



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]



■ 关于我们 | [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

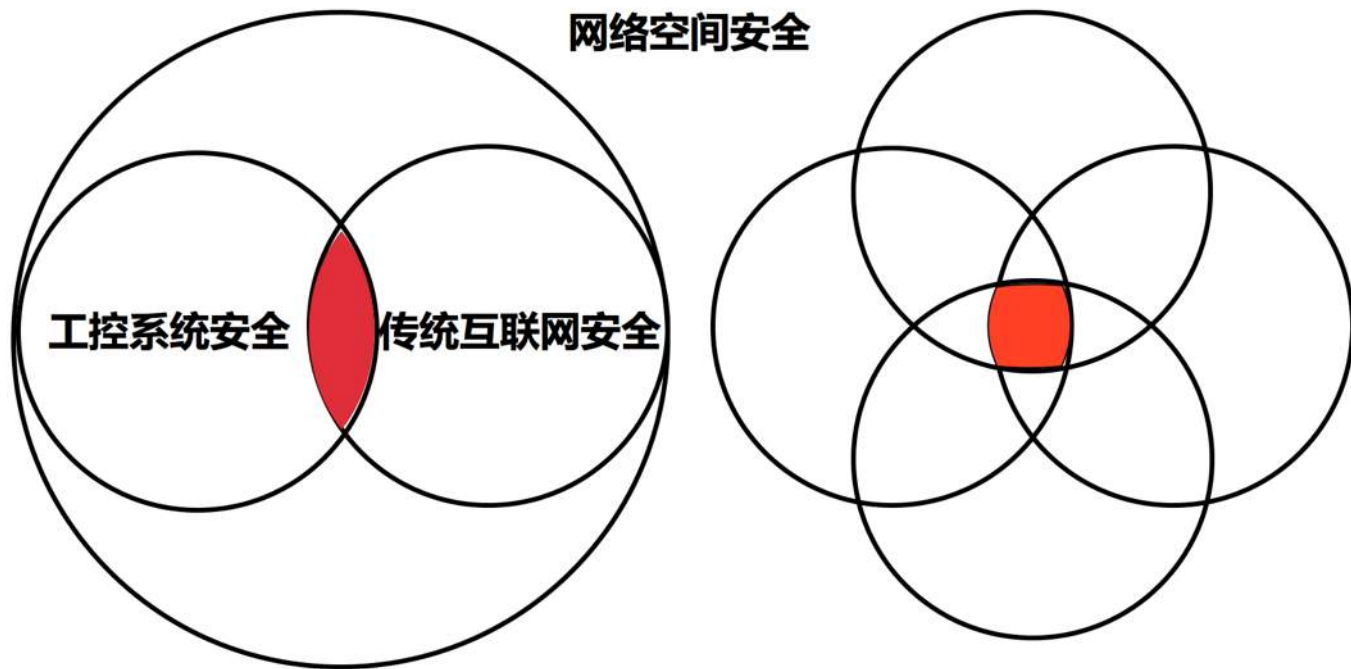
从威胁数据到威胁情报

Part. 01

基础威胁情报 VS. 高级威胁情报



基础威胁情报 VS. 高级威胁情报 | [灯塔实验室@KCon]





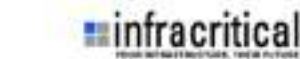
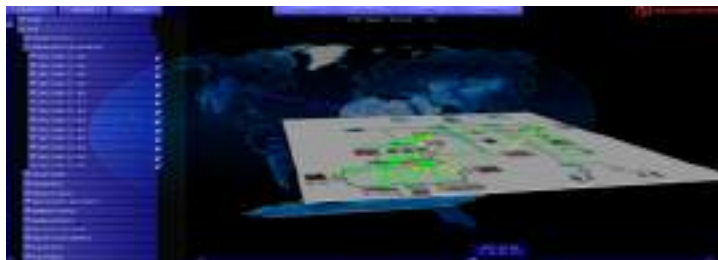
基础威胁情报 VS. 高级威胁情报 | [灯塔实验室@KCon]

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



Project SHINE
(SHodan INtelligence Extraction)

Findings Report

Based on intelligence gathered from the
SHODAN search engine between
14 Apr 2012 through 31 Jan 2014

1 Oct
2014



DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

Defense Advanced Research Projects Agency > Program Information

Plan X

Mr. Frank Pound





基础威胁情报 VS. 高级威胁情报 | [灯塔实验室@KCon]

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





基础威胁情报 VS. 高级威胁情报 | [灯塔实验室@KCon]

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

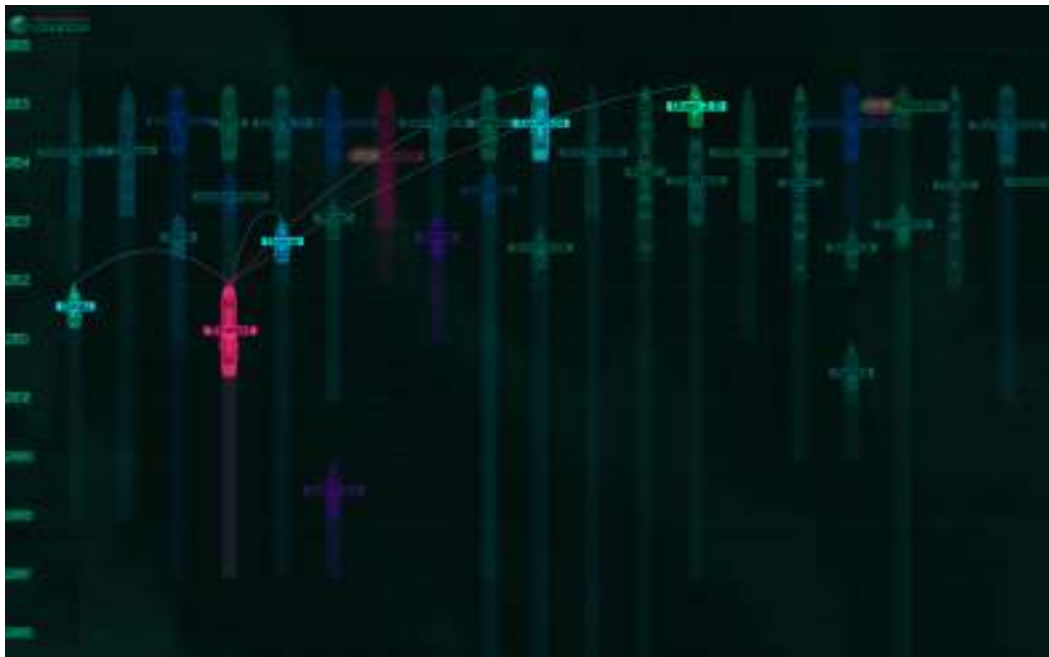
Stuxnet/Duqu/Flame
BlackEnergy

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



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

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/>

Internet connected ICS/SCADA/PLC Cheat Sheet 2013

Gleb Gritsai, Alexander Timorin, Alexander Zaitsev, Sergey Gordoychik, Valentin Shilenkov

www.scadastrangelove.org



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

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: 5 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: BMX RMS008MP
- Project information: Project - V6.0 HP-1
- Project revision: 0.0.197
- 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



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

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	57 1200	HTTP (80)	Location: /Default.mwsl
		SNMP(161)	Siemens, SIMATIC 57, CPU-1200
	57 300	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)	OnUDE(H)CPU FTP server ready.
Moxa	NPort	HTTP (80)	Server: MoxaHttp

Vendor	Product	Protocol	Dork/Banner
Siemens	PCS7	http	57Web.css
Siemens	PCS7	url	Portal0000.htm
Siemens	SIMATIC	url	Portal/Portal.mwsl
Siemens	SIMATIC	url	57Web.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	SLCS	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



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

识别工具列举

插件名称	端口	描述
bacnet-discover.exe	43888	识别和枚举BACnet设备
atg-info.exe	10001	识别诺信自动化设备
codesys-v2-discover.exe	1205	识别和枚举Codesys v2控制器
espvr-info.exe	2222	识别PCS7/PLC 300控制器
esp3-info.exe	20030	识别ESP300设备
emip-enumrate.exe	44810	识别和枚举EtherCAT/OPB设备
fox-info.exe	1911	识别Niagara Fox软件
modbus-info.exe	502	枚举施耐德PLC信息
omroncp-info.exe	9609	识别和枚举欧姆龙PLC信息
omronadp-info.exe	9609	识别和枚举欧姆龙PLC信息
pospro-info.exe	1902	识别和枚举菲尼克斯PLC设备
preconos-info.exe	20547	识别和枚举使用Preconos的控制器
s7-enumerate.exe	102	识别和枚举西门子S7PLC设备
mms-identify.exe	402	识别并枚举支持40685015位的设备信息
modbus-discover.exe	502	识别并枚举Modbus设备信息
cr3-fingerprint.exe	589	识别并枚举红狮控制器信息
mosa-enm.exe	4800	识别并枚举MosaNPort设备信息
melsec-discover.exe	8007	识别并枚举三菱G系列PLC信息
melsec-discover-udp.exe	5006	识别并枚举三菱Q系列PLC信息

Vendor	System / Component	SCADAhacker Reference	Metasploit Reference
7-Technologies	IGSS	IGS-11-080-03 IGSA-11-132-01A	exploit/windows/scada/gss4_ksscalserver_start.rb exploit/windows/scada/gss4_ksscalserver_rename.rb exploit/windows/scada/gss4_msc.rb auxiliary/scada/igss_msc_17.rb
AzeoTech	DAQ Factory	Click Here	exploit/windows/scada/daq_factory_bsf.rb
35	CoDeSys	Click Here	exploit/windows/scada/codsys_web_server.rb
BACnet	OPC Client Operator Workstation	IGSA-10-264-01 n/a	exploit/windows/infrastructure/bacnet_cvr.rb exploit/windows/browser/teechart_pro.rb
Beckhoff	TwinCat	Click Here	auxiliary/scada/beckhoff_twincat.rb
General Electric	D20 PLC	Press Release DigitalBond S4	auxiliary/scada/ge_d20.rb unstable-modules/auxiliary/d20tpcd.rb
Iconics	Genesis32	IGS-11-080-02	exploit/windows/scada/iconics_genbroker.rb
Measureoft	ScadaPro	Click Here	exploit/windows/scada/scadapro_cmdexe.rb
Moxa	Device Manager	IGS-10-283-02 IGSA-10-301-01	exploit/windows/scada/moxa_mdmtop.rb
RealFlex	RealWin SCADA	IGS-11-308-01 IGSA-11-313-01	exploit/windows/scada/realwin_rpc_initialize.rb exploit/windows/scada/realwin_rpc_initialize_if.rb exploit/windows/scada/realwin_rpc_initialize.rb
		IGS-11-080-04 IGSA-11-110-01	exploit/windows/scada/realwin_rpc_initialize.rb exploit/windows/scada/realwin_rpc_initialize_if.rb
ScadaTec	Procyon	Click Here	exploit/windows/scada/procyon_gate_server.rb
ScadaTEC	ModbusTagServer ScadaPhone	Click Here	exploit/windows/infrastructure/scadaphone_zip.rb
Schneider Electric	CitectSCADA CitectFacilities		exploit/windows/scada/citect_scada_ocho.rb
Sinico System	Winlog	IGSA-11-017-02	exploit/windows/scada/winlog_runtime.rb
Siemens Technomatik	FactoryLink	IGS-11-080-01 IGSA-11-081-01	exploit/windows/scada/factorylink_casserver.rb exploit/windows/scada/factorylink_vm_09.rb
Unitronics	OPC Server	n/a	exploit/windows/browser/teechart_pro.rb

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



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

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

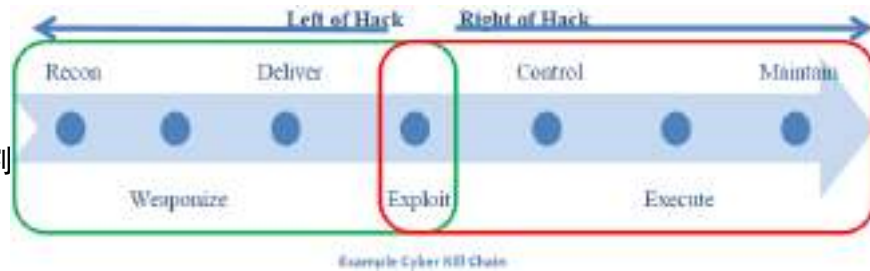
针对工控网络新型渗透模式

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”





信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

威胁捕获方式

传统安全防护设备

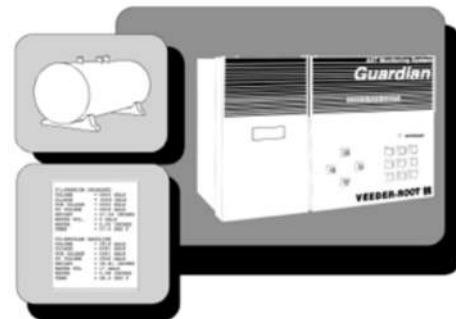
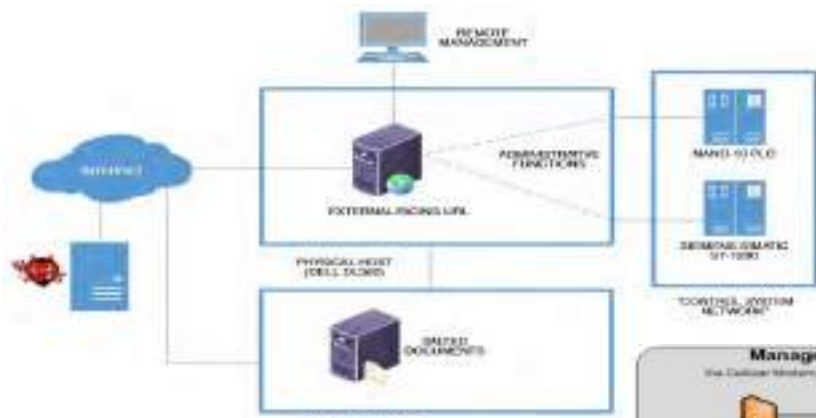
针对工控系统的蜜罐

思科PLC蜜罐

Digitalbond

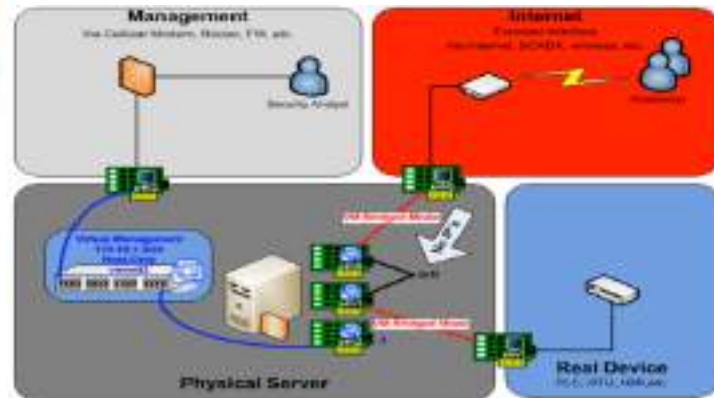
趋势科技

Conpot



SCADA HoneyNet Project: Building Honeypots for Industrial Networks

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





信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

工控蜜罐存在的问题

易被甄别

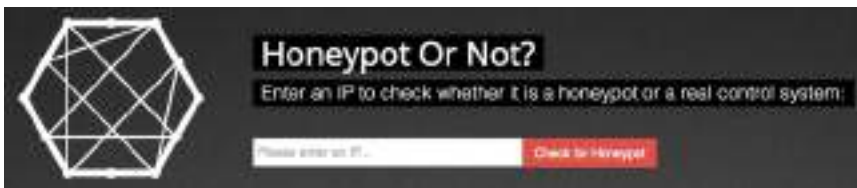
- 针对工控协议的仿真交互低
- 配置繁琐容易留下疏漏
- 缺少针对工控业务的仿真

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@LSI.informatik.rwth-aachen.de



RWTH AACHEN



Breaking Honeypots for Fun and Profit

Dean Sysman
Itamar Sher
Gadi Evron



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

主动监测国外蜜罐部署情况

23.1	7	102 印度 IN	Version: 0.0	System Name: PGJrandom.randint0x	1 f	Module Type: Siemens	SIMATIC	57-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment	
162	6	102 美国 US	Version: 0.0	System Name: PGJrandom.randint0x	1 f	Module Type: Siemens	SIMATIC	57-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment	
170	3	102 法国 FR	Version: 0.0	System Name: PGJrandom.randint0x	1 f	Module Type: Siemens	SIMATIC	57-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment	
160	01	102 美国 US	Version: 0.0	System Name: PGJrandom.randint0x	1 f	Module Type: Siemens	SIMATIC	57-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment	
142		102 美国 US	Version: 0.0	System Name: PGJrandom.randint0x	1 f	Module Type: Siemens	SIMATIC	57-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment	
23.8		102 美国 US	Version: 0.0	System Name: PGJrandom.randint0x	1 f	Module Type: Siemens	SIMATIC	57-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment	
23.8		102 美国 US	Version: 0.0	System Name: PGJrandom.randint0x	1 f	Module Type: Siemens	SIMATIC	57-200	Serial Number: 8675309	Plant Identification: Power Generation One	Copyright: Original Siemens Equipment	
165.1.1	102	瑞士 AUJ	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
162.246	102	北美地区 CA	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
167.99	102	美国 CA	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
47.84.1	102	新加坡城市 DE	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
385.10	102	德国 DE	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
90.149	102	德国 DE	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
46.102	102	俄罗斯 RU	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
104.238	102	美国 China	DE	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment
62.103	102	丹麦 DK	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
165.90	102	芬兰 FI	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
232.73	102	德国 GB	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
278.78	102	德国 GB	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
46.103	102	俄罗斯 GB	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	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		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
185.108	102	欧洲和中部 AS	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
114.142	102	印度 IN	Version: 0.0	System Name: Equip SIMAT		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Metachen Manufactures	Copyright: Original Siemens Equipment	
123.119	102	印度 IN	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
160.10	102	日本东京 JP	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
54.195	102	美国华盛顿州 JP	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
94.189	102	美国华盛顿州 JP	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
146.188	102	俄罗斯 RU	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
160.164	102	新加坡 Digital NL	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
66.610.1	102	波兰波兰 PR	Version: 0.0	System Name: Water Pump		Module Type: Siemens	West-5788	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
66.610.1	102	波兰波兰 PR	Version: 0.0	System Name: Water Pump		Module Type: Siemens	West-5788	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
66.610.1	102	波兰波兰 PR	Version: 0.0	System Name: Water Pump		Module Type: Siemens	West-5788	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
220.155	102	新加坡 Digital SG	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
128.188	102	新加坡 Digital SG	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
84.278	102	斯洛伐克 SK	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
160.107	102	斯洛伐克 SG	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	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		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
398.302	102	加拿大蒙特利尔 US	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	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		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
63.67.9	102	美国华盛顿州 US	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
52.90.2	102	美国华盛顿州 US	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	
186.35	102	波兰波兰 US	Version: 0.0	System Name: Water Pump		Module Type: Siemens	West-5788	Serial Number: 88111222	Plant Identification: AAA	Copyright: Original Siemens Equipment		
62.68.4	102	美国华盛顿州 US	Version: 0.0	System Name: Technodrome		Module Type: Siemens	SIMATIC	57-200	Serial Number: 88111222	Plant Identification: Mouser Factory	Copyright: Original Siemens Equipment	



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

通过Shodan搜索国外蜜罐案例

Shodan API

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

Total results: 4
103.6.87.106

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: PGTranbox.ravolist(0,t) f
Module: v.0.0
Plant identification: Power Generation One
OEM ID of a module:
Module name: Siemens, SIMATIC, 57-200
Serial number of module: 8675309

23.106.59.127

Mobis Technology Group, LLC
Added on 2016-07-21 12:57:12 GMT
United States, Phoenix
[Details](#)

Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: PGTranbox.ravolist(0,t) f
Module: v.0.0
Plant identification: Power Generation One
OEM ID of a module:
Module name: Siemens, SIMATIC, 57-200
Serial number of module: 8675309

162.218.89.26

ColoCrossing
Added on 2016-07-21 04:11:29 GMT
United States, Buffalo
[Details](#)

Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: PGTranbox.ravolist(0,t) f
Module: v.0.0
Plant identification: Power Generation One
OEM ID of a module:
Module name: Siemens, SIMATIC, 57-200
Serial number of module: 8675309

```
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, 57-200  
Serial number of module: 88111222  
  
TIME: 2016-07-29T05:42:17.030523
```



信息收集方式 VS. 威胁诱捕技术 | [灯塔实验室@KCon]

国外工控组合蜜罐案例

102
tcp
27

Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technadrome
Module: v.0.0
Plant identification: Mouser Factory
DEM ID of a module:
Module name: Siemens, SIMATIC, 57-200
Serial number of module: 88111222

8080
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=utf-8
Content-Length: 19949

8090
tcp
http

HTTP/1.1 400 Bad Request
Server: Apache-Coyote/1.1
Transfer-Encoding: chunked
Date: Sat, 30 Jul 2016 12:47:48 GMT
Connection: close



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

```
00000000 03 00 00 16 11 c0 00 00 00 14 00 c1 02 01 00 c2 .....2 .....
00000010 02 01 02 c0 01 0a .....
00000000 03 00 00 16 11 c0 00 14 00 03 00 c0 01 0a c1 02 .....
00000010 01 00 c2 02 01 02 .....
00000016 03 00 00 19 02 f0 00 32 01 00 00 00 00 00 03 00 .....2 .....
00000020 00 f0 00 00 01 00 01 01 c0 .....2 .....
00000016 03 00 00 1b 02 f0 00 32 03 00 00 00 00 00 00 00 .....2 .....
00000020 00 00 00 f0 00 00 01 00 01 00 f0 .....
0000002f 03 00 00 21 02 f0 00 32 07 00 00 00 00 00 03 00 ...2 .....
0000003f 00 00 01 12 04 11 44 01 00 ff 09 00 04 00 11 00 .....0 .....
0000004f 01 .....
00000031 03 00 00 99 02 f0 00 32 07 00 00 00 00 00 0c 00 .....2 .....
00000041 7c 00 01 12 00 12 04 01 01 00 00 00 00 ff 09 00 |.....
00000051 70 00 11 00 00 00 1c 00 04 00 01 36 45 53 37 20 x.....6ES7
00000061 31 35 31 20 38 41 42 30 31 20 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 20 .....6 ES7 151-
00000081 30 41 42 30 31 20 30 41 42 30 20 00 c0 00 02 00 8AB01-0A 00 ....
00000091 01 00 07 20 20 20 20 20 20 20 20 20 20 20 20 20 ... V.....8
000000a1 20 20 20 20 20 20 20 20 c0 56 03 02 03 00 01 42 ... V.....8
000000b1 6f 6f 74 20 4c 6f 61 64 65 72 20 20 20 20 20 20 out Load ar
000000c1 20 20 20 00 00 41 20 09 09 .....A .....
00000071 03 56 00 11 02 f0 00 32 07 00 00 00 00 00 00 00 ...2 .....
00000081 00 00 03 12 04 11 44 01 00 ff 09 00 04 00 11 00 .....0 .....
00000091 01 .....
00000163 03 00 00 ff 02 f0 00 32 07 00 00 00 00 00 0c 00 .....2 .....
00000173 da 00 01 12 00 12 04 01 01 12 01 00 00 ff 09 00 .....
00000183 d0 00 1c 00 00 00 22 00 0a 00 01 55 49 4d 41 54 .....SIMAT
00000193 40 41 20 31 30 30 20 31 20 00 00 00 00 00 00 00 IC 300(1) I...
000001a3 00 00 00 00 00 00 00 00 00 00 00 00 02 41 40 31 .....AN1
000001b3 32 41 50 53 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 00 00 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 6e 65 6e 0f30100 1 Siemens
00000203 73 20 45 71 75 69 70 6d 65 6e 74 00 00 00 00 00 00 a Equipm ent....
00000213 00 00 05 53 20 43 20 42 38 54 40 39 31 38 31 32 ...8 C-W 071091812
00000223 30 31 31 00 00 00 00 00 00 00 00 00 00 00 00 00 01.....
00000233 00 00 00 00 07 49 40 31 35 31 20 38 20 30 4c 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 00 05 .....
```

工控设备被动指纹信息

品牌型号：SSW-80430	CV543：补充 ✓
品牌/系列型号：其他	GV543：补充 ✓
提交时间: 2019-08-19	GV543：补充 ✓
品牌型号：-----	品牌/系列：未知
品牌/系列：西门	提交者：你这是自寻死路~
品牌/系列：补充 ✓	
品牌/系列：Schneider	

```
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\xff'
payload += 'USER-SEBUG.NET.*#username will be stored in'
self.send_delay(self.makeframe(payload), sock)
payload = '\x01\x04'
self.send_delay(self.makeframe(payload), sock)
payload = '\x01\x50\x15\x00\xe1\x0b'
```

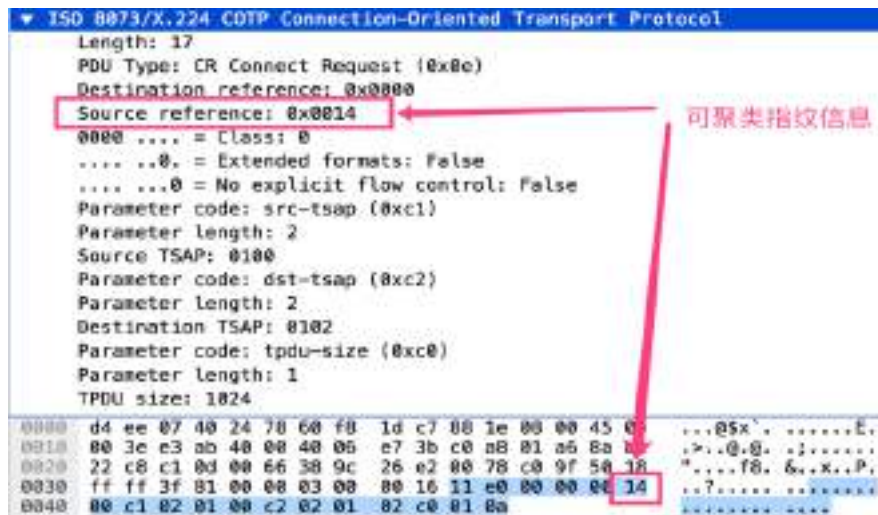
Name	Current Setting	Required	Description
LOCAL	/root/.ssh/known_hosts	yes	The local filename to store the dumped memory
OFFSET		yes	The starting offset to read the memory dump (hex allowed)
HOST		yes	The target address
PORT	11111	yes	The target port

```
! "%$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNPQRSTUVWXYZ[\]  
#pqrstuvwxy{|}~  
! "%$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNPQRSTUVWXYZ[\]  
#pqrstuvwxy{|}~  
USER-DEBUG.WE  
TTTT
```

《揭秘VxWorks一直击物联网安全罩门》



工控设备被动指纹信息

[illegible]

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

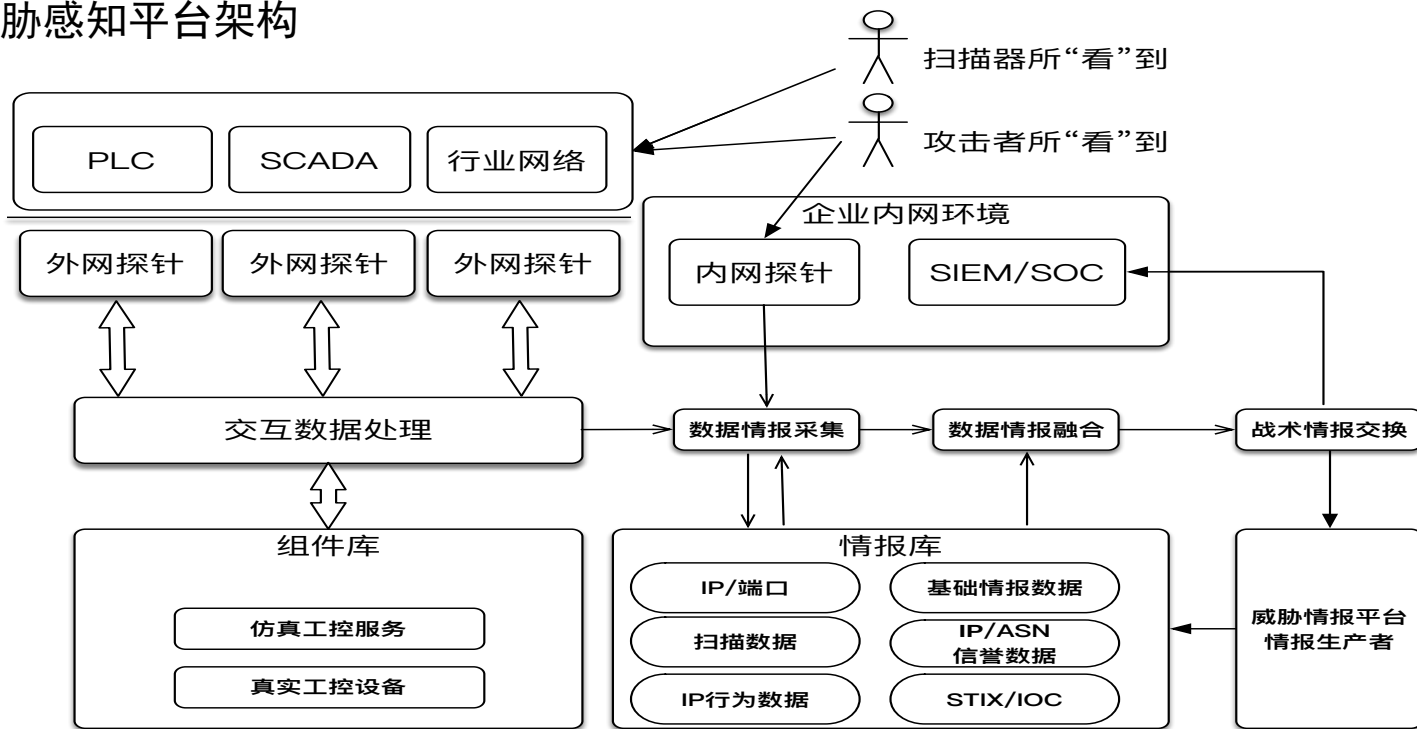
debug模式

[illegible]

```
{
  "function_code": 90,
  "slave_id": 0,
  "request": "00010000004005a0002",
  "response": "5a00fe50efc4783e829b5547f006039ae9e576b6fa2f1f2af modbus"
},
{
  "function_code": 90,
  "slave_id": 0,
  "request": "01bf00000005005a000606",
  "response": "5a00fe011d8f4942fa0b424d58524d533030384d5000 modbus"
},
{
  "function_code": 90,
  "slave_id": 0,
  "request": "000400000005005a000300",
  "response": "5a00fede44ef02b8fc62540ee7559f07dd3613668b9ea modbus"
},
{
  "function_code": 90,
  "slave_id": 0,
  "request": "000f0000000d005a002000140064000000f600",
  "response": "5a00fe00f600d6ff4da88b0b8e4393 modbus"
}
```

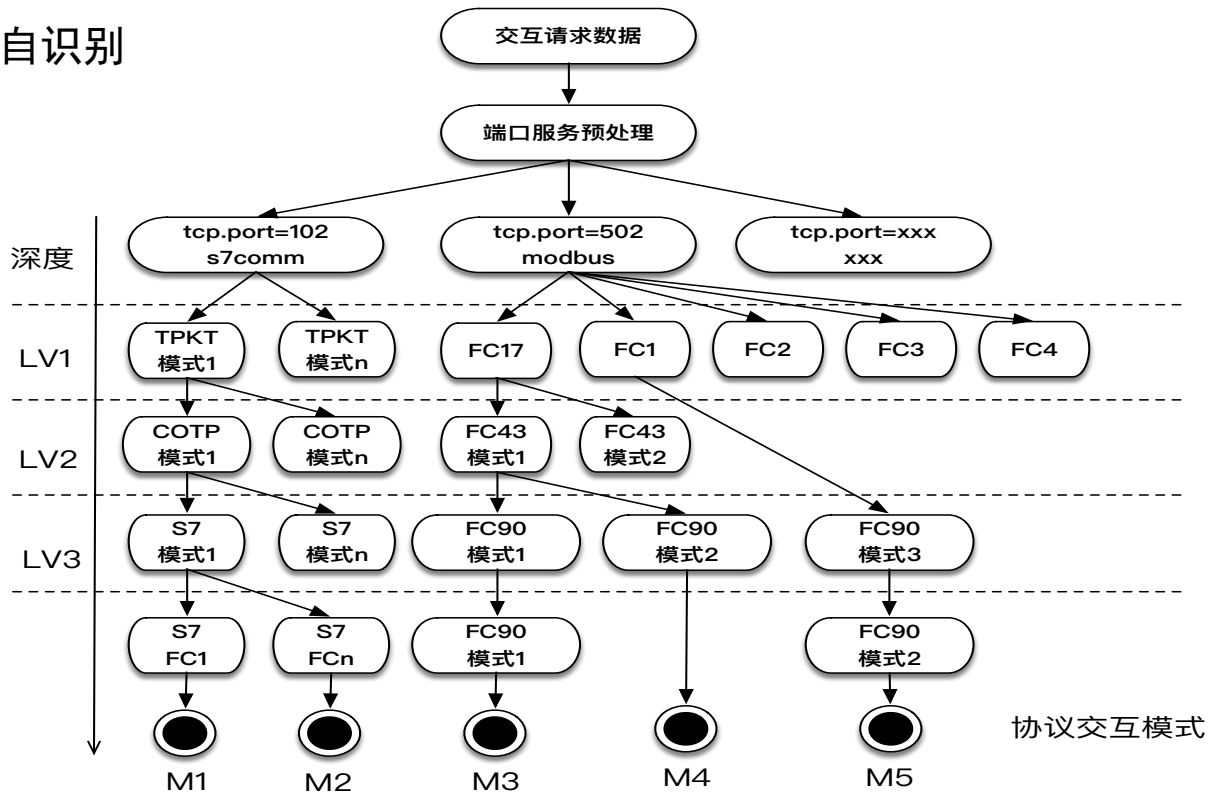


被动威胁感知平台架构





交互行为模式自识别



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

[illegible]

Part. 04

从威胁数据到威胁情报



从威胁数据到威胁情报 | [灯塔实验室@KCon]

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

	7673	55 d	epona.gmmi.net [68.4.24.181]
	7648	33 d	139.59.172.93 [139.59.172.93]
	7610	16 h	tor03.nijao [163.172.149.122]
	7572	146 d	37.48.80.101 [37.48.80.101]
	7570	38 d	62.210.125-130.rev.ponytelecom.eu [62.210.125.135]
	7505	209 d	barton.mellon.li [62.210.74.201]
	7504	13 d	tor.sebastianhahn.net [75.47.16.110]
	7551	17 h	tor2e1.digital-e-gesellschaft.ch [175.10.104.2620]
	7498	2 d	tor-exit.shodan.net [146.185.177.103]

	9001	9000	X	2016-03-07	HETZNER-AS, DE
	443	86	X	2016-05-04	DIGITALOCEAN-ASN-2, GB
	443	86	X	2016-04-16	AS12876, FR
	9001	9030	X	2015-10-29	LEASEWEB-NL, Netherlands, NL
	443	86	X	2016-07-14	AS12876, FR
	42842	34457	X	2015-01-16	AS12876, FR
	80	443	X	2014-04-09	HETZNER-AS, DE
	8463	8080	X	2015-06-17	AS-SOFTPLUS, CH
	9030	86	X	2014-04-09	DIGITALOCEAN-ASN-1, EU





对PLC-Blaster的监测

S7-300

FB65 "TCON"
FB63 "TSEND"
FB64 "TRCV"

S7-1200

TCON
TSEND/TUSEND
TRCV/TURCV

CP

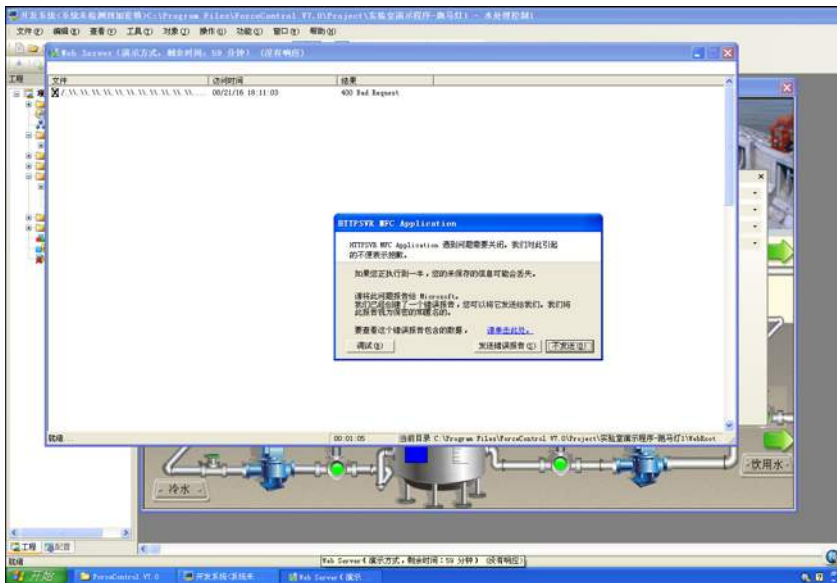
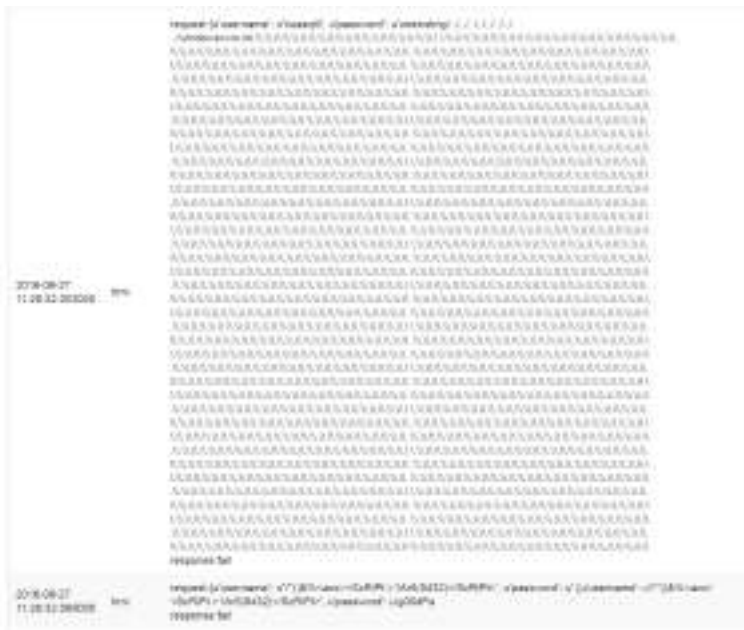
FC5 "AG_SEND"
FC6 "AG_RECV"

```
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
```



从威胁数据到威胁情报 | [灯塔实验室@KCon]

针对HMI的溢出攻击





针对HMI的web攻击

[illegible]



针对HMI的工控业务攻击

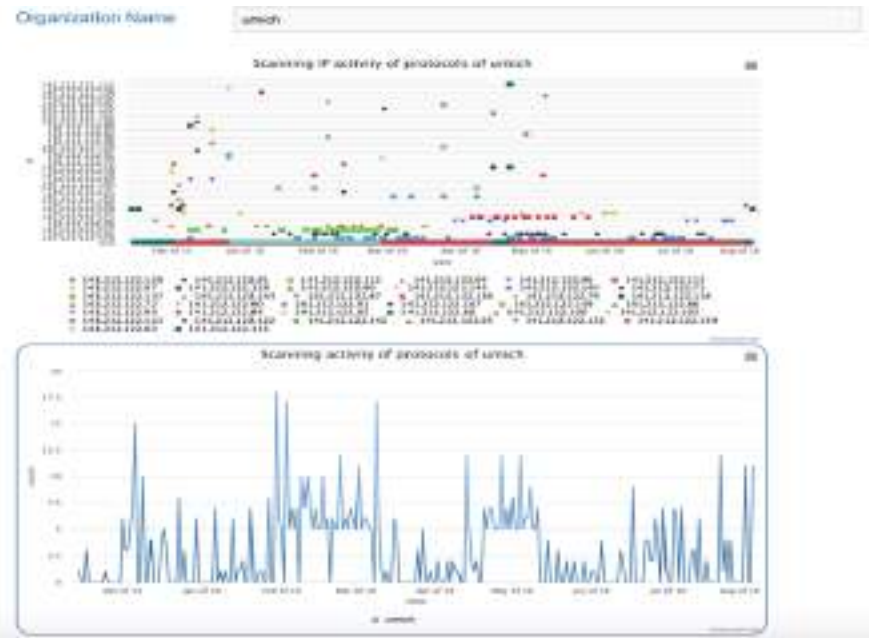
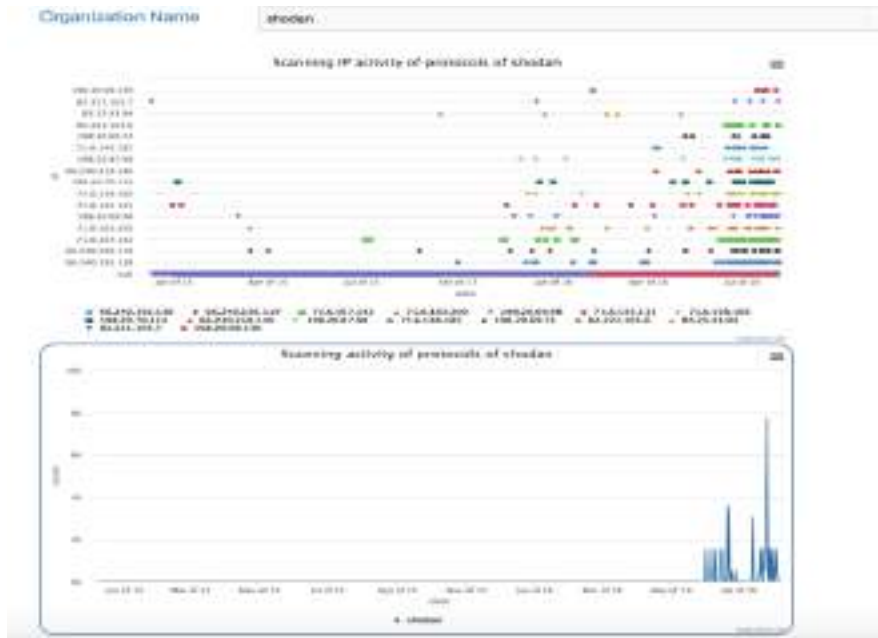


```
{u'REMOTE_USER': u'-' , u'HTTP_USER_AGENT': u'Mozilla/5.0 (Macintosh; Intel  
Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/52.0.2730.103 Safari/537.36', u'HTTP_REFERER':  
u'http://[REDACTED]/index', u'HTTP_VERSION': u'HTTP/1.1', u'bytes': u'1',  
u'REQUEST_METHOD': u'POST', u'REQUEST_URI': u'/t2/2'}
```



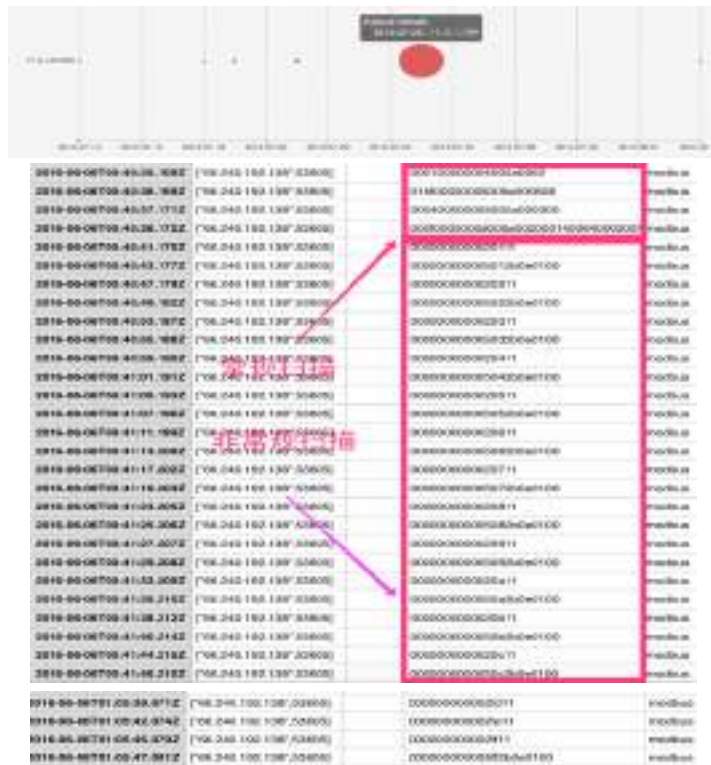
从威胁数据到威胁情报 | [灯塔实验室@KCon]

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

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

[illegible]

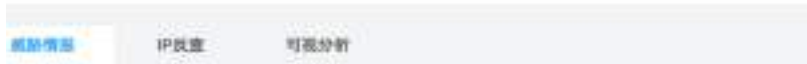
2016-07-19T16:20:31.529Z	[188.138.17.205,46332]	00010000000000000000	modbus
2016-07-19T16:20:32.630Z	[188.138.17.205,46332]	01000000000000000000	modbus
2016-07-19T16:20:33.633Z	[188.138.17.205,46332]	00040000000000000000	modbus
2016-07-19T16:20:34.535Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:37.538Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:38.538Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:43.542Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:45.545Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:48.549Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:51.552Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:55.557Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:20:57.560Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:01.562Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:03.564Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:07.567Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:09.569Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:13.573Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:15.576Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:19.580Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:21.586Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:23.587Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:27.589Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:31.593Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:33.596Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:37.599Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:39.601Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:43.604Z	[188.138.17.205,46332]	00000000000000000000	modbus
2016-07-19T16:21:45.606Z	[188.138.17.205,46332]	00000000000000000000	modbus





从威胁数据到威胁情报 | [灯塔实验室@KCon]

Shodan组织战术威胁情报



威胁情报摘要		
情报源	发现时间	情报类型
开源情报	2016-07-19	扫描
开源情报	2016-07-16	漏洞利用
开源情报	2016-07-16	漏洞利用, 恶意软件
开源情报	2016-07-06	恶意软件
开源情报	2016-07-07	僵尸网络
开源情报	2016-07-06	可疑
ThreatStack Labs	2016-07-06	垃圾邮件
ThreatStack Labs	2016-07-06	僵尸网络
ThreatStack Labs	2016-07-06	垃圾邮件, 僵尸网络

2016-07-23T11:29:13.412Z	["94.102.49.192",43071]	030100000004005a0002	modbus
2016-07-23T11:29:14.413Z	["94.102.49.192",43071]	01b00000005095a000606	modbus
2016-07-23T11:29:15.415Z	["94.102.49.192",43071]	090400000005005a000300	modbus
2016-07-23T11:29:16.417Z	["94.102.49.192",43071]	030100000000005a0002000140084000000	modbus
2016-07-23T11:29:18.419Z	["94.102.49.192",43071]	03000000000020111	modbus

indicator	comments	protocol	portlist	portlist_src	tags	description	updated_at
94.102.49.192			40152		scanner		2016-07-05 18:45:52 UTC
94.102.49.192			32900		scanner		2016-07-06 02:07:13 UTC
94.102.49.192			1911		scanner		2016-07-06 07:53:06 UTC
94.102.49.192			7779		scanner		2016-07-07 12:18:34 UTC
94.102.49.192			80		scanner		2016-07-11 05:13:32 UTC
94.102.49.192			289		scanner		2016-07-12 02:31:49 UTC
94.102.49.192			81		scanner		2016-07-13 03:36:36 UTC
94.102.49.192			49		scanner		2016-07-13 15:30:27 UTC
94.102.49.192			7547		scanner		2016-07-14 03:01:52 UTC
94.102.49.192			8000		scanner		2016-07-14 04:17:07 UTC
94.102.49.192			8888		scanner		2016-07-20 12:38:01 UTC
94.102.49.192			83		scanner		2016-07-20 13:23:13 UTC
94.102.49.192			6666		scanner		2016-07-20 17:57:16 UTC
94.102.49.192			2255		scanner		2016-07-25 12:40:34 UTC
94.102.49.192			4864		scanner		2016-07-31 16:08:03 UTC
94.102.49.192			4000		scanner		2016-08-01 19:02:52 UTC
94.102.49.192			175		scanner		2016-08-02 12:01:12 UTC
94.102.49.192			13145		scanner		2016-08-02 17:47:15 UTC
94.102.49.192			10000		scanner		2016-08-04 19:37:32 UTC
94.102.49.192			1311		scanner		2016-08-05 03:29:05 UTC
94.102.49.192			7474		scanner		2016-08-05 13:40:50 UTC
94.102.49.192			2678		scanner		2016-08-06 14:51:30 UTC



从威胁数据到威胁情报 | [灯塔实验室@KCon]

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

```
{'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': '00040000005005a000300', 'response': '5a00fe'}
{'function_code': 90, 'slave_id': 0, 'request': '000f000000d005a002000140064000000f600', 'response': '5a00fe'}
```



Z-One @plcsec · 6月1日

188.138.1.218 is Shodan scanning node? @achillean

查看翻译

ThreatBook Labs	2010-06-01	僵尸网络
开源情报	2010-06-20	僵尸网络
开源情报	2010-06-17	扫描
ThreatBook Labs	2010-06-17	僵尸网络
开源情报	2010-06-18	扫描
ThreatBook Labs	2010-06-12	僵尸网络
开源情报	2010-05-20	扫描
开源情报	2010-05-20	僵尸网络
ThreatBook Labs	2010-06-14	僵尸网络, 僵尸网络
开源情报	2010-06-20	僵尸网络, 僵尸网络
开源情报	2010-12-12	僵尸网络, 扫描
开源情报	2010-12-10	扫描
开源情报	2010-12-04	扫描
开源情报	2010-10-02	扫描
开源情报	2010-11-09	僵尸网络
开源情报	2010-11-05	扫描

indicator	comments	protocol	portlist	portlist_src	tags	description	updated_at
188.138.1.218	1		138		scanner		2015-11-12 25:40:00 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 14:55:00 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 12:40:01 UTC
188.138.1.218	1		143		scanner		2015-11-18 00:50:00 UTC
188.138.1.218	1		138		scanner		2015-11-09 04:35:00 UTC
188.138.1.218	1		138		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		23		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		3389		scanner		2015-12-13 02:55:01 UTC
188.138.1.218	1		102		scanner		2015-12-13 21:09:40 UTC
188.138.1.218	1		80		scanner		2015-12-17 11:21:50 UTC
188.138.1.218	1		23		scanner		2015-12-21 00:15:00 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 06:34:06 UTC
188.138.1.218	1		23		scanner		2016-01-02 15:21:46 UTC
188.138.1.218	1		3389		scanner		2016-01-05 15:55:00 UTC



从威胁数据到威胁情报 | [灯塔实验室@KCon]

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

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，避免设备端口接收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信息进行综合评判，通过产生量化的系数来进行蜜罐甄别。

<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行为分析报告》



从威胁数据到威胁情报 | [灯塔实验室@KCon]

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



[灯塔实验室@KCon]



T H A N K S

[灯塔实验室@KCon]