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)

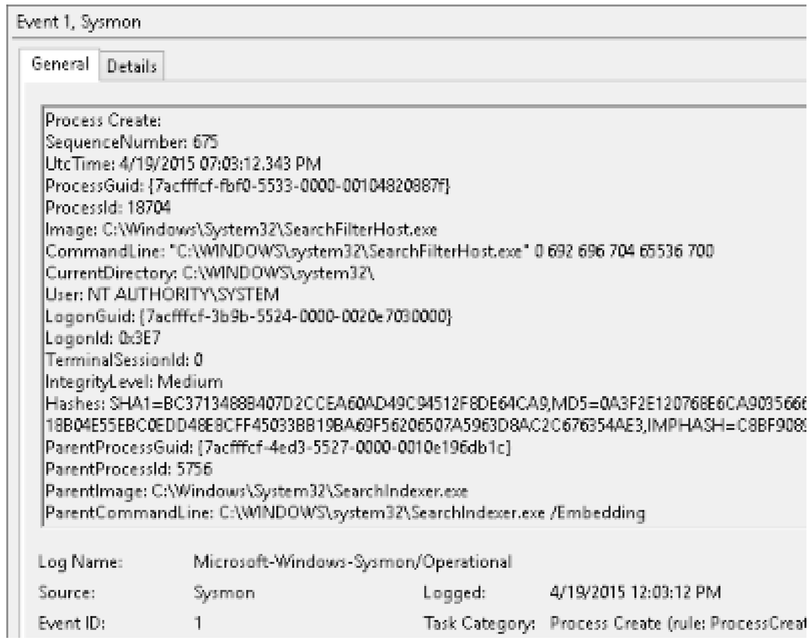
管道：

- 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

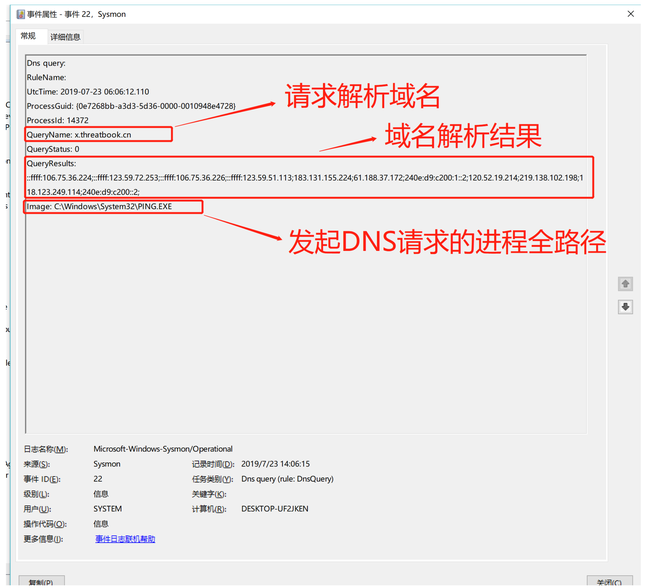
Sysmon使用

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”



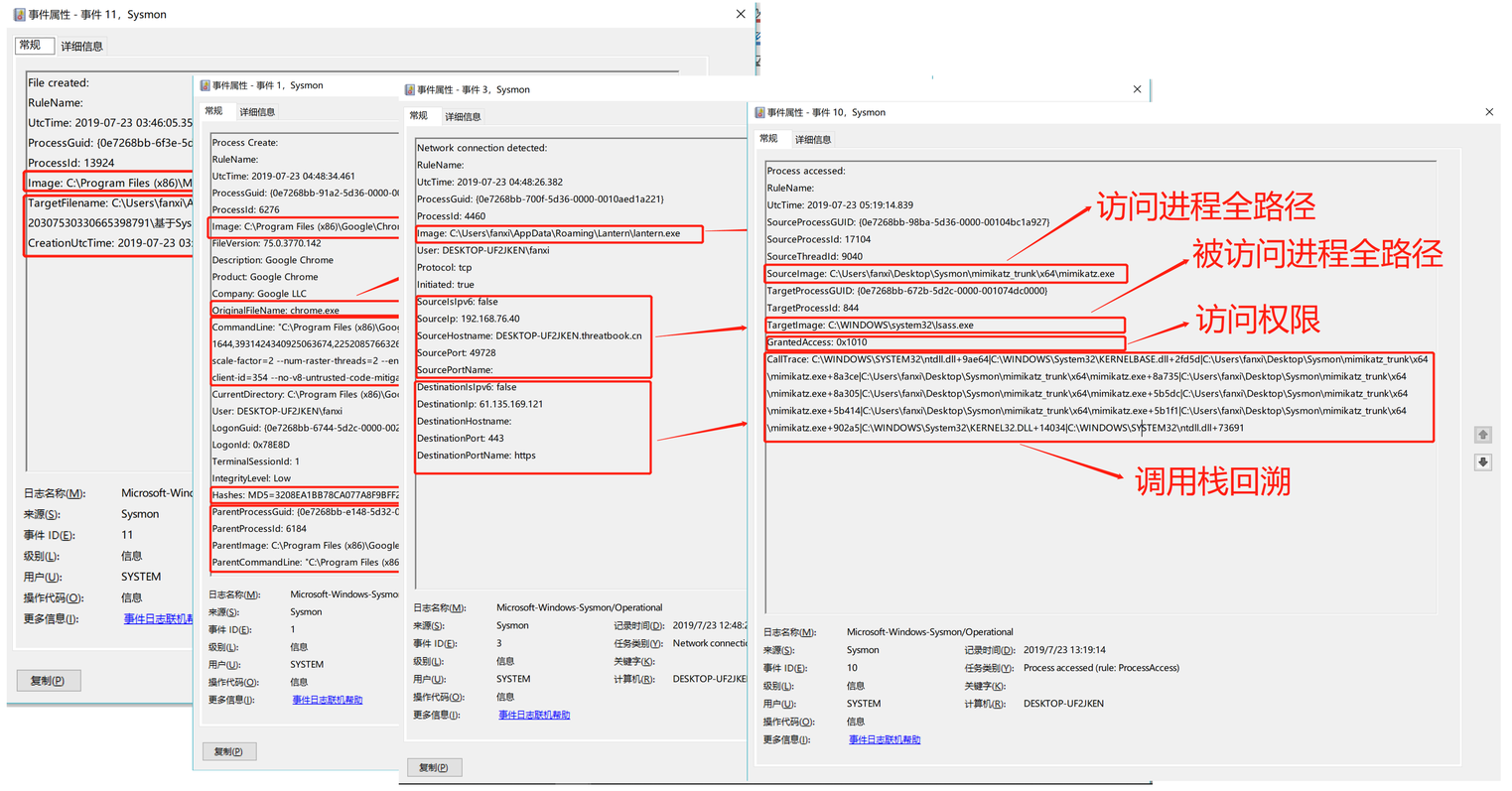
Sysmon 10.x

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



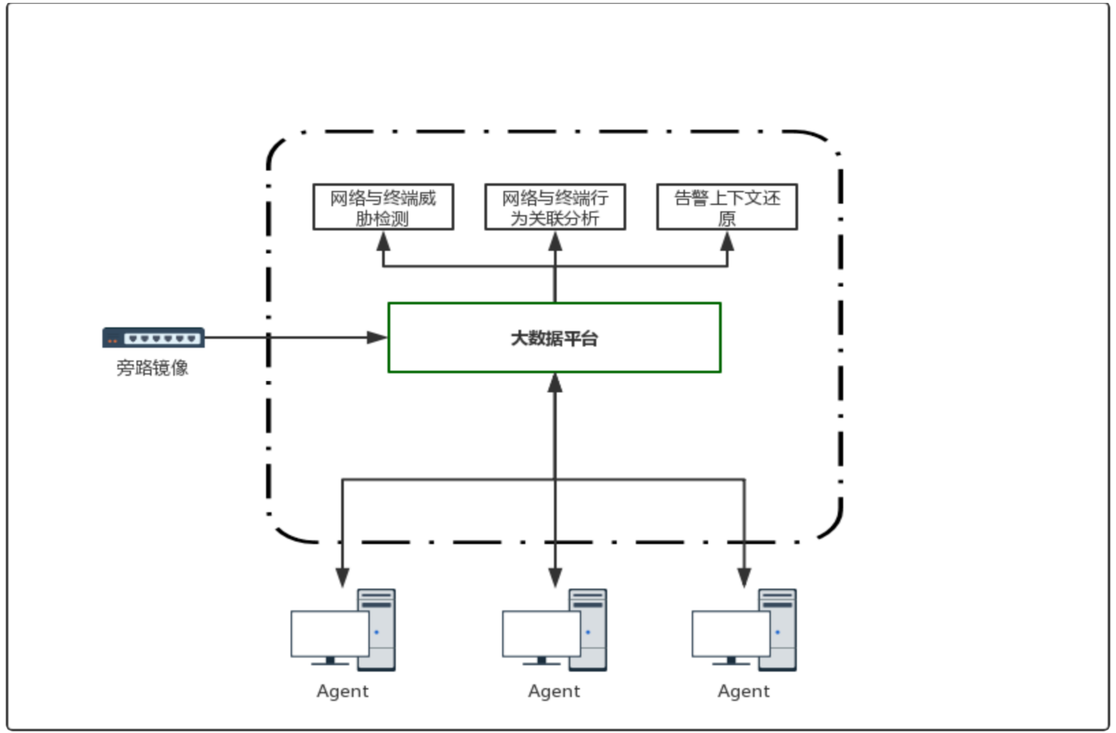
一步步建立企业级威胁检测与响应能力

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！！

```
<Sysmon schemaversion="4.10">
    <HashAlgorithms>md5,sha256</HashAlgorithms>
    <EventFiltering>

        <!-- Event ID 1 == Process Creation. -->
        <ProcessCreate onmatch="exclude">

        <!-- Event ID 2 == File Creation Time. -->
        <FileCreateTime onmatch="include"><!-- NULL -->

        <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED-->
        <NetworkConnect onmatch="exclude">

        <!--SYSMON EVENT ID 5 : PROCESS ENDED-->
        <!--DATA: UtcTime, ProcessGuid, ProcessId, Image-->
        <ProcessTerminate onmatch="include"> <!-- daiding -->

        <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL-->
        <!--DATA: UtcTime, ImageLoaded, Hashes, Signed, Signature, SignatureStatus-->
        <DriverLoad onmatch="exclude">

        <!-- Event ID 7 == Image Loaded. -->
        <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, ImageLoaded, Hashes, Signed, Signature, SignatureStatus-->
        <ImageLoad onmatch="include">

        <!-- Event ID 8 == CreateRemoteThread. -->
        <CreateRemoteThread onmatch="include">

        <!--SYSMON EVENT ID 9 : RAW DISK ACCESS-->
        <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, Device-->
        <RawAccessRead onmatch="include">

        <!-- Event ID 10 == ProcessAccess. -->
        <ProcessAccess onmatch="include">

        <!-- Event ID 11 == FileCreate. -->
        <!--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

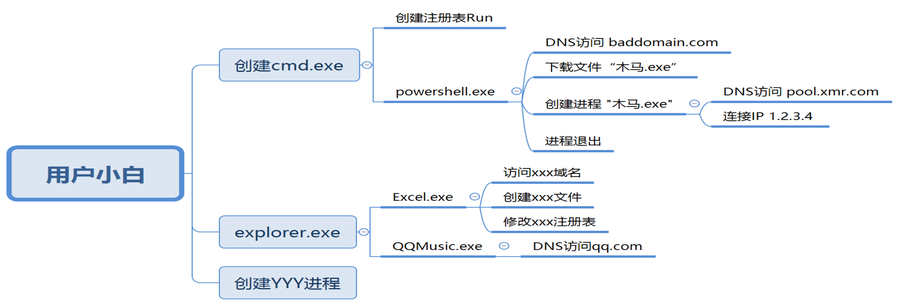
```
Subscription = pInstance->m_EvtSubscribe(NULL,
        pInstance->m_hSignalEvent,
        SYSMON_CHANNEL_PATH,
        SYSMON_XPATH,
        BookMark,
        NULL,
        NULL,
        EvtSubscribeStartAfterBookmark);

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

elasticsearch

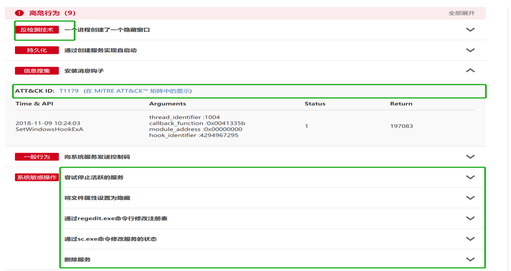
威胁检测

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

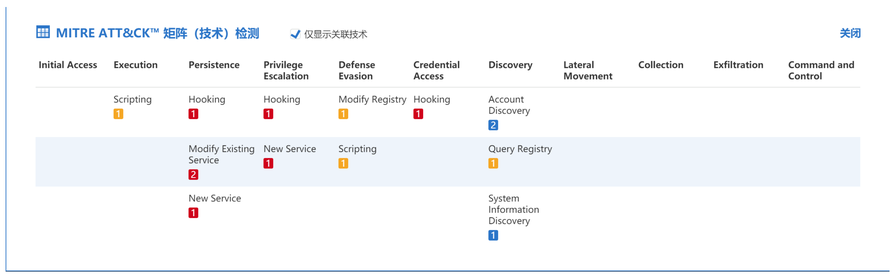
2. 终端日志分析

- 终端日志+情报
- 终端文件检测
- 终端主机行为检测



3. 行为分析

- 组合规则检测
- 基于ATT&CK的行为检测



响应：定位、处置及溯源

1. 终端行为还原

- 进程树
- 行为树

2. 告警自动化定位及处置

- 自动化定位木马进程
- 结合还原结果生成自动化处置建议

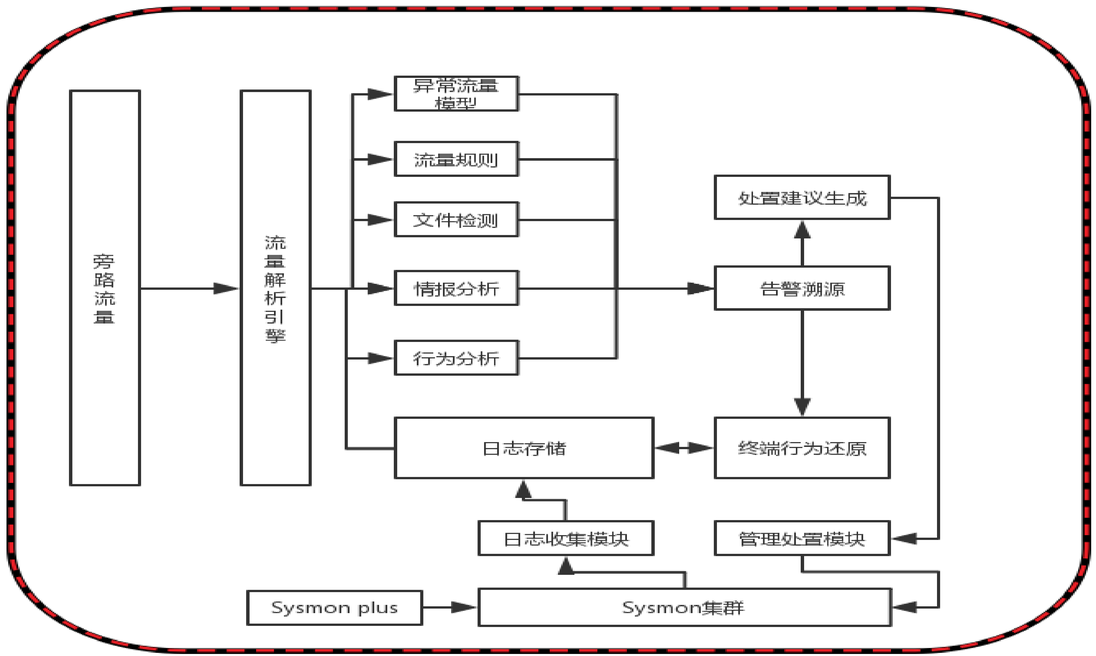
3. 告警内部溯源

- 溯源入侵源头

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

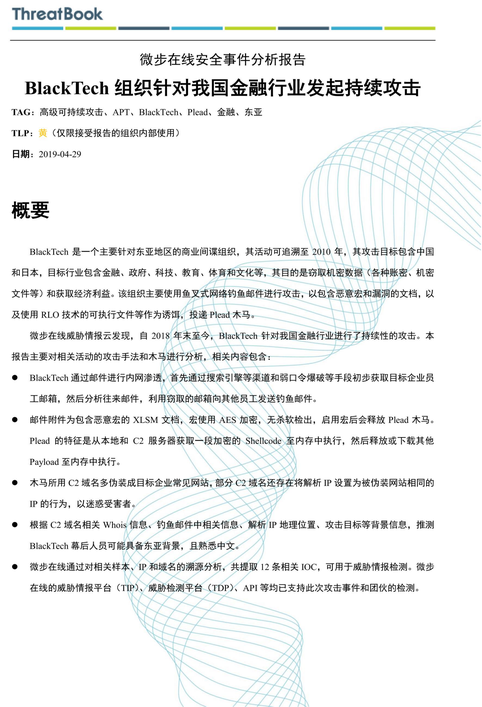
商业APT组织BlackTech最新攻击活动

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	**国内多家券商 + 多家高科技企业**
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



ThreatBook

微步在线安全事件分析报告

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

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	fcn.pool.miner... (176.9.2.145)	挖矿	2019-07-23 14:28:50	原始请求 进程还原
		pool.minergate... (176.9.2.145)	挖矿	2019-07-23 14:28:50	原始请求 进程还原
严重 C:\apt.exe	进程直连IOC	chinanetworkv... (144.202.47.216)	海莲花团伙	2019-07-23 14:28:50	原始请求 进程还原
高 C:\Program Files (x86)\Internet Explorer\iexplore.exe	进程直连IOC	fget-career.com(89.185.44.100)	Ramnit蠕虫	2019-07-23 14:28:50	原始请求 进程还原
信息 C:\torxz.exe	进程直连IOC	fcn-xmr.pool.m... (138.201.60.198)	挖矿	2019-07-23 14:28:50	原始请求 进程还原
		pool.minergate... (138.201.60.198)	挖矿	2019-07-23 14:28:50	原始请求 进程还原
严重 C:\Users\tip\AppData\Local\googleupd.exe	进程直连IOC	linenews.mypic... (198.55.121.100)	BlackTech...	2019-07-23 14:28:50	原始请求 进程还原

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

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\AppInit_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 Plugin		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	恶意	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

详细数据

节点信息

事件类型: DNS查询

主机: TIPPC1Agent

时间: 2019-07-23 14:28:50

Image: C:\Users\tip\AppData\Local\googleupd.exe

查询域名: linenews.mypicture.info

查询类型: AAAA

查询返回状态: success

查询返回结果: 198.55.121.100

动态链接库: C:\windows\system32\lpk.dll

进程ID: 3028

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	不局限于特定目标
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

ThreatBook

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。

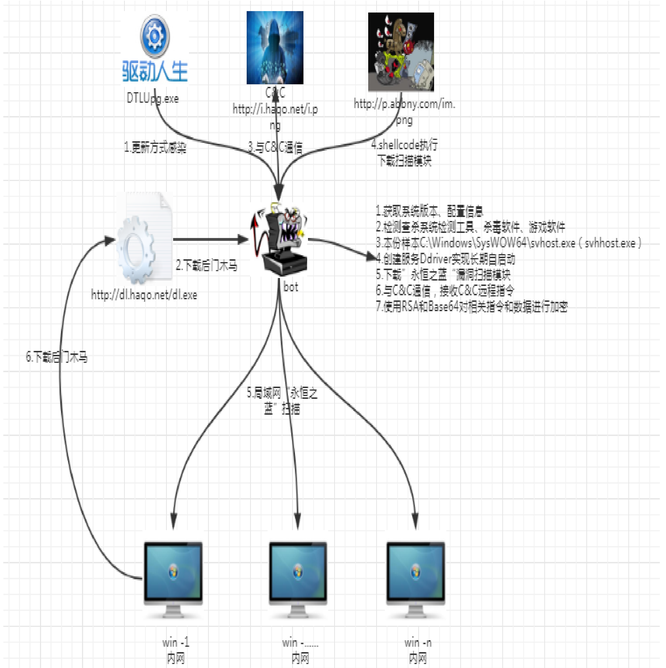
微步在线针对此事件共关联发现 3 条 IOC，均已添加到威胁情报库中，微步在线威胁情报平台（TDP）、威胁情报管理平台（TIP）、API 均已支持此次威胁的检测发现。如需微步在线协助，请与我们联系 contactus@threatbook.cn

……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

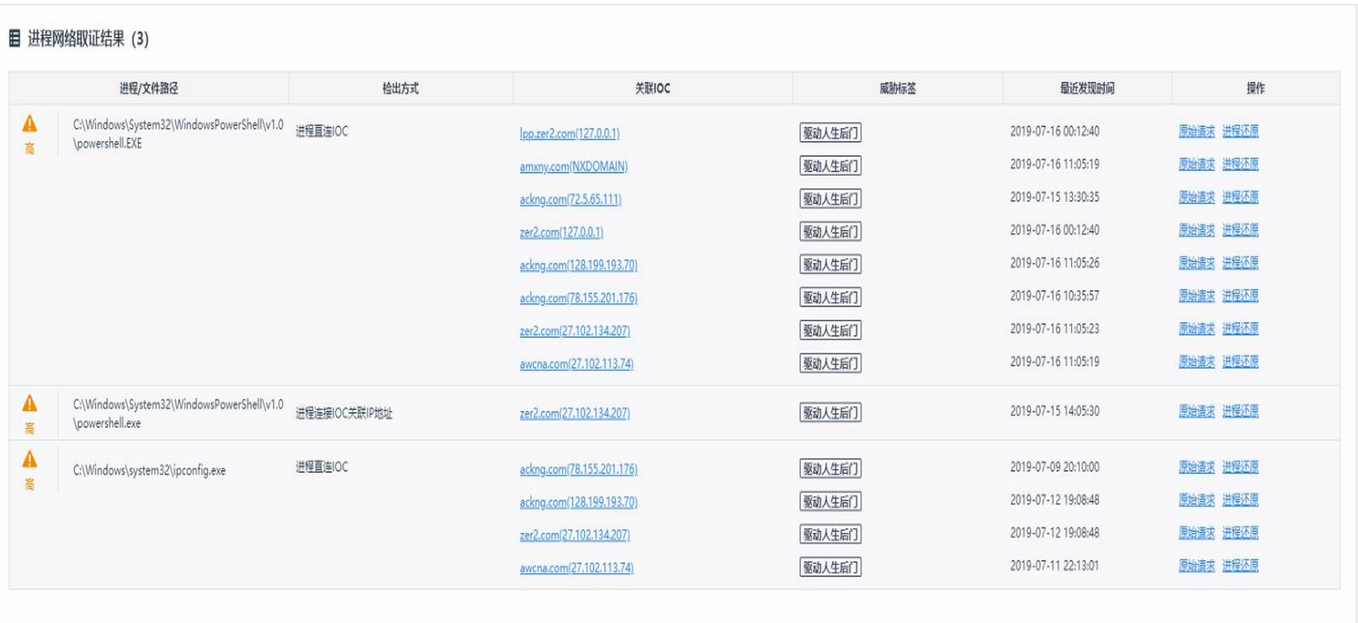
……详　情……

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



驱动人生供应链攻击事件取证&处置

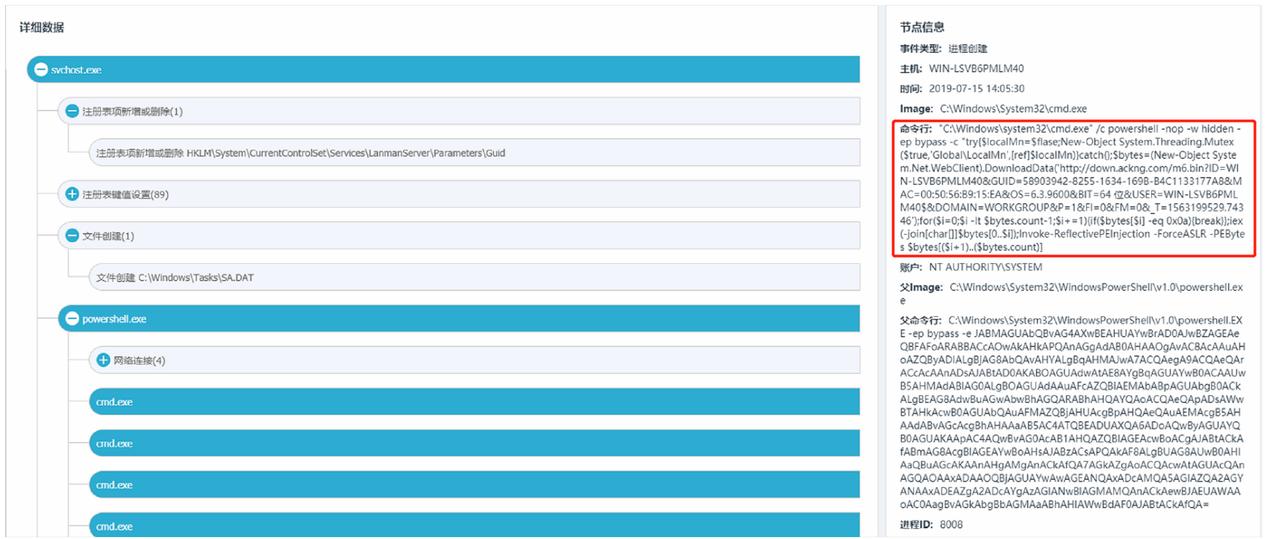
1. 基于Sysmon DNS 日志
2. 直接定位驱动人生后门利用powershell执行恶意代码


```
{
  "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,
  "pc": "",
  "agent_id": "4ac8f8e38df9b6d1af1db4800a1d1965"
}
```


1. 删除木马计划任务：
   - C:\\Windows\System32\Taks\Rtsa
   - C:\Windows\System32\Tasks\Microsoft\Windows\Customer Experience Improment 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



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

CTIC