



网络空间威胁对抗与防御技术研讨会
暨 第八届安天网络安全冬训营

智者安天下

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

威胁框架：细粒度对抗

長纓縛展

从安天的安全引擎说起



- 生态合作伙伴突破**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**国家级安全内核**。

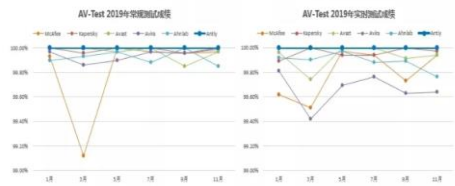
生态稳步发展

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



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	安天追踪威胁分析系统+安天深海威胁检测系统
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

安天引擎的2020

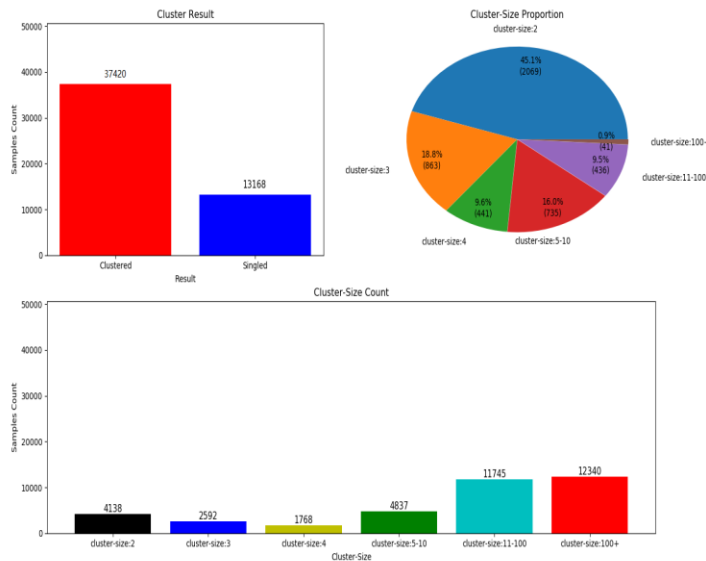


- AVLSDK已在全面实现对国产化主流操作系统和硬件架构的适配

- 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



PHYTIUM 飞腾



長纓待展

CONTENTS

目 录

01

威胁情报与知识库的当前问题

02

可结合知识库的威胁检测引擎

03

应用案例

智者安天下



长缨待展

威胁框架：细粒度对抗

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



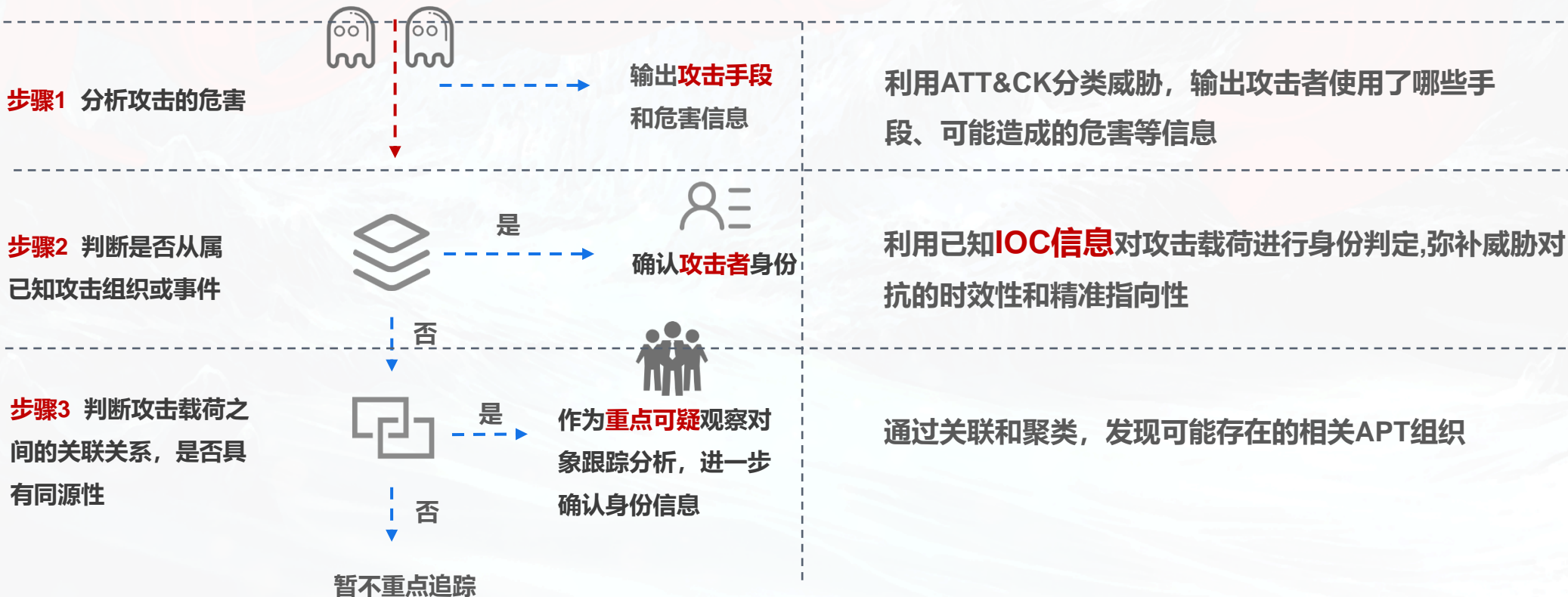
防御方的需求在变化

- 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

业界实现的方式



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**)



IOC信息
(IP、域名、Hash)

期望达成

发现、阻断和猎杀高级威胁行动



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。

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》

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
BF6E9CBCDA5EF3F6E836E63974	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
F48F28C1539DFCF6E836E63974	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
02BC5EDC93859E3B8EA5381D81	F6E836E63974	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
31E2FD7A131B71C77CB014E669	F6E836E63974	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
0C8AB2873E139998FBEBD88830	F6E836E63974	时间戳、导入表HASH相同, 代码段HASH不同	无关代码0xFF填充
C77CB014E6694C5A379BB1480C	F6E836E63974	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
0B5FD57A4F70083867ABE7E8F9	F6E836E63974	除时间戳外其余均相同	

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**。

44 / 68 engines detected this file

32.00 KB Size | 2018-11-20 02:17:58 UTC | 1 year ago

Community Score

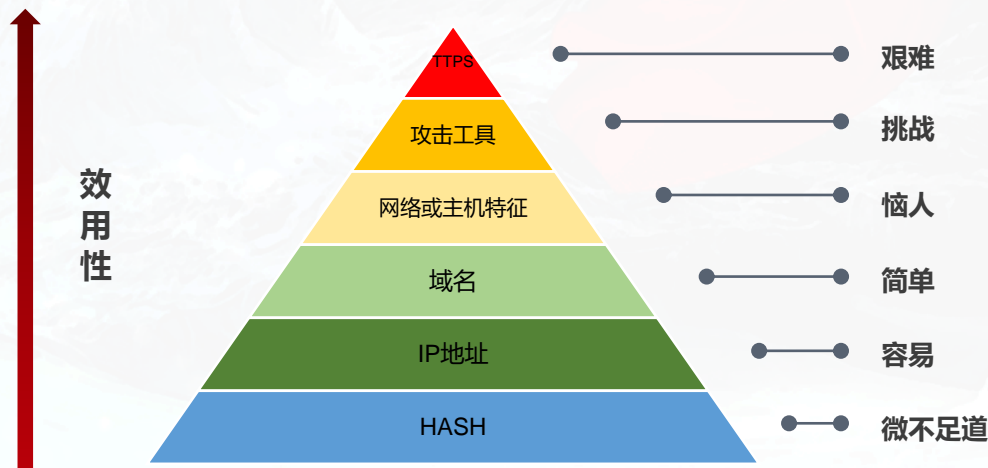
DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware		① Gen.Variant.Symmi.11490		AhnLab-V3 ① Trojan/RL.Genome.R245197
ALYac		① Gen.Variant.Symmi.11490		Antiy-AVL ① Trojan/Win32.Genome
Arcabit		① Trojan.Symmi.D2CE2		Avast ① Win32/Malware-gen
AVG		① Win32/Malware-gen		Avira (no cloud) ① HEUR/AGEN.1024771
BitDefender		① Gen.Variant.Symmi.11490		CMC ① Trojan.Win32.Genome!O
Cybereason		① Malicious.6696ad		Cylance ① Unsafe
Cyren		① W32/Trojan.LGTW-6862		DrWeb ① BackDoor.Poison.767
Emsisoft		① Gen.Variant.Symmi.11490 (B)		Endgame ① Malicious (high Confidence)
eScan		① Gen.Variant.Symmi.11490		ESET-NOD32 ① A Variant Of Win32/Poison.NSP

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

智者安天下



长缨待展

威胁框架：细粒度对抗

02

可结合知识库的威胁检测引擎

- 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

```
    "Vector_des": "the family of rat",
    "VecDict": {
      "VecContent": "family: DarkComet"
    },
    "VectorLabel": []
  },
  {
    "ThreatLevel": 1,
    "Vector_des": "the type of rat",
    "VecDict": {
      "VecContent": "type: pe"
    },
    "VectorLabel": []
  },
  {
    "ThreatLevel": 1,
    "Vector_des": "the network of rat",
    "VecDict": {
      "VecContent": "network: 2.tcp.ngrok.io:15944"
    },
    "VectorLabel": []
  },
  {
    "ThreatLevel": 1,
    "Vector_des": "the mutex of rat",
    "VecDict": {
      "VecContent": "mutex: DC_Mutex-UFXHUR2"
    },
    "VectorLabel": []
  },
  {
    "ThreatLevel": 1,
    "Vector_des": "the campaign ID of rat",
    "VecDict": {
      "VecContent": "campaign_ID: Sazan"
    },
    "VectorLabel": []
  },
  {
    "ThreatLevel": 1,
    "Vector_des": "the version of rat",
    "VecDict": {
```


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



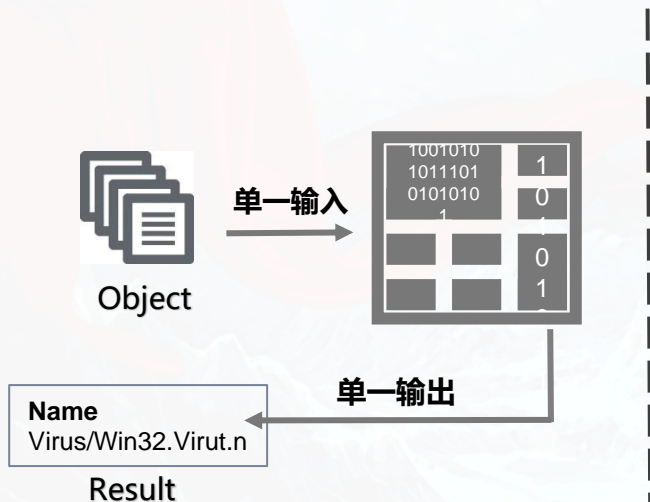
✓解包：压缩包，自解压包，安装包等共计40类



✓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



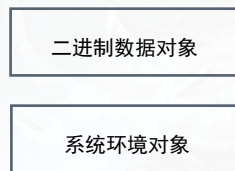
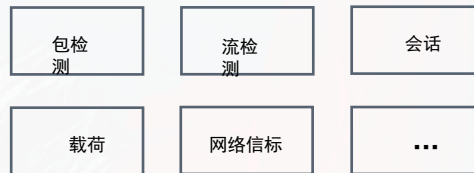
✓ 传统引擎

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。

网络层次检测



本地层次检测

多种输入

输出 1

- 黑白
 - 识别信息
 - 基础信息
- 多向量
 - 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@anty.cn

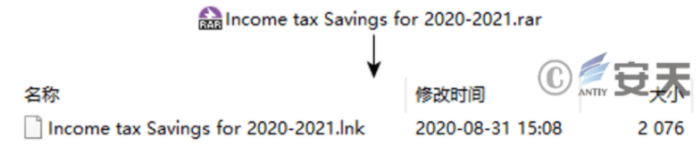
[上传报告](#) [上传样本](#)

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：漏阿文档+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](#)：



名称	修改时间	大小
Income tax Savings for 2020-2021.lnk	2020-08-31 15:08	2 076

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	569D721E44E1A31A53AEEA0E514AD794
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/莫灵花) | 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
莫灵花APT行动攻击报告	2016-11-15
莫灵花 (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



ANTY 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

样本: **0e92bf087ea41e49eeafeadb4c7dcca**

上传用户: simon@antiy.cn | 文件格式: BinExecute/Microsoft.EXE[X86] | 大小: 92.50 KB | 上传日期: 2020-12-12 | 分析次数: 5次 | 分析框架: ATT&CK

GeneralInfo	Certificate	{u'certificate': u'No digital signature'}
GeneralInfo	RichHeader	{u'CheckSum(Xor key)': u'0x070f06a4'}
GeneralInfo	RichHeader	{u'count': u'3', u'version': u'30729', u'id': u'0x5461', u'description': u'DLL import record in library file: VS2008 SP1 build 30729'}
GeneralInfo	RichHeader	{u'count': u'10', u'version': u'0', u'id': u'0x93', u'description': u'Import function count. Not necessarily accurate.'}
GeneralInfo	RichHeader	{u'count': u'11', u'version': u'40219', u'id': u'0x1', u'description': u'Total imports. Build 40219'}
GeneralInfo	RichHeader	{u'count': u'1', u'version': u'40219', u'id': u'0xae', u'description': u'Linker: VS2010 SP1 build 40219'}
GeneralInfo	PDBInfo	{u'VecContent': u'C:\cyrusis\Release\pdb\payload.pdb'}
GeneralInfo	CompilerInfo	{u'MajorLinkerVersion': u'10', u'MinorLinkerVersion': u'0'}
GeneralInfo	EntryPoint	{u'VecContent': u'0xa9d0'}
GeneralInfo	FuzzyHash	{u'TheFileFuzzyHash': u'1536:mBwl+KXpsqN5vhwYyhY9S4AjV1zNxCk7pZZac3+exc6M:Qv+asqN5aW/hLwKcNzCtXz'}
GeneralInfo	FuzzyHash	{u'text': u'768:bBNNi5pl+CVzfqXHKuAZTAr419saBgpwpB7+Evlw1wTg2AyQoR.bBwl+KXpsqN5vhwYyh'}
GeneralInfo	FuzzyHash	{u'rdata': u'192:dcl+LyzvblQusOo8Vdpk0rsJUfPKDKBmMnRKE9sfb8.GLe37usOo8Vd6cPKDKAKfb8'}
GeneralInfo	FuzzyHash	{u'data': u'768:KVQ+1uxk5x81e1YCD77pvd7pPacCPCRoA+emcJRC4TGbB:KV1zNxCk7pZZac3+exc6M'}
GeneralInfo	ImportHash	{u'VecContent': u'F86DEC4A80961955A89E7ED62046CC0E'}
GeneralInfo	FileFormat	{u'VecContent': u'BinExecute/Microsoft.DOS_PE_NE_LE[Gen]'
GeneralInfo	PESimilarityInfo	{u'VecContent': u'Disassembly_porportion:0.97'}
GeneralInfo	PESimilarityInfo	{u'VecContent': u'disassembly_instructions_cnt:12802'}
GeneralInfo	PESimilarityInfo	{u'VecContent': u'PE_Fingerprint_version:01000102'}
GeneralInfo	PESimilarityInfo	{u'VecContent': u'9E13B3EBE9E246B9B153BD822684668A'}
Execution	Command and Scripting Interpreter	{u'VecContent': u'found_cmd_exe'}
Execution	Execution through API	{u'VecContent': u'CreateProcess'}
Execution	Execution through Module Load	{u'VecContent': u'GetProcAddress'}
Persistence	Registry Run Keys / Startup Folder	{u'VecContent': u'found_autorun_registry'}

人工分析成果 提取向量 4 战术 5 技术 8 攻击组织 0 攻击事件 1

分析面板 分析历史

found_cmd_exe	2020-12-12	编辑
found_autorun_registry	2020-12-12	编辑
{u'VecContent': u'F86DEC4A80961955A89E7ED62046CC0E'}	2020-12-12	编辑
{u'VecContent': u'9E13B3EBE9E246B9B153BD822684668A'}	2020-12-12	提交

威胁判定: 恶意 关联组织: 白象 (WhiteElephant /白象/坠落的...

关联事件: 研究者发现Crysis勒索软件新变种 框架分析: 选择威胁框架

标签: 勒索软件 PDB信息 生成规则: 是的

备注: 勒索软件本体中解出的pdb路径

自动化关联分析

关联事件 5 关联组织 0

研究者发现Crysis勒索软件新变种	2017-08-17
友商发布2017年勒索软件威胁形势分析报告	2018-01-14
黑客利用垃圾邮件分发Dharma勒索软件	2020-02-20
勒索软件Crysis的198个解密密钥被公开	2017-05-28
CrySiS勒索病毒最新变种来袭, 加密后缀为kharma	2019-11-20
安全厂商发布2017年勒索软件回顾	2017-12-23

应用效果—更好的知识性



078d12eb9fc2b1665c0cc3001448b69b 1487d1dc13314bf04
 078d12eb9fc2b1665c0cc3001448b69b 1489d2adf0328b6d7
 07def14bd646461fb058c3ab2e1128e 153ac7591b9326ee6
 08a3776a2c40e569f645a62fdd2fcac3 15552ebdc4e6e5b4d
 08a3776a2c40e569f645a62fdd2fcac3 1579467859b48085b
 08f7ead1513bb921c9cdee334a370866 158ff697f8e609316
 09947ba52932d10d3c859511a6d31e8f 15e45c24dbe603402
 09cd5273640ab23112b719c65e4902 166044bf473fc262e
 0a0bcd8beb77e67a28a325d8d2a00254 1676ded041404671b
 0acd9f4ed3e3f3d9d011aa5e7cd03 168f2c46e159ce0b
 0ad9583aefede1f355759e0b674930cb 16c11b381c3f35283
 0b29cdf3c8c0459507e670e9c4547e0 16c140fb1b6d22e0
 0b38f7841ed347cc2a5ffa510a1c8f6 16ff55646196cf297
 0b8f197b4266e6b78ea0dcb9b3496e9 176e2277be875e55a
 0ba19063dea4ccae0afcd4208781f16b 1785f20ad40883fee5
 0bbe6cab66d76bab44874dc3995d8f 17a31d1075ebce41b
 0c0eb91f318da38e6684bd5250f68378 187dc6afa65cbdd8e
 0c2cbfbc3c93b3502f9a60f5fa1188ad 18b9e5fad0f015a0c
 0cace87b377a00df82839c659fc3adea 18bc477fa12048fab
 0d466e84b10d61031a62affcfff6e31a 1972ae990751fa1b1
 0d5956dac2ac56f29ee8fa121450973 1981cc08cdad971e

Operation Hangover: Unveiling an Indian Cyberattack Infrastructure Appendix

MDS	所属组织	所属组件	功能
078d12eb9fc2b1665c0cc3001448b69b	Kaspersky	Microsoft	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.Win32.Agent.hvjb	Worm.Win32/Foler.C	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Downloader.Win32.Agent.hhgu	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Worm.Win32.Agent.ali	Worm.Win32/Foler.C	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.Win32.VB.cfz	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Exploit.Win32.CV#-2012-0158.j	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.Win32.Bahanut.o	Trojan.Win32/Rinoad.gnb	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.Win32.APosT.ltv	TrojanSpy.Win32/Dayek.A	
078d12eb9fc2b1665c0cc3001448b69b	HEUR:Trojan.Win32.HangOver.gen	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Virus.Win32.Virut.ce	Worm.Win32/Foler.C	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.Win32.Agent.hnll	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.Agent.chfl	TrojanSpy.Win32/Dayek.A	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.Win32.APosT.flo	TrojanSpy.Win32/Hanoveirfn	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.acqh	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.acqh	TrojanSpy.Win32/Hanove.C	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Downloader.Win32.AutoI1.xd	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.adar	TrojanSpy.Win32/Dayek.A	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Dropper.Win32.Ducler.vrp	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	HEUR:Trojan.Win32.HangOver.gen	TrojanSpy.Win32/Hanove.F	
078d12eb9fc2b1665c0cc3001448b69b	HEUR:Trojan.Win32.HangOver.gen	TrojanSpy.Win32/Hanove.F	
078d12eb9fc2b1665c0cc3001448b69b	Worm.Win32.Agent.ali	Worm.Win32/Foler.C	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Downloader.Win32.VB.bkrb	TrojanDownloader.Win32/Adobch.A	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.acqh	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.Agent.chju	TrojanSpy.Win32/Hanove.F	
078d12eb9fc2b1665c0cc3001448b69b	HEUR:Trojan.VBS.Sagent.gen	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.VBS.Starter.dy	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Worm.Win32.Agent.ali	Worm.Win32/Foler.C	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.acqh	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	HEUR:Trojan.Win32.HangOver.gen	Backdoor.Win32/Hanove.A	
078d12eb9fc2b1665c0cc3001448b69b	Not Found	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Downloader.Win32.Agent.gzkr	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.acqh	TrojanSpy.Win32/Hanoveirfn	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.adar	TrojanSpy.Win32/Dayek.A	
078d12eb9fc2b1665c0cc3001448b69b	HEUR:Trojan.Script.Generic	TrojanSpy.Win32/Linog.A	
078d12eb9fc2b1665c0cc3001448b69b	Backdoor.Win32.RShot.vsl	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.Agent.cpfz	Not Found	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.KeyLogger.acqh	TrojanSpy.Win32/Hanoveirfn	
078d12eb9fc2b1665c0cc3001448b69b	Trojan.Win32.Agent.hvjb	Worm.Win32/Foler.C	
078d12eb9fc2b1665c0cc3001448b69b	Trojan-Spy.Win32.Agent.chfl	Not Found	

某白象分析报告

各反病毒引擎厂商检测结果

MDS	所属组织	所属组件	功能
096cd3773640ab23112b719c65e4902	白象	Backdoor	白象所用的后门软件，可执行shell命令
0796f11996f7456ef37d81a5b846b61b	白象	KeyLogger	白象组织使用的KeyLogger工具，具有开机自启功能
08a3776a2c40e569f645a62fdd2fcac3	白象	KeyLogger	白象组织使用的KeyLogger工具，具有开机自启功能
0d466e84b10d61031a62affcfff6e31a	白象	Dropper	白象组织使用的Dropper文件，释放VBS脚本并执行
1489d2adf0328b6d7b42170095f966c9	白象	Downloader	白象组织使用的Downloader文件，下载恶意载荷并执行，窃
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
153ac7591b9326ee83cd36180d39665e	白象	Http	白象组织使用的联网组件

```

"result": {
  "desc": "0796f1096f7456ef37d81a5b846b61b",
  "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.l1

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

```
....."ATT&CKVector":{
....."Execution":{
.....  "Command and Scripting Interpreter":{
.....    "WindowsCommandShell":["found_shell_in_macro"]
.....  },
.....  "User Execution":{
.....    "MaliciousFile":["found_macor_in_file"]
.....  }
.....},
....."Persistence":{
.....  "Boot or Logon Autostart Execution":{
.....    "Registry Run Keys / Startup Folder":["found_autorun_registry"]
.....  },
....."Defense Evasion":{
.....  "Obfuscated Files or Information":{
.....    "Software Packing ":["found_zip_file"]
.....  }
.....}
```

• 发现宏

```
.....},
....."Discovery":{
.....  "System Information Discovery":{
.....    "no_subtech":["found_get_machinename_api"]
.....  },
.....  "Query Registry":{
.....    "no_subtech":["could_query_registry"]
.....  },
.....  "File and Directory Discovery":{
.....    "no_subtech":["found_getfiles_api_1"]
.....  },
.....  "Process Discovery":{
.....    "no_subtech":["found_getprocesses_api"]
.....  }
.....},
```

• 获取机器名称

```
....."Command and Control":{
.....  "Application Layer Protocol":{
.....    "Web Protocols":["found_http_connection_2"]
.....  }
.....},
....."Collection":{
.....  "Screen Capture":{
.....    "no_subtech":["could_get_sceen_img_1"]
.....  }
.....}
.....}
```

• 获取屏幕截图

安天引擎输出向量映射ATT&CK案例



威胁知识运营系统
simon@antiy.cn

5

11

命中情况 战术 **5** 技术 **11**

选择框架 工控框架

基本信息

MD5 *****ea8d47951abffec38f*****

文件格式 Document/Microsoft Doc[Word 98-2003]...

文件大小 423.50 KB (433664 字节)

编程语言 无

处理程序 无

病毒名称 Trojan[Downloader]MSOffice.Agent.now

原始文件名 无

关联组织 透明部落

多引擎分析

37/61

标签 Crimson 透明部落 APT 诱饵

远控 apt36 盗窃

transparent tribe

关联事件

安全厂商披露“透明部落”行动最新攻击目标

Transparent Tribe攻击活动更新

APT36 jumps on the coronavirus bandwagon, ...

Transparent Tribe: Evolution analysis, part 1

检测规则

① 发现shell命令

TA0002 执行 (10)	TA0003 持久化 (18)	TA0004 提权 (12)	TA0005 防御规避 (37)	TA0006 凭证访问 (14)	TA0007 发现 (25)	TA0008 横向移动 (9)	TA0009 收集 (17)	TA0011 命令与控制 (16)	TA0010 数据渗出 (9)	TA0040 影响 (13)
T1069 利用命令和脚本解释器	T1098 操纵账户	T1548 滥用提升控制权限机制	T1548 滥用提升控制权限机制	T1110 暴力破解	T1087 发现账户	T1210 利用远程服务漏洞	T1560 压缩/加密收集的数据	T1071 使用应用层协议	T1020 自动渗出数据	T1531 删除账户权限
T1203 利用主机软件漏洞执行	T1197 利用BITS服务	T1134 操纵访问令牌	T1134 操纵访问令牌	T1555 获取密码存储中的凭证	T1010 发现应用程序窗口	T1534 执行内部鱼叉式钓鱼攻击	T1123 捕获音频	T1092 通过可移动介质通信	T1030 限制传输数据大小	T1485 拦截数据
T1559 利用进程间通信	T1547 利用自动启动执行引导或登录	T1547 利用自动启动执行引导或登录	T1197 利用BITS服务	T1212 利用凭证访问漏洞	T1217 发现浏览器书签	T1570 横向传输文件或工具	T1119 自动收集	T1132 编码数据	T1048 使用非C2协议回传	T1486 造成恶劣影响的数据加密
T1106 利用API	T1037 利用初始化脚本引导或登录	T1037 利用初始化脚本引导或登录	T1140 反混淆/解密文件或信息	T1187 强制认证	T1580 发现云基础设施	T1563 远程服务会话劫持	T1115 收集剪贴板数据	T1001 混淆数据	T1041 使用C2信道上回传	T1565 篡改数据
T1053 利用计划任务/工作	T1176 添加浏览器扩展插件	T1543 创建或修改系统进程	T1006 直接访问卷	T1056 输入捕捉	T1538 云服务仪表板	T1021 利用远程服务	T1530 收集云存储对象的数据	T1568 使用动态参数	T1011 使用其他网络介质回传	T1491 篡改可见内容
T1129 利用共享模块执行	T1554 篡改客户端软件	T1546 事件触发执行	T1480 执行范围保护	T1557 利用中间人攻击(MITM)	T1526 云服务发现	T1091 通过可移动介质复制	T1602 收集配置库的数据	T1573 使用加密信道	T1052 使用物理介质回传	T1561 擦除磁盘
T1072 利用第三方软件部署工具	T1136 创建账户	T1068 利用漏洞提权	T1211 利用漏洞规避防御	T1556 修改身份验证过程	T1482 发现域信任	T1072 利用第三方软件部署工具	T1213 收集信息库数据	T1008 使用备用信道	T1567 使用Web服务回传	T1499 端点侧拒绝服务(DoS)
T1569 利用系统服务	T1543 创建或修改系统进程	T1484 利用策略修改	T1222 修改文件和目录权限	T1040 网络嗅探	T1083 发现文件和目录	T1080 污染共享内容	T1005 收集本地系统数据	T1105 使用人工工具传输	T1029 定时传输	T1495 损坏附件
T1204 诱导用户执行	T1546 事件触发执行	T1574 执行流程劫持	T1484 修改策略	T1003 操作系统凭证转储	T1046 扫描网络服务	T1550 使用备用身份验证材料	T1039 收集网络共享驱动数据	T1104 创建多级信道	T1537 将数据转移到云账户	T1490 禁止系统恢复
T1047 利用Windows管理规范(WMI)	T1133 利用外部远程服务	T1055 进程注入	T1564 隐藏行为	T1528 窃取应用程序访问令牌	T1135 发现网络共享	T1025 收集可移动介质数据	T1095 使用标准/非标准应用层协议	T1498 网络侧拒绝服务(DoS)		
	T1574 执行流程劫持	T1053 利用计划任务/工作	T1574 执行流程劫持	T1558 窃取或伪造Kerberos凭证	T1040 网络嗅探	T1074 数据暂存	T1571 使用非标准端口	T1496 资源劫持		
	T1525 植入容器映像	T1078 利用有效账户	T1562 削弱防御机制	T1539 窃取Web会话Cookie	T1201 发现密码策略	T1114 收集电子邮件	T1572 使用协议隧道	T1489 禁用服务		
	T1137 启动Office应用程序		T1070 删除主机中的信标	T1111 双因子认证拦截	T1120 发现主机接入设备	T1056 输入捕捉	T1090 使用代理	T1529 系统关机/重启		
	T1542 在操作系统前启动		T1202 间接执行命令	T1552 未受保护凭证	T1069 发现权限组	T1185 浏览器中间人攻击(MiB)	T1219 利用远程访问软件			
	T1053 利用计划任务/工作		T1036 伪装	T1057 发现进程		T1557 利用中间人攻击(MITM)	T1205 使用流量命令			
	T1505 利用服务器软件组件		T1556 修改身份验证过程	T1012 查询注册表		T1113 获取屏幕截图	T1102 利用合法Web服务			
	T1205 使用流量命令		T1578 修改云计算基础设施	T1018 发现远程系统		T1125 捕获视频				
	T1078 利用有效账户		T1112 修改注册表	T1518 发现软件						

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

*****f853f2e666ef062102db*****
选择框架 工控框架

命中情况 战术 5 技术 11
切换英文

基本信息	TA0002 执行 (10)	TA0003 持久化 (18)	TA0004 提权 (12)	TA0005 防御规避 (37)	TA0006 凭证访问 (14)	TA0007 发现 (25)	TA0008 横向移动 (9)	TA0009 收集 (17)	TA0011 命令与控制 (16)	TA0010 数据渗出 (9)	TA0040 影响 (13)
MD5 *****f853f2e666ef062102db*****	T1059 利用命令和脚本解释器	T1098 操纵账户	T1548 适用提升控制权限机制	T1548 适用提升控制权限机制	T1110 暴力破解	T1087 发现账户	T1210 利用远程服务漏洞	T1560 压缩/加密收集的数据	T1071 使用应用层协议	T1020 自动渗出数据	T1531 删除账户权限
文件格式 Document/Microsoft Word 98-2003...	T1203 利用主机软件漏洞执行	T1197 利用BITS服务	T1134 操纵访问令牌	T1134 操纵访问令牌	T1555 获取密码存储中的凭证	T1010 发现应用程序窗口	T1534 执行内部鱼叉式钓鱼攻击	T1123 捕获音频	T1092 通过可移动介质通信	T1030 限制传输数据大小	T1485 损毁数据
文件大小 146 KB (150,016 字节)	T1559 利用进程间通信	T1547 利用自动启动执行引导或登录	T1547 利用自动启动执行引导或登录	T1197 利用BITS服务	T1212 利用凭证访问漏洞	T1217 发现浏览器书签	T1570 横向传输文件或工具	T1119 自动收集	T1132 编码数据	T1048 使用非C2协议回传	T1486 造成恶劣影响的数据加密
编译语言 无	T1106 利用API	T1037 利用初始化解脚本引导或登录	T1037 利用初始化解脚本引导或登录	T1140 反混淆解密文件或信息	T1187 强制认证	T1580 发现云基础设施	T1563 远程服务会话劫持	T1115 收集剪贴板数据	T1001 混淆数据	T1041 使用C2信道回传	T1565 操纵数据
处理器架构 无	T1053 利用计划任务/工作	T1176 添加浏览器扩展插件	T1543 创建或修改系统进程	T1006 直接访问卷	T1056 输入捕捉	T1538 云服务仪表盘	T1021 利用远程服务	T1530 收集云存储对象的数据	T1568 使用动态参数	T1011 使用其他网络介质回传	T1491 篡改可见内容
病毒名称 Trojan[Downloader]/MSOffice.Agent.afu	T1129 利用共享模块执行	T1554 篡改客户端软件	T1546 事件触发执行	T1480 执行范围保护	T1557 云服务发现	T1526 云服务发现	T1091 通过可移动介质复制	T1602 收集配置库的数据	T1573 使用加密信道	T1052 使用物理介质回传	T1561 擦除磁盘
原始文件名 无	T1072 利用第三方软件部署工具	T1136 创建账户	T1068 利用漏洞提权	T1211 利用漏洞规避防御	T1556 修改身份验证过程	T1482 发现域信任	T1072 利用第三方软件部署工具	T1213 收集信息库数据	T1008 使用备用信道	T1567 使用Web服务回传	T1499 端点侧拒绝服务 (DoS)
关联组织 海莲花	T1569 利用系统服务	T1543 创建或修改系统进程	T1484 利用组策略修改	T1222 修改文件和目录权限	T1040 网络嗅探	T1083 发现文件和目录	T1005 污染共享内容	T1005 收集本地系统数据	T1105 使用入口工具传输	T1029 定时传输	T1495 损坏固件
多引擎分析 39/67	T1204 诱导用户执行	T1546 事件触发执行	T1574 执行流程劫持	T1484 修改组策略	T1003 操作系统凭证值	T1046 扫描网络服务	T1550 使用备用身份验证材料	T1039 收集网络共享驱动数据	T1104 创建多级信道	T1537 将数据转移到云账户	T1490 禁止系统恢复
介质复制	T1047 利用Windows管理规范 (WMI)	T1133 利用外部远程服务	T1055 进程注入	T1564 隐藏行为	T1528 窃取应用程序访问令牌	T1135 发现网络共享	T1025 收集可移动介质数据	T1095 使用标准非应用层协议	T1095 使用标准非应用层协议	T1498 网络侧拒绝服务 (DoS)	T1498 网络侧拒绝服务 (DoS)
标签 海莲花 APT CVE-2018-20250 漏洞利用 钓鱼 诱饵 CVE-2017-0144 CVE-2017-11882 CVE-2017-8570 CVE-2017-0199 spear-phishing email	T1574 执行流程劫持	T1053 利用计划任务/工作	T1574 执行流程劫持	T1558 窃取或伪造Kerberos凭证	T1040 网络嗅探	T1074 数据暂存	T1571 使用非标准端口	T1572 使用协议隧道	T1571 使用非标准端口	T1496 资源劫持	T1496 资源劫持
关联事件 境外APT组织“海莲花”(OceanLotus)最新攻击活动解析 疑似海莲花又有新活动, 攻击目标似为国内大型企业 深度分析及防护: 加密木马攻击, 海莲花 海莲花 (OceanLotus) 团伙漏洞利用类攻击样本分析	T1525 植入容器映像	T1078 利用有效账户	T1562 削弱防御机制	T1539 窃取Web会话Cookie	T1201 发现密码策略	T1114 收集电子邮件	T1056 输入捕捉	T1090 使用代理	T1090 使用代理	T1529 系统关机/重启	T1529 系统关机/重启
检测规则 ① 使用cmd.exe执行命令	T1137 启动Office应用程序	T1070 删除主机中的信标	T1111 双因子认证拦截	T1120 发现主机接入设备	T1069 发现权限组	T1185 浏览器中间人攻击 (MitB)	T1219 利用远程访问软件	T1205 使用流量信令	T1102 利用合法Web服务	T1102 利用合法Web服务	T1102 利用合法Web服务
	T1542 在操作系统前启动	T1202 间接执行命令	T1552 未受保护凭证	T1057 发现进程	T1012 查询注册表	T1018 发现远程系统	T1125 捕获视频				
	T1053 利用计划任务/工作	T1036 仿真	T1556 修改身份验证过程	T1018 发现远程系统	T1518 发现软件						
	T1505 利用服务软件组件	T1578 修改云计算基础设施	T1112 修改注册表								
	T1205 使用流量信令										
	T1078 利用有效账户										



安天引擎映射ATT&CK框架的意义



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	命令与控制	渗出	影响						
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用_bash_profile和...	启动代理	利用服务器软件组件	捕获访问令牌	绕过Gatekeeper	Process Doppelgänger	捕获账户	发现账户	利用AppleScript	捕获音频	利用常用端口	自动导出数据	删除账户权限		
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能	启动守护进程	利用服务器注册表权限...	借助辅助功能	利用Setuid和Setgid位	填充二进制文件	修改组策略	替换进程内存	查看Bash历史	发现应用程序窗口	利用应用程序部署软件	自动收集	通过可移动介质通信	压缩数据	篡改数据
利用外部远程服务	利用命令行	加入空格隐藏扩展名	捕获账户	利用Launchctl	利用Setuid和Setgid位	利用AppCert DLL(注...)	SID历史注入	利用BITS服务	隐藏文件目录	进程注入	暴力破解	发现浏览器书签	利用组件对象模型(C...	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据...
添加硬件	利用HTML编译文件	利用系统中的第三方...	利用AppCert DLL(注...)	添加LC_LOAD_DYLIB	修改快捷方式	利用AppInit DLL(注...)	利用启动项	绕过用户账户控制(UAC)	隐藏用户	冗余访问	凭证传播	发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容置换攻击...
通过可移动介质复制	利用组件对象模型(C...	利用Trap命令	利用AppInit DLL(注...)	利用linux本地任务调度	会话发起协议(SIP)和...	利用Windows应用程...	利用Sudo命令	清除命令历史	隐藏窗口	利用Regsvcs/Regasm	获取Web浏览器凭证	发现文件和目录	执行内部鱼叉式钓鱼...	收集本地系统数据	使用自定义加密协议	通过备选协议回传	删除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用受信任的开发工具	利用Windows应用程...	利用登录项	利用启动项	绕过用户账户控制(U...	利用Sudo缓存凭证	利用CMSTP	HISTCONTROL	利用Regsvr32	获取文件中的凭证	扫描网络服务	利用登录脚本	收集网络共享驱动数据	编码数据	通过C2信道回传	删除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协议...	诱导用户执行	利用认证包	利用登录脚本	利用系统组件	DLL搜索顺序劫持	利用有效账户	代码签名	映像劫持	使用Rootkit	获取注册表中的凭证	发现网络共享	利用密码哈希认证	收集可移动介质数据	混淆数据	通过其他网络介质回传	端点拒绝服务(DoS)
通过服务执行鱼叉式...	通过API执行	利用Windows管理规...	利用BITS服务	利用LSASS驱动程序	利用Systemd服务	Dylib劫持	使用Web Shell	投递后编译	阻止信标捕获	利用Rundll32	利用凭证访问漏洞	网络嗅探	利用Ticket认证	回传数据准备	前置域名	通过物理介质回传	损坏固件
入侵供应链	通过模块加载执行	利用Windows远程管...	使用Bootkit	修改现有服务	利用Windows时间服务	提示用户输入合法凭...		利用HTML编译文件	删除工具中的信标	使用脚本	强制认证	发现密码策略	利用远程桌面协议	收集电子邮件	使用域名生成算法(DGA)	定时传输	禁止系统恢复
利用受信关系	利用主机软件漏洞	利用XSL文件执行脚本	添加浏览器扩展插件	Netsh Helper DLL	利用Trap命令	利用事件监控守护进程		利用组件劫持	删除主机中的信标	执行签名的二进制文...	利用Hook	发现主机接入设备	拷贝远程文件	输入捕捉	使用备用信道	网络侧拒绝服务(DoS)	资源劫持
利用有效账户	利用图形用户界面(GUI)		更改默认文件关联	新建服务	利用有效账户	利用漏洞提权		利用连接代理	安装根证书	会话发起协议(SIP)和...	欺骗用户输入凭证	发现权限组	利用远程服务	浏览器中间人攻击(MitB)	利用多跳代理	创建多级信道	篡改运行时数据
	利用InstallUtil		利用组件劫持	启动Office应用程序	使用Web Shell	额外窗口内存注入(E...		利用控制面劫持	利用InstallUtil	软件外壳	使用Kerberoasting技术	查询注册表	共享Webroot目录	捕获视频	使用多协议通信	禁用服务	
	利用Launchctl		组件对象模型(COM)...	路径拦截	利用Windows事件订...	利用文件系统权限漏洞		利用HTML编译文件	利用Launchctl	加入空格隐藏扩展名	利用Keychain	发现远程系统	SSH劫持		使用多层加密	篡改本地存储数据	
	利用linux本地任务调度		创建账户	修改属性列表	Winlogon Helper D...	利用Hook		使用DCShadow技术	利用Launchctl	加入空格隐藏扩展名	利用Keychain	发现远程系统	SSH劫持		使用多层加密	篡改本地存储数据	
	利用LSASS驱动程序		DLL搜索顺序劫持	端口敲门		启动守护进程		反混淆/解码文件等信息	LC_MAIN劫持	模板注入	LLMNR/NBT-NS投毒...	发现安全软件	污染共享内容		端口敲门	系统关机/重启	
	利用Mshta		Dylib劫持	端口监控		启动守护进程		禁用安全工具	仿冒	修改文件时间戳	网络嗅探	发现软件	利用系统中的第三方...		利用访问访问工具		
	利用PowerShell		利用事件监控守护进程	利用PowerShell配置...		新建服务		DLL搜索顺序劫持	修改注册表	利用受信任的开发工具	利用Password Filter...	发现系统信息	利用Windows管理页...		拷贝远程文件		
	利用Regsvcs/Regasm		利用外部远程服务	利用Rc.common文件		伪造父进程		DLL旁路加载	利用Mshta	利用有效账户	收集私钥	发现系统网络配置	利用Windows远程管...		使用标准应用层协议		
	利用Regsvr32		利用文件系统权限漏洞	重启应用程序		路径拦截		按条件执行	删除网络共享连接	虚拟化/沙箱逃逸	利用Securityd内存	发现系统网络连接			使用标准加密协议		
	利用Rundll32		隐藏文件和目录	冗余访问		修改属性列表		利用漏洞规避防御	利用NTFS交换数据流...	利用Web服务	窃取Web会话Cookie	发现系统所有者/用户			使用标准非应用层协议		
	利用计划任务		利用Hook	添加注册表运行键/启...		端口监控		额外窗口内存注入(EW...	混淆文件等信息	利用XSL文件执行脚本	双因子认证拦截	发现系统服务			利用不常用端口		
	使用脚本		利用Hypervisor	利用计划任务		利用PowerShell配置...		修改文件和目录权限	伪造父进程			发现系统时间			利用Web服务		
	利用windows服务		映像劫持	利用屏幕保护程序		进程注入		删除文件	修改属性列表			虚拟化/沙箱逃逸					
	利用签名的二进制文...		利用内核模块和扩展	利用SSP DLL(注册表...		利用计划任务		文件系统逻辑偏移	端口敲门								

- 不相关
- 无效 (未覆盖)
- 有效
 - 可防御/可拦截
 - 可检测/可记录
 - 可降低机会
 - 可输出知识

智者安天下



长缨待展

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

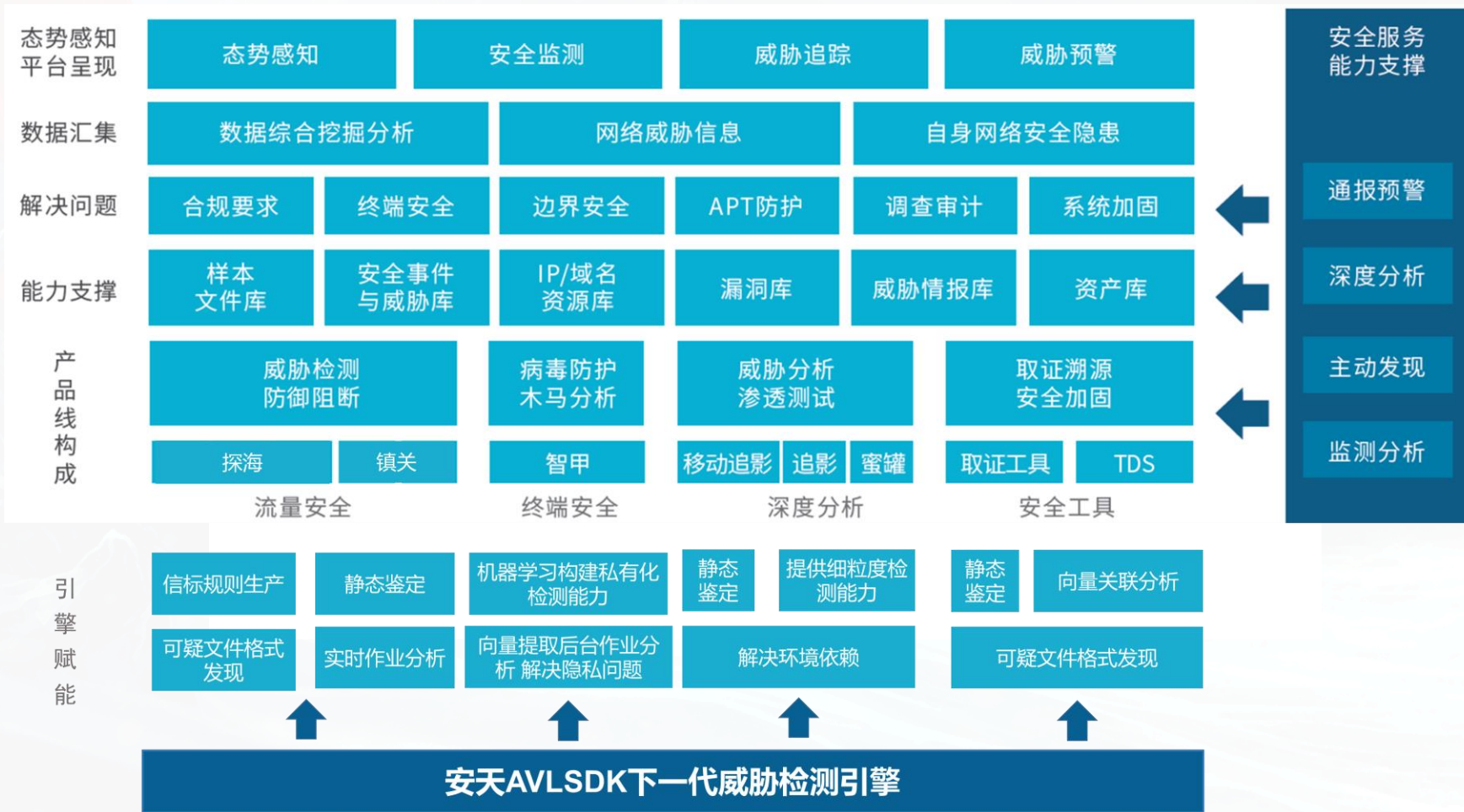
形成有效判定能力，其知识化的输出可以让分析人员**快速了解威胁**，使分析人员聚焦于高等级威胁攻击载荷深入分析层面。



· 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



震网样本实例一引擎输出结果



```
"result": {
  "desc": "2BDA3159666B29BF6F912A69B9325435",
  "malware_info": {
  },
  "format": {
  },
  "packer": {
  },
  "hformat": {
    "id": 1,
    "name": " BinExecute/Microsoft.EXE[:X86] "
  },
  "sfx": {
  }
},
"knowledge": {
  "sid": 40,
  "malware_name": "Worm/Win32.Stuxnet",
  "type": "APT",
  "description": "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。",
  "tags": [
    "APT",
    "Dropper"
  ],
  "group": [
    {
      "name": "Equation Group",
      "info": {
        "id": "G001",
        "publish_name": "Equation Group",
        "alias_name": [
          "Tilded Team",
          "Lamberts",
          "APT-EQGRP",
          "方程式组织"
        ]
      }
    }
  ],
  "target_location": [
    "巴基斯坦",
    "阿富汗",
    "印度",
    "伊朗",
    "伊拉克"
  ],
  "member": [],
  "org_nature": "超高级能力国家/地区行为体",
  "ttp": {
    "attack_method": [
      "U盘摆渡",
      "漏洞利用"
    ],
    "persistence_method": "防火墙固件植入",
    "algorithm": [
      "AES"
    ]
  },
  "purpose": [
    "窃密",
    "破坏"
  ],
  "location": [
    "美国"
  ]
}
```

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
- 战术技术过程

①组织信息



方程式(Equation Group)

性质:	超能力国家/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:	方程式组织是具有超自然超能力的超能力国家/地区行为体,又名Tilded Team、Equation Group等,由卡斯基于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、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、监听等攻击行动。该组织主要采用零日漏洞利用、U盘渗透攻击、数十种常见品牌硬件修改、攻击取得原子化、多种加密算法、安全软件规避、持久化等攻击手法,利用的高漏洞涉及CVE-2010-2568、CVE-2011-3402、CVE-2015-2360、打印后台程序顺序漏洞(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、Fairy、GrayFish等攻击武器。		
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FastNets事件链分析报告 https://www.anty.cn/research/notice/report/research_report/20190601.html		
	2017-01-26 安天破解方程式组织病毒式主机作业 https://www.anty.cn/research/notice/report/research_report/663.html		

④威胁分析

MD5:	28DA315966829BF6F912A6989325435	威胁名称:	Worm/Win32.Stuxnet
组织信息:	方程式组织是一个美国的超能力国家行为体,又名Tilded Team、Equation Group等,由卡斯基于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:	Tilded	工具组件:	Stuxnet Dropper
威胁描述:	需网Dropper样本,搜索.stub,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rootkit,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

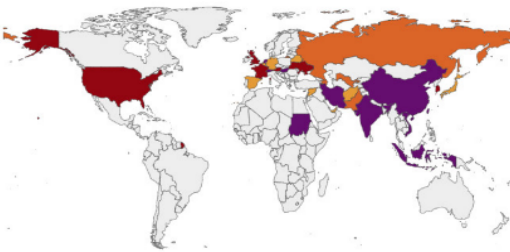
战术技术过程

初始访问	执行	持久化	提权	防前规避	凭证访问	发现	横向运动	收集	命令控制	渗透	对抗
		T1179 挂钩	T1179 挂钩	T1140 反恶意解密文件或信息	T1179 挂钩					T1022 数据加密	
				T1014 Rootkit							

ANTY 安天 智者安天下

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、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、监听等攻击行动。其攻击意图包括窃取、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、勒索、窃取信息、修改PLC、监视、控制、间谍活动、收集受害主机信息、获取基础设施等。



③攻击活动



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	NSA/CSS 矩阵检测 MITRE ATT&CK矩阵 (技术) 检测	初始访问	T1193鱼叉式钓鱼附件	用户接收附件时 检测附件
执行	执行	执行	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	持久化	持久化	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	发现	发现	T1124系统时间发现 T1082系统信息发现	监控系统敏感API调用, 包括: GetSystemInfo、GetSystemTime
凭证访问	凭证访问	凭证访问	T1033系统所有者/用户发现	监控 系统敏感API调用, GetUserName
横向移动	横向移动	横向移动	T1003凭证转储	进程监控, PowerShell执行参数检测, 脚本文件检测
持久化	持久化	持久化	T1021远程服务	网络连接监控, 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
凭证访问	凭证访问	凭证访问	T1060注册表运行键值/启动文件夹	创建启动项检测
命令控制	命令控制	命令控制	T1179 Hooking	内存存在异常钩子
			T1071标准应用层协议 T1022数据加密	进程联网情况检测
			T1094自定义命令和控制协议	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



网络空间威胁对抗与防御技术研讨会
暨 第八届安天网络安全冬训营

智者安天下

谢谢大家

长缨缚展

威胁框架：细粒度对抗