网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

内部资料

网空威胁框架解析及事件模型在捕获分析中的应用

安天捕获分析技术中心

提纲

- 网空威胁框架解析
- 实战中需要完善
- 网空威胁事件模型
- 威胁事件模型应用案例

01 网空威胁框架解析

CSS网空威胁框架

NSA/CSS 网空威胁框架-详细丰富的行为定义

管理	交互	存在	存在	影响	持续
规划	投放	安装/执行	凭证访问	监控	命令与控制
确定战略和目标	带有附件的鱼叉式钓鱼邮件	磁盘写入	凭证转储	利用弱访问控制	常用端口
分析任务	带有恶意链接的鱼叉式钓鱼邮件	内存中执行代码	网络嗅探	跟踪访问	不常用端口
制定行动计划	网站	解释脚本	键盘记录	被动收集	标准应用层协议
选择战略目标	可移动介质	二进制文件替换	社会工程学	为其他行动创造条件	标准非应用层协议
获准执行行动	SQL注入	命令行	密码破解	渗出	自定义应用层协议
发布行动任务	DNS/缓存投毒	由用户启用	添加或修改凭证	利用CDS/MLS传输	使用链式协议
资源开发	虚拟化攻击	进程注入	劫持活动的凭证	利用脚本收集和过滤数据	使用可移动介质
能力开发	异常网络设备连接	修改配置实现启动	查找文件中的凭证	压缩数据	备用信道
获得资金	受信网站	通过受信应用执行不受信代码	横向移动	节流数据	多协议通信
人员与培训资源	合法的远程访问	计划任务	应用部署软件	将数据存储到制定位置	使用对等连接
建立联盟和伙伴关系	设备交换（非法跨域）	通过服务控制器执行	应用程序本地漏洞利用	通过C2信道回传	建立对等网络
获取行动所需基础设施	利用CDS或MLS配置错误	第三方软件	操作系统漏洞利用	通过非C2信道回传	使用僵尸网络
创建僵尸网络	物理网桥	利用远程管理服务	采用登录脚本	通过其他网络介质回传	加密通信
供应链预置	自动传输可信服务	利用系统接口实现启动	利用对等连接	从本地系统收集	使用多层加密
研究	CDS或MLS穿透	传输工具包	远程交互式登录	从网络资源收集	使用标准加密
确定情报差距	供应链/可信源入侵	内部侦察	利用远程管理服务	有计划的传输	使用自定义加密
确定能力差距	无线接入	账户枚举	远程服务	点对点传输	发送心跳
收集情报	借助公共网络基础设施实施侵害	文件系统枚举	通过可移动介质复制	通过物理介质渗出	自动使用C2
	短信（SMS）	组权限枚举	共享webroot目录	边信道（数据散射）	手动使用C2
准备	二维码	本地网络连接枚举	污染共享内容	编码数据	规避
侦察	编码数据	本地网络设置枚举	远程文件共享	破解加密	编码数据
网络爬取	木马	操作系统枚举	中继通信	泄露数据/信息	加密数据
网络地形绘制	利用	所有者/用户枚举	利用密码哈希认证	修改	使用合法凭证
利用社交媒体	应用程序本地漏洞利用	进程枚举	利用ticket认证	破解加密	文件填充
扫描	操作系统漏洞利用	软件枚举	持久化	修改数据	禁用安全产品
选择战术目标	应用程序远程漏洞利用	服务枚举	利用合法凭证	造成物理影响	干扰安全产品
目标调查	社会工程学	窗口枚举	辅助功能	克隆数据、系统	直接访问磁盘
TCP指纹识别	虚拟化攻击	键盘记录	系统启动时自动加载	更改系统进程的运行状态	阻止主机信标上传
Banner提取	破解加密	屏幕捕获	库搜索劫持	修改进程结果	恶意软件免杀处理
社会工程学	利用弱访问控制	音视频录制	创建新服务	修改机器间通讯	删除日志数据
识别密码系统	远程shell	提权	路径拦截	篡改网站	操纵受信任的进程
凭证骗取	缓冲区溢出漏洞	使用合法凭证	计划任务	拒绝	进程注入
边信道（数据散射）	漏洞利用工具包	辅助功能	替换服务文件	分布式拒绝服务（DDoS）	仿冒合法文件
环境预制	零日漏洞利用	系统启动时自动加载	链接修改	加密数据使其不可用	将文件存储在非常规位置
建立跳板	反检测编码	库搜索劫持	修改文件类型关联	拒绝服务/中断	混淆数据
应用数据文件中添加可利用点	劫持	创建新服务	修改BIOS	降低性能	使用rootkit
分配行动所需基础设施	冒充/欺骗	路径拦截	安装hypervisor rootkit	破坏	利用受信应用执行不受信代码
网站植入或预埋	重放攻击	计划任务	使用登录脚本	部分磁盘/操作系统删除（损坏）	软件打包
预置载荷	协议滥用	替换服务文件	修改MBR	全部磁盘/操作系统删除（变砖）	使用签名内容
建立物理抵近点	利用受信关系	链接修改	修改现有服务	数据删除（部分）	为恶意内容签名
持续		操纵受信进程	修改服务配置	数据删除（全部）	删除工具包
分析、评估、反馈		进程注入	Web shell	破坏硬件	根据环境调整行为
针对性改进		应用程序本地漏洞利用	后门		延迟活动
实施效果评估		操作系统漏洞利用			采用反逆向措施
		修改服务配置			采用反取证措施
					仿冒合法流量
					规避数据大小限制

攻击阶段

管理			准备		交互		存在					影响				持续		
规划	资源开发	研究	侦察	环境预制	投放	利用	安装、执行	内部侦察	提权	凭证访问	横向移动	持久化	监控	渗出	修改	拒绝	破坏	分析、评估、反馈	命令与控制	规避

管理、准备

管理		准备		
规划	资源开发	研究	侦察	环境预制
确定战略和目标 分析任务 制定行动计划 选择战略目标 获准执行行动 发布行动任务	能力开发 获得资金 人员与培训资源 建立联盟和伙伴关系 获取行动所需基础设施 创建僵尸网络 供应链预置	确定情报差距 确定能力差距 收集情报	网络爬取 网络地形绘制 利用社交媒体 扫描 选择战术目标 目标调查 TCP指纹识别 Banner提取 社会工程学 识别密码系统 凭证骗取 边信道（数据散射）	建立跳板 应用数据文件中添加可利用点 分配行动所需基础设施 网站植入或预埋 预置载荷 建立物理抵近点

交互

交互			
投放		利用	
带有附件的鱼叉式钓鱼邮件	利用CDS或MLS配置错误	应用程序本地漏洞利用	漏洞利用工具包
带有恶意链接的鱼叉式钓鱼邮件	物理网桥	操作系统漏洞利用	零日漏洞利用
网站	自动传输可信服务	应用程序远程漏洞利用	反检测编码
可移动介质	CDS或MLS穿透	社会工程学	劫持
SQL注入	供应链/可信源入侵	虚拟化攻击	冒充/欺骗
DNS/缓存投毒	无线接入	破解加密	重放攻击
虚拟化攻击	借助公共网络基础设施实施侵害	利用弱访问控制	协议滥用
异常网络设备连接	短信（SMS）	远程shell	利用受信关系
受信网站	二维码	缓冲区溢出漏洞	
合法的远程访问	编码数据		
设备交换（非法跨域）	木马		

存在

存在					
安装/执行	内部侦察	提权	凭证访问	横向移动	持久化
磁盘写入 内存中执行代码 解释脚本 二进制文件替换 命令行 由用户启用 进程注入 修改配置实现启动 通过受信应用执行不受信代码 计划任务 通过服务控制器执行 第三方软件 利用远程管理服务 利用系统接口实现启动 传输工具包	账户枚举 文件系统枚举 组权限枚举 本地网络连接枚举 本地网络设置枚举 操作系统枚举 所有者/用户枚举 进程枚举 软件枚举 服务枚举 窗口枚举 键盘记录 屏幕捕获 音视频录制	使用合法凭证 辅助功能 系统启动时自动加载 库搜索劫持 创建新服务 路径拦截 计划任务 替换服务文件 链接修改 操纵受信进程 进程注入 应用程序本地漏洞利用 操作系统漏洞利用 修改服务配置	凭证转储 网络嗅探 键盘记录 社会工程学 密码破解 添加或修改凭证 劫持活动的凭证 查找文件中的凭证	应用部署软件 应用程序本地漏洞利用 操作系统漏洞利用 采用登录脚本 利用对等连接 远程交互式登录 利用远程管理服务 远程服务 通过可移动介质复制 共享webroot目录 污染共享内容 远程文件共享 中继通信 利用密码哈希认证 利用ticket认证	利用合法凭证 辅助功能 系统启动时自动加载 库搜索劫持 创建新服务 路径拦截 计划任务 替换服务文件 链接修改 修改文件类型关联 修改BIOS 安装hypervisor rootkit 使用登录脚本 修改MBR 修改现有服务 修改服务配置 Web shell 后门

影响

影响					
监控	渗出		修改	拒绝	破坏
利用弱访问控制 跟踪访问 被动收集 为其他行动创造条件	利用弱访问控制 跟踪访问 被动收集 为其他行动创造条件 渗出 利用CDS/MLS传输 利用脚本收集和过滤数据 压缩数据 节流数据 将数据存储到制定位置 通过C2信道回传 通过非C2信道回传	通过其他网络介质回传 从本地系统收集 从网络资源收集 有计划的传输 点对点传输 通过物理介质渗出 边信道（数据散射） 编码数据 破解加密 泄露数据/信息	破解加密 修改数据 造成物理影响 克隆数据、系统 更改系统进程的运行状态 修改进程结果 修改机器间通讯 篡改网站	分布式拒绝服务（DDoS） 加密数据使其不可用 拒绝服务/中断 降低性能	部分磁盘/操作系统删除（损坏） 全部磁盘/操作系统删除（变砖） 数据删除（部分） 数据删除（全部） 破坏硬件

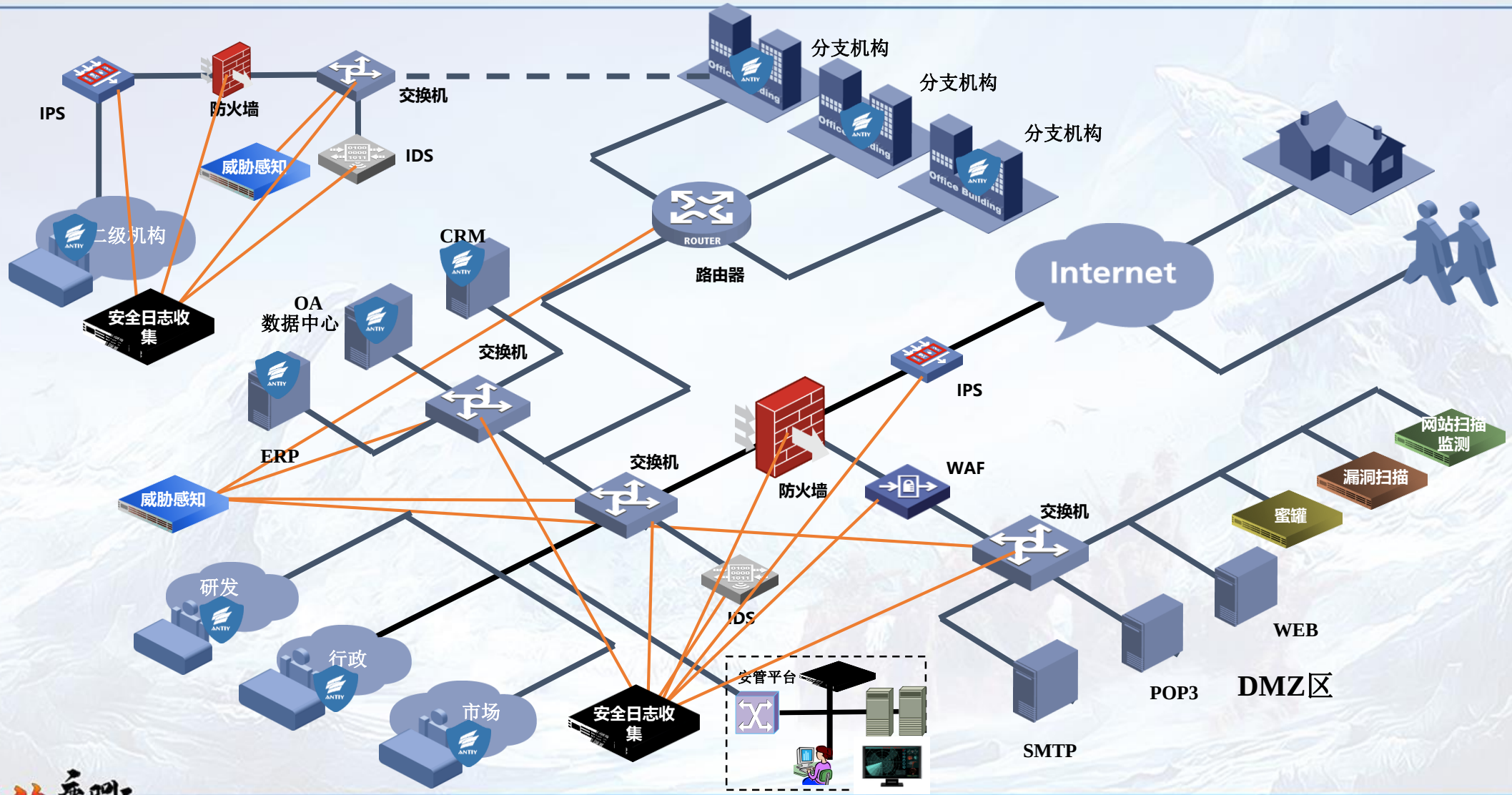
持续

持续				
分析、评估、反馈	命令与控制		规避	
针对性改进 实施效果评估	常用端口 不常用端口 标准应用层协议 标准非应用层协议 自定义应用层协议 使用链式协议 使用可移动介质 备用信道 多协议通信 使用对等连接	建立对等网络 使用僵尸网络 加密通信 使用多层加密 使用标准加密 使用自定义加密 发送心跳 自动使用C2 手动使用C2	编码数据 加密数据 使用合法凭证 文件填充 禁用安全产品 干扰安全产品 直接访问磁盘 阻止主机信标上传 恶意软件免杀处理 删除日志数据 操纵受信任的进程 进程注入 仿冒合法文件 将文件存储在非常规位置	混淆数据 使用rootkit 利用受信应用执行不受信代码 软件打包 使用签名内容 为恶意内容签名 删除工具包 根据环境调整行为 延迟活动 采用反逆向措施 采用反取证措施 仿冒合法流量 规避数据大小限制

02 实战需要完善补充

实战结合
钻石模型
STIX

威胁感知数据来源多样

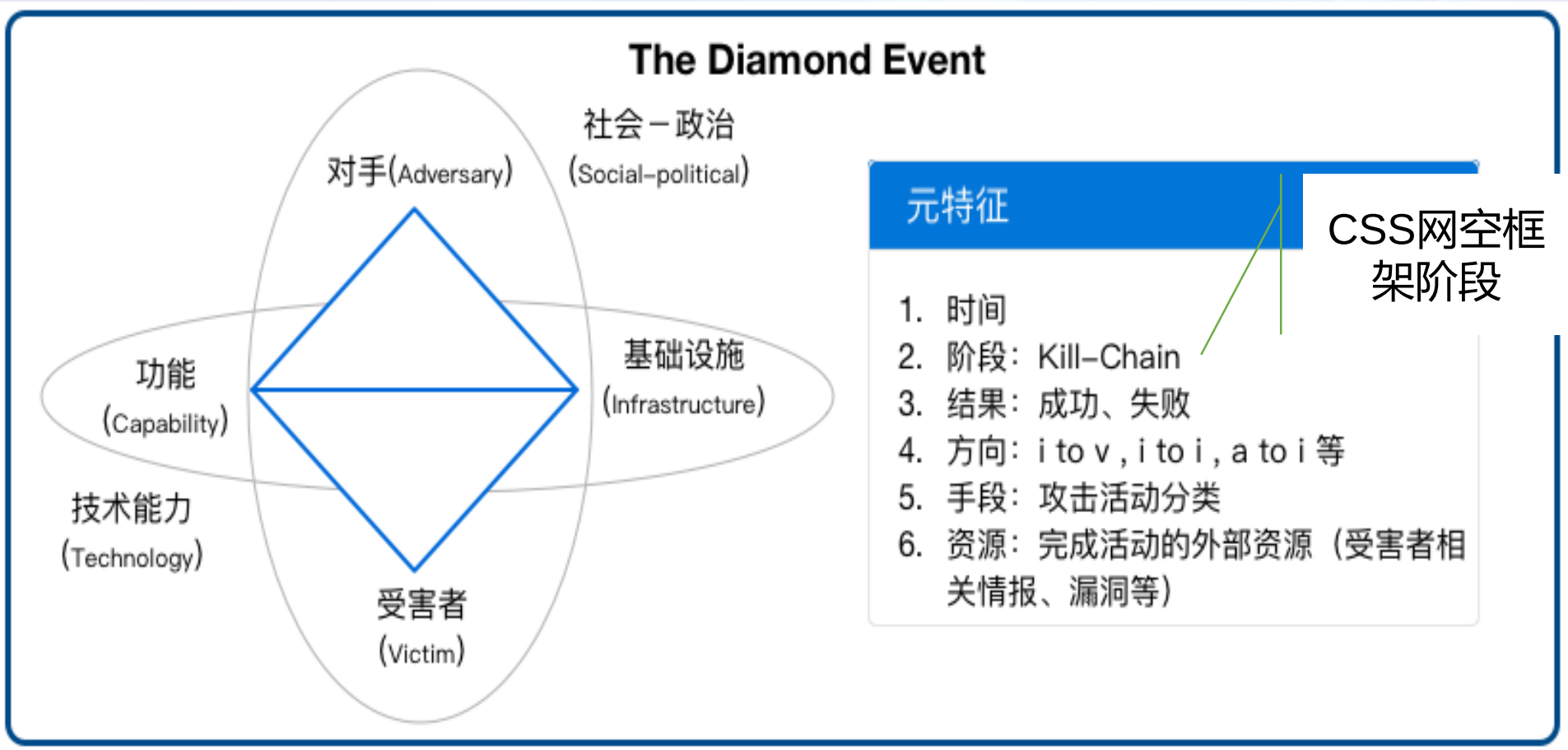

IPS
防火墙
交换机
IDS
威胁感知
分支机构
分支机构
分支机构
Office Building
二级机构
安全日志收集
CRM
OA
数据中心
交换机
ROUTER
路由器
Internet
ERP
威胁感知
交换机
IPS
防火墙
WAF
交换机
网站扫描监测
漏洞扫描
蜜罐
研发
行政
市场
IDS
安管平台
安全日志收集
WEB
POP3
DMZ区
SMTP

多元异构数据

对框架进一步丰富

- 威胁行为补充
  - 实战中补充更多威胁行为点
- 威胁事件主体客体补充
  - 攻击者、攻击设施、受害资产等描述
- 需要补充非威胁事件的表达
  - 基本行为
  - 网空实体
- 事件行为之间关系表达
  - 需要支持关联关系推理表达

钻石模型


The Diamond Event
社会－政治
(Social-political)
对手(Adversary)
功能
(Capability)
基础设施
(Infrastructure)
技术能力
(Technology)
受害者
(Victim)
元特征
1. 时间
2. 阶段：Kill-Chain
3. 结果：成功、失败
4. 方向：i to v , i to i , a to i 等
5. 手段：攻击活动分类
6. 资源：完成活动的外部资源（受害者相关情报、漏洞等）
CSS网空框架阶段

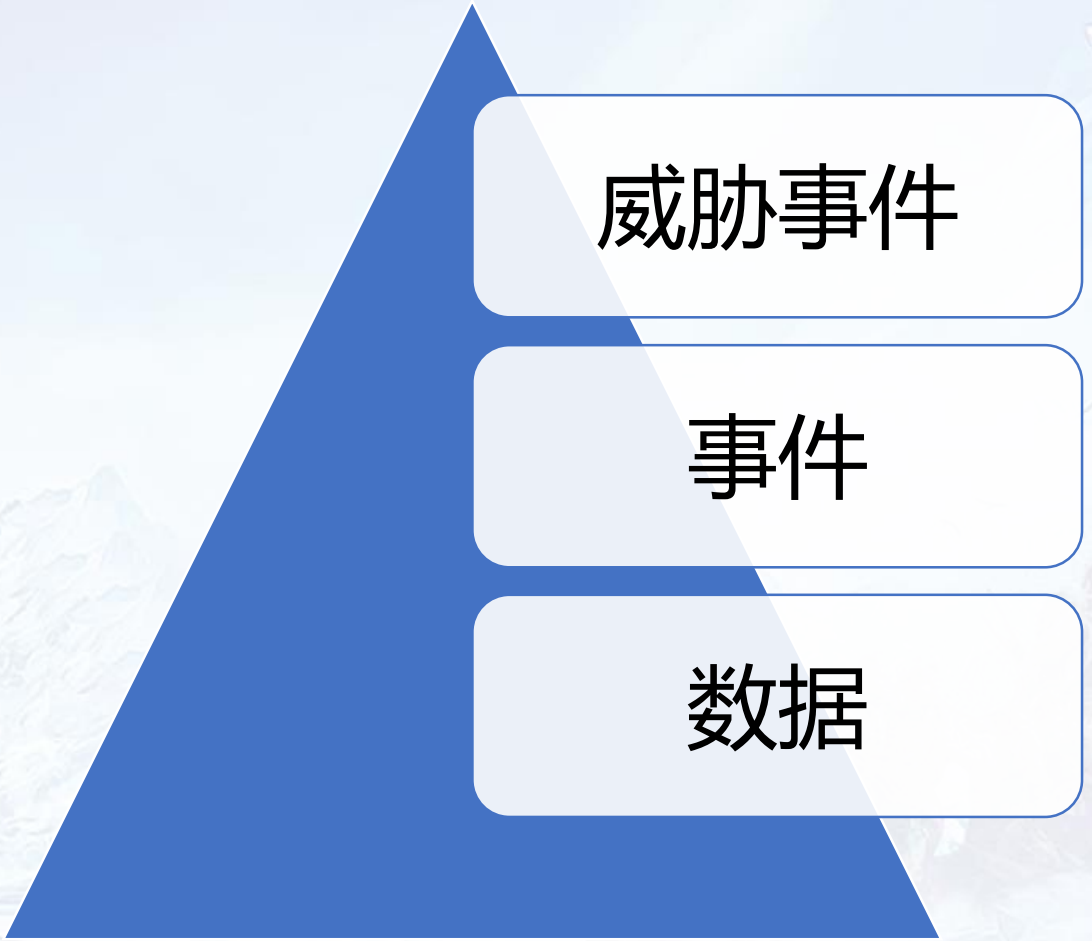
STIX-实体较多


```
{
  "type": "attack-pattern",
  "id": "attack-pattern--01",
  "created": "2015-05-15T09:11:12.515000Z",
  "modified": "2015-05-15T09:11:12.515000Z",
  "name": "Initial Compromise",
  "external_references": [
    {
      "source_name": "capec",
      "description": "spear phishing",
      "external_id": "CAPEC-163"
    }
  ],
  "kill_chain_phases": [
    {
      "kill_chain_name": "mandiant-attack-
                          lifecycle-model",
      "phase_name": "initial-compromise"
    }
  ]
}
```

03 网空威胁事件模型

基础事件
威胁事件
知识图谱
数据转换

网空威胁事件模型



事件

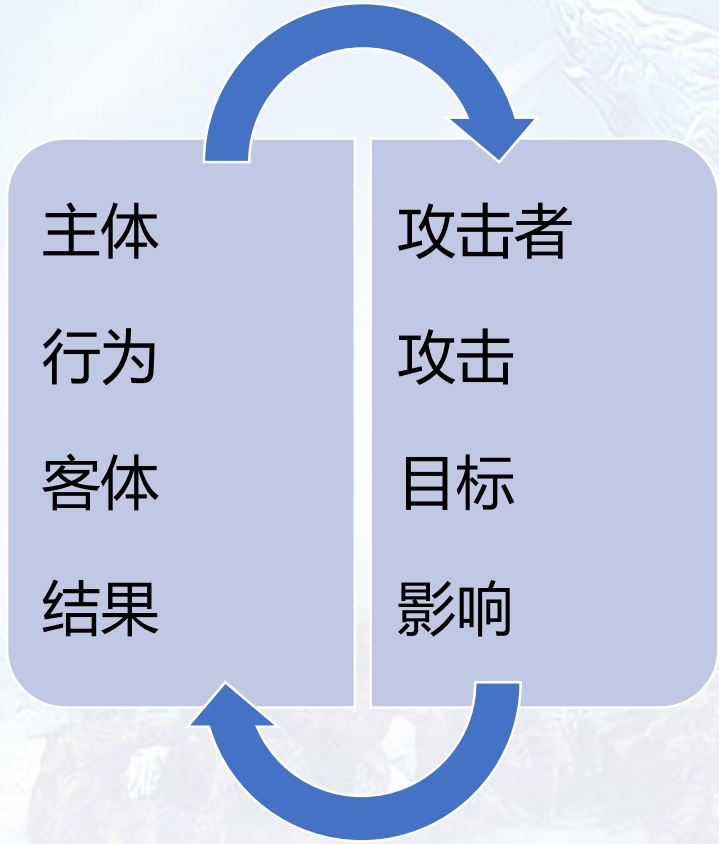
- 核心特征
  - 主体（user）： 网络世界实体
  - 客体(object) ： 动作目标实体
  - 行为（Action）： 行为主体作用于行为客体时所应用的工具和使用的方法
- 元特征
  - 时间
  - 位置
  - 结果(result)

非威胁事件表达

- 需要对原始数据进行抽象表达
- 非威胁类型的事件可以用于攻击链补充
- 非威胁事件通过和威胁事件关联可以推理转化
- 非威胁行为
  - 恶意程序访问正常网站测试连通性（从网络测观察不到恶意）
  - 黑客笔记本登录黑客控制服务器（登录是非威胁的）

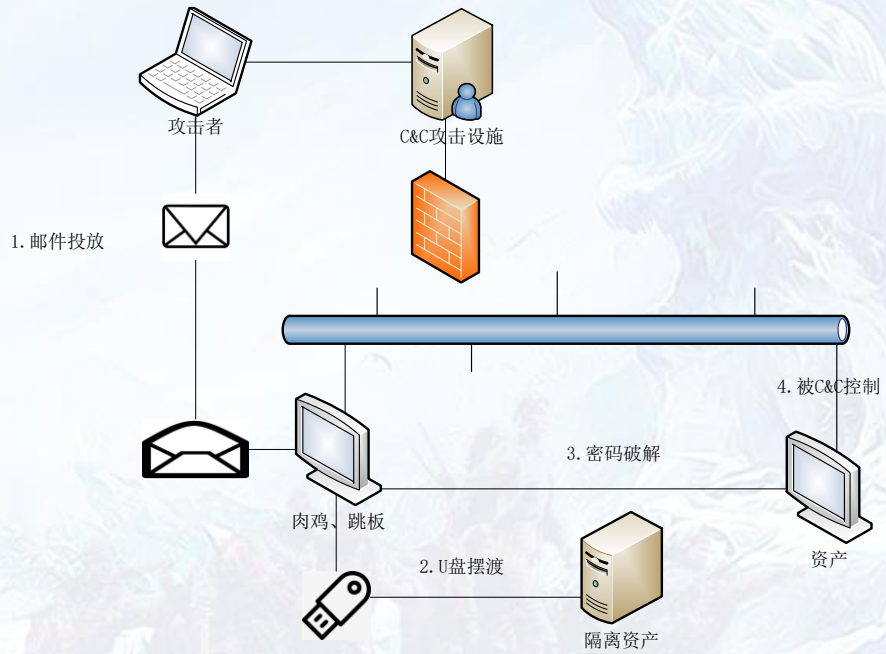
威胁事件（incident）

- 核心特征
  - 攻击者Attackers（攻击人、攻击设施）
  - 攻击行为attack （工具、方法, NSA-CSS行为）
  - 攻击目标Target （受攻击组织、资产）
- 元特征
  - 时间
  - 位置
  - 攻击结果
  - 阶段（NSA-CSS行为阶段划分）



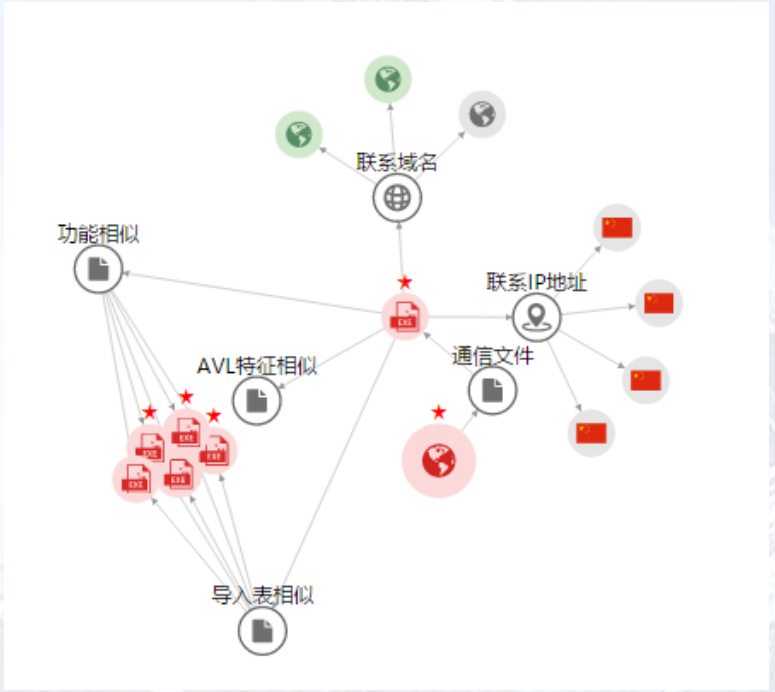
威胁事件-攻击设施

- 攻击者拥有
  - 购买、租赁用于攻击、控制、放置恶意程序网络主机
  - IP地址、域名、邮件地址、USB设备
- 攻击者利用
  - 第三方空间、博客
  - 跳板、肉鸡、代理



可融合威胁与非威胁事件的知识图谱

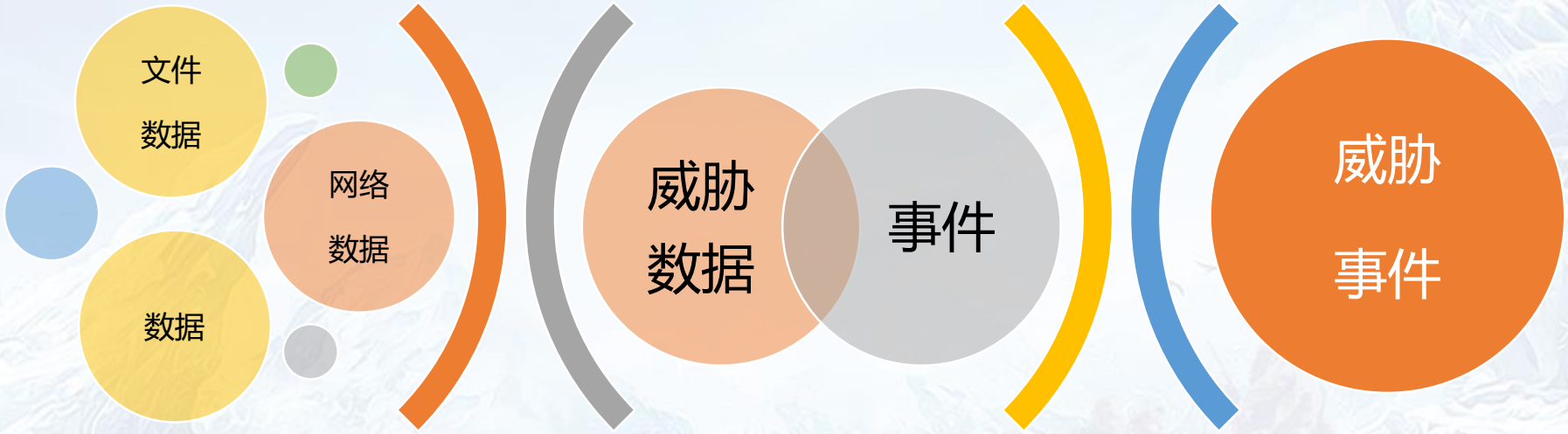
非威胁事件知识图谱	威胁事件知识图谱
实体-关系-实体	实体-关系-实体
实体-属性-值	实体-属性-值
物理实体：用户、计算机IP、目标计算机	物理实体：攻击者、受害者、攻击设施、受害资产
逻辑实体：工具、进程、域名、账户、数据	逻辑实体：恶意程序、受害文件、账户、数据
关系：连接、登录、读取、上传、下载、复制、控制、请求域名	关系：1）行为阶段：扫描、入侵、安装、控制、恶意目的 2）具体行为：漏洞入侵、密码爆破、邮件投放



CSS网空威胁框架行为与实体关系实例

威胁阶段行为	产品/系统	实例	实体关系
侦查->扫描	捕风蜜罐|探海流量	端口扫描	扫描IP、扫描、目标IP
传输->带有恶意链接的钓鱼邮件	追影沙箱	恶意链接钓鱼邮件	发件人、收件人、URL
传输->带有附件的钓鱼邮件	追影沙箱	恶意附件钓鱼邮件	发件人、收件人、附件文件
传输->SQL注入	捕风蜜罐|探海流量|WAF		攻击设施IP、目标IP
传输->木马	探海流量|捕风蜜罐|追影沙箱	远控木马下载	放马IP、URL、样本、目标IP
传输->可移动介质	追影沙箱|智甲终端	移动介质传播	目标IP、U盘
漏洞利用->远程代码执行漏洞	捕风蜜罐	例：ms17-010漏洞利用	攻击设施IP、目标IP
漏洞利用->应用程序漏洞	追影沙箱	例：CVE-2012-0158漏洞	样本、目标主机IP
凭证访问->密码破解	捕风蜜罐	弱密码猜解	攻击设施IP、目标IP
漏洞利用->缓冲区溢出漏洞	捕风蜜罐	缓冲区溢出攻击	攻击设施IP、目标IP
安装/执行->命令行	捕风蜜罐|智甲终端	程序执行cmd命令	目标IP、样本
安装/执行->计划任务	捕风蜜罐|智甲终端	计划任务	目标IP、样本
安装/执行->使用可信应用程序执行不受信用代码	捕风蜜罐|智甲终端	系统进程释放可执行程序	目标IP、样本
安装/执行->木马	捕风蜜罐|智甲终端	运行木马程序	目标IP、样本

转换



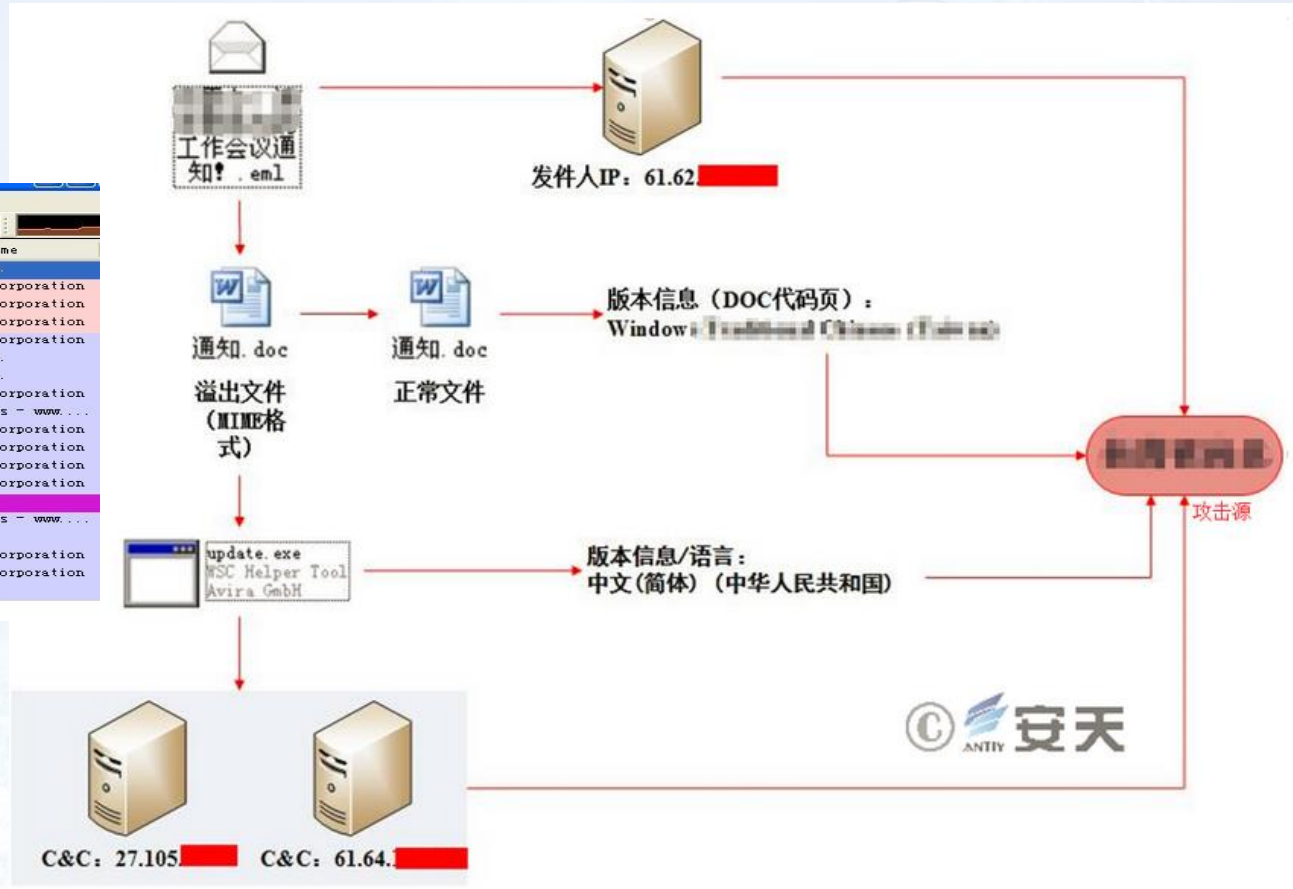
04 网空威胁事件模型防御应用

APT案例

蜜网攻击捕获案例

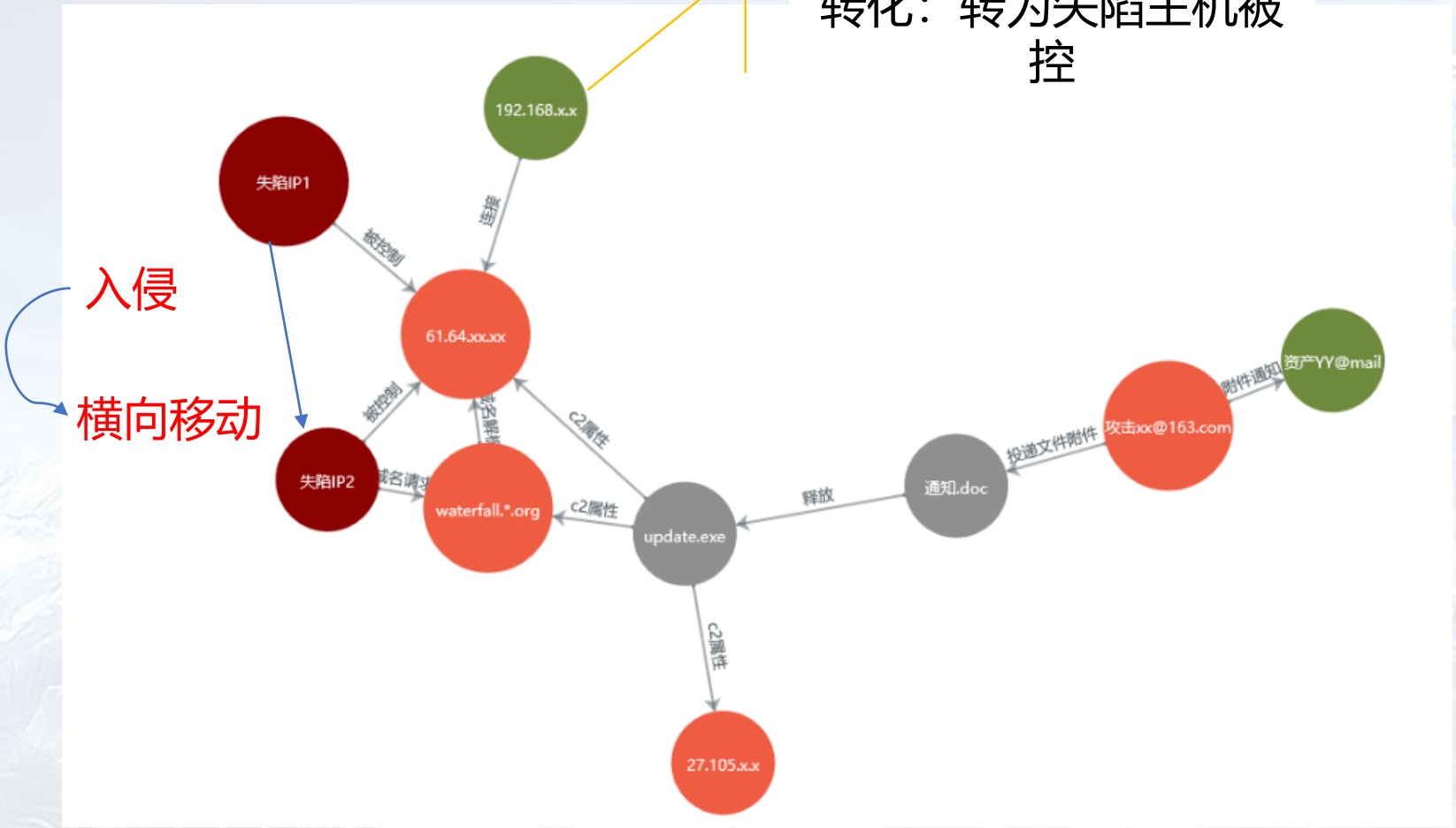
绿斑APT


File Options View Process Find Users Help
Process PID CPU Description Company Name
VMwareServ... 1616 VMware Tools Service VMware, Inc.
alg.exe 168 Application Layer Gat... Microsoft Corporation
svchost.exe 1860 Generic Host Process ... Microsoft Corporation
lsass.exe 716 LSA Shell (Export Ver... Microsoft Corporation
explorer.exe 1340 Windows Explorer Microsoft Corporation
VMwareTray.exe 1988 VMware Tools tray app... VMware, Inc.
VMwareUser.exe 1996 VMware Tools Service VMware, Inc.
ctfmon.exe 2008 CTF Loader Microsoft Corporation
procexp.exe 752 Sysinternals Process ... Sysinternals - www....
cmd.exe 304 Windows Command Proce... Microsoft Corporation
conime.exe 1608 Console IME Microsoft Corporation
notepad.exe 1144 记事本 Microsoft Corporation
IEXPLORE.EXE 248 Internet Explorer Microsoft Corporation
hfs.exe 1172 1.54 rejetto
Tcpview.exe 1332 TCP/UDP endpoint viewer Sysinternals - www....
IPAnalyse.exe 1180 IPAnalyse Microsoft ...
msimn.exe 2528 Outlook Express Microsoft Corporation
WINWORD.EXE 3592 Microsoft Office Word Microsoft Corporation
update.exe 3612 WSC Helper Tool Avira GmbH


工作会议通知!.eml
发件人IP：61.62
通知.doc
溢出文件（MIME格式）
通知.doc
正常文件
版本信息（DOC代码页）：
Window
update.exe
WSC Helper Tool
Avira GmbH
版本信息/语言：
中文(简体)（中华人民共和国）
攻击源
C&C：27.105
C&C：61.64.
© ANTIY 安天

攻击链知识图谱

更早时间审计记录连接转化：转为失陷主机被控

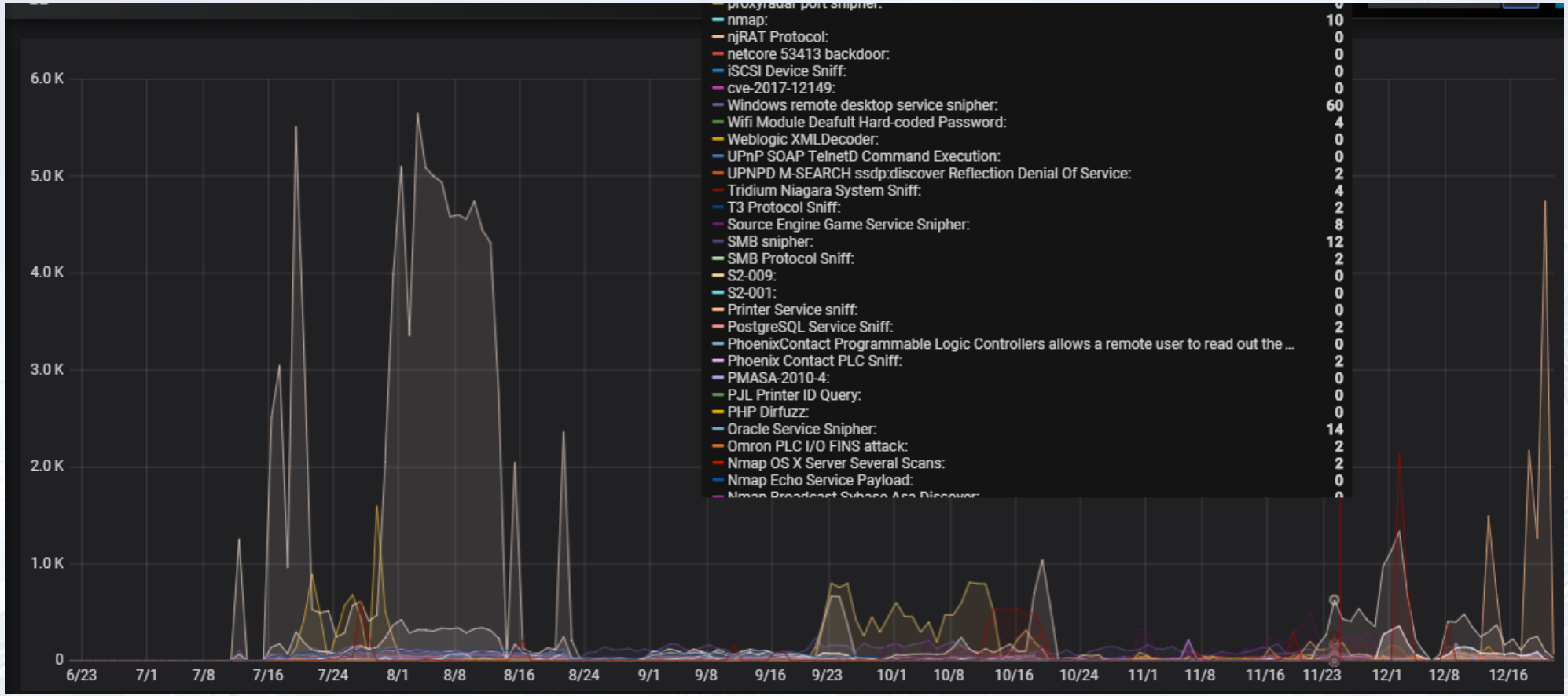


循环的三大步骤

准备-扫描

数据源自安天捕风蜜网系统

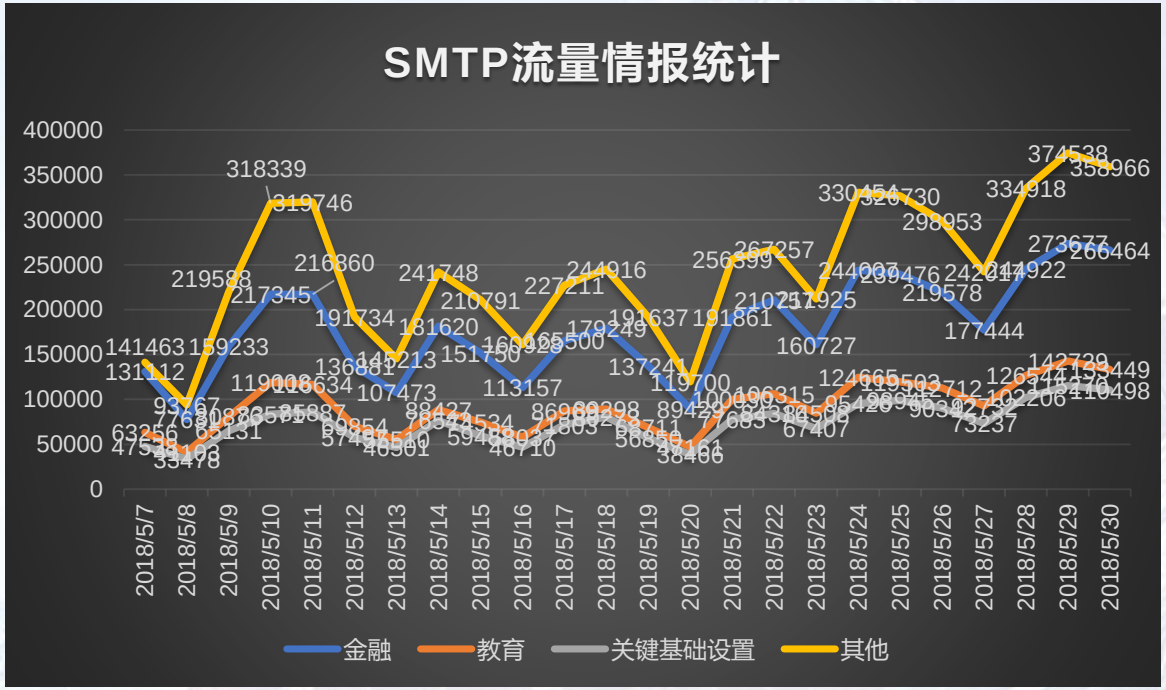
入侵-利用



数据源自安天捕风蜜网系统

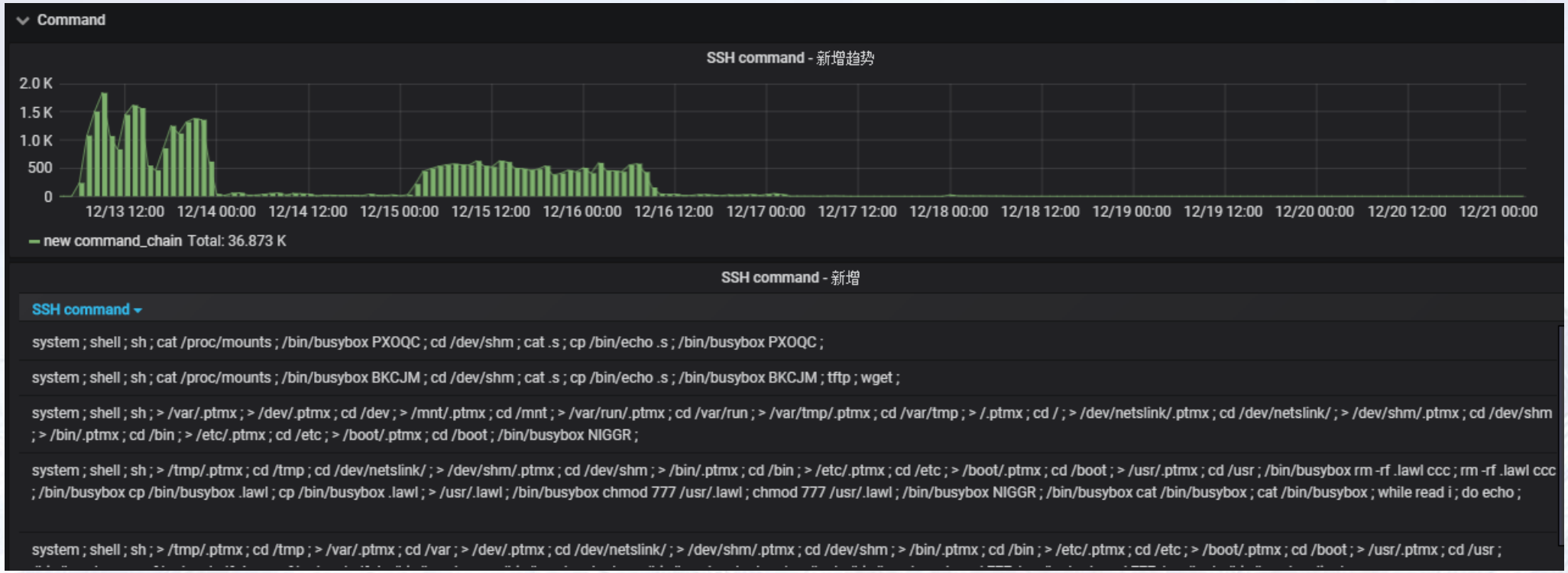
入侵-投放

- 企业的邮箱有**8,261,027**个，而这些企业邮箱中，95%的比例位于日本，
- @softbank（软银）、@standardbank（标准银行）、@hbtoyota（丰田Toyota）、wvc.edu（文纳赤谷学院）、yahoo（雅虎）等大型金融、教育、互联网、关键基础设施等类型企业。
- 也有少部邮箱为中国境内的邮件服务商用户。
- 2018年，5月28日，在监测到的SMTP流量情报中，发现有黑客正通过“鱼叉攻击”手段向@softbank（软银）、@yahoo等金融、关键基础设施等类型的企业传播最新变异的勒索木马——GANDCRAB v3。



数据源自安天捕风蜜网系统

存在-安装

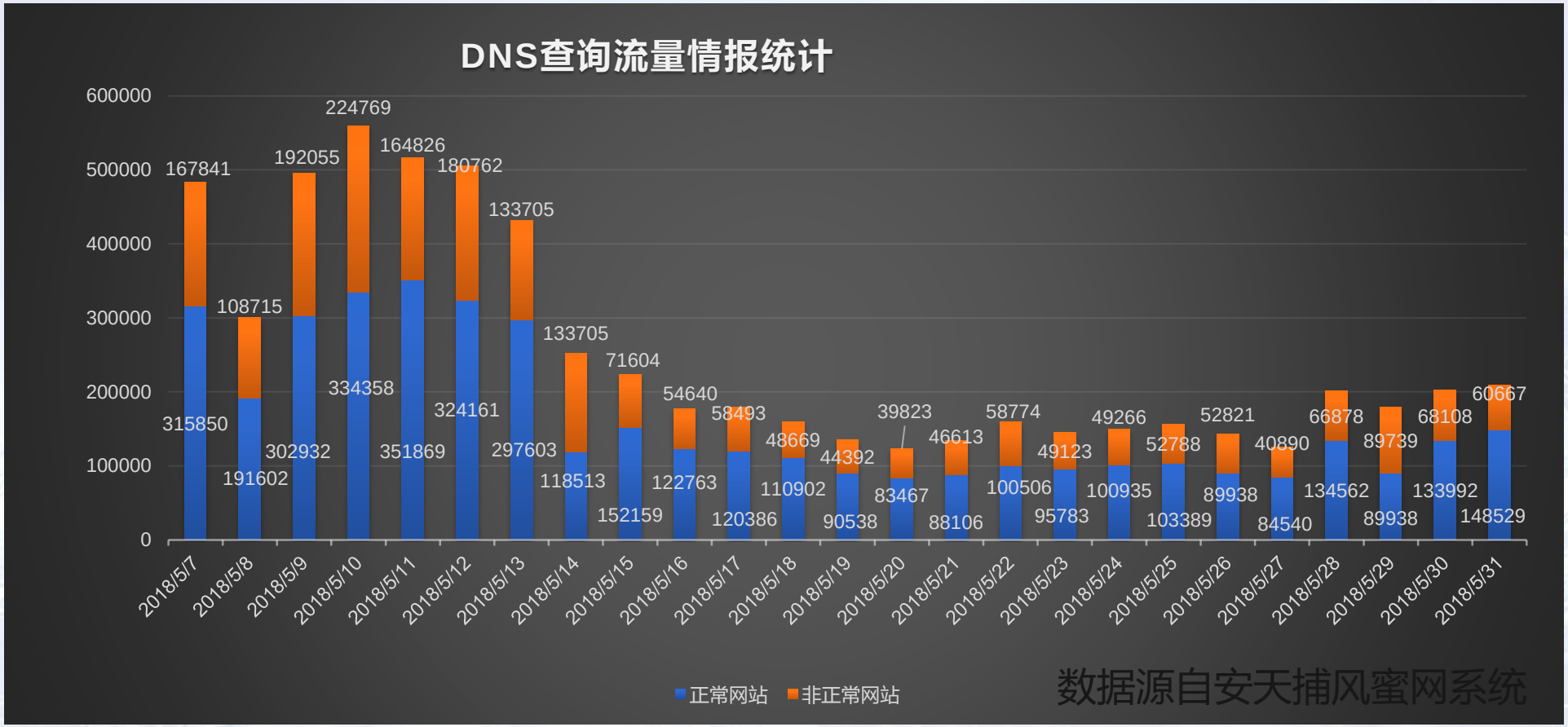


数据源自安天捕风蜜网系统

控制

family	network.ip	network.domain	network.port
Trojan/Linux.Ganiw	115.231.218.64:8226	fk.appledoesnt.com:30000	-
Trojan/Linux.Ganiw	118.24.26.156:8880	shenhaozhe.com:55000	-
Trojan/Linux.MrBlack	223.111.145.217	-	828
Trojan/Linux.MrBlacK	132.232.194.49	-	7777
Trojan/Linux.Ganiw	115.231.218.64:8226	fk.appledoesnt.com:30000	-
Trojan/Linux.Mayday	59.47.72.179:10991, 208.98.15.162:2847, 93.115.86.209:10991	-	-
Trojan/Linux.Mayday	95.47.72.172:52000, 208.98.15.162:2847, 93.115.86.209:10991	-	-
Trojan/Linux.MrBlack	115.231.222.151	-	8000
Trojan/Win32.Ceatrg	-	shadow-ghost.no-ip.org	1337

域名请求


DNS查询流量情报统计
600000
500000
400000
300000
200000
100000
0
167841
315850
108715
191602
192055
302932
224769
334358
164826
351869
180762
324161
133705
297603
133705
118513
71604
152159
54640
122763
58493
120386
48669
110902
44392
90538
39823
83467
46613
88106
58774
100506
49123
95783
49266
100935
52788
103389
52821
89938
40890
84540
66878
134562
89739
89938
68108
133992
60667
148529
2018/5/7
2018/5/8
2018/5/9
2018/5/10
2018/5/11
2018/5/12
2018/5/13
2018/5/14
2018/5/15
2018/5/16
2018/5/17
2018/5/18
2018/5/19
2018/5/20
2018/5/21
2018/5/22
2018/5/23
2018/5/24
2018/5/25
2018/5/26
2018/5/27
2018/5/28
2018/5/29
2018/5/30
2018/5/31
正常网站
非正常网站
数据源自安天捕风蜜网系统

目的影响

BoT样本

提取C&C

多地通信C&C获取攻击目的

传播其它恶意程序

DDoS攻击　　窃取文档

加密勒索

网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰