

网络空间 工控设备的发现与入侵

余弦 2014/11/21

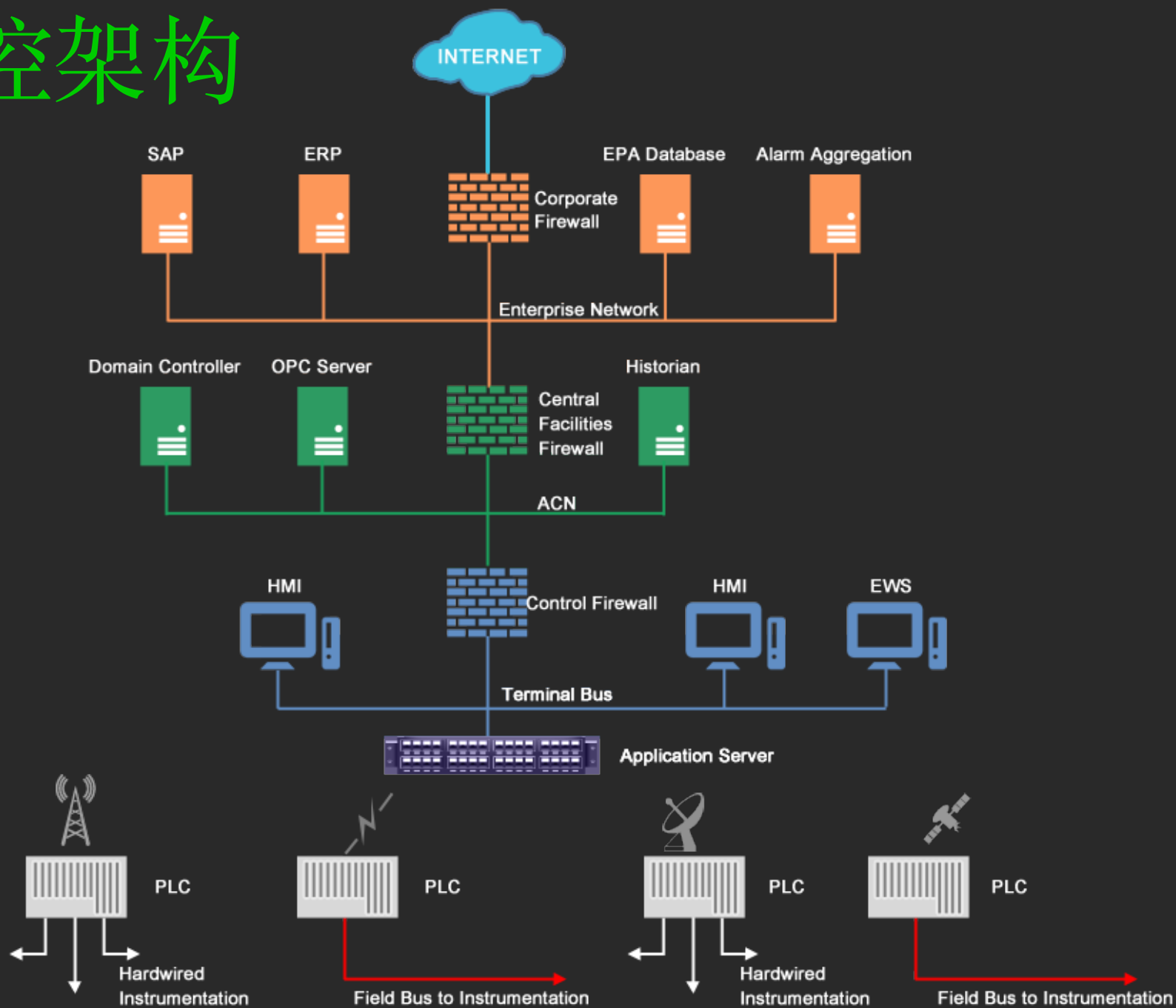
关于我

- 知道创宇
 - 技术VP
 - ZoomEye项目负责人
 - 专注技术路线与创造力
- 《Web前端黑客技术揭秘》作者
- 自然规律敬畏者

研究思路

- 工控架构
 - 模块组件
 - 通信协议
- 架构里的缺陷
 - 以协议研究为出发点
 - 网络空间里暴露了什么
- 如何入侵
- 进一步思考

工控架构



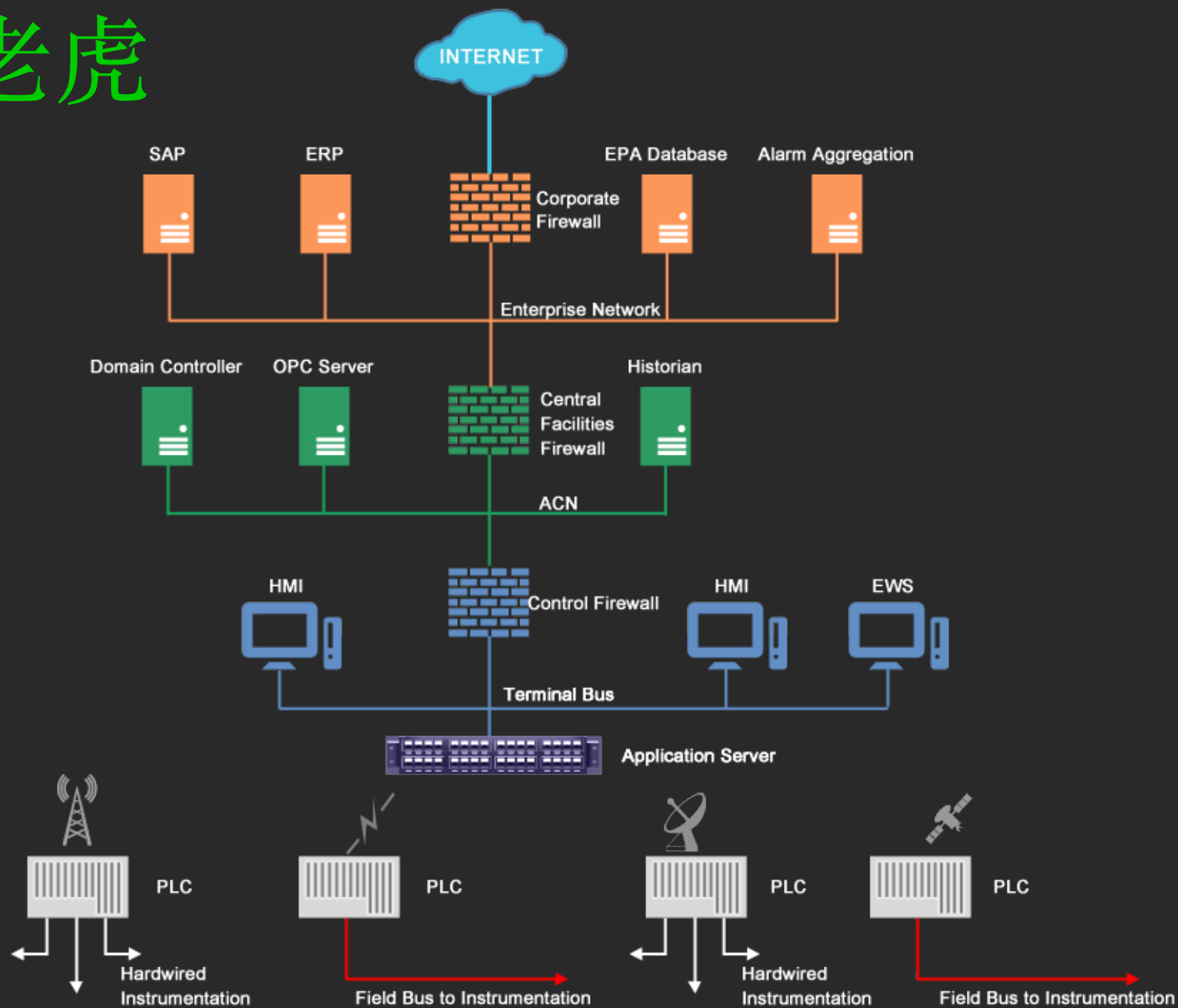
模块组件

- 大组件
 - SCADA
 - HMI
 - PLC
 - RTU
 - ...
- 小组件
 - 操作系统：Win/VxWorks/QNX/Linux/...
 - 服务：Web/Telnet/OPC/...

通信协议

- 应用于这些设备或标准的通信协议
 - Ethernet/IP
 - Modbus
 - IEC 61850-8-1(MMS)
 - IEC 61870-5-101/104
 - Siemens S7的102端口
 - ProfiNET
 - DNP3
 - Tridium Niagara Fox
 - ...

纸老虎

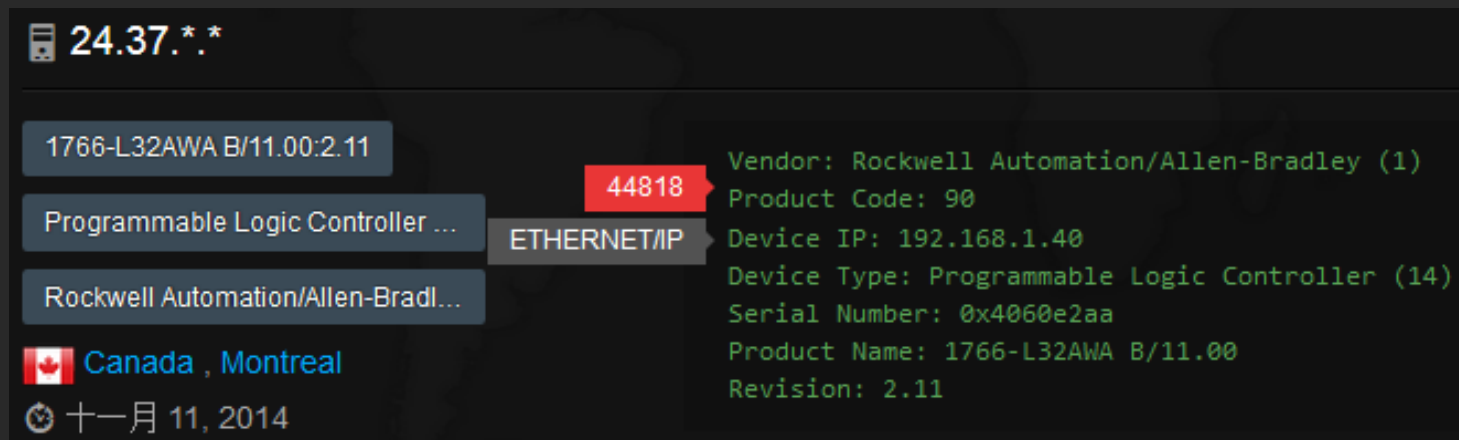


架构里的缺陷

- 未经真正安全考验的组件与协议
 - 如果有Web服务，那就有Web服务该有的缺陷
 - 经典渗透技巧大多适用于工控网络
- 稳定性优先+懒 → 升级难
- 互联网的便利性，让工控组件暴露在网络空间里
- 以协议研究为出发点

Ethernet/IP

- Port: 44818
- 应用层的CIP协议可以抓到设备相关信息



- Python: <https://github.com/paperwork/pyenip>
- Wireshark dissector
 - `src/epan/dissector/packet-etherip.c`

Ethernet/IP

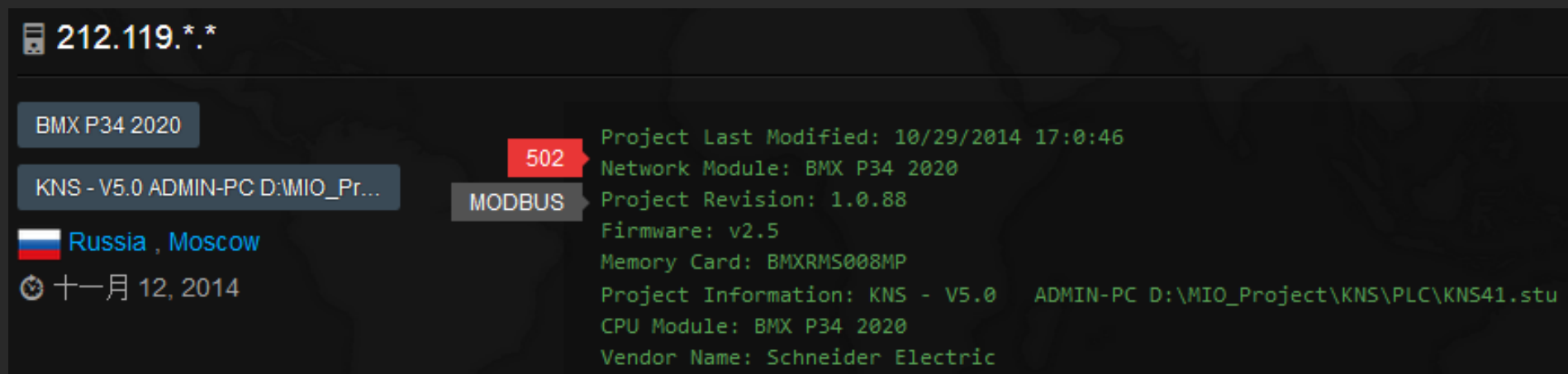
- ZoomEye搜索：
 - 探测日期：2014/11/11
 - 搜索语法：port:44818
 - 全球总数：**3168**

Country	
UNITED STATES	2049
CANADA	313
SPAIN	91
DENMARK	87
SOUTH KOREA	78
TAIWAN	72
AUSTRALIA	63
ITALY	28
BRAZIL	27
CHINA	27

<http://www.zoomeye.org/search?q=port:44818&t=host>

Modbus

- Port: 502
- 抓取设备相关信息



— Wireshark dissector

- src/epan/dissector/packet-mbtcp.c

- 认证与加密缺失

Modbus

- ZoomEye搜索：
 - 探测日期：2014/11/12
 - 搜索语法：port:502
 - 全球总数：**1054**

Country	
FRANCE	273
UNITED STATES	175
RUSSIA	103
DENMARK	94
SPAIN	86
ITALY	49
BRAZIL	31
CANADA	27
CZECHIA	15
AZERBAIJAN	14

<http://www.zoomeye.org/search?q=port:502&t=host>

IEC 61870-5-101/104

- Port: 2404
- 判断是否使用该协议



- Wireshark dissector
 - src/epan/dissectors/packet-iec104.c
- 认证与加密缺失

IEC 61870-5-101/104

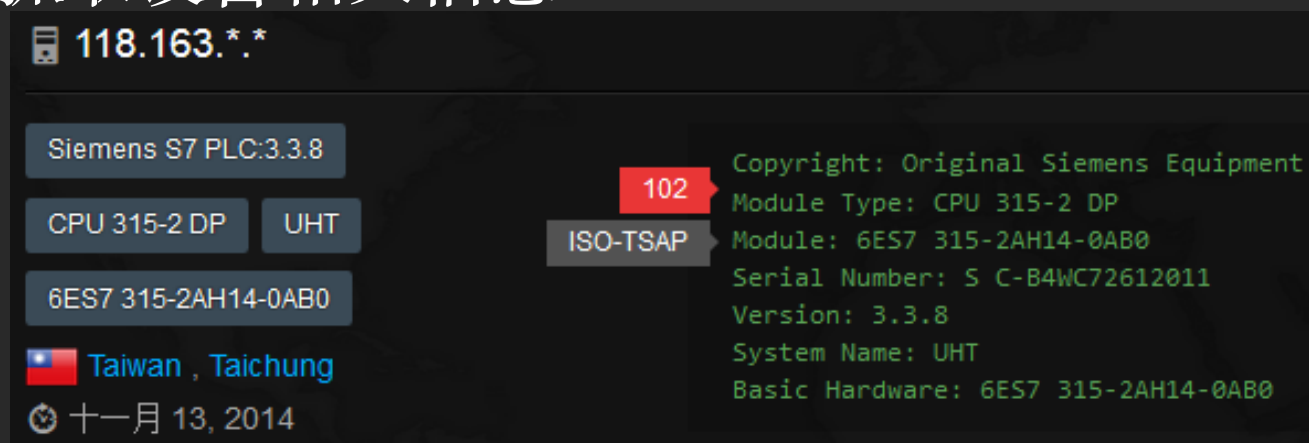
- ZoomEye搜索：
 - 探测日期：2014/11/12
 - 搜索语法：port:2404
 - 全球总数：277

Country	
RUSSIA	100
UNITED STATES	60
TURKEY	32
BRAZIL	13
SPAIN	12
CHINA	5
CZECHIA	5
CANADA	4
COLOMBIA	4
HUNGARY	4

<http://www.zoomeye.org/search?q=port:2404&t=host>

Siemens S7

- Port: 102
- 抓取设备相关信息

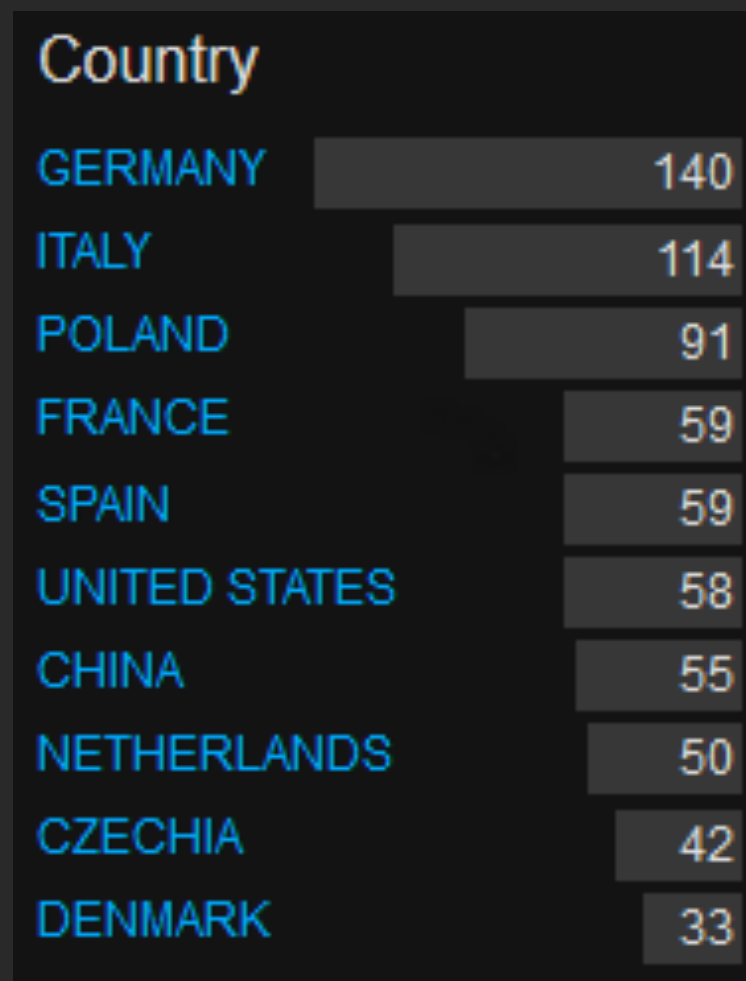


- http://proscan.org/blog/wp-content/uploads/2014/11/37_enumerate.nse_.txt
- Wireshark plugins
 - <http://sourceforge.net/projects/s7commwireshark/>

- 弱加密，易破解

Siemens S7

- ZoomEye搜索：
 - 探测日期：2014/11/13
 - 搜索语法：port:102
app:"Siemens S7 PLC"
 - 全球总数：**1126**

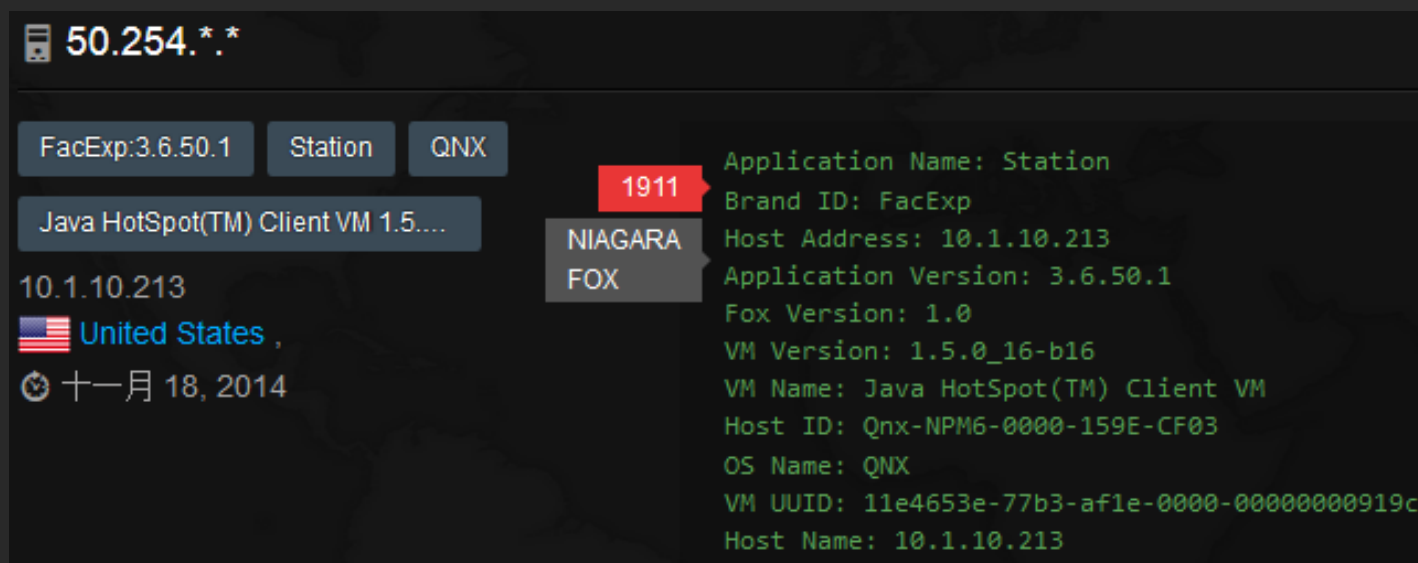


[http://www.zoomeye.org/search?q=port:102 app:"Siemens S7 PLC"&t=host](http://www.zoomeye.org/search?q=port:102+app:"Siemens+S7+PLC"&t=host)



Tridium Niagara Fox

- Port: 1911
- 抓取设备相关信息



Tridium Niagara Fox

- ZoomEye搜索：
 - 探测日期：2014/11/18
 - 搜索语法：port:1911
 - 全球总数：11531

Country	
UNITED STATES	8937
CANADA	697
NETHERLANDS	331
UNITED KINGDOM	316
AUSTRALIA	266
NORWAY	156
FINLAND	137
FRANCE	94
TURKEY	65
ITALY	64

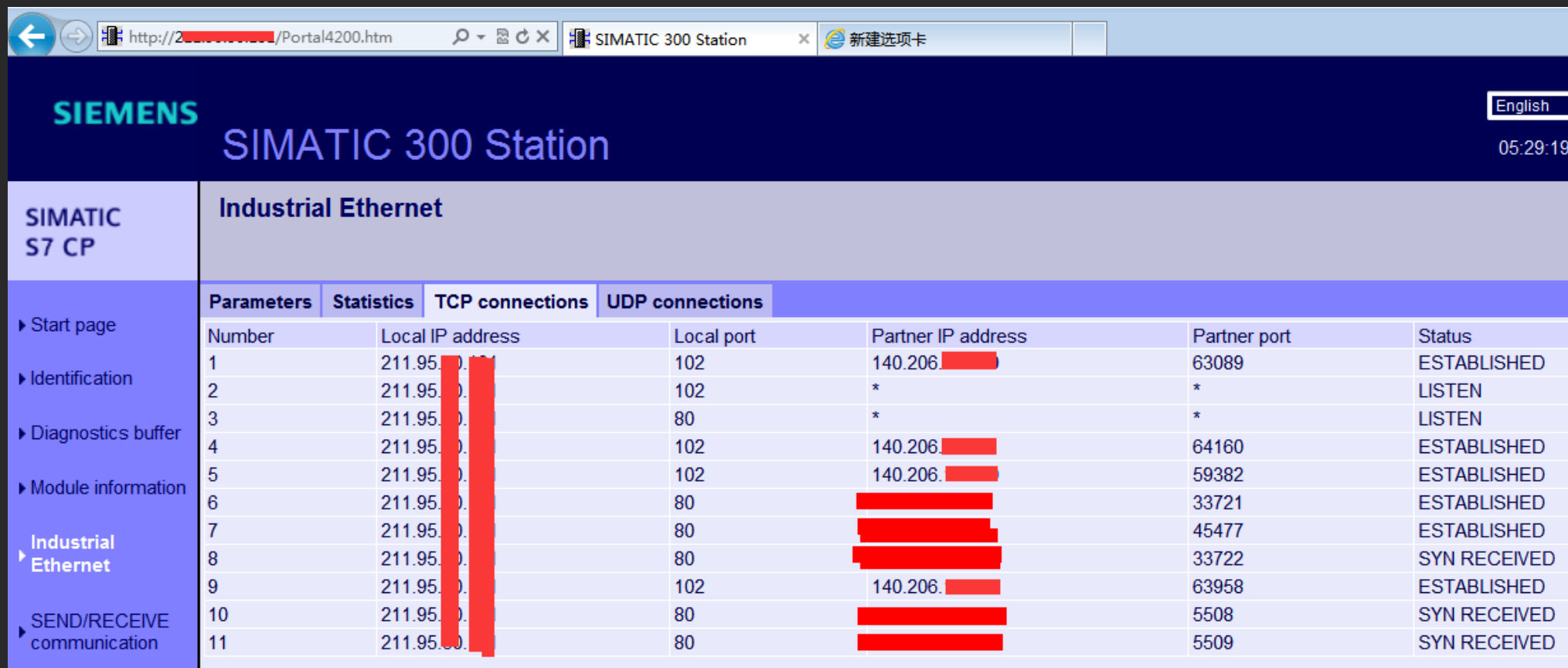
<http://www.zoomeye.org/search?q=port:1911&t=host>

如何入侵

- 当剖析完工控架构后，入侵其实没什么特别之处
- 唯一要说的特别就是：有可能更容易.....

案例一：Siemens S7 PLC

- 以Siemens S7 PLC为例
 - S7 PLC自带嵌入式Web服务

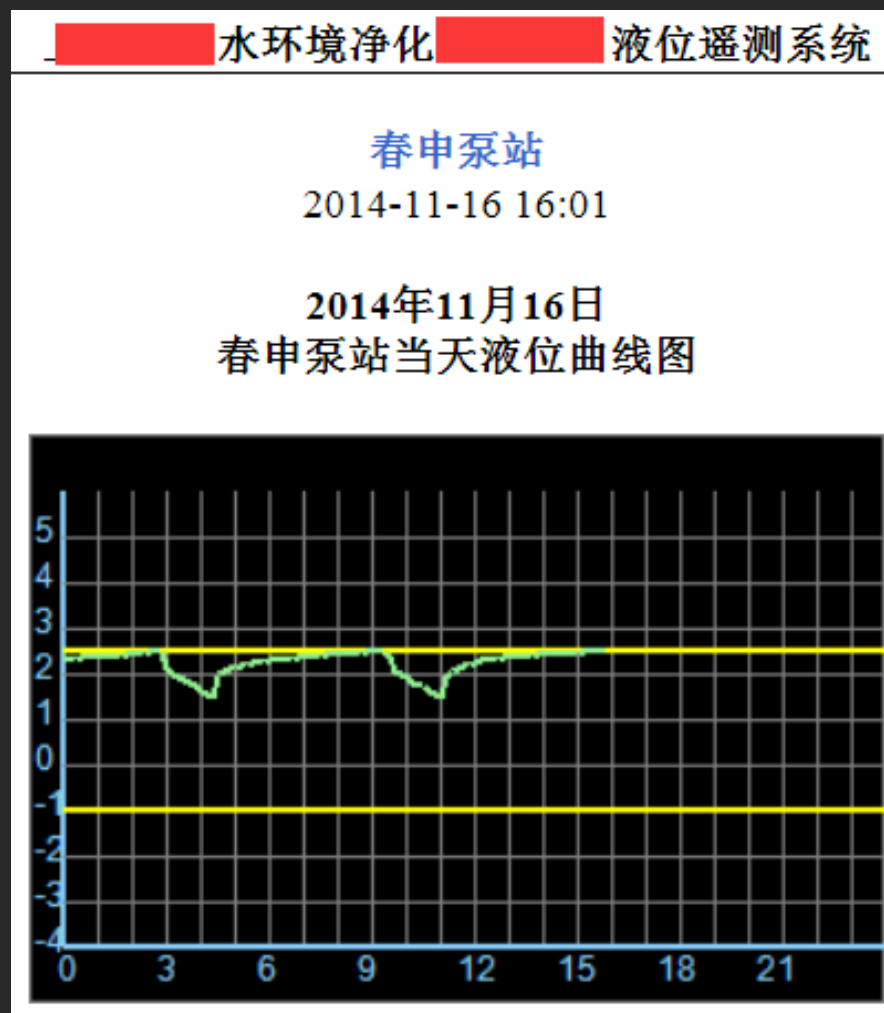


The screenshot shows the Siemens SIMATIC 300 Station web interface. The browser address bar displays 'http://211.95.10.101/Portal4200.htm'. The page title is 'SIMATIC 300 Station'. The left sidebar contains navigation links: 'Start page', 'Identification', 'Diagnostics buffer', 'Module information', 'Industrial Ethernet' (selected), and 'SEND/RECEIVE communication'. The main content area is titled 'Industrial Ethernet' and contains a table with tabs for 'Parameters', 'Statistics', 'TCP connections', and 'UDP connections'. The 'TCP connections' tab is active, showing a table of 11 connections. The table columns are: Number, Local IP address, Local port, Partner IP address, Partner port, and Status. The Local IP address for all connections is 211.95.10.101. The Partner IP addresses are 140.206.10.101, *, *, 140.206.10.101, 140.206.10.101, and several redacted addresses. The Partner ports are 63089, *, *, 64160, 59382, 33721, 45477, 33722, 63958, 5508, and 5509. The Status column shows 'ESTABLISHED' for connections 1, 4, 5, 6, 7, 9, and 10; 'LISTEN' for connections 2 and 3; and 'SYN RECEIVED' for connections 8 and 11.

Number	Local IP address	Local port	Partner IP address	Partner port	Status
1	211.95.10.101	102	140.206.10.101	63089	ESTABLISHED
2	211.95.10.101	102	*	*	LISTEN
3	211.95.10.101	80	*	*	LISTEN
4	211.95.10.101	102	140.206.10.101	64160	ESTABLISHED
5	211.95.10.101	102	140.206.10.101	59382	ESTABLISHED
6	211.95.10.101	80	[Redacted]	33721	ESTABLISHED
7	211.95.10.101	80	[Redacted]	45477	ESTABLISHED
8	211.95.10.101	80	[Redacted]	33722	SYN RECEIVED
9	211.95.10.101	102	140.206.10.101	63958	ESTABLISHED
10	211.95.10.101	80	[Redacted]	5508	SYN RECEIVED
11	211.95.10.101	80	[Redacted]	5509	SYN RECEIVED

上位IP

- S7 PLC Web上可以发现连接本PLC 102端口的上位IP:
 - 140.206.***.***
 - 也开通了Web服务
 - 污水处理系统



S7 PLC C段

- 对S7 PLC的C段进行探测
 - 发现：海康威视DVR监控、Modbus子站等

211.95	.1	:80	DNVRS-Webs	
211.95	.1	:102	NO	0
211.95	.1	:80	NO	0
211.95	.1	:80	DNVRS-Webs	
211.95	.1	:102	NO	0
211.95	.1	:80	NO	0
211.95	.1	:8080	NO	Apache/1.3.28 (Unix) mod_ssl/2.8.15...
211.95	.1	:80	DNVRS-Webs	
211.95	.1	:502	NO	0
211.95	.1	:80	NO	mox_httpd/1.00.02 26 Apr 2005
211.95	.1	:80	DNVRS-Webs	
211.95	.1	:502	NO	0
211.95	.1	:80	NO	mox_httpd/1.00.02 26 Apr 2005
211.95	.1	:80	DNVRS-Webs	
211.95	.1	:502	NO	0
211.95	.1	:80	NO	mox_httpd/1.00.02 26 Apr 2005
211.95	.2	:80	DNVRS-Webs	
211.95	.2	:80	DNVRS-Webs	
211.95	.2	:80	NO	Virata-EmWeb/R6_0_1
211.95	.2	:80	NO	Jetty(8.1.16.v20140903)
211.95	.2	:8080	NO	localhost
211.95	.2	:80	NO	lighttpd/1.4.30
211.95	.3	:0	NO	Apache

海康威视DVR监控

HIKVISION DS-7804HW-E1/M



预览 回放 日志 配置

2014年11月16日 星期日 16:08:31

2014年11月16日 星期日 16:08:31

站

- 站外部
- 站内部
- NA
- NA



站外 站内

HIKVISION DS-7804HW-E1/M

预览 回放 日志 配置

2014年10月20日 星期一 14:52:33

2014年10月20日 星期一 14:52:33

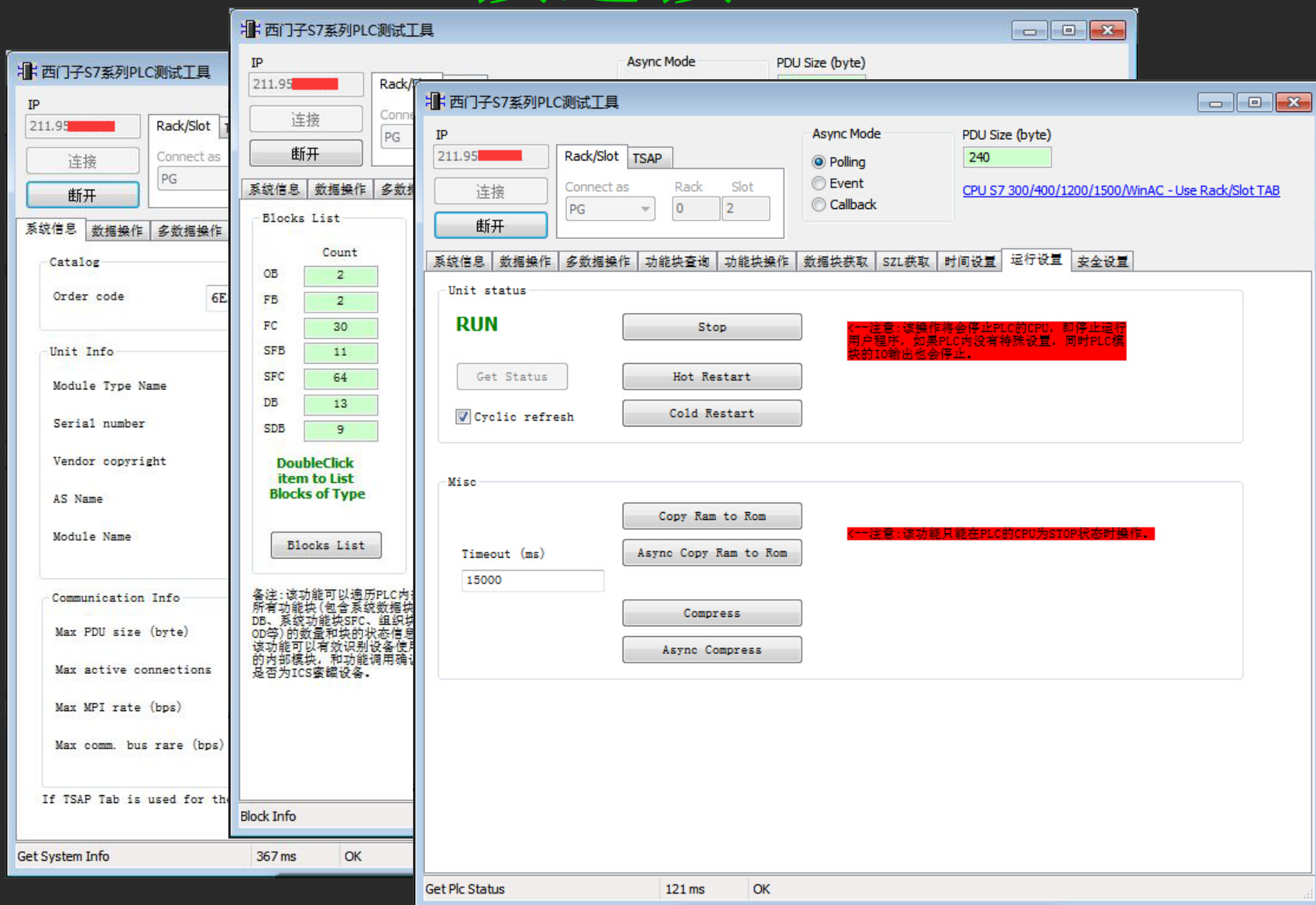
泵站

- 站外
- 内部
- NA
- NA



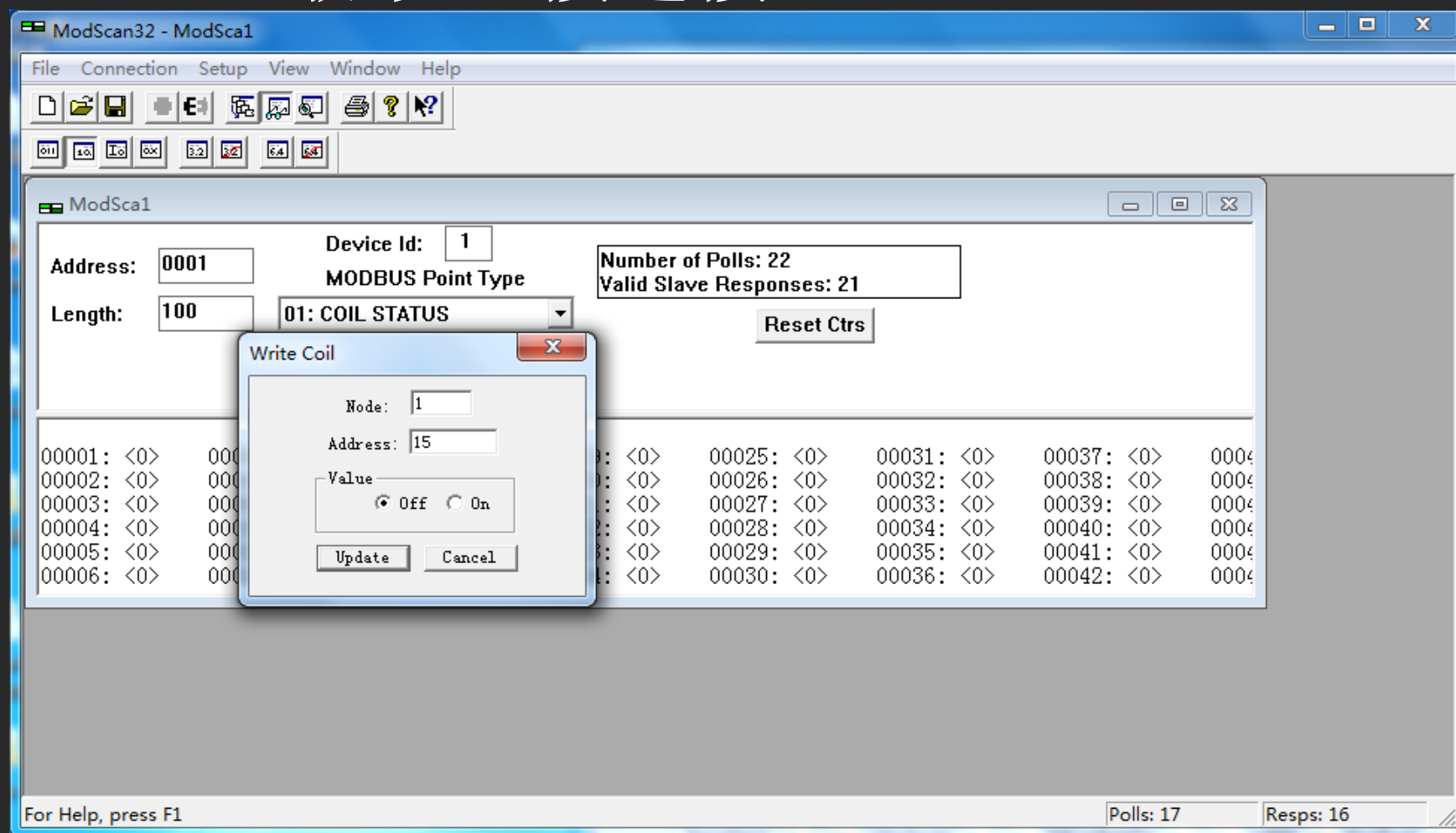
站外 内部

直接连接PLC



案例二：Schneider PLC

- Modbus协议直接连接



进一步思考

•

又是Web安全

- 很多工控沦陷是从Web开始.....
 - 应用层的HTTP协议是最Human的协议
 - Web服务杂乱充斥在工控架构中
 - 几乎没有经过真正安全考验

又是Web安全

收藏夹 PowerLogic?PM800 PowerLogic?PM800 Events

Übersicht Gasübernahme Gastrocknung Gasübergabe System
Flowsheet Biologischer Wäscher Entschwefelung Offgas-Schieber Meldungen
Login / Statistik Chemischer Wäscher Gasreinigung Raumlüftüberwachung Nominierung
Rohbiogas-Analytik Biogasverdichter Produktgasanalyse Nebenanlagen Trends

Uhrzeit: ##:##:##
Datum: ##.##.####

= Biogasverdichter =

Recycle-Gas Gasübergabe
Gasanalyse
Analysengas-Rückführung
Gasübernahme

Automatik Produktqualität
Automatik Volumenstrom
Automatik Produktdruck
Automatik Feeddruck
Manuell
Freigabe FU

Sollwert FU ###.## %
Motorleistung #####W?

Frequenz-Um
FU Soll %
+10% +1%
100
80
60
40
20
0
-10% -1%

Öldruckwächter
Saugdruckwächter
Enddruckwächter
Kühlwassertemperaturwächter

Grenzwert Niveauwächter Saugbehälter
Grenzwert Niveauwächter Zwischenkühler
Störung Niveauwächter Saugbehälter
Störung Niveauwächter Zwischenkühler

Zeitpunkt Datum Status Wichtigkeit Quittiert Alarm Mitteilung

TU WIEN
TECHNISCHE UNIVERSITÄT WIEN
VIENNA UNIVERSITY OF TECHNOLOGY
INSTITUTE OF CHEMICAL ENGINEERING
THERMAL PROCESS ENGINEERING & SIMULATION
axiom
ANGEWANDTE PROZESSTECHNIK

Proficy HMI/SCADA CIMP... Proficy HMI/SCADA C...

Login

Login to CIMPLICITY Thin Client Server

User name:
Password:

Login Cancel

Gastrocknung
Nebenanlagen
Kühlwasser-Vorlauf
Kühlwasser-Rücklauf
Gastrocknung

最脆弱的重要架构

- 工控靠隔离 → 封闭 → 一旦被接触到，这将会是最脆弱的重要架构
- 这个行业确实需要安全/黑客的进入

攻防对抗：蜜罐

ZoomEy

88111222

公网设备

公网设备Web 服务全球视角

找到约 34 条结果。(0.076 秒)

Service

iso-tsap34

Country

UNITED STATES11

NETHERLANDS5

MEXICO3

TAIWAN3

CANADA1

COLOMBIA1

CZECHIA1

FRANCE1

GERMANY1

MAURITIUS1

App

Siemens S7 PLC34

Device

217.109.105.16

Siemens S7 PLC:0.0

Siemens, SIMATIC, S7-200

Technodrome

France, Créteil

十一月 13, 2014

132.247.146.133

Siemens S7 PLC:0.0

SIMATIC S7-200Technodrome

Mexico, Mexico City

十一月 13, 2014

102

ISO-TSAP

Copyright: Original Siemens Equipment
Module Type: Siemens, SIMATIC, S7-200
Plant Identification: Mouser Factory
Serial Number: 88111222
Version: 0.0
System Name: Technodrome

102

ISO-TSAP

Copyright: Original Siemens Equipment
Module Type: SIMATIC S7-200
Plant Identification: Mouser factory
Serial Number: 88111222
Version: 0.0
System Name: Technodrome

Q&A

- 感谢：
 - ZoomEye Team: zoomeye.org
 - Z-0ne: plcscan.org