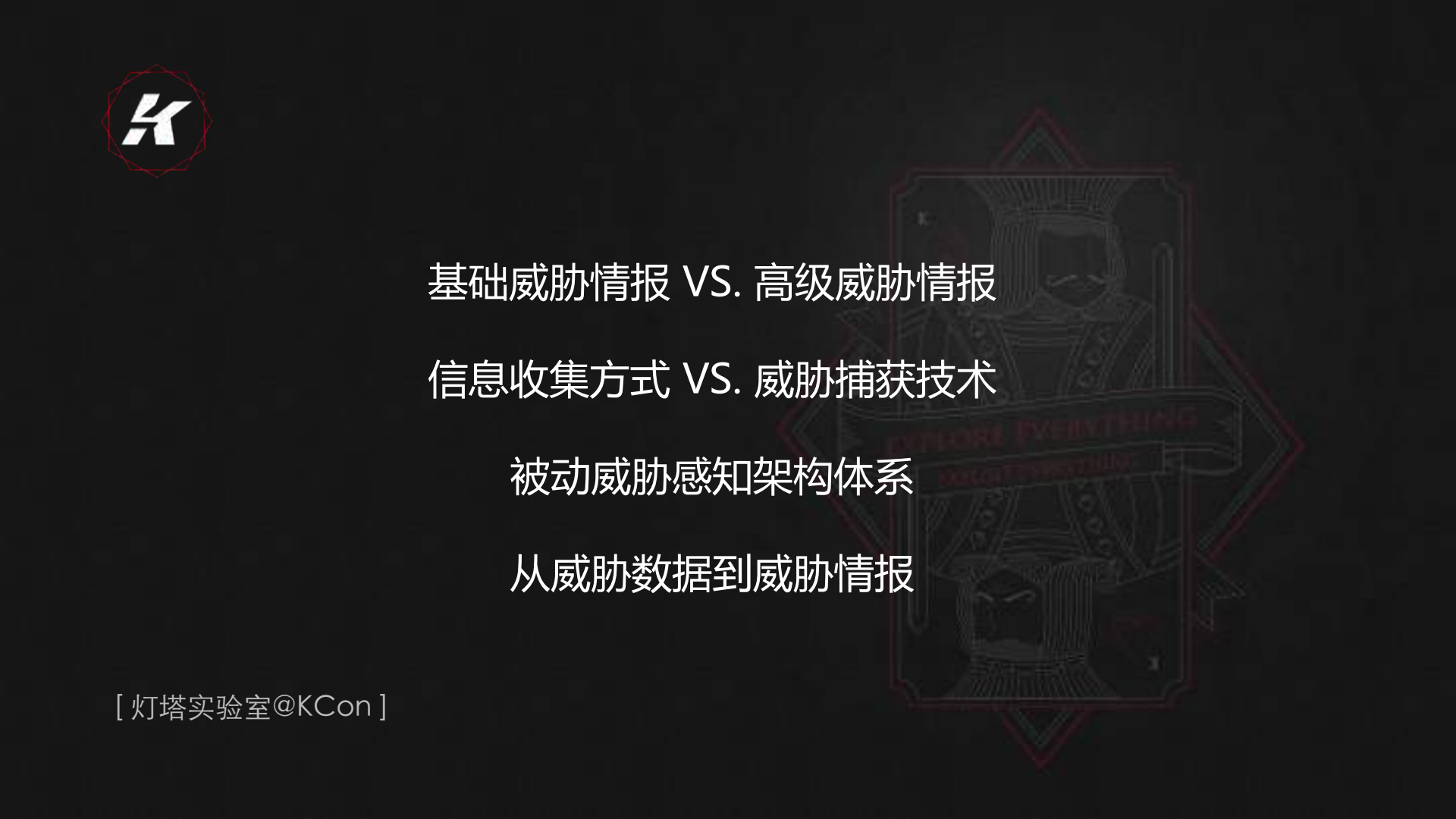
感知 · 诱捕 · 情报 · 协作

网络空间工控系统威胁情报

[Kimon@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



基础威胁情报 VS. 高级威胁情报

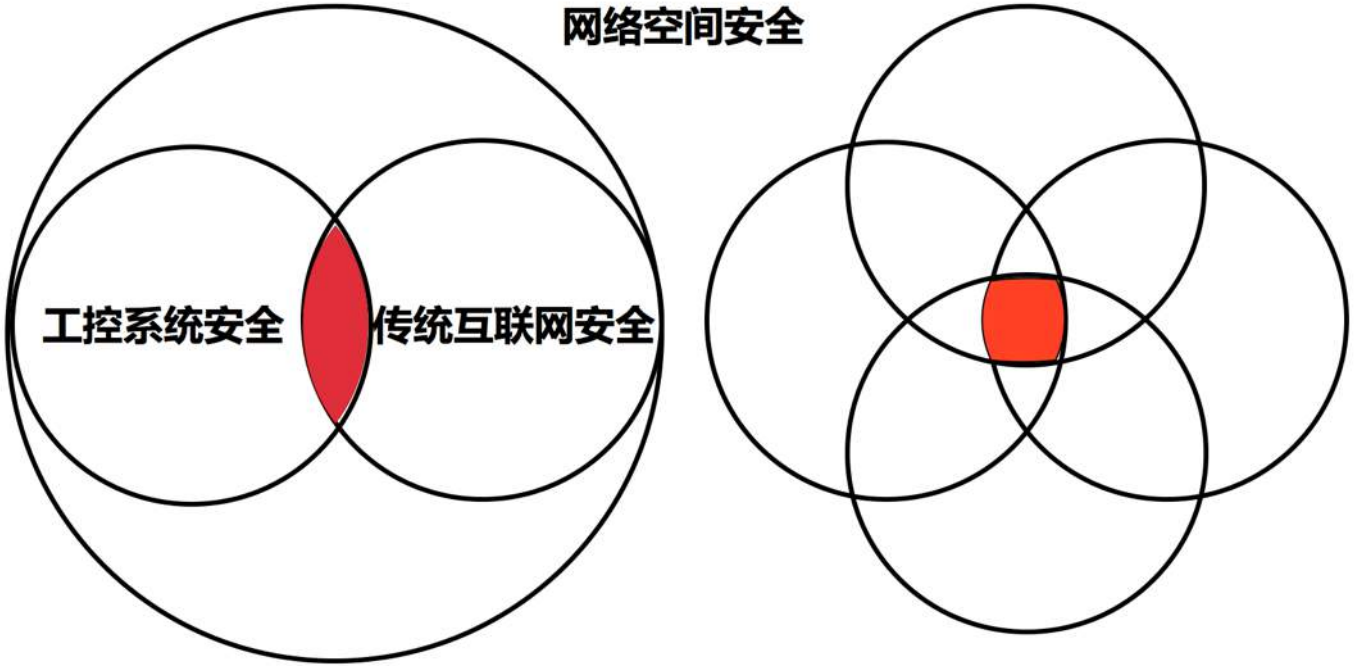
信息收集方式 VS. 威胁捕获技术

被动威胁感知架构体系

从威胁数据到威胁情报

Part. **01**

基础威胁情报 VS. 高级威胁情报

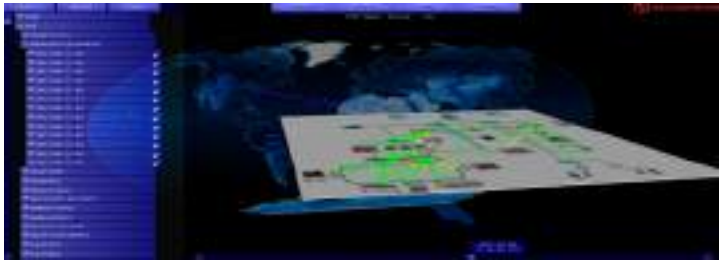

网络空间安全
工控系统安全
传统互联网安全

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

绘制网络空间地图，构建上帝视角感知能力



DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Defense Advanced Research Projects Agency > Program Information

Plan X

Mr. Frank Pound

BEACON LAB 灯塔实验室

基础威胁情报（数据情报）

流量/文件
BGP/AS/路由/Whois/指纹
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

DOMAINTOOLS
FARSIGHT SECURITY
virustotal
ThreatBook
360 INTERNET SECURITY CENTER
Recorded Future
THREATCONNECT
alienvault
MaxMind®
IBM X-Force Exchange

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.

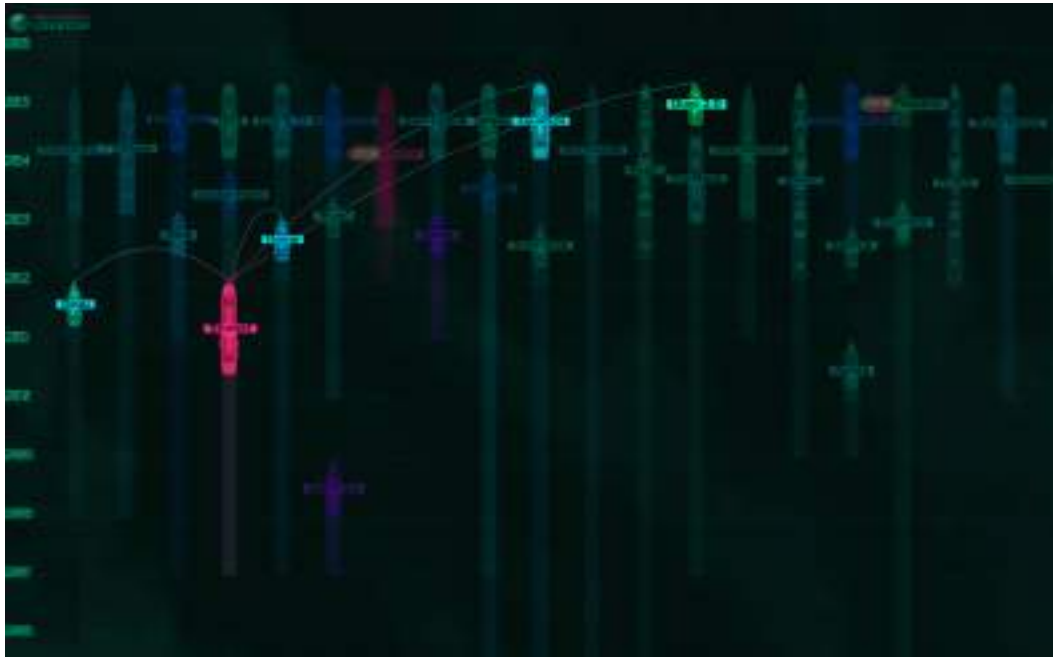
工控系统威胁情报

国家关键信息基础设施

针对能源、关键制造等行业的威胁加剧
- Stuxnet/Duqu/Flame
- BlackEnergy

针对SCADA系统的威胁加剧
- 远程可控制SCADA、PLC
- 遍布互联网的工控资产
- 针对工控专有协议的探测

针对工控设施的威胁行为更值得研究
- 全球网络空间“底线”
- 具备上层战略特征



https://apt.securelist.com

Part. **02**

信息收集方式VS. 威胁诱捕技术

开放的互联网设备搜索平台

Shodan	shodan.io
Censys	censys.io
ZoomEye	zoomeye.org
ICSfind	icsfind.org
IVRE	ivre.rocks
Rapid7	scan.io

开源扫描器框架

nmap	nmap.org
zmap	zmap.io
masscan	github.com/robertdavidgraham/masscan

基于指纹识别平台的工控设备信息收集方式

《ICS/SCADA/PLC Google/Shodanhq Cheat Sheet》

http://scadastrangelove.org/

《Internet connected ICS/SCADA/PLC Cheat Sheet》

http://www.scadaexposure.com/

利用标准且公开/私有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、模块信息等信息

```
Copyright: Original Siemens Equipment
PLC name: p-Faellung
Module type: CPU 314
Unknown (129): Boot Loader            A
Module: 6ES7 314-1AG14-0AB0  v.0.4
Basic Firmware: v.3.3.2
Module name: CPU 314
Serial number of module: S C-C1T496792012
Plant identification:
Basic Hardware: 6ES7 314-1AG14-0AB0  v.0.4
```

BMX P34 2020 Version: v2.5

```
Unit ID: 0
— Device Identification: Schneider Electric BMX P34 2020
— CPU module: BMX P34 2020
— Memory card: BMXRMS008MP
— Project information: Project - V6.0   HP-1
— Project revision: 0.0.107
— Project last modified: 2016-06-02 14:30:46
```

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

BEACON LAB 灯塔实验室

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)	Q*UDE(H)CPU FTP server ready.
Moxa	NPort	HTTP（80）	Server: MoxaHttp

Vendor	Product	Protcol	Dork/Banner
Siemens	PCS7	http	S7Web.css
Siemens	PCS7	url	Portal0000.htm
Siemens	SIMATIC	url	Portal/Portal.mwsl
Siemens	SIMATIC	url	S7Web.css
Siemens	SIMATIC HMI Miniweb	url	/CSS/Miniweb.css
Siemens	SIMATIC HMI Miniweb	title	Miniweb Start Page
Rockwell Automation	CompactLogix	title	Rockwell Automation
Rockwell Automation	CompactLogix	title	Device Name
Rockwell Automation	SLC5	title	1747-L552
schneider electric	PowerLogic PM800	header	PowerLogic PM800
Schneider Electric	PowerLogic ION8650	header	8650 ION
Schneider Electric	PowerLogic ION8600	header	8600 ION
Schneider Electric	PowerLogic ION7650/7550	header	ION 7550
Schneider Electric	PowerLogic ION7650/7550	header	ION 7650
Schneider Electric	PowerLogic ION7300	header	ION 7300
Schneider Electric	PowerLogic ION6200	header	ION6200
Schneider Electric	PowerLogic PM1200	header	PM1200
Schneider Electric	PowerLogic DM6200	header	DM6200
Schneider Electric	PowerLogic Branch Current Monitor	header	BCM42
Schneider Electric	PowerLogic Ethernet Gateway (EGX)	header	EGX100
Schneider Electric	PowerLogic EGX300	header	EGX300
Schneider Electric	PowerLogic ION7550RTU	header	ION 7550RTU
Schneider Electric	Modicon\Quantum	title	Quantum CPU Web Server
Schneider Electric	Modicon\Premium	title	Premium CPU Web Server

识别工具列举

插件名称	端口	描述
BACnet-discover-enumerate.nse	47808	识别和枚举BACnet设备
etg-info.nse	10001	请求通信自动状态信息
codesys-v2-discover.nse	1200	识别和枚举CoDeSys v2协议
cspvs-info.nse	2222	识别PCS7/S7 300协议
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协议
modicon-info.nse	502	枚举施耐德PLC信息
omronfp-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
precontos-info.nse	20547	识别和枚举使用Precontos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	识别和枚举三菱电系列PLC信息
melsecq-discover-udp.nse	5006	识别和枚举三菱电系列PLC信息

Vendor	System / Component	SCADAhacker Reference	Metasploit Reference
7-Technologies	IGSS	ICS-11-080-03 ICSA-11-132-01A	exploit/windows/scada/igss9_igssdataserver_listall.rb exploit/windows/scada/igss9_igssdataserver_rename.rb exploit/windows/scada/igss9_misc.rb auxiliary/admin/scada/igss_exec_17.rb
AzeoTech	DAQ Factory	Click Here	exploit/windows/scada/daq_factory_bof.rb
3S	CoDeSys	Click Here	exploit/windows/scada/codesys_web_server.rb
BACnet	OPC Client	ICSA-10-264-01	exploit/windows/fileformat/bacnet_csv.rb
	Operator Workstation	n/a	exploit/windows/browser/teechart_pro.rb
Beckhoff	TwinCat	Click Here	auxiliary/dos/scada/beckhoff_twincat.rb
General Electric	D20 PLC	Press Release	auxiliary/gather/d20pass.rb
		DigitalBond S4	unstable-modules/auxiliary/d20/fgbd.rb
Iconics	Genesis32	ICS-11-080-02	exploit/windows/scada/iconics_genbroker.rb exploit/windows/scada/iconics_webhmi_setactivexguid.rb
Measuresoft	ScadaPro	Click Here	exploit/windows/scada/scadapro_cmdexe.rb
Moxa	Device Manager	ICS-10-293-02 ICSA-10-301-01	exploit/windows/scada/moxa_mdmtool.rb
RealFlex	RealWin SCADA		exploit/windows/scada/realwin.rb
		ICS-11-308-01 ICSA-11-313-01	exploit/windows/scada/realwin_scpc_initialize.rb exploit/windows/scada/realwin_scpc_initialize_rf.rb
			exploit/windows/scada/realwin_scpc_txtevent.rb
		ICS-11-080-04 ICSA-11-110-01	exploit/windows/scada/realwin_on_fc_binfile_a.rb exploit/windows/scada/realwin_on_fcs_login.rb
Scadatec	Procyon	Click Here	exploit/windows/scada/procyon_core_server.rb
ScadaTEC	ModbusTagServer ScadaPhone	Click Here	exploit/windows/fileformat/scadaphone_zip.rb
Schneider Electric	CitectSCADA CitectFacilities		exploit/windows/scada/citect_scada_odbc.rb
Sielco Sistemi	Winlog	ICSA-11-017-02	exploit/windows/scada/winlog_runtime.rb
Siemens Technomatix	FactoryLink	ICS-11-080-01 ICSA-11-091-01	exploit/windows/scada/factorylink_csaservice.rb exploit/windows/scada/factorylink_vrn_09.rb
Unitronics	OPC Server	n/a	exploit/exploits/windows/browser/teechart_pro.rb

https://scadahacker.com/resources/msf-scada.html

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

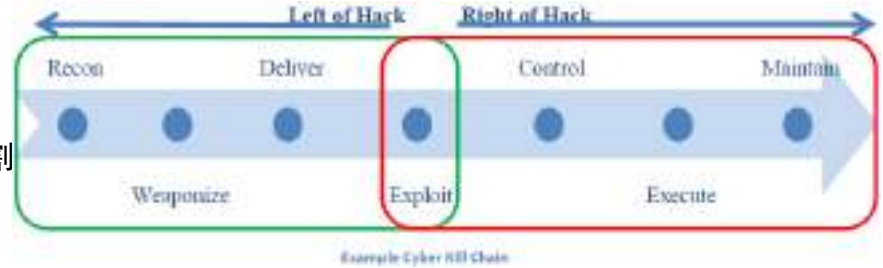
针对工控网络新型渗透模式

PLC Blaster

网络空间设备搜索平台

时间轴设备信息态势

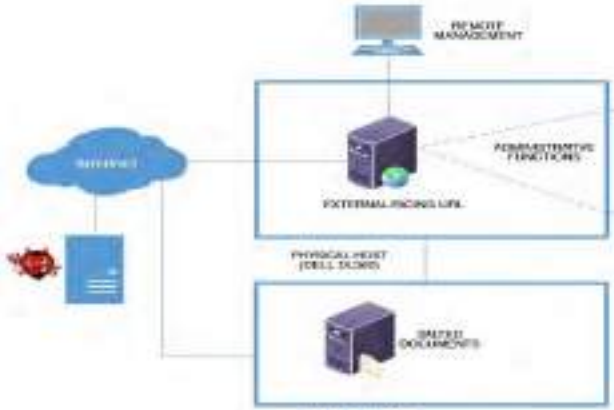
提供互联网“靶标”

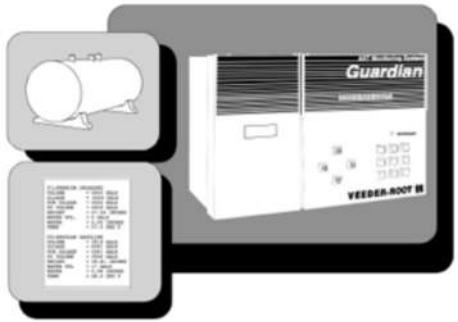


威胁捕获方式

传统安全防御设备

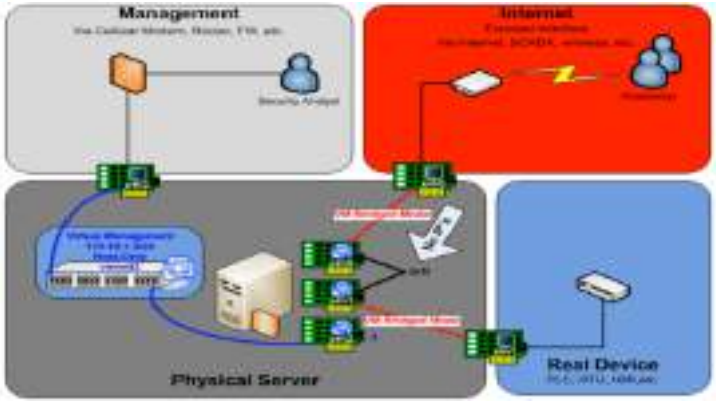
针对工控系统的蜜罐
- 思科PLC蜜罐
- Digitalbond
- 趋势科技
- Conpot





SCADA HoneyNet Project: Building Honeypots for Industrial Networks

Venkat Pothamsetty and Matthew Franz
Critical Infrastructure Assurance Group(CIAG)
Cisco Systems, Inc.

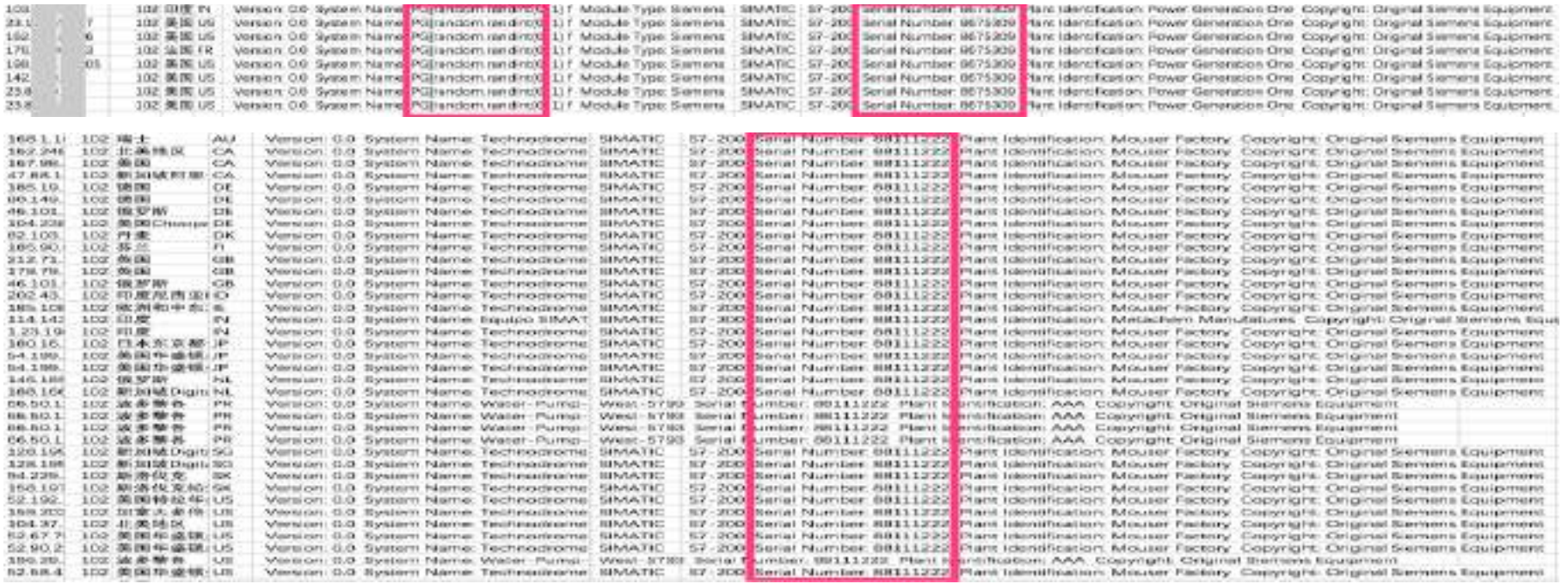


工控蜜罐存在的问题

- 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

BEACON LAB 灯塔实验室

主动监测国外蜜罐部署情况



通过Shodan搜索国外蜜罐案例

Shodan API

```
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
```

BEACON LAB 灯塔实验室

国外工控组合蜜罐案例

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 18:47:48 GMT
Connection: close
```

BEACON LAB
灯塔实验室

Part. **03**

被动威胁感知技术

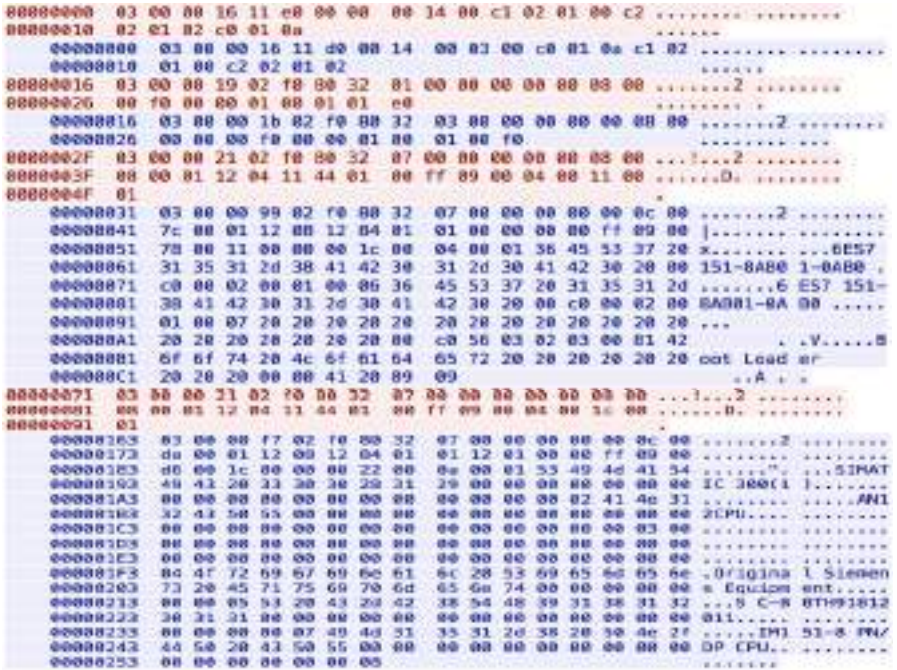
工控设备主动指纹信息

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

通过模拟S7comm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



工控设备被动指纹信息


```
payload = '\x00\x20\x00\x13\x00\x00\x00\x00\x00\x64\x00'
self.send_delay(self.makeframe(payload), sock)
payload = '\x00\x20\x00\x13\x00\x64\x00\x00\x00\x9c\x00'
self.send_delay(self.makeframe(payload), sock)
payload = '\x00\x10\x43\x4c\x00\x00\x0f'
payload += 'USER-SEBUG.NET.'#username will be stored in remote plc
self.send_delay(self.makeframe(payload), sock)
payload = '\x01\x04'
self.send_delay(self.makeframe(payload), sock)
payload = '\x01\x50\x15\x00\x01\x0b'
```

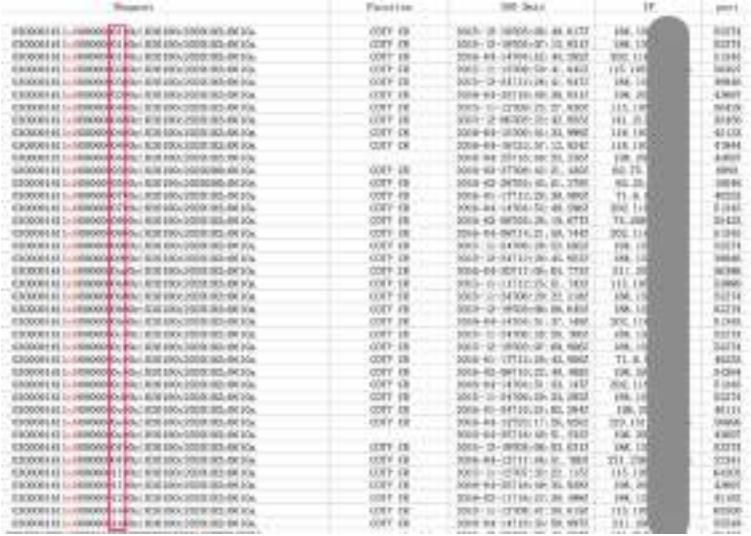
```
Basic options:
  Name     Current Setting                                  Required  Description
  ----     ---------------                                  --------  -----------
  LPATH    /root/.msf5/logs/vxworks_memory.dmp              yes       The local filename to store the dumped memory
  OFFSET   0                                                yes       The starting offset to read the memory dump (hex allowed)
  RHOST                                                     yes       The target address
  RPORT    17185                                            yes       The target port
```

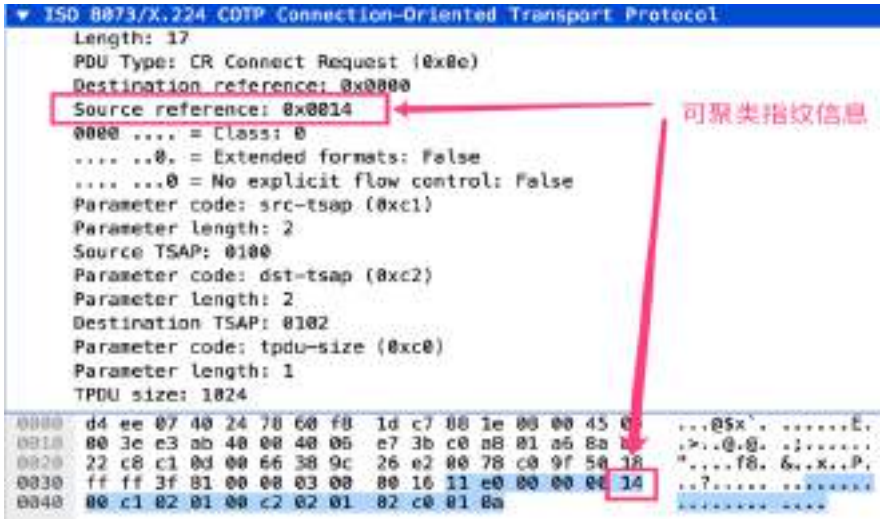
```
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]
^pqrstuvwxyz{|}~
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]
^pqrstuvwxyz{|}~
USER-SEBUG.NET TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
aTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
aTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
aTTTT
 TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
aTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
aTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
```

《揭秘VxWorks—直击物联网安全罩门》

BEACON LAB 灯塔实验室

工控设备被动指纹信息




▼ 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
可聚类指纹信息

工控设备被动指纹信息

通过modbus协议获取设备项目文件信息

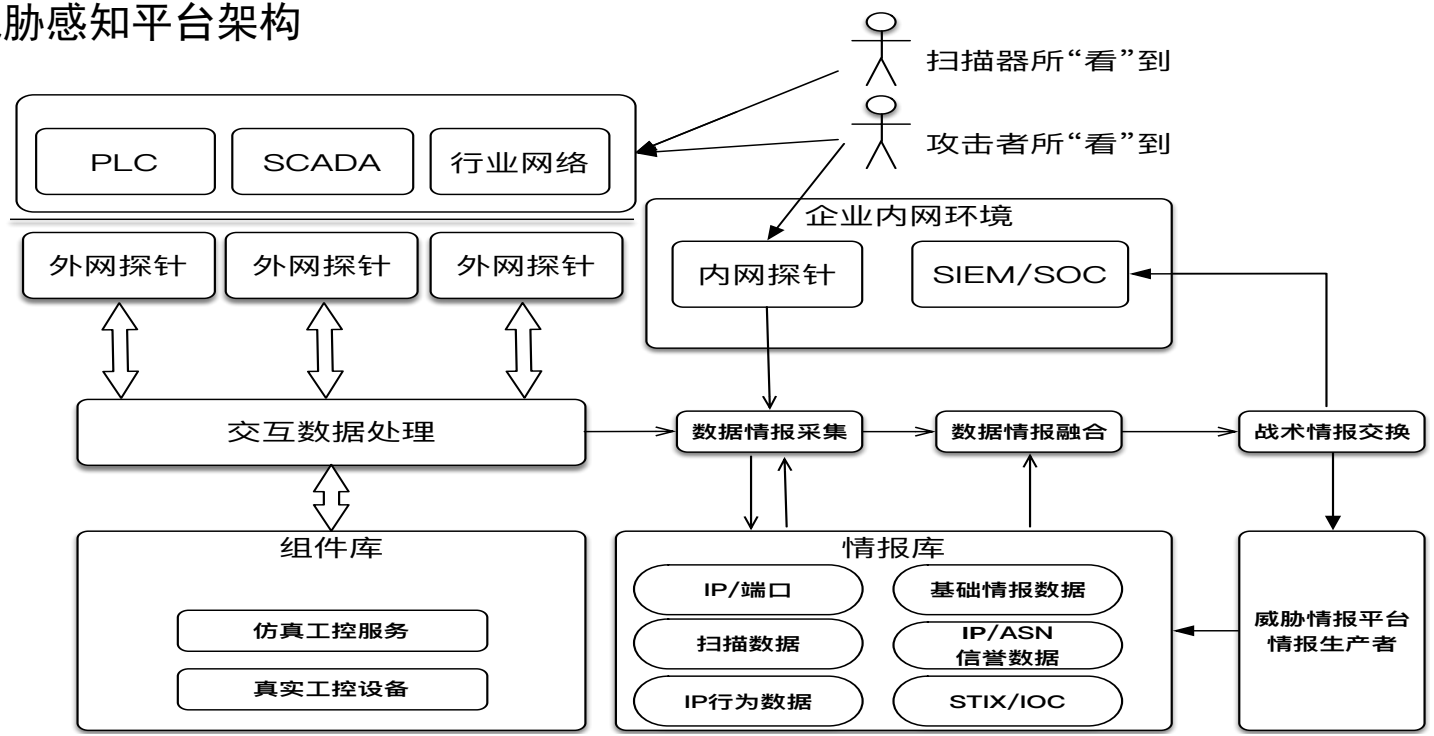
Redpoint nse脚本指纹

debug模式

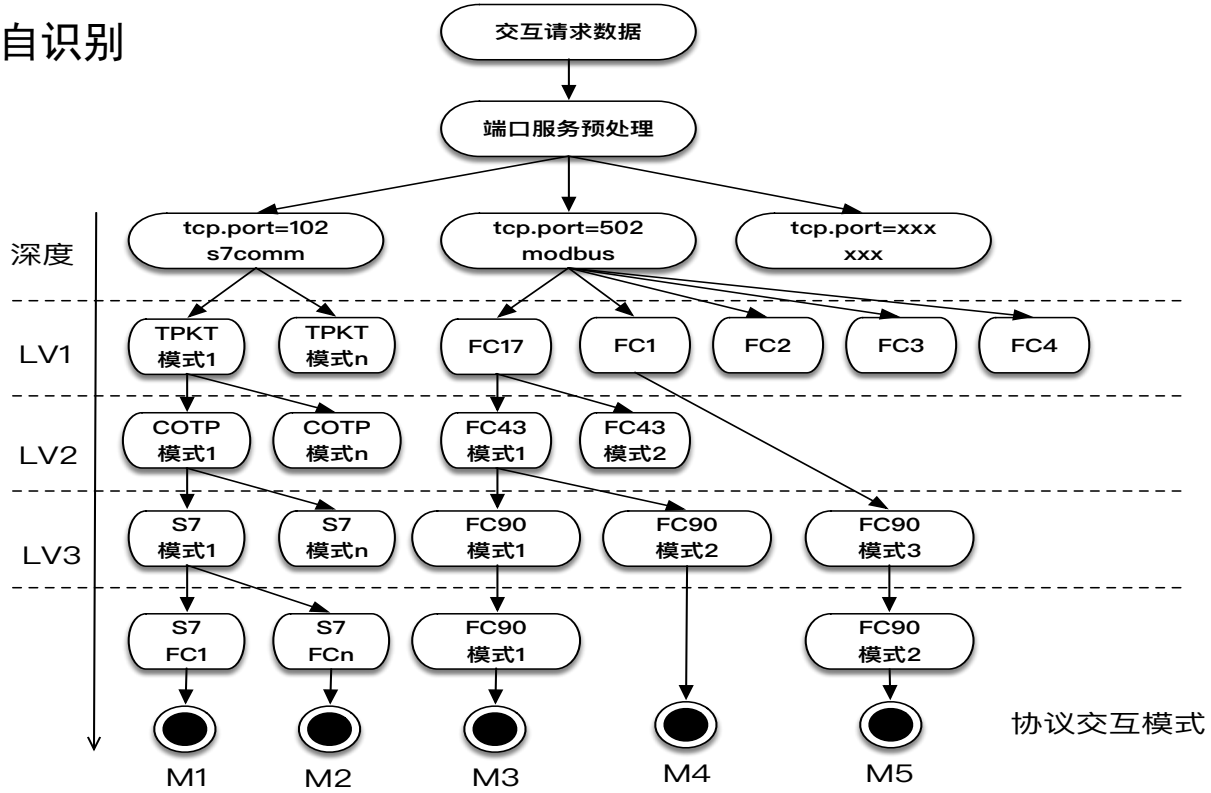
{u'type': u'NEW_CONNECTION'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000b0000000fe005a00fe005454545454545454545454545454545454545454545454545454545454545454545454545454545454545454545454545454545454545454545454',	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00070000000d005a000300', u'response': u'5a00fe7c0b452c8825f3514cbf1b3099875fc9a02c7a6ac8d85b86c6e4ab3825	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00080000000d005a000304', u'response': u'5a00fe0a323b3d74731a99877d816c54e42bf2818051a00e75dc8a994ca7382	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00090000004005a0004', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000a0000000d005a000100', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000b0000000fe005a003a0000010203040506070809a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000c0000004005a0004', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000d0000004005a0004', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000e0000004005a0004', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000f0000000d005a002000130000000006400', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00100000000d005a002000130064000000c00', u'response': u'5a00fe00f6002832866b74df786435d8e1657cb12cf4674	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00110000000d005a002000140000000006400', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00120000000d005a002000140064000000f600', u'response': u'5a00fe00f600d34c46b114eb3076e06d45ce4d70d0abb45	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00130000000d005a002000140064000000f600', u'response': u'5a00fe001000455f323131303352e73747500000000'}	modbus
{u'type': u'CONNECTION_LOST'}	modbus

{u'function_code': 90, u'slave_id': 0, u'request': u'00010000004005a0002', u'response': u'5a00fe50efc4783e829b5547f006039ae9e576b6fa2f1f2a	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'01bf0000000d005a000606', u'response': u'5a00fe011d8f4942fa0b424d58524d5330303384d5000'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'00040000000d005a000300', u'response': u'5a00fede44ef02b8fc62540ee7559f07dd3613668b9ea	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000f0000000d005a002000140064000000f600', u'response': u'5a00fe00f600d6ff4da88b0b8e4393	modbus

被动威胁感知平台架构


扫描器所“看”到
攻击者所“看”到
PLC
SCADA
行业网络
外网探针
外网探针
外网探针
企业内网环境
内网探针
SIEM/SOC
交互数据处理
数据情报采集
数据情报融合
战术情报交换
组件库
仿真工控服务
真实工控设备
情报库
IP/端口
基础情报数据
扫描数据
IP/ASN
信誉数据
IP行为数据
STIX/IOC
威胁情报平台
情报生产者

交互行为模式自识别


交互请求数据
端口服务预处理
深度
tcp.port=102
s7comm
tcp.port=502
modbus
tcp.port=xxx
xxx
LV1
TPKT
模式1
TPKT
模式n
FC17
FC1
FC2
FC3
FC4
LV2
COTP
模式1
COTP
模式n
FC43
模式1
FC43
模式2
LV3
S7
模式1
S7
模式n
FC90
模式1
FC90
模式2
FC90
模式3
S7
FC1
S7
FCn
FC90
模式1
FC90
模式2
M1
M2
M3
M4
M5
协议交互模式

自识别后人工分析

提取常见扫描脚本/工具的交互模式
- Nmap Script（Redpoint）
- Msf module
- Git中的常见针对协议的脚本

提取扫描者、扫描器的行为模式
- Shodan
- Censys
- Rapid7

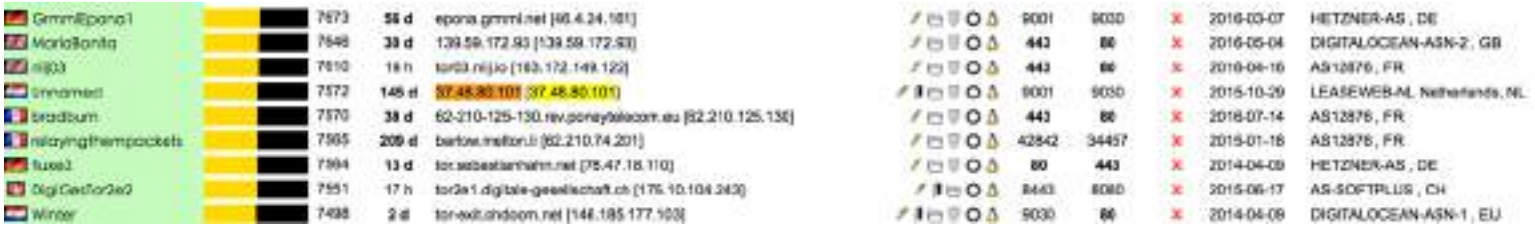
Part. **04**

从威胁数据到威胁情报

真实的捕获案例

#向DB1数据区写入数据
2016-02-10 15:25:44 [209.133.66.214] Write request, Area : DB1, Start : 0, Size : 452 --> OK
2016-02-10 15:25:45 [209.133.66.214] Write request, Area : DB1, Start : 452, Size : 60 --> OK
#向DB1、2、3数据区写入数据
2016-02-22 06:54:19 [93.115.95.202] Write request, Area : DB1, Start : 0, Size : 16 --> OK
2016-02-22 06:54:19 [93.115.95.202] Write request, Area : DB2, Start : 0, Size : 16 --> OK
2016-02-22 06:54:19 [93.115.95.202] Write request, Area : DB3, Start : 0, Size : 16 --> OK
#删除CPU程序块
2016-02-22 06:54:43 [93.115.95.202] CPU Control request : Block Insert or Delete --> OK
#冷启动PLC CPU
2016-02-22 06:58:09 [37.48.80.101] CPU Control request : Warm START --> OK
#停止PLC CPU
2016-02-22 06:58:21 [37.48.80.101] CPU Control request : STOP --> OK
#修改PLC系统时间
2016-02-22 07:03:02 [37.48.80.101] System clock write requested

- 攻击动作
  - 写内存数据
  - 操作CPU状态
  - 修改系统时钟
  - 删除系统程序
- 攻击影响
  - 数据异常
  - 程序停止运行
  - 系统时间异常
  - 系统运行故障



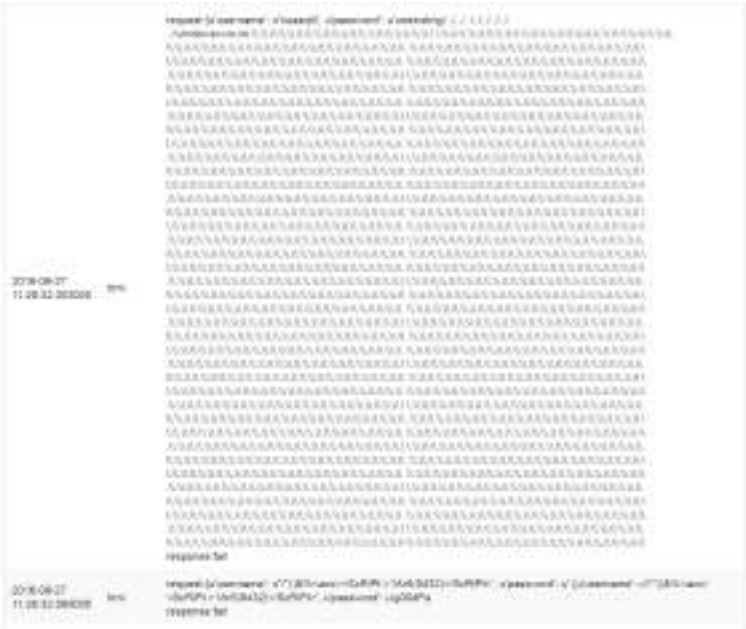
BEACON LAB 灯塔实验室

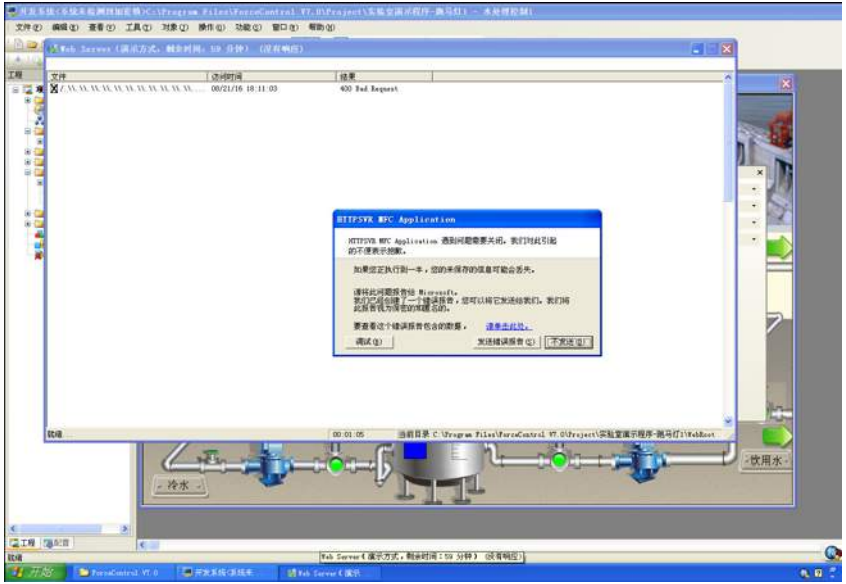
对PLC-Blaster的监测

- S7-300
  - FB65 "TCON"
  - FB63 "TSEND"
  - FB64 "TRCV"
- S7-1200
  - TCON
  - TSEND/TUSEND
  - TRCV/TURCV
- CP
  - FC5 "AG_SEND"
  - FC6 "AG_RECV"

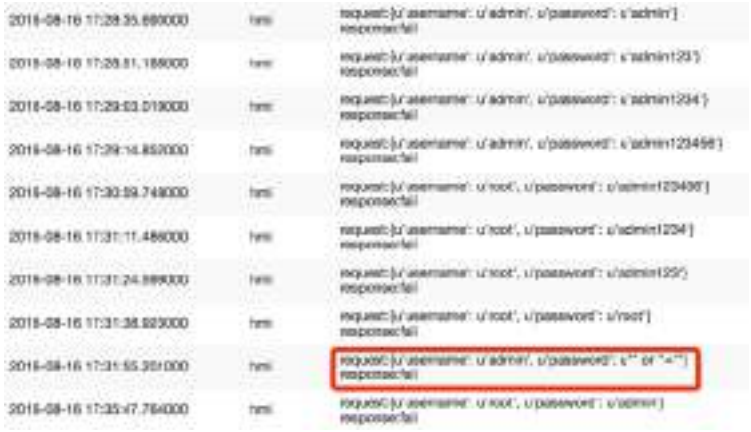
```
Module: 6ES7 314-6EH04-0AB0
Basic Hardware: 6ES7 314-6EH04-0AB0
Version: 3.3.11
System Name: SIMATIC 300(1)
Module Type: CPU 314C-2 PN/DP
Serial Number: S Q-F1U061912015
Copyright: Original Siemens Equipment
Blocks Name: Count(Num)
OB: 1
FB: 0
FC: 13
DB: 5
SDB: 9
SFC: 77
SFB: 23
COMMFC: FC5,FC6
```

针对HMI的溢出攻击





针对HMI的web攻击



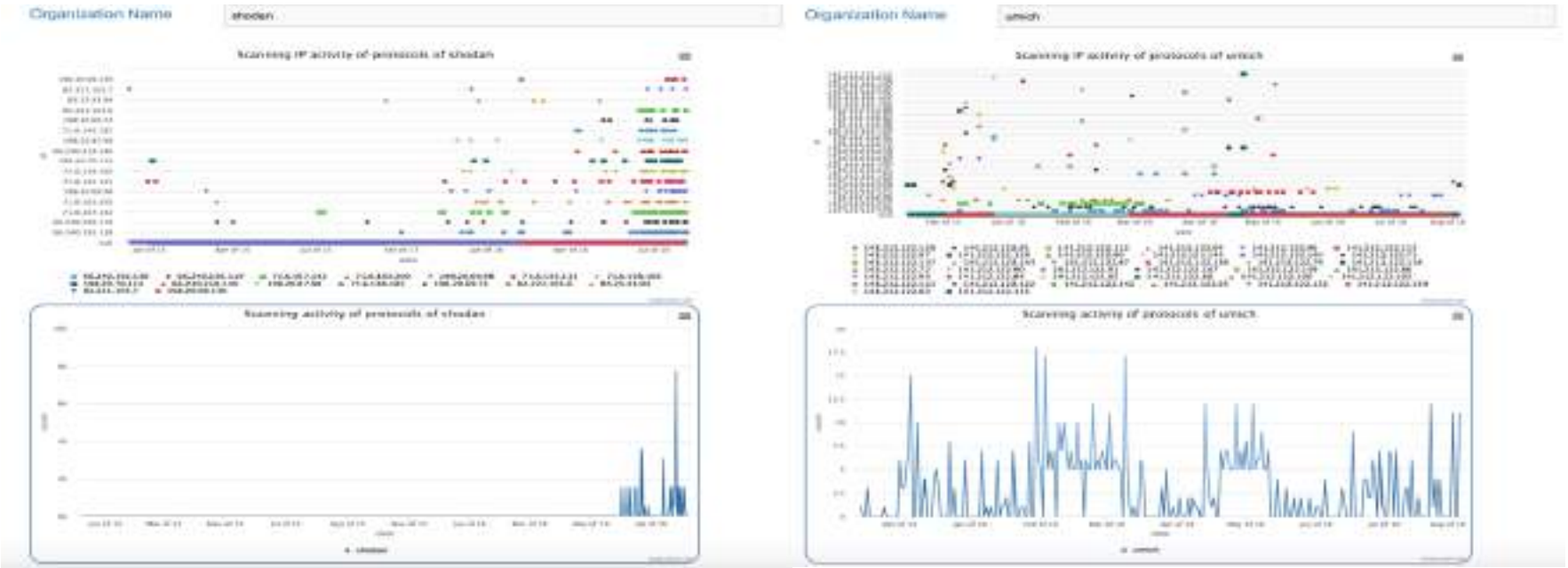
```
{"username":"npqxkatf","password":"\u0026nslookup ujSQ6uCk\u0026'\\\"`0\u0026nslookup ujSQ6uCk\u0026`"}
{"username":"response.write(9738914*9518300)","password":"g00dPa$$w0rD"}
{"username":"ejqrwsuf","password":"-1 OR 2+967-967-1=0+0+0+1"}
{"username":"set|set\u0026set","password":"g00dPa$$w0rD"}
{"username":"f771lDGP","password":"g00dPa$$w0rD"}
{"username":"'+response.write(9738914*9518300)+'","password":"g00dPa$$w0rD"}
{"username":"ejqrwsuf","password":"-1' OR 2+32-32-1=0+0+0+1 -- "}
{"username":"$(nslookup 3XtwkTTb)","password":"g00dPa$$w0rD"}
{"username":"nuasqitl","password":"../../../../../../../../../../etc/passwd"}
{"username":"\"+response.write(9738914*9518300)+\"","password":"g00dPa$$w0rD"}
{"username":"ejqrwsuf","password":"-1' OR 2+395-395-1=0+0+0+1 or 'BSRDFiqp'='"}
{"username":"\u0026nslookup sx2JYYj0\u0026'\\\"`0\u0026nslookup sx2JYYj0\u0026`","password":"g00dPa$$w0rD"}
{"username":"nuasqitl","password":"../../../../../../../../../../../../../../proc/version"}
{"username":"buwamqht","password":"g00dPa$$w0rD"}
{"username":"awetfwqk","password":"${9999175+9999401}"}
{"username":"ejqrwsuf","password":"-1\" OR 2+166-166-1=0+0+0+1 -- "}
{"username":"nuasqitl","password":"..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%00.jpg"}
{"username":"buwamqht","password":""}
{"username":"ejqrwsuf","password":"if(now()=sysdate(),sleep(9.955),0)/*'XOR(if(now()=sysdate(),sleep(9.955),0))OR'\"XOR(i
{"username":"${9999009+10000163}","password":"g00dPa$$w0rD"}
{"username":"nuasqitl","password":"../../../../../../../../../../etc/passwd\u0000.jpg"}
{"username":"buwamqht","password":"12345'\"\\'\\\")"}
{"username":"ejqrwsuf","password":"(select(0)from(select(sleep(9.955)))v)/*'+(select(0)from(select(sleep(9.955)))v)+'\"+(sele
{"username":"eeukssbh","password":"http://some-inexistent-website.acu/some_inexistent_file_with_long_name?.jpg"}
{"username":"nuasqitl","password":"..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%00.jpg"}
{"username":"buwamqht","password":null}
{"username":"ejqrwsuf","password":"1 waitfor delay '0:0:9.955' -- "}
{"username":"eeukssbh","password":"1some_inexistent_file_with_long_name\u0000.jpg"}
{"username":"nuasqitl","password":"/../../../../../../../../../../etc/passwd\u0000.jpg"}
{"username":"buwamqht","password":"g00dPa$$w0rD"}
{"username":"ejqrwsuf","password":"6fG0tJsT'"}
{"username":"eeukssbh","password":"Http://testasp.vulnweb.com/t/fit.txt"}
{"username":"nuasqitl","password":".\\\\/.\\\\/.\\\\/.\\\\/.\\\\/.\\\\/etc/passwd"}
{"username":"","password":"g00dPa$$w0rD"}
{"username":"ejqrwsuf","password":"EOn3dPFf'"}
```

BEACON LAB 灯塔实验室

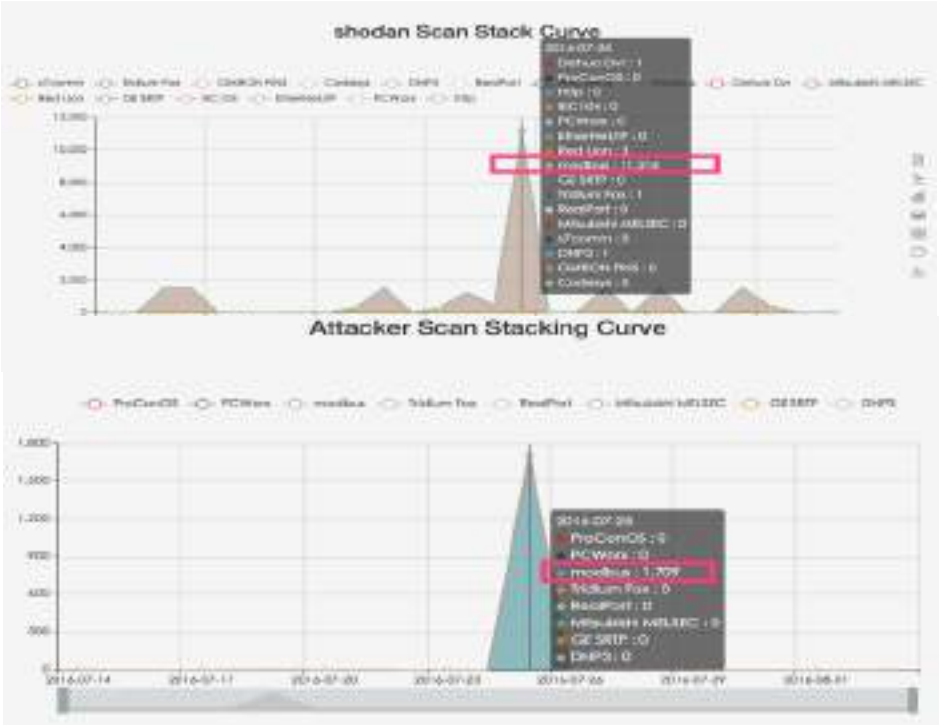
针对HMI的工控业务攻击

{u'REMOTE_USER': u'-', u'HTTP_USER_AGENT': u'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[redacted] Safari/537.36', u'HTTP_REFERER': u'http://[redacted]/index', u'HTTP_VERSION': u'HTTP/1.1', u'bytes': u'1', u'REQUEST_METHOD': u'POST', u'REQUEST_URI': u'/t2/2'}

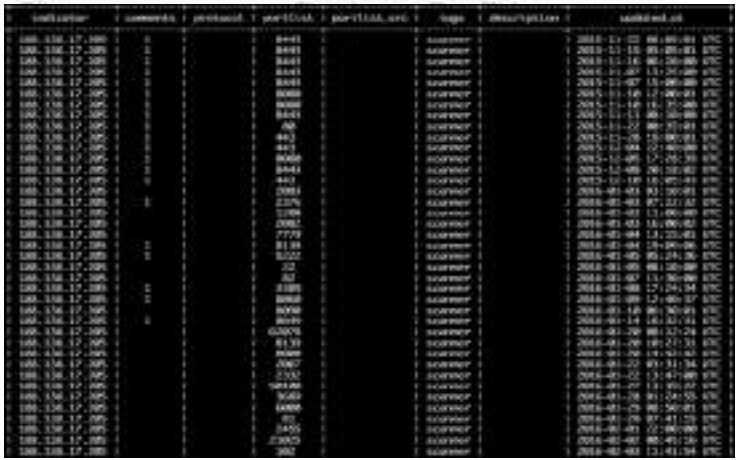
Shodan组织战术威胁情报



Shodan组织战术威胁情报



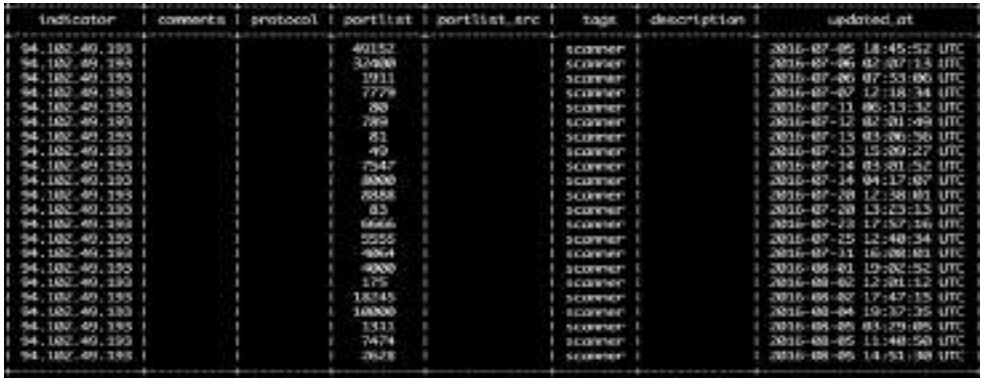
Shodan组织战术威胁情报



BEACON LAB 灯塔实验室

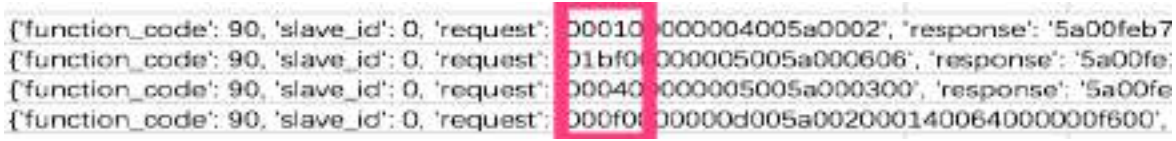
Shodan组织战术威胁情报

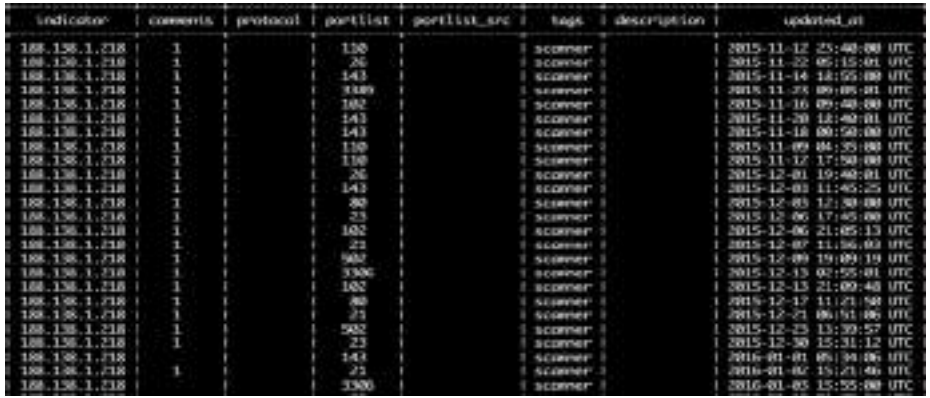
2016-07-23T11:29:13.412Z	["94.102.49.190",43071]		000100000004005a0002	modbus
2016-07-23T11:29:14.413Z	["94.102.49.190",43071]		01bf00000005005a000606	modbus
2016-07-23T11:29:15.415Z	["94.102.49.190",43071]		000400000005005a000300	modbus
2016-07-23T11:29:16.417Z	["94.102.49.190",43071]		000f0000000d005a002000140084000000f	modbus
2016-07-23T11:29:18.419Z	["94.102.49.190",43071]		000000000020111	modbus



BEACON LAB 灯塔实验室

Shodan组织战术威胁情报





BEACON LAB 灯塔实验室

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很高。

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功能码进行的确认探，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同时对社区关注很高，目前已经集成了我们曾经发布的GE SRTP、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。

BEACON LAB 灯塔实验室

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Ethenet/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

BEACON LAB 灯塔实验室


THANK YOU!
ICS Security Workspace
KISA Korea Internet & Security Agency
enisa
ICS-CERT
GovCERT
Swiss Governmental Computer Emergency
ICS Security Workspace
Russian GOV
picscan.org/blog/2016/03/census-scanning-from-siemens-s7-plc-cpustatus/

[灯塔实验室@KCon]

T H A N K S

[灯塔实验室@KCon]