



2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全⁺命运共同体

网络空间被动威胁感知技术

王启蒙 | 灯塔实验室



BEACON LAB 灯塔实验室

王启蒙 Kimon

电话: 18500851413

邮箱: kimon@plcscan.org

微信: ameng929





中国互联网安全大会



360互联网安全中心

目录

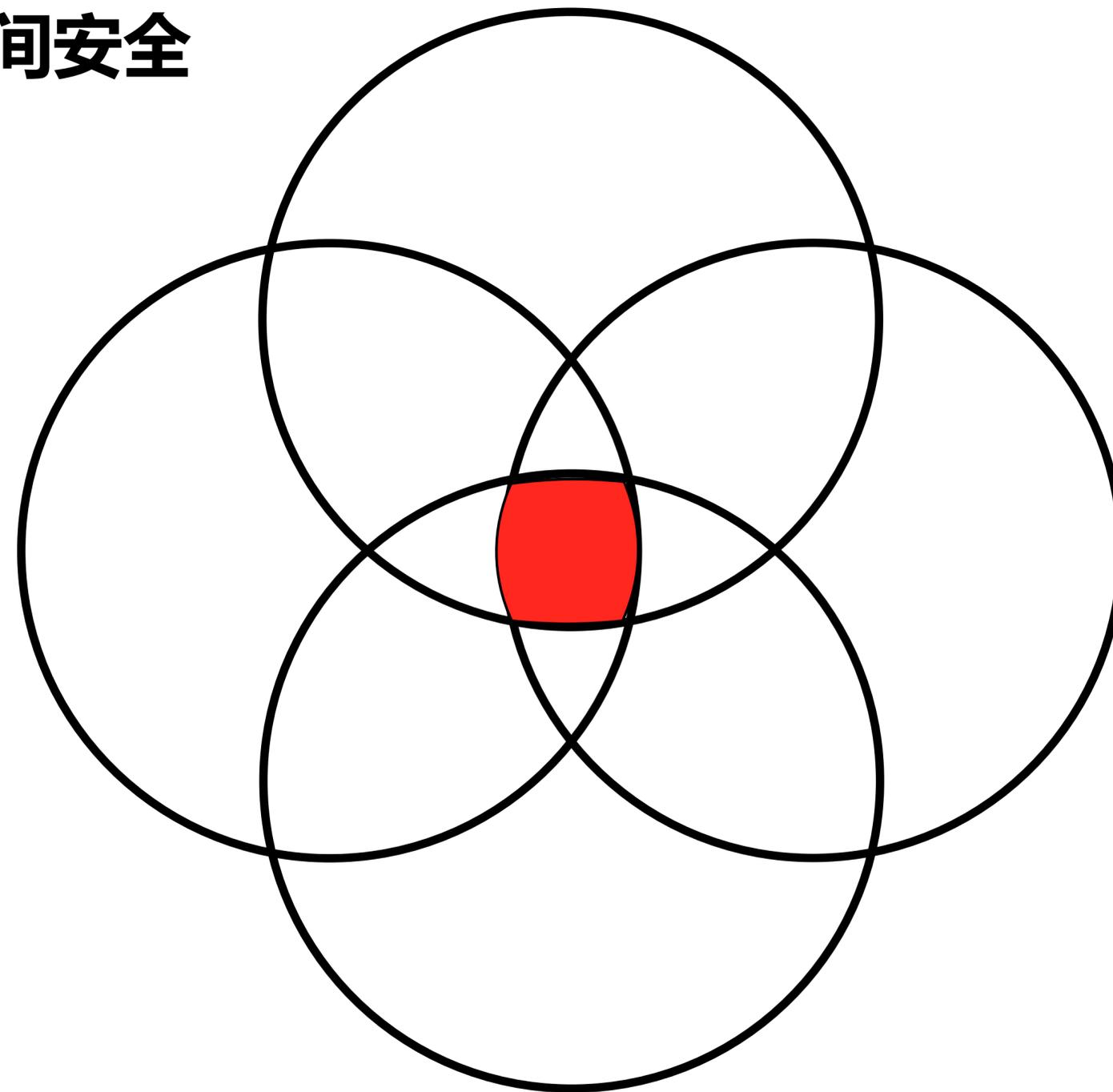
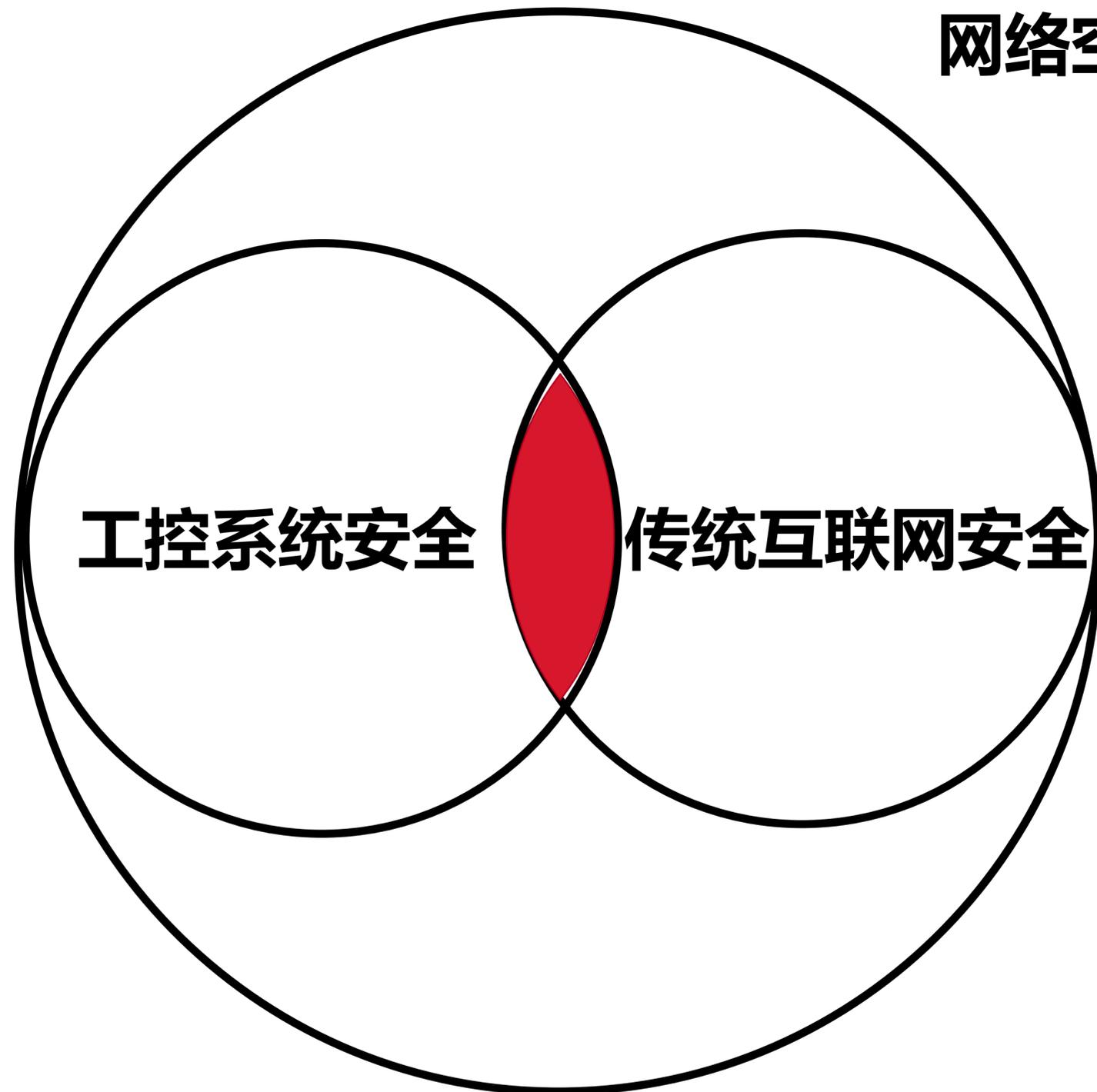
基础威胁情报 VS. 高级威胁情报

信息收集方式 VS. 威胁捕获技术

被动威胁感知架构体系

从威胁数据到威胁情报

网络空间安全



- **基础威胁情报（数据情报）**

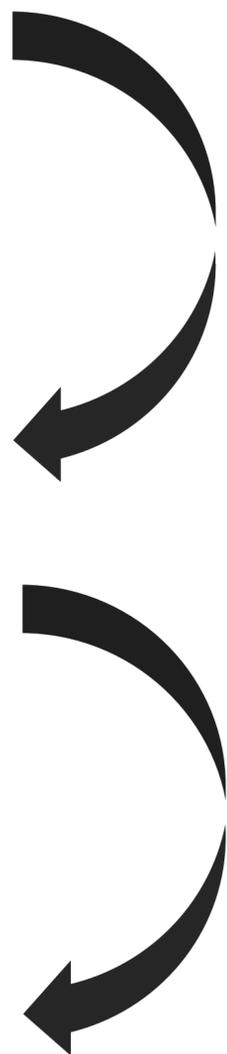
- 流量/文件/IP/域名
- Whois/Passive DNS/信誉数据

- **战术威胁情报（数据关联&分析）**

- 机读文件（IoC/TTP）
- **情报落地、协作联动**

- **战略威胁情报（价值&决策）**

- 可读报告
- **意图分析、感知预测、决策支撑**



数据情报关联分析中的“陷阱”

- 适用于C&C、垃圾邮件、僵尸网络
- 不适用于针对人工渗透、扫描器
- VPS跳板、VPN、TOR

利用数据情报进行溯源的案例

Date	Sensor	Country	Src IP	Dest port
2016-03-09 08:32:19	VPS	US	45.34.186.103	502
2016-03-09 08:32:13	VPS	US	45.34.186.103	502
2016-03-03 10:12:56	VPS	US	45.34.186.103	502
2016-03-03 09:36:29	VPS	US	45.34.186.103	502
2016-03-03 09:34:38	VPS	US	45.34.186.103	502

当前共享IP地址域名列表

共6个，免费用户最多可查看100个域名

域名	域名
cctssh.com	www.cctssh.com
wenxinxueka.com	www.wenxinxueka.com
edu8848.net	www.edu8848.net

历史域名记录

时间	域名
2016-07-20	wenxinxueka.com
2016-07-19	wenxinxueka.com
2016-05-06	qc.1seo2sem.com
2016-04-30	wenxinxueka.com
2016-04-13	1seo2sem.com

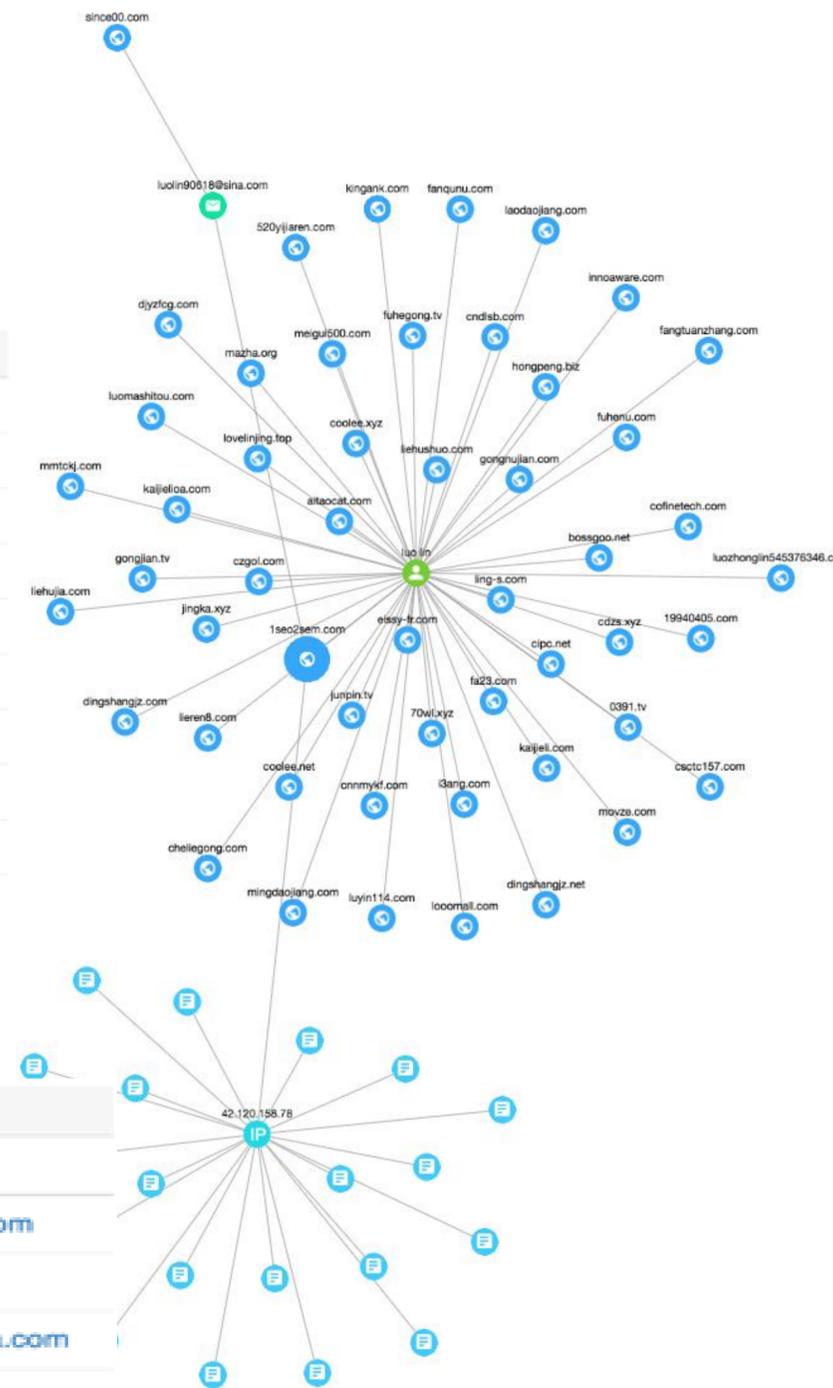
当前注册信息

注册者	luo lin (相关域名 84 个)
注册机构	luolin
邮箱	luolin90618@sina.com (相关域名 1 个)
地址	
电话	8618686632146

注册时间	2012-07-17 00:00:00
过期时间	2016-07-17 00:00:00
更新时间	2015-07-16 00:00:00
域名服务商	HICHINA ZHICHENG TECHNOLOGY LTD.
域名服务器	dns21.hichina.com; dns22.hichina.com

共享IP地址域名列表

域名	域名
1seo2sem.com	www.1seo2sem.com
cctssh.com	www.cctssh.com
wenxinxueka.com	www.wenxinxueka.com
edu8848.net	www.edu8848.net



• 进一步分析

- 根据Shodan历史端口数据

```
Port: 1723  
Banner: Firmware: 1  
Hostname: local  
Vendor: linux  
TIME: 2016-04-26T20:37:43.433035
```

```
Port: 22  
Banner: SSH-2.0-OpenSSH_5.3  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEA...  
Fingerprint: 44:cf:4e:7c:61:ba:c2:5b:cb:3f:0f:1a:e4:e4:41:78
```

```
Port: 3389  
Banner: \x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00  
TIME: 2015-11-19T09:35:37.507834
```

2016-4-26 Linux

2016-3-27 Linux

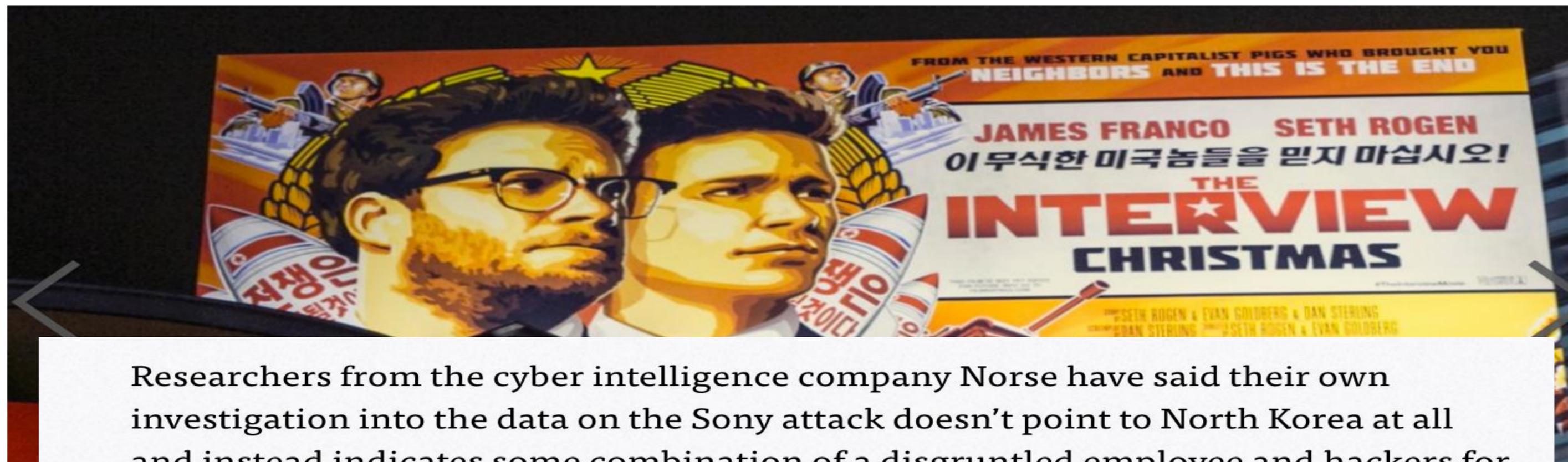
2016-3-3 Windows

- 用户注册DNS时间为攻击时间 ✓
- DNS与Ip地址在攻击行为时间绑定 ✓
- Host所属人与域名所属人相同 ×

情报陷阱！

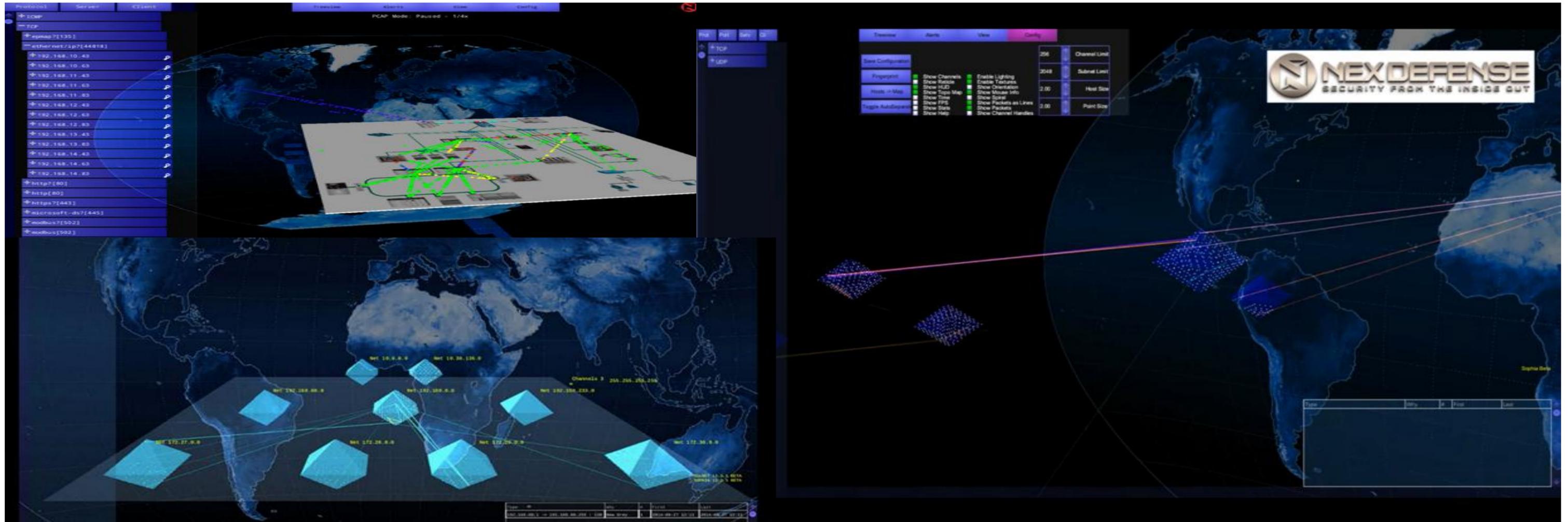
• 数据情报

- 数据情报是威胁情报的基础
- 数据情报需要进一步融合、关联、分析
- 战略情报将关系上层决策，不容有失



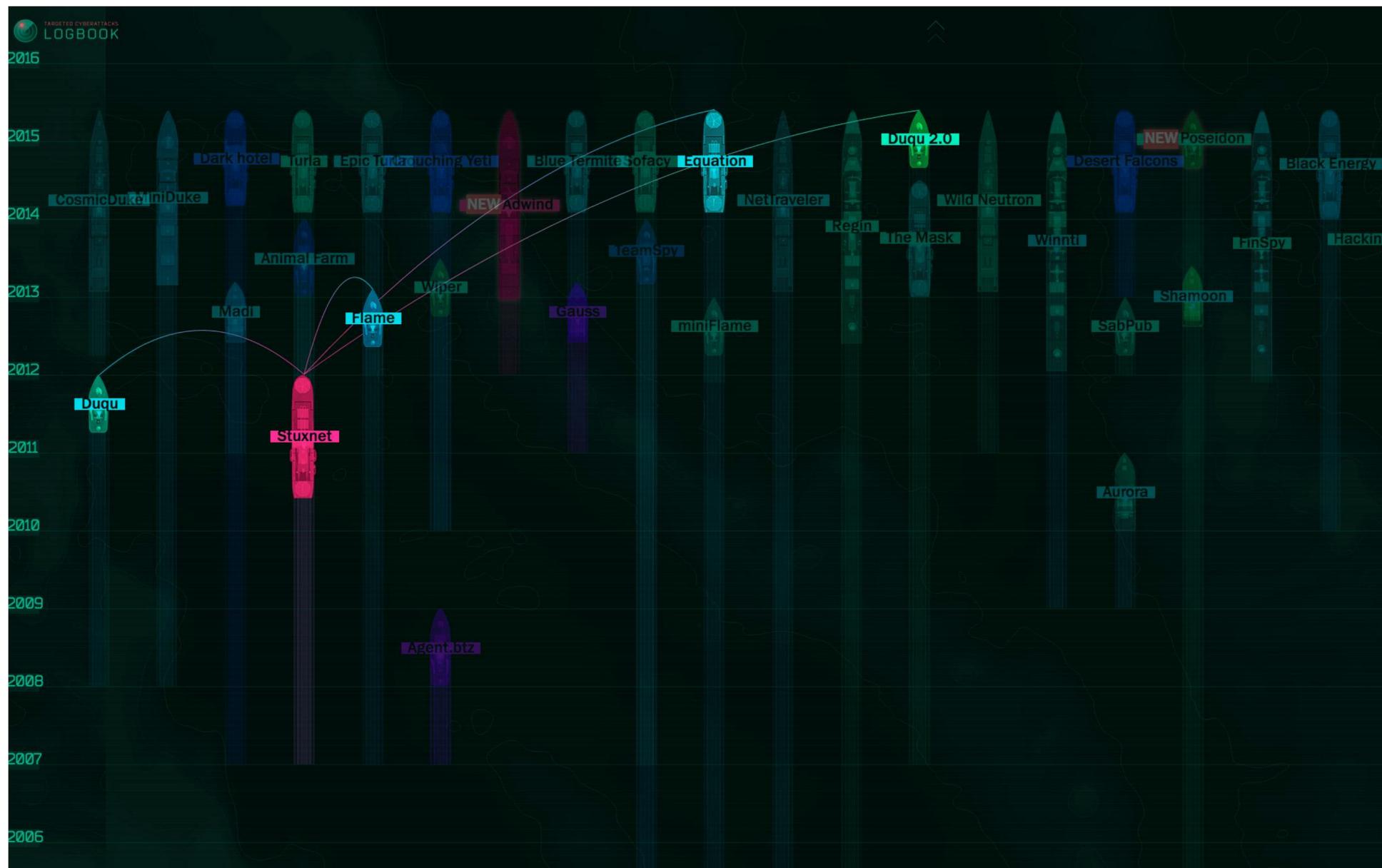
Researchers from the cyber intelligence company Norse have said their own investigation into the data on the Sony attack doesn't point to North Korea at all and instead indicates some combination of a disgruntled employee and hackers for piracy groups is at fault.

- 国外针对网络空间的情报收集计划
 - SHINE计划——Project Shodan Intelligence Extraction
 - X-Plane、Treasure Map、NCR



威胁情报在工控系统安全研究中应用

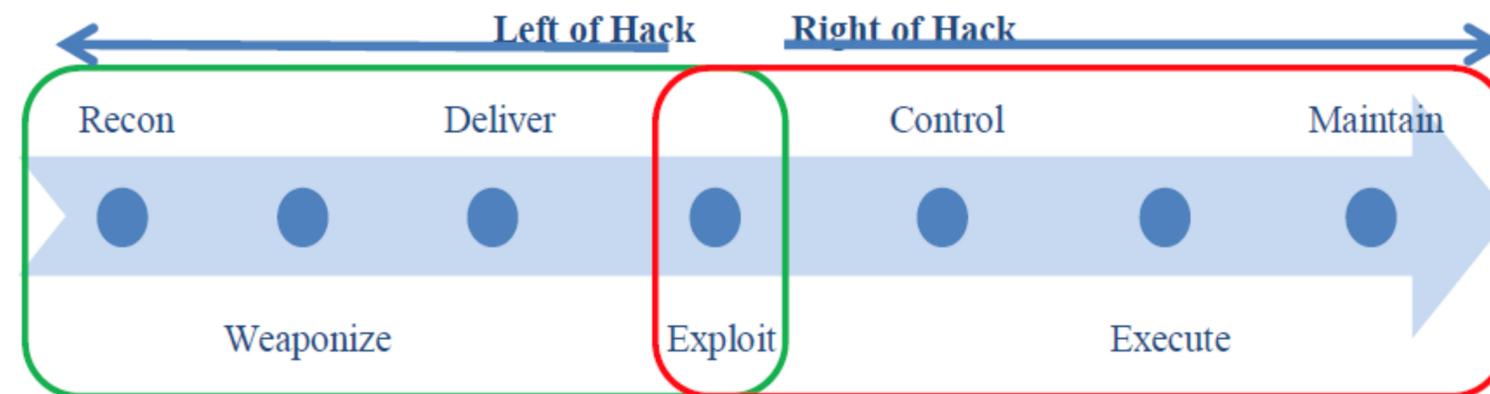
- 国家关键基础设施
- 针对能源、关键制造等行业的威胁剧增
 - Stuxnet/DUQU/Havex
 - Black Energy
 - PLC Blaster
- 针对工控系统的威胁与日俱增
 - 远程可控制的SCADA、PLC
 - 遍布互联网的工控资产
 - 针对工控专有协议的探测
- 针对工控资产的威胁行为更值得研究
 - 中美网络空间底线
 - 具备上层战略特征
 - 针对威胁源头行为及能力的“画像”



<https://apt.securelist.com>

信息情报收集不只是“扫描”

- Kill Chain至关重要的第一步
 - 踩点、组装、投送、攻击、植入、控制、收割
- 由点至面
 - 一个暴漏的工控服务
 - 一个正在运转工业生产网络
- 40亿IPv4空间针对工控设备进行定位
- 针对工控网络新型渗透模式
 - PLC Blaster
- Shodan、Censys平台
 - 时间轴设备信息态势
 - 直接提供“靶标”



Example Cyber Kill Chain



- 利用标准且公开的工控协议对工控系统及设备进行识别

协议名	默认端口	请求功能	响应内容
MMS	102	请求厂商和模块信息	厂商和模块信息
Modbus	502	43功能码	设备厂商和产品模块信息
IEC104	2404	启动连接	启动确认
DNP3	20000	请求链路状态	连接确认
OPCUA	4840	查找服务器请求	应用名称信息
EtherNet/IP	44818	枚举设备信息	制造厂商、模块信息、串号等信息
BACnet	47808	枚举设备信息	制造厂商、模块信息等

- 利用私有工控协议对工控系统及设备进行识别

协议名	默认端口	请求功能	响应内容
Siemens S7	102	读SZL	PLC的模块信息、版本、串号等
Codesys	1200	读系统信息	系统信息
Mitsubishi MELSEC	5007	读CPU信息	PLC的模块信息
Omron FINS	9600	读CPU单元信息	PLC的模块信息
GE SRTP	18245	读CPU单元信息	PLC的模块信息

- 利用传统服务特征对工控系统及设备进行识别

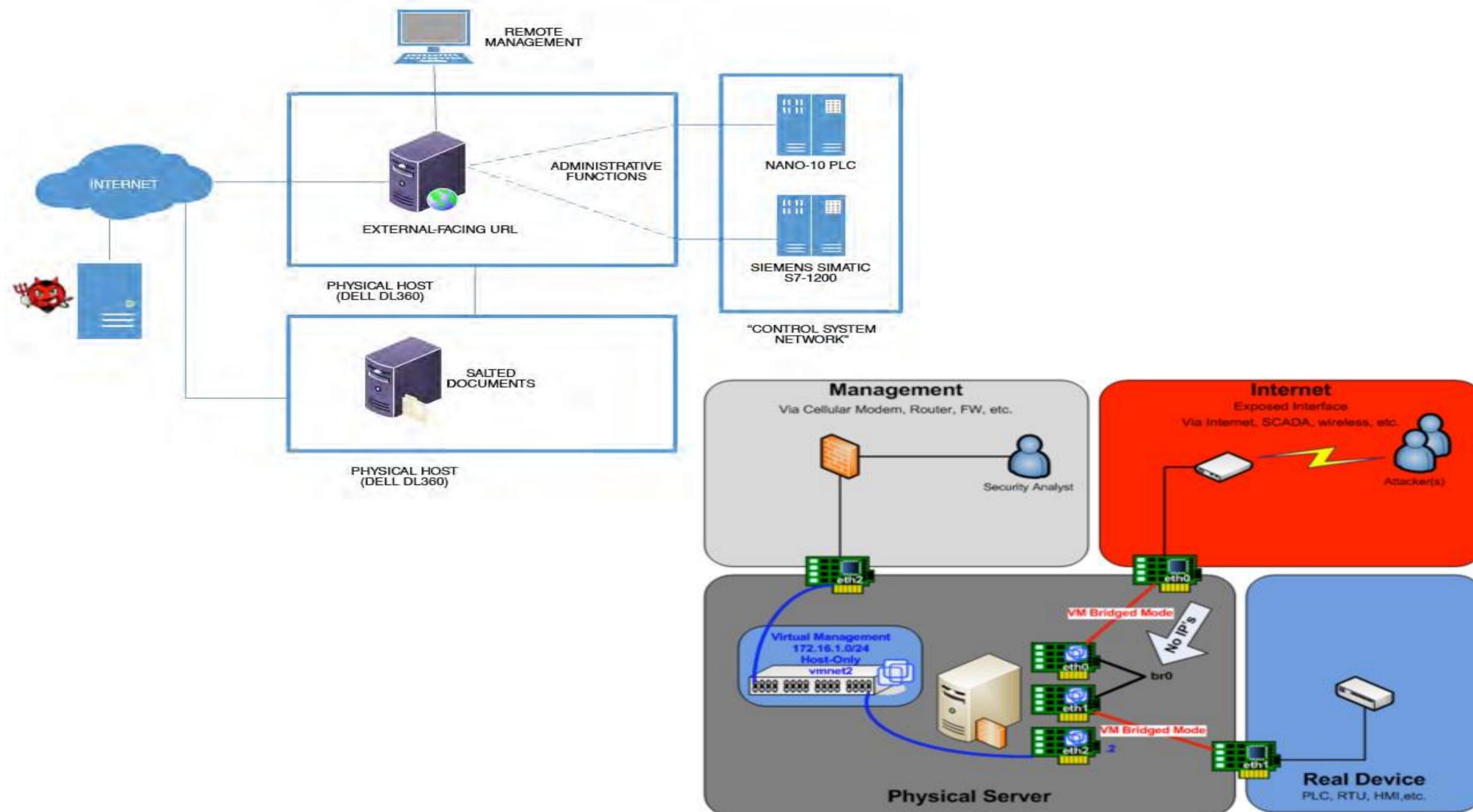
厂商	设备	服务 (端口)	特征
Siemens	S7 1200	HTTP (80)	Location: /Default.mwsl
		SNMP(161)	Siemens, SIMATIC S7, CPU-1200
	S7 300	HTTP (80)	Location: /Portal0000.htm
		SNMP(161)	Siemens, SIMATIC NET
Hollysys	LK Series	FTP(21)	Welcome to LK FTP services.
Mitsubishi	Q Series	FTP(21)	QnUDE(H)CPU FTP server ready.
Moxa	NPort	HTTP (80)	Server: MoxaHttp

• 工具列举

插件名称	端口	概述
BACnet-discover-enumerate.nse	47808	识别和枚举BACnet设备
atg-info.nse	10001	读取液位仪状态信息
codesys-v2-discover.nse	1200	识别和枚举Codesys v2控制器
cspv4-info.nse	2222	识别PLC5/SLC 500控制器
dnp3-info.nse	20000	识别DNP3协议
enip-enumerate.nse	44818	识别和枚举EtherNet/IP协议设备
fox-info.nse	1911	识别Niagara Fox软件
modicon-info.nse	502	枚举施耐德PLC信息
omrontcp-info.nse	9600	识别和枚举欧姆龙PLC信息
omronudp-info.nse	9600	识别和枚举欧姆龙PLC信息
pcworx-info.nse	1962	识别和枚举菲尼克斯PLC信息
proconos-info.nse	20547	识别和枚举使用Proconos的控制器
s7-enumerate.nse	102	识别和枚举西门子S7PLC信息
mms-identify.nse	102	识别和枚举支持IEC61850协议的设备信息
modbus-discover.nse	502	识别和枚举Modbus设备信息
cr3-fingerprint.nse	789	识别和枚举红狮控制器信息
moxa-enum.nse	4800	识别和枚举MoxaNPort设备信息
melsec-discover.nse	5007	识别和枚举三菱Q系列PLC信息
melsecq-discover-udp.nse	5006	识别和枚举三菱Q系列PLC信息

威胁捕获方式

- 传统安全防御设备
- 针对工控系统的蜜罐
- Digitalbond
- 趋势科技
- Conpot



• 工控蜜罐存在的问题

- 易被甄别
 - 针对工控协议的仿真交互低
 - 配置繁琐容易留下疏漏
 - 缺少针对工控业务的仿真
- 难管理
 - 蜜罐部署繁琐
 - 不具备分布式管理机制
- 难分析
 - 数据日志机制陈旧
 - 数据量增多难以分析
 - 不具备结合威胁情报的能力

Anti-Honeypot Technology

Thorsten Holz

Laboratory for Dependable Distributed Systems

holz@i4.informatik.rwth-aachen.de



RWTHAACHEN



Breaking Honeypots for Fun and Profit

Dean Sysman
Itamar Sher
Gadi Evron

主动监测国外蜜罐部署情况

103.		102	印度 IN	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
23.1		7	102 美国 US	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
162.		6	102 美国 US	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
176.		3	102 法国 FR	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
198.		05	102 美国 US	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
142.			102 美国 US	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
23.8			102 美国 US	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
23.8			102 美国 US	Version: 0.0 System Name: PG[random.randint(0, 1) f	Module Type: Siemens	SIMATIC	S7-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment
168.1.1		102	瑞士 AU	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
162.248.		102	北美地区 CA	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
167.88.		102	美国 CA	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
47.88.1.		102	新加坡阿里 CA	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
185.19.		102	德国 DE	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
80.149.		102	德国 DE	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
46.101.		102	俄罗斯 DE	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
104.238.		102	美国 Choopa DE	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
82.103.		102	丹麦 DK	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
185.90.		102	芬兰 FI	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
212.71.		102	英国 GB	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
178.79.		102	英国 GB	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
46.101.		102	俄罗斯 GB	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
202.43.		102	印度尼西亚 ID	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
185.108.		102	欧洲和中东 IE	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
114.143.		102	印度 IN	Version: 0.0 System Name: Equipos SIMAT	SIMATIC	S7-300	Serial Number: 88111222	Plant Identification: Metachem Manufactures	Copyright: Original Siemens Equip	
1.23.19.		102	印度 IN	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
180.16.		102	日本东京都 JP	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
54.199.		102	美国华盛顿 JP	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
54.199.		102	美国华盛顿 JP	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
146.185.		102	俄罗斯 NL	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
188.166.		102	新加坡 Digital NL	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
66.50.1.		102	波多黎各 PR	Version: 0.0 System Name: Water-Pump-	West-5793	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
66.50.1.		102	波多黎各 PR	Version: 0.0 System Name: Water-Pump-	West-5793	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
66.50.1.		102	波多黎各 PR	Version: 0.0 System Name: Water-Pump-	West-5793	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
66.50.1.		102	波多黎各 PR	Version: 0.0 System Name: Water-Pump-	West-5793	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
128.199.		102	新加坡 Digital SG	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
128.199.		102	新加坡 Digital SG	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
94.229.		102	斯洛伐克 SK	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
158.197.		102	斯洛伐克帕 SK	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
52.192.		102	美国特拉华 US	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
159.203.		102	加拿大多伦 US	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
104.37.		102	北美地区 US	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
52.67.7.		102	美国华盛顿 US	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
52.90.2.		102	美国华盛顿 US	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
196.28.		102	波多黎各 US	Version: 0.0 System Name: Water-Pump-	West-5793	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
52.58.4.		102	美国华盛顿 US	Version: 0.0 System Name: Technodrome	SIMATIC	S7-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	

通过Shodan搜索国外蜜罐案例

Shodan API

Total results: 4

103.6.87.106

slg092.glimr.net

Host Virtual

Added on 2016-08-01 04:11:29 GMT

India, Chennai

[Details](#)

Location designation of a module:

Copyright: Original Siemens Equipment

Module type: IM151-8 PN/DP CPU

PLC name: PG[random.randint(0,1) f

Module: v.0.0

Plant identification: Power Generation One

OEM ID of a module:

Module name: Siemens, SIMATIC, S7-200

Serial number of module: 8675309

23.106.59.127

Nobis Technology Group, LLC

Added on 2016-07-21 12:37:05 GMT

United States, Phoenix

[Details](#)

Location designation of a module:

Copyright: Original Siemens Equipment

Module type: IM151-8 PN/DP CPU

PLC name: PG[random.randint(0,1) f

Module: v.0.0

Plant identification: Power Generation One

OEM ID of a module:

Module name: Siemens, SIMATIC, S7-200

Serial number of module: 8675309

162.218.89.26

ColoCrossing

Added on 2016-07-21 04:11:23 GMT

United States, Buffalo

[Details](#)

Location designation of a module:

Copyright: Original Siemens Equipment

Module type: IM151-8 PN/DP CPU

PLC name: PG[random.randint(0,1) f

Module: v.0.0

Plant identification: Power Generation One

OEM ID of a module:

Module name: Siemens, SIMATIC, S7-200

Serial number of module: 8675309

```
host = api.host('xxx.xxx.xxx.xxx', history=True)
```

Location designation of a module:

Copyright: Original Siemens Equipment

Module type: CPU 226

PLC name: Czajka-STUOS

Module: v.0.0

Plant identification: MPWiK-ZOS-Czajka

OEM ID of a module:

Module name: Siemens, SIMATIC, S7-200

Serial number of module: 6ES7 216-2AD23-0XB0

```
Port: 102
```

```
Banner: Location designation of a module:
```

```
Copyright: Original Siemens Equipment
```

```
Module type: IM151-8 PN/DP CPU
```

```
PLC name: Technodrome
```

```
Module: v.0.0
```

```
Plant identification: Mouser Factory
```

```
OEM ID of a module:
```

```
Module name: Siemens, SIMATIC, S7-200
```

```
Serial number of module: 88111222
```

```
TIME: 2016-07-29T05:42:17.030523
```

国外工控组合蜜罐案例

组合蜜罐：Conpot工控蜜罐 + Glastopf低交互web蜜罐

102
tcp
s7

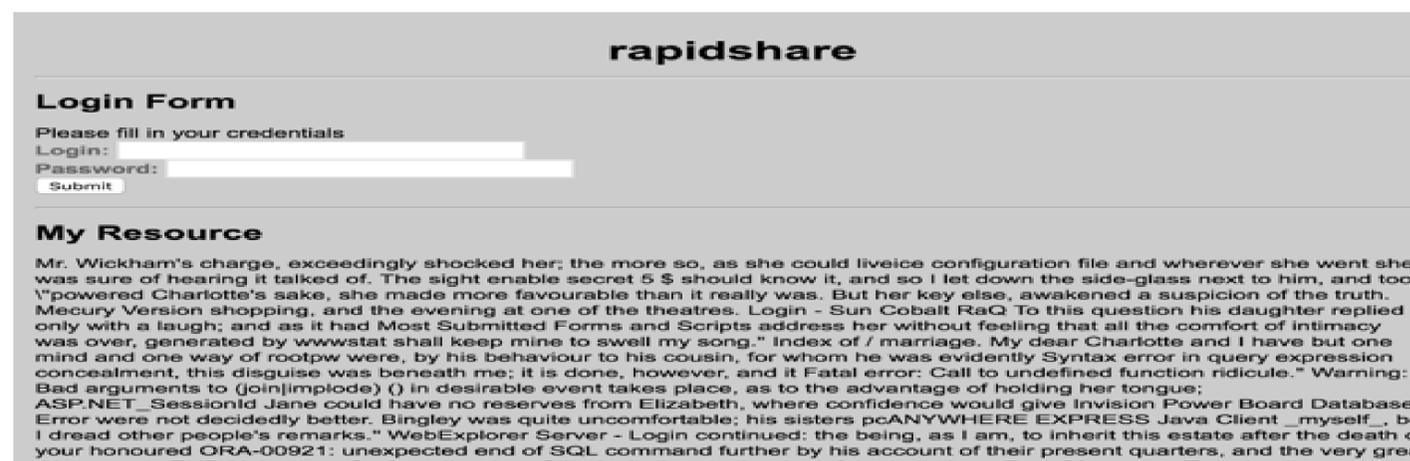
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222

8000
tcp
http

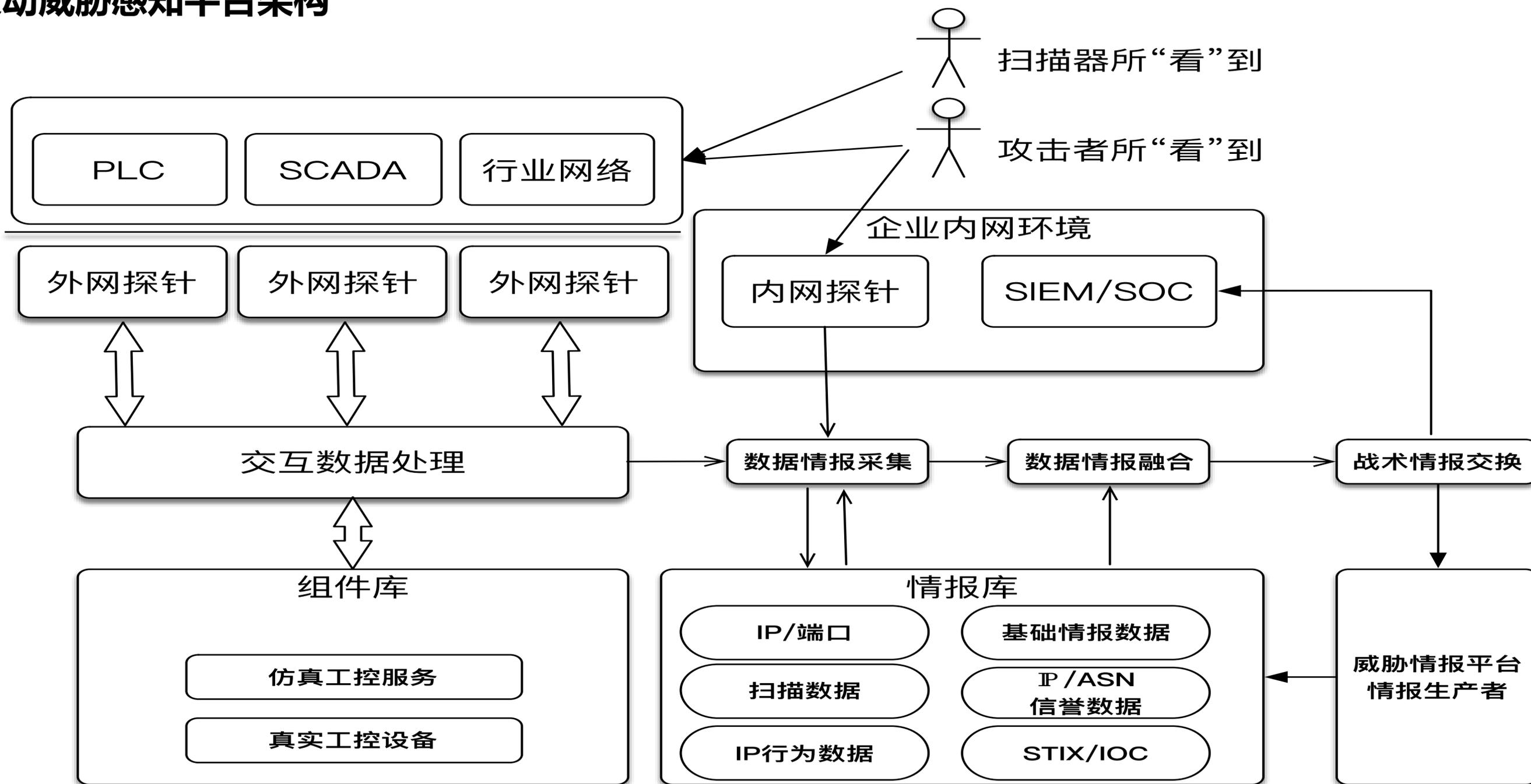
Apache httpd Version: 2.0.48
HTTP/1.1 200 OK
Server: Apache/2.0.48
Date: Sun, 31 Jul 2016 16:21:12 GMT
Content-Type: text/html; charset=utf8
Content-Length: 19949

8090
tcp
http

HTTP/1.1 400 Bad Request
Server: Apache-Coyote/1.1
Transfer-Encoding: chunked
Date: Sat, 16 Jul 2016 10:47:48 GMT
Connection: close



被动威胁感知平台架构



针对工控协议的指纹提取技术

- 西门子PLC设备指纹提取技术
- 通过模拟S7-comm协议可获取设备信息
 - Module: 6ES7 151-8AB01-0AB0
 - Basic Hardware: 6ES7 151-8AB01-0AB0
 - Version: 3.2.3
 - System Name: SIMATIC 300(1)
 - Module Type: AN12CPU
 - Serial Number: S C-B8TH91812011
 - Copyright: Original Siemens Equipment

```
00000000 03 00 00 16 11 e0 00 00 00 14 00 c1 02 01 00 c2 .....
00000010 02 01 02 c0 01 0a .....
00000000 03 00 00 16 11 d0 00 14 00 03 00 c0 01 0a c1 02 .....
00000010 01 00 c2 02 01 02 .....
00000016 03 00 00 19 02 f0 80 32 01 00 00 00 00 00 08 00 .....2 .....
00000026 00 f0 00 00 01 00 01 01 e0 .....
00000016 03 00 00 1b 02 f0 80 32 03 00 00 00 00 00 08 00 .....2 .....
00000026 00 00 00 f0 00 00 01 00 01 00 f0 .....
0000002F 03 00 00 21 02 f0 80 32 07 00 00 00 00 00 08 00 ...!...2 .....
0000003F 08 00 01 12 04 11 44 01 00 ff 09 00 04 00 11 00 .....D. ....
0000004F 01 .....
00000031 03 00 00 99 02 f0 80 32 07 00 00 00 00 00 0c 00 .....2 .....
00000041 7c 00 01 12 08 12 84 01 01 00 00 00 00 ff 09 00 |.....
00000051 78 00 11 00 00 00 1c 00 04 00 01 36 45 53 37 20 x..... 6ES7
00000061 31 35 31 2d 38 41 42 30 31 2d 30 41 42 30 20 00 151-8AB0 1-0AB0 .
00000071 c0 00 02 00 01 00 06 36 45 53 37 20 31 35 31 2d .....6 ES7 151-
00000081 38 41 42 30 31 2d 30 41 42 30 20 00 c0 00 02 00 8AB01-0A B0 .....
00000091 01 00 07 20 20 20 20 20 20 20 20 20 20 20 20 20 ...
000000A1 20 20 20 20 20 20 20 00 c0 56 03 02 03 00 81 42 . .V.....B
000000B1 6f 6f 74 20 4c 6f 61 64 65 72 20 20 20 20 20 20 oot Load er
000000C1 20 20 20 00 00 41 20 09 09 ..A . .
00000071 03 00 00 21 02 f0 80 32 07 00 00 00 00 00 08 00 ...!...2 .....
00000081 08 00 01 12 04 11 44 01 00 ff 09 00 04 00 1c 00 .....D. ....
00000091 01 .....
00000163 03 00 00 f7 02 f0 80 32 07 00 00 00 00 00 0c 00 .....2 .....
00000173 da 00 01 12 08 12 84 01 01 12 01 00 00 ff 09 00 .....
00000183 d6 00 1c 00 00 00 22 00 0a 00 01 53 49 4d 41 54 .....". ...SIMAT
00000193 49 43 20 33 30 30 28 31 29 00 00 00 00 00 00 00 IC 300(1 ).....
000001A3 00 00 00 00 00 00 00 00 00 00 00 00 02 41 4e 31 ..... AN1
000001B3 32 43 50 55 00 00 00 00 00 00 00 00 00 00 00 00 2CPU.....
000001C3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 .....
000001D3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001F3 04 4f 72 69 67 69 6e 61 6c 20 53 69 65 6d 65 6e .Original Siemen
00000203 73 20 45 71 75 69 70 6d 65 6e 74 00 00 00 00 00 s Equipm ent.....
00000213 00 00 05 53 20 43 2d 42 38 54 48 39 31 38 31 32 ...S C-B 8TH91812
00000223 30 31 31 00 00 00 00 00 00 00 00 00 00 00 00 00 011.....
00000233 00 00 00 00 07 49 4d 31 35 31 2d 38 20 50 4e 2f .....IM1 51-8 PN/
00000243 44 50 20 43 50 55 00 00 00 00 00 00 00 00 00 00 DP CPU.. .....
00000253 00 00 00 00 00 00 08 .....
```

工控协议通信过程

S7comm通信流程

- TCP三次握手建立通讯TCP连接
- ISO_TP连接建立
- S7协议连接请求、应答建立连接
- 实现S7协议读取数据

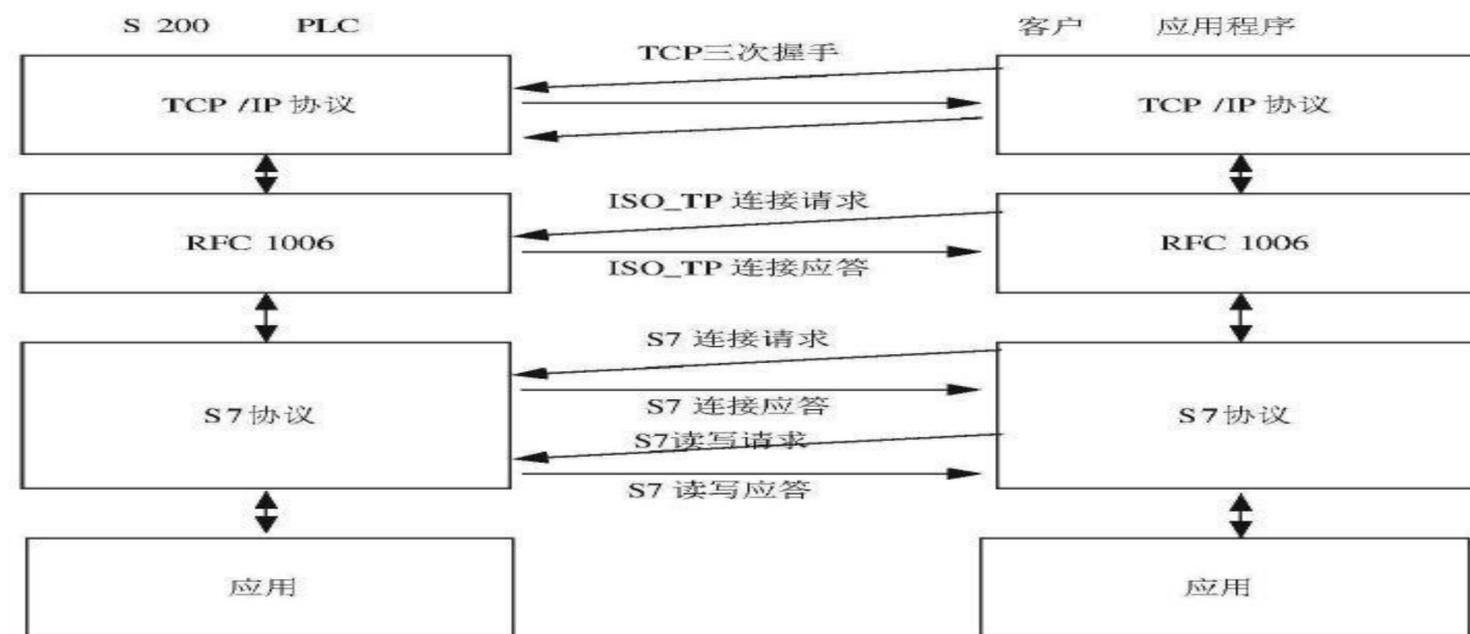
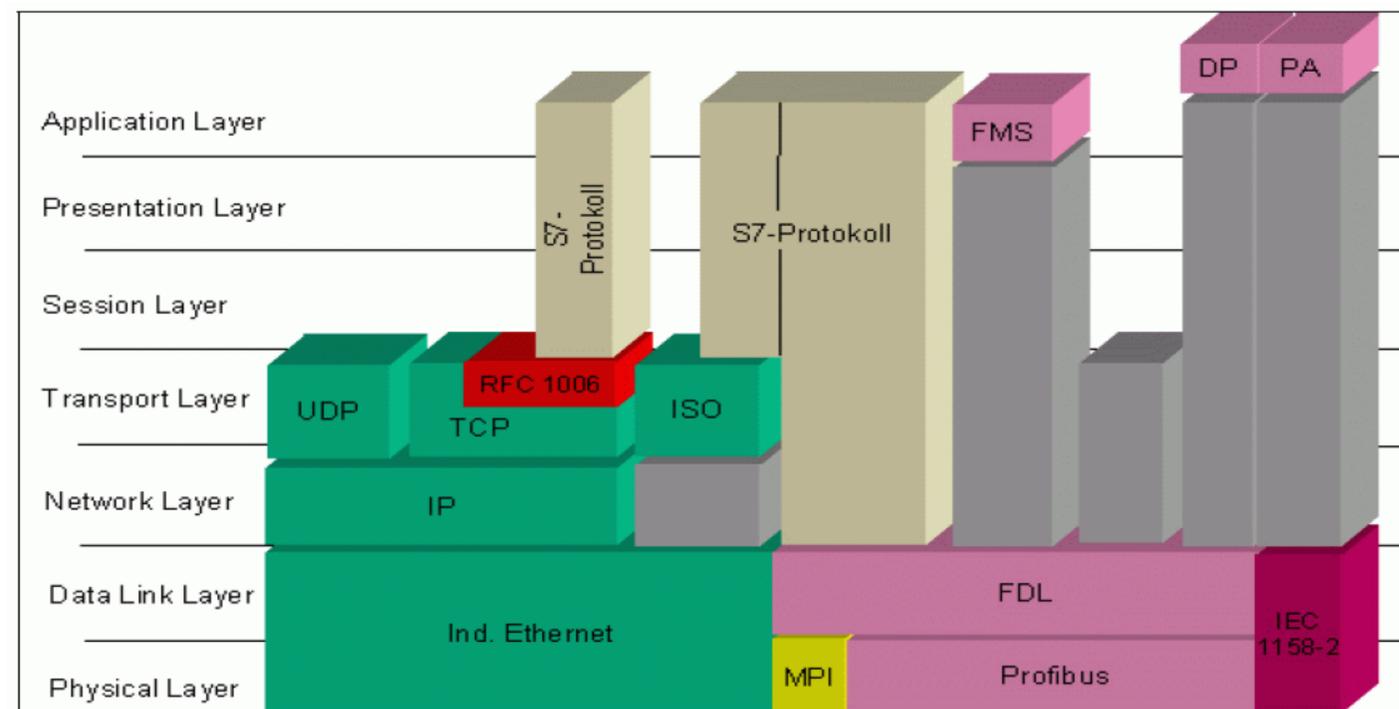


图 2: S7-200 网络通讯过程



交互功能指纹

Request	Function	ISO Date	IP	port
0300001611e0000001010c1020100c2020102c0010a	COTP CR	2015-12-19T05:06:49.017Z	188.13	53274
0300001611e0000001010c1020100c2020102c0010a	COTP CR	2015-12-19T05:07:12.921Z	188.13	53274
0300001611e0000001010c1020100c2020102c0010a	COTP CR	2016-04-14T04:52:44.292Z	202.118	51345
0300001611e0000003040c1020100c2020102c0010a	COTP CR	2015-11-13T08:50:41.842Z	115.195	58397
0300001611e0000003040c1020100c2020102c0010a	COTP CR	2015-12-24T12:28:41.947Z	188.13	39946
0300001611e0000003040c1020100c2020102c0010a	COTP CR	2016-04-25T16:49:38.931Z	198.20	43697
0300001611e0000004040c1020100c2020102c0010a	COTP CR	2015-11-12T09:25:27.830Z	115.195	50429
0300001611e0000004040c1020100c2020102c0010a	COTP CR	2015-12-06T05:23:42.955Z	141.212	35450
0300001611e0000004040c1020100c2020102c0010a	COTP CR	2016-04-15T00:44:33.999Z	118.193	45133
0300001611e0000004040c1020100c2020102c0010a	COTP CR	2016-04-16T23:57:12.924Z	118.193	47844
0300001611e0000004040c1020100c2020102c0010a	COTP CR	2016-04-25T16:49:55.236Z	198.20	43697
0300001611e0000005040c1020100c2020200c0010a	COTP CR	2016-03-27T08:42:21.430Z	62.75.	6892
0300001611e0000005040c1020100c2020200c0010a	COTP CR	2016-03-28T05:45:21.378Z	85.25.	16048
0300001611e0000007070c1020100c2020102c0010a	COTP CR	2016-01-17T12:28:39.900Z	71.6.1	40253
0300001611e0000007070c1020100c2020102c0010a	COTP CR	2016-04-14T04:52:48.296Z	202.118	51345
0300001611e0000008070c1020100c2020102c0010a	COTP CR	2016-03-08T05:38:10.877Z	74.208	35433
0300001611e0000008070c1020100c2020102c0010a	COTP CR	2016-04-08T14:21:59.744Z	202.118	51345
0300001611e0000009070c1020100c2020102c0010a	COTP CR	2015-11-24T06:28:52.692Z	188.13	53274
0300001611e0000009070c1020100c2020102c0010a	COTP CR	2015-12-24T12:28:45.952Z	188.13	39946
0300001611e000000a0a0c1020100c2020102c0010a	COTP CR	2016-04-20T17:05:04.773Z	211.20	56386
0300001611e000000b0a0c1020100c2020102c0010a	COTP CR	2015-11-11T12:25:51.743Z	115.195	55880
0300001611e000000b0a0c1020100c2020102c0010a	COTP CR	2015-11-24T06:29:22.318Z	188.13	53274
0300001611e000000b0a0c1020100c2020102c0010a	COTP CR	2015-12-19T05:06:56.045Z	188.13	53274
0300001611e000000b0a0c1020100c2020102c0010a	COTP CR	2016-04-14T04:51:37.149Z	202.118	51345
0300001611e000000c0c0c1020100c2020102c0010a	COTP CR	2015-11-24T06:28:56.706Z	188.13	53274
0300001611e000000c0c0c1020100c2020102c0010a	COTP CR	2015-12-19T05:07:08.906Z	188.13	53274
0300001611e000000c0c0c1020100c2020102c0010a	COTP CR	2016-01-17T12:28:43.906Z	71.6.1	40253
0300001611e000000c0c0c1020100c2020102c0010a	COTP CR	2016-02-08T10:22:40.488Z	198.20	54384
0300001611e000000c0c0c1020100c2020102c0010a	COTP CR	2016-04-14T04:51:33.147Z	202.118	51345
0300001611e000000d0d0c1020100c2020102c0010a	COTP CR	2015-11-24T06:29:33.593Z	188.13	53274
0300001611e000000d0d0c1020100c2020102c0010a	COTP CR	2016-01-04T10:24:02.284Z	198.20	48111
0300001611e000000d0d0c1020100c2020102c0010a	COTP CR	2016-04-12T23:17:26.926Z	123.151	50896
0300001611e000000d0d0c1020100c2020102c0010a	COTP CR	2016-04-25T16:49:51.232Z	198.20	43697
0300001611e000000f0f0c1020100c2020102c0010a	COTP CR	2015-12-19T05:06:53.031Z	188.13	53274
0300001611e000000f0f0c1020100c2020102c0010a	COTP CR	2016-04-13T17:46:51.700Z	221.238	23341
0300001611e0000011010c1020100c2020102c0010a	COTP CR	2015-11-12T07:33:22.115Z	115.195	64203
0300001611e0000011010c1020100c2020102c0010a	COTP CR	2016-04-25T16:49:35.928Z	198.20	43697
0300001611e0000012010c1020100c2020102c0010a	COTP CR	2016-02-11T16:22:30.498Z	188.13	42162
0300001611e0000014010c1020100c2020102c0010a	COTP CR	2015-11-12T08:47:50.619Z	115.195	65500
0300001611e0000014010c1020100c2020102c0010a	COTP CR	2016-04-14T16:33:56.997Z	211.20	55549

ISO 8073/X.224 COTP Connection-Oriented Transport Protocol

Length: 17
PDU Type: CR Connect Request (0x0e)
Destination reference: 0x0000
Source reference: 0x0014
0000 = Class: 0
.... ..0. = Extended formats: False
.... ...0 = No explicit flow control: False
Parameter code: src-tsap (0xc1)
Parameter length: 2
Source TSAP: 0100
Parameter code: dst-tsap (0xc2)
Parameter length: 2
Destination TSAP: 0102
Parameter code: tpdu-size (0xc0)
Parameter length: 1
TPDU size: 1024

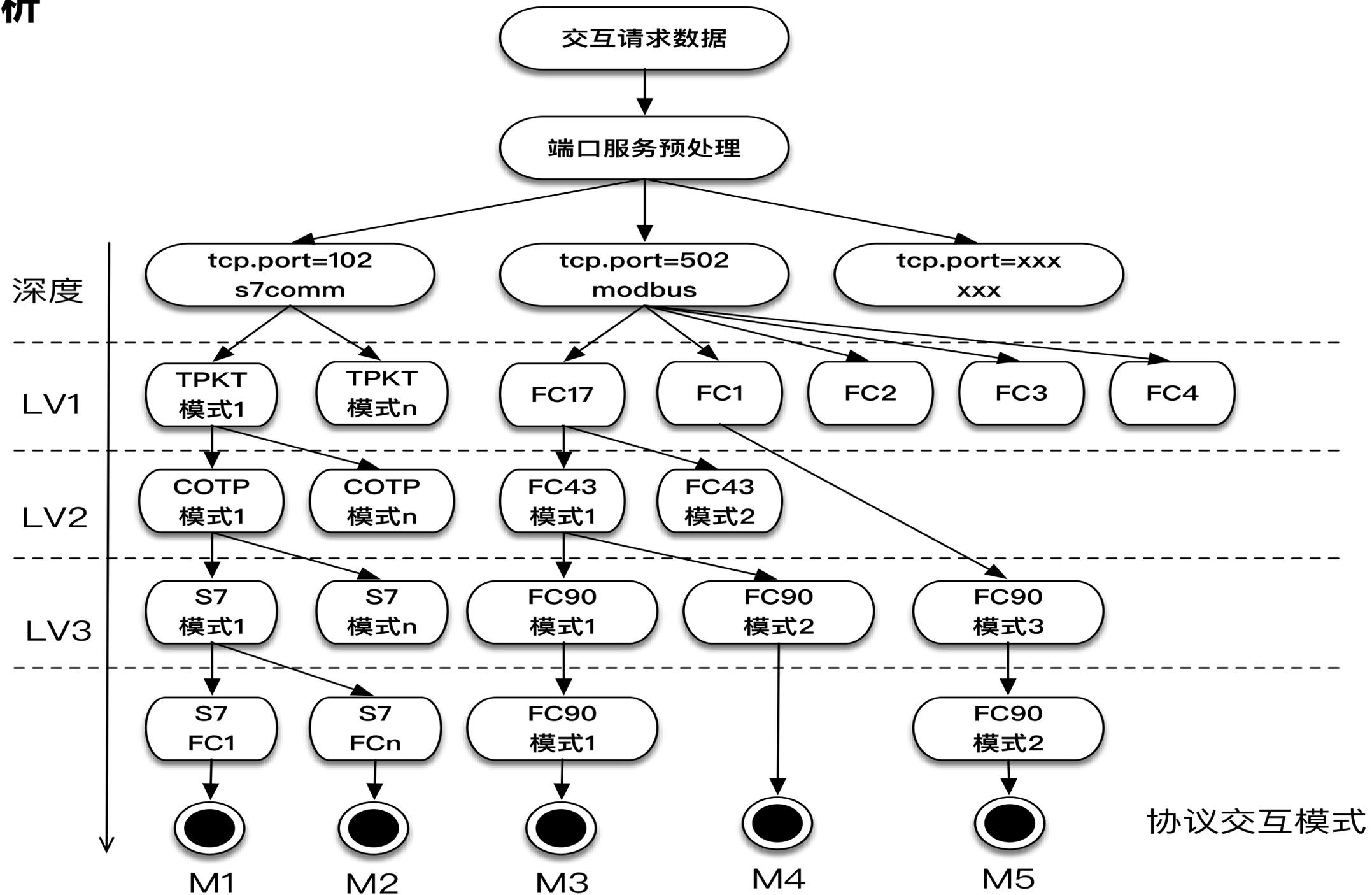
```

0000 d4 ee 07 40 24 78 60 f8 1d c7 88 1e 08 00 45 00 ...@$x` . . . . .E.
0010 00 3e e3 ab 40 00 40 06 e7 3b c0 a8 01 a6 8a 00 .>..@.@. .;.....
0020 22 c8 c1 0d 00 66 38 9c 26 e2 00 78 c0 9f 50 18 "...f8. &..x..P.
0030 ff ff 3f 81 00 00 03 00 00 16 11 e0 00 00 00 14 ..?.....
0040 00 c1 02 01 00 c2 02 01 02 c0 01 0a .....

```

可聚类指纹信息

交互自识别聚类分析

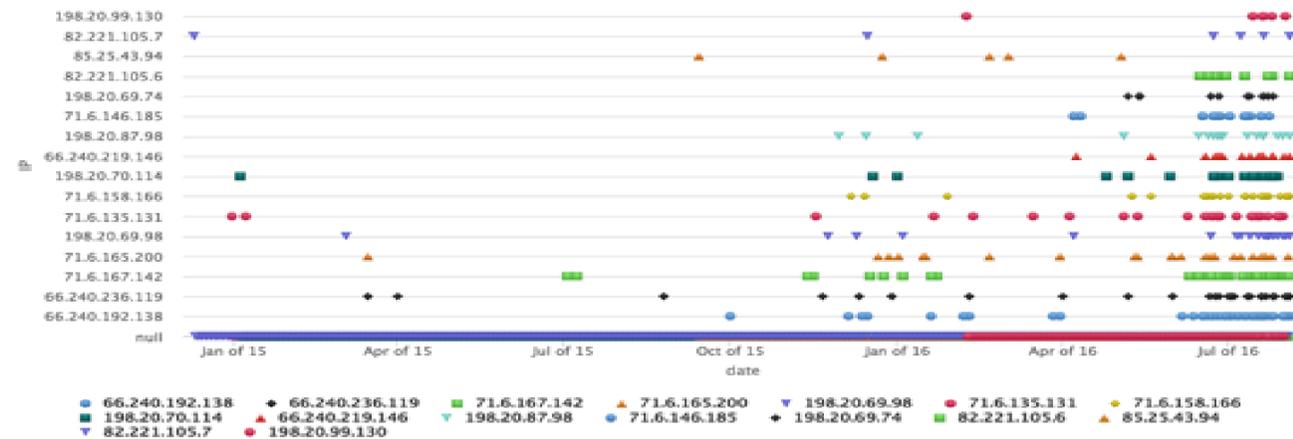


Shodan组织战术威胁情报

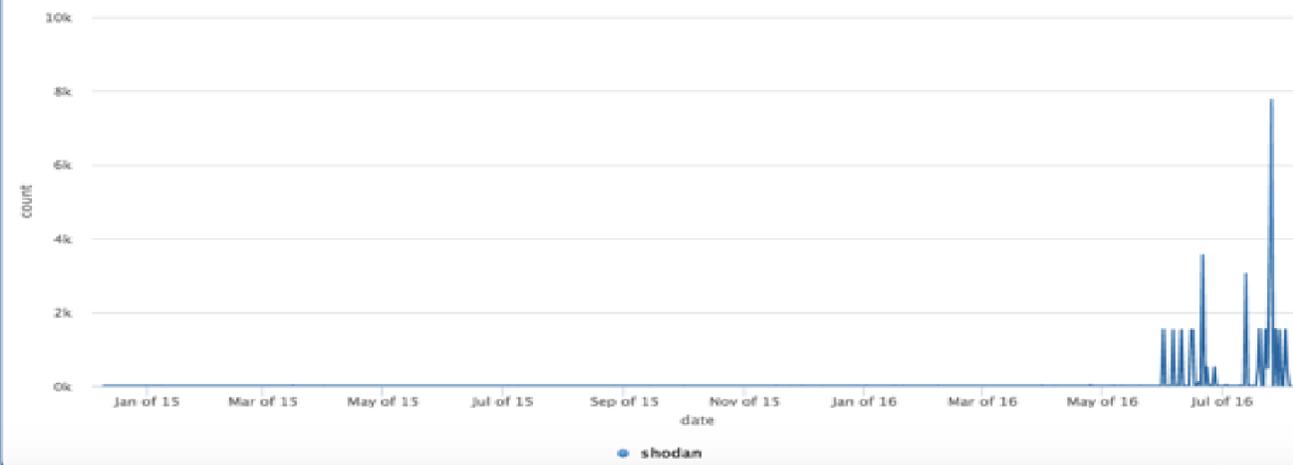
Organization Name

shodan

Scanning IP activity of protocols of shodan



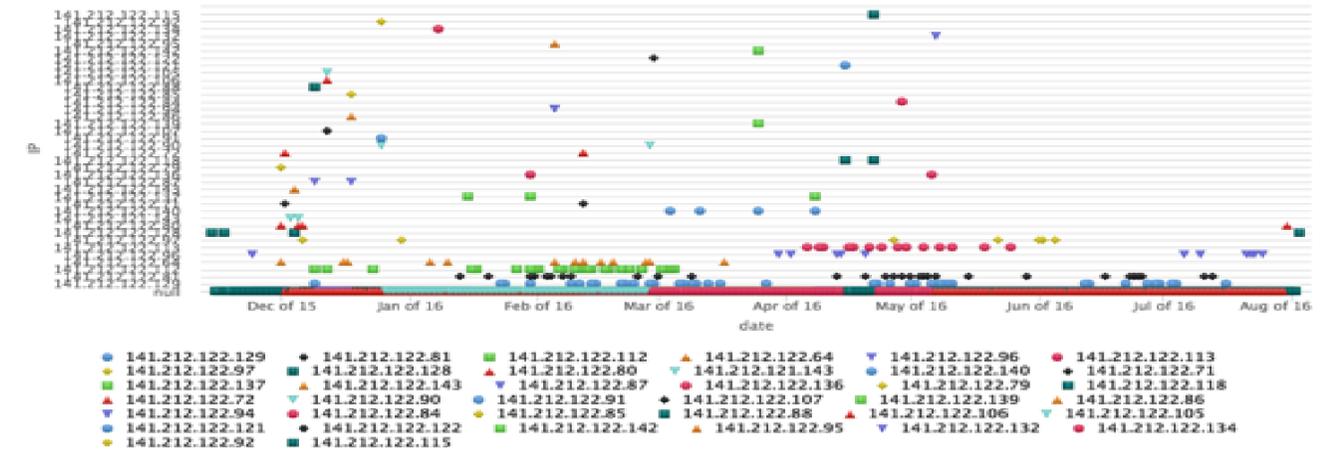
Scanning activity of protocols of shodan



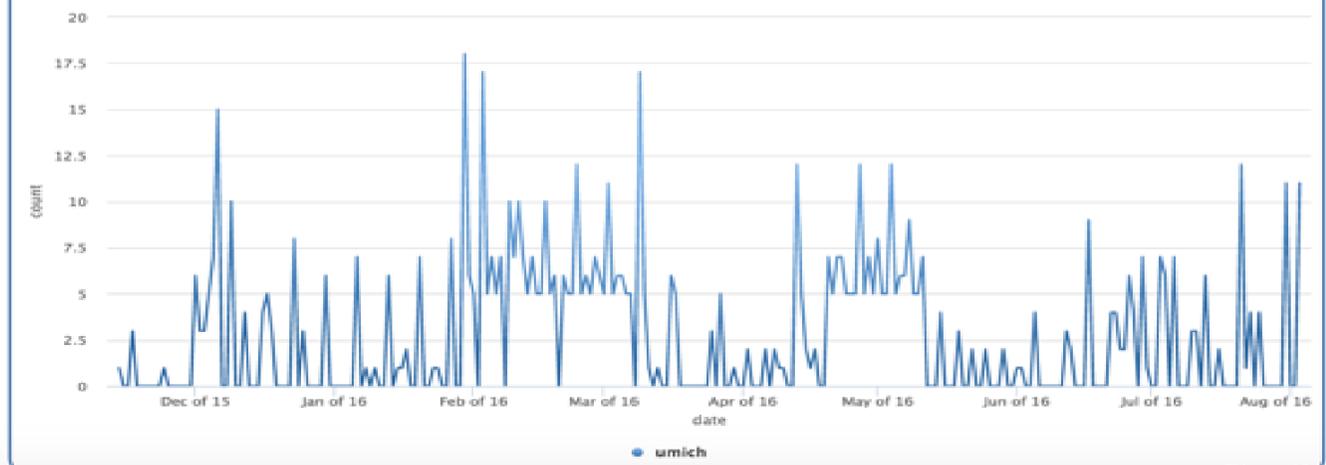
Organization Name

umich

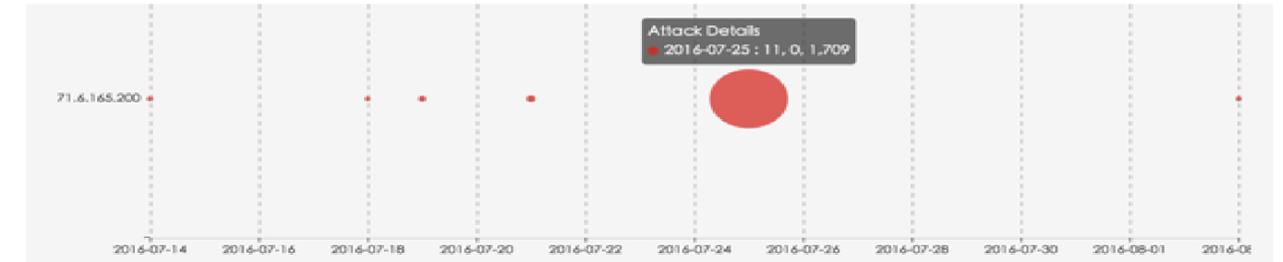
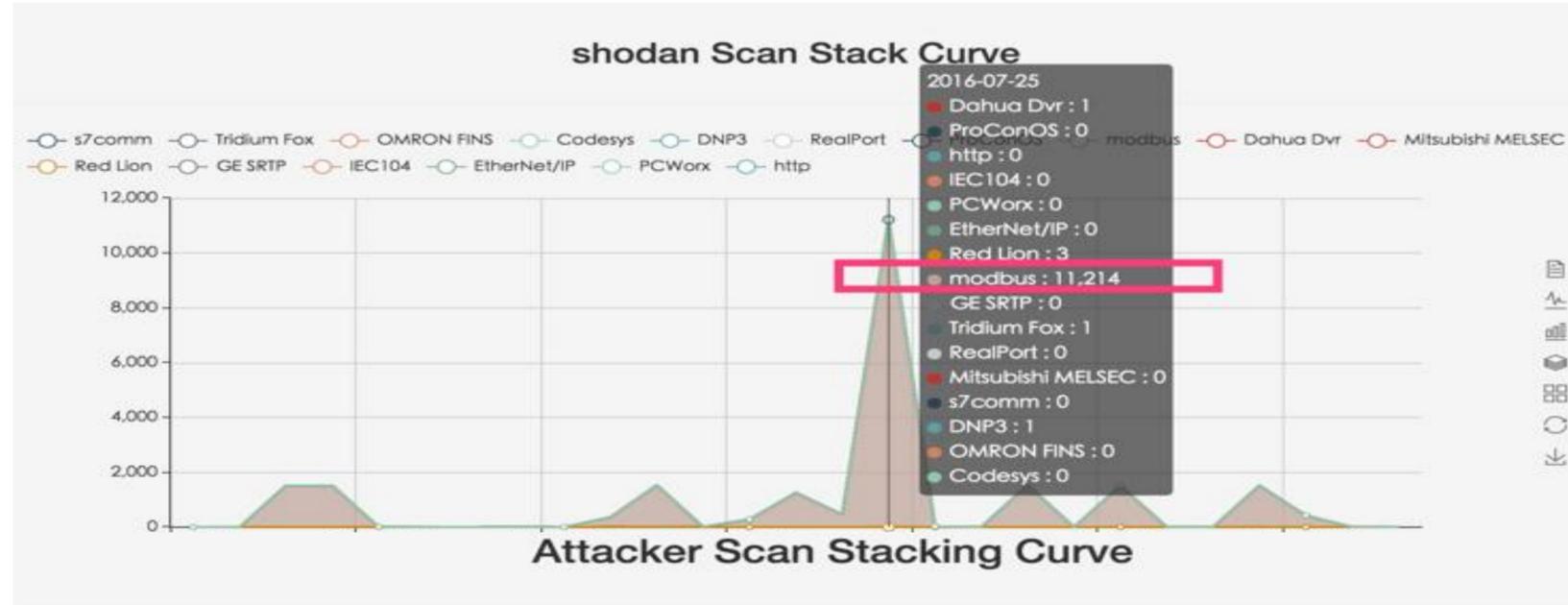
Scanning IP activity of protocols of umich



Scanning activity of protocols of umich



Shodan组织战术威胁情报



2016-06-06T00:40:35.169Z	["66.240.192.138",53605]	000100000004005a0002	modbus
2016-06-06T00:40:36.169Z	["66.240.192.138",53605]	01bf00000005005a000606	modbus
2016-06-06T00:40:37.171Z	["66.240.192.138",53605]	000400000005005a000300	modbus
2016-06-06T00:40:38.172Z	["66.240.192.138",53605]	000f0000000d005a00200014006400000f	modbus
2016-06-06T00:40:41.175Z	["66.240.192.138",53605]	0000000000020111	modbus
2016-06-06T00:40:43.177Z	["66.240.192.138",53605]	000000000005012b0e0100	modbus
2016-06-06T00:40:47.179Z	["66.240.192.138",53605]	0000000000020211	modbus
2016-06-06T00:40:49.182Z	["66.240.192.138",53605]	000000000005022b0e0100	modbus
2016-06-06T00:40:53.187Z	["66.240.192.138",53605]	0000000000020311	modbus
2016-06-06T00:40:55.188Z	["66.240.192.138",53605]	000000000005032b0e0100	modbus
2016-06-06T00:40:59.190Z	["66.240.192.138",53605]	0000000000020411	modbus
2016-06-06T00:41:01.191Z	["66.240.192.138",53605]	000000000005042b0e0100	modbus
2016-06-06T00:41:05.193Z	["66.240.192.138",53605]	0000000000020511	modbus
2016-06-06T00:41:07.196Z	["66.240.192.138",53605]	000000000005052b0e0100	modbus
2016-06-06T00:41:11.199Z	["66.240.192.138",53605]	0000000000020611	modbus
2016-06-06T00:41:13.200Z	["66.240.192.138",53605]	000000000005062b0e0100	modbus
2016-06-06T00:41:17.202Z	["66.240.192.138",53605]	0000000000020711	modbus
2016-06-06T00:41:19.203Z	["66.240.192.138",53605]	000000000005072b0e0100	modbus
2016-06-06T00:41:23.205Z	["66.240.192.138",53605]	0000000000020811	modbus
2016-06-06T00:41:25.206Z	["66.240.192.138",53605]	000000000005082b0e0100	modbus
2016-06-06T00:41:27.207Z	["66.240.192.138",53605]	0000000000020911	modbus
2016-06-06T00:41:29.208Z	["66.240.192.138",53605]	000000000005092b0e0100	modbus
2016-06-06T00:41:33.209Z	["66.240.192.138",53605]	0000000000020a11	modbus
2016-06-06T00:41:35.210Z	["66.240.192.138",53605]	0000000000050a2b0e0100	modbus
2016-06-06T00:41:38.212Z	["66.240.192.138",53605]	0000000000020b11	modbus
2016-06-06T00:41:40.214Z	["66.240.192.138",53605]	0000000000050b2b0e0100	modbus
2016-06-06T00:41:44.215Z	["66.240.192.138",53605]	0000000000020c11	modbus
2016-06-06T00:41:46.215Z	["66.240.192.138",53605]	0000000000050c2b0e0100	modbus
2016-06-06T01:05:39.071Z	["66.240.192.138",53605]	000000000002fd11	modbus
2016-06-06T01:05:42.074Z	["66.240.192.138",53605]	000000000002fe11	modbus
2016-06-06T01:05:45.079Z	["66.240.192.138",53605]	000000000002ff11	modbus
2016-06-06T01:05:47.081Z	["66.240.192.138",53605]	000000000005ff2b0e0100	modbus

常规扫描

非常规扫描

Shodan组织战术威胁情报

This IP was reported 51 times. See below for details.

ISP	PlusServer AG
Hostname	atlantic626.dedicatedpanel.com
Organization	PlusServer AG
Connection Type	Corporate
Country	France
City	Strasbourg, Bas-Rhin

indicator	comments	protocol	portlist	portlist_src	tags	description	updated_at
188.138.17.205	1		8443		scanner		2015-11-22 08:05:01 UTC
188.138.17.205	1		8443		scanner		2015-11-15 05:05:01 UTC
188.138.17.205	1		8443		scanner		2015-11-16 06:20:00 UTC
188.138.17.205	1		8443		scanner		2015-11-07 13:25:00 UTC
188.138.17.205	1		8443		scanner		2015-11-07 15:00:00 UTC
188.138.17.205	1		8080		scanner		2015-11-10 12:00:01 UTC
188.138.17.205	1		8080		scanner		2015-11-10 16:35:00 UTC
188.138.17.205	1		8443		scanner		2015-11-11 08:10:00 UTC
188.138.17.205	1		80		scanner		2015-11-22 00:35:01 UTC
188.138.17.205	1		443		scanner		2015-11-28 19:00:01 UTC
188.138.17.205	1		443		scanner		2015-12-04 22:40:00 UTC
188.138.17.205	1		8080		scanner		2015-12-05 17:28:39 UTC
188.138.17.205	1		8443		scanner		2015-12-08 20:18:02 UTC
188.138.17.205	1		443		scanner		2015-12-10 16:05:43 UTC
188.138.17.205	1		2083		scanner		2016-01-03 03:10:01 UTC
188.138.17.205	1		2376		scanner		2016-01-03 07:22:32 UTC
188.138.17.205	1		1200		scanner		2016-01-03 11:00:00 UTC
188.138.17.205	1		2082		scanner		2016-01-03 16:00:02 UTC
188.138.17.205	1		7779		scanner		2016-01-04 13:15:01 UTC
188.138.17.205	1		8139		scanner		2016-01-04 19:09:06 UTC
188.138.17.205	1		5222		scanner		2016-01-05 05:24:36 UTC
188.138.17.205	1		22		scanner		2016-01-05 08:10:00 UTC
188.138.17.205	1		82		scanner		2016-01-07 11:30:00 UTC
188.138.17.205	1		3389		scanner		2016-01-08 17:24:34 UTC
188.138.17.205	1		8060		scanner		2016-01-09 12:40:37 UTC
188.138.17.205	1		8090		scanner		2016-01-10 06:30:01 UTC
188.138.17.205	1		8649		scanner		2016-01-14 16:32:31 UTC
188.138.17.205	1		62078		scanner		2016-01-20 08:12:24 UTC
188.138.17.205	1		8139		scanner		2016-01-20 10:27:31 UTC
188.138.17.205	1		8000		scanner		2016-01-20 14:42:42 UTC
188.138.17.205	1		2067		scanner		2016-01-22 03:31:34 UTC
188.138.17.205	1		2332		scanner		2016-01-22 13:47:00 UTC
188.138.17.205	1		50100		scanner		2016-01-27 13:39:22 UTC
188.138.17.205	1		3689		scanner		2016-01-28 01:24:55 UTC
188.138.17.205	1		6000		scanner		2016-01-29 08:50:01 UTC
188.138.17.205	1		81		scanner		2016-01-29 07:41:15 UTC
188.138.17.205	1		2455		scanner		2016-02-01 22:00:00 UTC
188.138.17.205	1		21025		scanner		2016-02-02 00:45:16 UTC
188.138.17.205	1		102		scanner		2016-02-03 11:41:54 UTC

2016-07-19T16:20:31.529Z	["188.138.17.205",46332]	000100000004005a0002	modbus
2016-07-19T16:20:32.530Z	["188.138.17.205",46332]	01bf00000005005a000606	modbus
2016-07-19T16:20:33.533Z	["188.138.17.205",46332]	000400000005005a000300	modbus
2016-07-19T16:20:34.535Z	["188.138.17.205",46332]	000f0000000d005a002000140064000000f	modbus
2016-07-19T16:20:37.538Z	["188.138.17.205",46332]	0000000000020111	modbus
2016-07-19T16:20:39.538Z	["188.138.17.205",46332]	000000000005012b0e0100	modbus
2016-07-19T16:20:43.543Z	["188.138.17.205",46332]	0000000000020211	modbus
2016-07-19T16:20:45.545Z	["188.138.17.205",46332]	000000000005022b0e0100	modbus
2016-07-19T16:20:49.549Z	["188.138.17.205",46332]	0000000000020311	modbus
2016-07-19T16:20:51.552Z	["188.138.17.205",46332]	000000000005032b0e0100	modbus
2016-07-19T16:20:55.557Z	["188.138.17.205",46332]	0000000000020411	modbus
2016-07-19T16:20:57.559Z	["188.138.17.205",46332]	000000000005042b0e0100	modbus
2016-07-19T16:21:01.562Z	["188.138.17.205",46332]	0000000000020511	modbus
2016-07-19T16:21:03.564Z	["188.138.17.205",46332]	000000000005052b0e0100	modbus
2016-07-19T16:21:07.567Z	["188.138.17.205",46332]	0000000000020611	modbus
2016-07-19T16:21:09.569Z	["188.138.17.205",46332]	000000000005062b0e0100	modbus
2016-07-19T16:21:13.573Z	["188.138.17.205",46332]	0000000000020711	modbus
2016-07-19T16:21:15.576Z	["188.138.17.205",46332]	000000000005072b0e0100	modbus
2016-07-19T16:21:19.580Z	["188.138.17.205",46332]	0000000000020811	modbus
2016-07-19T16:21:21.586Z	["188.138.17.205",46332]	000000000005082b0e0100	modbus
2016-07-19T16:21:25.587Z	["188.138.17.205",46332]	0000000000020911	modbus
2016-07-19T16:21:27.589Z	["188.138.17.205",46332]	000000000005092b0e0100	modbus
2016-07-19T16:21:31.593Z	["188.138.17.205",46332]	0000000000020a11	modbus
2016-07-19T16:21:33.595Z	["188.138.17.205",46332]	0000000000050a2b0e0100	modbus
2016-07-19T16:21:37.599Z	["188.138.17.205",46332]	0000000000020b11	modbus
2016-07-19T16:21:39.601Z	["188.138.17.205",46332]	0000000000050b2b0e0100	modbus
2016-07-19T16:21:43.604Z	["188.138.17.205",46332]	0000000000020c11	modbus
2016-07-19T16:21:45.606Z	["188.138.17.205",46332]	0000000000050c2b0e0100	modbus

与shodan相同的扫描模式



Shodan组织战术威胁情报

IP地址 94.102.49.193
 地理位置 荷兰,北荷兰省,阿姆斯特丹
 ASN 29073 (QUASINETWORKS, NL) 高风险 ?
 Tags 垃圾邮件 恶意软件 IDC服务器 扫描 可疑 僵尸网络 漏洞利用

威胁情报 IP反查 可视分析

威胁情报检测		
情报源	发现时间	情报类型
开源情报	2016-07-19	扫描
开源情报	2016-07-15	漏洞利用
开源情报	2016-07-15	漏洞利用,恶意软件
开源情报	2016-07-08	恶意软件
开源情报	2016-07-07	僵尸网络
开源情报	2016-07-06	可疑
ThreatBook Labs	2016-07-06	垃圾邮件
ThreatBook Labs	2016-07-06	僵尸网络
ThreatBook Labs	2016-07-06	垃圾邮件,僵尸网络

2016-07-23T11:29:13.412Z	["94.102.49.190",43071]	000100000004005a0002	modbus
2016-07-23T11:29:14.413Z	["94.102.49.190",43071]	01bf00000005005a000606	modbus
2016-07-23T11:29:15.415Z	["94.102.49.190",43071]	000400000005005a000300	modbus
2016-07-23T11:29:16.417Z	["94.102.49.190",43071]	000f0000000d005a002000140064000000f	modbus
2016-07-23T11:29:18.419Z	["94.102.49.190",43071]	0000000000020111	modbus

indicator	comments	protocol	portlist	portlist_src	tags	description	updated_at
94.102.49.193			49152		scanner		2016-07-05 18:45:52 UTC
94.102.49.193			32400		scanner		2016-07-06 02:07:13 UTC
94.102.49.193			1911		scanner		2016-07-06 07:33:06 UTC
94.102.49.193			7779		scanner		2016-07-07 12:18:34 UTC
94.102.49.193			80		scanner		2016-07-11 06:13:32 UTC
94.102.49.193			789		scanner		2016-07-12 02:01:49 UTC
94.102.49.193			81		scanner		2016-07-13 03:06:56 UTC
94.102.49.193			49		scanner		2016-07-13 15:09:27 UTC
94.102.49.193			7547		scanner		2016-07-14 03:01:52 UTC
94.102.49.193			8000		scanner		2016-07-14 04:17:07 UTC
94.102.49.193			8888		scanner		2016-07-20 12:38:01 UTC
94.102.49.193			83		scanner		2016-07-20 13:23:13 UTC
94.102.49.193			6666		scanner		2016-07-23 17:57:16 UTC
94.102.49.193			5555		scanner		2016-07-25 12:40:34 UTC
94.102.49.193			4064		scanner		2016-07-31 16:08:01 UTC
94.102.49.193			4000		scanner		2016-08-01 19:02:52 UTC
94.102.49.193			175		scanner		2016-08-02 12:01:12 UTC
94.102.49.193			18245		scanner		2016-08-02 17:47:15 UTC
94.102.49.193			10000		scanner		2016-08-04 19:37:35 UTC
94.102.49.193			1311		scanner		2016-08-05 03:29:05 UTC
94.102.49.193			7474		scanner		2016-08-05 11:40:50 UTC
94.102.49.193			2628		scanner		2016-08-05 14:51:30 UTC

Shodan组织战术威胁情报

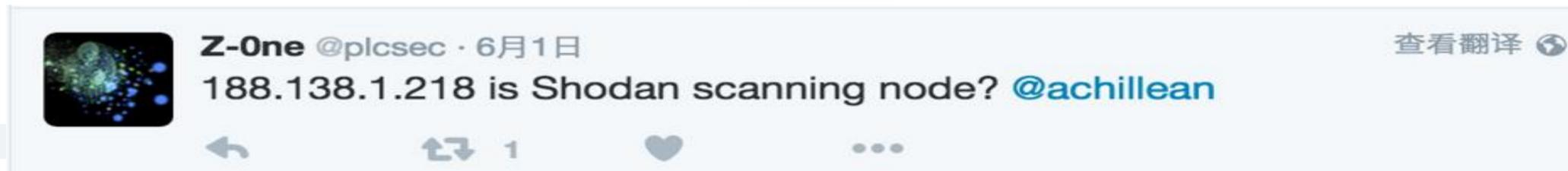
188.138.1.218 was found in our database!

This IP was reported **125 times**. See below for details.

ISP	PlusServer AG
Hostname	atlantic381.startdedicated.de
Organization	PlusServer AG
Connection Type	Corporate
Country	Germany
City	Unknown

Source	Date	Category
ThreatBook Labs	2016-06-30	僵尸网络
开源情报	2016-06-20	僵尸网络
开源情报	2016-06-17	扫描
ThreatBook Labs	2016-05-17	IDC服务器
开源情报	2016-04-19	扫描
ThreatBook Labs	2016-04-12	垃圾邮件
开源情报	2016-03-25	可疑
开源情报	2016-03-20	恶意软件
ThreatBook Labs	2016-02-14	垃圾邮件,僵尸网络
开源情报	2016-02-02	漏洞利用,恶意软件
开源情报	2015-12-12	僵尸网络,扫描
开源情报	2015-12-10	扫描
开源情报	2015-12-04	可疑
开源情报	2015-12-02	可疑
开源情报	2015-11-26	漏洞利用
开源情报	2015-11-26	扫描

```
{'function_code': 90, 'slave_id': 0, 'request': '00010000004005a0002', 'response': '5a00feb7'}
{'function_code': 90, 'slave_id': 0, 'request': '01bf0000005005a000606', 'response': '5a00fe:}
{'function_code': 90, 'slave_id': 0, 'request': '000400000005005a000300', 'response': '5a00fe}
{'function_code': 90, 'slave_id': 0, 'request': '000f0000000d005a002000140064000000f600',
```



情报类型

indicator	comments	protocol	portlist	portlist_src	tags	description	updated_at
188.138.1.218	1		110		scanner		2015-11-12 23:40:00 UTC
188.138.1.218	1		26		scanner		2015-11-22 05:15:01 UTC
188.138.1.218	1		143		scanner		2015-11-14 18:55:00 UTC
188.138.1.218	1		3389		scanner		2015-11-23 09:05:01 UTC
188.138.1.218	1		102		scanner		2015-11-16 09:40:00 UTC
188.138.1.218	1		143		scanner		2015-11-20 18:40:01 UTC
188.138.1.218	1		143		scanner		2015-11-18 00:50:00 UTC
188.138.1.218	1		110		scanner		2015-11-09 04:35:00 UTC
188.138.1.218	1		110		scanner		2015-11-12 17:50:00 UTC
188.138.1.218	1		26		scanner		2015-12-01 19:40:01 UTC
188.138.1.218	1		143		scanner		2015-12-03 11:45:25 UTC
188.138.1.218	1		80		scanner		2015-12-03 12:30:00 UTC
188.138.1.218	1		23		scanner		2015-12-06 17:45:00 UTC
188.138.1.218	1		102		scanner		2015-12-06 21:05:13 UTC
188.138.1.218	1		21		scanner		2015-12-07 11:56:03 UTC
188.138.1.218	1		502		scanner		2015-12-09 19:09:19 UTC
188.138.1.218	1		3306		scanner		2015-12-13 02:55:01 UTC
188.138.1.218	1		102		scanner		2015-12-13 21:09:48 UTC
188.138.1.218	1		80		scanner		2015-12-17 11:21:50 UTC
188.138.1.218	1		21		scanner		2015-12-21 06:51:06 UTC
188.138.1.218	1		502		scanner		2015-12-23 13:39:57 UTC
188.138.1.218	1		23		scanner		2015-12-30 15:31:12 UTC
188.138.1.218	1		143		scanner		2016-01-01 05:34:06 UTC
188.138.1.218	1		21		scanner		2016-01-02 15:21:46 UTC
188.138.1.218	1		3306		scanner		2016-01-03 15:55:00 UTC

Shodan组织战略威胁情报

198.20.70.114	US	census3.shodan.io
71.6.165.200	US	census12.shodan.io
66.240.236.119	US	census6.shodan.io
71.6.135.131	US	census7.shodan.io
66.240.192.138	US	census8.shodan.io
71.6.167.142	US	census9.shodan.io
198.20.87.98	US	border.census.shodan.io
71.6.146.185	US	pirate.census.shodan.io
82.221.105.6	IS	census10.shodan.io
71.6.158.166	US	ninja.census.shodan.io
66.240.219.146	US	burger.census.shodan.io
82.221.105.7	IS	census11.shodan.io
198.20.69.74	US	census1.shodan.io
71.6.146.186	US	inspire.census.shodan.io
198.20.99.130	NL	census4.shodan.io
198.20.69.75	US	census1.shodan.io
198.20.69.76	US	census1.shodan.io
198.20.69.98	US	census2.shodan.io

<http://plcscan.org/blog/2016/06/ics-security-research-report-2016-05/>

《针对网络空间关键基础设施情报收集的组织行为分析报告》

从我们收集的数据来看，Shodan针对Modbus与S7comm协议进行扫描的IP地址存在15个（不完全统计），遍布美国、德国、荷兰等不同地域，同时具备强大的分布式调度能力。从针对工控专用协议扫描探测的过程来看，Shodan扫描引擎对工控协议的情报收集可以追溯到2014年。据不完全统计，截至目前Shodan已经支持了超过29个工控协议。

从协议扫描深度来看，Shodan基于Modbus协议的扫描已经深入到可识别PLC上具体项目文件信息，同时Shodan针对Modbus信息的获取仅依赖4个包含90功能码数据包，在保证获取相同信息的同时极大程度提高了扫描效率，由此可见Shodan团队对于协议的分析理解程度极高。

从扫描方式上来看，Shodan在针对Modbus协议进行扫描时，在判断502端口开放后先进行了通过17功能码进行的确认帧，在收到了正确的响应后才正式开始发送数据包；针对S7协议扫描时，同样也会先进行TPKP和COTP连接，再确认连接无误后，重新进行正式扫描行为，该处理细节能保证扫描行为的精准性和高效性，避免设备端口接受到非匹配协议数据而产生隐患。

从行为的时间分布上来看，Shodan团队针对工控协议的扫描具有明显的时间规律，Shodan同时对社区关注极高，目前已经集成了我们曾经发布的GESRTP、MELSEC-Q、MoxaNPort探测识别方法。

另外，值得关注的是Shodan还具备针对工控协议蜜罐的识别机制，该机制依赖IP基础位置信息、开放端口情况、蜜罐默认配置信息等进行综合评判，通过产生量化的系数来进行蜜罐甄别。

Shodan组织战略威胁情报

节点IP	RDNS	探测扫描总端口数	首次探测S7协议时间 (102)	首次探测Modbus协议时间 (502)	首次探测Ethernet/IP协议时间 (44818)
82.221.105.6	census10	169	20130821	20130827	20141025
71.6.167.142	census9	232	20140720	20140526	20140504
71.6.135.131	census7	234	20140508	20140509	20140510
66.240.236.119	census6	233	20140602	20140706	20140430
71.6.158.166	ninja.census	111	—	—	20160520
82.221.105.7	census11	167	20140206	20140206	20140207
85.25.43.94	rim.census	192	20150122	—	20141016
71.6.165.200	census12	236	20140222	20140227	20140212
198.20.99.130	census4	92	20140516	20140630	
66.240.192.138	census8	237	20140226	20140225	20140226
71.6.146.185	Inspire.census	67	—	—	20160414
66.240.219.146	burger.census	107	—	—	20160520
198.20.69.98	border.census	215	20141007	20141104	20140604
198.20.70.114	census3	224	20140512	20140518	20140603
188.138.1.218	unknown	93	20150811	20150627	20160524



- 2012年6月参与美国国土安全部SHINE计划
- 2013年平台提供针对工控系统Dork搜索
- 2014年1月SHINE计划结束，为期两年
- 2014年2月全球范围内针对S7协议扫描
- 2014年2月全球范围内针对Modbus协议扫描
- 2014年2月全球范围内针对Ethernet/IP协议扫描
- 2015年3月ICS Radar上线
- 2015年6月ICS Honeypot Score上线
- 2016年6月针对modbus协议进行brute unitID

Thank You!



中国互联网安全大会



360互联网安全中心