HW防守 | Windows应急响应基础

原创 璠淳 Timeline Sec 今天

常见的应急响应事件分类：

web入侵：网页挂马、主页篡改、Webshell

系统入侵：病毒木马、勒索软件、远控后门

网络攻击：DDOS攻击、DNS劫持、ARP欺骗

入侵排查思路

web入侵：对中间价日志进行分析

系统入侵：计划任务，系统爆破痕迹（系统日志），进程进行分析

网络攻击：流量分析

1、 检查系统账号安全

查看服务器是否有弱口令，远程管理端口是否对公网开放

检查方法：查看网络连接对应的进程

```
Netstat -anb | findstr 进程
```

查看日志：

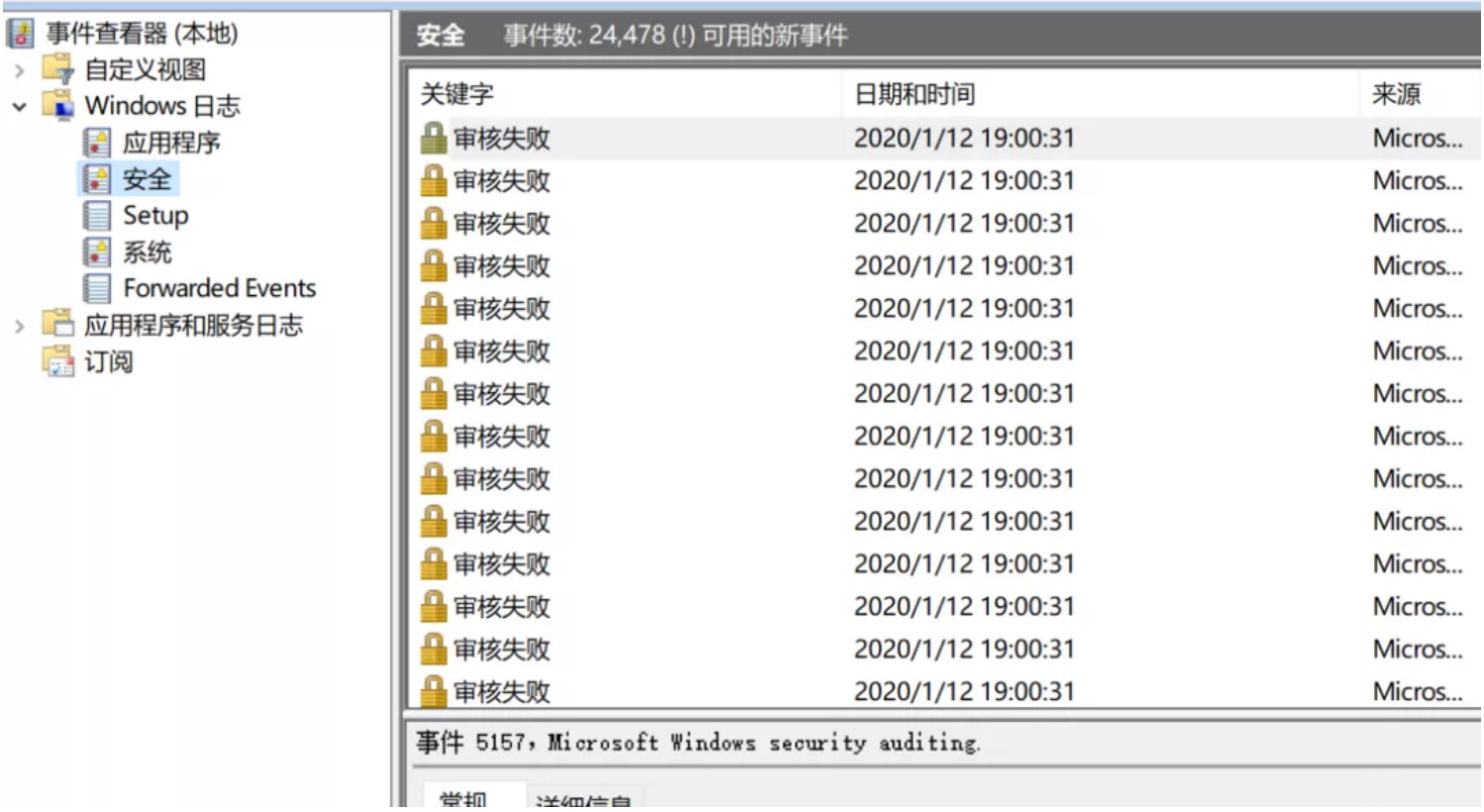
打开控制面板——系统和安全——查看事件日志，就进入了事件查看器

打开左侧事件查看器（本地）——Windows日志——安全

筛查4776事件（远程登陆日志）查看是否有登陆频率过高事件

重要的事件 ID（安全日志，Security.evtx）

- 4624：账户成功登录
- 4648：使用明文凭证尝试登录
- 4778：重新连接到一台 Windows 主机的会话
- 4779：断开到一台 Windows 主机的会话



2、查看服务器是否存在可疑账号、新增账号。

检查方法：打开 cmd 窗口，输入lusrmgr.msc命令，查看是否有新增/可疑的账号，如有管理员群组的（Administrators）里的新增账户，如有，请立即禁用或删除掉。

3、查看服务器是否存在隐藏账号、克隆账号。

检查方法：

a、打开注册表 ，查看管理员对应键值。

b、使用D盾_web查杀工具，集成了对克隆账号检测的功能

c.windows账号信息，隐藏账号

【开始】→【运行】→【compmgmt.msc】→【本地用户和组】→【用户】（用户名以$结尾的为隐藏用户，如：admin$）

4、结合日志，查看管理员登录时间、用户名是否存在异常。

检查方法：

a、Win+R打开运行，输入“eventvwr.msc”，回车运行，打开“事件查看器”。

b、导出Windows日志--安全，利用Log Parser进行分析。

LogParser.exe -i:EVT -o:DATAGRID "SELECT TimeGenerated as LoginTime,EXTRACT_TOKEN(Strings,5,'|') as username,EXTRACT_TOKEN(Strings, 8, '|') as LogonType,EXTRACT_TOKEN(Strings, 17, '|') AS ProcessName,EXTRACT_TOKEN(Strings, 18, '|') AS SourceIP FROM 日志位置 where EventID=4624"

5、检查异常端口、进程

检查端口连接情况，是否有远程连接、可疑连接。

检查方法：

a、netstat -ano 查看目前的网络连接，定位可疑的ESTABLISHED

b、根据netstat 定位出的pid，再通过tasklist命令进行进程定位

```
tasklist | findstr “PID”
```

6、进程

检查方法：

a、开始--运行--输入msinfo32，依次点击“软件环境→正在运行任务”就可以查看到进程的详细信息，比如进程路径、进程ID、文件创建日期、启动时间等。

b、打开D盾_web查杀工具，进程查看，关注没有签名信息的进程。

c、通过微软官方提供的 Process Explorer 等工具进行排查 。

d、查看可疑的进程及其子进程。可以通过观察以下内容：

没有签名验证信息的进程

没有描述信息的进程

进程的属主

进程的路径是否合法

CPU或内存资源占用长时间过高的进程

7、计划任务

控制面板 — 管理工具 — 任务计划程序

或运行 — taskschd.msc

通过命令查看计划任务schtasks

存放计划任务的文件

- C:\Windows\System32\Tasks\
- C:\Windows\SysWOW64\Tasks\
- C:\Windows\tasks\
- *.job（指文件）

8、查看可疑目录及文件

查看 host ：

type %systemroot%\System32\drivers\etc\hosts

Window 2003 C:\Documents and Settings

Window 2008R2 C:\Users\

Recent是系统文件夹，里面存放着你最近使用的文档的快捷方式，查看用户recent相关文件，通过分析最近打开分析可疑文件：

单击【开始】>【运行】，输入%UserProfile%\Recent，分析最近打开分析可疑文件。
temp(tmp)相关目录下查看有无异常文件 ： Windows产生的临时文件

9、中间件日志分析（分析是否上传webshell，sql注入等操作）

tomcat：安装目录下logs文件夹localhost_access_log.日期.txt（我们分析一般针对这个进行分析）

这个是存放访问tomcat的请求的所有地址以及请求的路径、时间，请求协议以及返回码等信息(重要)

例如：

```
127.0.0.1 - - [29/May/2020:12:03:06 +0800] "GET /tomcat.css HTTP/1.1" 200 5581
```

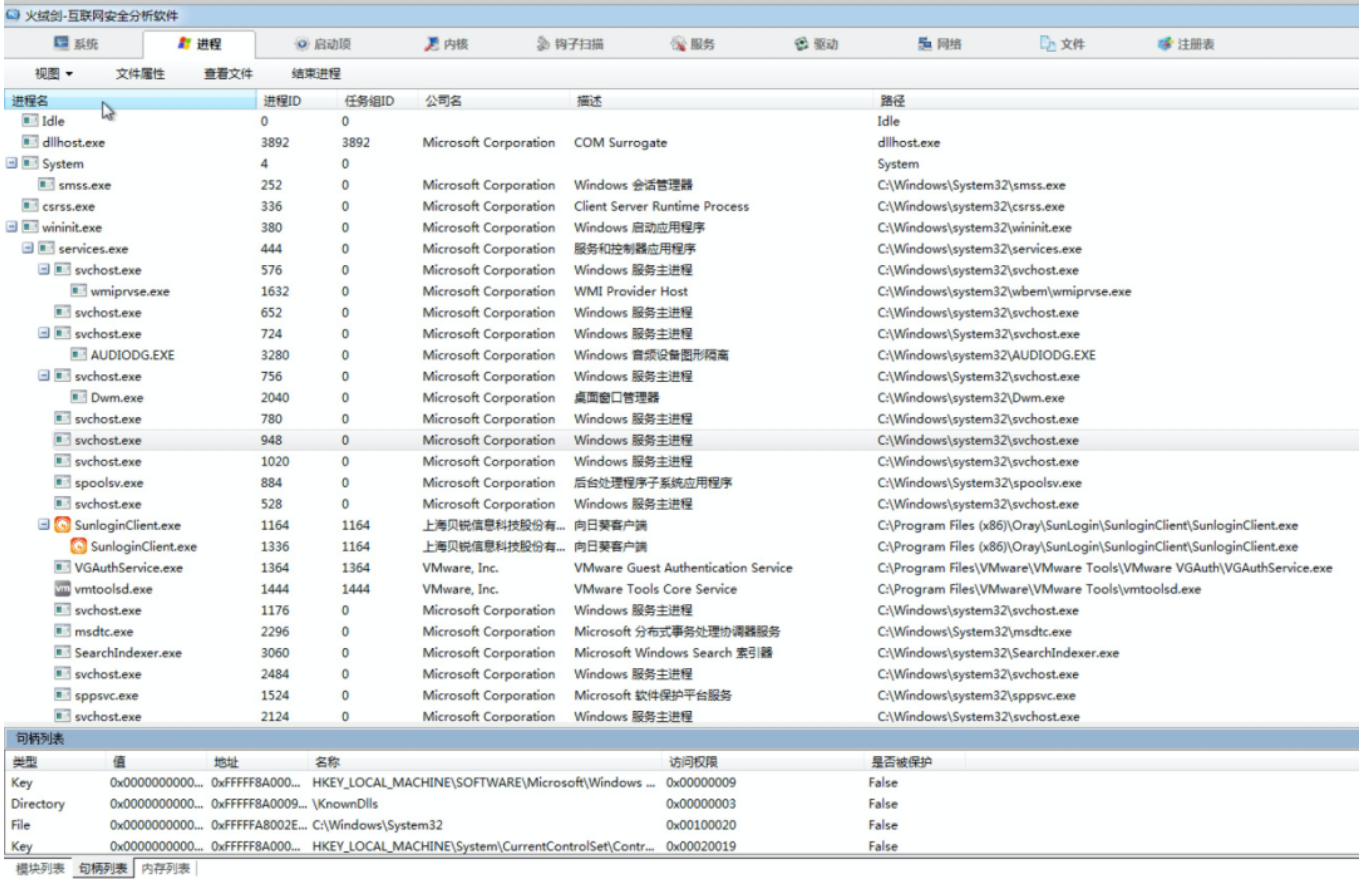
请求IP -- 请求时间 ---请求方式---请求路径---请求协议---状态码---字节包
对请求路径进行分析，定位攻击者

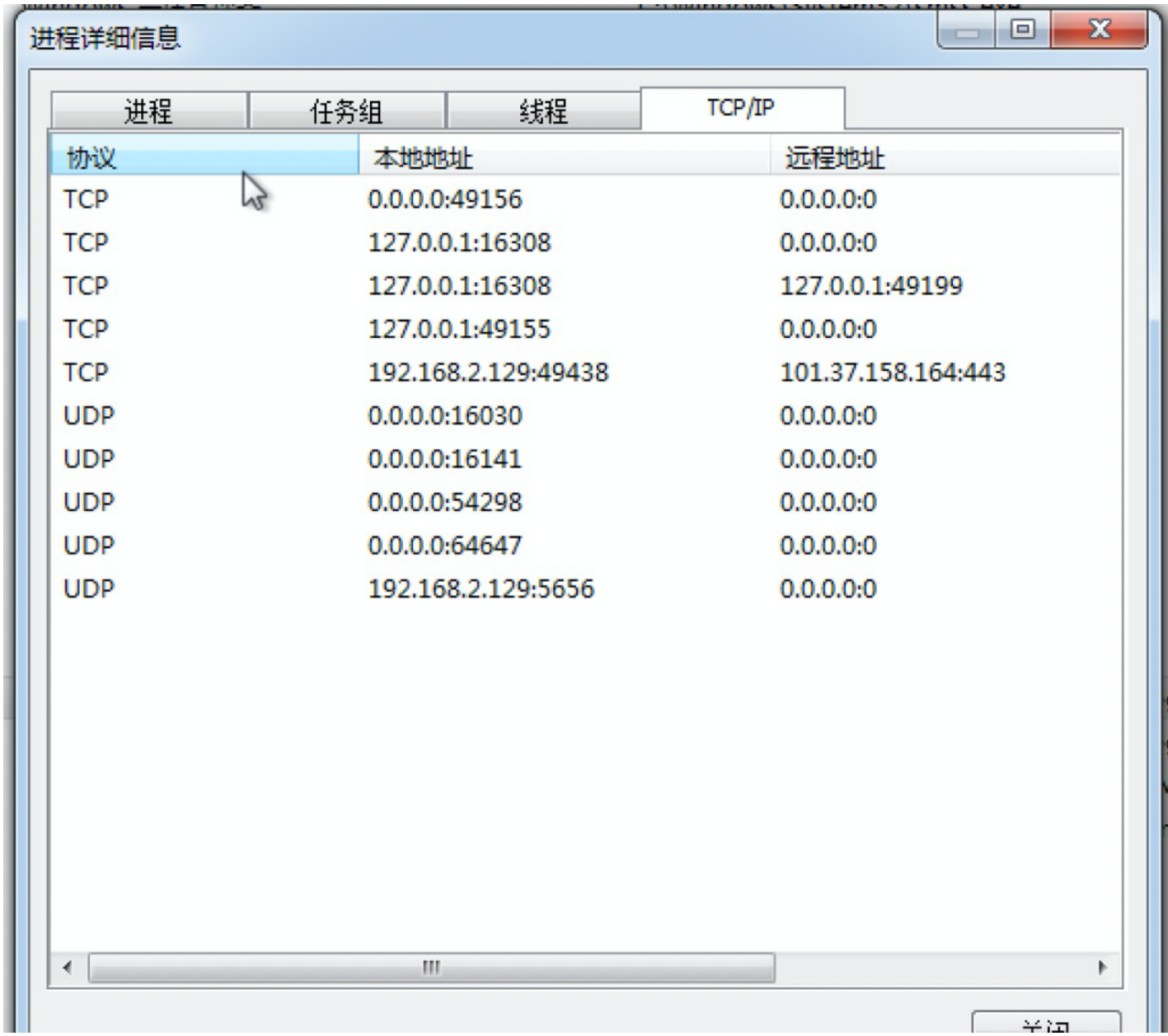
apache：安装目录下logs文件夹 access.log（格式与tomcat一致）

```
127.0.0.1 - - [13/May/2020:20:26:48 +0800] "GET /index.php HTTP/1.1" 404 196
```

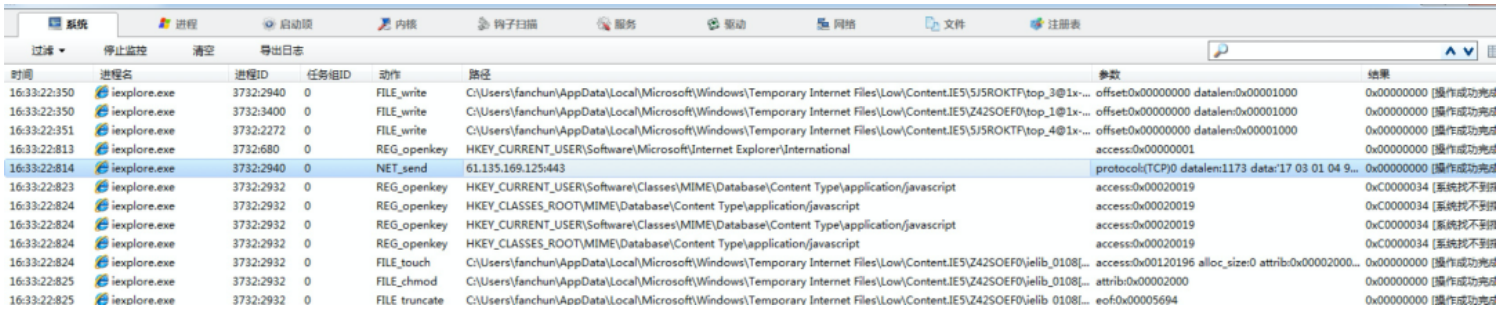
请求IP -- 请求时间 ---请求方式---请求路径---请求协议---状态码---字节包
对请求路径进行分析，定位攻击者

工具推荐：**火绒剑**
可对程序连接网络信息进行查看


火绒剑-互联网安全分析软件
系统
进程
启动项
内核
钩子扫描
服务
驱动
网络
文件
注册表
视图
文件属性
查看文件
结束进程
进程名 进程ID 任务组ID 公司名 描述 路径
Idle 0 0 Idle
dllhost.exe 3892 3892 Microsoft Corporation COM Surrogate dllhost.exe
System 4 0 System
smss.exe 252 0 Microsoft Corporation Windows 会话管理器 C:\Windows\System32\smss.exe
csrss.exe 336 0 Microsoft Corporation Client Server Runtime Process C:\Windows\system32\csrss.exe
wininit.exe 380 0 Microsoft Corporation Windows 启动应用程序 C:\Windows\system32\wininit.exe
services.exe 444 0 Microsoft Corporation 服务和控制器应用程序 C:\Windows\system32\services.exe
svchost.exe 576 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
wmiprvse.exe 1632 0 Microsoft Corporation WMI Provider Host C:\Windows\system32\wbem\wmiprvse.exe
svchost.exe 652 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
svchost.exe 724 0 Microsoft Corporation Windows 服务主进程 C:\Windows\System32\svchost.exe
AUDIODG.EXE 3280 0 Microsoft Corporation Windows 音频设备图形隔离 C:\Windows\system32\AUDIODG.EXE
svchost.exe 756 0 Microsoft Corporation Windows 服务主进程 C:\Windows\System32\svchost.exe
Dwm.exe 2040 0 Microsoft Corporation 桌面窗口管理器 C:\Windows\system32\Dwm.exe
svchost.exe 780 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
svchost.exe 948 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
svchost.exe 1020 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
spoolsv.exe 884 0 Microsoft Corporation 后台处理程序子系统应用程序 C:\Windows\System32\spoolsv.exe
svchost.exe 528 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
SunloginClient.exe 1164 1164 上海贝锐信息科技股份有... 向日葵客户端 C:\Program Files (x86)\Oray\SunLogin\SunloginClient\SunloginClient.exe
SunloginClient.exe 1336 1164 上海贝锐信息科技股份有... 向日葵客户端 C:\Program Files (x86)\Oray\SunLogin\SunloginClient\SunloginClient.exe
VGAuthService.exe 1364 1364 VMware, Inc. VMware Guest Authentication Service C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
vmtoolsd.exe 1444 1444 VMware, Inc. VMware Tools Core Service C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
svchost.exe 1176 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
msdtc.exe 2296 0 Microsoft Corporation Microsoft 分布式事务处理协调器服务 C:\Windows\System32\msdtc.exe
SearchIndexer.exe 3060 0 Microsoft Corporation Microsoft Windows Search 索引器 C:\Windows\system32\SearchIndexer.exe
svchost.exe 2484 0 Microsoft Corporation Windows 服务主进程 C:\Windows\system32\svchost.exe
sppsvc.exe 1524 0 Microsoft Corporation Microsoft 软件保护平台服务 C:\Windows\system32\sppsvc.exe
svchost.exe 2124 0 Microsoft Corporation Windows 服务主进程 C:\Windows\System32\svchost.exe
句柄列表
类型 值 地址 名称 访问权限 是否被保护
Key 0x0000000000... 0xFFFFF8A000... HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows ... 0x00000009 False
Directory 0x0000000000... 0xFFFFF8A0009... \KnownDlls 0x00000003 False
File 0x0000000000... 0xFFFFFA8002E... C:\Windows\System32 0x00100020 False
Key 0x0000000000... 0xFFFFF8A000... HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contr... 0x00020019 False
模块列表
句柄列表
内存列表


进程详细信息
进程
任务组
线程
TCP/IP
协议 本地地址 远程地址
TCP 0.0.0.0:49156 0.0.0.0:0
TCP 127.0.0.1:16308 0.0.0.0:0
TCP 127.0.0.1:16308 127.0.0.1:49199
TCP 127.0.0.1:49155 0.0.0.0:0
TCP 192.168.2.129:49438 101.37.158.164:443
UDP 0.0.0.0:16030 0.0.0.0:0
UDP 0.0.0.0:16141 0.0.0.0:0
UDP 0.0.0.0:54298 0.0.0.0:0
UDP 0.0.0.0:64647 0.0.0.0:0
UDP 192.168.2.129:5656 0.0.0.0:0

可以对某一时段发包信息进行监控（进程迁移操作时，可监控程序行为判断）



时间	进程名	进程ID	任务组ID	动作	路径	参数	结果
16:33:22:350	iexplore.exe	3732:2940	0	FILE_write	C:\Users\fanchun\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\5J5ROKTF\top_3@1x-...	offset:0x00000000 datalen:0x00001000	0x00000000 [操作成功完成
16:33:22:350	iexplore.exe	3732:3400	0	FILE_write	C:\Users\fanchun\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\Z42SOEF0\top_1@1x-...	offset:0x00000000 datalen:0x00001000	0x00000000 [操作成功完成
16:33:22:351	iexplore.exe	3732:2272	0	FILE_write	C:\Users\fanchun\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\5J5ROKTF\top_4@1x-...	offset:0x00000000 datalen:0x00001000	0x00000000 [操作成功完成
16:33:22:813	iexplore.exe	3732:680	0	REG_openkey	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\International	access:0x00000001	0x00000000 [操作成功完成
16:33:22:814	iexplore.exe	3732:2940	0	NET_send	61.135.169.125:443	protocol:(TCP)0 datalen:1173 data:'17 03 01 04 9...	0x00000000 [操作成功完成
16:33:22:823	iexplore.exe	3732:2932	0	REG_openkey	HKEY_CURRENT_USER\Software\Classes\MIME\Database\Content Type\application/javascript	access:0x00020019	0xC0000034 [系统找不到指
16:33:22:824	iexplore.exe	3732:2932	0	REG_openkey	HKEY_CLASSES_ROOT\MIME\Database\Content Type\application/javascript	access:0x00020019	0xC0000034 [系统找不到指
16:33:22:824	iexplore.exe	3732:2932	0	REG_openkey	HKEY_CURRENT_USER\Software\Classes\MIME\Database\Content Type\application/javascript	access:0x00020019	0xC0000034 [系统找不到指
16:33:22:824	iexplore.exe	3732:2932	0	REG_openkey	HKEY_CLASSES_ROOT\MIME\Database\Content Type\application/javascript	access:0x00020019	0xC0000034 [系统找不到指
16:33:22:824	iexplore.exe	3732:2932	0	FILE_touch	C:\Users\fanchun\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\Z42SOEF0\jelib_0108[...	access:0x00120196 alloc_size:0 attrib:0x00002000...	0x00000000 [操作成功完成
16:33:22:825	iexplore.exe	3732:2932	0	FILE_chmod	C:\Users\fanchun\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\Z42SOEF0\jelib_0108[...	attrib:0x00002000	0x00000000 [操作成功完成
16:33:22:825	iexplore.exe	3732:2932	0	FILE_truncate	C:\Users\fanchun\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\Z42SOEF0\jelib_0108[...	eof:0x00005694	0x00000000 [操作成功完成

本篇完

欢迎投稿HW防守相关文章！

关注我们看更多HW类文章

Timeline Sec 团队

安全路上，与你并肩前行

文章已于2020-06-02修改