安天下一代引擎结合知识库如何揭示载荷的ATT&CK战术能力

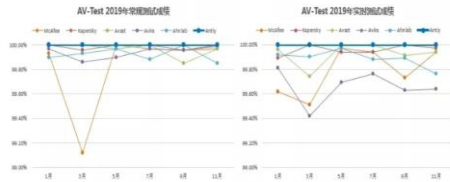
安天基础引擎研发部

从安天的安全引擎说起

- 生态合伙伙伴突破**100家**
- 内置安天网络检测引擎的网络设备和网络安全设备累计超过**90万台**
- 安天移动安全引擎覆盖手机和其他类型智能终端累计超过**22亿部，已经成为国民级安全内核。**

生态稳步发展

AV-TEST 2019年度移动反病毒软件测评成绩



2019中国网络安全技术对抗赛比赛结果

名次	单位	参赛产品
第一名	北京安天网络安全技术有限公司	安天追影威胁分析系统+安天探海威胁检测系统
第二名	北京兰云科技有限公司	兰眼下一代威胁感知系统
第三名	网神信息技术（北京）股份有限公司	网神SecIDS 3600入侵检测系统

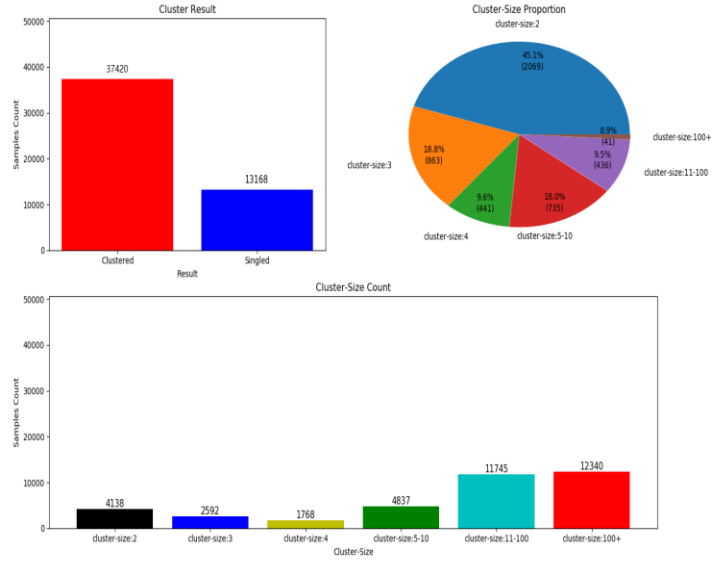
能力始终如一

- 2018年， AV-TEST移动安全检测唯一年度检测能力全满分厂商
- 2019年度， AV-TEST移动安全检测年度检测能力全双满分厂商
- 2018年国家应急中心安全引擎技术对抗赛双赛第一名
- 2019年国家应急中心安全引擎技术对抗赛（两赛合一）第一名

安天引擎的2020

- AVLSDK已在全面实现对国产化主流操作系统和硬件架构的适配

- 增加AI检测能力，实现指令级代码同源及检测能力，从学术化的研究转化为可工程化实现的能力



長纓待展

CONTENTS

目 录

01 威胁情报与知识库的当前问题

变化中的攻击方与防御方

对手在变化

目标在变化

防御方的需求在变化

- 用户的单点需求
- 用户的面的需求
- 用户的立体需求

满足防御方需求的解决办法

以捕获到一些攻击载荷为例

步骤1 分析攻击的危害

输出**攻击手段**和危害信息

步骤2 判断是否从属已知攻击组织或事件

是

确认**攻击者**身份

否

步骤3 判断攻击载荷之间的关联关系，是否具有同源性

是

作为**重点可疑**观察对象跟踪分析，进一步确认身份信息

否

暂不重点追踪

业界实现的方式

利用ATT&CK分类威胁，输出攻击者使用了哪些手段、可能造成的危害等信息

利用已知**IOC信息**对攻击载荷进行身份判定,弥补威胁对抗的时效性和精准指向性

通过关联和聚类，发现可能存在的相关APT组织

现有威胁知识输出方式的真实效果

业内常见的知识输出方式

IOC情报

（对攻击方所使用的装备或基础设施的**指向能力**）

结合

传统反病毒引擎

（海量的恶意代码的检测和辨识能力）

期望达成

发现、阻断和猎杀高级威胁行动

IOC信息

（IP、域名、Hash）

这种检测能力组合虽然对类似海莲花、白象、绿斑一类的APT攻击具有一定的价值，但在过去十年内对于对抗来自更高水平的威胁行为体的活动，其实收效甚微。针对类似毒曲II、方程式等高级威胁行动或组织的发现、阻断和猎杀活动中，这些信息几乎无法发挥任何作用。

效果不佳的主要原因 —效用性

木马名称：Stuxnet

出现时间：2010年6月

主要功能：攻击用于数据采集与监控的工业控制系统。

描述：震网使用模块种类繁多，自身逻辑复杂，利用了多个零日漏洞，通过一套完整的入侵和传播流程，突破工业专用局域网的物理限制，攻击用于数据采集与监控的工业控制系统。

分类	数量	说明
DROPPER	1200+	~WTR4132.tmp,其STUB节的内容变换、样本自身代码的升级与发布、人工二进制更改，组合操作生成多个样本
DROPPER LOADER	460+	~WTR4141.tmp，通过少量原始样本，经过二进制修改、签名、追加损坏签名、签名后继续追加文件等操作，造成样本量增加
LNK	20+	漏洞利用载荷，用于加载恶意DLL文件
其他文件	100+	CAB文件、驱动文件、Step 7使用的DLL等
编译器版本	10+	多版本编译器表明工程代码经过多人编译，生成母体样本基数变大

样本1	样本2	异同	原因
BF6E9CBCDA5EF3	F6E836E63974	时间戳相同，代码段，导入表Hash均不同，但代码对比一致	输出文件类型不同，EXE和DLL
F48F28C1539DFC	F6E836E63974	时间戳、导入表HASH、代码段HASH相同，文件HASH不同	Stub包裹内容不同
02BC5EDC93859E	3B8EA5381D81	时间戳、导入表HASH、代码段HASH相同，文件大小不同	有签名和无签名
31E2FD7A131B71	C77CB014E669	时间戳、导入表HASH、stub段hash相同、文件大小相同，代码段HASH不同	链接器版本不同
0C8AB2873E1399	98FBEBD88830	时间戳、导入表HASH相同，代码段HASH不同	无关代码0xFF填充
C77CB014E6694C	5A379BB1480E	时间戳、导入表HASH、代码段HASH、STUB段HASH、文件大小相同，文件HASH不同	PE头部无关数据被0xFF填充
0B5FD57A4F7008	3867ABE7E8F9	除时间戳外其余均相同	

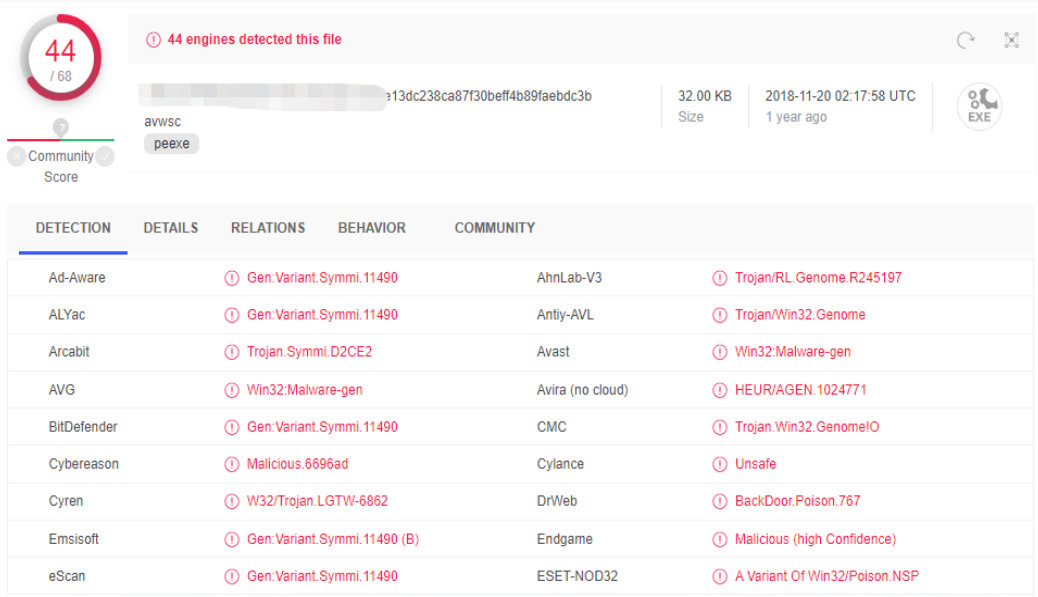
震网样本集差异分析

——《对Stuxnet蠕虫攻击工业控制系统事件的综合分析报告》

效果不佳的主要原因 —知识性

- **传统引擎的输出不具备丰富的知识性**

1. 原有的知识工程体系，不能满足直接定位到高级网空威胁行为体的精准要求
2. 单一病毒名输出的方式缺乏**知识性**，无法满足用户对于威胁想要深入了解的需求。在现有防御体系中，没有把传统引擎当作一个关键环节来看待，原因主要是普遍把引擎作为一个基础支撑能力看待，作为**黑箱**使用，没有把引擎的输出作为**知识供给**。

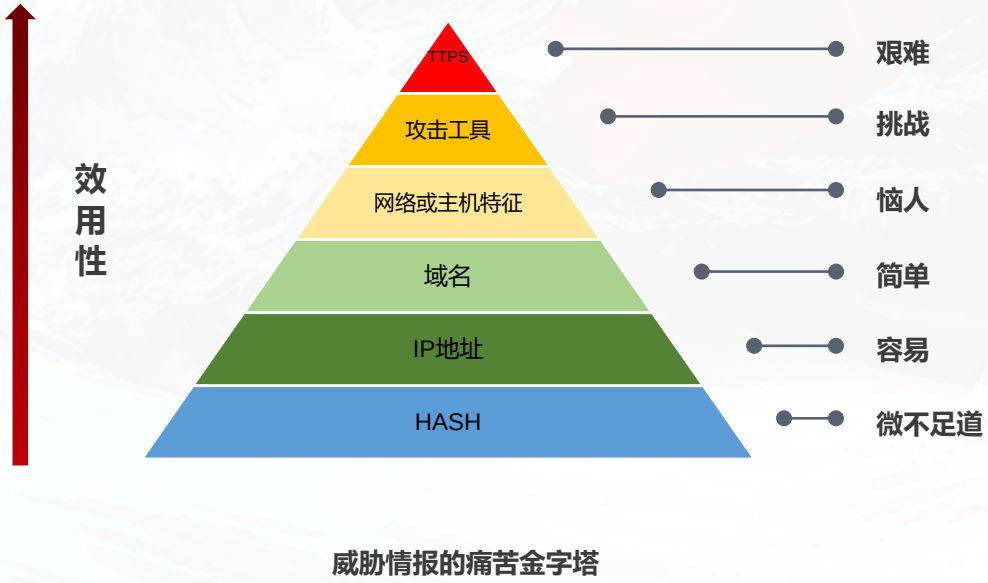


VirusTotal网站对某高级威胁样本的检测结果

效果不佳的主要原因—效用性

- **IOC类知识检测的鲁棒性较差**

人们试图通过IOC信息来为高级威胁对抗提供更好的指向性，这是目前阶段知识输出的一种**常态**，但对于超高能力的网空威胁活动，实际**IOC**几乎是**无效**的。



威胁情报的痛苦金字塔

02 可结合知识库的威胁检测引擎

安天引擎结合知识库

- 支持多种输入与输出，可输出ATT&CK框架、TCTF框架、向量等信息，并以此向知识库查询

下一代威胁检测引擎

- 全面格式识别
- 深度预处理
- 虚拟化执行等机制

输出

高价值威胁知识

- 攻击技术
- 基础信息
- 属性信息
- 结构信息
- 身份信息
- 环境信息

结合

知识库

- 武器库
- 组织库
- 事件库
- 画像
- ….

达成

客户防御场景下的可消费信息

- 对攻击手段的揭示
- 对高级威胁攻击方身份的揭示
- 对高级威胁的发现、阻断

动静态检测相结合

- 解决不可执行文件

- 解决组件分批下发的问题

- 提升检测效率

当前主流以动态为主的ATT&CK提取的缺陷

- 特定的主进程名称才会触发相关流程

```
if ( StrStrIW(&Filename, L"SearchIndexer.exe") )
{
  ThrdAddr = 0;
  v12 = beginthreadex(0i64, 0, sub_1800037B0, hModule, 0, &ThrdAddr);
}
else if ( StrStrIW(&Filename, L"explorer.exe") )
{
  ThreadId = 0;
  v14 = CreateThread(0i64, 0i64, sub_1800063B0, 0i64, 0, &ThreadId);
}
else if ( StrStrIW(&Filename, L"msdtc.exe") )
{
  Sleep(0x7530u);
  pszPath = 0;
  memset(&v17, 0, 0x206ui64);
  v4 = wgetenv(L"SystemRoot");
  wsprintfW(&pszPath, L"%s\\System32\\wimsvc.exe", v4);
  if ( PathFileExistsW(&pszPath) )
  {
    GetStartupInfoW(&StartupInfo);
```

- **检查父子进程名**

安天引擎利用静态配置解密信息进行检测

- att&ck技术点： 解密/去混淆文件或信息

Hash	ed7c90582042a0a6e304088ed5d32706
Network	2.tcp.ngrok.io:15944
Mutex	DC_MUTEX-UFXHUR2
Version of rat	#KCMDDC51#
Campaign ID of rat	Sazan

安天引擎能力的维度--深入的识别与解析

识别能力

✓全格式识别能力

✓编译器与壳识别能力

1.可识别编译器：>500（包含小版本）

2.可识别壳： >3000（包含小版本）

解析能力

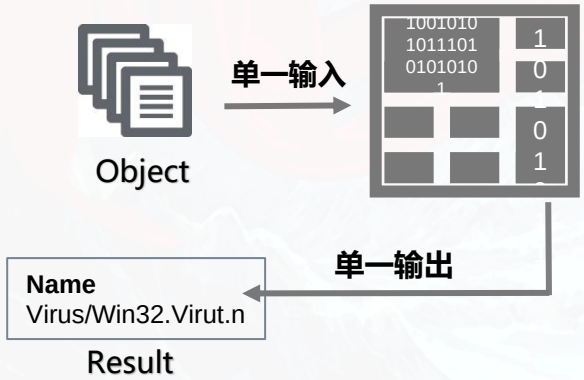
✓全格式解析能力

✓解包：压缩包，自解压包，安装包等共计40类

✓脱壳：加密壳、压缩壳等30+种

识别及拆解能力	可识别格式	支持识别：可执行文件、包裹、文档、媒体文件、图片文件、软件关联格式、脚本、文本格式、其它格式等九大类格式
		格式数（含版本）**298**
	可识别编译器	编译器种类**40**
		编译器种类（含版本)**108**
	可识别壳	可识别壳种**类数434**
		可识别壳种类数（含版本）**861**
	可识别包裹	可识别包裹数目**58**
	拆解能力	可深度拆解的可执行程序的种类：下载器、释放器**134**种
		可深度预处理的复合文档的格式数目**24**
		可脱壳种类数**31**
		可拆解包裹数**58**

安天引擎能力的维度--多种输入输出对象

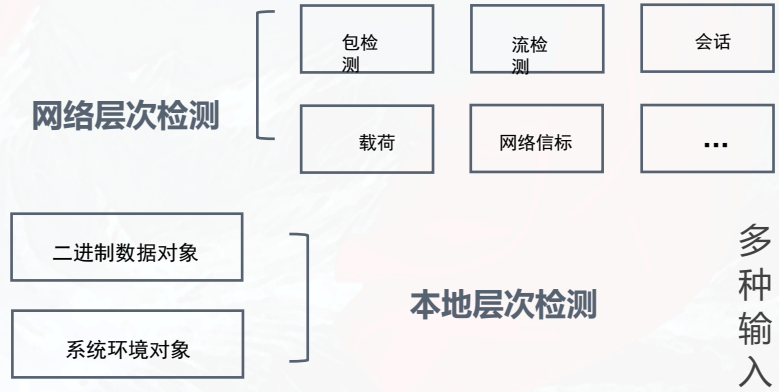


✓ **传统引擎**

主要是以单一对象为输入，以单一结果为输出。而随着威胁的进一步演进和泛化，威胁检测已不能仅仅停留在对单一对象进行鉴定上。

✓ **AVLSDK威胁检测引擎**

多种输入对象，多种输出结果。威胁检测多样化。



输出 1

- 黑白
- 多向量
  - 识别信息
  - 基础信息
  - 附加信息
  - 行为信息
- 核心行为
  - 远控 广告
  - DDoS 下载
  - 窃取
- 威胁行为
  - 传播 伪装
  - 隐蔽 对抗
  - 信息获取 攻击

输出 2

- 组织名称
- 组织简介
- 攻击领域
- 攻击方式
- 活跃时间
- 利用漏洞

输出 3

ATT&CK框架信息

初始访问、执行、持久化、提权、防御规避、凭证访问、发现、横向移动、收集、命令控制、渗透

安天引擎后台分析运营系统

威胁知识运营系统　样本分析　事件分析　攻击组织分析　人工分析　框架管理　simon@antiy.cn

上传报告　上传样本

报告：苦象组织近期网络攻击活动及泄露武器分析

作者 安天CERT | 大小 2.23MB | 上传日期 2020-12-12 | 分析次数 2次 | 分析框架 ATT&CK

2.2 投递木马

近期苦象组织常用的执行流程有：漏洞文档＋MSI程序、CHM文件+MSI程序等，此次也类似，采用LNK+ MSI程序手法。攻击者以未知手段（可能是鱼叉式钓鱼邮件、社交平台等）向目标投递一份RAR压缩包，包内包含恶意快捷方式Income tax Savings for 2020-2021.lnk：

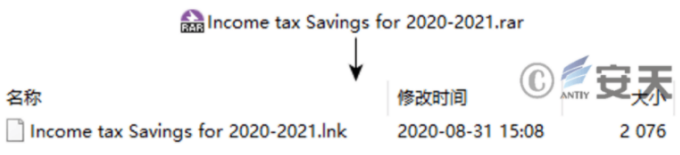


图 2-3 诱饵文件

表2-2 LNK样本标签

病毒名称	Trojan[LNK]/Downloader.LNK.Gen
原始文件名	Income tax Savings for 2020-2021.lnk
MD5	569D721E44E1A31A53AEAA0E514AD794
文件大小	2.03 KB (2076 bytes)
文件格式	Windows shortcut
创建时间	2009:07:13 23:49:07+00:00
压缩包存放时间	2020:08:31 15:08:07
相对路径	..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
图标文件名	%ProgramFiles%\Windows Photo Viewer\PhotoAcq.dll
VT检测结果	16/59

快捷方式被点击运行后，会执行一段Powershell命令：

powershell.exe" -exec start "(New-Object -comObject WScript.Shell).CreateShortcut('Requirement list for Aug 2020.lnk').Description;

人工分析成果　提取向量 8　战术 0　技术 0　攻击组织 1　攻击事件 1

分析面板　分析历史

鱼叉式钓鱼邮件	2020-12-12	编辑
社交平台	2020-12-12	编辑
Income tax Savings for 2020-2021.lnk	2020-12-12	编辑
%ProgramFiles%\Windows Photo Viewer\PhotoAcq.dll	2020-12-12	提交

威胁判定：恶意　关联组织：苦象(Bitter/苦象/T-APT-17/蓑灵花)
关联事件：苦象组织近期网络攻击活动及泄露武器分析　框架分析：选择威胁框架
标签：选择标签　生成规则：是的
备注：

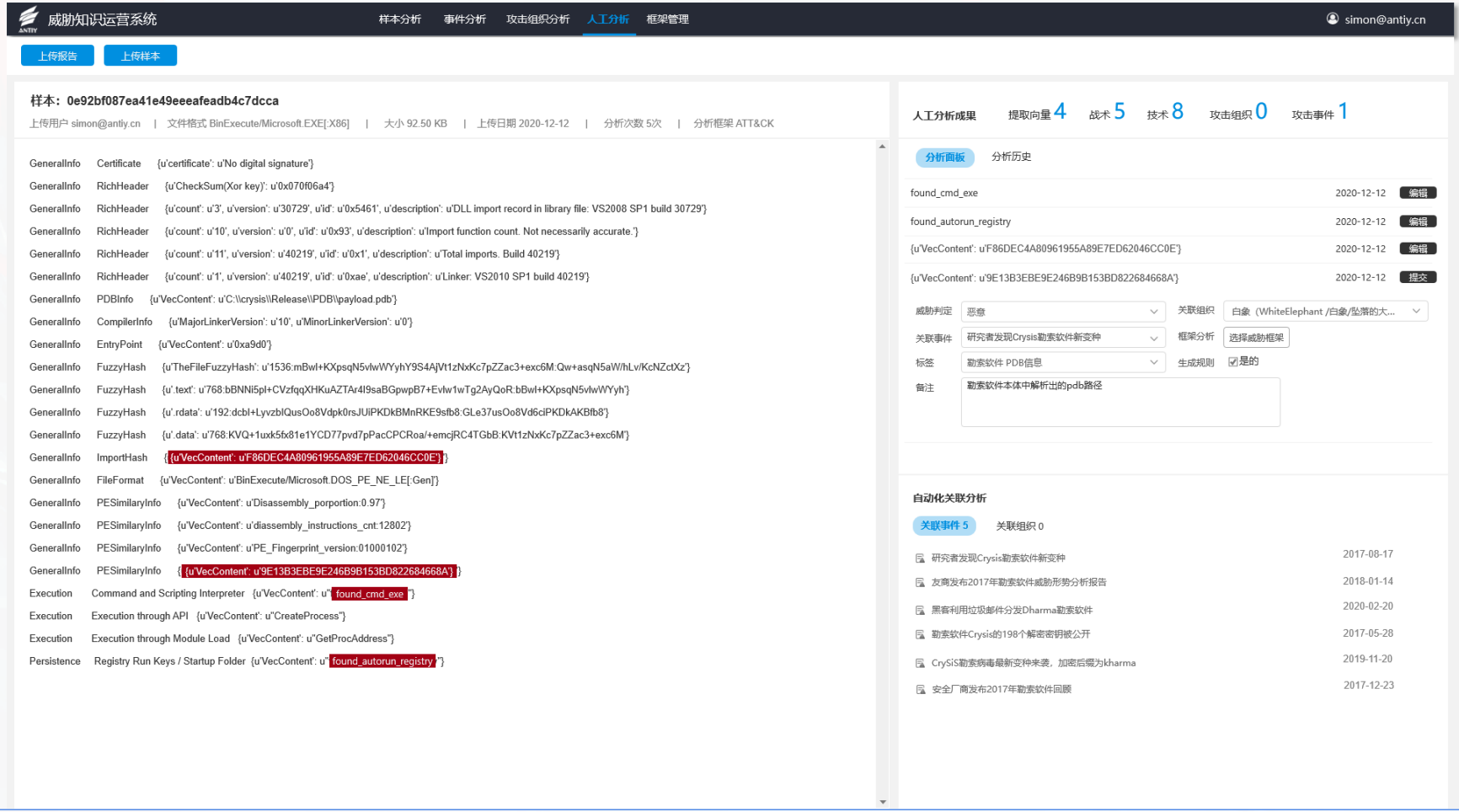
MsAulis.exe　2020-12-12　提交

自动化关联分析

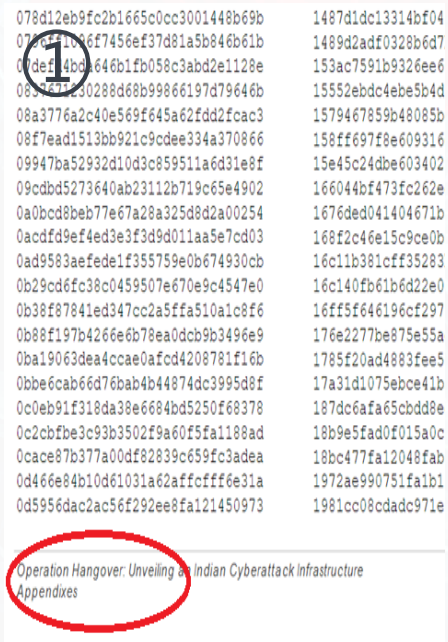
关联事件 5　关联组织 1

苦象组织近期网络攻击活动及泄露武器分析	2020-09-10
安天发布苦象组织近期网络攻击活动及纳入武器分析	2020-09-17
蓑灵花APT行动攻击报告	2016-11-15
蓑灵花（BITTER）APT组织针对中国境内军工、核能、政府等敏感机构的最新攻击活动报告	2018-12-25
“Bitter”团伙持续对我国发起定向攻击	2019-03-28

安天引擎后台分析运营系统



应用效果—更好的知识性



某白象分析报告

	MD5	Kaspersky	Microsoft
1	MD5	Kaspersky	Microsoft
2	08a3776a2c40e569f645a62fdd2fcac3	Trojan.Win32.Agent.hwjb	Worm:Win32/Foler.C
3	0acdfd9ef4ed3e3f3d9d011aa5e7cd03	Trojan-Downloader.Win32.Agent.hhgu	NotFound
4	15e45c24dbe6034024fcffe4c358556b	Worm.Win32.Agent.ali	Worm:Win32/Foler.C
5	0ca8e67b37a00df82839c659fc3adea	Trojan.Win32.VB.cefz	NotFound
6	17a31d1075ebce41ba48a9efacb79d28	Exploit.Win32.CVE-2012-0158.j	NotFound
7	18bc477fa12048fab8ec93d5ff942cf5	Trojan.Win32.Bahamut.o	Trojan:Win32/Rimod!gmb
8	1972ae990751fa1b1532aa792bd5c160	Trojan.Win32.APosT.ity	TrojanSpy:Win32/Dayek.A
9	1487d1dc13314bf0431792b37ec67e2d	HEUR:Trojan.Win32.HangOver.gen	NotFound
10	16c11b381cff35283b879ec1a84f72e4	Virus.Win32.Virut.ce	Worm:Win32/Foler.C
11	0ad9583aefede1f355759e0b674930cb	Trojan.Win32.Agent.hnll	NotFound
12	09947ba52932d10d3c859511a6d31e8f	Trojan-Spy.Win32.Agent.chfl	NotFound
13	0ba19063dea4ccae0afcd4208781f16b	Trojan.Win32.APosT.flo	TrojanSpy:Win32/Dayek.A
14	0c0eb91f318da38e6684bd5250f68378	Trojan-Spy.Win32.KeyLogger.acqh	TrojanSpy:Win32/Hanove!rfn
15	166044bf473fc262ed97283c6e157eb5	Trojan-Spy.Win32.KeyLogger.acqh	NotFound
16	1489d2adf0328b6d7b42170095f966c9	Trojan-Spy.Win32.KeyLogger.acqh	TrojanSpy:Win32/Hanove.C
17	168f2c46e15c9ce0ba6e698a34a6769e	Trojan-Downloader.Win32.AutoIt.xd	NotFound
18	0796ff1096f7456ef37d81a5b846b61b	Trojan-Spy.Win32.KeyLogger.adar	TrojanSpy:Win32/Dayek.A
19	1981cc08cdadc971e28768dc04d98637	Trojan-Dropper.Win32.Dycler.vrp	NotFound
20	078d12eb9fc2b1665c0cc3001448b69b	HEUR:Trojan.Win32.HangOver.gen	TrojanSpy:Win32/Hanove.F
21	0bbe6cab66d76bab4b44874dc3995d8f	HEUR:Trojan.Win32.HangOver.gen	TrojanSpy:Win32/Hanove.F
22	0c2cbfbe3c93b3502f9a60f5fa1188ad	Worm.Win32.Agent.ali	Worm:Win32/Foler.C
23	0d466e84b10d61031a62affcfff6e31a	Trojan-Downloader.Win32.VB.bkrb	TrojanDownloader:Win32/Adodb.A
24	16ff5f646196cf29792f5b159d1288b8	Trojan-Spy.Win32.KeyLogger.acqh	NotFound
25	0b88f197b4266e6b78ea0dcb9b3496e9	Trojan-Spy.Win32.Agent.chju	TrojanSpy:Win32/Hanove.A
26	0d5956dac2ac56f292ee8fa121450973	HEUR:Trojan.VBS.SAgent.gen	NotFound
27	187dc6afa65cbdd8ee87a58271b56864	Trojan.VBS.Starter.dy	NotFound
28	0a0bcd8beb77e67a28a325d8d2a00254	Worm.Win32.Agent.ali	Worm:Win32/Foler.C
29	176e2277be875e55ad7211ff5e8df7a5	Trojan-Spy.Win32.KeyLogger.acqh	NotFound
30	153ac7591b9326ee63cd36180d39665e	HEUR:Trojan.Win32.HangOver.gen	Backdoor:Win32/Hanove.A
31	158ff697f8e609316e2a9fbe8111e12a	NotFound	NotFound
32	0b29cd6fc38c0459507e670e9c4547e0	Trojan-Downloader.Win32.Agent.gzkf	NotFound
33	1785f20ad4883fee549f0aec5d20aaca	Trojan-Spy.Win32.KeyLogger.acqh	TrojanSpy:Win32/Hanove!rfn
34	0837671230288d68b99866197d79646b	Trojan-Spy.Win32.KeyLogger.adar	TrojanSpy:Win32/Dayek.A
35	16c140fb61b6d22e02aa2b04748b5a34	HEUR:Trojan.Script.Generic	TrojanSpy:Win32/Linog.A
36	09cdbd5273640ab23112b719c65e4902	Backdoor.Win32.RShot.vsl	NotFound
37	15552ebdc4ebe5b4d2f71ab2d2e574cb	Trojan-Spy.Win32.Agent.cpfz	NotFound
38	08f7ead1513bb921c9cdee334a370866	Trojan-Spy.Win32.KeyLogger.acqh	TrojanSpy:Win32/Hanove!rfn
39	07defd4bda646b1fb058c3abd2e1128e	Trojan.Win32.Agent.hwjb	Worm:Win32/Foler.C
40	0b38f87841ed347cc2a5ffa510a1c8f6	Trojan-Spy.Win32.Agent.chfl	NotFound

各反病毒引擎厂商检测结果

	MD5	所属组织	所属组件	功能
1	MD5	所属组织	所属组件	功能
2	09cdbd5273640ab23112b719c65e4902	白象	Backdoor	白象所用的后门软件，可执行shell命令
3	0796ff1096f7456ef37d81a5b846b61b	白象	KeyLogger	白象组织使用的KeyLogger工具，具有开机自启功能
4	0837671230288d68b99866197d79646b	白象	KeyLogger	白象组织使用的KeyLogger工具，具有开机自启功能
5	0d466e84b10d61031a62affcfff6e31a	白象	Dropper	白象组织使用的Dropper文件，释放VBS脚本并执行
6	1489d2adf0328b6d7b42170095f966c9	白象	Downloader	白象组织使用的Downloader文件，下载恶意载荷并执行，窃
7	078d12eb9fc2b1665c0cc3001448b69b	白象	Ron Tools	白象组织使用的后门工具，因其pdb信息而命名，下载恶意载
8	153ac7591b9326ee63cd36180d39665e	白象	Http	白象组织使用的联网组件


```
"result": {
  "desc": "0796ff1096f7456ef37d81a5b846b61b",
  "malware_info": {...},
  "format": {
    "id": 22,
    "name": "PE"
  },
  "packer": {...},
  "hformat": {
    "id": 1,
    "name": " BinExecute/Microsoft.EXE[:X86] "
  },
  "sfx": {...}
},
"knowledge": {
  "sid": 46,
  "malware_name": "Trojan[Spy]/Win32.KeyLogger",
  "type": "APT",
  "description": "白象组织使用的KeyLogger工具，具有开机自启功能",
  "tags": [
    "APT",
    "KeyLogger",
    "开机自启"
  ],
  "group": [
    {
      "name": "白象",
      "info": {
        "id": "G003",
        "publish_name": "白象",
        "alias_name": [
          "Chinastrats",
          "Patchwork",
          "Sarit",
          "Quilted Tiger",
          "Dropping Elephant",
          "APT-C-09",
          "Monsoon"
        ],
        "target_industry": [
          "政府",
```


安天下一代威胁检测引擎输出结果

应用效果--更好的效用性

文件HASH：7c498b7ad4c12c38b1f4eb12044a9def

- **卡巴斯基输出** Backdoor.Win32.Agent.mytihl
- **ESET输出** Win32/Poison.NOL
- **安天下一代威胁检测引擎配合情报平台的输出结果**

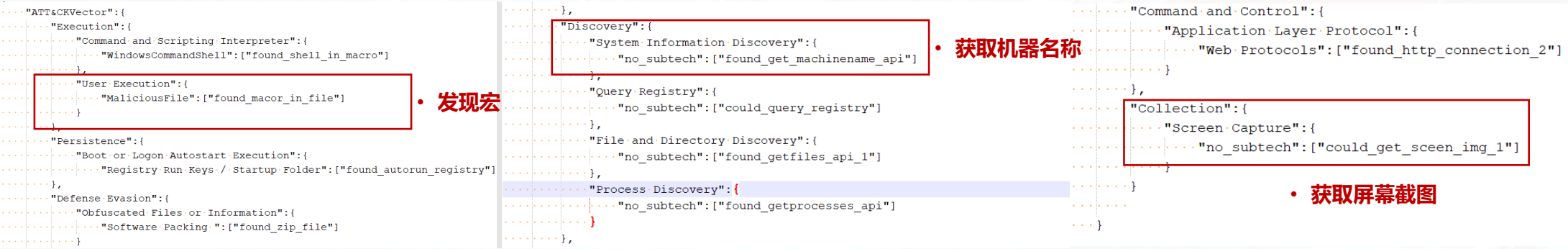
组织名称：绿斑
别名：APT-C-01，毒云藤
攻击目标：中国
攻击领域：政府,军事,科研
攻击方式：钓鱼邮件，水坑攻击
活跃时间：2011年,2012年,2013年,2014年,2017年
利用漏洞
CVE-2012-0158,CVE-2014-4114,CVE-2017-8759,CVE-2017-0199
组织简介
2018年9月安天实验室曝光了绿斑组织，该组织至少从2007年开始活跃，擅长对目标实施鱼叉攻击和水坑攻击、植入修改后的ZXShell、Poison Ivy、XRAT商业木马，并使用动态域名作为其控制基础设施。

普通引擎仅能将其认定为商马，安天的引擎可以依靠情报判断出该样本从属绿斑组织

文件属性信息
文件格式：PE文件
文件版本信息
文件名：avwsc.exe
产品名：AntiVir Desktop
公司名：Avira GmbH
文件结构信息
导入表哈希：
F93AFE4A0FB30B1293FCAA32DDAF59F1
时间戳：1325650785
身份信息
上线ID：motices
上线密码：ps135790
互斥体：)!qacA.I1
解密信息
解密偏移=0x628B 解密方式=异或 密钥=0x22

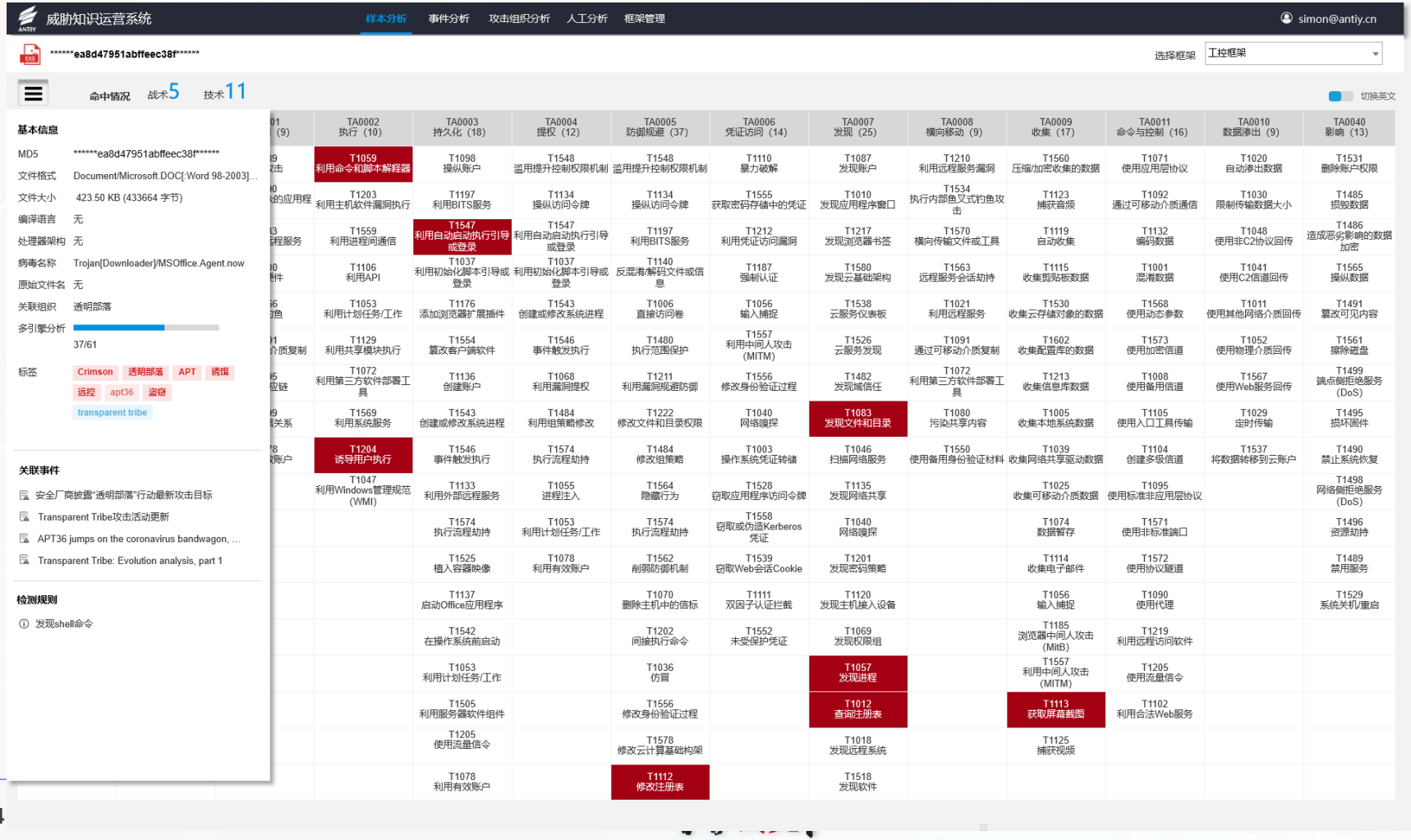
安天引擎输出向量映射ATT&CK案例

- 透明部落向量提取实例



- 发现宏
- 获取机器名称
- 获取屏幕截图

安天引擎输出向量映射ATT&CK案例



架：细粒度对抗

安天引擎输出向量映射ATT&CK案例

- 海莲花向量提取实例

```
"ATT&CKVector":{
    "Execution":{
        "Command and Scripting Interpreter":{
            "PowerShell":["found_powershell_command_execution"],
            "WindowsCommandShell":["found_cmd_exe_c"]
        },
        "User Execution":{
            "MaliciousFile":["found_macor_in_file"]
        }
"Persistence":{
    "Boot or Logon Autostart Execution":{
        "Registry Run Keys / Startup Folder":["found_autorun_registry"]
},
"Defense Evasion":{
    "File and Directory Permissions Modification":{
        "Linux and Mac File and Directory Permissions Modification":["found_chmod_x_command"],
        "Modify Registry":["could_set_registry"]
    }
},
```

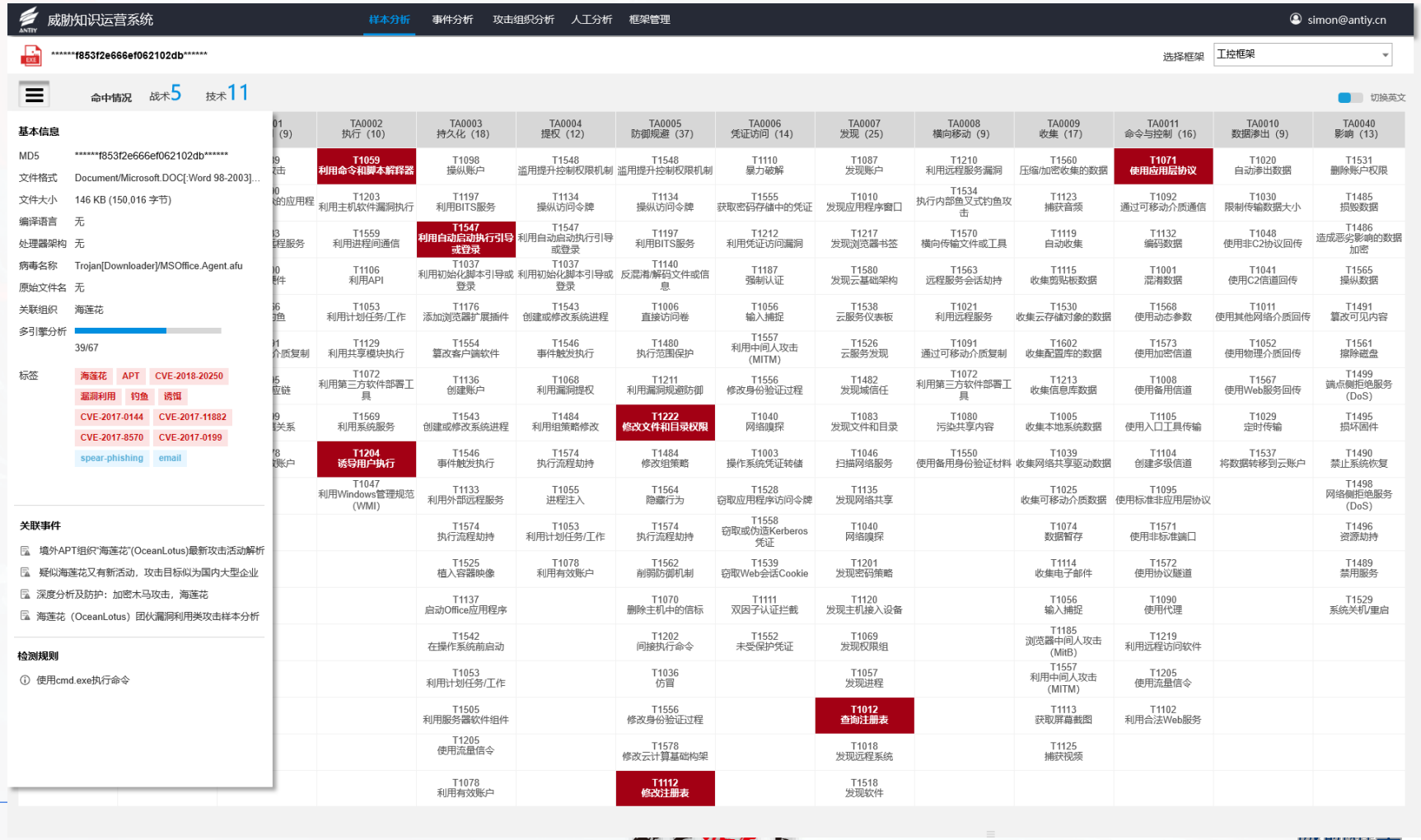
- 发现cmd.exe

- 修改注册表

```
"Discovery":{
    "System Information Discovery":{
        "no_subtech":["query_env_computername"]
    },
    "Query Registry":{
        "no_subtech":["could_query_registry"]
    }
},
"Command and Control":{
    "Application Layer Protocol":{
        "Web Protocols":["found_http_connection"]
    }
}
```

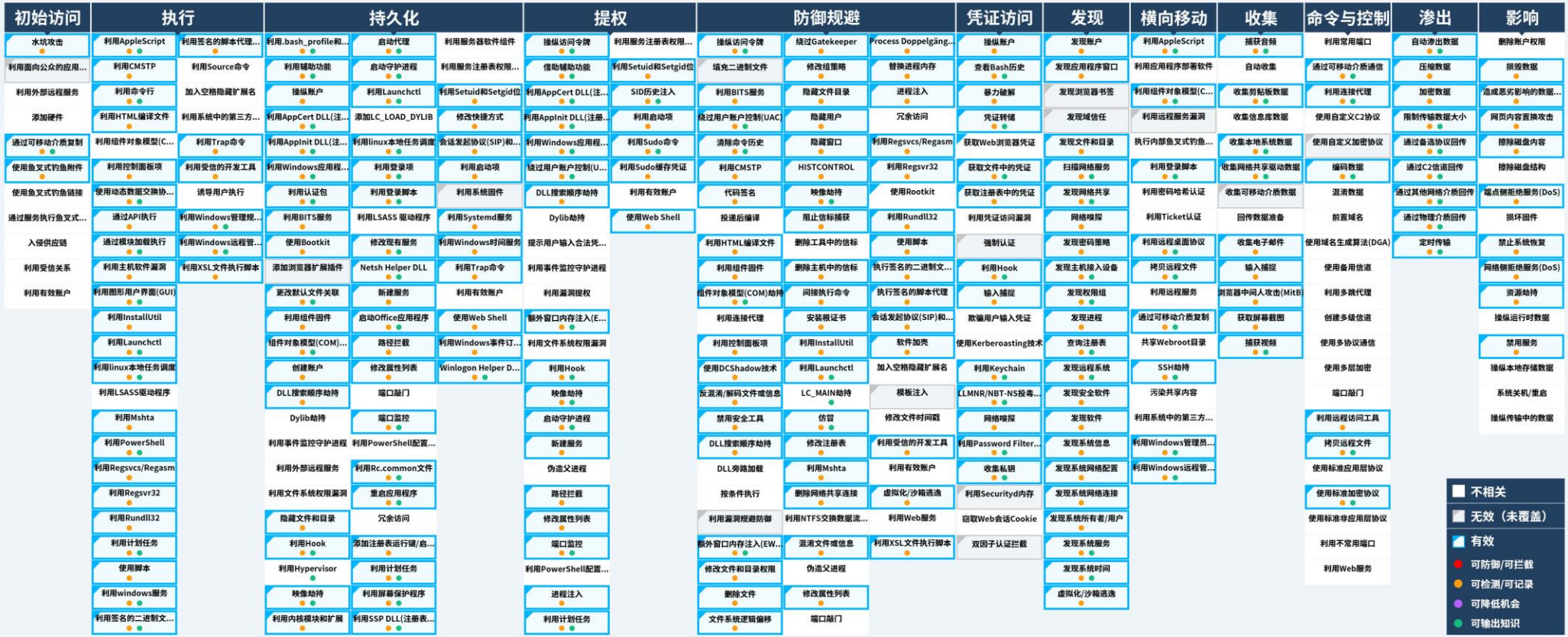
- 查询注册表

安天引擎输出向量映射ATT&CK案例



威胁框架：细粒度对抗

安天引擎映射ATT&CK框架的意义



智者安天下

威胁框架：细粒度对抗

03 应用案例

适用场景

- 可以在所有可嵌入安天AVLSDK威胁检测引擎的场景下工作，主要面向对高级威胁检测有需求的用户、面向监管型用户、面向合作伙伴。

· 检测产品

形成针对于攻击者的控制通道、传输通道的检测及拦截能力，在**流量检测监测**设备上提升威胁检测的深度。

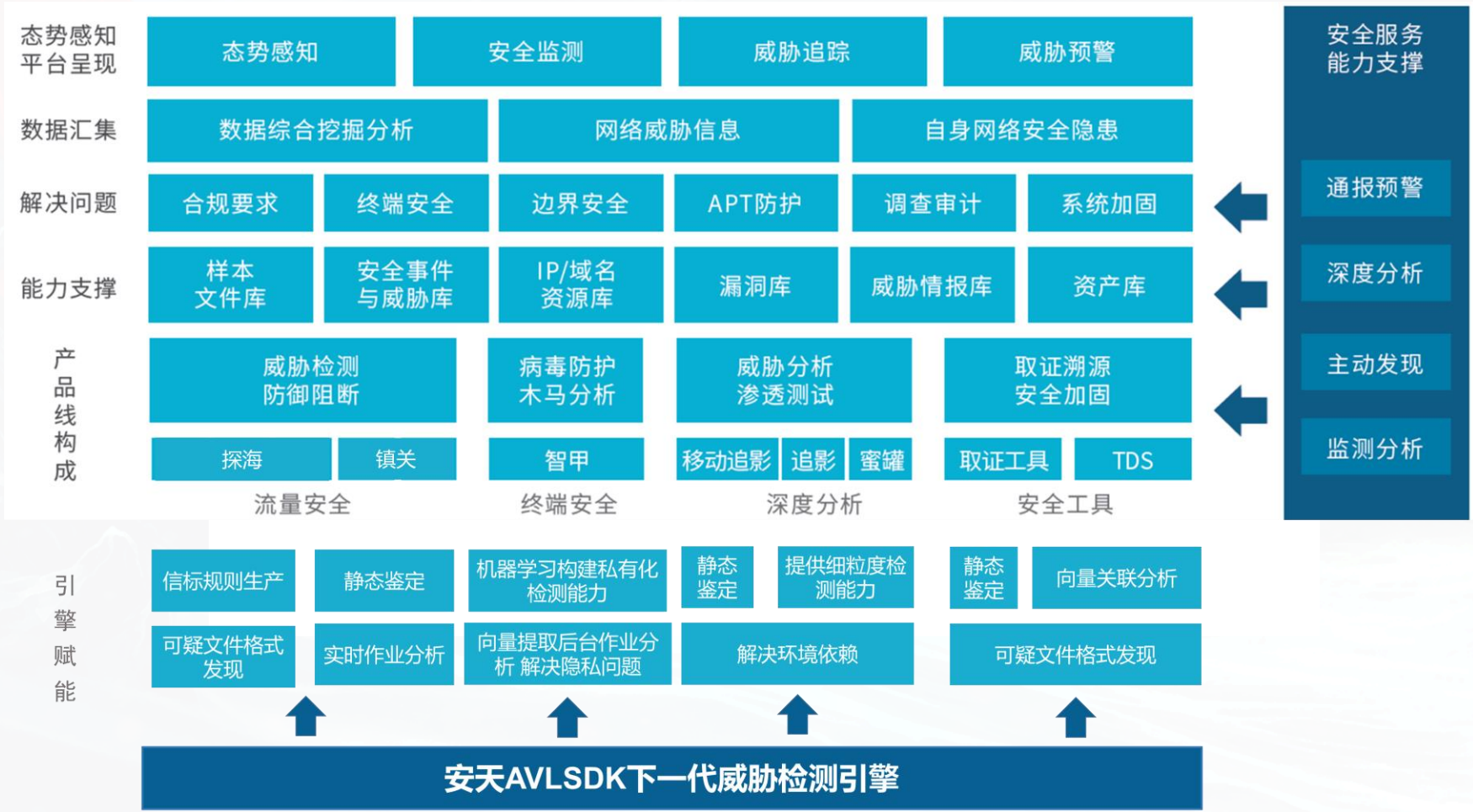
· 分析产品

形成有效判定能力，其知识化的输出可以让分析人员**快速了解威胁**，使分析人员聚焦于高等级威胁攻击载荷深入分析层面。

· 人工分析作业

精准的检测结果也可以让安全运维人员从海量威胁事件中**快速定位高等级威胁**，知识化的输出能力可以让其理解威胁并快速进行进一步的响应。

安天下一代威胁检测引擎对安天全线产品的支撑



震网样本实例—引擎输出结果

安天下一代引擎对震网样本输出信息

震网样本实例—安天追影分析系统产品界面

APT攻击组织"方程式"情报分析报告

组织信息　意图及目标　攻击活动　技术战术过程

①组织信息

方程式(Equation Group)

性质：超高能力国家/地区行为体　　别名：Equation/方程式/方程式集团/EquationGroup

归属地：美国　　成员：未知

首次公开：2015-02-16 00:00:00　　最后活跃：2019-12-20 14:48:20

组织描述：方程式组织是具有美国背景的超高能力国家/地区行为体，又名Tilded Team、Equation Group等，由卡巴斯基于2015年2月16日首次披露，是一个活跃了近20年的攻击组织。该组织主要针对伊朗、中东、中国、印度、俄罗斯、德国、西班牙、韩国等国家/地区，针对工业控制系统、SWIFT服务提供商、核工业、教育、政府、金融、科研、运营商、网络安全等行业进行破坏、修改、窃密、监视等攻击行动。该组织主要采用零日漏洞利用、U盘摆渡攻击、数十种罕见品牌硬盘固件修改、攻击载荷原子化、多种加密算法、安全软件规避、持久化等攻击手法，利用的漏洞涉及CVE-2010-2568、CVE-2011-3402、CVE-2015-2360、打印机后台程序服务漏洞（MS10-061）、快捷方式文件解析漏洞（MS10-046）、RPC远程执行漏洞（MS08-067）等，使用EquationLaser、EquationDrug、DoubleFantasy、TripleFantasy、Fanny、GrayFish等攻击装备。

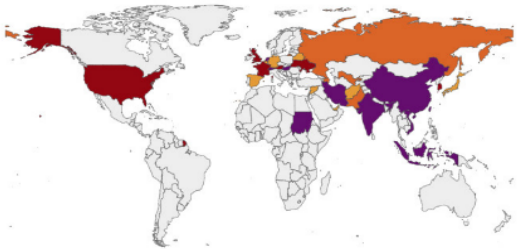
标签：方程式　APT

研究报告：2019-06-01　"方程式组织"攻击SWIFT服务提供商EastNets事件复盘分析报告　https://www.antiy.cn/research/notice&report/research_report/20190601.html

2017-01-26　安天图解方程式组织权术式主机作业　https://www.antiy.cn/research/notice&report/research_report/663.html

②意图及目标

"方程式"组织主要针对伊朗、中东、中国、印度、俄罗斯、德国、西班牙、韩国等国家/地区，针对工业控制系统、SWIFT服务提供商、核工业、教育、政府、金融、科研、运营商、网络安全等行业进行破坏、修改、窃密、监视等攻击行动。其攻击意图包括窃密、破坏、获取系统信息、系统破坏、修改可编程逻辑控制器（PLC）的代码、窃取机密信息、修改数据、物理影响、收集信息、修改硬盘固件、隐藏、窃取信息、修改PLC、监视、控制、间谍、间接活动、收集受害主机信息、获取基础设施等。



③攻击活动

研究人员发现了2014年出现的恶意软件Stuxnet新组件，这揭示了参与Stuxnet恶意软件的早期开发的第四个组织。此次发现的Stuxshop新模块与另一种名为Flowershop的恶意软件家族与存在关联，Stuxshop是一个旨在提供基本C&C和登记计划功能的模块，此外所发现的新版本Stuxnet的Duqu 1.5、Flame 2.0也与Flowershop存在关联。Flowershop于2015年被发现，它与泄露方程式工具Territorial Dispute（TeDi）有关。

载荷分析：

④威胁分析

MD5:	2BDA3159666B29BF6F912A69B9325435	威胁名称：	Worm/Win32.Stuxnet
组织信息：	方程式 方程式组织是一个美国的超高能力国家行为体，又名Tilded Team、Equation Group等，由卡巴斯基于2015年2月16日首次披露，是一个活跃了近20年的攻击组织。该组织主要针对伊朗、中东、中国、印度、俄罗斯、德国、西班牙、韩国等国家/地区。		
框架信息：	Tided	工具组件：	Stuxnet Dropper
威胁描述：	震网Dropper样本，搜索.stub节，解密并执行,该节包含Stuxnet DLL文件，该节包含Stuxnet DLL文件，这个DLL包含了stuxnet的所有功能。同时，该文件还被用作用户模式rookit，用于隐藏stuxnet文件。具有挂钩API行为。		
标签：	Stuxnet　APT　Dropper　Equation　释放文件　Rootkit　Hook　Shellcode		
情报向量拓展：	关键字：Dropper 其他：.stub		

⑤战术技术过程

战术技术过程

MITRE ATT&CK

初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向运动	收集	命令控制	渗漏	对抗
		T1179 挂钩	T1179 挂钩	T1140 反混淆/解码文件或信息 T1014 Rootkit	T1179 挂钩					T1022 数据加密	

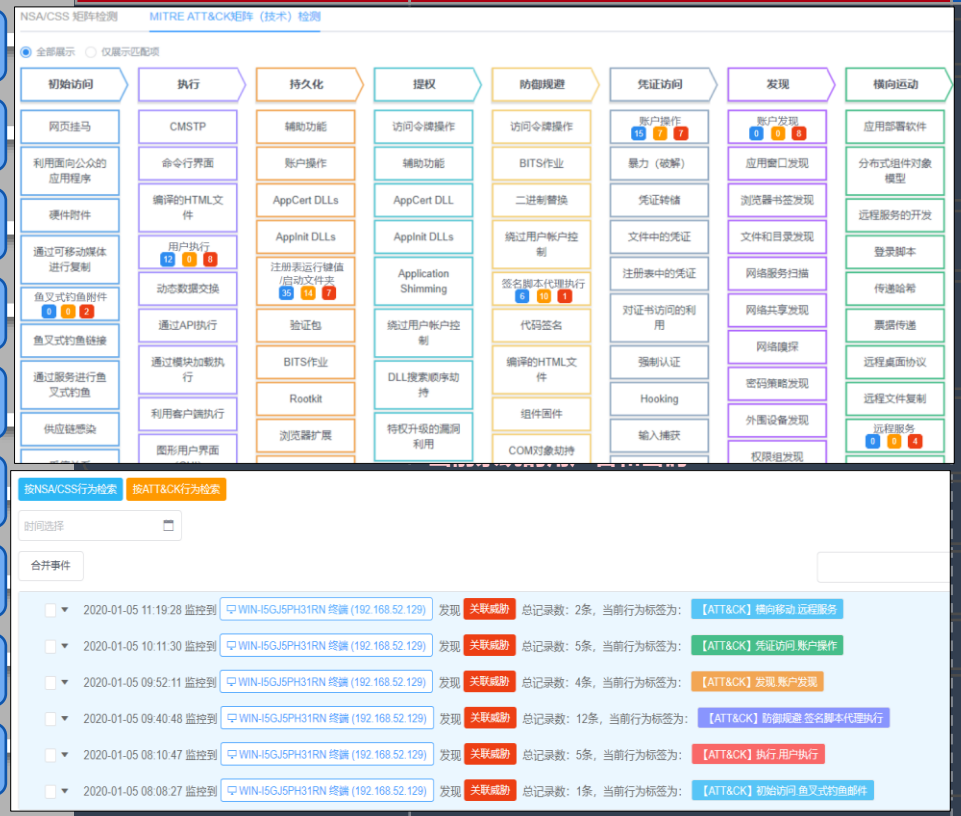
安天 智者安天下

智者安天下

威胁框架：细粒度对抗

安天智甲融合威胁框架后的防御过程演示

战术环节	攻击动作	攻击技术	输出标签	防御技术
初始访问	鱼叉式钓鱼附件	T1193	T1193鱼叉式钓鱼附件	用户接收附件时 检测附件
执行	脚本	T1064	T1064脚本	检测邮件附件是否 包含SFX自解压文件 文件防御，解压时释放文件到启动目录，检测该文件
防御规避	用户执行 绕过用户帐户控制	T1204 T1088	T1204用户执行 T1088绕过用户帐户控制	进程防御，EXPLORER启动文件时对启动文件进行检测
发现	系统时间发现 系统信息发现 系统所有者/用户发现	T1124 T1082 T1033	T1124系统时间发现 T1082系统信息发现 T1033系统所有者/用户发现	监控系统敏感API调用，包括：GetSystemInfo、GetSystemTime 监控 系统敏感API调用，GetUserName
凭证访问	凭证转储	T1003	T1003凭证转储	进程监控，PowerShell执行参数检测，脚本文件检测
横向移动	远程服务	T1021	T1021远程服务	网络链接监控，敏感端口向内网高频横向扩散行为检测，敏感端口向本机恶意入侵检测
持久化	注册表运行键值/启动文件夹	T1060	T1060注册表运行键值/启动文件夹	创建启动项检测
凭证访问	Hooking	T1179	T1179 Hooking	内存存在异常钩子
命令控制	标准应用层协议 数据加密 自定义命令和控制协议	T1071 T1022 T1094	T1071标准应用层协议 T1022数据加密 T1094自定义命令和控制协议	进程联网情况检测 CMD执行命令及参数



攻击者操作

安天智甲终端防御系统已完成主流攻击动作到ATT&CK的映射和标签化输出

安天智甲处置

谢谢大家