基于沙箱的威胁情报输出

主讲人 追影 康学斌

课程提纲Contents

- 威胁与价值
- 沙箱分析价值输出
- 协同实例

ANTIY 安天 | 智者安天下

威胁情报与价值

- 威胁
- 价值
- 流程

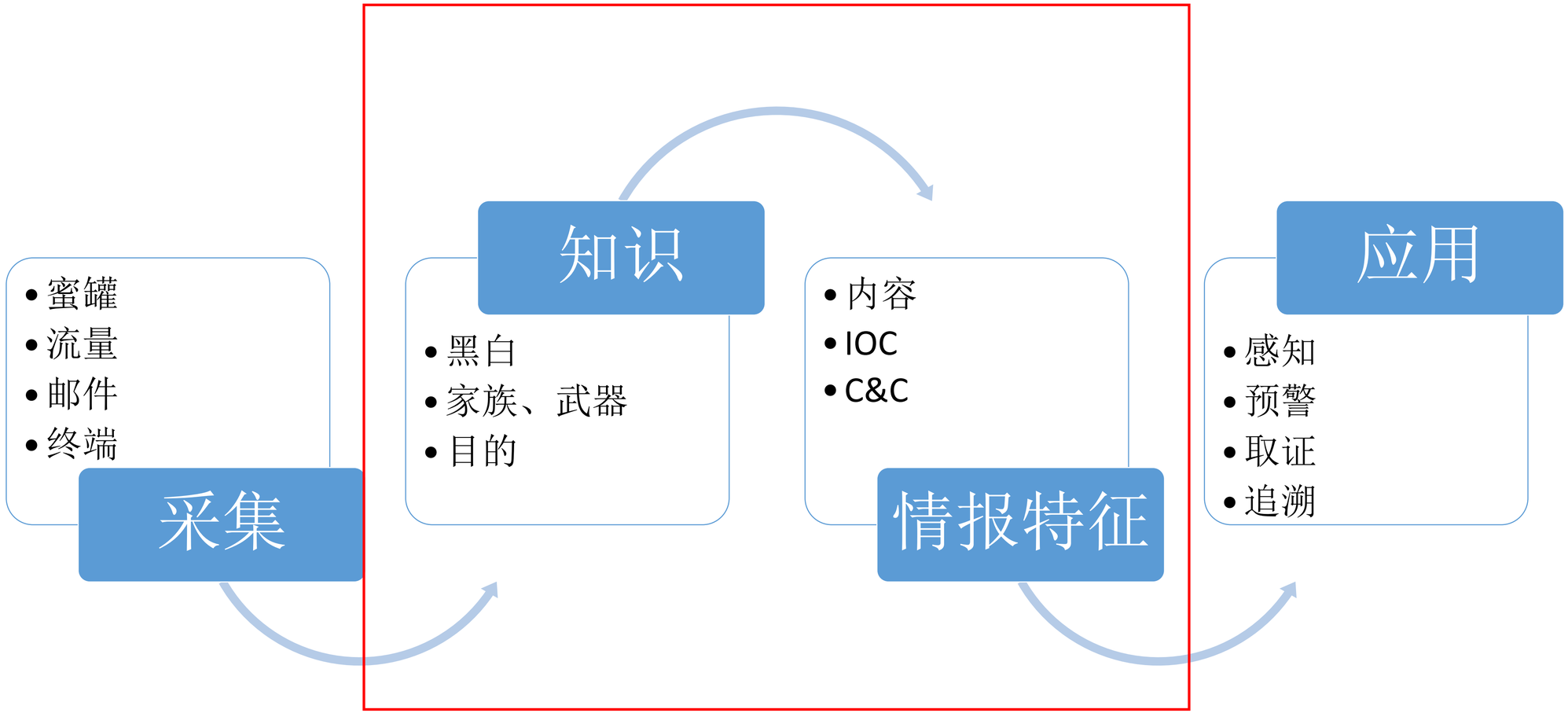
提升网络威胁监控预警溯源能力

- 如何监控到更多僵木蠕活动？
- APT等组织发现监控？
- DDoS攻击信息掌握？
- 终端取证验证？
- 如何追溯攻击者？
- 基于威胁类型进行决策

沙箱可支持环境

- 邮件服务器安全分析
- 流量还原文件分析
- 蜜罐捕获文件分析
- 终端联动文件分析
- SOC/SIME平台文件分析

沙箱输入输出情报流程



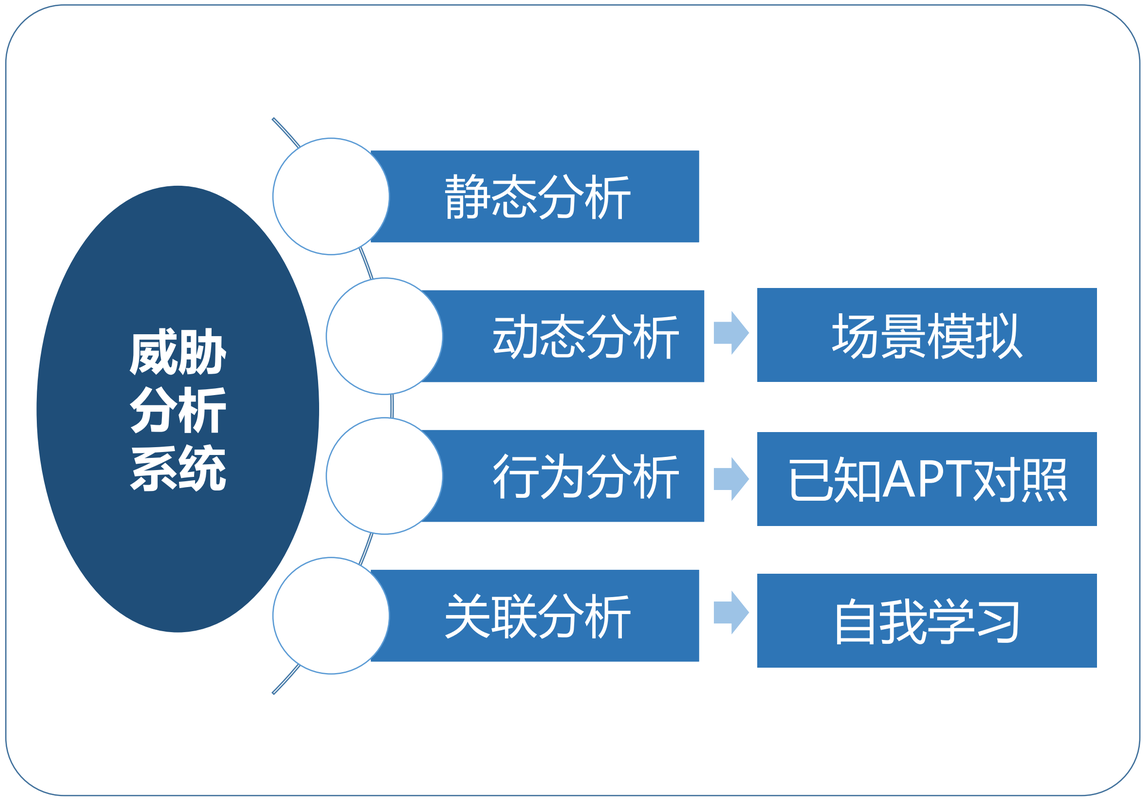
沙箱分析

- 知识
- 特征
- C&C

动静结合，深度分析

多来源

- 安天智甲
- 安天镇关
- 安天探海
- 手工提交
- 第三方设备

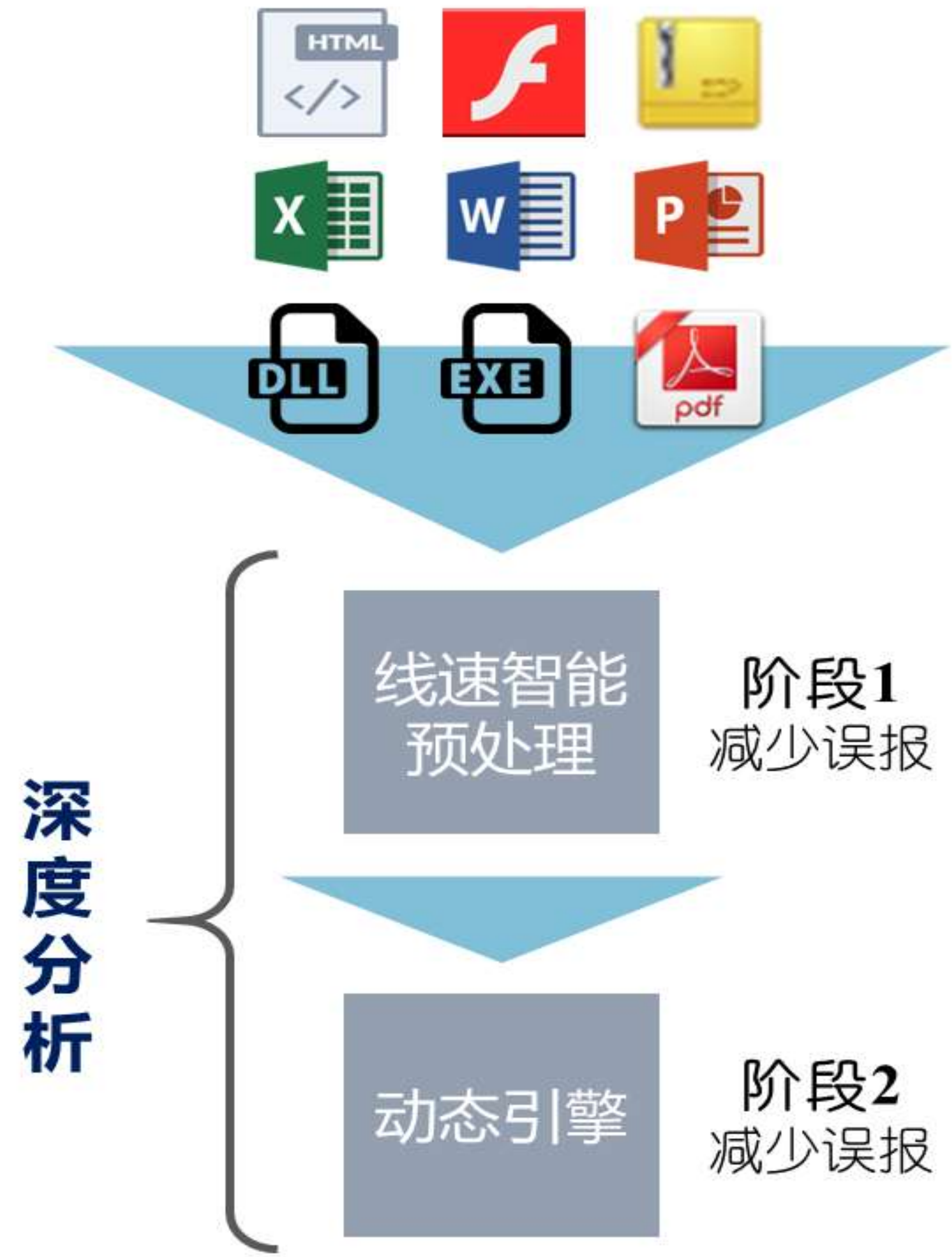


- 分析报告
- 处置建议

人工关联分析

本地化沙箱动态分析

1. 可疑文件传输异步分析
2. 发现未知恶意文件
3. 发现0day/1day漏洞
4. 行为识别免杀木马
5. 知识赋予
6. 提供C&C联动



沙箱分析赋予知识

- 判别黑白
- 威胁分类
  - RAT、DDoS、勒索、APT
- 家族
  - 生成器关联、家族特征
- 组织
  - APT组织、黑产团伙

病毒名：Trojan[RAT]/Win32.Zegost.DQ

家族：Zegost

核心目的：RAT

标签：RAT、Zegost、Backdoor

描述：Trojan[RAT]/Win32.Zegost是一种后门类远程控制木马，有延时行为，程序通过Lc
的PE动态库dll文件，来执行反向连接。接受远程命令完成有害操作：发送系统信息，
等。

实例：MD5:edcca6090c663b63b689dce57e55538c

参考：

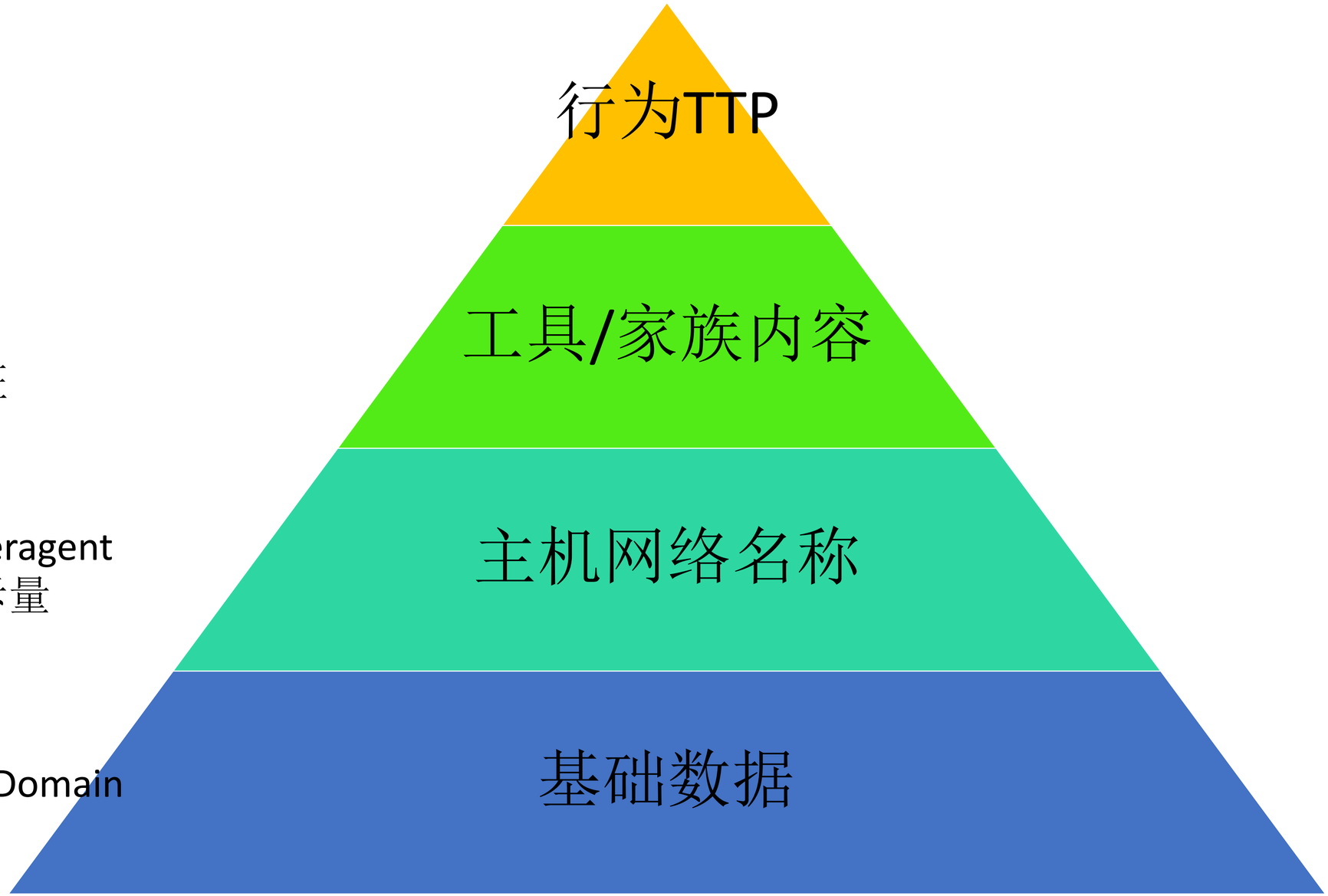
[1] http://telussecuritylabs.com/threats/show/TSL20100323-05

[2] http://v.virscan.org/Backdoor.Win32.Zegost.html

赋予知识-分类与分析

- 分类方法
  - 相似比较
    - 生成器的生成服务端相似
    - 已知家族样本相似
  - 家族知识特征检测
- 核心目的行为、核心目的代码
  - RAT:上线、控制命令、键盘记录
  - DDoS: 攻击CC攻击代码
  - 勒索:加密文件，密钥算法、tor
  - Banker:各种密码窃取、拦截网银网站

沙箱中的特征类型与抗衰减

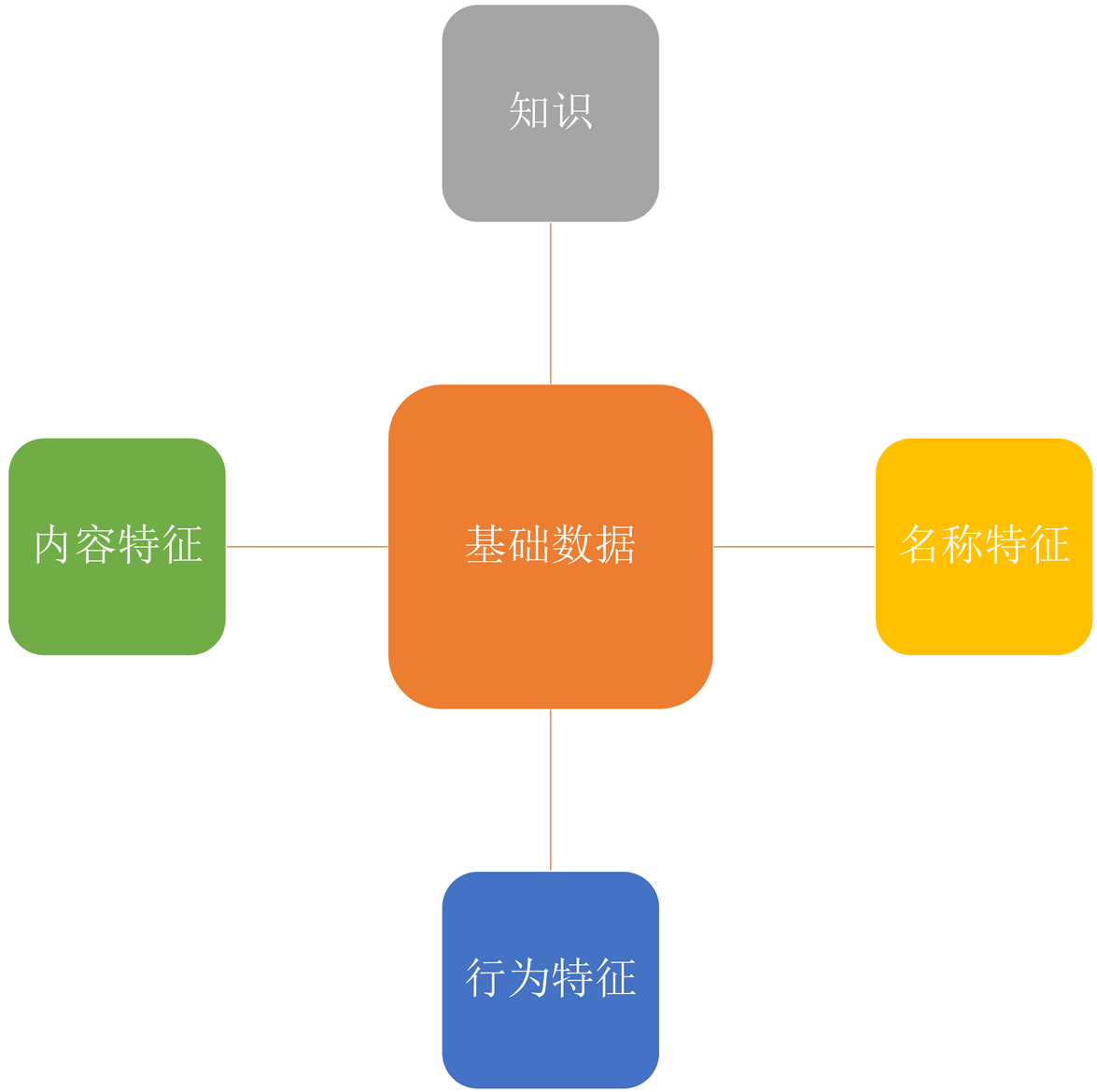


家族Yara
通信正则特征

IP:PORT 、useragent
文件名、互斥量

MD5、URL、Domain

知识与特征关联



挖掘-C&C提取

- C&C形式
  - 域名、IP、IP：PORT、URL、email
- 动态方法
  - 首包通信特征匹配上线数据发送信道即C&C
  - 污点数据追踪系统信息数据被作为上线数据发送到C&C
  - 黑名单域名IP检测
  - 白名单过滤防误报
- 静态方法
  - 配置解密
  - 字符串

挖掘-数据包提取

- 首包激发提取
- 首包家族识别

C&C(动态监控污点追踪)

网络监控

C&C(动态监控污点追踪)

C&C	污点数据
172.31.122.100:9999	0x0211FE94-----XP 0x0211FE94-----Win XP SP3 0x0211FEF4-----4*3391MHz 0x0211FF14-----100 Mbps
103.56.63.171:6666	0x0211FE94-----XP 0x0211FE94-----Win XP SP3 0x0211FEF4-----4*3391MHz 0x0211FF14-----100 Mbps
103.56.63.171:6666	0x01E1FE94-----XP 0x01E1FE94-----Win XP SP3 0x01E1FEF4-----4*3391MHz 0x01E1FF14-----100 Mbps
172.31.122.100:9999	0x01E1FE94-----XP 0x01E1FE94-----Win XP SP3 0x01E1FEF4-----4*3391MHz 0x01E1FF14-----100 Mbps

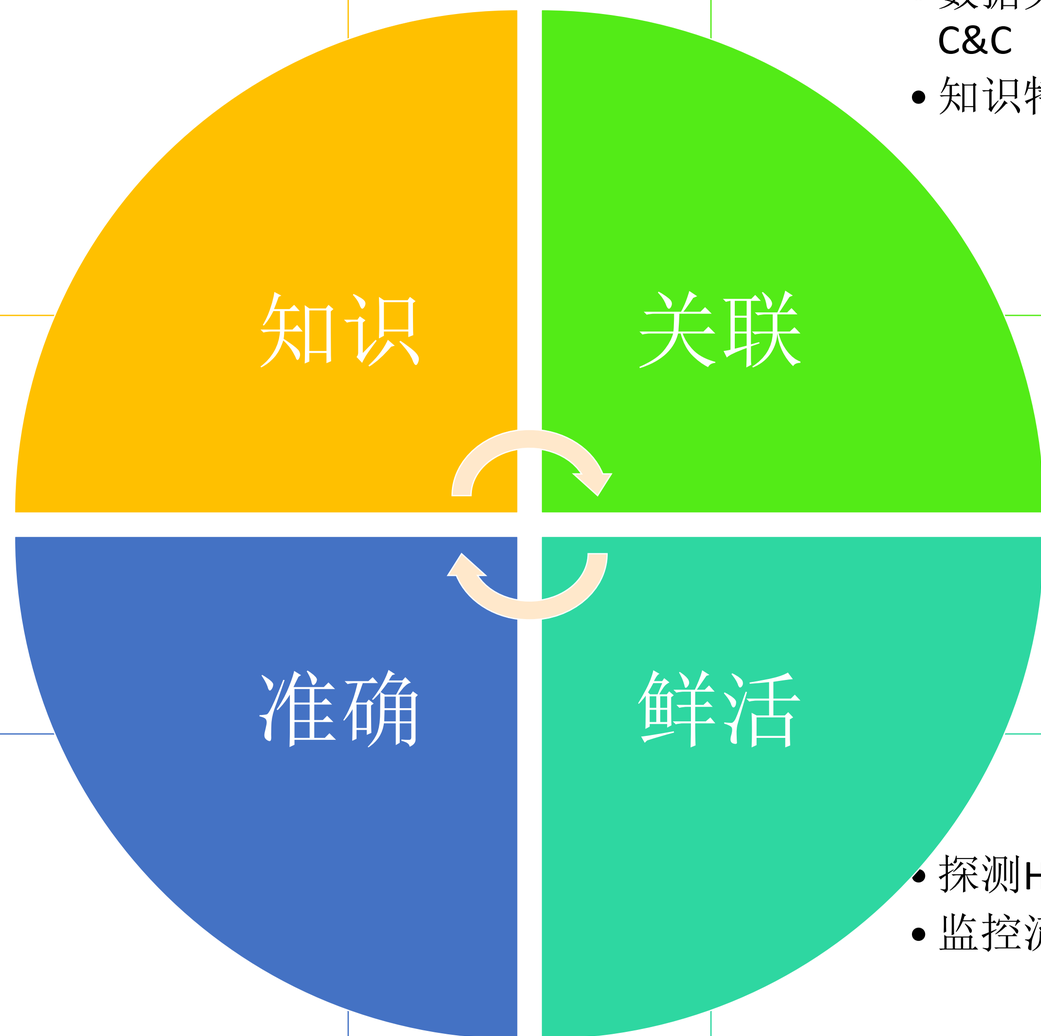
pcap网络发包

```
00 00 00 77 00 00 00 04 08 00 00 57 69 6e 20   |  wWin
58 50 20 53 50 33 00 00 00 00 00 00 00 00 00   |  XP SP3
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   |
```

产出威胁情报特性

- 黑白
- 分类
- 家族
- 组织

- 数据关联MD5 C&C
- 知识特征关联



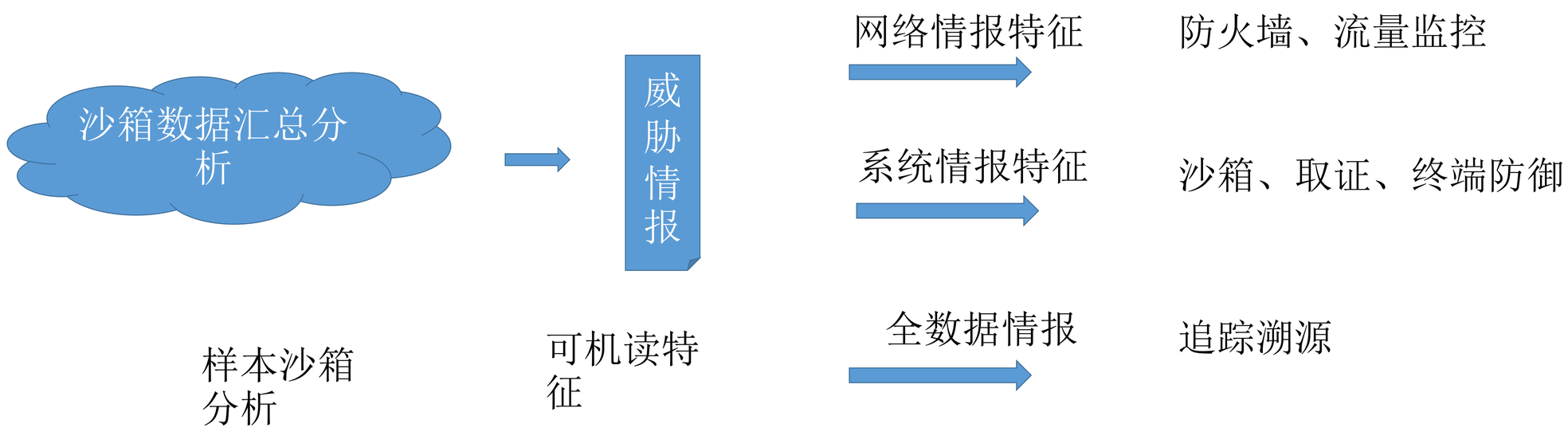
- 时间信誉
- 恶意

- 探测HFS
- 监控流量

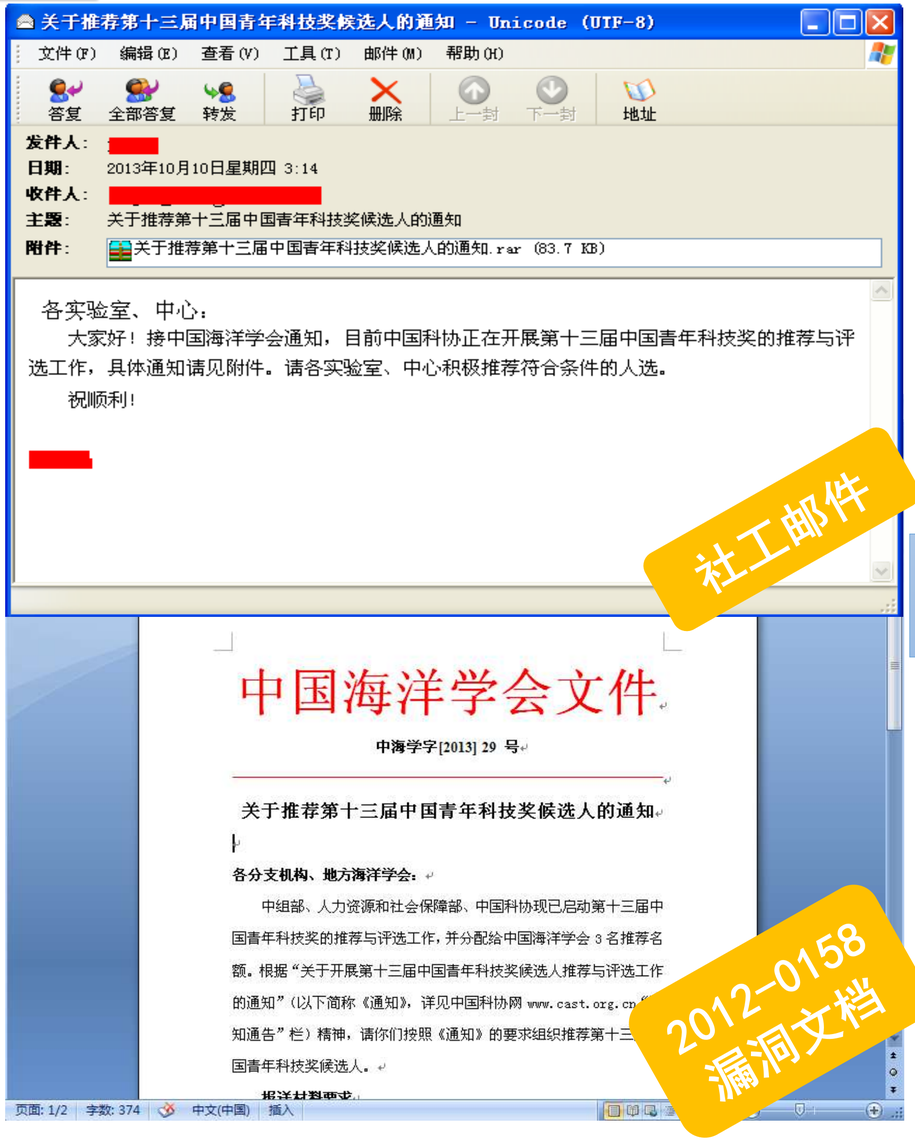
情报协同

- 防护
- 取证
- 监控
- 追溯

协同价值


沙箱数据汇总分析
威胁情报
样本沙箱分析
可机读特征
网络情报特征
防火墙、流量监控
系统情报特征
沙箱、取证、终端防御
全数据情报
追踪溯源

攻击文档



社工邮件

2012-0158
漏洞文档

下载二进制样本

根据已有样本分析配置后，统计的出样本收集文档的类型：

.doc、*.xls*、*.ppt*、*.wps*、*.pdf

- 获取 IE 自动保存的邮箱账户密码和对应网址，对 IE6 和 IE6 以上的版本采取不同的方法。
- 收集网络信息，主机信息，进程信息，记录在%Application Data%\Microsoft\Windows\Profiles.log
- 样本根据各自的配置，收集全盘包含指定关键字的文件路径、收集 C 盘 Program Files 目录下的 EXE 文件，将收集到的文件路径信息同样记录在 Application Data\Microsoft\Windows\Profiles.log。

```
if ( *driver != 65 )
{
  collect_profiles(driver, "201", v102, v104, v105, v106);
  collect_profiles(driver, "军", v84, v85, v102, v104);
  collect_profiles(driver, "项", v86, v87, v88, v89);
}
```

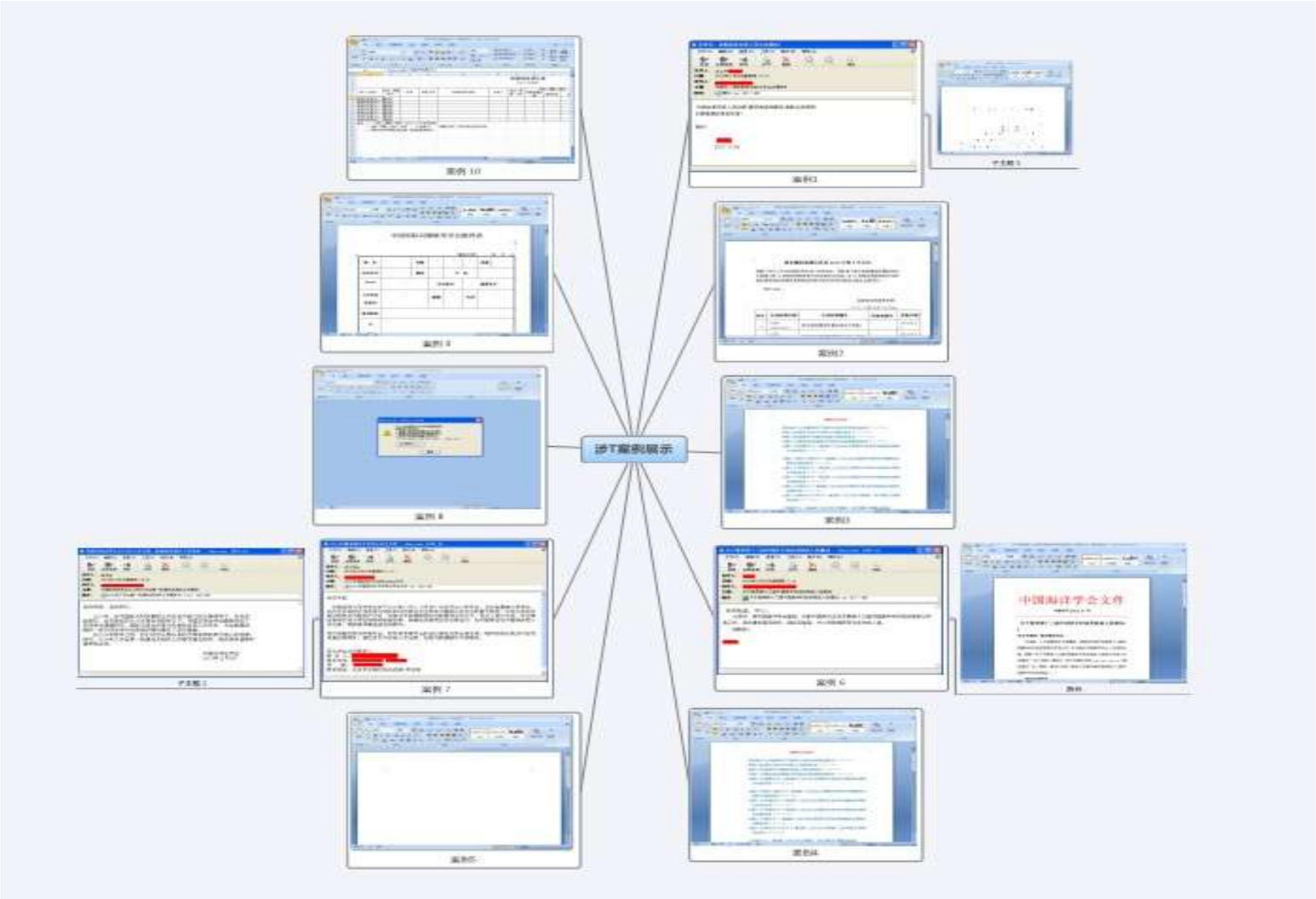
图 27 收集指定关键文件列表

根据目前已捕获样本，我们总结出该系列样本关注的关键字，各个 下列关键字中的三个，根据关键字对攻击目标进行收集操作

201、申、项、报、告、部、战、军、航、对台、国防

二进制样本特点

普通的APT-来自某方的攻击



- 原始攻击邮件：4封
- 使用漏洞附件：15个
- 使用漏洞：
  - ✓ CVE-2012-0158
  - ✓ CVE-2014-4114

- 部分RAT：
  - ✓ Poison Ivy RAT
  - ✓ Gh0st
  - ✓ HttpBots
  - ✓ ZXSHELL

邮件感知

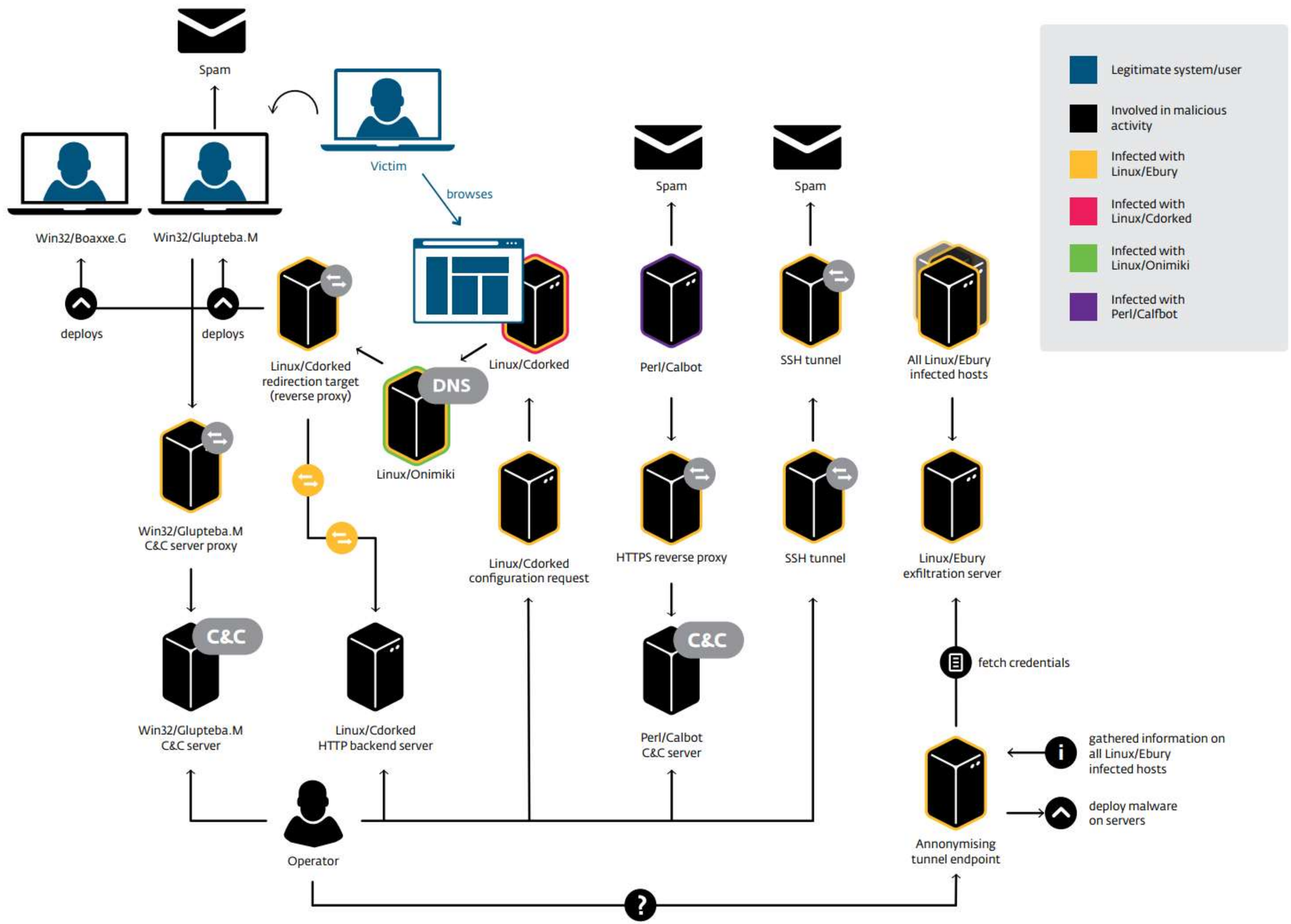
- 未知威胁
  - 免杀木马
  - 0day漏洞

Antiy Labs

•W

•ht

cc


Spam
Victim
browses
Win32/Boaxxe.G
Win32/Glupteba.M
deploys
deploys
Linux/Cdorked redirection target (reverse proxy)
DNS
Linux/Cdorked
Linux/Onimiki
Win32/Glupteba.M C&C server proxy
C&C
Win32/Glupteba.M C&C server
Linux/Cdorked HTTP backend server
Operator
Linux/Cdorked configuration request
Spam
Spam
Perl/Calbot
SSH tunnel
All Linux/Ebury infected hosts
HTTPS reverse proxy
SSH tunnel
Linux/Ebury exfiltration server
C&C
Perl/Calbot C&C server
fetch credentials
gathered information on all Linux/Ebury infected hosts
deploy malware on servers
Annonymising tunnel endpoint
?
Legitimate system/user
Involved in malicious activity
Infected with Linux/Ebury
Infected with Linux/Cdorked
Infected with Linux/Onimiki
Infected with Perl/Calbot

- 分类：spam
- 家族：Glupteba

A.4.5. Win32/Glupteba.M

Dropped by the exploit kit in non-English speaking countries.

- 5196a8a034611aaa112232767aafd74b8ef71279
- 20467521bfd58e9ed388ce83467d73e8fd0293a7
- f634f305a655b06f2647b82b58f7d3920546ac89
- 25a819d658d02548b2e5bdb52d2002df2f65b03a
- 6180d8c1c6967d15a0abb0895103ccc817e43362
- 051a89a7a335062829a8e938b8d4e3e2b532f6ff

变种

- 变种1：Glupteba.app
  - 伪装成其他正常应用软件更新进程，并将自身添加到注册表启动项Run键下，完成自启动。另外在系统启动目录下释放快捷方式.lnk文件。
  - 启动参数格式为"/app (MD5HASH)"
  - 典型MD5：2E6682932F826269B0F84A93AAB9E609
- 变种2：Glupteba.svc
  - 伪装成其他正常应用软件更新进程，并注册为服务，完成自启动。
  - 启动参数格式为"/svc (MD5HASH)"或"/svc"
  - 典型MD5:870048278C0C7A4B77231DAECBF46A68
- 变种3：Glupteba.none
  - 伪装成其他正常应用软件更新进程。
  - 启动不需要参数。
  - 典型MD5：055308d715791362e409c39a3486d6a5
- 变种4：Glupteba.rootkit
  - 复制自身到系统启动文件目录下，并以rootkit技术隐藏文件，文件名为chkntfs.exe。
  - 典型MD5：049892d7a823aafa4018e33d35261bd2

主机名称特征

- 伪装为其他应用软件更新进程
  - Google更新进程Google\Update\gupdate.exe
  - windows更新进程Microsoft\Windows\winupdate.exe
  - NVIDIA更新进程NVIDIA
- 启动方式：

  1）注册自启动，以特定参数启动病毒进程，参数格式如下：
  - "/app (MD5HASH)"
  - "/svc (MD5HASH)"或"/svc"　　名称特征
  - 不带参数
  - 2）其中一种变种利用rootkit技术隐藏自身及指定的文件、进程和网络链接等信息
- 特殊互斥量
  - “Global\MD7H82HHF7EH2D73“
  - Global\Mp6c3Ygukx29GbDk”

网络名称—C&C

- 该家族特殊目的域名
  - server-%s.192-168-0-255.com，"%s"为1-30之间的数字
- 其他域名
  - synergy.eamobile.com
  - microsoft-report.com
  - project.andhiequest.com

通信数据

- 模拟网络抓包—首包
  - /start?uptime=100&downlink=2222&uplink=2222&id=0012EC0E&statpass=BPASS&version=5&guid=bff5ffee-cfbe-4c9c-93d0-85942289208d&comment=4.00112 HTTP/1.0)

– 模拟网络抓包—心跳包

- 1) GET
- /user/api/core/authenticateUser?hwId=0&apiVer=1.0.0&email=JayDee84@hotmail.com&password=guys&uid=2563523 HTTP/1.1\r\n
- 疑是攻击者邮箱：JayDee84@hotmail.com
- 2) Host: synergy.eamobile.com\r\n
- 访问恶意地址。

可扩展通信特征变种

- 特征一：
  - 被控端发给控制端的tcp payload中包含"comment="，tcp payload的第5个字节开始满足正则(/.*?\?uptime=.*?\x26downlink=.*?\x26uplink=.*?\x26id=[0-9A-Z]{8}\x26statpass=.*?\x26version=.*?\x26guid=.{36}\x26comment=.*? HTTP)
- 特征二：
  - 被控端发给控制端的tcp payload中包含"comment="，tcp payload的第5个字节开始满足正则(/.*?\?uid=.*?\x26downlink=.*?\x26uplink=.*?\x26id=[0-9A-Z]{8}\x26statpass=.*?\x26version=.*?\x26guid=.{36}\x26comment=.*? HTTP)
- 说明
  - 两条网络特征区别不大，仅由“uptime”变为“uid
  - 该家族中的4个变种样本中，都有发现上述两条网络特征

可扩展文件内容特征

- {"virus_familyname":"Trojan/Win32.Glupteba","virus_feature": ["|0047006F006F0067006C0065005500700064006100740065004200650074|"], "level": 4}
- {"virus_familyname": " Trojan/Win32.Glupteba ", "virus_feature": ["GET /stat?uptime=%d&downlink=%d&uplink=%d&id=%s&statpass=%s&version=%d&features=%d&guid=%s&comment=%s&p=%d&s=%s HTTP/1.0"], "level": 4}
- {"virus_familyname":" Trojan/Win32.Glupteba","virus_feature":["Global\\Mp6c3Ygukx29GbDk"], "level": 4}

TTP

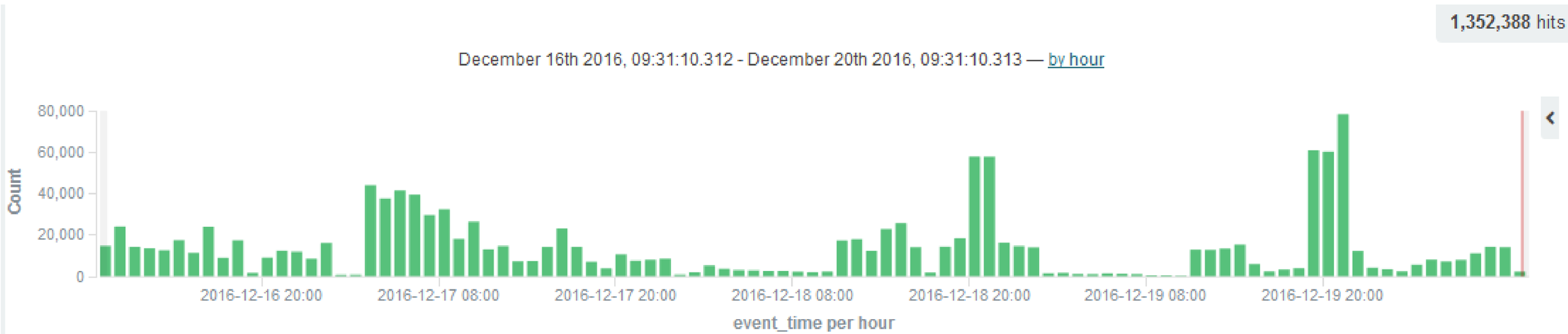
- 双开机自启动
  - 释放PE文件创建快捷方式.lnk文件到系统启动目录下
  - 释放PE文件路径添加到注册表自启动Run键下
- 添加延迟重命名项
  - 自删除病毒母体
- 通信
  - 上线HTTP参数

取证案例

- 时间：2014年09月05日
- 地点：xx省公安厅
- ＩＰ：5.*.*.143/37.*.*.149
- 样本信息
  - 伪装应用软件更新进程daemonupd.exe
  - 启动参数："/app D5CECDD1B59D60D044ECD2AF38485"
  - 网络特征为1号网络特征
  - 互斥量均为”Global\Mp6c3Ygukx29GbDK”

- 时间：2014年09月19日
- 地点：xx省地税
- ＩＰ：３７.**.**.１５８
- 样本信息
  - 伪装应用软件更新进程daemonupd.exe
  - 网络特征均为1号网络特征
  - 互斥量均为”Global\Mp6c3Ygukx29GbDK”

僵尸网络DDoS监控


1,352,388 hits
December 16th 2016, 09:31:10.312 - December 20th 2016, 09:31:10.313 — by hour
Count
80,000
60,000
40,000
20,000
0
2016-12-16 20:00
2016-12-17 08:00
2016-12-17 20:00
2016-12-18 08:00
2016-12-18 20:00
2016-12-19 08:00
2016-12-19 20:00
event_time per hour

追溯案例-样本分析

- MD5： 8B23922AE8FAA55FCED2EB9F1A9903B6
  - 病毒名：Trojan/Win32.STORMDDOS2
  - C&C： 222.186.56.8:8080
- MD5： fa6b0f1229237ccf92260b8314ea9d7a
  - 病毒名：Trojan[ddos]/linux.dofloo
  - 222.186.56.8:48080
  - *上线*VERSONEX:Linux-3.2.0-4-4kc-malta-mips|0|0 MHz|120MB|47MB|Hacker

追溯案例- IDS

- **捕获时间@2015-11-18 14:43:35**

恶意代码名称: Trojan/Win32.STORMDDOS2

源IP: 111.113.14.90

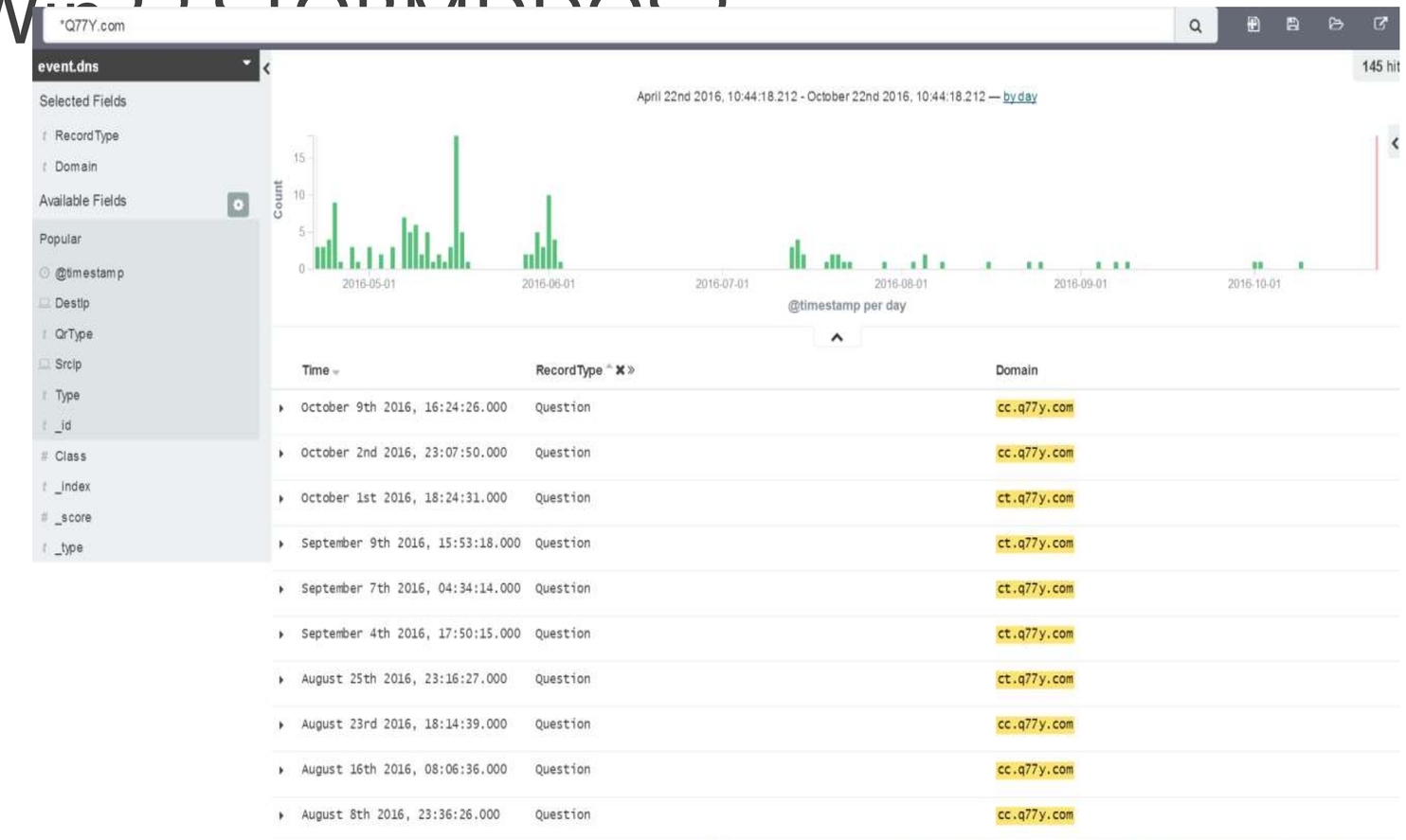
源端口: 49436

目的IP: 222.186.56.8

目的端口: 8080

网络协议: TCP

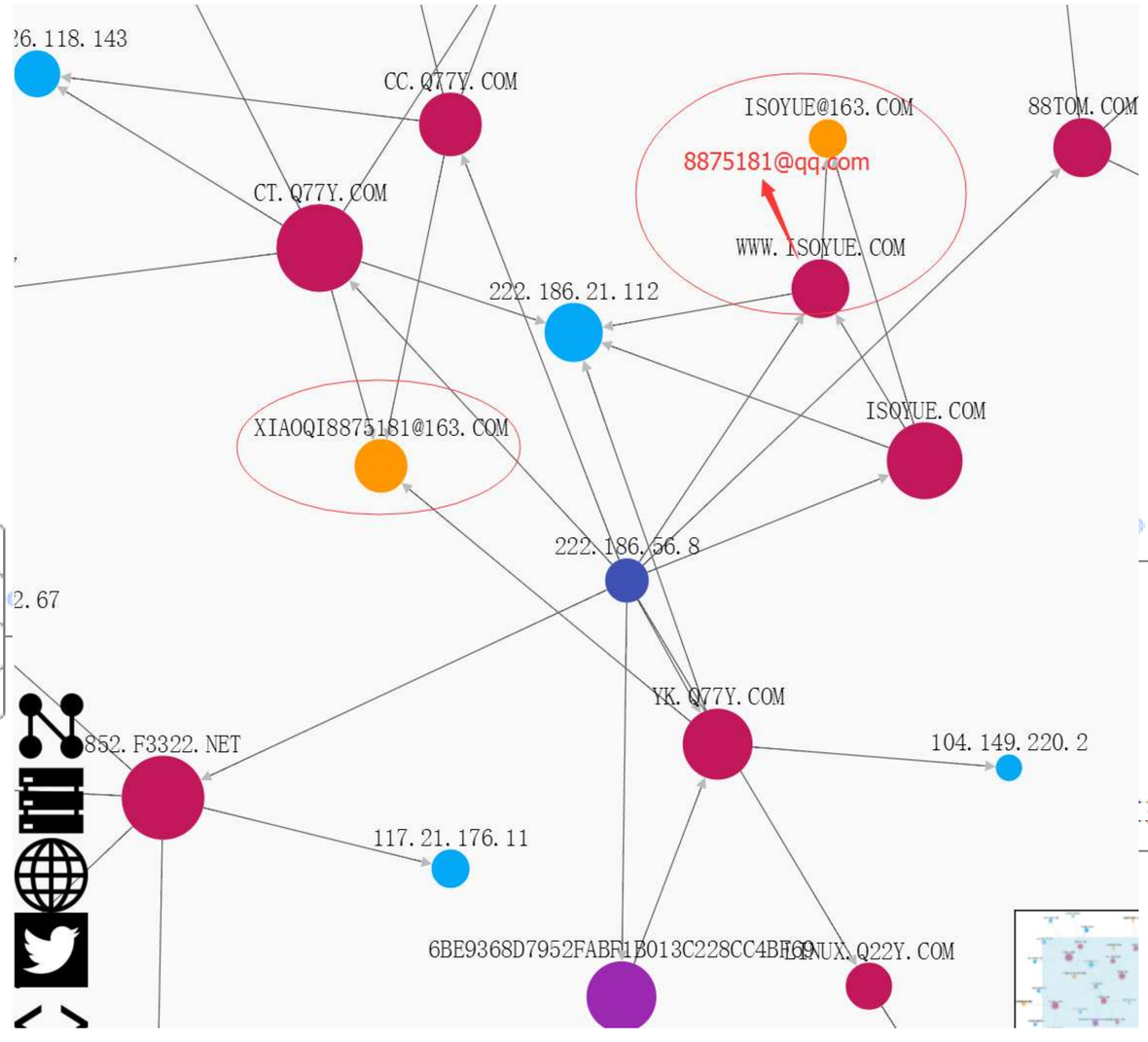
通信方向: C2S



追溯案例-蜜罐-SSH暴力破解

- 传播linux类型肉鸡
- Sep 28 23:40:09 cp107sj sshd[18208]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.186.56.8
  Sep 28 23:40:11 cp107sj sshd[18204]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.186.56.8
  Sep 28 23:40:11 cp107sj sshd[18208]: Failed password for invalid user ubnt from 222.186.56.8 port 1989 ssh2
  Sep 28 23:40:13 cp107sj sshd[18204]: Failed password for invalid user ubnt from 222.186.56.8 port 1626 ssh2
  Sep 28 23:40:18 cp107sj sshd[18206]: pam_unix(sshd:auth):

追溯案例-关联溯源



接非法D单,打死付款.

韩国项目的联系,免杀全过.

1990-5-11

15555592855

isoyue@gmail.com

222.186.56.8

其它

- 对抗
- 速度

安天 | 智者安天下

对抗

- 反虚拟机
- 反沙箱
- 反安全分析

性能

- 多种动态环境结合
- 反病毒虚拟机
- 隔离或监控细分

感谢大家参与本次交流