHookKingDll 走两步 注入进程
样本 E:\daemon\target\wmi_query3.ps1
打开方式 C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
分析样本
检测衍生进程
危险行为 调度信息和文本过 网络服务配置 网络流量 扩展应用 关于我们
衍生文件
全局挂钩的作用，勾上全局挂钩之后，可以直接双击运行样本，每个运行的样本自动
这时候，你打开pdf，一旦漏洞被触发，就会被检测到。

网络服务配置

动态行为分析工具32,64位通用
远程投放IP
127.0.0.1
端口
2315
开机启动
全局挂钩
注入内核
inlineHookKingDll
走两步
注入进程
样本
./target/notepad.exe
打开方式
分析样本
检测衍生进程
14656()
危险行为
调度信息和文本过滤
网络服务配置
网络流量
扩展应用
关于我们
请允许下列端口通过防火墙
日志服务端口
2313
start
stop
调度端口
2314
start
stop
远程服务端口
2315
start
stop
强制代理端口
2316
start
stop
协议
TCP
UDP
衍生文件
14656
C:\WINDOWS\SYSTEM
C:\Windows\Fonts\static
C:\WINDOWS\Globaliza
C:\WINDOWS\Registral
C:\Users\AT\AppData\L
C:\WINDOWS\system32
C:\Users\AT\AppData\L
C:\Users\AT\AppData\L

是否检测衍生进程
10200()
危险行为鉴定记录
ID
CNName
8 访问文件尾部
9 获取系统信息（处理
10 创建窗口
11 创建窗口
12 创建窗口
13 创建窗口
14 创建窗口
15 获取当前用户的界面
16 创建窗口
衍生文件
10200
C:\WINDOWS\SYSTEM32
C:\Windows\Fonts\staticca
C:\WINDOW
C:\WINDOW
打开文件所在目录(Z)

流量分析

危险行为 | 调度信息和文本过滤 | 网络服务配置 | 网络流量 | 扩展应用 | 关于我们

协议: TCP

字段格式: 4, 1, 1, 4, 2, 2, 14, 4

clean

流量解析: Hex / Int / Str / Unicode / Utf-8

数据长度显示: 1 / 2 / 4 / 8

```
FE EF 9F F9
00
01
00 00 07 01
00 00
00 00
00 00 6B 6B 00 00 00 00 00 00 00 00 00 00
00 00 00 00
0C 00 00 00 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30
```

协议: TCP

字段格式: 4, 1, 1, 4, 2, 2, 14, 4

clean

流量解析: Hex / Int / Str / Unicode / Utf-8

数据长度显示: 1 / 2 / 4 / 8

```
<?xml

<?xml version="1.0"?>
<监控服务>
  <监控信息>
    <控制命令 ZD编号=ZD_ID 设备IP=10.250.130.13 命令编号=123 设备编号=IPMeta 命令描述=申请参
  </控制命令>
  </监控信息>
</监控服务>
```

协议: TCP

字段格式: 4, 1, 1, 4, 2, 2, 14, 4

clean

流量解析: Hex / Int / Str / Unicode / Utf-8

数据长度显示: 1 / 2 / 4 / 8

```
4188008446
0
1
17235968
0
0
1802174464 0 0 0
0
12 1836597052 1702240364 1869181810 824327534 1059205166 3879471678 2397475227 2375870119 1C
```

更多功能留给大家自己探索。。。

礼品相送

- 行为显微镜（Action Scope）
- 系统深度分析工具（ATool）
  - 辅助专业人员开展手动处置工作，具有已知威胁有效检测，未知威胁及时发现，顽固感染一键处置等功能特点。
- 精细化扫描工具（ScanTool）
  - 便携绿色版自动化检测工具，能够在不破坏主机环境的前提下对主机的完整环境信息进行采集并输出详细的扫描日志与报告，为专业分析人员快速定位威胁及取证工作提供有力支撑。

谢谢大家