



黑客眼中的工控4.0

——工控系统安全威胁与应对探索
by Kimon

关于我

- 中国科技大学苏研院
- ADF安全研究团队
- 物联网安全、工控安全



王启蒙 Kimon

qmwang@vip.126.com

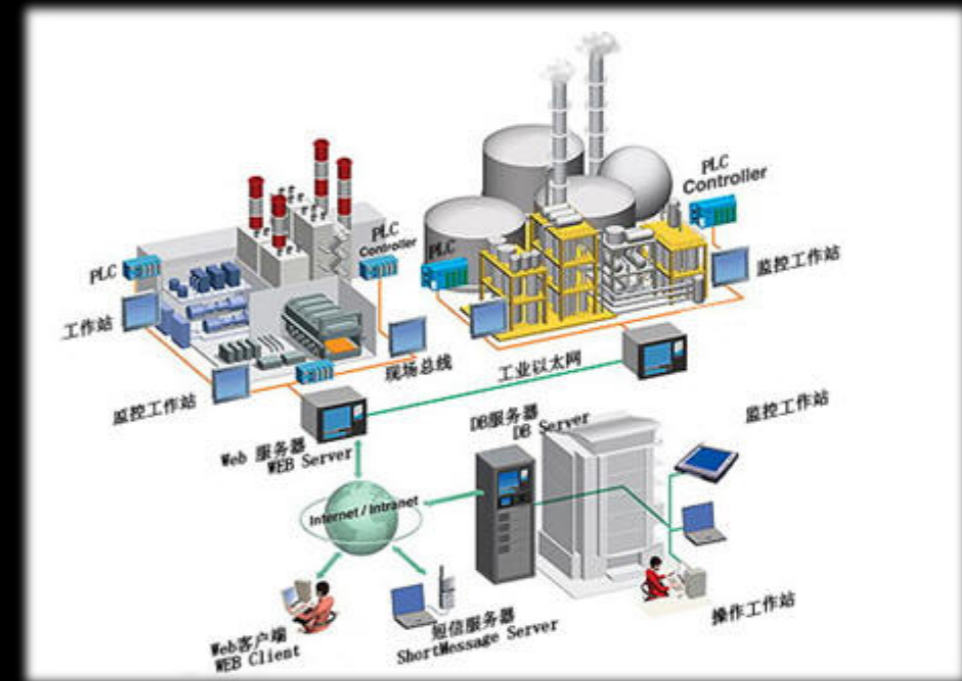
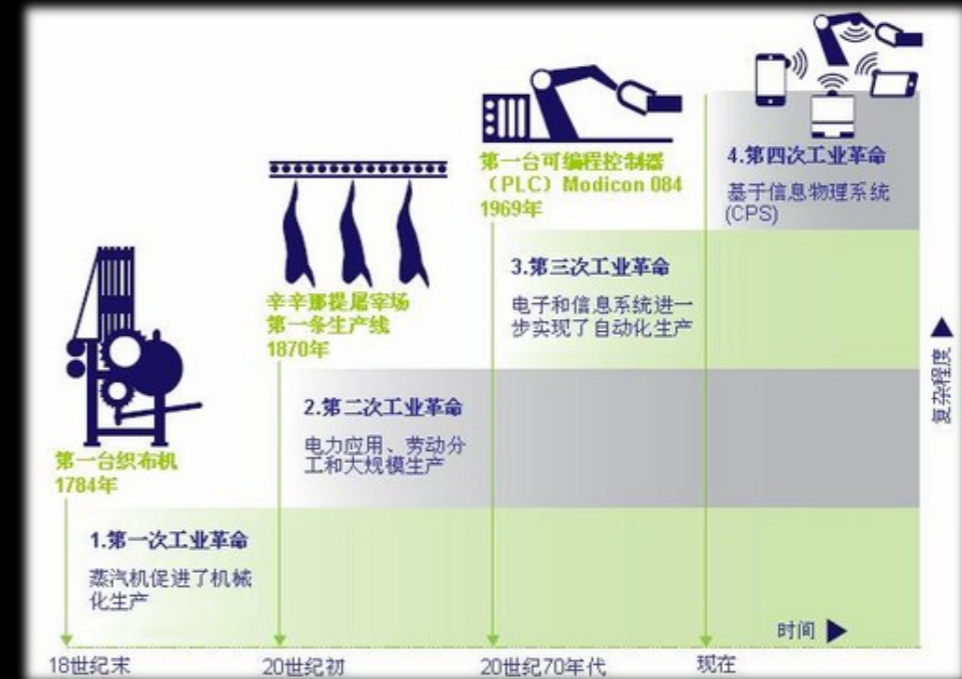
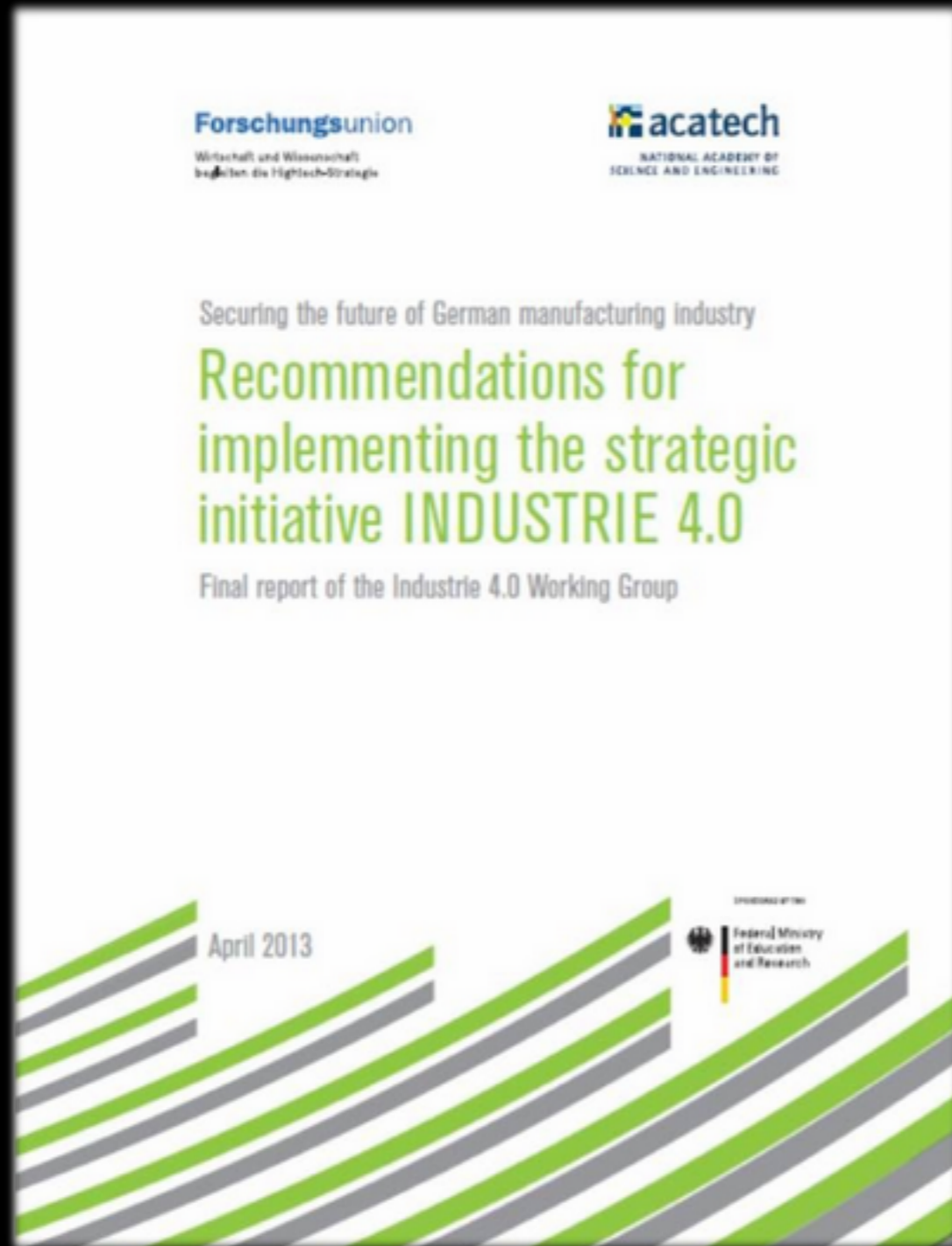
13758178689

提纲

- 工控背景
- 工控系统
- 入侵方式
- 应对探索



工业4.0与两化融合



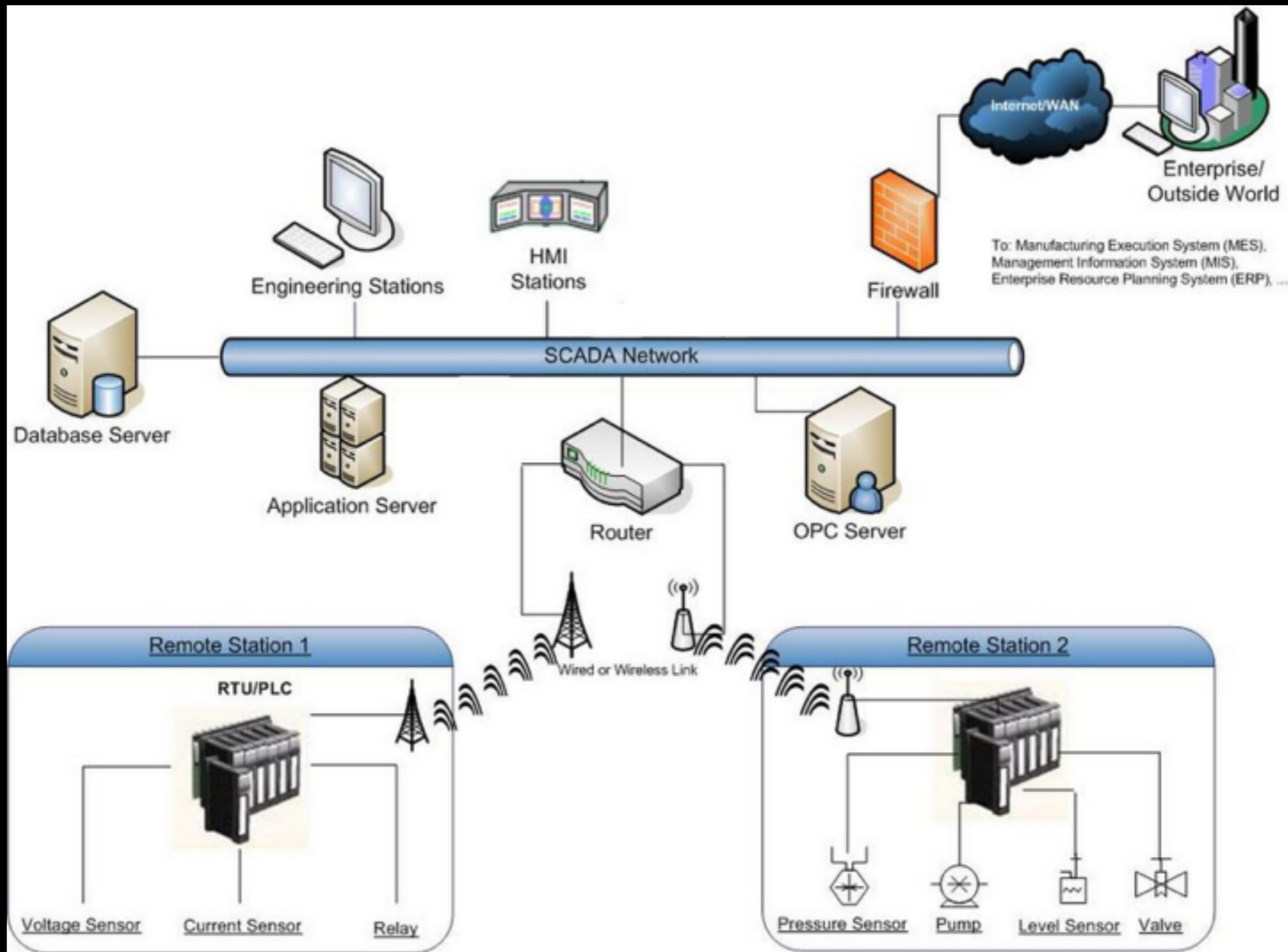


工控系统

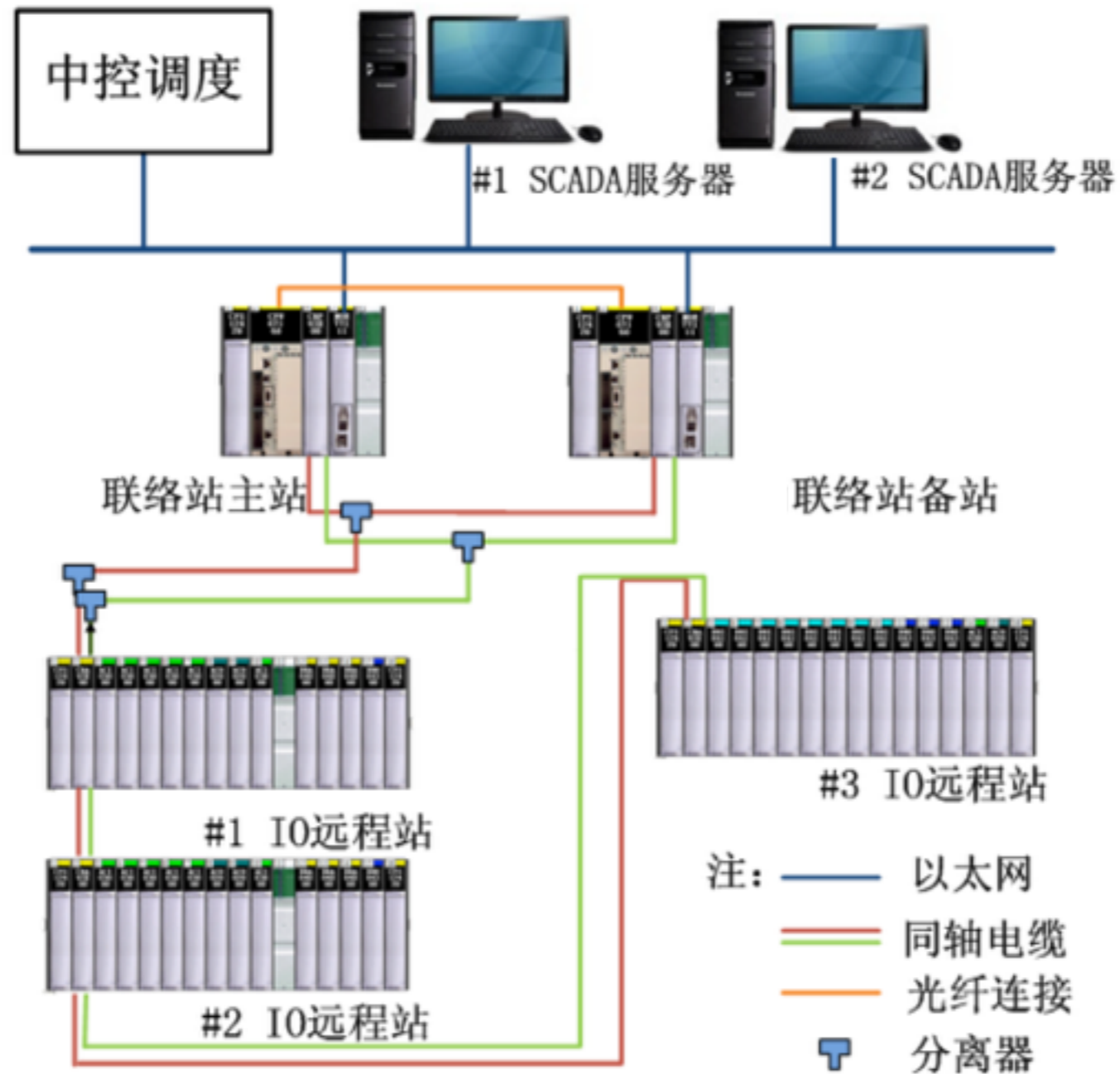
- ICS 工业控制系统
- SCADA 数据采集与监控系统
- DCS 分散式控制系统



SCADA系统



SCADA系统



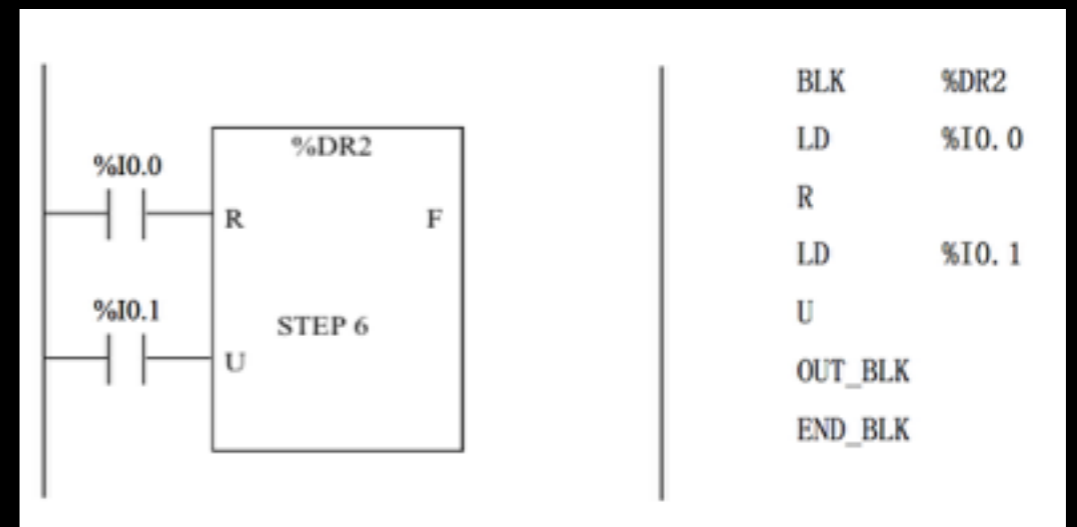
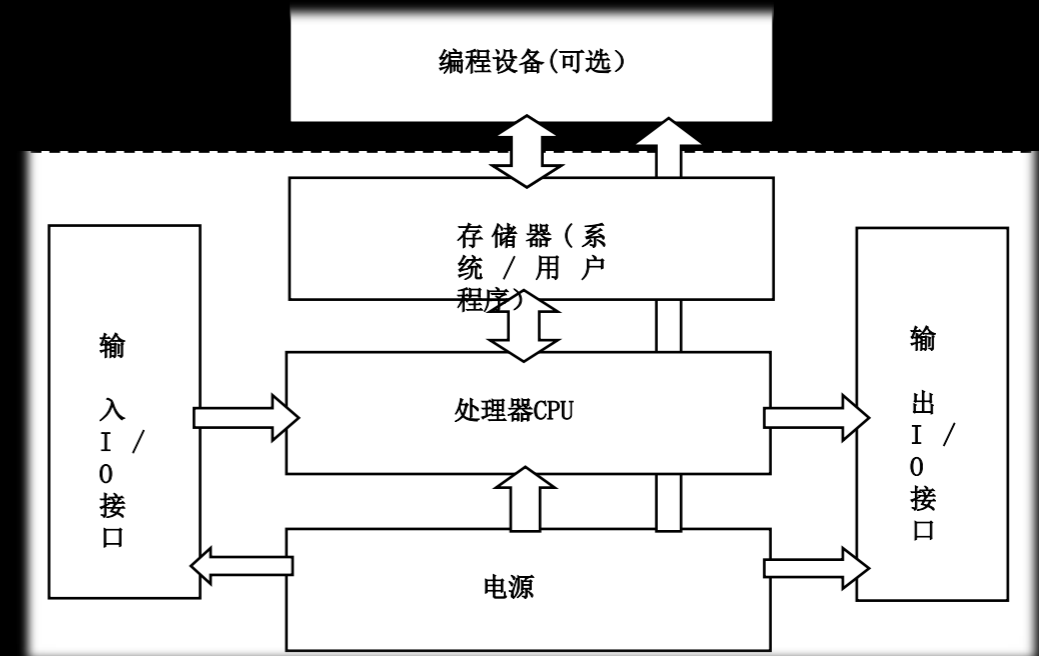
工控组件

- PLC可编程逻辑控制器
- RTU远程控制单元
- HMI人机交互界面
- 现场设备



PLC

- PLC实质是一种用于工业的计算机
- CPU、存储器、输入输出接口电路、功能模块、通信模块、电源
- 输入采样阶段、用户程序执行阶段、数据刷新阶段
- 梯形图LAD
顺序流程图SFC
指令表IL

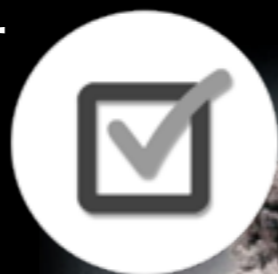


威胁趋势



威胁来源

协议安全



网络隔离



安全意识



漏洞管理



工业网络协议

- Modbus
- S3/S5/S7
- DNP3
- Profinet
- Ethernet/IP
- ...



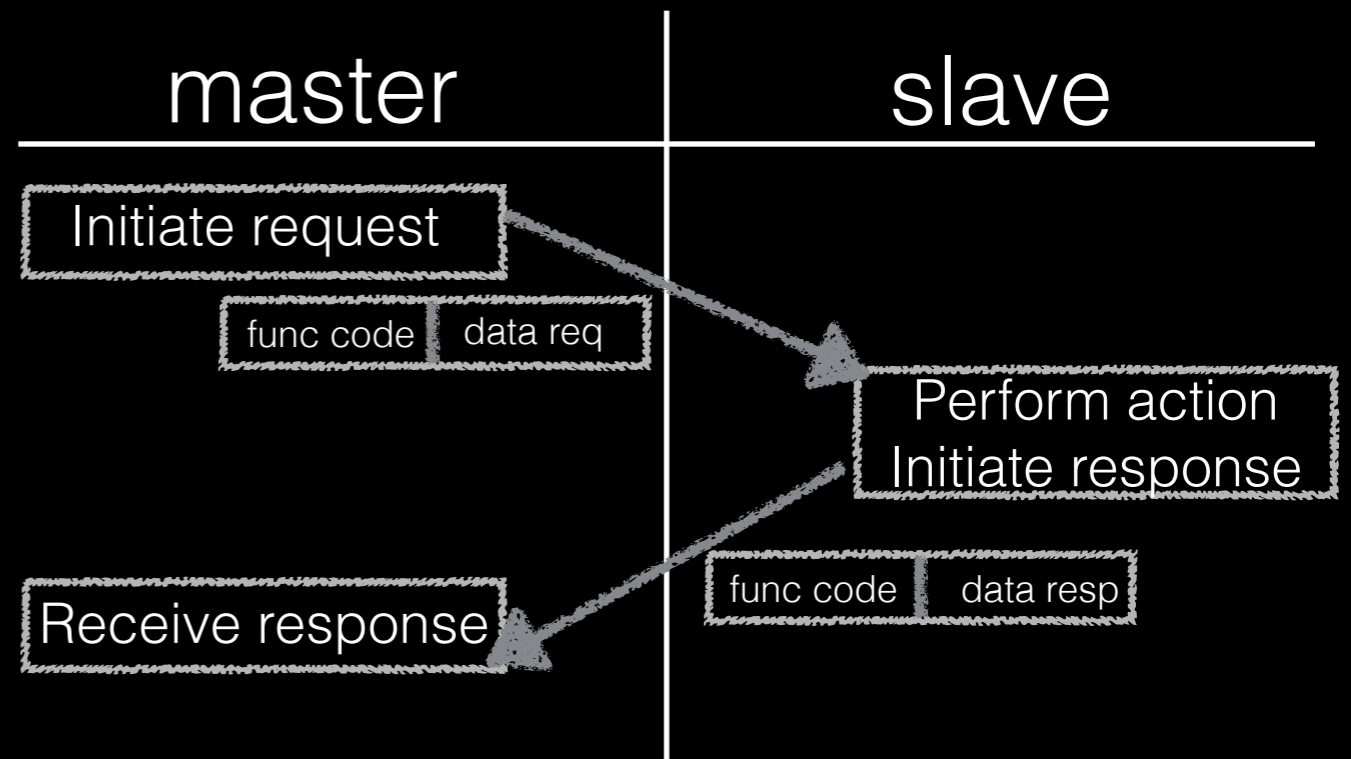
Modbus协议

- 全球第一个真正用于工业现场的总线协议
- 施耐德电子（Schneider Electric）发布于1979年
- 标准开放，免费使用
- 目前作为工业标准工业网络传输协议之一

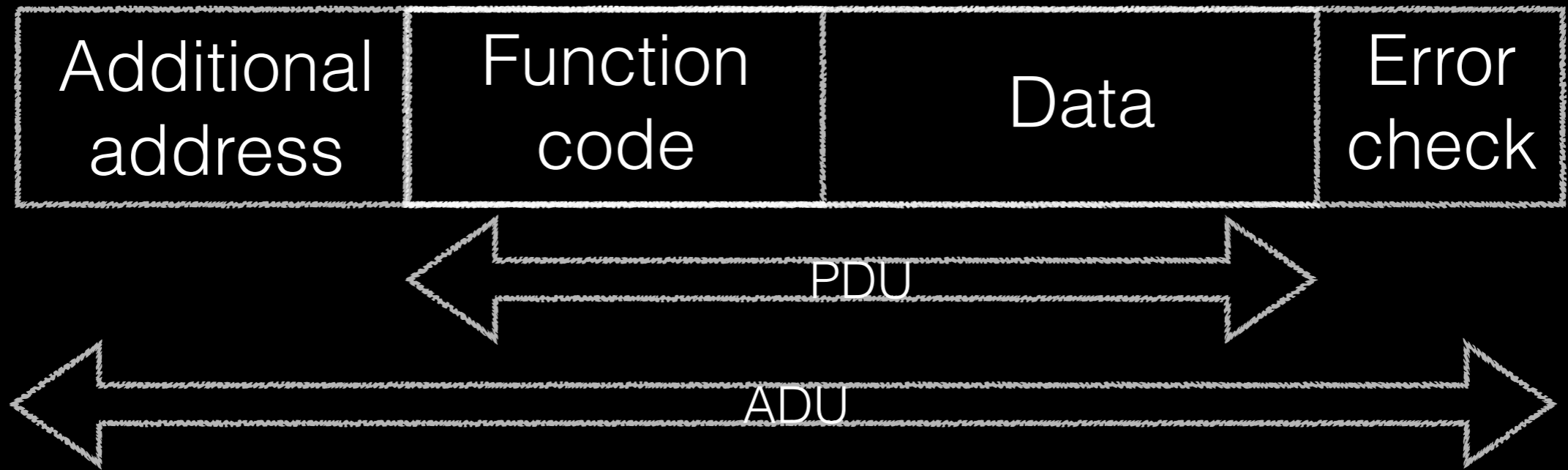


Modbus协议

- Master/Slave模式
- 8位地址长度，每个Master可支持247个Slave
- 简单清晰的协议内容
- 无加密与身份认证

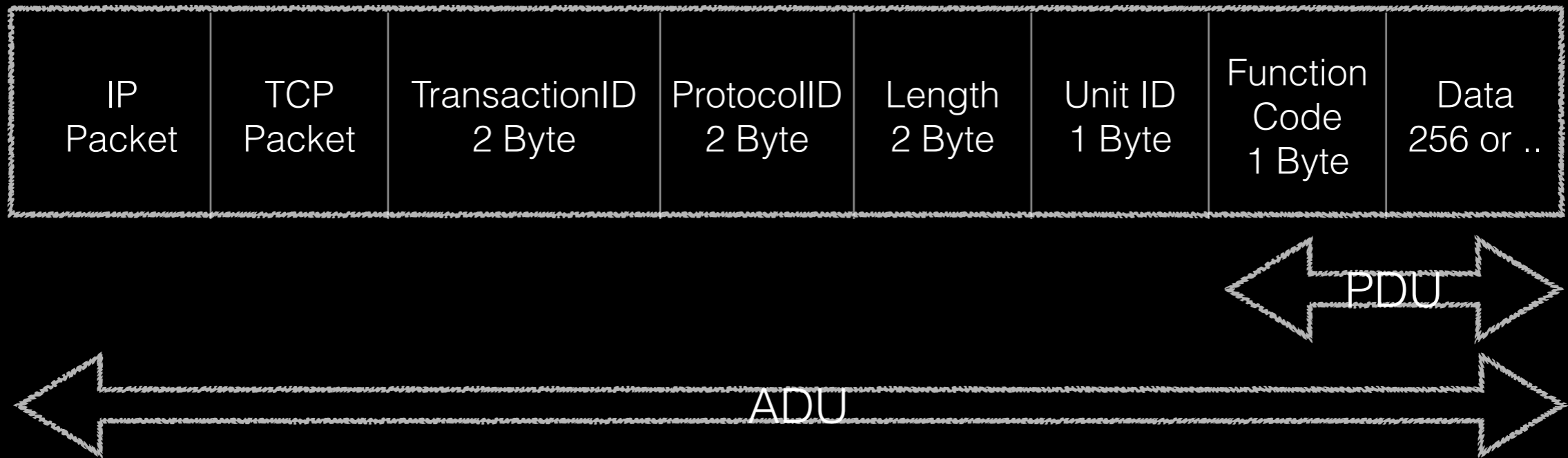


Modbus协议



Modbus Frame

Modbus协议



Modbus TCP Frame

Modbus协议

Function Name	Function Code
Read Coils	0x01
Write Single Coil	0x05
Write Multiple Coils	0x15
Read Input Register	0x04
Write Single Register	0x06
Read/Write Multiple Register	0x23

Modbus协议

Function type		Function name	Function code	
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	2
		Internal Bits or Physical Coils	Read Coils	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit access	Physical Input Registers	Read Input Registers	4
		Internal Registers or Physical Output Registers	Read Holding Registers	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access	Read File Record	20	
		Write File Record	21	
Diagnostics	Read Exception Status	7		
	Diagnostic	8		
	Get Com Event Counter	11		
	Get Com Event Log	12		
	Report Slave ID	17		
	Read Device Identification	43		
Other	Encapsulated Interface Transport	43		

[维基百科——Modbus所有功能码](http://en.wikipedia.org/wiki/Modbus)
<http://en.wikipedia.org/wiki/Modbus>

Modbus协议

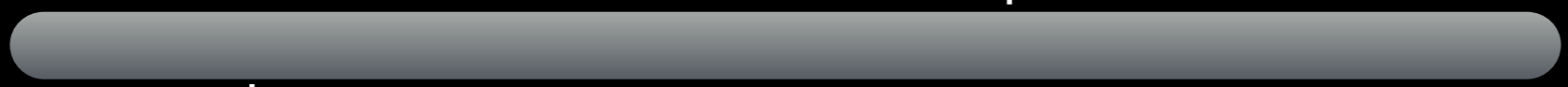
```
[-] Modbus/TCP
  Transaction Identifier: 0
  Protocol Identifier: 0
  Length: 5
  Unit Identifier: 255

[-] Modbus
  Function Code: Encapsulated Interface Transport (43)
  MEI type: Read Device Identification (14)
  Read Device ID: Basic Device Identification (1)
  Object ID: VendorName (0)
```

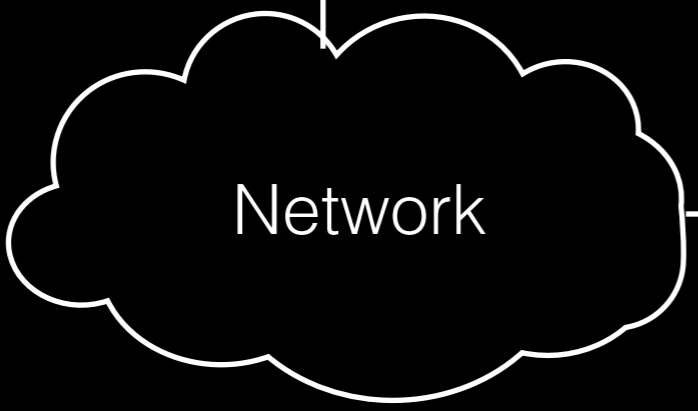
0000	00	0c	29	28	1c	ff	00	50	56	c0	00	08	08	00	45	00	..)(...P V.....E.
0010	00	3f	03	8a	40	00	40	06	0b	55	c0	a8	d5	01	c0	a8	.?...@.@. .U.....
0020	d5	87	fb	3e	01	f6	59	b5	6d	16	e0	bc	71	1e	80	18	...>..Y. m...q...
0030	10	15	30	6f	00	00	01	01	08	0a	13	01	bc	e6	05	88	..0o....
0040	11	ce	00	00	00	00	05	ff	2b	0e	01	00				+...



Modbus协议



RS-232/RS-485



Modbus TCP

入侵方式

工业化信息化融合推进

工控组件脆弱性

设备升级维护成本高

安全意识薄弱

攻击面

更脆弱的系统
更多的攻击面

模拟环境

探索发现目标

协议分析

设备识别

攻击工具/框架

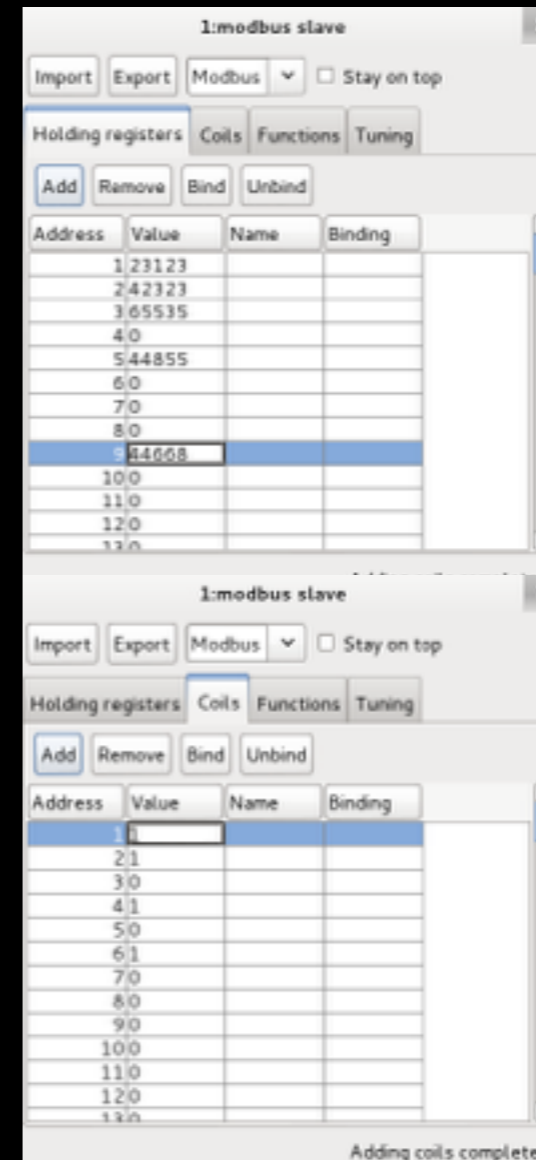
手动攻击测试

模拟环境

[ModbusPal]

Slave节点仿真模拟

<http://modbuspal.sourceforge.net/>



网络分析

[Wireshark]

<https://www.wireshark.org/>
Modbus/S7/DNP3协议解析

The image shows a screenshot of the Wireshark network traffic analysis tool. The main window displays a list of captured packets. Packet 3559 is selected and expanded to show its details. The packet is a Modbus/TCP response from 192.168.213.135 to 192.168.213.1. The details pane shows the following information:

- Transaction Identifier: 0
- Protocol Identifier: 0
- Length: 50
- Unit Identifier: 255
- Modbus
 - Function Code: Encapsulated Interface Transport (43)
 - MEI type: Read Device Identification (14)
 - Read Device ID: Basic Device Identification (1)
 - Conformity Level: Basic Device Identification (stream and individual) (0x81)

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII:

```
0000 00 50 56 c0 00 08 00 0c 29 28 1c ff 08 00 45 00  .PV.....)(....E.  
0010 00 6c 60 d1 40 00 40 06 ad e0 c0 a8 d5 87 c0 a8  .l'@.@. ....  
0020 d5 01 01 f6 fb 3e e0 bc 71 1e 59 b5 6d 21 80 18  ....>.. q.Y.m!..  
0030 01 c5 2c 39 00 00 01 01 08 0a 05 88 11 ce 13 01  ..9.....  
0040 bc e6 00 00 00 00 00 32 ff 2b 0e 01 81 00 00 03  ....2.+.....  
0050 00 14 53 63 68 6e 65 69 64 65 72 20 45 6c 65 63  ..Schnei der Elec  
0060 74 72 69 63 20 20 01 0c 42 4d 58 20 50 33 34 20  tric .. BMX P34  
0070 32 30 32 30 02 04 76 32 2e 32                    2020..v2 .2
```

本地模拟攻防

[mbtget]

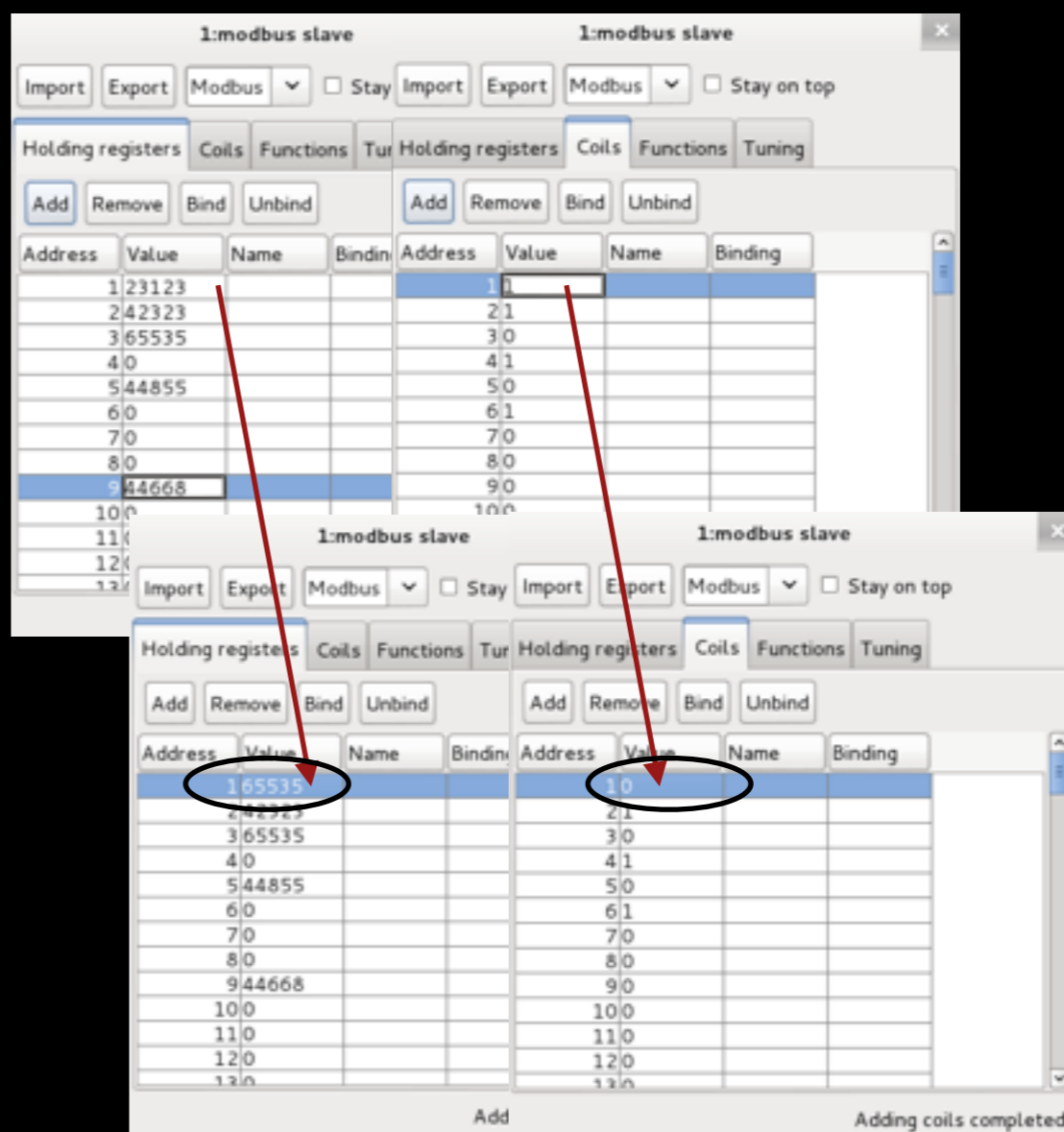
Perl脚本Modbus协议工具

<https://github.com/sourceperl/mbtget>

```
root@kali:~/ICS/mbtget# mbtget -r1 -a 0 -n 8 127.0.0.1
values:
1 (ad 00000): 0
2 (ad 00001): 1
3 (ad 00002): 0
4 (ad 00003): 1
5 (ad 00004): 0
6 (ad 00005): 1
7 (ad 00006): 0
8 (ad 00007): 0
```

```
root@kali:~/ICS/mbtget# mbtget -r3 -a 0 -n 8 127.0.0.1
values:
1 (ad 00000): 23123
2 (ad 00001): 42323
3 (ad 00002): 65535
4 (ad 00003): 0
5 (ad 00004): 44855
6 (ad 00005): 0
7 (ad 00006): 0
8 (ad 00007): 0
```

```
root@kali:~/ICS/mbtget# mbtget -w5 0 -a 0 -d 127.0.0.1
Tx
[97 0B 00 00 00 06 01] 05 00 00 00 00
Rx
[97 0B 00 00 00 06 01] 05 00 00 00 00
bit write ok
root@kali:~/ICS/mbtget# mbtget -w6 65535 -a 0 -d 127.0.0.1
Tx
[40 14 00 00 00 06 01] 06 00 00 FF FF
Rx
[40 14 00 00 00 06 01] 06 00 00 FF FF
word write ok
```



本地模拟攻防

[Metasploit Framework]

auxiliary/scanner/scada/modbus_findunitid

auxiliary/scanner/scada/modbusclient

auxiliary/scanner/scada/modbusdetected

```
msf auxiliary(modbusclient) > info

Name: Modbus Client Utility
Module: auxiliary/scanner/scada/modbusclient
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
EsMnemon <esm@mnemonic.no>
Arnaud SOULLIE <arnaud.soullie@solucom.fr>

Available actions:
Name          Description
----          -
READ_COIL     Read one bit from a coil
READ_REGISTER Read one word from a register
WRITE_COIL    Write one bit to a coil
WRITE_REGISTER Write one word to a register

Basic options:
Name          Current Setting  Required  Description
----          -
DATA          1                no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
DATA_ADDRESS  0                yes       Modbus data address
RHOST         127.0.0.1        yes       The target address
RPORT         502              yes       The target port
UNIT_NUMBER   1                no        Modbus unit number

Description:
This module allows reading and writing data to a PLC using the
Modbus protocol. This module is based on the 'modiconstop.rb'
Basecamp module from DigitalBond, as well as the mbtget perl script.
```

探索发现目标

Shodan Search Engine Results for port:502

Showing results 1 - 10 of 21,510

TOP COUNTRIES

United States	4,132
France	1,204
Spain	915
Sweden	759
Canada	671

TOP ORGANIZATIONS

Verizon Wireless	1,593
Orange	934
Kddi Corporation	618
Telefonica de Espana	486
Deutsche Telekom AG	200

TOP OPERATING SYSTEMS

Linux 2.4.x	40
Windows 7 or 8	28
Linux 2.4-2.6	21
Linux 2.6.x	19
Linux 3.x	18

TOP PRODUCTS

BMX P34 2020	821
BMX P34 2020	750

128.125.31.86
fl-ph-1002.usc.edu
University of Southern California
Added on 2015-08-07 10:14:37 GMT
United States, Los Angeles
Details

Unit ID: 0
-- Slave ID Data: - Triacta,Powerhawk,4224-128V-2P-24,1.46,1185 (2d83ff547269616374612c5805)

166.148.41.149
149.sub-166-148-41.myvzw.com
Verizon Wireless
Added on 2015-08-07 10:14:37 GMT
United States
Details

Unit ID: 0

95.89.30.231
ip5f591ee7.dynamic.kabel
Kabel Deutschland
Added on 2015-08-07 10:14:37 GMT
Germany, Bann
Details

PLC、RTU..工控设备
无一幸免

网络空间
搜索引擎

ZoomEye ICS

通过 ZoomEye 探索世界各地工业控制系统

Protocols

Siemens S7 TCP 102 port:102	Modbus TCP 502 port:502	IEC 60870-5-104 TCP 2404 port:2404	DNP3 TCP 20000 port:20000	EtherNet/IP TCP 44818 port:44818	BACnet TCP 47808 port:47808
Tridium Niagara Fox TCP 1911 port:1911	Crimson V3 TCP 789 port:789	OMRON FINS TCP 9600 port:9600	PCWorx TCP 1962 port:1962	ProConOs TCP 20547 port:20547	MELSEC-Q TCP 5007 port:5007

黑暗“Google”

探索发现目标

[Nmap]

modbus-discover.nse

modbus-enum.nse

```
root@kali:/usr/share/nmap/scripts# nmap --scan-delay=1 -p502 --script modbus-discover.nse

Starting Nmap 6.47 ( http://nmap.org ) at 2015-08-07 18:17 CST
Nmap scan report for 90-25-187-213.wifi4all.it (213.187.25.90)
Host is up (0.76s latency).
PORT      STATE SERVICE
502/tcp   open  modbus
| modbus-discover:
|   Positive error response for sid = 0x1 (ILLEGAL FUNCTION)
|_  DEVICE IDENTIFICATION: Schneider Electric TM258LF42DT4L V02.00.31.15

Nmap done: 1 IP address (1 host up) scanned in 9.85 seconds
```

注意

《NIST SP800-82》

- 1.降低扫描速度—scan-delay=1
- 2.TCP替代UDP
- 3.避免使用nmap指纹识别 -sC
- 4.不推荐nmap
- 5.不要尝试对运行中的设备进行测试

探索发现目标

[plcscan]

TCP/502 TCP/102端口PLC识别工具

code.google.com/p/plcscan

```
root@kali:~/ICS/plcscan# python plcscan.py -h
Usage: plcscan.py [options] [ip range]...

Scan IP range for PLC devices. Support MODBUS and S7COMM protocols

Options:
  -h, --help                show this help message and exit
  --hosts-list=FILE         Scan hosts from FILE
  --ports=PORTS             Scan ports from PORTS
  --timeout=TIMEOUT        Connection timeout (seconds)

Modbus scanner:
  --brute-uid               Brute units ID
  --modbus-uid=UID          Use uids from list
  --modbus-function=NOM    Use modbus function NOM for discover units
  --modbus-data=DATA       Use data for for modbus function
  --modbus-timeout=TIMEOUT Timeout for modbus protocol (seconds)

S7 scanner options:
  --src-tsap=LIST          Try this src-tsap (list) (default: 0x100,0x
  --dst-tsap=LIST          Try this dst-tsap (list) (default: 0x102,0x

root@kali:~/ICS/plcscan# python plcscan.py 127.0.0.1 --brute-uid
Scan start...
127.0.0.1:502 Modbus/TCP
Unit ID: 0
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 255
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 1
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 2
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 3
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 4
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 5
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 6
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 7
  Device: Schneider Electric   BMX P34 2020 v2.2
Unit ID: 8
  Device: Schneider Electric   BMX P34 2020 v2.2
```

探索发现目标

[ModTest]

针对Modbus分析协议、扫描、指纹识别、Fuzzing、甄别蜜罐

<https://github.com/ameng929/ModTest>

```
Usage: ModTest.py [options] [ip]...

Scan IP range for PLC devices, Support MODBUS and...

Options:
  -h, --help                show this help message and exit
  --host-list=FILE          Scan hosts from file
  --ports=PORTS             Scan ports
  --timeout=TIMEOUT        Connection timeout (seconds)

Modbus Tester:
  --brute-uid               Brute units ID
  --modbus-uid=UID         Use uids from list
  --modbus-function=NOM    Use modbus function NOM for discover units
  --modbus-data=DATA       Use data for for modbus function
  --modbus-timeout=TIMEOUT
                          Timeout for modbus protocol (seconds)
  -f, --func-fuzzing       Modbus FunctionCode Fuzzing
  -d, --debug              Debug-verbose mode
  -i, --device-info-scan   Scan Schneider PLC for more device information
```

探索发现目标

[ModTest]

Modbus分析协议

<https://github.com/ameng929/ModTest>

```
qmwang@MacBook-Pro:~/Documents/workspace/ModTest% python ModTest.py 192.168.213.135 -d
Scan start...
192.168.213.135:502...
-----send package:
0000  00 00 00 00 00 05 00 2B  0E 01 00                .....+...
None

-----recv package:
0000  00 00 00 00 00 32 00 2B  0E 01 81 00 00 03 00 14  .....2.+.....
0010  53 63 68 6E 65 69 64 65  72 20 45 6C 65 63 74 72  Schneider Electr
0020  69 63 20 20 01 0C 42 4D  58 20 50 33 34 20 32 30  ic ..BMX P34 20
0030  32 30 02 04 76 32 2E 32                                     20..v2.2
None
192.168.213.135:502 Modbus/TCP
```


探索发现目标

[ModTest]

Modbus Fuzzing

<https://github.com/ameng929/ModTest>

方式:

针对Function Code

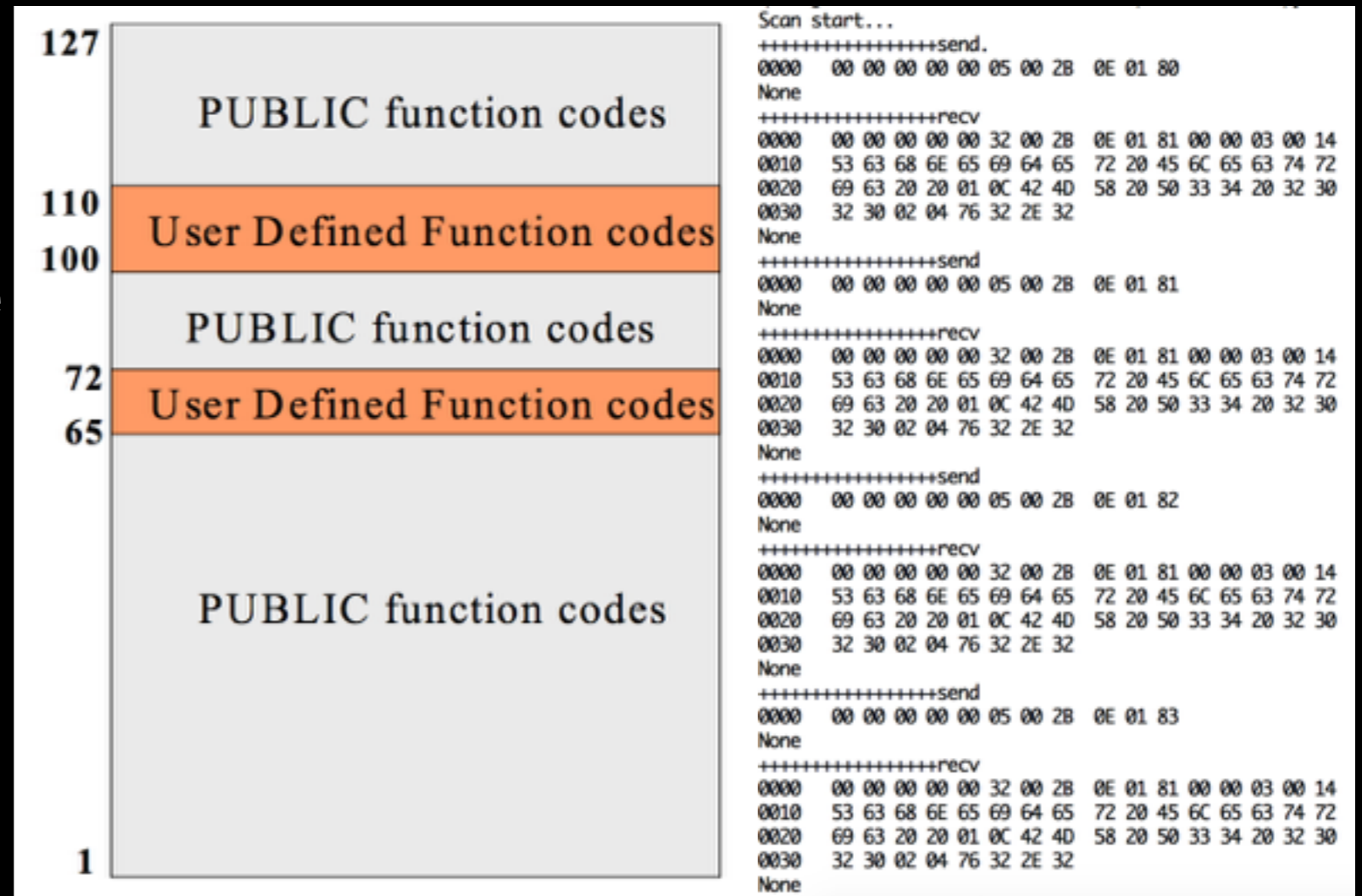
针对Diagnostics Code

发现:

90/91/99功能码

识别工控蜜罐的方式

拒绝服务



探索发现目标

[ModTest]

Modbus 指纹识别

<https://github.com/ameng929/ModTest>

识别更多的plc设备信息
更邪恶的入侵方式

...

```
qmwang@MacBook-Pro:~/Documents/workspace/ModTest% python ModTest.py -i 192.168.1.101
Scan start...
-----send2...
0000  00 0F 00 00 00 0D 00 5A  00 20 00 14 00 64 00 00  .....Z. ...d..
0010  00 F6 00
None
-----recv
0000  00 0F 00 00 00 FD 00 5A  00 FE 00 F6 00 00 00 00  .....Z.....
0010  00 00 00 00 00 00 00 00  00 00 00 00 00 01 00 46  .....F
0020  A5 61 B5 3A 97 D8 48 8A  1B 09 3D 54 A1 AE EB B2  .a.:..H...=T....
0030  BC B7 DD E5 94 D3 40 B0  92 DE 7A 83 5C 35 62 00  .....@...z.\5b.
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0050  0A 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00a0  00 00 00 00 00 00 00 00  00 50 72 6F 67 65 74 74  .....Progett
00b0  6F 00 00 00 00 00 00 00  00 00 56 38 2E 30 00 00  o.....V8.0..
00c0  00 49 56 41 4E 2D 50 43  00 00 00 00 00 00 00 00  .IVAN-PC.....
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0100  00 00 00
None
```


入侵方式

[Unity Pro XL]

施耐德PLC编程软件

<http://www.schneider-electric.com/>

发现：
可远程接入设备
但远程传输项目失败
原因：
Unity Pro XL版本多样
兼容性差



入侵方式

分析Unity Pro XL软件协议、认证方式

20496 5398.02666 192.168.213.136 90.176.192.168 Modbus/ 64 Query: Trans: 4681; Unit: 0, Func: 90: Unknown function (90)

20497 5398.02692 90.176.192.168 192.168.213.136 TCP 60 asa-appl-proto > idp-infotrieve [ACK] Seq=1 Ack=11 win=64240 Len=0

20498 5398.49632 90.176.192.168 192.168.213.136 Modbus/ 116 Response: Trans: 4681; Unit: 0, Func: 90: Unknown function (90)

20499 5398.51105 192.168.90.176.192.168 Modbus/ 65 Query: Trans: 4682; Unit: 0, Func: 90: Unknown function (90)

20500 5398.51138 90.176.192.168 192.168.213.136 TCP 60 asa-appl-proto > idp-infotrieve [ACK] Seq=63 Ack=22 win=64240 Len=0

20501 5398.94502 90.176.192.168 192.168.213.136 Modbus/ 77 Response: Trans: 4682; Unit: 0, Func: 90: Unknown function (90)

20502 5398.94833 192.168.90.176.192.168 Modbus/ 1082 Query: Trans: 4683; Unit: 0, Func: 90: Unknown function (90)

20503 5398.94861 90.176.192.168 192.168.213.136 TCP 60 asa-appl-proto > idp-infotrieve [ACK] Seq=86 Ack=1050 win=64240 Len=0

20504 5399.37990 90.176.192.168 192.168.213.136 Modbus/ 1082 Response: Trans: 4683; Unit: 0, Func: 90: Unknown function (90)

20505 5399.38773 192.168.90.176.192.168 Modbus/ 65 Query: Trans: 4684; Unit: 0, Func: 90: Unknown function (90)

20506 5399.38799 90.176.192.168 192.168.213.136 TCP 60 asa-appl-proto > idp-infotrieve [ACK] Seq=1114 Ack=1061 win=64240 Len=0

20507 5399.44915 192.168.90.176.192.168 Modbus/ 65 Query: Trans: 4685; Unit: 0, Func: 90: Unknown function (90)

20508 5399.44945 90.176.192.168 192.168.213.136 TCP 60 asa-appl-proto > idp-infotrieve [ACK] Seq=1114 Ack=1072 win=64240 Len=0

20509 5399.76633 90.176.192.168 192.168.213.136 Modbus/ 111 Response: Trans: 4684; Unit: 0, Func: 90: Unknown function (90)

20510 5399.77724 192.168.90.176.192.168 Modbus/ 65 Query: Trans: 4686; Unit: 0, Func: 90: Unknown function (90)

20511 5399.77747 90.176.192.168 192.168.213.136 TCP 60 asa-appl-proto > idp-infotrieve [ACK] Seq=1171 Ack=1083 win=64240 Len=0

20512 5400.10850 90.176.192.168 192.168.213.136 Modbus/ 77 Response: Trans: 4685; Unit: 0, Func: 90: Unknown function (90)

20513 5400.12117 192.168.90.176.192.168 Modbus/ 1082 Query: Trans: 4687; Unit: 0, Func: 90: Unknown function (90)

20514 5400.12139 90.176.192.168 192.168.213.136 TCP 60 asa-appl-proto > idp-infotrieve [ACK] Seq=1194 Ack=2111 win=64240 Len=0

Frame 20496: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0

Ethernet II, Src: Vmware_b1:29:93 (00:0c:29:b1:29:93), Dst: Vmware_fb:69:a0 (00:50:56:fb:69:a0)

Internet Protocol Version 4, Src: 192.168.213.136 (192.168.213.136), Dst: 192.168.192.168

Transmission Control Protocol, Src Port: idp-infotrieve (2966), Dst Port: asa-app1-prot0 (502), seq: 1, Ack: 1, Len: 10

Modbus/TCP

Transaction Identifier: 4681

Protocol Identifier: 0

Length: 4

Unit Identifier: 0

Modbus

Function Code: Unknown (90)

Data: 0002

0000 00 50 56 fb 69 a0 00 0c 29 b1 29 93 08 00 45 00 .PV.i...).)...E.

0010 00 32 f3 6d 40 00 80 06 62 a7 c0 a8 d5 88 5a b0 .2.m@... b.....Z.

0020 b3 cf 0b 96 01 f6 8a 26 cc 3c b5 f0 dd 2e 50 18& .<....P.

0030 fa f0 06 69 00 00 12 49 00 00 00 04 00 5a 00 02 ...1..:IZ..

软件使用Modbus功能码90进行通信
协议内容无加密!

入侵方式

分析Unity Pro XL软件协议、认证方式

```
00000895 12 56 00 00 00 0d 00 5a 00 20 00 14 00 64 00 00 .v.....Z . ...d..
000008A5 00 f6 03
00000B93 12 56 00 00 03 fd 00 5a 00 fe 00 f6 03 00 00 00 .v.....Z .....
00000BA3 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0f .....
00000BB3 43 fb f0 f4 b9 e9 43 88 24 1e 98 aa 8a 0c 60 68 C.....C. $. ....`h
00000BC3 38 2b 7f 27 00 a4 46 9d f9 c7 5e ce 9d 98 a6 00 8+. ' ..F. ..^.....
00000BD3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000BE3 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000BF3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000C03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000C13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000C23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000C33 00 00 00 00 00 00 00 00 00 53 74 61 74 69 6f 6e ..... .Station
00000C43 00 00 00 00 00 00 00 00 00 56 35 2e 30 00 00 00 ..... .V5.0...
00000C53 4b 55 4e 41 52 54 2d 4e 42 32 00 43 3a 5c 56 4f KUNART-N B2.C:\VO
00000C63 44 41 52 4e 41 5c 53 63 68 6e 65 69 64 65 72 5c DARNA\Sc hneider\
00000C73 55 6e 69 74 79 5c 42 50 53 20 42 72 6c 6f 68 5c Unity\BP S Brloh\
00000C83 62 70 73 5f 62 72 6c 6f 68 5f 76 37 30 2e 73 74 bps_brlo h_v70.st
00000C93 75 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 u.....
```

协议中发现读取PLC设备信息通信数据

0x00, 0x0f, 0x00, 0x00, 0x00, 0x0d, 0x00, 0x5a, 0x00, 0x20,
0x00, 0x14, 0x00, 0x64, 0x00, 0x00, 0x00, 0xf6, 0x03

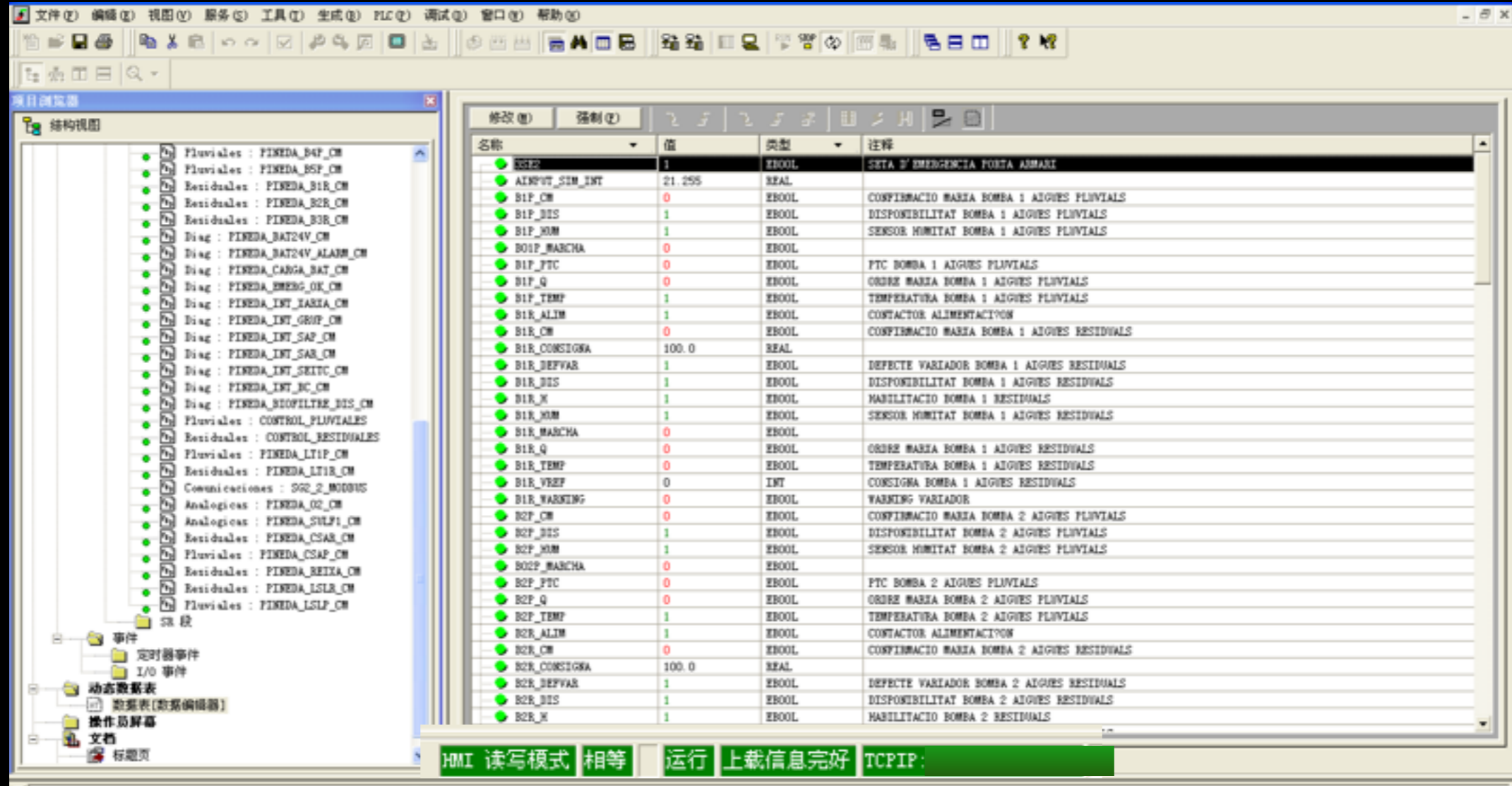
重放请求，获得PLC设备项目信息

针对应答数据选择针对的Unity Pro XL软件

V5.0  Unity Pro XL 5.0

入侵方式

通过针对版本的Unity Pro XL软件获取到PLC权限



可查看实时数据表、修改上传PLC程序、停止PLC执行!!!

入侵方式

通过Shodan进行设备探索与入侵

The screenshot displays three search results from Shodan, each for a Schneider Electric BMX P34 2020 PLC. Each entry includes the IP address, ISP, country, and a list of project files. The files are consistently named with a version number (e.g., V5.0) and a .STU extension.

IP Address	ISP	Country	Project File
82.127.145.229	Orange	France	ASTR-VIL-P D:\Users\astreinte-vil\Desktop\roanne_26822014.STU
90.176.179.207	Telefonica Czech Republic, a.s.	Czech Republic	KUNART-NB2 C:\VODARNA\Schneider\Unity\BPS Brloh\bps_brloh_v70.stu
81.242.46.201	Belgacom Skynet	Belgium	LA2330 C:\AQIPLUS_GEO\HUIDIG PLC2\WZI_GEEL_PLC2_UNITY_V6.STU

针对施耐德PLC编程软件的Dork
port:502 V5.0 .stu
V5.0——编程软件版本号
.stu——施耐德PLC程序后缀

应对探索

[工控蜜罐]

协议仿真scapy、pymodbus

<https://github.com/tecpal/PyModbus>

- 对读写PLC Coil、Register值的响应
- 对43功能码读取PLC设备信息的响应
- 对17功能码请求从节点信息的响应
- 对90功能码读取Modicon PLC信息的响应

应对探索

[工控蜜罐]

Web管理登陆界面

The image shows a screenshot of the Schneider Electric BMX NOE 0100 B web management interface. The page features the Schneider Electric logo in the top left corner. A green header bar displays the product name "BMX NOE 0100 B". Below the header, there is a navigation menu with tabs for "Home", "Documentation", and "URL". A secondary navigation bar contains buttons for "Monitoring", "Control", "Diagnostics", "Maintenance", and "Setup". On the left side, there is a "Home" link and a "Languages" dropdown menu listing English, French, German, Italian, and Spanish. The main content area shows a photograph of the BMX NOE 0100 B device. Overlaid on the bottom right of the page is a dark grey login form with the "airOS™" logo. The login form includes fields for "Username:" and "Password:", and a "Login" button.

应对探索

[工控蜜罐]
其他选择组件

- FTP
- SNMP
- TELNET
- 其他工控协议

The screenshot displays a network scanner interface with the following sections:

- Ports:** A row of four colored boxes containing the numbers 21, 80, 161, and 502.
- Services:** A list of detected services with their corresponding port numbers and protocols:
 - 21 FTP:** 220 host FTP server (VxWorks 6.4) ready. 530 Login failed. 214- The following commands are recognized (* =>'s unimplemented). USER EPRT STRU REST CWD SYST XMKD CDUP PASS PASV MODE RNFR XCWD STAT RMD XCUP QUIT LPSV RETR RNTD LIST HELP XRMD STOU PORT EPSV STOR ABOR NLST NOOP PWD SIZE LPRT TYPE APPE DELE SITE MKD XPWD MDTM 214 Direct comments to ftp-bugs@host. 530 Please login with USER and PASS.
 - 80 HTTP:** HTTP/1.0 302 Redirect Server: Schneider-WEB/V2.2.0 Date: FRI OCT 03 00:59:36 1980 Pragma: no-cache Cache-Control: no-cache Content-length: 198 Content-Type: text/html Location: http://166.239.227.42/index.htm
 - 161 SNMP:** Schneider-Electric BMX NOE 0100 REV0280 Modicon M340 Ethernet 1 Port 10/100 RJ45
 - 502 Modbus:** BMX NOE 0100 Version: V2.80
 - Unit ID: 0
 - Device Identification: Schneider Electric BMX NOE 0100 V2.80
 - CPU module: BMX P34 1000
 - Memory card: BMXRMS000MP
 - Project information: JR GILLAM_PS - PS V8.0 UNITY-8 \\vboxsrv\VMShare\MCCAYSVI LLE PLC PROGS FROM LAPTOP\JR
 - Project revision: 0.0.78
 - Project last modified: 2015-03-27 15:18:56
 - Unit ID: 255
 - Device Identification: Schneider Electric BMX NOE 0100 V2.80

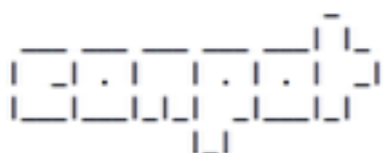
应对探索

[工控蜜罐]

conpot

<https://github.com/mushorg/conpot>

```
# conpot --template default
```



Version 0.4.0
Glastopf Project

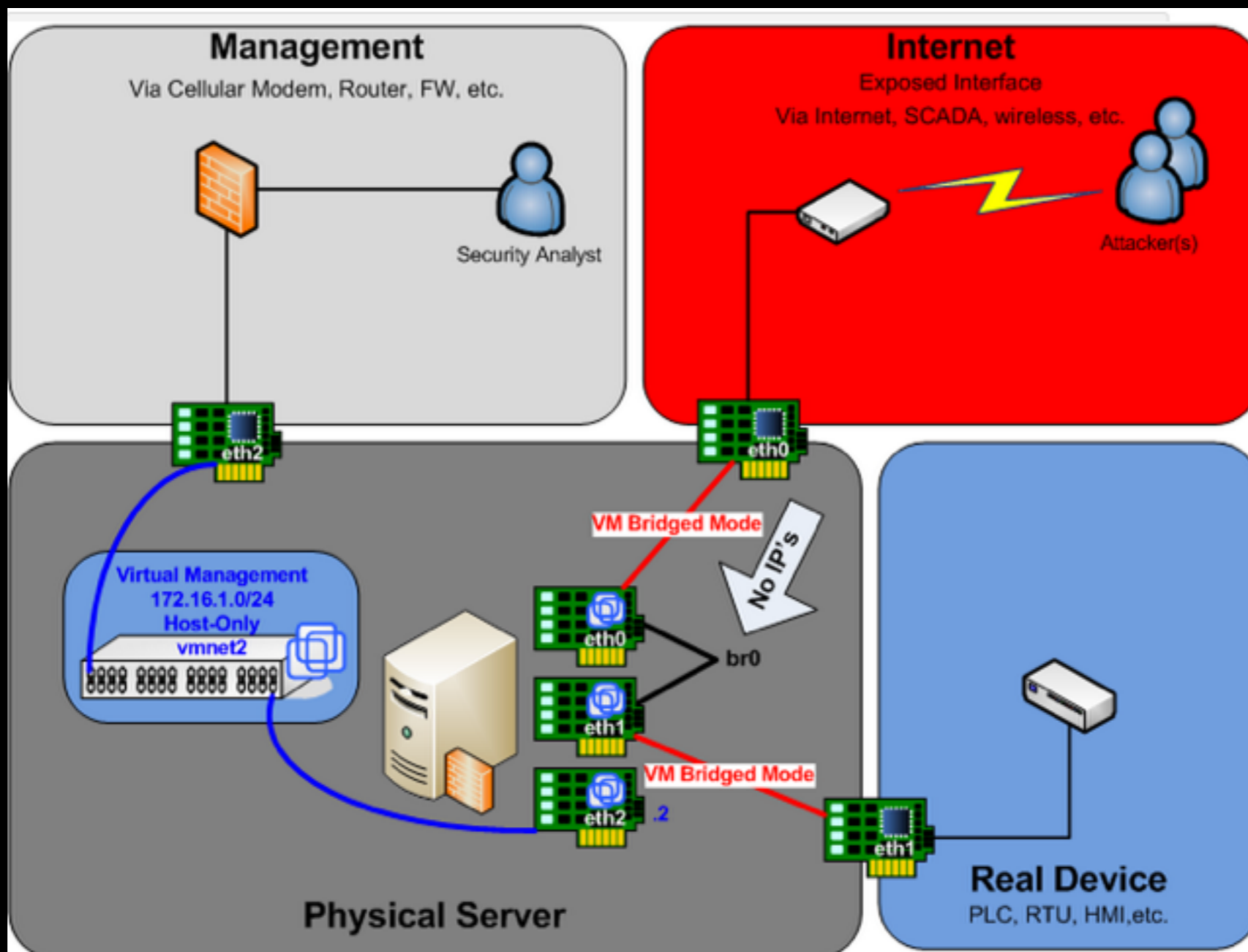
```
2015-05-27 16:05:08,355 Starting Conpot using template: /usr/local/lib/python2.7/dist-packages/Conpot-0.4.0-py2.7.egg/conp
2015-05-27 16:05:08,366 Starting Conpot using configuration found in: /usr/local/lib/python2.7/dist-packages/Conpot-0.4.0-
2015-05-27 16:05:08,428 Starting new HTTP connection (1): www.telize.com
2015-05-27 16:05:08,861 Fetched xxx.xxx.xxx.xxx as external ip.
2015-05-27 16:05:08,891 Conpot modbus initialized
2015-05-27 16:05:08,893 Found and enabled ('modbus', <class 'conpot.protocols.modbus.modbus_server.ModbusServer' at 0xb4f1e3
2015-05-27 16:05:08,898 Conpot S7Comm initialized
2015-05-27 16:05:08,899 Found and enabled ('s7comm', <class 'conpot.protocols.s7comm.s7_server.S7Server'>) protocol.
2015-05-27 16:05:08,902 Found and enabled ('http', <class 'conpot.protocols.http.web_server.HTTPServer'>) protocol.
2015-05-27 16:05:08,905 Found and enabled ('snmp', <class 'conpot.protocols.snmp.snmp_server.SNMPServer'>) protocol.
2015-05-27 16:05:08,915 Conpot Bacnet initialized using the /usr/local/lib/python2.7/dist-packages/Conpot-0.4.0-py2.7.egg/
2015-05-27 16:05:08,916 Found and enabled ('bacnet', <class 'conpot.protocols.bacnet.bacnet_server.BacnetServer'>) protoco
2015-05-27 16:05:08,922 IPMI BMC initialized.
2015-05-27 16:05:08,923 Conpot IPMI initialized using /usr/local/lib/python2.7/dist-packages/Conpot-0.4.0-py2.7.egg/conpot
2015-05-27 16:05:08,923 Found and enabled ('ipmi', <class 'conpot.protocols.ipmi.ipmi_server.IpmiServer'>) protocol.
2015-05-27 16:05:09,003 No proxy template found. Service will remain unconfigured/stopped.
2015-05-27 16:05:09,015 Modbus server started on: ('0.0.0.0', 502)
2015-05-27 16:05:09,017 S7Comm server started on: ('0.0.0.0', 102)
2015-05-27 16:05:09,018 HTTP server started on: ('0.0.0.0', 80)
2015-05-27 16:05:09,285 SNMP server started on: ('0.0.0.0', 161)
2015-05-27 16:05:09,286 Bacnet server started on: ('0.0.0.0', 47808)
2015-05-27 16:05:09,286 IPMI server started on: ('0.0.0.0', 623)
2015-05-27 16:05:09,287 connecting to hpfriends.honeycloud.net:20000
2015-05-27 16:05:14,006 Privileges dropped, running as nobody/nogroup.
```

应对探索

[工控蜜罐]

SCADA Honeynet

<http://www.digitalbond.com/tools/scada-honeynet/>



应对探索

[工控蜜罐]

Modhoney

在PyModbus与Z-one版本上进行了改进与优化

<https://github.com/ameng929/Modhoney>

```
Received = array('B', [33, 0, 0, 0, 0, 6, 2, 4, 0, 1, 0, 0, 0])
ID= 2, Fun.Code= 4, Address= 1, Length= 0
Received = array('B', [33, 0, 0, 0, 0, 6, 2, 4, 0, 1, 0, 0, 0])
ID= 2, Fun.Code= 4, Address= 1, Length= 0
Received = array('B', [33, 0, 0, 0, 0, 6, 2, 4, 0, 1, 0, 0, 0])
ID= 2, Fun.Code= 4, Address= 1, Length= 0
Received = array('B', [33, 0, 0, 0, 0, 6, 2, 4, 0, 1, 0, 0, 0])
ID= 2, Fun.Code= 4, Address= 1, Length= 0
```

```
Received = array('B', [0, 0, 0, 0, 0, 2, 0, 17, 0, 0, 0, 0, 0])
ID= 0, Fun.Code= 17
```

```
Received = array('B', [0, 0, 0, 0, 0, 5, 0, 43, 14, 1, 0, 0, 0])
```

```
502
Modbus
BMX P34 20302 Version: v2.2

Unit ID: 0
-- Device Identification: Schneider Electric BMX P34 20302 v2.2
-- CPU module: BMX P34 20302
-- Memory card: BMXRMS008BMP
-- Project information: Progetto - V5.0 MASSIMOURBA9562 \\psf\Dropbox\PLC\HOFMANN\POV
0\PLCPOVO V3 2.STU
-- Project revision: 0.0.217
-- Project last modified: 2015-05-21 14:32:04

Unit ID: 255
-- Device Identification: Schneider Electric BMX P34 20302 v2.2
```

增加了对于TransactionID的识别与应答
增加了对于功能码90的识别与应答
配合conpot更容易被网络搜索引擎发现

应对探索

[工控蜜罐]

Modhoney

在PyModbus与Z-one版本上进行了改进与优化

<https://github.com/ameng929/Modhoney>

```
GET request from ('103.233.194.106', 60811): ('/phpMyAdmin/scripts/setup.php', ['Host: 103.56.112.82\r\n'], None).  
response to ('103.233.194.106', 60811): 404. 95710883-e1b9-4ba8-a2d8-9f381b57161d  
GET request from ('103.233.194.106', 61029): ('/pma/scripts/setup.php', ['Host: 103.56.112.82\r\n'], None). 9571088  
response to ('103.233.194.106', 61029): 404. 95710883-e1b9-4ba8-a2d8-9f381b57161d  
GET request from ('103.233.194.106', 61257): ('/myadmin/scripts/setup.php', ['Host: 103.56.112.82\r\n'], None). 957  
response to ('103.233.194.106', 61257): 404. 95710883-e1b9-4ba8-a2d8-9f381b57161d
```

```
HEAD request from ('60.177.39.7', 55035): ('/2.php', ['User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.1025  
103.56.112.82\r\n'], None). 3f679959-b61d-42fb-8fb9-8752f11a546a  
response to ('60.177.39.7', 55035): 404. 3f679959-b61d-42fb-8fb9-8752f11a546a  
HEAD request from ('60.177.39.7', 55035): ('/admin.php', ['User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.  
ost: 103.56.112.82\r\n'], None). 3f679959-b61d-42fb-8fb9-8752f11a546a  
response to ('60.177.39.7', 55035): 404. 3f679959-b61d-42fb-8fb9-8752f11a546a  
HEAD request from ('60.177.39.7', 55035): ('/login.php', ['User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.0.  
ost: 103.56.112.82\r\n'], None). 3f679959-b61d-42fb-8fb9-8752f11a546a  
response to ('60.177.39.7', 55035): 404. 3f679959-b61d-42fb-8fb9-8752f11a546a  
HEAD request from ('60.177.39.7', 55035): ('/02nfdiy.php', ['User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.19 (KHTML, like Gecko) Chrome/18.  
Host: 103.56.112.82\r\n'], None). 3f679959-b61d-42fb-8fb9-8752f11a546a  
response to ('60.177.39.7', 55035): 404. 3f679959-b61d-42fb-8fb9-8752f11a546a
```

增加了对于TransactionID的识别与应答
增加了对于功能码90的识别与应答
配合conpot更容易被网络搜索引擎发现

应对探索


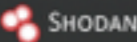
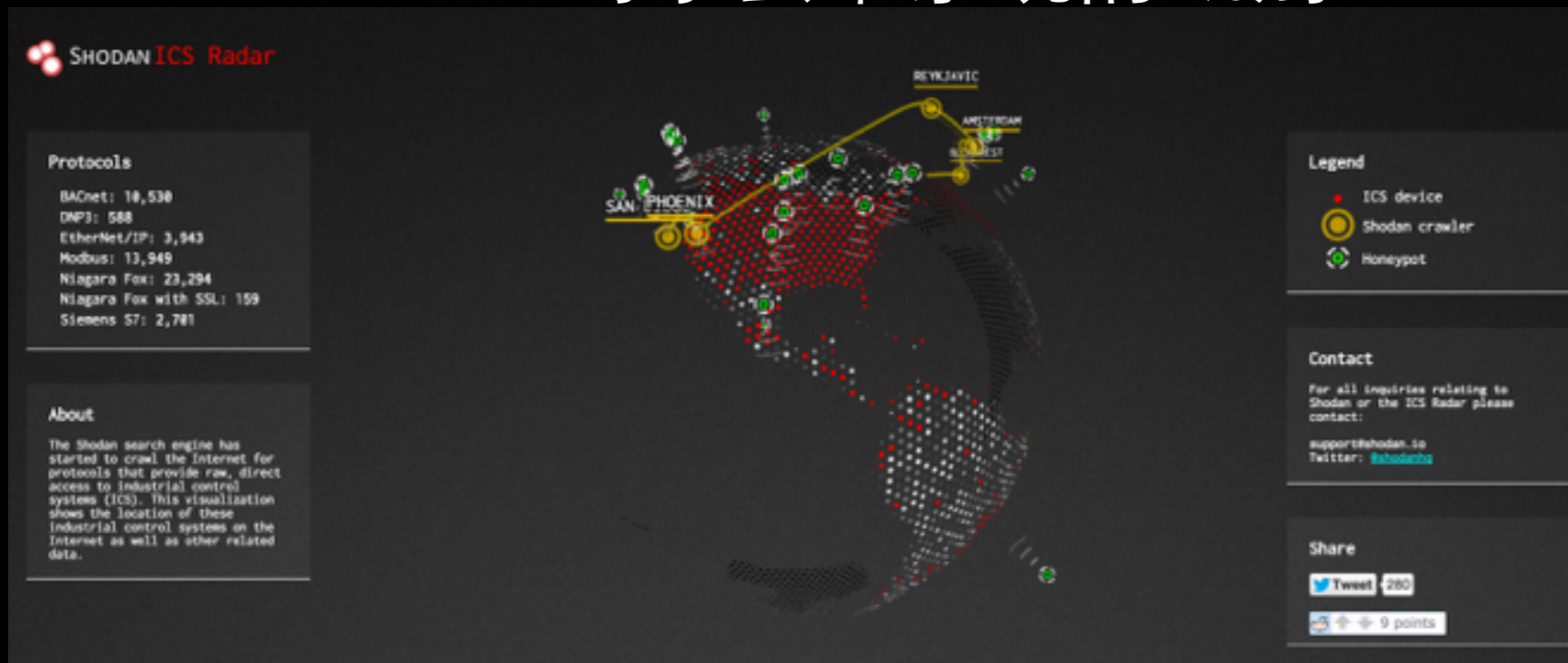
[工控蜜罐]
发现

198.	20.	70.114	Shodan
71.	6.216.	34	Rapid7
169.	54.233.	119	Credit Suisse Group / CANA
185.	35.	62. 11	Switzerland Group
85.	25.185.	112	BSB-Service GmbH Germany
62.	75.207.	109	Intergen AG Germany
178.	19.104.	138	Livenet sp. z o.o.
141.212.122.	xxx		University of Michigan College of Engineering

蜜罐捕获数据主要为协议扫描
其中严重的威胁为对地址数据的改写

应对探索

Shodan对于蜜罐系统的甄别



Honeypot Or Not?

Enter an IP to check whether it is a honeypot or a real control system:

Please enter an IP...

Looks like a real system!

应对探索

蜜罐甄别方法

Function code	1 Byte	0x2B
MEI Type*	1 Byte	0x0E
Read Device ID code	1 Byte	01 / 02 / 03 / 04
Object Id	1 Byte	0x00 to 0xFF

```
Scan start...
+++++send
0000  00 00 00 00 00 05 00 2B 0E 04 80 .....+...
None
+++++recv
0000  00 00 00 00 00 03 00 AB 02 .....
None
recv.functionId != 43
Read Device Identification Error, error code: '\x02'
```

Real

```
Scan start...
+++++send.
0000  00 00 00 00 00 05 00 2B 0E 04 80 .....+...
None
+++++recv
0000  00 00 00 00 00 32 00 2B 0E 01 81 00 00 03 00 14 .....2.+.....
0010  53 63 68 6E 65 69 64 65 72 20 45 6C 65 63 74 72 Schneider Electr
0020  69 63 20 20 01 0C 42 4D 58 20 50 33 34 20 32 30 ic ..BMX P34 20
0030  32 30 02 04 76 32 2E 32 20..v2.2
None
```

Honey

对于43(0x2B)功能码中的异常数据的应答

应对探索

蜜罐甄别方法

Function code	1 Byte	0x01
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of coils	2 Bytes	1 to 2000 (0x7D0)

```
qmwang@MacBook-Pro:~/Documents/workspace/ModTest% python ModTest.py -f 1 -d '\x00\x13\x00\x13\x00' 24.159.192.236 -v
Scan start...
24.159.192.236:502...
-----send package:
0000 00 00 00 00 00 07 00 01 00 13 00 13 00
None
-----recv package:
0000 00 00 00 00 00 03 00 81 03
None
```

Real

```
qmwang@MacBook-Pro:~/Documents/workspace/ModTest% python ModTest.py -f 1 -d '\x00\x13\x00\x13\x00' 192.168.213.135 -v
Scan start...
192.168.213.135:502...
-----send package:
0000 00 00 00 00 00 07 00 01 00 13 00 13 00
None
-----recv package:
0000 00 00 00 00 00 06 00 01 03 55 56 57
None
```

Honey

对于01(0x01)功能码中的异常数据的应答

应对探索

工控蜜罐的必要性

- 发现网络空间扫面引擎IP地址，拦截扫描
- 了解扫描引擎的指纹识别方法，收集信息
- 掌握黑客的进一步攻击行为
- 收集异常数据中可能的0-Day
- 健壮蜜罐系统，使其更难被甄别，更好的伪装

应对探索

[Snort for ICS]

开源入侵检测

<https://www.snort.org>

<http://www.digitalbond.com/tools/quickdraw/>

SID	Message
1111001	Modbus TCP - Force Listen Only Mode
1111002	Modbus TCP - Restart Communications Option
1111003	Modbus TCP - Clear Counters and Diagnostic Registers
1111004	Modbus TCP - Read Device Identification
1111005	Modbus TCP - Report Slave ID
1111006	Modbus TCP - Unauthorized Read Request to a PLC
1111007	Modbus TCP - Unauthorized Write Request to a PLC
1111008	Modbus TCP - Illegal Packet Size, Possible DOS Attack
1111009	Modbus TCP - Non-Modbus Communication on TCP Port 502
1111010	Modbus TCP - Slave Device Busy Exception Code Delay
1111011	Modbus TCP - Acknowledge Exception Code Delay
1111012	Modbus TCP - Incorrect Packet Length, Possible DOS Attack
1111013	Modbus TCP - Points List Scan
1111014	Modbus TCP - Function Code Scan

Rule: 1111015	
SID	1111015
Message	Schneider Modicon Function Code 90 - Download Ladder Logic Started
Rule	alert tcp any any -> any 502 (flow: established,to_server; content: "[00 5a 01 34 00 01]"; msg: "Schneider Modicon Function Code 90 - Download Ladder Logic Started";sid:1111015;priority:2; threshold:type limit, track by_src, count 1 , seconds 60;)
Summary	UnityPro will download the Ladder Logic from the PLC upon connection to the PLC. This can also be done by a Metasploit Module. This would allow an attacker to gather information about the PLC and then change it to upload new logic to the PLC later.
Impact	Recon
Detailed Information	Modicon is a PLC brand that is released by Schneider Electric. The PLCs utilize the Modbus protocol with a proprietary function code (FC 90).
Affected Systems	Modicon PLCs
Attack Scenarios	An attacker with IP connectivity sends a requests to download the ladder logic from the PLC.
Ease of Attack	Simple. There are multiple tools that can be used to perform this task.
False Positives	None known
False Negatives	None known
Corrective Action	Identify if this host is allowed download the Ladder Logic.
Contributors	Stephen Hilt

应对探索

[ModbusSec]
协议传输身份认证

<http://www.digitalbond.com/tools/basecamp/>

{Ethernet | TCP | Modbus}

{Ethernet | TCP | Tunnel | Modbus}

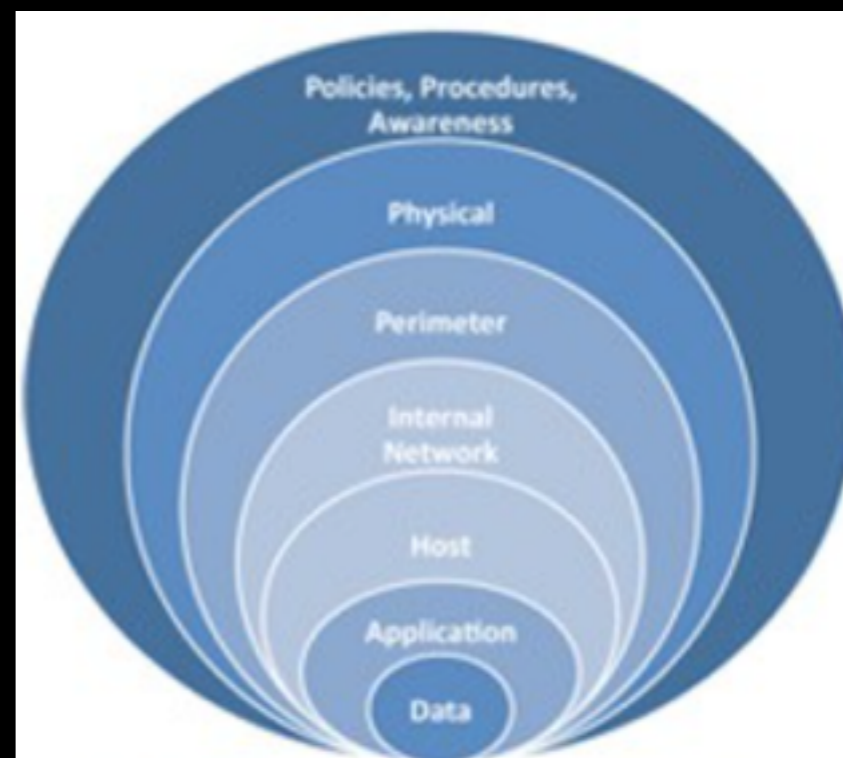
{Ethernet | TCP | Modbus | Tunnel | Modbus}

应对探索

[安全模块解决方案]

- 工业防火墙
- 网络隔离设备
- VPN接入
- 认证管理
- ...

纵深防御



Layers of Defense in Depth
Layers of Defense in Depth



工控安全联盟

感谢聆听