第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

锻造能力型工程师队伍
提供赋能式的安全服务

安天 安全运营中心

红旗漫卷

敌情想定是前提，网络安全实战化

提纲

- 前言
- APT攻击分析取证实战
- 安全监测实战
- 应急响应实战
- 安天安全服务的使命和愿景

1 前言

安天安全服务定位

ANTIY

- 威胁情报
- 技术积累
- 产品能力

能力积累

平台助力

- 赛博超脑
- 态势感知

- 安全运营
- 安全分析
- 应急响应

安全服务

安天安全服务内容

APT事件响应

海莲花
白象
方程式
……

应急响应

魔窟、暗云、
异鬼、必加、
魔鼬、挖矿
木马……

高级安全咨询

威胁建模
威胁情报
安全架构

永恒之蓝
Wpa2
Meltdown(熔毁)
Spectre(幽灵)
微软SMB漏洞
BlueBorne……

安全漏洞

两会
一带一路峰会
金砖国家峰会
中国共产党第十九次全国代表大会
中国共产党与世界政党高层对话

网络安保

国家部委、监管部门

运营商、交通、能源、民航等行业

2 APT攻击分析取证实战

安天威胁检测系统发现恶意域名请求

安天探海威胁检测系统(PTD)

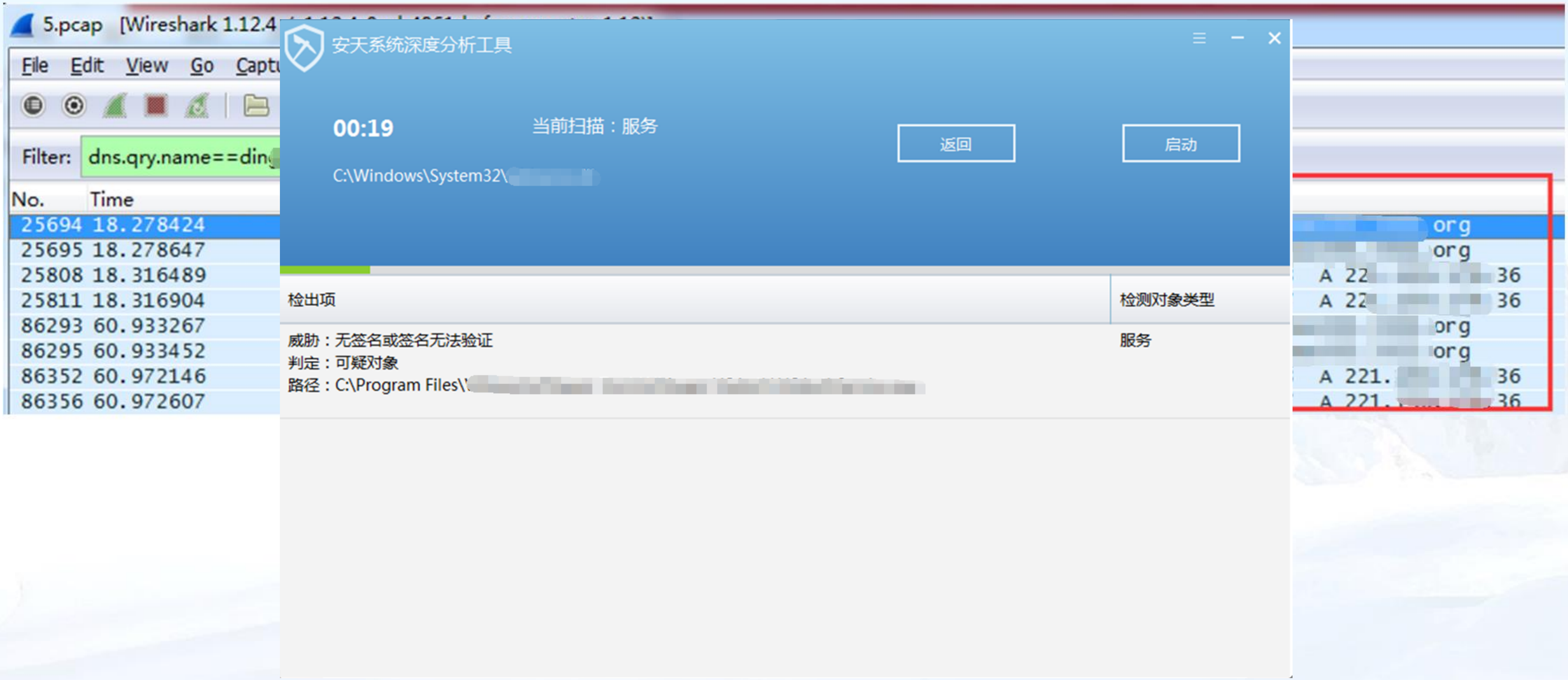
威胁检测系统　首页>>威胁分析>>网络行为　07-14 15:29:25

- 系统摘要
- 威胁分析
  - 恶意文件
  - 恶意邮件
  - 网络行为
  - 未知文件
  - 敏感流量
- 统计报表
- 配置管理
- 流量分析
- 沙箱配置

查询结果：1151-1200/1240条 (24/25页)　[列定制] [展示] [查询] [导出]　分页:

检出时间	威胁等级	威胁名称	威胁类型	扩展信息	协议	源地址	目的地址
13:33:41	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}ding org{NA}221 5{QR}1{TI}BD23	DNS		
13:33:09	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}ding org{NA}221 36{QR}1{TI}558F	DNS		
13:32:36	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}ding org{NA}221. 6{QR}1{TI}B5D2	DNS		
13:32:05	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}ding org{NA}221 {QR}1{TI}59FB	DNS		
13:31:32	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}ding org{NA}221. {QR}1{TI}3B11	DNS		
13:31:01	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt org{NA}221. 6{QR}1{TI}F97B	DNS		
13:30:29	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt rg{NA}221 6{QR}1{TI}F853	DNS		
13:29:59	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt rg{NA}221 36{QR}1{TI}2FCB	DNS		
13:29:27	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt org{NA}221 6{QR}1{TI}A78D	DNS		
13:28:54	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt org{NA}221 36{QR}1{TI}D3B5	DNS		
13:28:23	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt org{NA}221. 6{QR}1{TI}5A8A	DNS		
13:27:51	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt org{NA}221. 6{QR}1{TI}9F11	DNS		
13:27:21	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}dingt org{NA}221 36{QR}1{TI}2739	DNS		
13:26:49	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}ding org{NA}221 6{QR}1{TI}69AF	DNS		
13:26:18	高	Trojan[Backdoor]/Win32.collect	恶意域名解析	{DNS}ding org{NA}221. 6{QR}1{TI}615C	DNS		

定位A客户问题主机

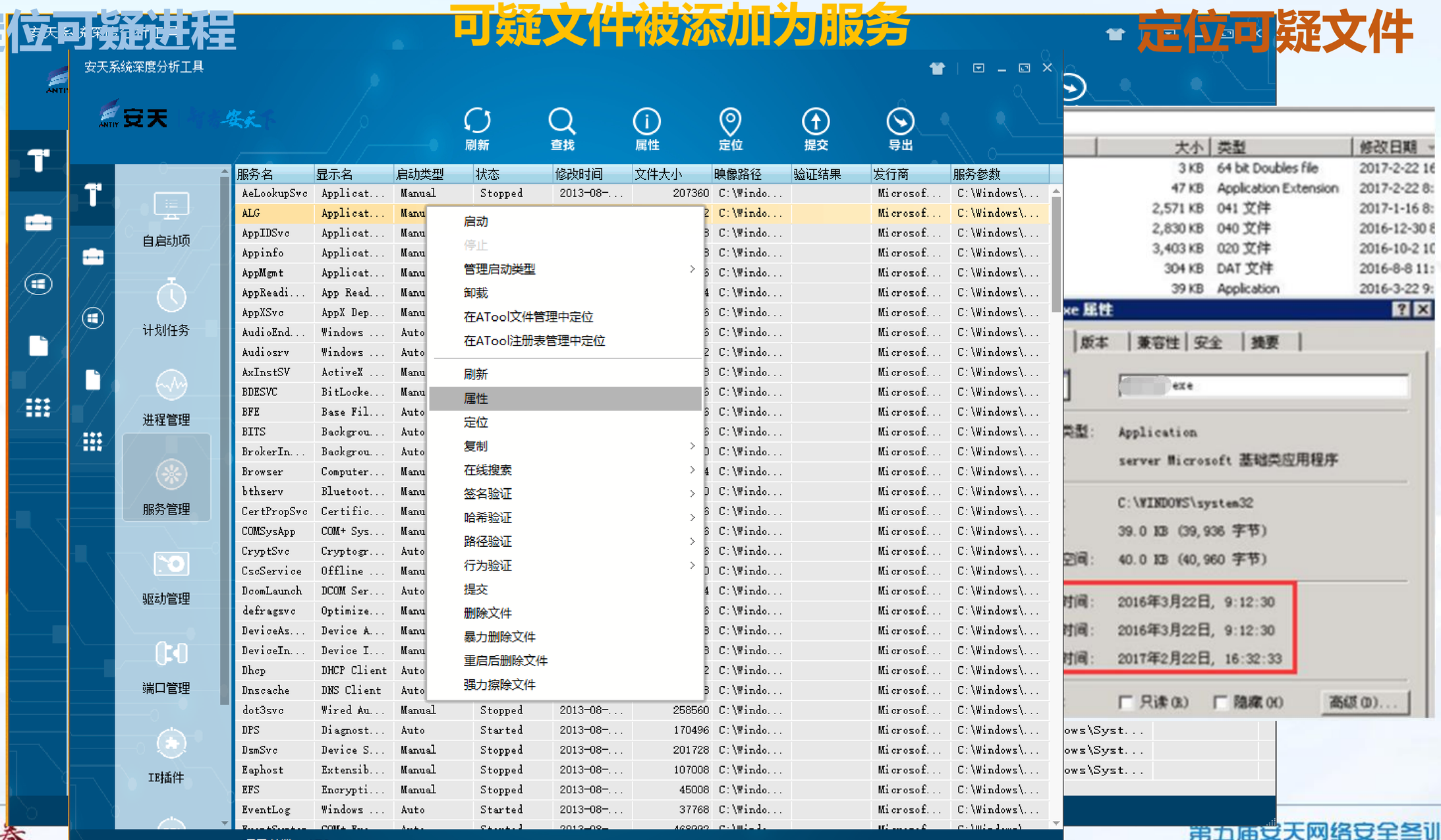

5.pcap [Wireshark 1.12.4
File Edit View Go Captu
Filter: dns.qry.name==din
No. Time
25694 18.278424
25695 18.278647
25808 18.316489
25811 18.316904
86293 60.933267
86295 60.933452
86352 60.972146
86356 60.972607
安天系统深度分析工具
00:19
当前扫描：服务
C:\Windows\System32\
返回
启动
检出项
检测对象类型
威胁：无签名或签名无法验证
判定：可疑对象
路径：C:\Program Files\
服务
org
org
A 22 36
A 22 36
org
org
A 221. 36
A 221. 36

定位分析

定位可疑进程

可疑文件被添加为服务

定位可疑文件



安天追影威胁分析系统检测结果

安天追影威胁分析系统(PTA)

文件 [redacted] exe：

基本信息/概述

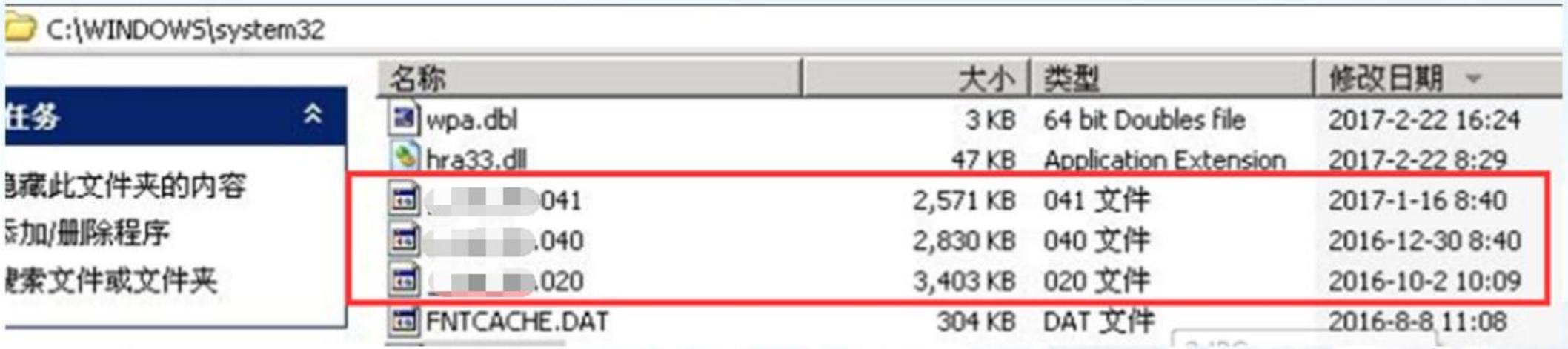
名称	[redacted].exe
大小	39.00 KB
文件格式	exe
MD5	[redacted]dfb7
分析时间	2017-02-23 10:24:00
分析环境	winxp 32bit,office 2007
恶意判定	black
病毒类型	DDOS
病毒名	Trojan[DDoS]/[redacted]
标签	[redacted]

文件是分布式拒绝服务攻击类型,主要目的是分布式拒绝服务攻击,文件类型是[redacted]检测是否为调试状态;通过movefile重命名，删除自身;获取磁盘类型;查找浏览器进程;获取计算机系统版本;自复制释放系统目录;独占模式打开文件;访问免费域名;获取计算机系统信息;获取CPU信息;疑似获取CPU信息;疑似桌面控制;

汇总发现

发现危险	危险等级
[redacted]劫持	★★★★
检测是否为调试状态	★★★
通过movefile重命名，删除自身	★★★

威胁评估



✓信息窃取

✓远程控制

✓拒绝服务攻击

✓发送垃圾邮件

✓下载其他恶意代码

✓占用系统资源

✓潜伏时间长达一年

✓窃取大量机密文件

✓全能力商业木马

3 安全监测实战

B客户安全监测目标

加强重要信息管理系统及全网的网络安全防护

在网络中部署安全监测设备，监控全网数据流量

发现网络中的攻击行为，重大安全事件及安全隐患

威胁事件深度分析，配合处置及应急响应

针对B客户的安全监测成果

完成24次例行巡检

全网及重要系统安全监测月报各12份

发现高危事件21次，中低危事件132次

事件深度分析与应急响应19次

针对B客户的重大安全事件响应

- 1月 • 异常外连日本IP应急响应
- 3月 • IMDDoS木马深入分析
- 4月 • Struct2漏洞排查
- 5月 • Wannacry勒索软件爆发应急响应
- 6月 • Petya伪装勒索病毒排查
- 6月 • Virut感染型病毒应急响应
- 7月 • 钓鱼邮件深入分析
- 8月 • 异鬼木马排查
- 9月 • 服务器后门应急响应
- 10月 • 十九大重保网络安全保障
- 10月 • 重要信息系统渗透测试
- 12月 • 暗云3木马应急响应

B客户网络发现的高危事件

下载恶意程序，DDoS，窃取信息

共监测到10次

35个内网IP被感染

受害主机加入僵尸网络，受到远程控制

共监测到4次

4个内网IP成为僵尸主机

服务器被攻破，上传后门，窃取信息

共监测到1次

1个服务器被攻破

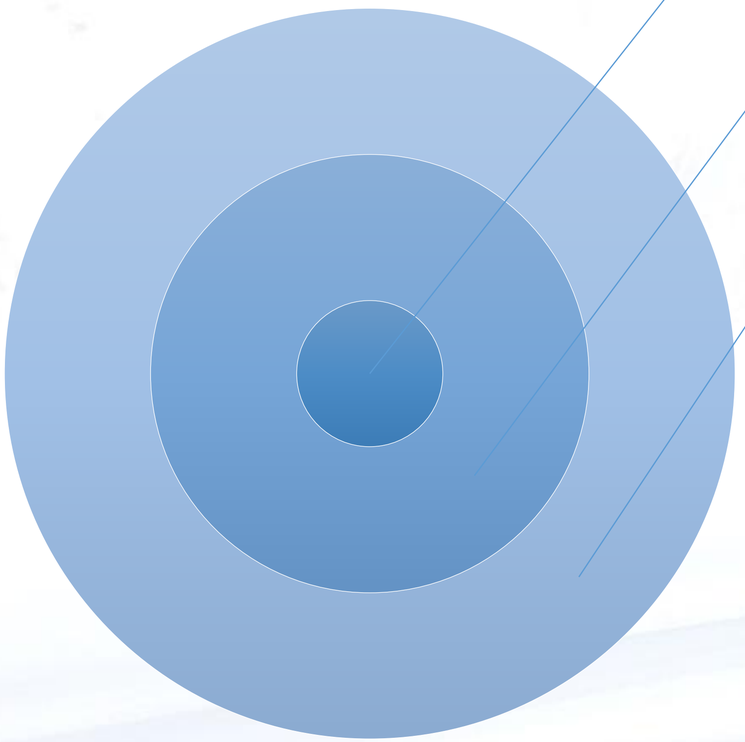
病毒感染并破坏大量系统文件

共监测到6次

21个内网IP被感染

B客户网络发现的中低危事件

风险软件下载



- 共监测到125次风险软件下载
- 125个IP下载并运行风险软件

可疑域名请求

域名关联恶意样本

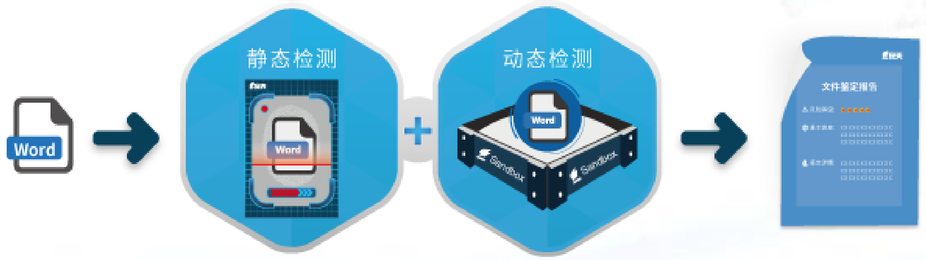
域名关联境外可疑IP

域名关联流氓软件

- 共监测到7次可疑域名请求
- 9个IP可能存在威胁

B客户安全监测全过程

安天探海：实时监测网络流量，发现威胁事件

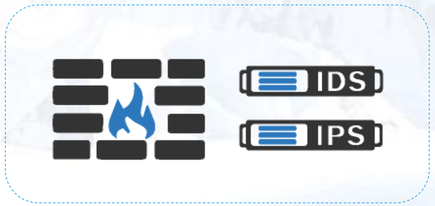


安天追影：对可疑对象深度分析发现未知威胁

自2016年12月-2017年12月总计发现共达**6118**疑似威胁事件，包括访问可疑链接、下载可疑文件、以及外部扫描。

统计关联分析

扫描类



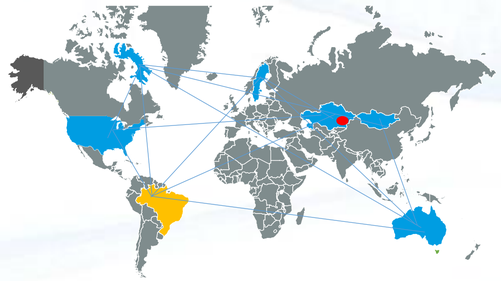
可疑威胁

钓鱼邮件事件深入分析

探海发现事件 → 提取文件 → 追影动态分析 → 人工深入分析 → 溯源 → 还原事件过程

- 安天探海设备发现有官方邮箱向国外发送大量钓鱼邮件；
- 邮件附件为银行相关主题的word文件
- 安天安全服务工程师现场提取文件，投入追影高级威胁分析系统动态分析；
- 发现word文件带有恶意功能的宏脚本，可下载窃密木马；
- 深入分析确认，该事件为外部人员攻破并入侵官方工作邮箱系统所为。

确定威胁



局域网 1[redacted]:55150 连接 美国 [redacted]:25

登录用户：ding[redacted]gov.cn

发送邮件：

FROM:	ding[redacted]gov.cn
TO:	hefalump@umich.edu
主题:	verify the provided data!

邮件附件：

附件名称	类型
copy_ej_0717.doc	Document/Microsoft.DOC[:Word 98-2003]

追踪入侵源头，进行修复和源头阻断，清除了感染源，解除当前威胁并对系统中存在的漏洞进行了修补。

4 应急响应实战

C客户应急响应实战

对数据库登录日志详细分析发现：非法身份“cy***”对数据库部分用户进行大量口令猜破，且成功猜破两个用户口令。

获取网络拓扑结构，定位服务器

事件取证分析

第一时间响应

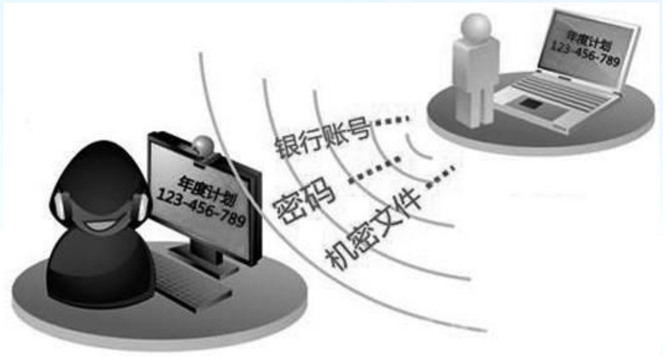
某部委工作人员发现Oracle数据库存在登录异常现象

事件证据生成

人工分析取证发现攻击者在“XXX门户统计软件”的网站后台植入了网页木马病毒，该Linux服务器留下部分工具。

C客户应急响应实战

事件人工深度分析



发现攻击者利用Linux服务器的“脏牛”漏洞提权后，获得操作系统权限，将用户服务器端植入控制操作系统的木马，导致内网被渗透，数据丢失。

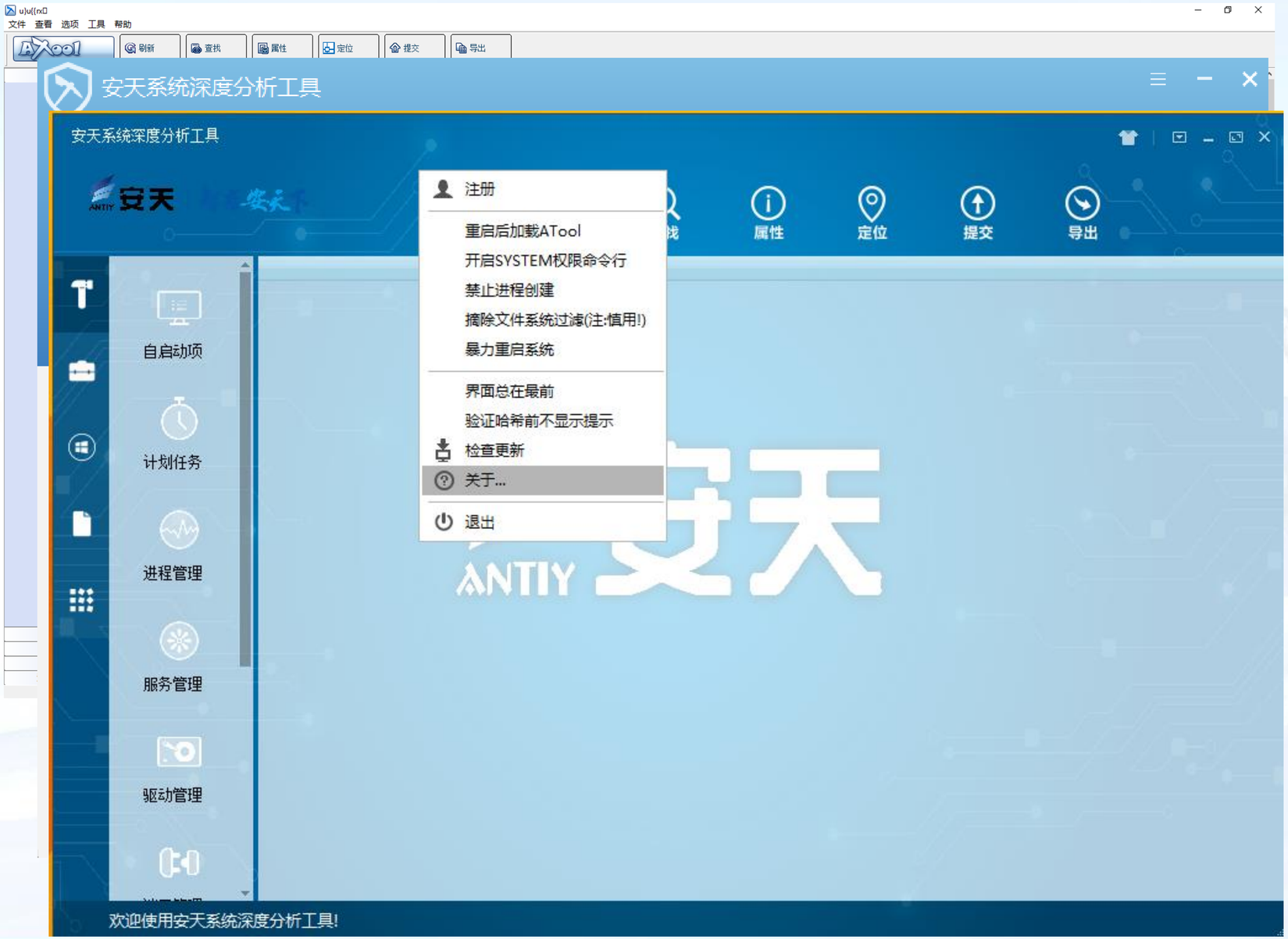
溯源关联分析

解决方案

应急响应人员迅速对网站、服务器存在的漏洞及安全隐患进行全面排查和修复，并提出了进一步的加固建议。

C客户应急响应实战

现场主机检测



5 安天安全服务的使命与愿景

安天安全服务使命

安天的安全服务工作以安天的18年技术研究工作为基础，**以及时响应安全事件和全力保障网络安全为初心，**逐渐开展起来，最终实现**服务于客户、赋能于客户，体现安天的国家安全使命感和责任感。**

技术研究工作

在过去的十余年，安天在恶意代码检测等方向发布了大量技术文献，参与多个信息安全开源项目，在各类学术和产业会议上做技术报告。

应急响应服务

安天为国家有关部门和公众提供重大恶意代码和安全事件的应急响应服务。

安全保障工作

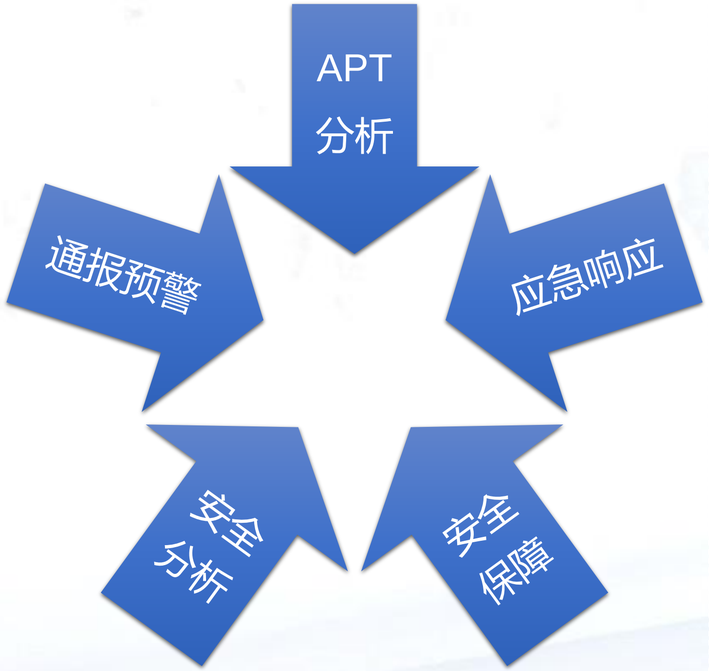
多次在重大网络事故和网络安全事件的响应中发挥关键作用，并荣获重大活动信息安全保卫工作突出贡献奖。

安全服务覆盖范围

安天安全运营中心**成立于2016年11月份**，经过**1年多**的逐步健壮整合发展，现已形成**近两百人**团队规模，覆盖**北京、黑龙江、吉林、辽宁、贵州、云南、湖南、湖北、山西、宁夏、浙江、江西、上海、广东、山东、江苏、广西等地区**。

安全服务价值

国家监管部门安全服务



2017年

两会
一带一路峰会
金砖国家峰会
中国共产党第十九次全国代表大会
中国共产党与世界政党高层对话

重大政治活动安保

重大活动安全保障

基于政企客户安全服务

自主先进核心技术后台支撑

解决方案

- （监管）态势感知和应急响应解决方案
- （军民）大规模、实景化靶场解决方案
- （政企）安全综合感知和安全运营平台
- （行业）金融、能源、交通威胁感知和风控运营平台

安全服务

- 面向资产的安全全周期检测和监测
- SAAS/DAAS数据和情报服务
- 威胁事件响应与调查
- 咨询和整体安全规划与设计

产品矩阵

工具
- 终端动态取证和调查工具
- 网络取证和调查工具
- 恶意代码分析和处理工具
- 威胁情报查询、管理平台
- 威胁排查和专杀工具

设备
- 智甲终端防御系统
- 探海威胁检测系统
- 追影威胁分析系统
- 镇关威胁阻断系统

系统/平台
- 威胁百科查询平台
- 在线威胁鉴定和检测平台
- 移动应用商店监测平台
- 移动仿冒应用监测平台

威胁情报大数据平台
安全运营支撑平台

- 大数据汇聚和融合
- 面向安全认知对抗的多维分析能力
- 可视化应用场景化应用
- 大数据建模未知威胁发现能力

安全运营支撑

服务和协同

场景和数据联动

数据驱动

威胁情报驱动

锻造能力型工程师队伍

依托安天18年的产品和分析技术积累，整合安天优势分析能力，培养和锻造一支能力型工程师队伍。

实战化	专业化	正规化

提供赋能式的安全服务

安全运营中心
Security Operation Center

锻造大批量能力型工程师，基于安天后端赛博超脑支撑平台和产品体系，将安天积累多年的经验赋能给客户，一起**“智者安天下”**！

第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

Thank You

关注安天冬训营官网

关注安天微信公众号

红旗漫卷

敌情想定是前提，网络安全实战化