

# Exploit PLC on the internet

Z-0ne

什么是PLC  
为什么会联网

# 概述

# PLC

- Programmable Logic Controller
  - 电源
  - CPU
  - 存储
  - I/O
  - 网络模块



# PLC功能

- PLC功能
  - 顺序控制
  - 逻辑控制
- PLC应用
  - 自动化控制
  - 过程控制



# 其他

- PLC内核
  - Codesys
  - ProConos
- 底层操作系统
  - Linux
  - Vxworks
  - WinCE
- 通信协议
  - 通用
    - Modbus
  - 私有
    - S7
    - Omron FINS

```
<none> login: root

BusyBox v1.1.3 (2006.12.24-23:23+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# cd /mnt/fs
# ls
DEFAULT.CHK      ErrorInfo.35A      ahbus.ko          rta_server
DEFAULT.PRG      ErrorInfo.35A.bak   get_pid.ko        rts_client
DOWNLOAD.SDB     ErrorInfo.35B      hss.ko           rts_server
DiagnoseHw       ErrorInfo.35B.bak  mem1.txt         s3tty.ko
ErrorInfo.10A     ErrorInfo.36B      mkdosfs         sdcard.ko
ErrorInfo.10A.bak ErrorInfo.9B      ntp              startsh
ErrorInfo.10B     Gateway.cfg      persist.dat      ver
ErrorInfo.10B.bak ErrorInfo.11B    route            woyun
ErrorInfo.11B     InitGateway     rta              rta_client_socket
ErrorInfo.11B.bak LkRTS
```

# PLC通信

- 串行
  - RS232/485
- 专用
  - MPI
- 以太网
  - TCP/IP
  - UDP

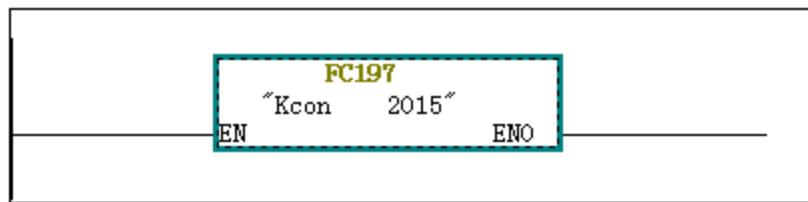


# 网络武器的目标

- Stuxnet作为网络武器其最终的目标也是西门子PLC
  - 劫持通信
  - 注入自己的逻辑程序

程序段 3: 标题:

注释:



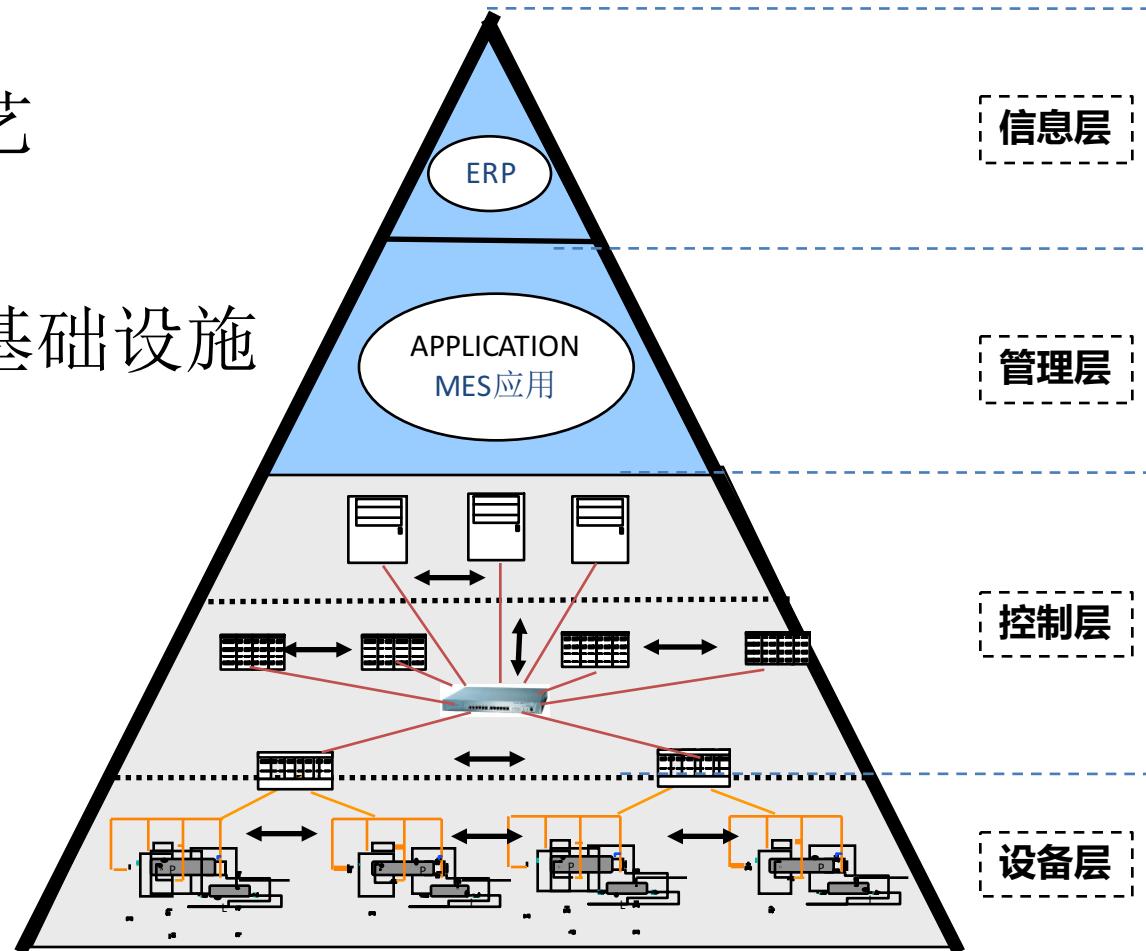
# 联网的隐患(1)

- PLC暴露在互联网是比SCADA更大的安全隐患
  - 未授权访问
  - 设备的用户等级保护缺失
  - 通信协议的脆弱性

```
+ Internet Protocol Version 4, Src: 192.168.1.209 (192.168.1.209), Dst: 192.168.1.209 (192.168.1.209)
+ Transmission Control Protocol, Src Port: 34407 (34407), Dst Port: 502 (502), Seq: 1, Len: 6
  Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 1
  Modbus
    Function Code: Write Single Coil (5)
    Reference Number: 7
    Data: ff00
    Padding: 0x00
0000  00 0c 29 62 23 63 00 00  00 00 01 40 08 00 45 00  ..)b#c... ...@..E.
0010  00 40 15 40 40 00 40 06  00 00 c0 a8 01 d1 c0 a8  .@.@@. @. .....
0020  01 16 86 67 01 f6 30 0d  ea 14 f7 cd c3 b4 80 18  ...g..0. .....
0030  40 f7 84 6a 00 00 01 01  08 0a 00 f3 64 5f 00 00  @..j.... ....d..
0040  14 de 00 00 00 00 00 06  01 05 00 07 ff 00  ..... .@...@...
```

# 联网的隐患(2)

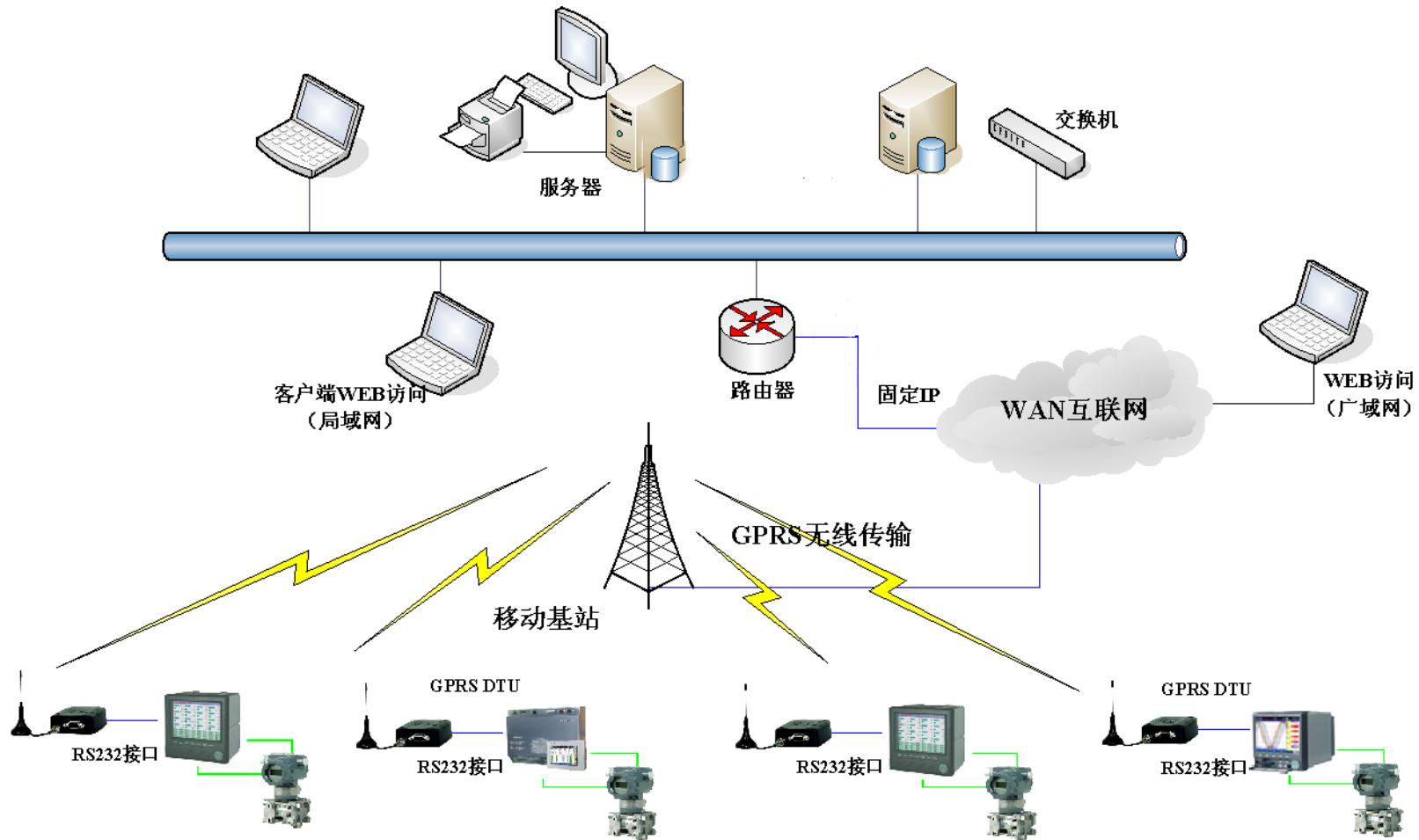
- PLC暴露在互联网是比SCADA更大的安全隐患
  - 控制流程工艺
  - 位于更底层
  - 可能为关键基础设施



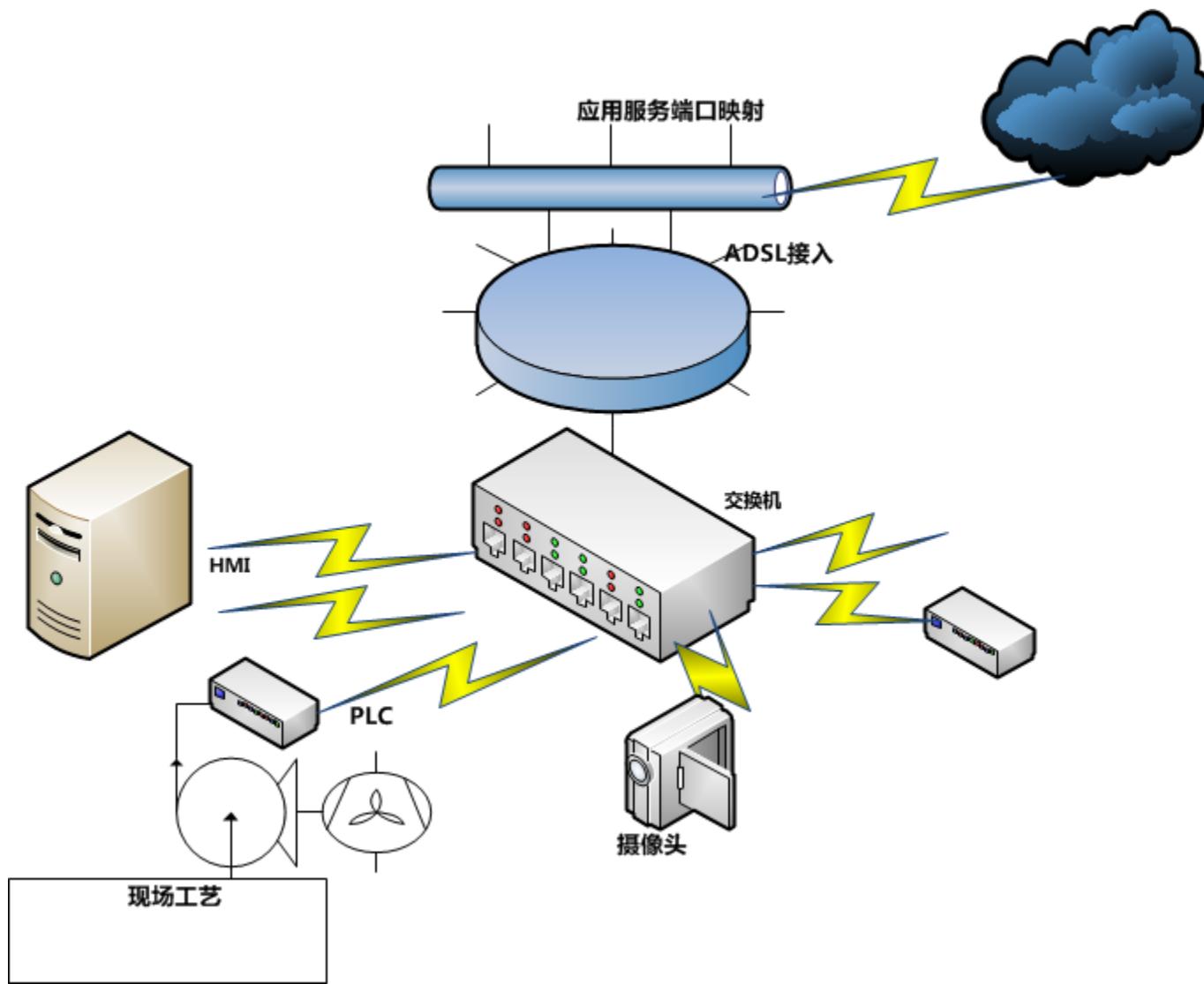
# 联网的趋势

- 远程数据通信/远程维护催生了联网的需求
  - 方便、快捷
  - 减少了现场运维的成本
  - 统一管理

# 联网的解决方案(1)



# 联网的解决方案(2)



# 联网的解决方案(2)

NR238

+ 首页

> 系统状态

> 外网接入配置

> 内网接入配置

> QoS

> 上网行为管理

> 网络安全

> 高级设置

- 虚拟服务
- 动态域名
- 静态路由
- 动态路由
- DMZ
- UPnP
- 应用网关
- FTP私有端口
- 域名解析

高级设置 >> 虚拟服务 >> 虚拟服务

虚拟服务

帮助 ?

虚拟服务列表

序列号	虚拟服务名称	内网主机IP地址	协议	外部端口	内部端口	操作
1	plc	192.168.1.12	tcp	502	502	
2	3	192.168.1.2	tcp	554	554	
3	2	192.168.1.2	tcp	8000	8000	
4	1	192.168.1.2	tcp	80	80	

每页: 10  条 首页 上一页 下一页 尾页 1/1 总数:32 条 已用:4 条 删除全部 增加

西门子PLC全球统计报告

西门子PLC公网蜜罐统计

西门子S7协议 蜜罐应用案例

联网的风险案例

# **PLC ON THE INTERNET**



CPU313C

SF

SIEMENS

PLC5

MAINT  
DC5V  
FRCE  
RUN  
STOP

PUSH

RUN  
STOP  
MRES

SIMATIC  
S7-300

X1  
4  
5  
6

313-5BG04-0AB0

DI16/D016xDC24V

0 1 2 3 4 5 6 7  
DI=2 IN

CP 343-1 Lean

SF  
BF  
DC5V  
RX/TX  
RUN  
STOP

X1P1  
X1P2  
MAINT

SIMATIC NET

343-1CX10-0XE0

X1  
8  
9  
10

# 西门子PLC CPU模块全球统计报告(1)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - <http://www.zoomeye.org/search?q=port%3A102>
  - <https://www.shodan.io/search?query=Module+port%3A102>
- 全球数据 (能成功读出模块型号的数据)
  - ZoomEye → 1446
  - Shodan → 2749
  - Plcscan.org → 2215

# 西门子PLC CPU模块全球统计报告(2)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - Nmap → s7-enumerate.nse(TSAP:0102)
  - PG mode
  - Rack:0 Slot:2

```
Completed NSE at 11:57, 0.10s elapsed
Nmap scan report for 192.168.1.200
Host is up, received arp-response <0.0013s latency>.
Scanned at 2015-08-16 14:39:36 中国标准时间 for 1s
PORT      STATE SERVICE REASON
102/tcp    open  iso-tsap syn-ack
| s7-enumerate:
|   Module: 6ES7 313-5BG04-0AB0
|   Basic Hardware: 6ES7 313-5BG04-0AB0
|   Version: 3.3.10
|   System Name: SIMATIC 300<1>
|   Module Type: CPU 313C
|   Serial Number: S Q-EOU072842014
|   Copyright: Original Siemens Equipment
|   Blocks Name: Count<Num>
|   OB: 2
|   FB: 5
|   FC: 1
|   DB: 10
|   SDB: 12
|   SFC: 64
|   SFB: 17
MAC Address: 00:1B:1B:CC:E4:52 <Siemens AG,>
Service Info: Device: specialized
Final times for host: srtt: 1250 rttvar: 4250  to: 100000
```

# 西门子PLC CPU模块全球统计报告(3)

- 国家排行

- 德国 350
- 意大利 255
- 美国 179
- 西班牙 146
- 土耳其 124
- 波兰 113
- 法国 108
- 捷克 74
- 丹麦 67
- 奥地利 64

# 西门子PLC CPU模块全球统计报告(4)

- 模块货号排行

– 6ES7 214-1AG31-0XB0	145
– 6ES7 214-1AE30-0XB0	142
– 6ES7 212-1HE31-0XB0	129
– 6ES7 315-2AG10-0AB0	129
– 6ES7 151-8AB01-0AB0	121
– 6ES7 315-2EH14-0AB0	120
– 6ES7 315-2AH14-0AB0	88
– 6ES7 214-1BG31-0XB0	74
– 6ES7 314-6EH04-0AB0	74
– 6ES7 313-5BF03-0AB0	73

# 西门子PLC CPU模块全球统计报告(5)

• 固件版本排行	
– Version: 3.0.2	472
– Version: 2.2.0	142
– Version: 2.6.0	113
– Version: 4.0.0	96
– Version: 2.6.11	76
– Version: 3.2.10	76
– Version: 3.2.6	69
– Version: 3.3.8	59
– Version: 3.2.3	59
– Version: 3.2.8	55

# 西门子PLC CP模块全球统计报告(1)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - Nmap → s7-enumerate.nse(TSAP:0100)
  - Rack:0 Slot:0
- 全球数据(能成功读出模块型号的数据)
  - Plcscan.org → 486

# 西门子PLC CP模块全球统计报告(2)

- 使用S7协议(TCP/102)对互联网进行扫描探测
  - Nmap → s7-enumerate.nse(TSAP:0100)
  - PG mode
  - Rack:0 Slot:0

```
Nmap scan report for 192.168.1.200
Host is up, received arp-response <0.0020s latency>.
Scanned at 2015-08-16 14:40:11 中国标准时间 for 1s
PORT      STATE SERVICE REASON
102/tcp    open  iso-tsap syn-ack
! s7-enumerate:
!: Module: 6GK7 343-1CX10-0XE0 \xAC\xDBuG
!: Basic Hardware: 6GK7 343-1CX10-0XE0 \xAC\xDB
!: Version: 3.0.23
!: Blocks Name: Count<Num>
!: OB: 0
!: FB: 0
!: FC: 0
!: DB: 0
!: SDB: 3
!: SFC: 0
!_ SFB: 0
MAC Address: 00:1B:1B:CC:E4:52 (Siemens AG, )
Service Info: Device: specialized
Final times for host: srtt: 2000 rttvar: 3750 to: 1000000
```

# 西门子PLC CP模块全球统计报告(3)

- 国家排行

- 意大利 91
- 德国 76
- 西班牙 32
- 法国 29
- 瑞士 26
- 捷克 25
- 丹麦 23
- 美国 18
- 波兰 14
- 中国 14

# 西门子PLC CP模块全球统计报告(4)

- 模块货号排行

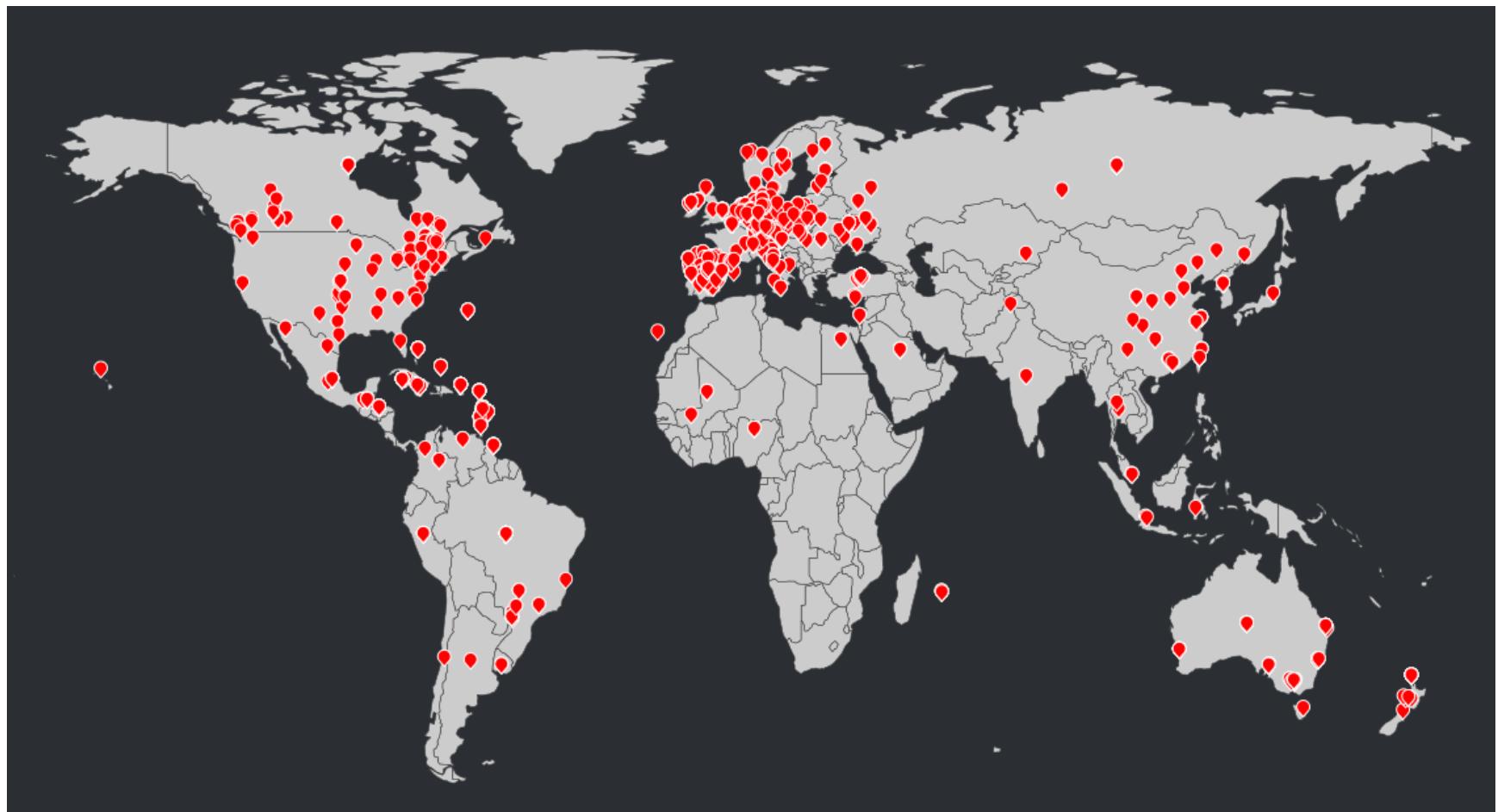
– 6GK7 343-1CX10-0XE0	305
– 6GK7 343-1EX30-0XE0	70
– 6GK7 343-1CX00-0XE0	19
– 6GK7 343-1EX11-0XE0	18
– 6GK7 443-1EX20-0XE0	16
– 6GK7 443-1EX11-0XE0	14
– 6GK7 343-1EX21-0XE0	14
– 6GK7 343-1EX20-0XE0	13
– Unknown	4
– 6GK7 343-1GX21-0XE0	3

# 西门子PLC CP模块全球统计报告(5)

- 固件版本排行

– Version: 3.0.23	104
– Version: 2.3.2	79
– Version: 2.0.16	60
– Version: 2.6.0	56
– Version: 2.1.14	31
– Version: 2.2.20	22
– Version: 1.1.5	15
– Version: 2.5.0	14
– Version: 1.2.3	9
– Version: 1.0.26	8

# 西门子PLC全球分布图形化统计



# 西门子PLC 蜜罐统计报告(1)

- Conpot
  - 不推荐默认配置
  - 特征
    - S7(TCP/102)
      - Serial number of module: 88111222
- 全球数据
  - ZoomEye → 48
  - Shodan → 61
  - Plcscan.org → 30

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

# 西门子PLC 蜜罐统计报告(2)

SHODAN

88111222 port:102

Explore Contact Us Blog Enterprise Access

Exploits Maps Download Results Create Report

## TOP COUNTRIES



United States	12
Japan	12
Germany	5
Taiwan, Province of China	2
Netherlands	1

## TOP ORGANIZATIONS

Open Computer Network	10
DigitalOcean	3
Amazon	2
iCare.com Ltd	1
Viasat Communications	1

Showing results 1 - 10 of 61

**153.222.88.168**

p25168-ipngn3201funabasi.chiba.ocn.ne.jp  
Open Computer Network

Added on 2015-08-14 11:19:40 GMT

• Japan  
[Details](#)

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**

**45.55.198.19**

Added on 2015-08-14 09:24:08 GMT

[Details](#)

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**

# 西门子S7协议 蜜罐应用案例(1)

- 通过监听TCP/102端口并仿真S7协议收集扫描信息
  - 记录连入端口的IP、时间
  - 回复伪装的模块信息
  - 输出协议操作的详细日志

# 西门子S7协议 蜜罐应用案例(2)

2015-07-09 09:27:20 [71.6.167.142] Client added

2015-07-09 09:27:20 [71.6.167.142] The client requires a PDU size of 480 bytes

2015-07-09 09:27:20 [71.6.167.142] Client added

2015-07-09 09:27:21 [71.6.167.142] The client requires a PDU size of 480 bytes

2015-07-09 09:27:21 [71.6.167.142] Read SZL request, ID:0x0011 INDEX:0x0001 --> OK

2015-07-09 09:27:21 [71.6.167.142] Read SZL request, ID:0x001c INDEX:0x0001 --> OK

2015-07-09 09:27:21 [71.6.167.142] Client disconnected by peer

2015-07-09 09:27:25 [71.6.167.142] Client disconnected by peer

C:\Users\Administrator>nslookup 71.6.167.142

服务器: google-public-dns-a.google.com

Address: 8.8.8.8

名称: census9.shodan.io

Address: 71.6.167.142

# 西门子S7协议 蜜罐应用案例(3)

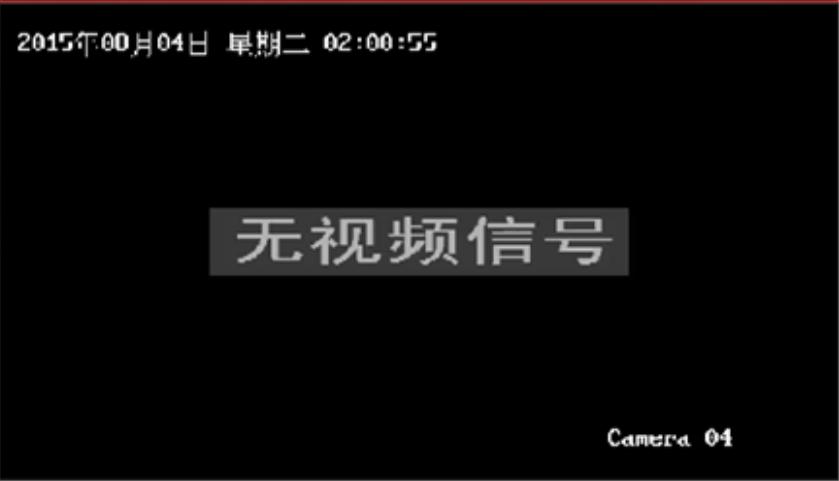
2015-05-06 19:53:49 [5.61.38.11] Client added  
2015-05-06 19:53:55 [5.61.38.11] Client added  
2015-05-06 19:53:58 [5.61.38.11] The client requires a PDU size of 480 bytes  
2015-05-06 19:53:58 [5.61.38.11] Client disconnected by peer  
2015-05-06 19:53:59 [5.61.38.11] Read S7L request, ID:0x0011 INDEX:0x0000 --> OK  
2015-05-06 19:53:59 [5.61.38.11] Read S7L request, ID:0x001c INDEX:0x0000 --> OK  
2015-05-06 19:54:00 [5.61.38.11] Read S7L request, ID:0x0132 INDEX:0x0004 --> OK  
2015-05-06 19:54:02 [5.61.38.11] Block of type OB list requested (start sequence) --> NOT AVAILABLE  
2015-05-06 19:54:03 [5.61.38.11] Block of type FB list requested (start sequence) --> NOT AVAILABLE  
2015-05-06 19:54:03 [5.61.38.11] Block of type FC list requested (start sequence) --> NOT AVAILABLE  
2015-05-06 19:54:03 [5.61.38.11] Block of type DB list requested (start sequence) --> OK  
2015-05-06 19:54:04 [5.61.38.11] Block info requested DB 1 --> OK  
2015-05-06 19:54:04 [5.61.38.11] Block info requested DB 2 --> OK  
2015-05-06 19:54:05 [5.61.38.11] Block info requested DB 3 --> OK

# 针对数据的验证(1)

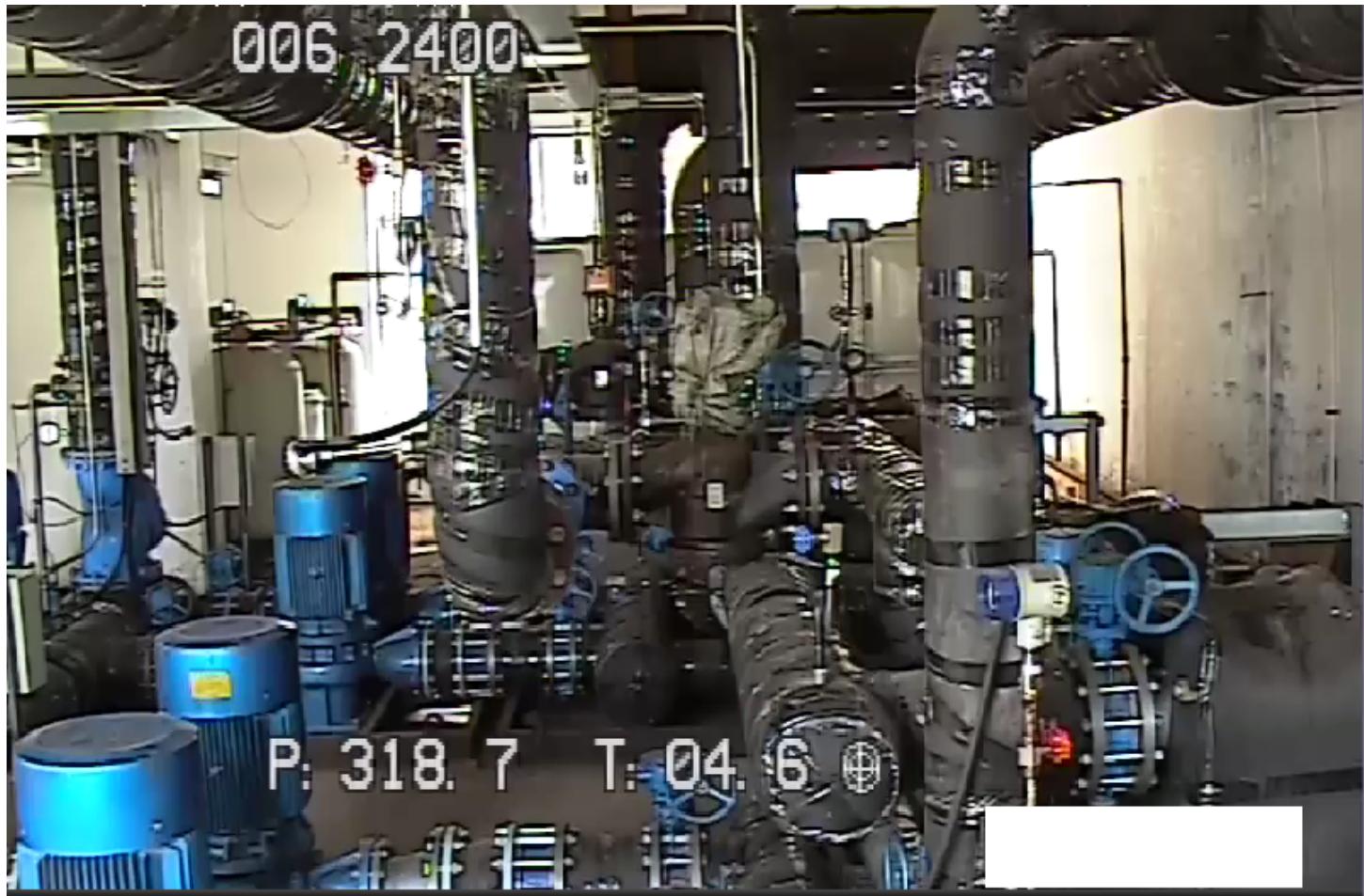


无视频信号

# 针对数据的验证(2)



# 针对数据的验证(3)



# 针对数据的验证(4)



# 针对数据的验证(5)



# 针对数据的验证(6)



S7-300 PLC的等级保护功能

S7-300 PLC的等级保护功能缺陷

S7协议对口令密码传输的缺陷

S7-300 PLC内部程序字节码的转换

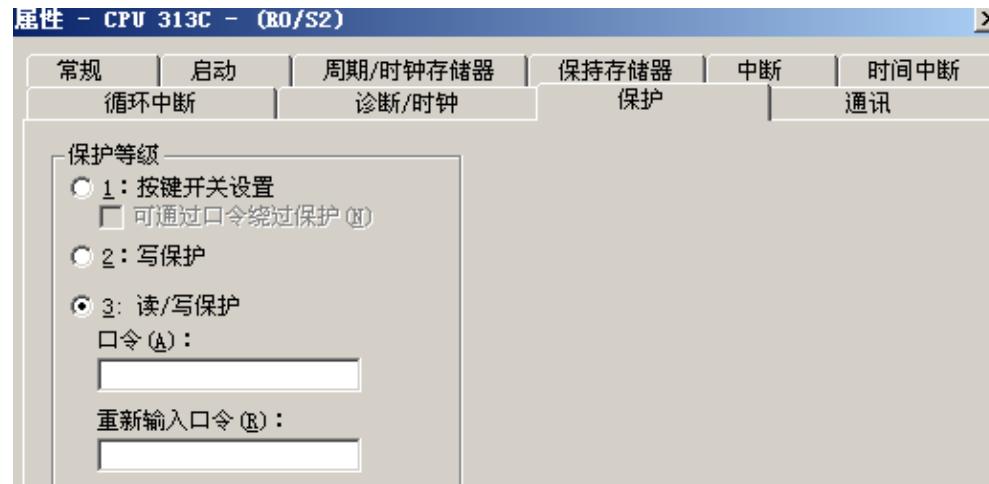
利用TCP/UDP连接功能实现端口扫描

利用通信功能块实现特定Socket通信

## **EXPLOITS S7 PLC**

# S7-300的等级保护(1)

- 口令保护
  - 来自Step7帮助文件
    - “保护CPU中的用户程序，防止未授权的修改(写保护)”
    - “保护用户程序的编程技术内容(读保护)”
    - “防止将会干涉进程的在线功能”



# S7-300的等级保护(2)

## • 口令保护帮助

### "保护"标签

如果CPU提供SFC 109 "PROTECT"，则可使用该SFC来增大保护级别，也可以将保护级别重新设置为所组态的数值。

#### 如果设置口令保护级别：

- 已授权用户具有读写访问权限，不考虑钥匙开关的位置以及设置的保护级别。总之，如果以MODE=12调用SFC?09 "PROTECT"，则即使具有
- 下列限制适用于未授权用户：
  - 保护级别1：钥匙开关设置
  - 保护级别2：写保护，与键开关位置无关
  - 保护级别3：读/写保护，与键开关位置无关

#### 注意：

口令的最大长度为8个字符。

#### 口令保护的模块在操作中的特性：

在执行在线功能之前，将检查授权并提示用户输入口令。

**实例：**模块已设置为保护级别2，并且您希望执行"修改变量"功能。要执行此写访问功能，必须输入口令。

或者，不考虑在线功能的类型，您可以在SIMATIC管理器中输入受保护模块的口令：

1. 在SIMATIC管理器中，选择受保护的模块或者其S7程序。
2. 选择菜单命令PLC > 授权 > 设置，然后在下一个对话框中输入口令。

输入口令后，在退出上一个S7应用程序或取消访问权限(PLC > 授权 > 取消)之前，该授权将始终有效。

#### 注意：

# S7-300的等级保护缺陷

- 帮助文件对口令保护注意事项的定义
  - “无法限制过程控制、监视和通信功能。例如，无法使用口令保护来防止对“设置时间/日期”功能的访问。”
- 其他“例如”
  - 启用LV2/LV3也可以操作CPU工作状态

# S7协议对口令密码传输的弱加密(1)

```
+ INTERNET PROTOCOL version 4, Src: 192.168.1.25 (192.168.1.25), Dst: 192.168.1.22 (192.168.1.22)
+ Transmission Control Protocol, Src Port: 5277 (5277), Dst Port: 102 (102), Seq: 446, Ack: 862, Len:
+ TPKT, Version: 3, Length: 37
+ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
S7 Communication
+ Header: (Userdata)
  Parameter: (Request) ->(Security) ->(PLC password)
    Parameter head: 0x000112
    Parameter length: 4
    Unknown (Request/Response): 0x11
    0100 .... = Type: Request (4)
    .... 0101 = Function group: Security (5)
    Subfunction: PLC password (1)
    Sequence number: 0
  Data
    Return code: Success (0xff)
    Transport size: OCTET STRING (0x09)
    Length: 8
    Data: 6467021277670212
0000  00 0c 29 62 23 63 00 50  56 c0 00 01 08 00 45 00  ..)b#c.P V.....E.
0010  00 59 42 c2 00 00 40 06  b4 5f c0 a8 01 17 c0 a8  .YB...@. ...-----
0020  01 16 14 9d 00 66 65 cb  ed a4 ec 64 e2 eb 80 18  ....fe. ...d.....
0030  40 08 13 2d 00 00 01 01  08 0a 00 18 17 7d 00 01  @...-... ....}...
0040  41 69 03 00 00 25 02 f0  80 32 07 00 00 cf 1e 00  Ai...%. 2.....
0050  08 00 0c 00 01 12 04 11  45 01 00 ff 09 00 08 64  ..... E.....d
0060  67 02 12 77 67 02 12  g..wg..
```

# S7协议对口令密码传输的弱加密(2)

- Hydra已集成基于S7协议的口令破解模块

```
// Fill Data
ReqData->Ret      =0xFF;
ReqData->TS        =TS_ReqOctet;
ReqData->DLen      =SwapWord(0x0008); // 8 bytes data : password
// Encode the password
ReqData->Pwd[0]=opData[0] ^ 0x55;
ReqData->Pwd[1]=opData[1] ^ 0x55;
for (c = 2; c < 8; c++){
    ReqData->Pwd[c]=opData[c] ^ 0x55 ^ ReqData->Pwd[c-2];
};

IsoSize=sizeof(TS7ReqHeader)+sizeof(TReqFunSecurity)+sizeof(TReqDataSecurity);
Result=isoExchangeBuffer(0,IsoSize);

// Get Return
if (Result==0)
{
    if (ResParams->Err!=0)
        Result=CpuError(SwapWord(ResParams->Err));
};

return Result;
```

# S7-300 MC7字节码的传输

The screenshot displays two software interfaces side-by-side. On the left is the SIMATIC Manager (TIA Portal) interface for a SIMATIC 300 station. The central area shows a ladder logic program with two main sections: '程序段 1: 标题' containing 'TEST1' and '程序段 2: 标题' containing 'TEST2'. Each section has a coil labeled 'M0.1' and a contact labeled 'Q0.1' or 'Q0.2'. On the right is the Wireshark network traffic capture window titled '\*本地连接 2 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]'. The filter bar at the top shows 'tcp.port == 102'. The list view shows multiple TCP packets exchanged between the local host (172.18.15.104) and another host (172.18.15.142). The details view for the selected packet shows the protocol as S7COMM, length as 237 bytes, and the data payload as hex and ASCII. The hex dump reveals the S7-300 MC7 byte code structure.

No.	Time	Source	Destination	Protocol	Length	Info
166	4.60133200	172.18.15.142	172.18.15.104	S7COMM	237	ROSCTR:[Ack_Dat]
167	4.60282600	172.18.15.104	172.18.15.142	TCP	60	iso-tsap > arbo
168	4.60397100	172.18.15.104	172.18.15.142	TCP	60	iso-tsap > arbo
171	4.65702900	172.18.15.104	172.18.15.142	S7COMM	89	ROSCTR:[Job]
172	4.65719100	172.18.15.142	172.18.15.104	COTP	61	DT TPDU (0) [co
173	4.65738800	172.18.15.142	172.18.15.104	S7COMM	74	ROSCTR:[Ack_Dat]
174	4.65863200	172.18.15.104	172.18.15.142	TCP	60	iso-tsap > arbo
175	4.65974200	172.18.15.104	172.18.15.142	TCP	60	iso-tsap > arbo
176	4.69531800	172.18.15.142	172.18.15.104	S7COMM	97	ROSCTR:[Job]
177	4.69676800	172.18.15.104	172.18.15.142	TCP	60	iso-tsap > arbo
178	4.72158100	172.18.15.104	172.18.15.142	S7COMM	74	ROSCTR:[Ack_Dat]
179	4.72171900	172.18.15.142	172.18.15.104	COTP	61	DT TPDU (0) [co
180	4.72312200	172.18.15.104	172.18.15.142	TCP	60	iso-tsap > arbo

# MC7 字节码转换(1)

- 研究目的与意义
  - 脱离官方编译器S7kafapx.exe实现对PLC程序的转换与修改
  - S7协议大量字段已被解码但是程序下载功能未被解码
  - Stuxnet核心功能
- 故事

# MC7 字节码转换(2)

- S7-300 PLC程序块解析

- 组织块（OB）（主程序块负责所有FC程序块的调用）
- 数据块（DB）（用于存放用户和系统定义的变量数据）
- 程序块（FC）（由用户编写的程序块）
- 功能块（FB）（由用户编写的专用数据块）
- 系统程序块（SFC）（调用系统某些功能时自动创建）
- 系统功能块（SFB）（调用系统某些数据功能时自动创建）
- 系统数据块（SDB）（由编程软件自动生成主要存放PLC的硬件组态等信息，用户无法直接打开和更改）

# MC7 字节码转换(3)

- 70 70 //MC7开始头部标志
- 01 01
- 02 //块创建的语言 hex:0x02 LAD (KOP)
- 08 //块类型 hex:0x08 OB
- 00 01 //块编号 hex:0x00,0x01
- 00 00 00 96 //块总长度
- 00 00 00 00 //是否设置密码
- 03 22 C8 2E 2C 20 //最后修改时间
- 03 9D CB 0C 11 4C //上次修改时间
- 00 1C //内部块数据表长度
- 00 30
- 00 14 //本地数据长度
- 00 02 //MC7执行代码长度

# MC7 注入实例(1)

STL:

A M 8.0

AN T 6

L S5T#3S

SD T 0

NOP 0

NOP 0

NOP 0

NOP 0

STL:

A T 0

= L 20.0

A L 20.0

BLD 102

= Q 124.0

A L 20.0

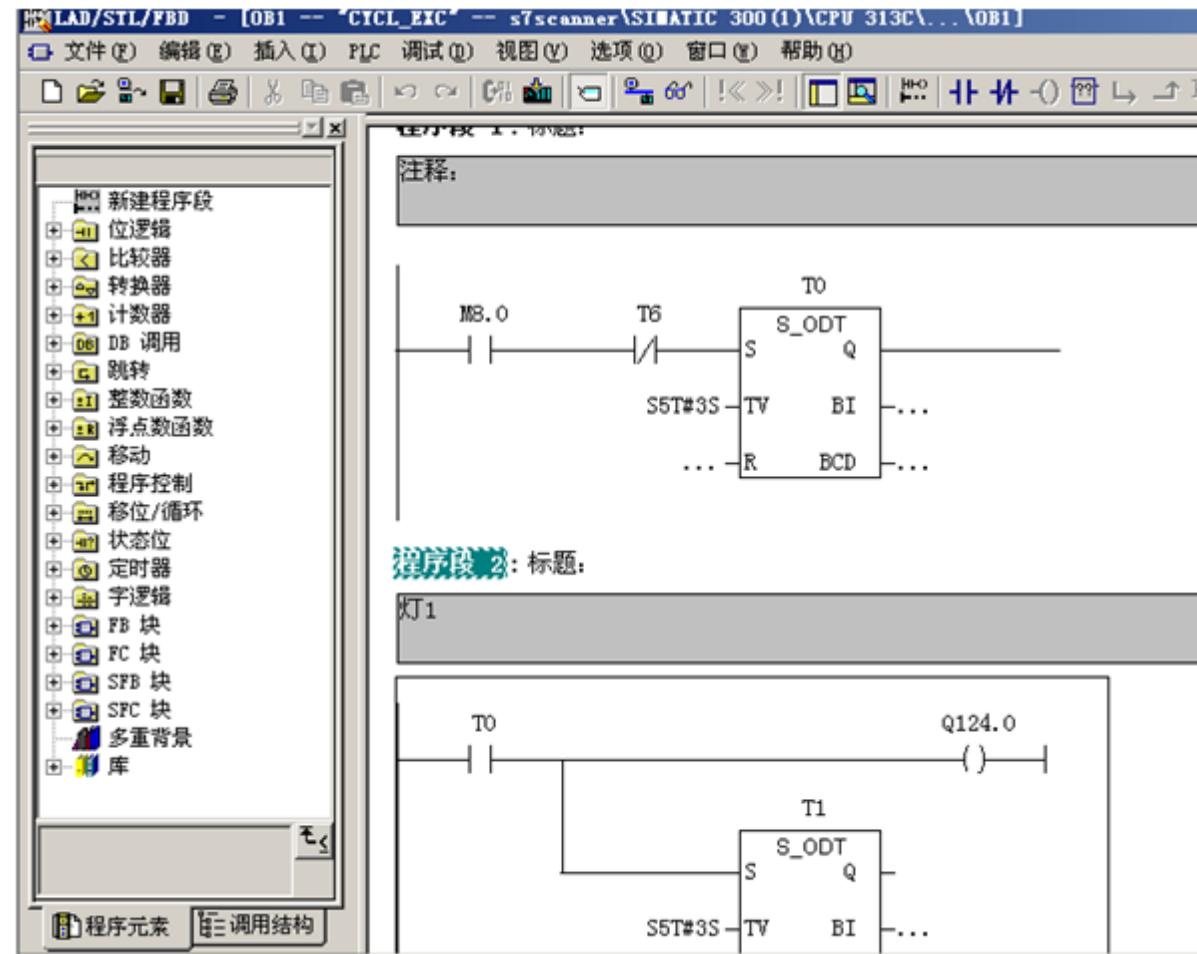
L S5T#3S

SD T 1

NOP 0

NOP 0

NOP 0



# MC7 注入实例(2)

序号	源IP	目的IP	协议	描述
4	0.646.192.168.1.200	192.168.1.209	S7COMM	
5	0.646.192.168.1.209	192.168.1.200	S7COMM	
6	0.648.192.168.1.200	192.168.1.209	TCP	
7	0.678.192.168.1.200	192.168.1.209	S7COMM	
8	0.679.192.168.1.209	192.168.1.200	S7COMM	
9	0.681.192.168.1.200	192.168.1.209	TCP	
10	0.703.192.168.1.200	192.168.1.209	S7COMM	
11	0.704.192.168.1.209	192.168.1.200	S7COMM	
12	0.705.192.168.1.200	192.168.1.209	TCP	
13	0.722.192.168.1.200	192.168.1.209	S7COMM	
89			ROSCTR:[Ack_Data]	Function:[Start upload]
79			ROSCTR:[Job]	Function:[Upload]
60	102-10036		[ACK]	Seq=36 Ack=61 Win=2048 Len=0
301			ROSCTR:[Ack_Data]	Function:[Upload]
79			ROSCTR:[Job]	Function:[Upload]
60	102-10036		[ACK]	Seq=283 Ack=86 Win=2048 Len=0
187			ROSCTR:[Ack_Data]	Function:[Upload]
79			ROSCTR:[Job]	Function:[End upload]
60	102-10036		[ACK]	Seq=416 Ack=111 Win=2048 Len=0
74			ROSCTR:[Ack_Data]	Function:[End upload]

Protocol Data Unit Reference: 2816  
Parameter length: 2  
Data length: 226  
Error class: No error (0x00)  
Error code: 0x00

Parameter: (Upload)  
Function: Upload (0xe)  
Parameter data: 01

Data  
Data: 00de00fb70700101020800010000014a000000000367c109...

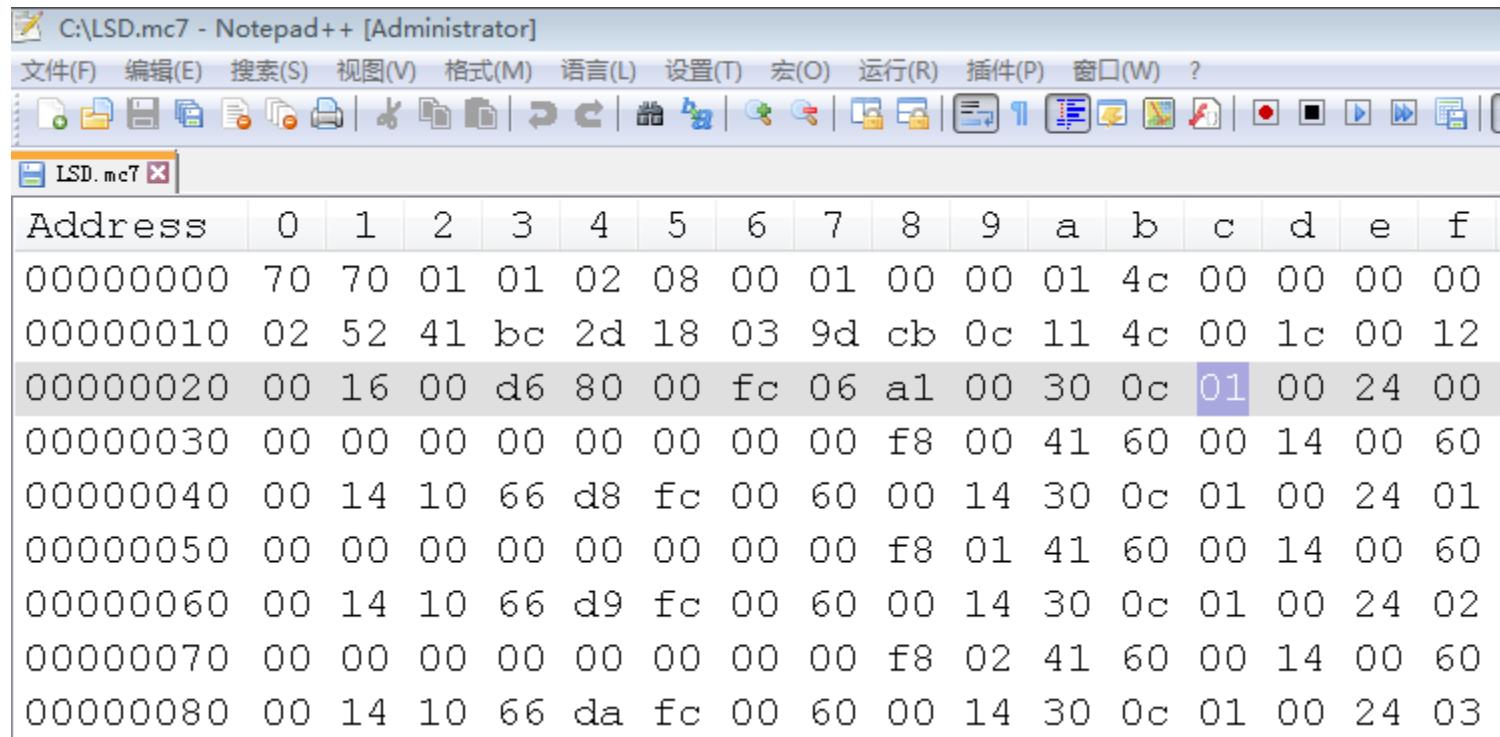
地址	十六进制值	字符显示
0030	08 00 fd 50 00 00 03 00 00 f7 02 f0 80 32 03 00	...P.....2..
0040	00 0b 00 00 02 00 e2 00 00 1e 01 00 de 00 fb 70	.....J..P.
0050	70 01 01 02 08 00 01 00 00 01 4a 00 00 00 00 03	g...-..L..
0060	67 c1 09 2d 18 03 9d cb 0c 11 4c 00 1c 00 12 00	.....0...\$..
0070	16 00 d4 80 08 fc 06 30 0c 03 00 24 00 00 00 00	.....A....
0080	00 00 00 00 00 f8 00 41 60 00 14 00 60 00 14 10	f...0...\$.
0090	66 d8 fc 00 60 00 14 30 0c 03 00 24 01 00 00 00	f...0...\$.
00a0	00 00 00 00 f8 01 41 60 00 14 00 60 00 14 10	f...0...\$.
00b0	66 d9 fc 00 60 00 14 30 0c 03 00 24 02 00 00 00	f...0...\$.
00c0	00 00 00 00 f8 02 41 60 00 14 00 60 00 14 10	f...0...\$.
00d0	66 dd fc 00 60 00 14 30 0c 03 00 24 03 00 00 00	f...0...\$.
00e0	00 00 00 00 f8 03 41 60 00 14 00 60 00 14 10	f...0...\$.
00f0	66 db fc 00 60 00 14 30 0c 03 00 24 04 00 00 00	f...0...\$.
0100	00 00 00 00 f8 04 41 60 00 14 00 60 00 14 10	f...0...\$.
0110	66 dc fc 00 60 00 14 30 0c 03 00 24 05 00 00 00	f...0...\$.
0120	00 00 00 00 f8 05 41 60 00 14 00 60	f...0...\$.

# MC7 注入实例(3)

// Word	
L 2#00000000	30 02 00 00
L 2#1111111111111111	30 02 FF FF
L W#16#0000	30 07 00 00
L W#16#FFFF	30 07 FF FF
L C#0	30 08 00 00
L c#999	30 08 09 99
L 0	30 03 00 00
L 255	30 03 00 FF
L 65535	30 03 FF FF
L -1	30 03 FF FF
L 'S'	30 05 00 53
L 'S7'	30 05 53 37
L S5T#0MS	30 0C 00 00
L S5T#10MS	30 0C 00 01
L S5T#1S	30 0C 01 00
L B#(0, 0)	30 06 00 00
L B#(255, 128)	30 06 FF 80
L D#1990-1-1	30 0A 00 00
L D#2009-8-22	30 0A 1C 05

# MC7 注入实例(4)

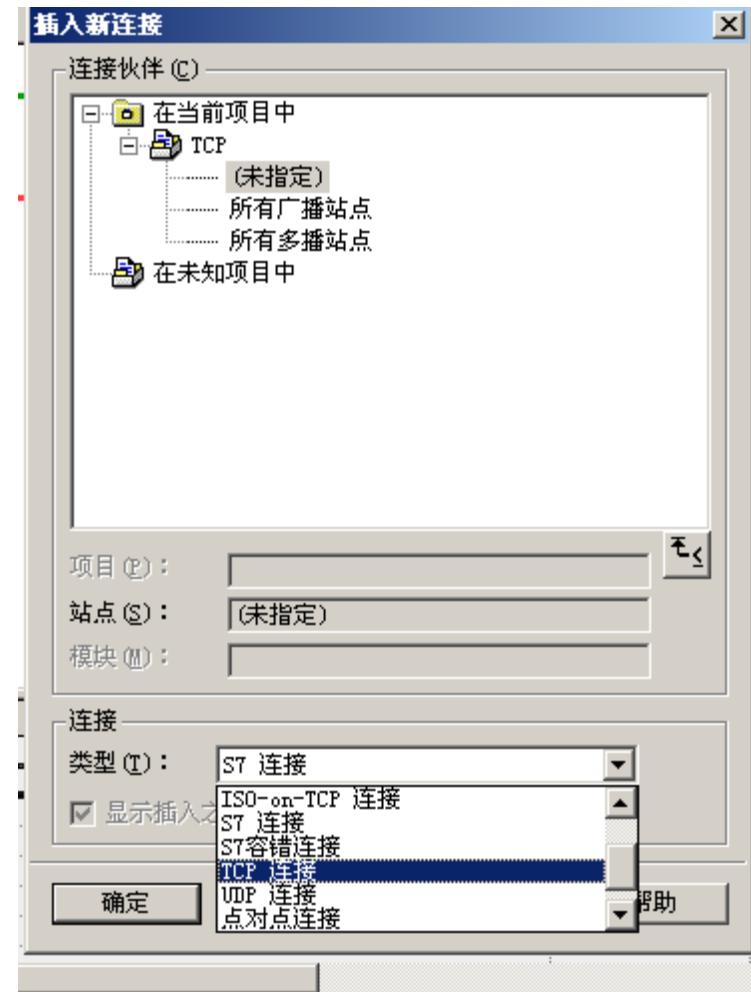
- 在无等级保护的情况下修改定时器的时间为1秒



Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00000000	70	70	01	01	02	08	00	01	00	00	01	4c	00	00	00	00
00000010	02	52	41	bc	2d	18	03	9d	cb	0c	11	4c	00	1c	00	12
00000020	00	16	00	d6	80	00	fc	06	a1	00	30	0c	01	00	24	00
00000030	00	00	00	00	00	00	00	00	f8	00	41	60	00	14	00	60
00000040	00	14	10	66	d8	fc	00	60	00	14	30	0c	01	00	24	01
00000050	00	00	00	00	00	00	00	f8	01	41	60	00	14	00	60	
00000060	00	14	10	66	d9	fc	00	60	00	14	30	0c	01	00	24	02
00000070	00	00	00	00	00	00	00	f8	02	41	60	00	14	00	60	
00000080	00	14	10	66	da	fc	00	60	00	14	30	0c	01	00	24	03

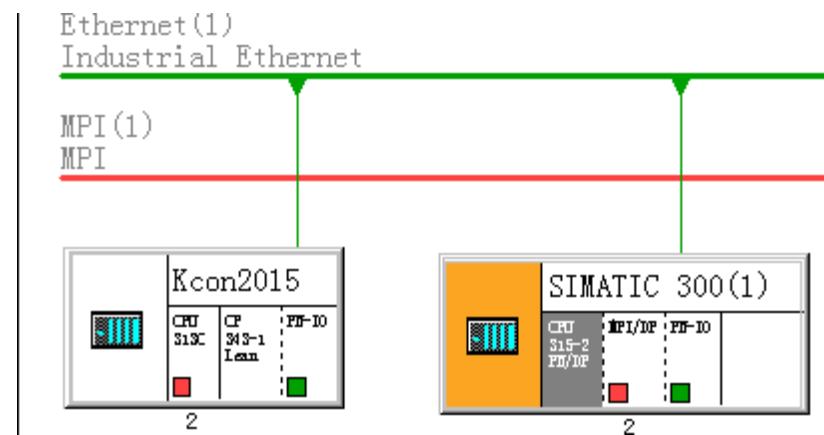
# S7 300 PLC支持多种连接方式

- 多种连接方式
  - S7连接
  - 冗余的S7连接
  - 点对点连接
  - FMS连接
  - FDL连接
  - ISO传输连接
  - ISO on TCP连接
  - TCP连接
  - UDP连接
  - 电子邮件连接



# S7 300 PLC支持多种连接对象

- 多种连接连接对象
  - 相同型号PLC CPU与PLC CPU之间通信
  - 不同型号PLC CPU与PLC CPU之间通信
  - PLC与上位机之间通信
  - PLC与其他以太网设备通信



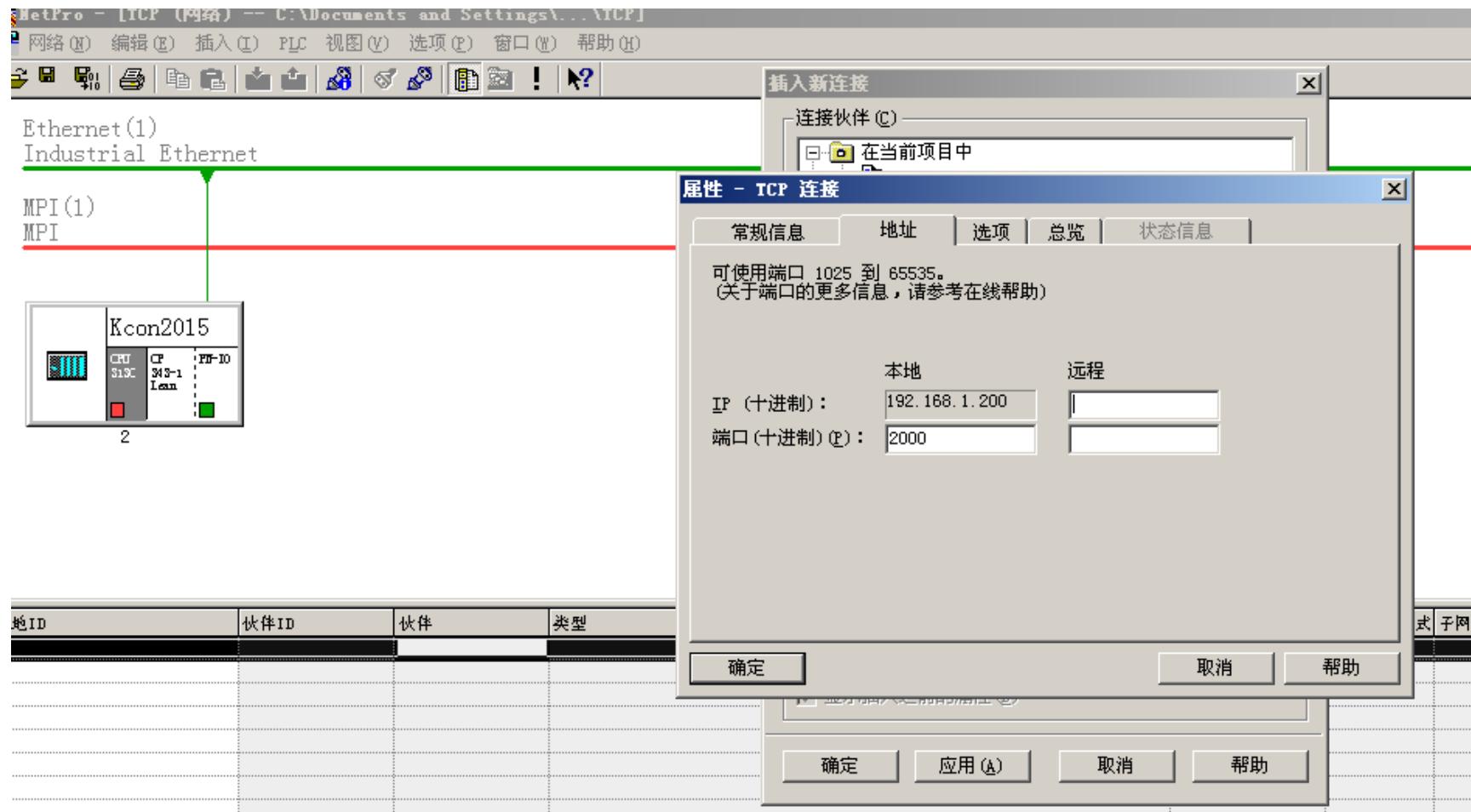
# S7 300 CP的FC5/6功能

- 通信功能块
  - FC5→ “AG\_SEND”
  - FC6→ “AG\_RECV”
- 异步通信方式
- 类似传统Socket通信
  - SEND功能
  - RECV功能

# CP的自定义Socket通信

- 选择连接方式
  - S7
  - TCP/UDP
  - 激活连接的建立
- 调用FC5/FC6
  - FC
- 使用DB构建收发缓冲区
  - 背景数据块

# 自定义Socket通信实现(1)



# 自定义Socket通信实现(2)

- FC5 STL:

CALL "AG\_SEND"

ACT :=L20.0

ID :=1

LADDR :=W#16#100

SEND :=P#DB99.DBX0.0

BYTE 38

LEN :=38

DONE :=M99.1

ERROR :=M99.2

STATUS:=MW100

- FC6 STL:

CALL "AG\_RECV"

ID :=1

LADDR :=W#16#100

RECV :=P#DB199.DBX0.0

BYTE 1024

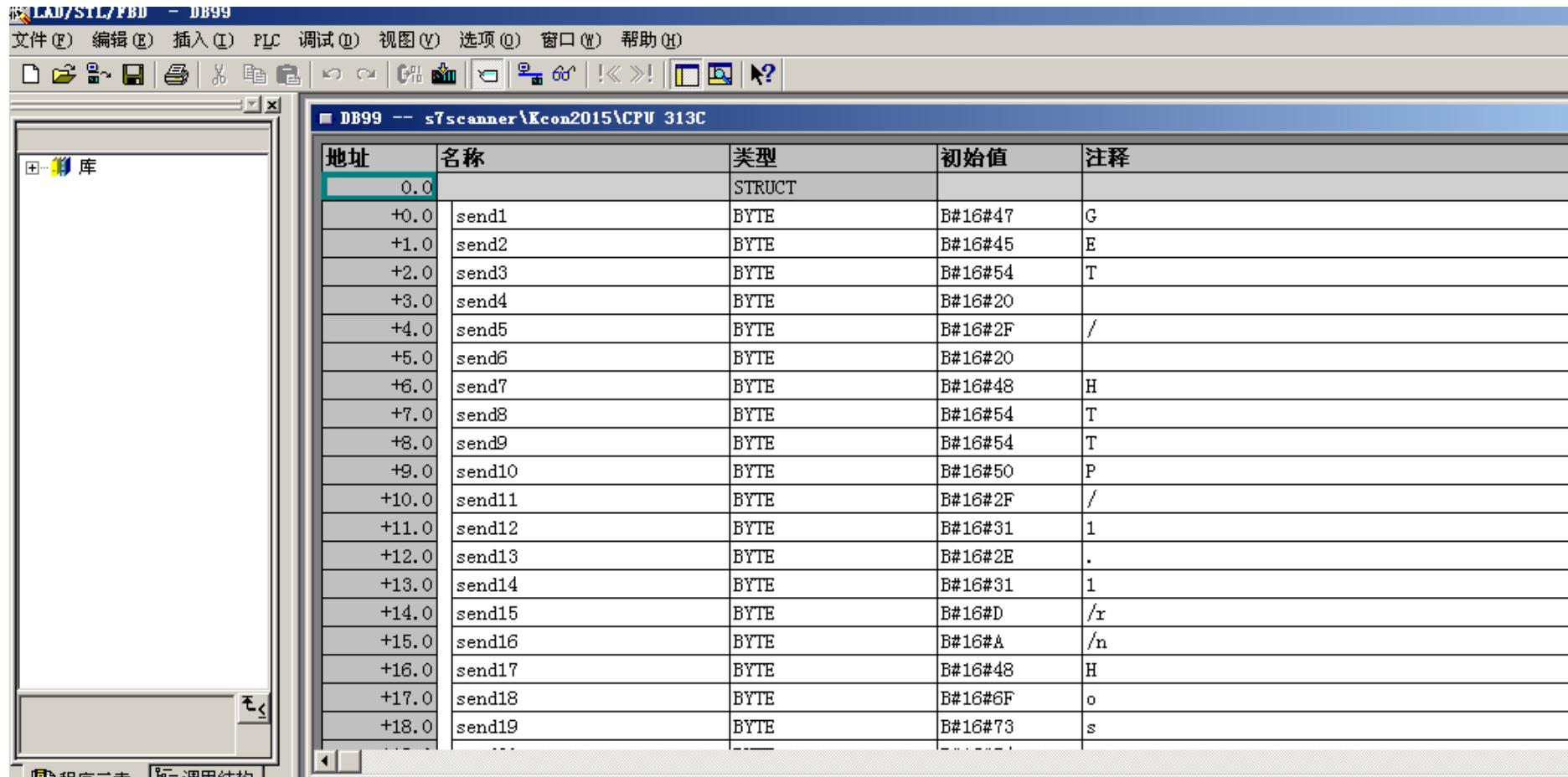
NDR :=M99.3

ERROR :=M99.4

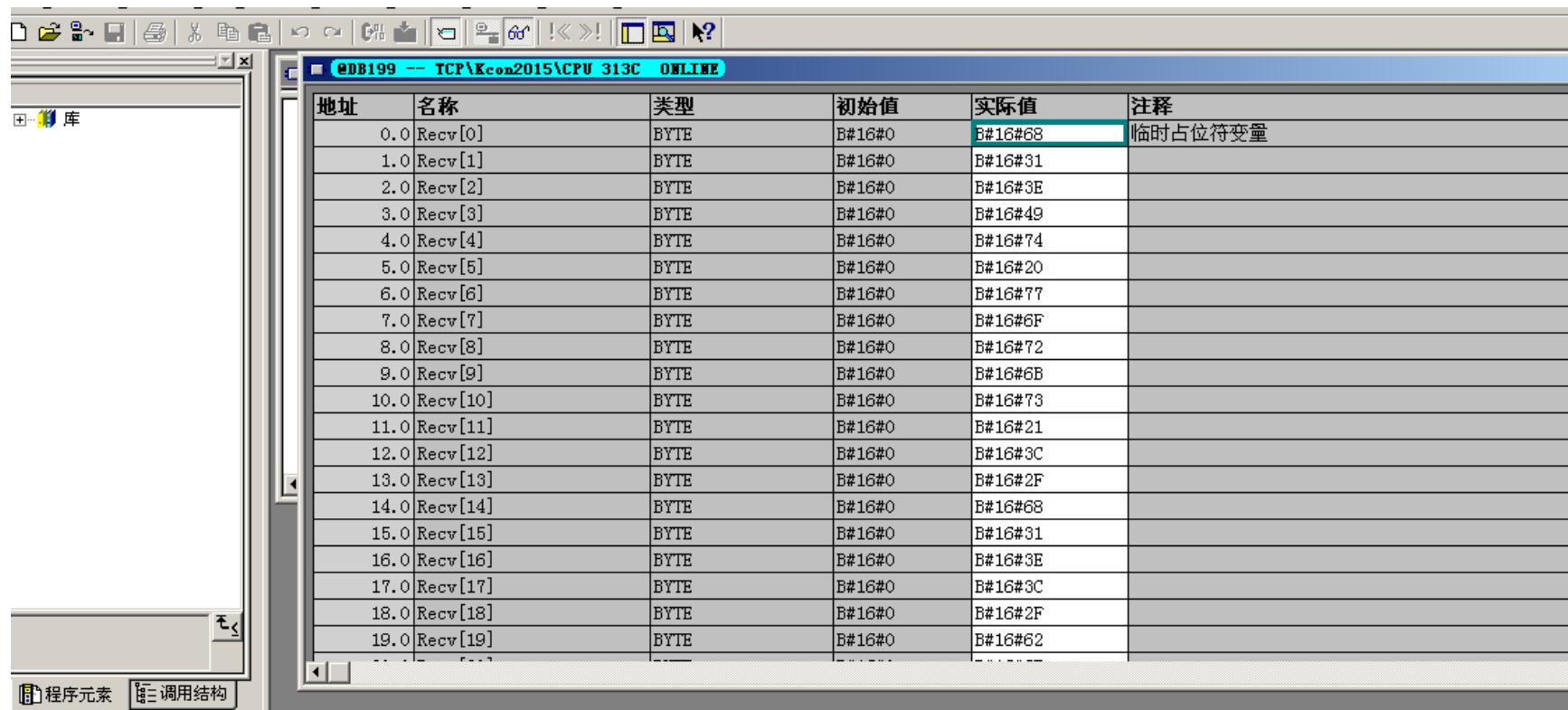
STATUS:=MW102

LEN :=DB99.DBW38

# 自定义Socket通信实现(3)



# 自定义Socket通信实现(4)



# 自定义Socket通信实现(5)

DB Number  
199

DB Dump : 1026 bytes

54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D 0A	HTTP/1.1 200 OK..
44 61 74 65 3A 20 53 75 6E 2C 20 31 36 20 41 75	Date: Sun, 16 Au
67 20 32 30 31 35 20 30 38 3A 35 33 3A 33 33 20	g 2015 08.53.33
47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70 61	GMT..Server: Apa
63 68 65 2F 32 2E 32 2E 32 32 20 28 44 65 62 69	che/2.2.22 .Debi
61 6E 29 0D 0A 58 2D 50 6F 77 65 72 65 64 2D 42	an...X-Powered-B
79 3A 20 50 48 50 2F 35 2E 34 2E 33 35 2D 30 2B	y: PHP/5.4.35-0.
64 65 62 37 75 32 0D 0A 56 61 72 79 3A 20 41 63	deb7u2..Vary: Ac
63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 0D 0A 43	ept-Encoding: C
6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34	ontent-Length: 4
34 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A	..Content-Type:
20 74 65 78 74 2F 68 74 6D 6C 0D 0A 0D 0A 3C 68	text/html.....h
74 6D 6C 3E 3C 62 6F 64 79 3E 3C 68 31 3E 49 74	tml..body..hi..It
20 77 6F 72 6B 73 21 3C 2F 68 31 3E 3C 2F 62 6F	works...hi...bo
64 79 3E 3C 2F 68 74 6D 6C 3E 48 54 54 50 2F 31	dy...html..HTTP/1
2E 31 20 32 30 30 20 4F 4B 0D 0A 44 61 74 65 3A	.1 200 OK..Date:
20 53 75 6E 2C 20 31 36 20 41 75 67 20 32 30 31	Sun, 16 Aug 201
35 20 30 38 3A 35 33 3A 33 33 20 47 4D 54 0D 0A	5 08.53.33 GMT..
53 65 72 76 65 72 3A 20 41 70 61 63 68 65 2F 32	Server: Apache/2
2E 32 2E 32 32 20 28 44 65 62 69 61 6E 29 0D 0A	.2.22 .Debian...
58 2D 50 6F 77 65 72 65 64 2D 42 79 3A 20 50 48	X-Powered-By: PH

DB Get      Async DB Get

# 自定义Socket通信实现(6)

- Black Hat USA 2015
  - INTERNET-FACING PLCS - A NEW BACK ORIFICE
    - FB65 "TCON"
    - FB63 "TSEND"
    - FB64 "TRCV"
    - 通过S7-300 PLC的内部通信块实现Socks5代理功能
    - 更高级、更灵活

S7 PLC特性

如何构造测试工具

# **RELEASED EXPLOITS TOOLS**

# S7 PLC特性

- 非标签方式寻址
- 功能块按照数字编号排序
  - FC 1
  - SDB 1001
- 变量数据是按地址寻址
  - M0.0 → bit 0000
  - M0.1 → bit 0001
  - DB1.DBX1~
- 方便遍历测试而不需要进行枚举
  - For i in range(000000,001234)

# 通用性增强

- 可设置连接模块与槽号
  - Rack
  - Slot
- S7连接的初始化方式
  - PG
  - OP
  - S7

# 工具实现

- S7 Fuzz Tools
  - Get Module info
  - Set CPU Run/Stop
  - Fuzz Set Value
  - Fuzz DB Data
  - Fuzz Block

# S7 Fuzz Tools 测试用例与效果(1)

- 测试设备
  - CPU: 6ES7 313-5BG04-0AB0
  - CP: 6GK7 343-1CX10-0XE0
- 启用等级保护
- 用例:
  - Rack:0 Slot:2
- 结果

# S7 Fuzz Tools 测试用例与效果(2)

- 测试设备
  - CPU: 6ES7 313-5BG04-0AB0
  - CP: 6GK7 343-1CX10-0XE0
- 不启用等级保护
- 用例:
  - Rack:0 Slot:2
- 结果

# MC7Code Inject测试用例与效果(1)

- 测试设备
  - CPU: 6ES7 313-5BG04-0AB0
  - CP: 6GK7 343-1CX10-0XE0
- 不启用等级保护
- 用例:
- 结果

总结

# About

- site:
  - [plcscan.org](http://plcscan.org)