威胁情报和检测引擎结合有效提升安全防护能力

安天研究院威胁情报部

長纓待展

CONTENTS

目 录

01 威胁情报的应用现状和挑战

威胁情报的内容和标准

【概念定义】威胁情报是一种基于证据的知识，包括了情境、机制、指标、隐含和实际可行的建议。威胁情报描述了现存的、或者是即将出现针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。

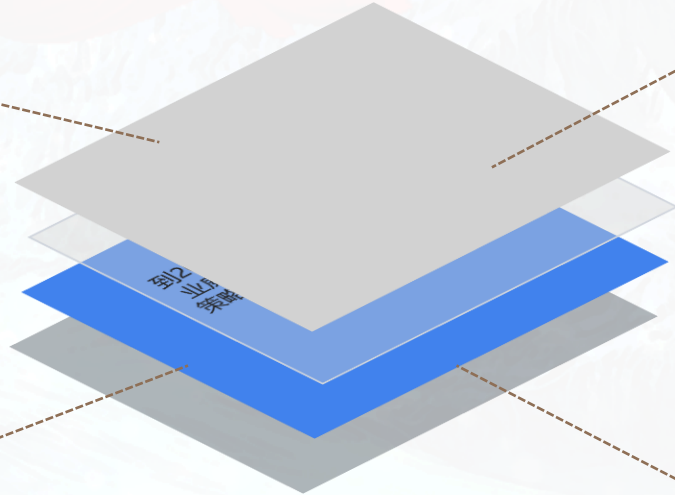
---- Gartner，2013年

威胁情报应包括安全威胁相关的五方面信息：

- 上下文（context）：亦可理解为条件或环境，指具体威胁存在的环境或起作用的场景。
- 机制（mechanism）：指情报所涉及威胁所采用的方法和途径。
- 指标（indicator）：主要指威胁目前是否正在作用于目标的识别特征。
- 可能结果（implication）：指威胁可能对目标造成的破坏性结果。
- 可操作建议（actionable advice）：指可用于指导安全人员采取措施阻止或避免被威胁影响的有效建议。

威胁情报的使用价值

Gartner：2020年，超过15%的大型企业将使用商业威胁情报（TI）服务来告知其安全策略

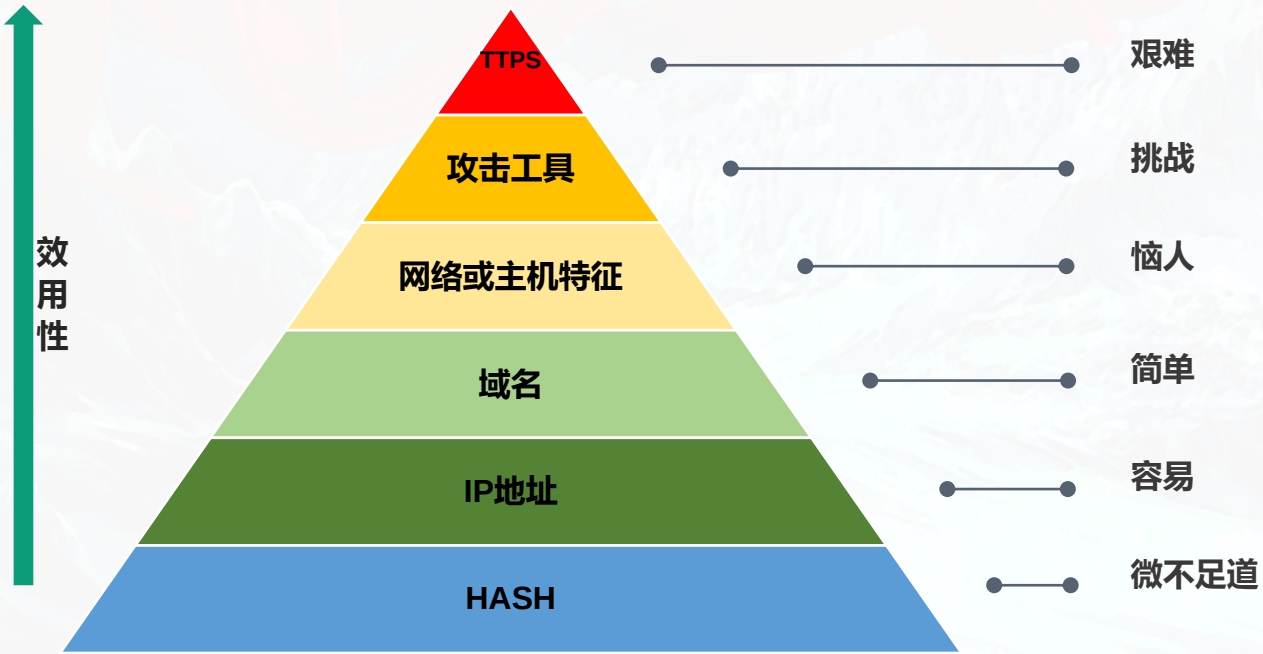


如何跟得上包括恶意攻击、攻击方法、安全漏洞、黑客目标等等在内的如潮水般海量的安全威胁信息?

如何向决策层报告具体安全威胁的危险、影响和处置?

面对未来的安全威胁，如何获取更多的主动?

威胁情报应用面临挑战



威胁情报的痛苦金字塔

- 高级威胁检测能力不足
- 威胁信息输出不够
- 高效应用困难
- 集成难度高

应用中的挑战： ① 提升高级威胁的检测能力

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。

扫描了解详情

——《对Stuxnet蠕虫攻击工业控制系统事件的综合分析报告》

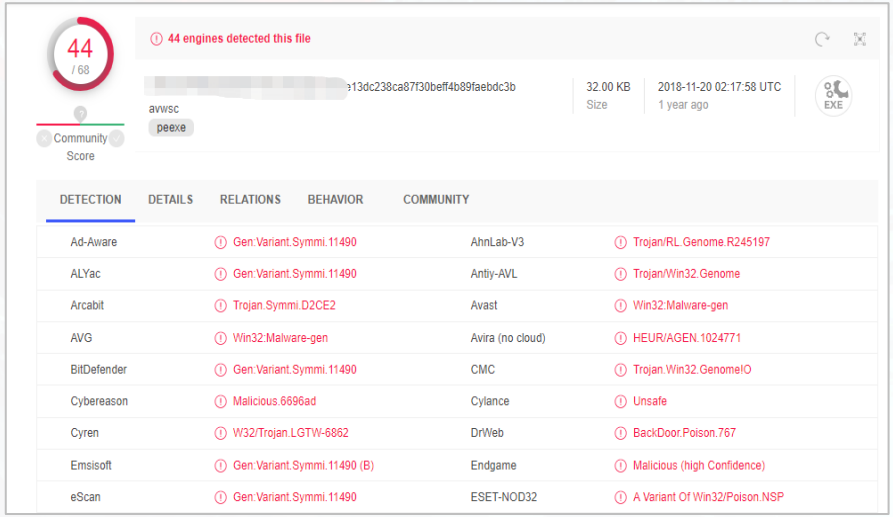
震网样本集差异分析

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

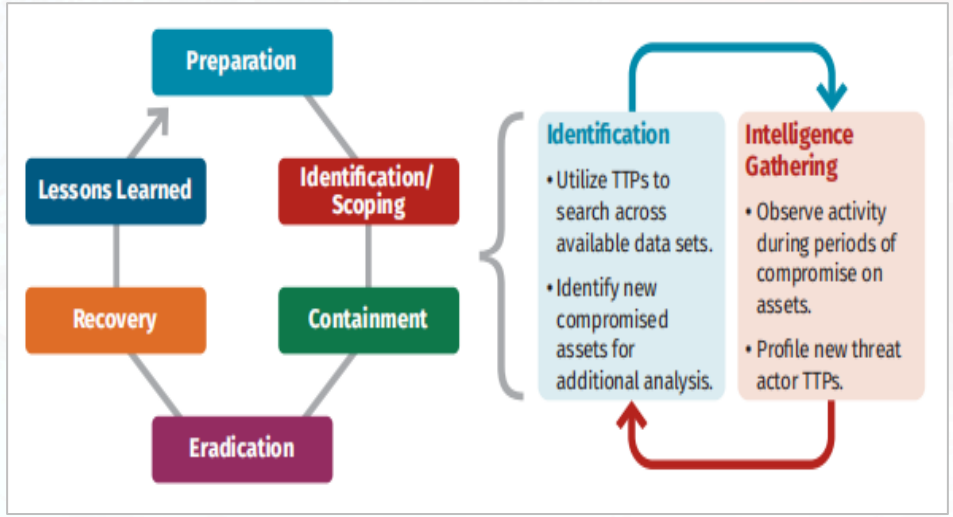
样本1	样本2	异同	原因
BF6E9CBCDA5EF33EBA2EBECC4EBFC493	F6E836E6397437A8DCFE213E33525F1F	时间戳相同，代码段，导入表Hash均不同，但代码对比一致	输出文件类型不同，EXE和DLL
F48F28C1539DFC439FD2C4B353E55514	F6E836E6397437A8DCFE213E33525F1F	时间戳、导入表HASH、代码段HASH相同，文件HASH不同	Stub包裹内容不同
02BC5EDC93859B2ECE717CE24ED186D5	3B8EA5381D81C64E07CFA1FC09ECC87E	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
31E2FD7A131B719B703BB6F4C362BB8A	C77CB014E6694DAD2D4AC9259FC12D8E	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
0C8AB2873E139981AFF77ECEF3744603	98FBEBD8883021FBE6464C37ACF17938	时间戳、导入表HASH相同，代码段HASH不同	无关代码0xFF填充
C77CB014E6694DAD2D4AC9259FC12D8E	5A379BB1480DE8E2396E7DD29634C458	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
0B5FD57A4F7008698CA60F71F330CFA3	3867ABE7E8F9659C49F6486C6E66AC9F	除时间戳外其余均相同	

应用中的挑战： ② 提升威胁信息丰富性，支撑安全运营

- 有效安全运营，需要快速的响应；需要合理的归并、排序、及其依据
- 相对较少的检测结果输出，无法支撑有效的安全运营决策



VirusTotal网站对某高级威胁样本的检测结果

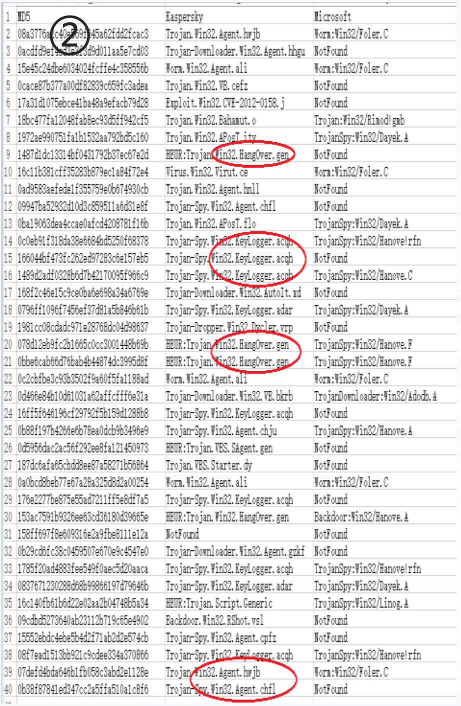


SANS — 《具备DDI可见性的增强事件响应》

应用中的挑战：②提升威胁信息丰富性，支撑安全运营

提升威胁识别能力，有助于避免遗漏重要威胁

某白象分析报告



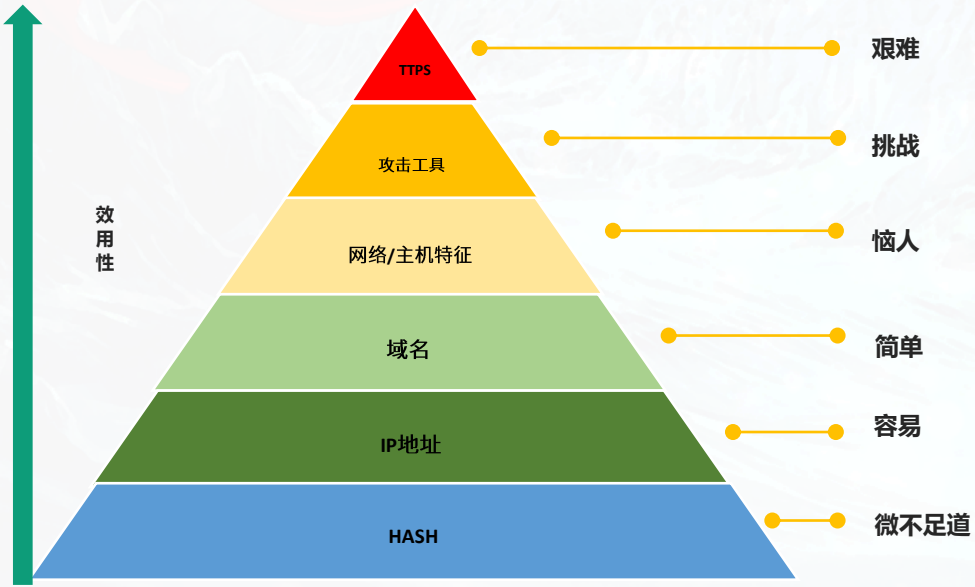
各反病毒引擎厂商检测结果

安天威胁检测引擎输出结果

扫码查看《白象的舞步——来自南亚次大陆的攻击

应用中的挑战： ③有效的威胁情报，应用困难

威胁情报规则目前集中在痛苦金子塔的下层，其效用性较低。



威胁情报痛苦金字塔

FireEye红队工具失窃事件跟进分析

时间： 2020年12月14日 来源： 安天CERT

1.概述

火眼公司（FireEye）红队工具失窃事件曝光后，安天CERT迅速跟进，发布《FireEye红队工具失窃事件分析和思考》[1]（点击查看），报告中以威胁框架视角对失窃的工具进行了功能点评，回顾了历史上多起网络军火失窃和扩散事件，并对本次事件做出谨慎地分析猜测。随着针对该事件的深入分析，安天CERT重新梳理了本次失窃工具对应的ATT&CK能力映射图谱，并对相应的能力进行评估与研判。

安天CERT利用FireEye的开源虚拟机测试套件CommandoVM线索与公开的规则对样本库进行扫描筛选，梳理了一些疑似FireEye的失窃工具并结合情报对工具进行初步分类：基于开源项目的工具、基于内置Windows二进制文件的工具（利用白文件实现免查杀功能的工具）、FireEye红队自研工具以及目前未确认的部分工具。其中自研工具包括侦查工具、持久化工具、内存转储工具、恶意宏模板工具以及利用D语言、Golang、C#等语言编写的后门程序。安天CERT对其中FireEye的部分自研工具进行了分析并评估可能产生的影响，同时针对部分相关规则使用了小规模白名单集合测试其误报率和规则质量。

扫描了解详细

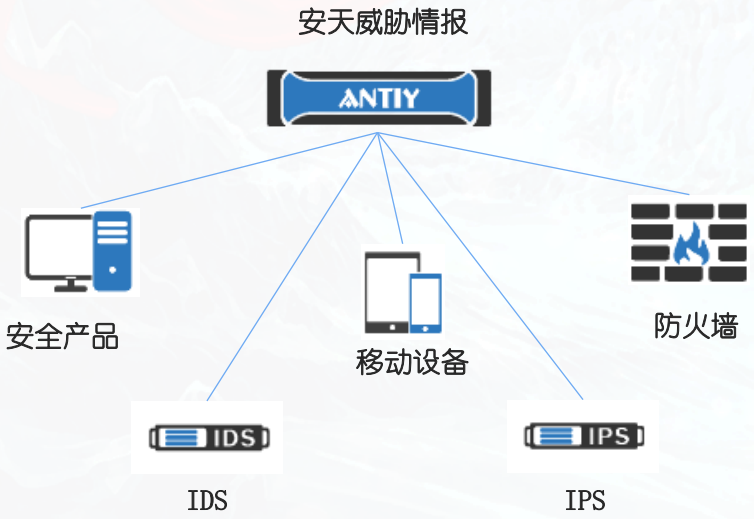
Yara规则

Snort规则

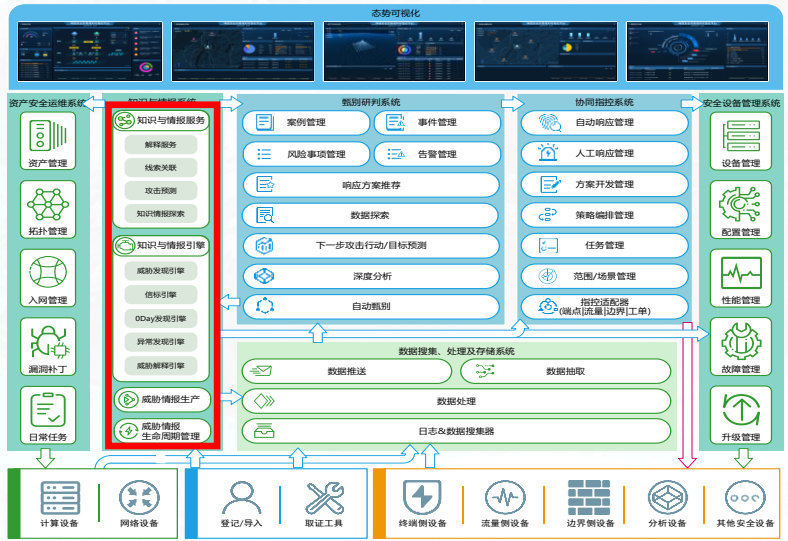
```
# Copyright 2020 by FireEye, Inc.
# You may not use this file except in compliance with the license. The license should
have been received with this file. You may obtain a copy of the license at:
# https://github.com/fireeye/sunburst_countermeasures/blob/main/LICENSE.txt
alert tcp $HOME_NET any -> any 443 (msg:"Backdoor.BEACON"; content:"|16 03 03|";
depth:3; content:"inconeupdate.com"; sid:77600840; rev:1;)
```

应用中的挑战： ④ 降低整合难度

情报集成安全产品



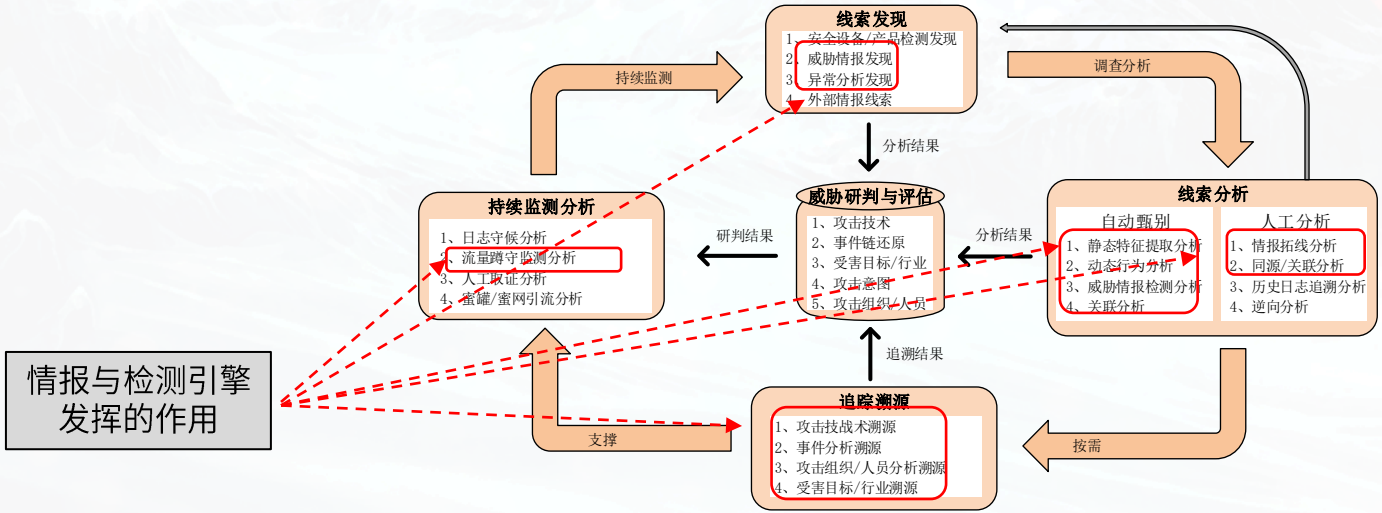
情报集成态势感知系统



02 威胁情报和检测引擎结合的实践

总体思路：情报与监测引擎结合，赋能全环节安全运营

- 结合恶意代码的动静态深度分析，**生产更深度的情报**
- 面向高级威胁行为体的情报融合，**关联整编更具价值的情报**
- 针对重要威胁的人机结合分析 ，**提升预警和响应支撑能力**



针对常规威胁，全量格式解析，支撑威胁分析和潜在威胁发现

全格式识别解析

✓ **格式识别能力**

可识别文件格式：286类，3500余种（包含小版本）

可执行文件: 39 ;　　包裹: 21

文档: 25　　媒体文件:32

✓ **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）

✓ **格式解析能力**

文档类：DOC，XLS，PPT，PDF，RTF ...；　媒体文件：SWF 等

可执行文件：Microsoft.PE[:X86]，　Microsoft.MSIL，Linux.ELF 等

✓ **解包：压缩包，自解压包，安装包等共计40类**

对于各种包的解析，使引擎能够更精准的定位到包中真正恶意的文件。

✓ **脱壳：加密壳、压缩壳等30+种**

对主流样本格式解析的深入解析，在方便检测的同时，也便于引擎提取尽可能多的向量。

细粒度行为向量提取

静态向量

- **行为**
  IP，URL，自启动
  信息获取，对抗
  传播，控制，隐藏
  窃取，欺骗.....
- **API**
  模块相关操作
  网络访问相关
  文件基本操作
  进程基本操作
  .....
- **文件结构**
  导入导出表
  编译器信息
  数字签名
  .....

远控静态配置解密

IP，URL，MAIL，DOMAIN.....
手机号、QQ号、身份ID.....

数字签名

证书信息：颁发者，使用者，有效期，算法
签名信息：证书链，签名人名字，签名时间
判定标签：伪造，吊销，过期，证书不完整.....

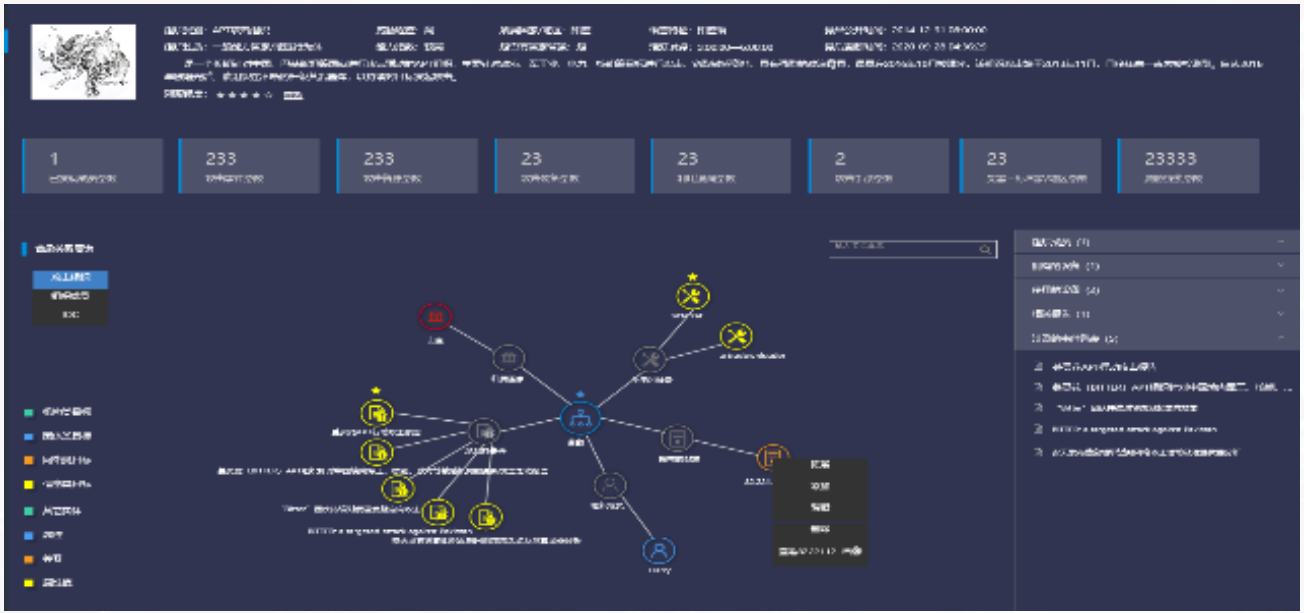
针对重点威胁，恶意代码动静态结合、生产更深度的情报信息

动静态结合深度分析

行为揭示与情报生产

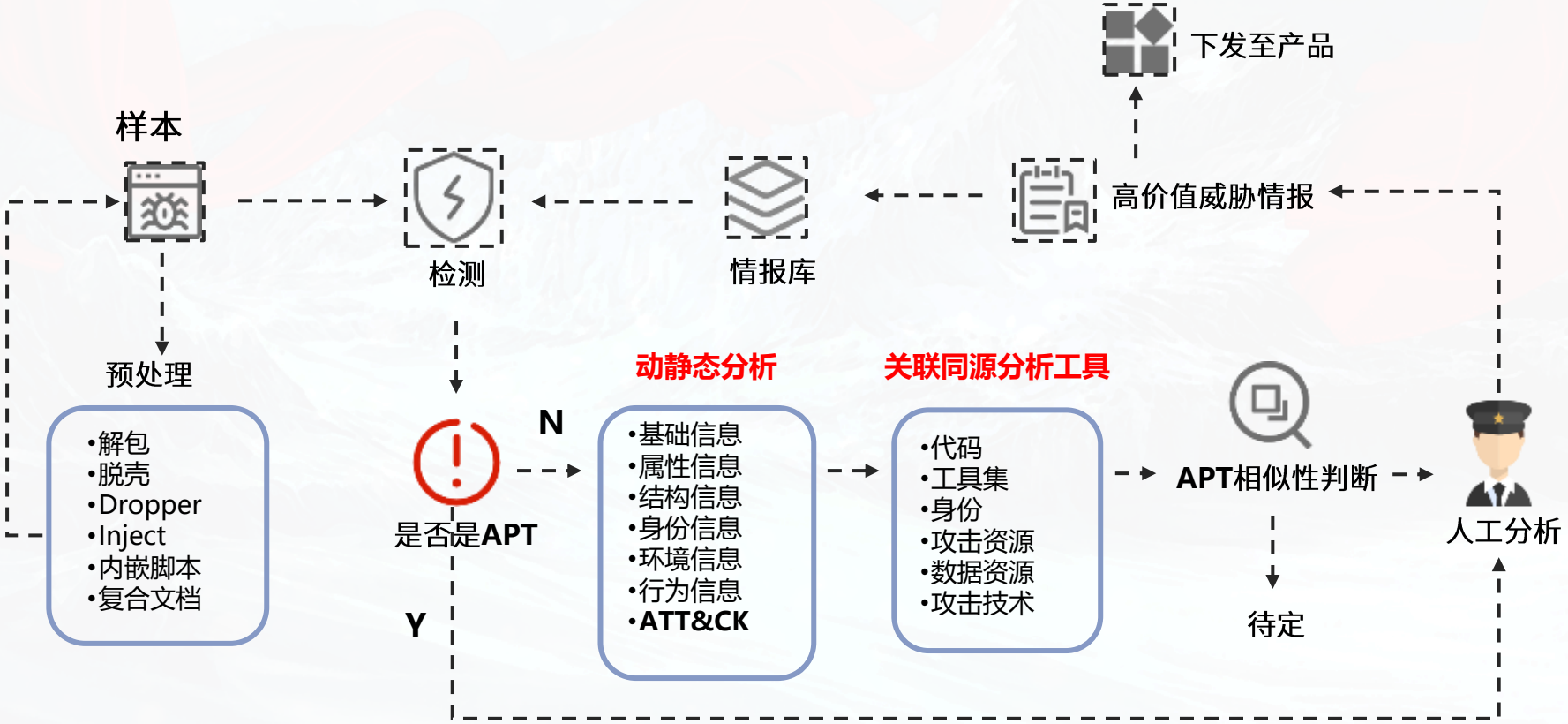
- **行为揭示：**涵盖文件（58）、进程（52）、注册表（41）、网络（104）、服务（18）、系统（43）、反调试（3）、证书（5）、剪贴板（5）、加解密（23）、设备（3）、浏览器（9）、office（11）、内存（3）、网络管理（10）、flash（3）、其他（32）
- **行为分析规则：**覆盖网络类（52）、注册表类（322）、进程类（288）、文件类（84）、其他（369）等类别行为分析规则
- **行为关联：**关联识别APT攻击事件150+；可检测超过600种远控程序；对域名的检测特征数量超过160万，对IP的检测特征超过10万，对URL的检测特征超过20万
- **威胁框架覆盖：**覆盖ATT&CK 176个技术点
- 支持API调用日志、截图、衍生文件、进程内存DUMP等的输出

针对高级威胁行为体，融合整编更具价值的信息

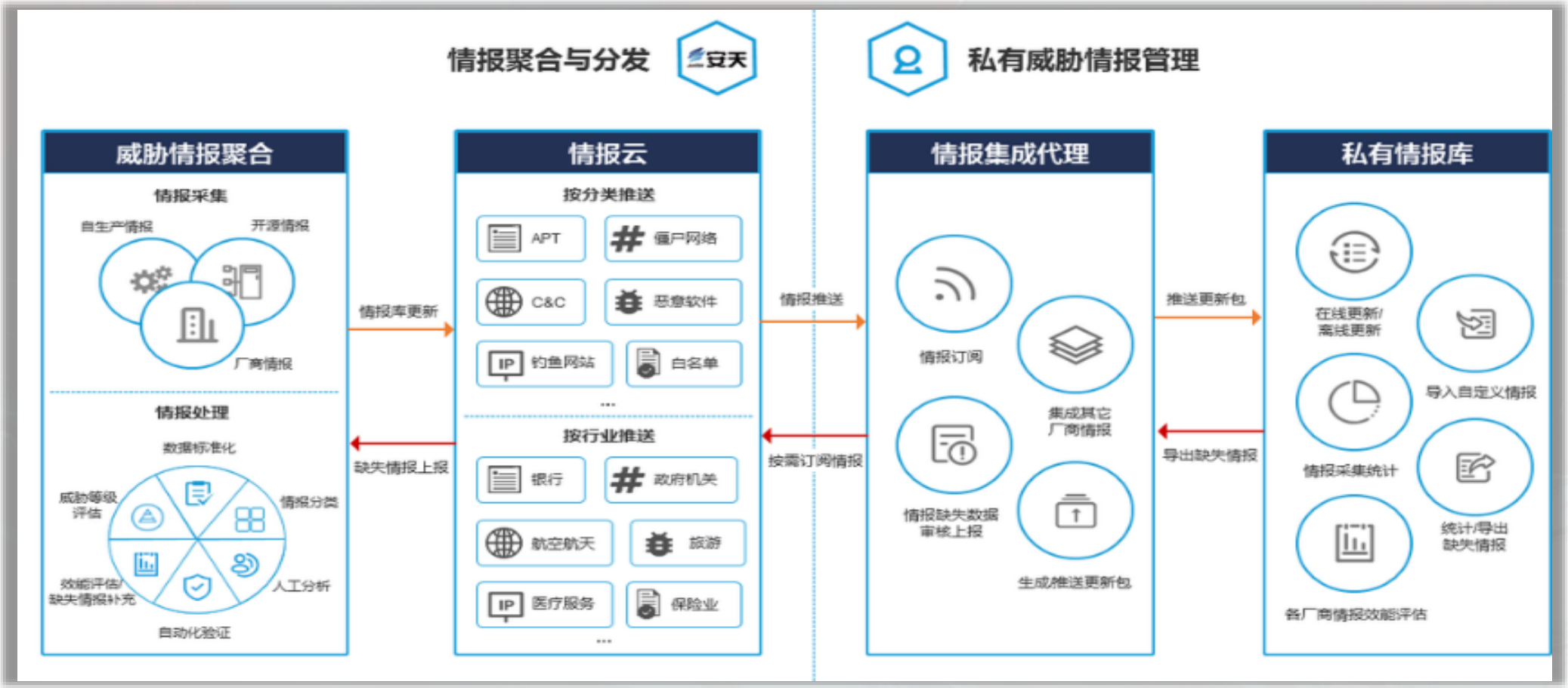


- 持续跟踪分析近**300**个攻击组织
- 涉及**30**多个国家
- 累计生产可机读**IOC**数量**12w+**
- 跟踪发现**2000+**篇**APT**攻击分析报
- 自主发现或进行深度分析并公开发布的**30**左右篇报告
- 其中包括方程式组织、白象、“绿斑”组织、幼象组织、APT-TOCS(海莲花)、响尾蛇、Stuxnet(震网)、DUQU(毒曲)、Flame、沙虫组织、Darkhotel组织、FIN6组织等

面向追踪溯源，提供多种溯源手段



客户侧的多源情报聚合管理



威胁情报和检测引擎结合的适用场景

安天的高价值威胁情报可以在所有嵌入安天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

部署方式	服务方式	使用者	使用目的
独立使用	情报系统	分析人员	了解攻击相关上下文，分析安全事件间的关联
数据对接	分析系统	业务系统日志	威胁发现
安全产品对接	引擎SDK	安全产品	威胁防御
集成流量探针	情报规则	安全设备	威胁检测

检测

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

自动分析

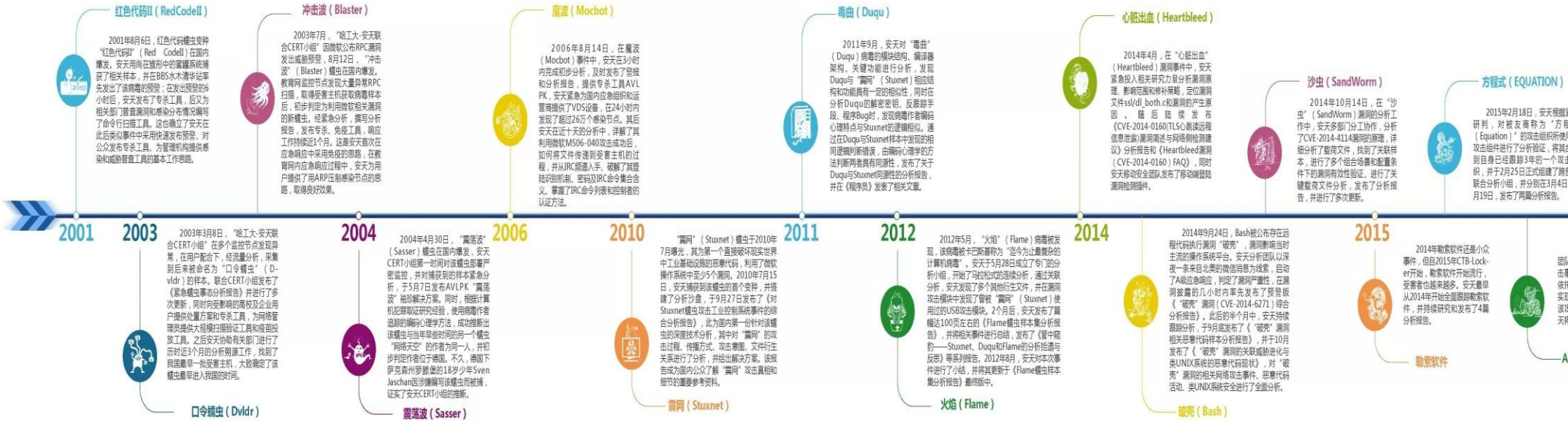
形成有效判定能力，其知识化的输出可以让分析人员快速了解威胁，使分析人员聚焦于高等级威胁攻击载荷深入分析层面

人工分析

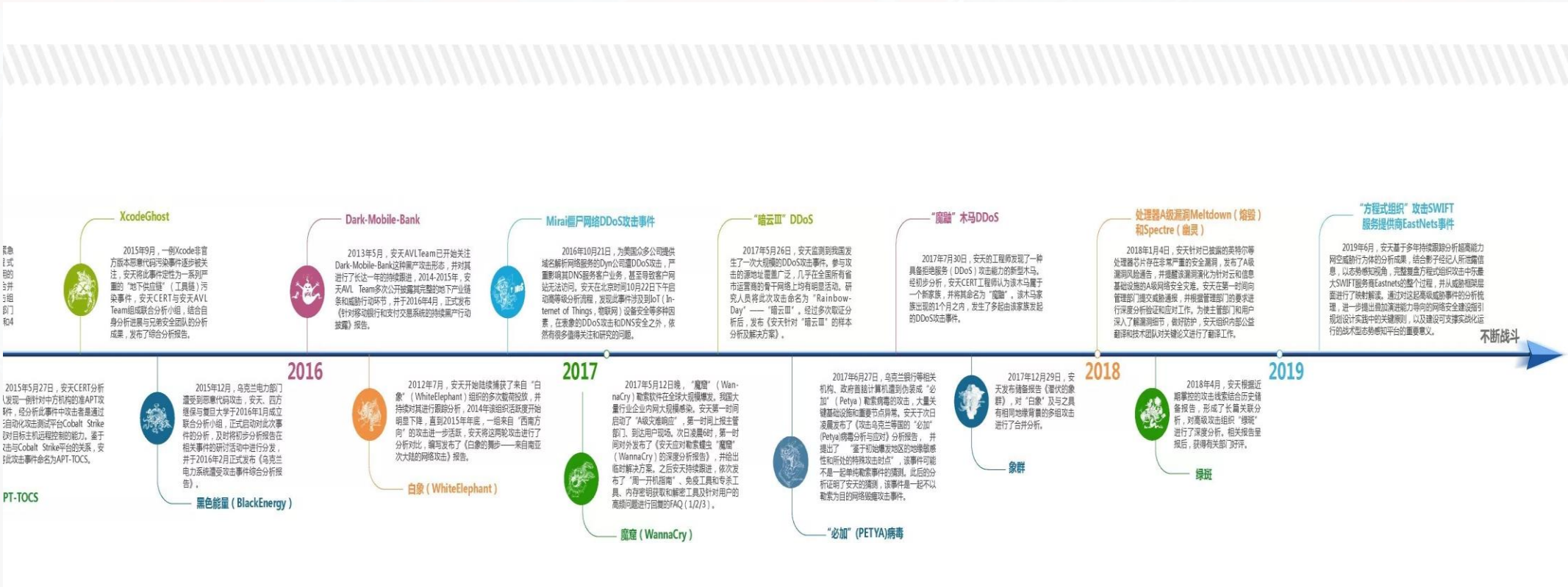
精准的检测结果也可以让安全运维人员从海量威胁事件中快速定位高等级威胁，知识化的输出能力可以让其理解威胁并快速进行进一步的响应

高级威胁分析能力支撑的威胁情报

安天重大事件应急响应与深度威胁分析历程



高级威胁分析能力支撑的威胁情报

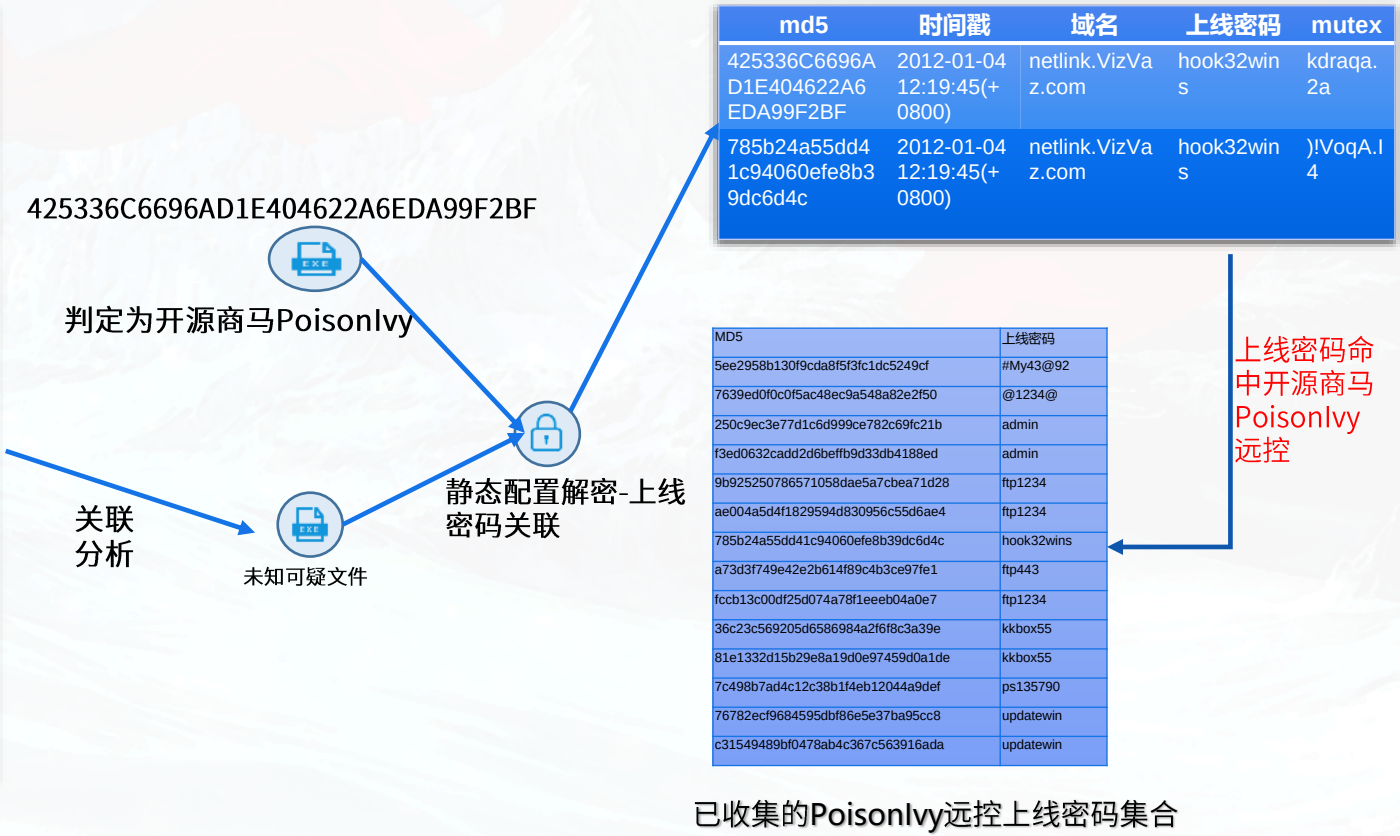


03 应用效果

威胁检测提升
攻击者识别
追踪溯源
威胁预警

威胁检测能力提升：①恶意样本检测能力提升

原始文件名	B53sd.exe
MD5	785b24a55dd41c94060efe8b39dc6d4c
处理器架构	Intel 386 or later, and compatibles
文件大小	32.00 KB (32768 bytes)
文件格式	Win32 EXE
加壳类型	NO
编译语言	Microsoft Visual C++
互斥量	)!VoqA.I4
密码	hook32wins
备注	可疑文件



威胁检测能力提升：②IP/域名检测能力提升

域名	revoltmax.com
域名解析IP	178.162.210.245
域名注册	munna.bhai124@gmail.com
注册者	Remax
电话号码	+1.6505434800
注册国家	US
城市	Menlo Park
检测结果	未知
备注	

域名	解析域名	注册邮箱	威胁类型	备注
revoltmax.com	178.162.210.245	munna.bhai124@gmail.com	远控C2地址	关联发现的威胁
outlookkz.com	95.211.205.164	munna.bhai124@gmail.com	远控C2地址	已知威胁

相同注册邮箱关联
远控C2地址

域名	IP	注册邮箱	威胁类型
revoltmax.com	178.162.210.245	munna.bhai124@gmail.com	远控C2
blingblingg.com	178.162.210.246	munna.bhai124@gmail.com	远控C2
eyescreem.com	95.211.205.166	munna.bhai124@gmail.com	远控C2
outlookkz.com	95.211.205.164	munna.bhai124@gmail.com	远控C2
dailychina.news	178.162.210.247	munna.bhai124@gmail.com	远控C2
asiandefnetwork.com	178.162.210.248	munna.bhai124@gmail.com	远控C2
xbladezz.com	178.162.210.243	munna.bhai124@gmail.com	远控C2
xmachinez.com	178.162.210.242 46.165.229.9	munna.bhai124@gmail.com	远控C2

收集和关联的远控C2地址集合

攻击者识别： ①通过C&C线索，对攻击者进行识别

MD5	url	威胁名称	首次发现时间	攻击目的	格式
****afa191824042 1b0a2749c2a3e24e	http://111.90.158.225/d/ft32	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/6	挖矿	BinExecute/Linux.ELF[:X86]
****cf699252377b4e477357e4bf8e63	http://111.90.158.225/d/ft32	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/9	挖矿	BinExecute/Linux.ELF[:X86]
****9fc3561e94051998d11381a00bbd	http://111.90.158.225/d/ft64	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/7	挖矿	BinExecute/Linux.ELF[:X64]
****543e84f19f49bcec27313600845e	http://111.90.158.225/d/ft64	RiskWare[RiskTool]/Linux.BitCoinMiner.n	2018/11/9	挖矿	BinExecute/Linux.ELF[:X64]
****25f47dd6c62077cf52aeb5a759e7	http://111.90.158.225/d/mn32.exe	RiskWare[RiskTool]/Win32.BitMiner.gen	2018/11/6	挖矿	BinExecute/Microsoft.EXE[:X86]
****8045df750419911c6e1bf493c747	http://111.90.158.225/d/ft32	Trojan/Linux.CoinMiner.fd	2018/11/26	挖矿	BinExecute/Linux.ELF[:X86]
****a18d7949bcfc2b0928cfd8683478	http://111.90.158.225/d/ft32	Trojan/Linux.CoinMiner.fd	2018/12/15	挖矿	BinExecute/Linux.ELF[:X86]
****8a6c72c06d1892132d5e1d793b4b	http://111.90.158.225/d/fast.exe	Trojan/Win32.Occamy.c	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****8a6c72c06d1892132d5e1d793b4b	http://111.90.158.225/d/ft.exe	Trojan/Win32.Occamy.c	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****bbef96b8507715dc4d975e7f8f5f	http://111.90.158.225/d/ft.exe	Trojan/Win32.Occamy.c	2018/12/13	刷广告/刷流量	BinExecute/Microsoft.EXE[:X86]
****994a8f2fd5af2961166c8c456b6d	http://111.90.158.225/d/srv.exe	Trojan/Win32.Occamy.c	2018/12/14		BinExecute/Microsoft.EXE[:X86]
****74e871bce1df442b73bf927f1f39	http://111.90.158.225/d/mn64.exe	Trojan/Win32.Satan	2018/11/4		BinExecute/Microsoft.EXE[:X64]
****a336185bc2141f9c92a59a918c26	http://111.90.158.225/d/srv.exe	Trojan/Win32.Satan	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****2bc458d9e94e8fabfc8402cd2b78	http://111.90.158.225/d/srv.exe	Trojan/Win32.Skeeyah.a	2018/11/9		BinExecute/Microsoft.EXE[:X86]
****ee0187c61d8eb4348e939da5a366	http://111.90.158.225/d/conn32	Trojan[Exploit]/Linux.LuckyRansom	2018/11/18	勒索	BinExecute/Linux.ELF[:X86]
****a1dd0b7bb17a816c18cce18cdbc6	http://111.90.158.225/d/conn.exe	Trojan[Exploit]/Win32.ShadowBrokers.ae	2018/11/4		BinExecute/Microsoft.EXE[:X86]
****bbda5f7c02ca179a366232adbb96	http://111.90.158.225/d/conn.exe	Trojan[Exploit]/Win32.ShadowBrokers.ae	2018/11/16		BinExecute/Microsoft.EXE[:X86]
****4b74ee538dab998085e0dfaa5e8d	http://111.90.158.225/d/cry32	Trojan[Ransom]/Linux.LuckyRansom	2018/11/24	勒索	BinExecute/Linux.ELF[:X86]
****4e763a527f3ad43e9c30acd276ff	http://111.90.158.225/d/cpt.exe	Trojan[Ransom]/Win32.Crypmod.aatb	2018/11/24	勒索	BinExecute/Microsoft.EXE[:X86]

组织名称:Outlaw
归属国家:未知
组织性质:黑产组织
攻击意图:获取经济利益(挖矿+勒索)
攻击手法:漏洞利用、利用web shell等
影响平台:Linux
目标国家/地区:美国、欧洲
目标行业:金融行业、汽车行业等
利用漏洞:CVE-2016-8655、CVE-2016-5195
IOC指标:
http://111.90.158.225/d/ft32 (远控C2)

- 多平台开发能力 ------> 适应不同环境
- 持续不断的维护更新 ------> 以勒索、挖矿为目的
- 攻击目的多样 ------> 通过不断维护更新攻击载荷避免被检测

以获取经济利益为主要目的，技术能力强，有组织，有分工的黑客团伙

攻击者识别：②提取更多情报信息，进行威胁排查

组织名称:白象

别名:Monsoon、摩诃草、Patchwork、Dropping Elephant

归属国家:印度

组织性质:一般能力国家/地区行为体

攻击意图:窃取敏感数据

攻击手法:鱼叉式钓鱼、水坑攻击、0day漏洞利用、社会工程学等

影响平台:Windows、Android、macOS等

目标国家/地区:中国、巴基斯坦等

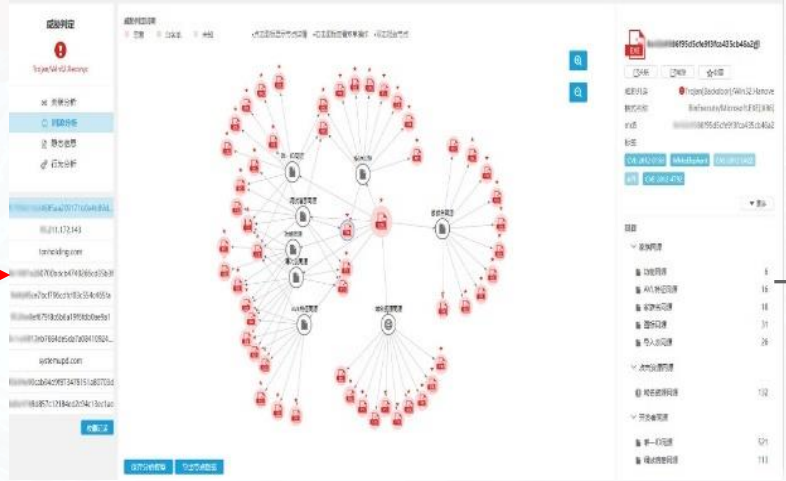
目标行业:政府、军事、教育等

利用漏洞:CVE-2017-0199、CVE-2017-8570等

攻击装备: HangOver、 DarkCometRAT、Quasar RAT、 Badnews等

IOC信息:1000+恶意样本、200+恶意URL

威胁排查



排查线索

用于排查恶意代码HASH值:

00a0a6071c335f78c161cb4a3dcdc435
00bd9447c13afbbb7140bef94e24b535
0128f683e508c807ec76d5092eaaf22c
01774e34e8a444685b1499eef3406cd0
01a7af987d7b2f6f355e37c8580cb45a
01adea2d3707a343f5a6d149565c7ec5

用于排查的恶意IOC:

activetalk.org
add-on-update.com
addon-updates.com
adminassistance.net

基于安天威胁检测引擎的向量输出能力
将白象象群的攻击工具聚合在一起

追踪溯源： ①未知攻击来源威胁样本，提取情报信息（C2）

原始文件名	xwizard.exe
MD5	02b2d905a72c4bb2abfc278b8ca7f722
文件大小	226.50 KB (231936 bytes)
文件格式	Win32 EXE
加壳类型	NO
编译语言	Microsoft Visual C++
时间戳	2015-12-01 09:25:33
请求网络地址	tonholding.com
备注	可疑文件

网络上搜索到的信息不包含工具载荷的Hash信息

1.工具信息

年份	国家	行业	恶意软件
2014	越南	网络安全	WINDSHIELD
2014	德国	制造业	WINDSHIELD
2015	越南	媒体	WINDSHIELD
2016	菲律宾	消费品	KOMPROGO WINDSHIELD SOUNDBITE BEACON
2016	越南	银行	WINDSHIELD
2016	菲律宾	技术基础设施	WINDSHIELD
2016	中国	医院	WINDSHIELD
2016	越南	媒体	WINDSHIELD
2016	美国	消费品	WINDSHIELD PHOREAL BEACON SOUNDBITE
2017	英国	咨询	SOUNDBITE

103.53.197.202	104.237.218.70	104.237.218.72
185.157.79.3	193.169.245.78	193.169.245.137
23.227.196.210	24.datatimes.org	80.255.3.87
blog.docksugs.org	blog.panggin.org	contay.deaftone.com
check.paidprefund.org	datatimes.org	docksugs.org
economy.bloghop.org	emp.gapte.name	facebook-cdn.net
gap-facebook.com	gl-appspot.org	help.checkonl.org
high.expbas.net	high.vphelp.net	icon.torrentart.com
images.chinabytes.info	imaps.qki6.com	img.fanspeed.net
job.supperpow.com	lighpress.info	menmin.strezf.com
mobile.pagmobiles.info	news.lighpress.info	notificeva.com
nsquery.net	pagmobiles.info	paidprefund.org
push.relasign.org	relasign.org	share.codehao.net
seri.volveri.net	ssl.zin0.com	static.jg7.org
syn.timeizu.net	teriava.com	timeizu.net
tonholding.com	tulationeva.com	untitled.po9z.com
update-flashs.com	vieweva.com	volveri.net
vphelp.net	yii.yiihao126.net	zone.apize.net

2.已知APT组织海莲花的公开信息和相关C&C信息列表

追踪溯源： ②基于C2信息，进行关联拓线，溯源到海莲花组织

追踪溯源

组织名称:APT-TOCS

别名:海莲花、 Cobalt Kitty 、 APT32 等

归属国家:越南

组织性质:一般能力国家/地区行为体

攻击意图:窃取敏感数据

攻击手法:鱼叉式钓鱼、水坑攻击、0day漏洞利用、社会工程学等

影响平台:Windows、 linux、Android、macOS等

目标国家/地区:中国、 ，柬埔寨、马来西亚等

目标行业:外交、政府、军事、教育等

利用漏洞: CVE-2017-11882、CVE-2017-8570等

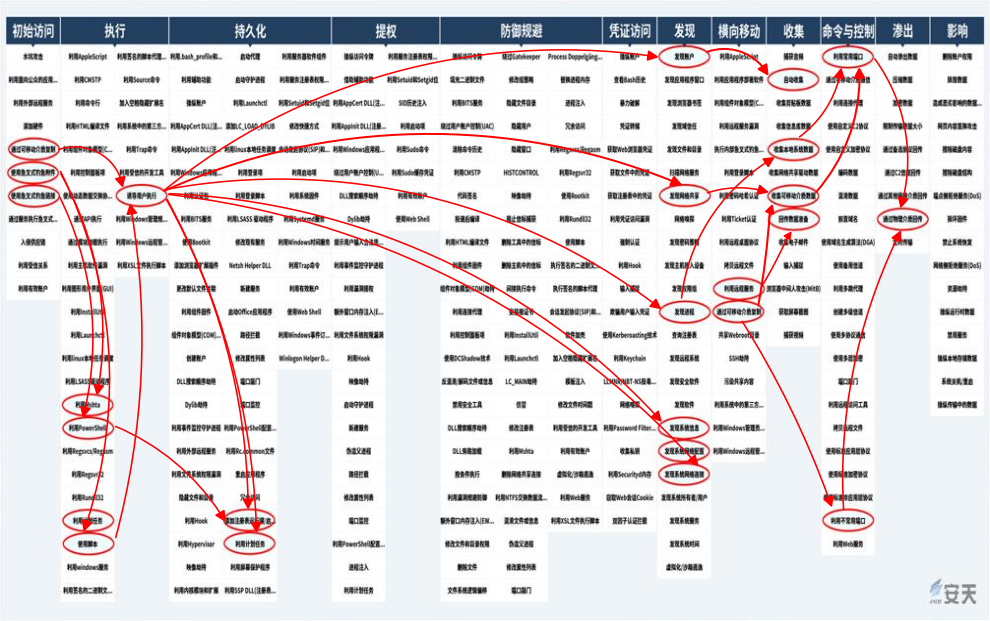
攻击装备: Cobalt Strike、DenesRAT、Mimikatz等 Quasar RAT、 Badnews等

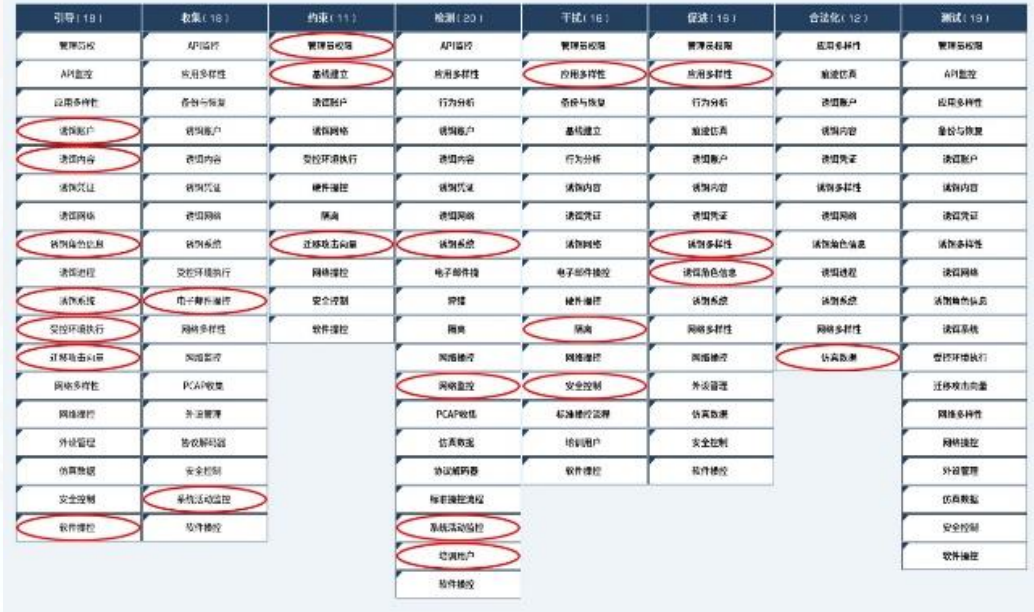
追踪溯源：③ 提取更多情报信息，进行威胁排查

威胁排查

样本MD5	文件路径	来源主机
0529b1d393f405bc2b2b33709dd57153	%SystemRoot%\System32\PlaySndSrv.dll	10.255.30.2
071528cc2401b8abdc878d609a8e60d5	%windir%\System32\control.exe	10.255.30.5
01b0b1418e8fee0717cf1c5f10a6086b	%appdata%\\mobsync.exe	10.255.30.34
05a08c3d6cf0855d16372c197424d824	%SystemRoot%\System32\PlaySndSrv.dll	10.255.44.23
018433e8e815d9d2065e57b759202edc	%windir%\System32\control.exe	10.255.45.24
0acae009a682a7f387018d29f896306a	%windir%\System32\control.exe	10.255.45.30

追踪溯源：④基于ATT&CK，分析差距，制定对抗方案





威胁预警：FireEye红队工具失窃事件的威胁预警

- 2020年12月8日，火眼公司（FireEye）在其官方网站发布公告称，“高度复杂的威胁行动者”攻击了其内网并窃取了用于测试客户网络的红队（Red Team）工具。
- 红队（Red Team）工具可以模拟多个威胁行为活动进行安全测试评估。
- 红队泄露的工具合计60款,包括开源项目工具、基于内置Windows二进制文件的工具、自研究工具以及其他未确认工具
- 本次被窃工具对应的ATT&CK能力映射图谱，覆盖了ATT&CK威胁框架12个战术阶段中的10个，可以实现118个技术动作。
- 为了防止潜在攻击者利用被窃取的红队工具进行网络攻击，针对Snort、Yara、ClamAV和OpenIOC等开源安全检测框架，公开发布了300多种对策，包括29个Snort规则文件、164个Yara规则文件、23个ClamAV规则文件、88个OpenIOC规则文件等。

威胁检测

高误报规则识别

漏洞预警

基于TTP提升防护能力

谢谢大家