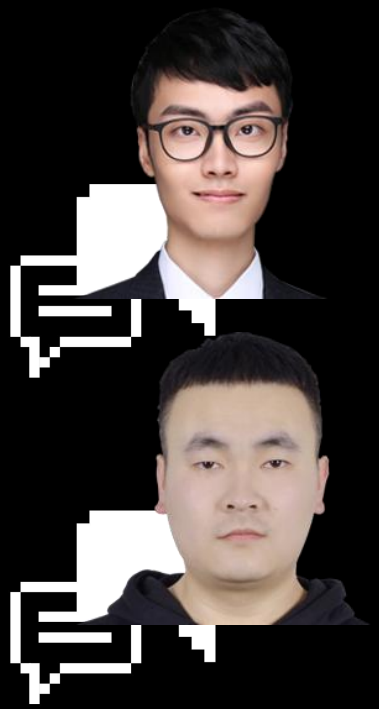


《你相信发电厂爆炸事件是工控黑客所为吗？》

中国网安 · 三零卫士 · 木星安全实验室

伍智波　实验室负责人

周坤　实验室高级安全研究员

CIS 网络安全创新大会
Cyber Security Innovation Summit

目录介绍

网络安全创新大会
Cyber Security Innovation Summit

网络安全创新大会
Cyber Security Innovation Summit

PART 01

工控概述

- 工业控制系统（ICS）部分厂商：

工业控制系统（ICS）所应用重点行业


电力


军工


冶金


医疗


能源


航空航天


食品


烟草


石油


交通


制药


物流


化工


汽车


造纸


海事


水处理


燃气


建材


半导体

- 工业控制系统（ICS）是一个通用简称，主要是用来描述不同类型的控制系统其中包含系统、网络、和控制用于操作、工业过程自动化设备。也就是对多种控制系统的总称，其中列举部分工业控制系统如下：
  - 可编程逻辑控制器（PLC）
  - 数据采集与监视控制系统（SCADA）系统
  - 集散分布式控制系统（DCS）
  - 远程终端单元（RTU）

➢ 什么是PLC?

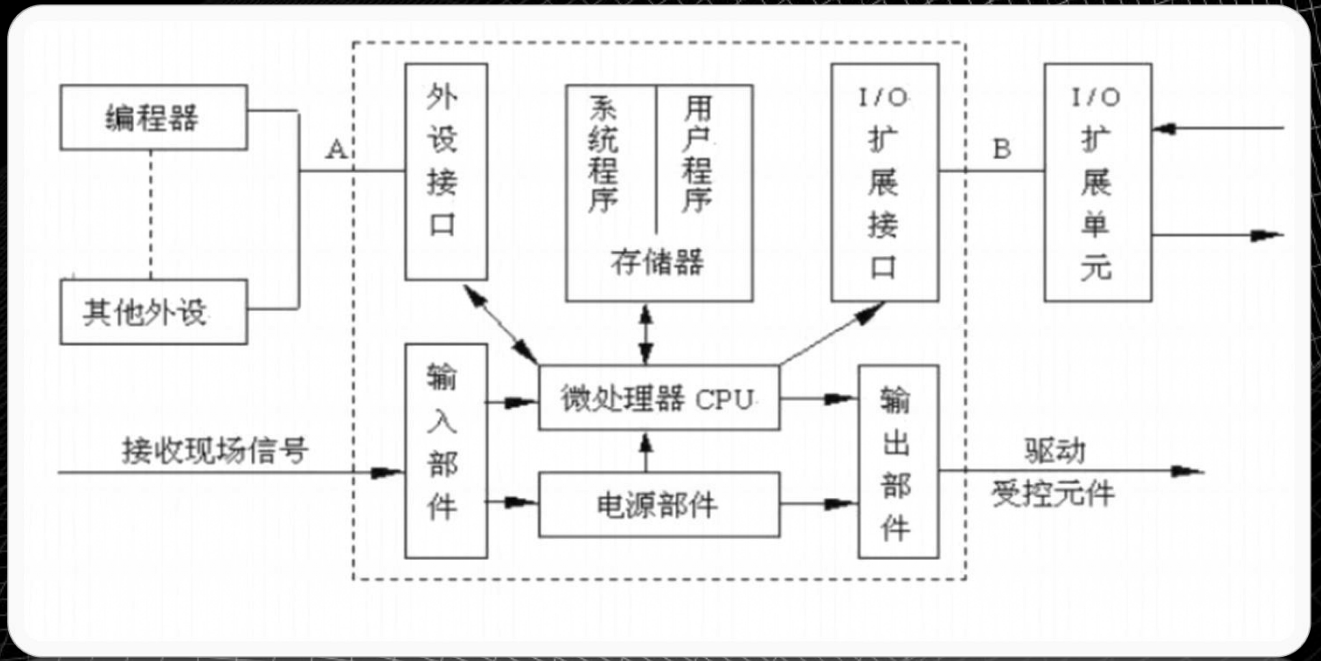
➢ PLC也就是Programmable logic Controller，直译可编程逻辑控制器。

在1987年国际电工委员会（International Electrical Committee）颁布的PLC标准草案中对PLC做了如下定义：

PLC是一种专门为在工业环境下应用而设计的数字运算操作的电子装置。它采用可以编制程序的存储器，用来在其内部存储执行逻辑运算、顺序运算、计时、计数和算术运算等操作的指令，并能通过数字式或模拟式的输入和输出，控制各种类型的机械或生产过程。

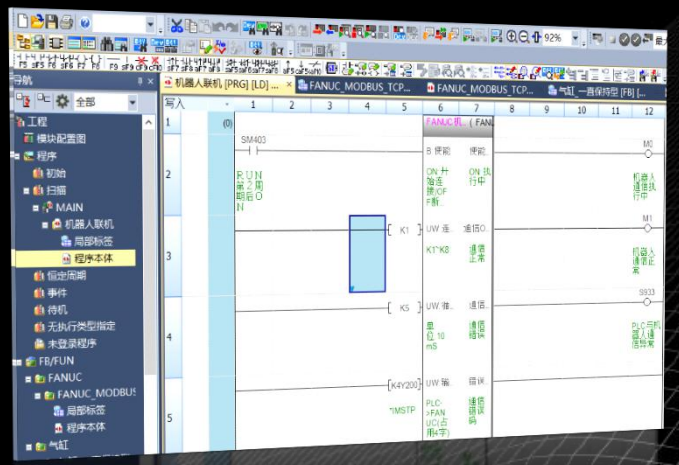
➢ PLC的构成

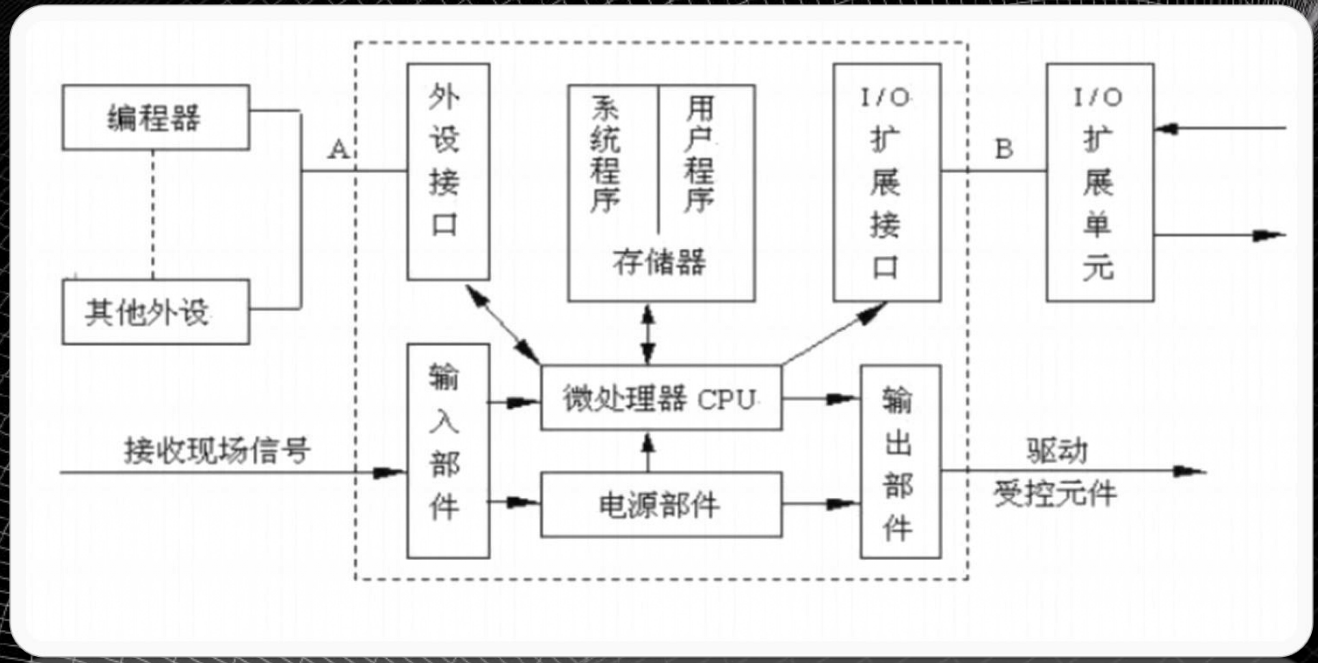
从结构上分，PLC分为固定式和组合式（模块式）两种。固定式PLC包括CPU板、I/O板、显示面板、内存块、电源等，这些元素组合成一个不可拆卸的整体。模块式PLC包括CPU模块、I/O模块、内存、电源模块、底板或机架，这些模块可以按照一定规则组合配置

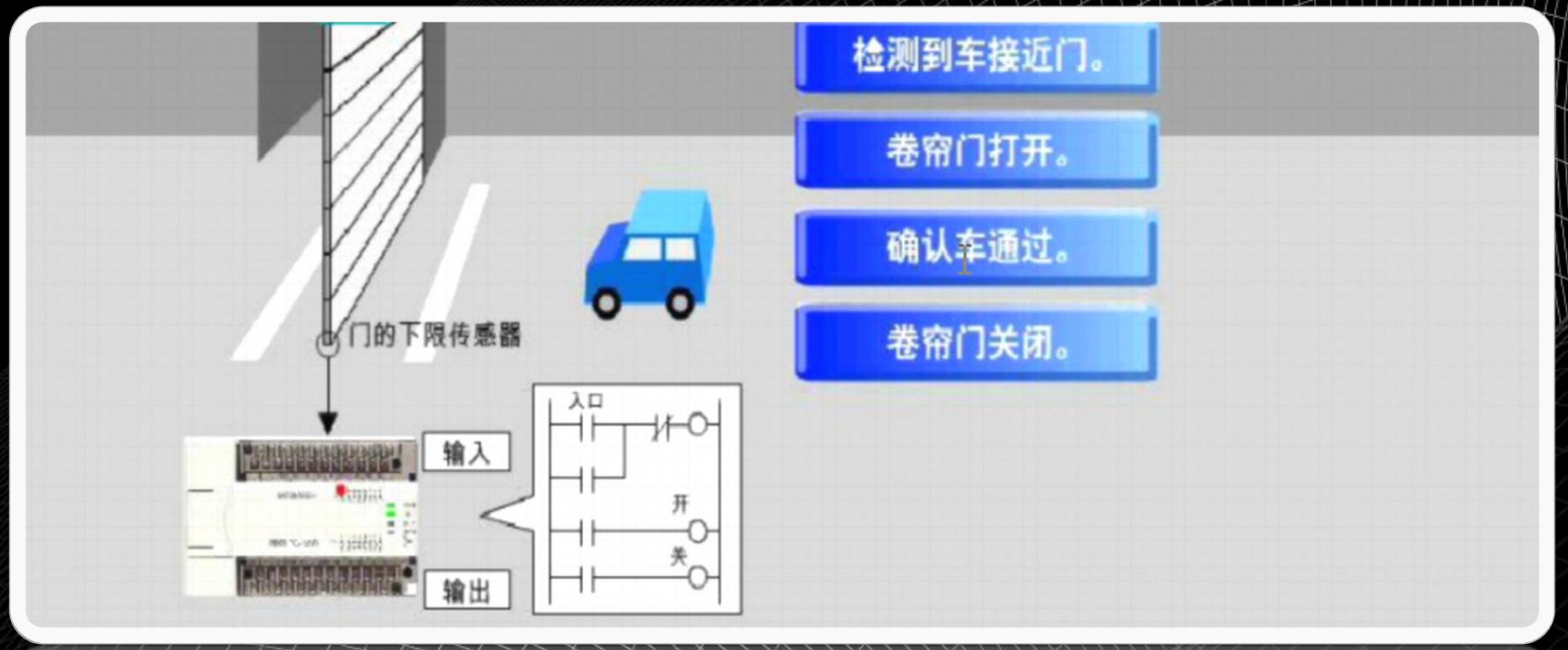


➢ PLC的构成

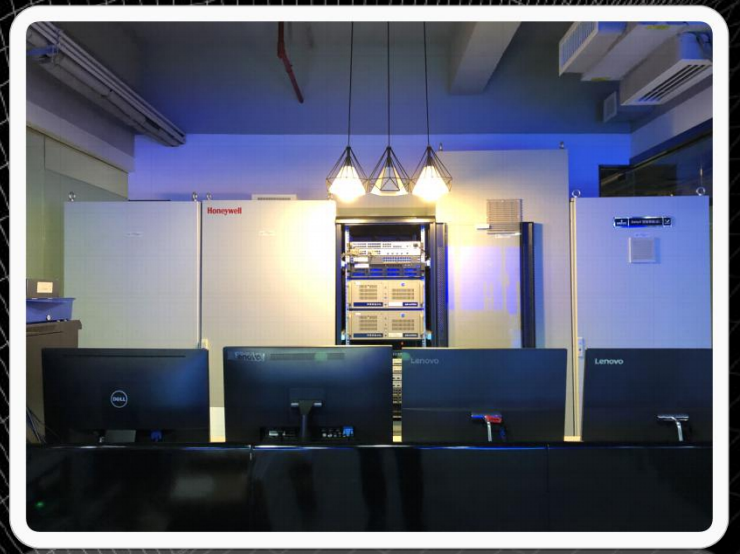
从结构上分，PLC分为固定式和组合式（模块式）两种。固定式PLC包括CPU板、I/O板、显示面板、内存块、电源等，这些元素组合成一个不可拆卸的整体。模块式PLC包括CPU模块、I/O模块、内存、电源模块、底板或机架，这些模块可以按照一定规则组合配置






检测到车接近门。
卷帘门打开。
确认车通过。
卷帘门关闭。
门的下限传感器
输入
输出
入口
开
关

- PLC的构成



工业控制系统（ICS）特点：

- 实时性要求高，强调实时I/O能力
- 可用性要求高，系统一旦上线，不能接受重新启动之类的响应，中断必须有计划和提前预定时间
- 工控硬件要求寿命长，防电磁干扰，防爆，防尘等要求非常严格；
- 特有的工业控制协议通讯协议，不同厂商控制设备采用不同通信协议，很多协议不公开
- 工控系统上线生产后，一般不会调整
- 工控系统要求封闭性比较强

- 工业控制系统（ICS）部分功能：
  - PLC与RTU主要用于获取设备状态
  - PLC可以用于设备本地本地控制
  - DCS通常用于局域网生产过程的整体控制
  - SCADA主要是从PLC和RTU采集监控数据

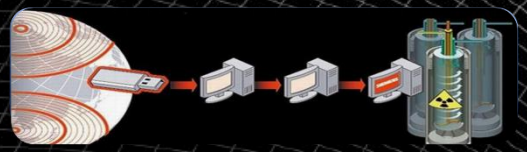
PART 02

工控系统脆弱性

全球工业控制系统攻击安全事件案例

- 2000年澳大利亚污水处理厂被攻击者非法攻击控制了150个污水泵站，总 计有100万公升的污水未经处理排入到自然水系
- 2003年美国Davis-Besse核电站受到Slammer蠕虫攻击，导致核电站计算机出现异常并连续数小时无法工作
- 2006年美国Browns Ferry核电站受到网络攻击，反应堆再循环泵的变频器（VFD）和冷凝除矿控制器（PLC）失效导致多组机组瘫痪。
- 2008年美国Hatch核电厂由于采集控制网络中的诊断数据，使得控制系统以为反应储水库水位下降导致整个机组被关闭
- 2010年震网Stuxnet病毒席卷全球工业界，该病毒感染全球45000个网络，伊朗、印尼、美国等多地工业工控系统均不能幸免，其中伊朗布什尔核电站最为严重
- 2014年德国钢铁厂遭受APT攻击导致工控系统的控制组件和整个生产线被全部停止运行
- 2015波兰航空公司地面操作系统遭遇黑客攻击导致长达5个小时瘫痪、超过1400明旅客滞留
- 2015年乌克兰电力系统遭遇黑客攻击导致伊万诺-弗兰科夫地区约超过一半的家庭（约140万）人停电

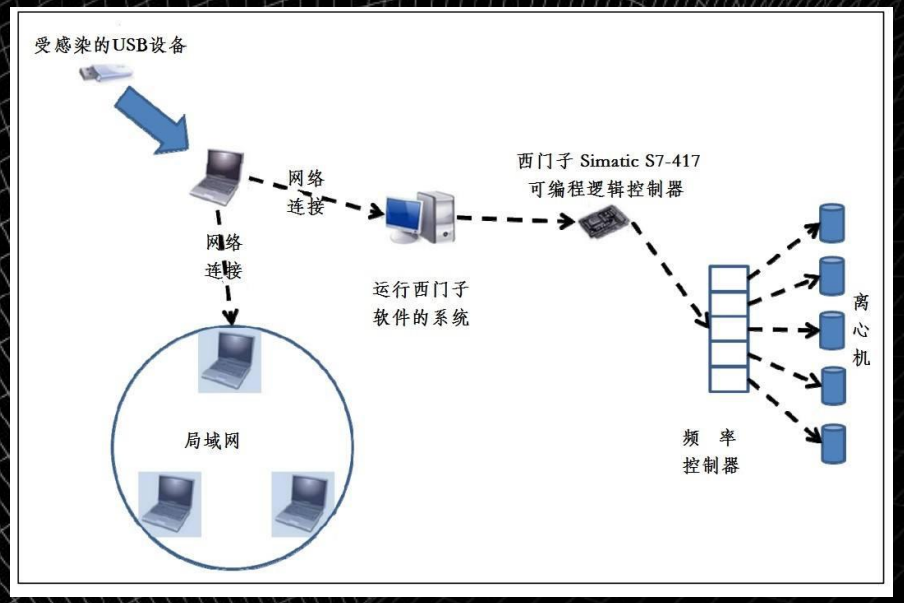
➢黑客针对工控攻击形式多样化

邮件	社工	DOS	工控漏洞
			
恶意代码	**U盘**	**人**	**系统漏洞**
			

伊朗核电站“震网”病毒事件

发生事件：2010年7月
攻击目标：伊朗核电站（物理隔离网络）
入侵方式：

- 收集核电站工作人员和其家庭成员信息
- 针对PC电脑发起攻击，成功控制PC电脑并感染所有接入的USB移动介质通过U盘将病毒摆渡核电站内部网络



利用西门子的漏洞，成功控制离心机的控制系统，修改了离心机参数，让其生产不出制造核武器的物质，但在人工检测显示端正常

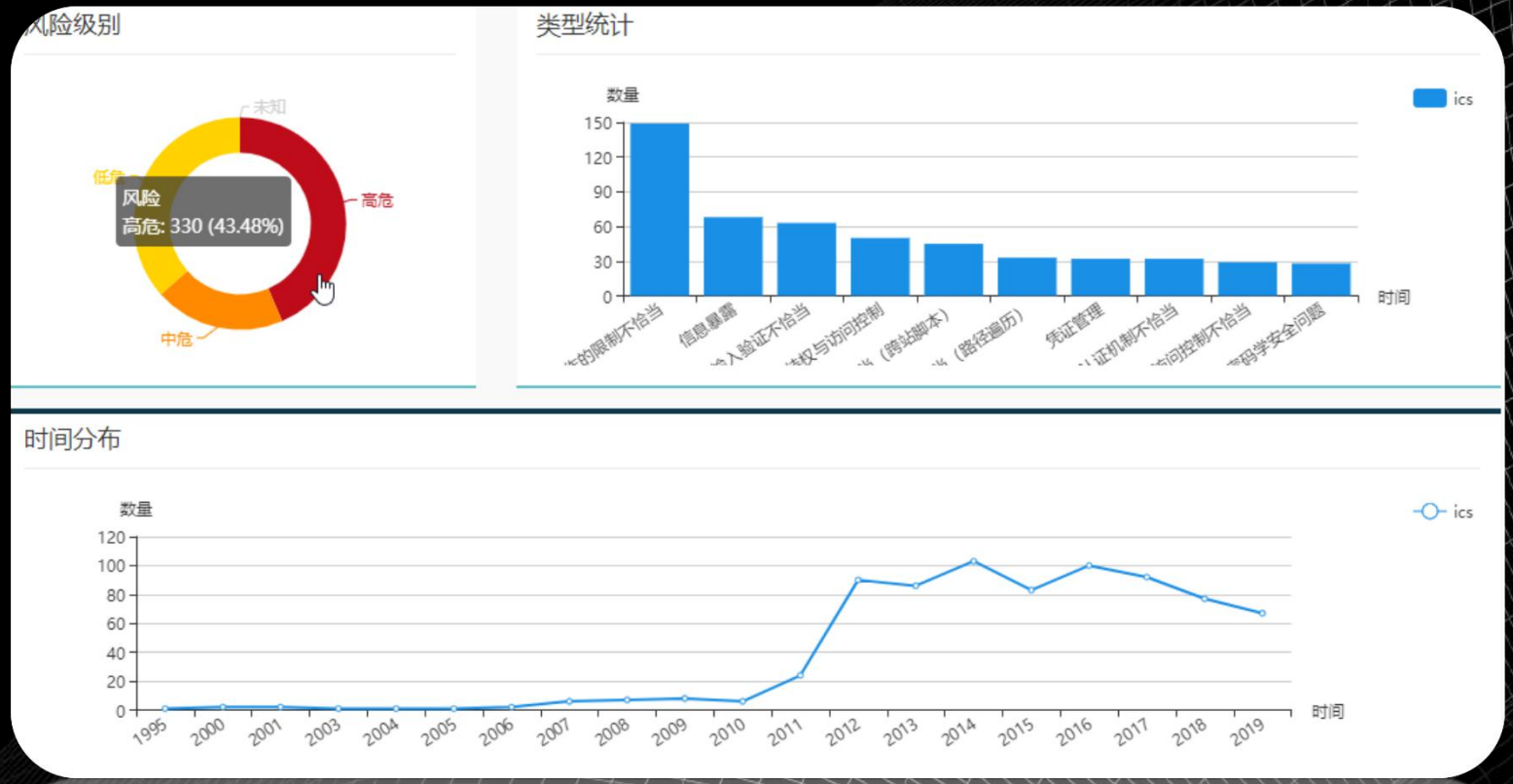
- 渗透手段： U盘
- 损失：“震网”蠕虫病毒攻击伊朗的轴浓缩设备，造成伊朗核电站离心机损坏，推迟发电达两年之久。
- 影响面：感染全球超过45000个网络

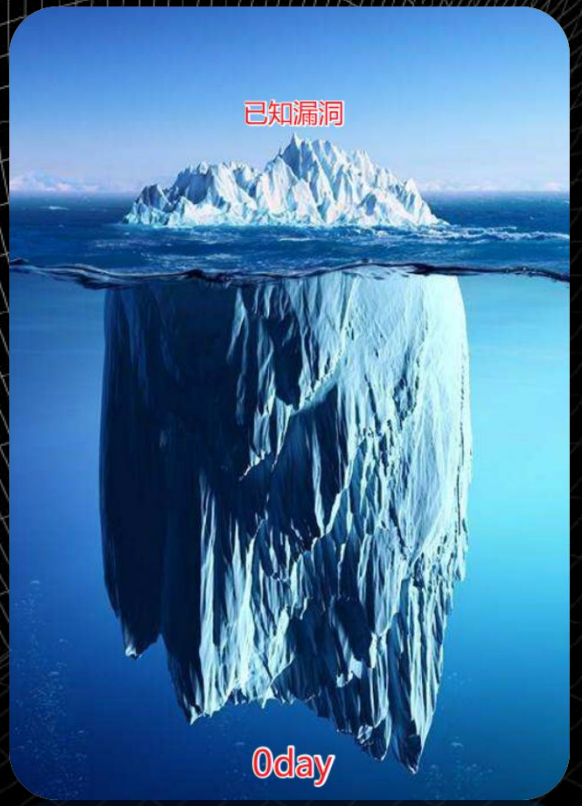
乌克兰电网遭受病毒攻击事件

- 2015年的最后一周，乌克兰至少有三个区域的电力系统被具有高度破坏性的恶意软件攻击并导致大规模的停电
- 12月23日，伊万诺-弗兰科夫斯克地区，有超过一半的家庭（约140万人）遭受了停电的困扰
- 整个停电事件持续了数小时之久，病毒关闭生产控制大区的控制服务器，使得二次信息系统丧失对物理设备的感知和控制导致部分设备运行中断而大面积停电。

工控系统脆弱性

- 归根结底就是工业控制系统的漏洞问题，截止到2019年，公开的工业控制系统的高危漏洞数总体仍然在增加





数据统计来自vulhub

➢工控安全与传统安全差异化

- 工控安全：可用性 > 完整性 > 机密性
- 传统安全：机密性 > 完整性 > 可用性

➢工控安全与传统安全差异化

工控安全	传统安全
专有私有协议	标准的通信协议
主要保护边缘客户端（设备、过程控制器）	主要保护IT资产、存储、传输信息
服务支持通常通过单一供应商	允许多元化的支持风格
实时性要求高、不接受延时	非实时、可以传输延迟
兼容性差、软硬件升级困难	实时补丁修复
专有操作系统、硬件	系统按照典型操作系统使用

网络安全创新大会
Cyber Security Innovation Summit

PART 03

工控漏洞挖掘

- 工程师站、操作员站PC端
- 工程师站、操作员站移动端
- 工程师站、操作员站WEB端
- 工程师站、操作员站网络端

木星安全实验室--工控小组

- 工程师站、操作员站PC端
  - 缓冲区溢出
  - 控件漏洞
  - 后门漏洞
  - 驱动漏洞
  - 弱口令
  - 安全配置错误
  - 身份认证绕过
  - 硬编码漏洞
  - 敏感信息泄露
  - ...

国内某工控厂商后门漏洞—发现第1次

```
text:007247F2                 call    ?DoModal@CDialog@@UAEHXZ ; CDialog::DoModal(void)
text:007247F7                 cmp     eax, 1
text:007247FA                 jz      short loc_724813
text:007247FC                 mov     dword ptr [ebp-4], 0FFFFFFFFh
text:00724803                 lea     ecx, [ebp-0A0h]
text:00724809                 call    sub_4614D0
text:0072480E                 jmp     loc_724BAC
text:00724813 ; ---------------------------------------------------------------------------
text:00724813
text:00724813 loc_724813:                             ; CODE XREF: text:007247FA↑j
text:00724813                 push    offset a12111024_12 ; "12111024"
text:00724818                 lea     eax, [ebp-3Ch]
text:0072481B                 push    eax
text:0072481C                 call    ??9@YG_NABVCString@@PBD@Z ; operator!=(CString const &,
text:00724821                 and     eax, 0FFh
text:00724826                 test    eax, eax
text:00724828                 jz      short loc_724841
text:0072482A                 mov     dword ptr [ebp-4], 0FFFFFFFFh
text:00724831                 lea     ecx, [ebp-0A0h]
```

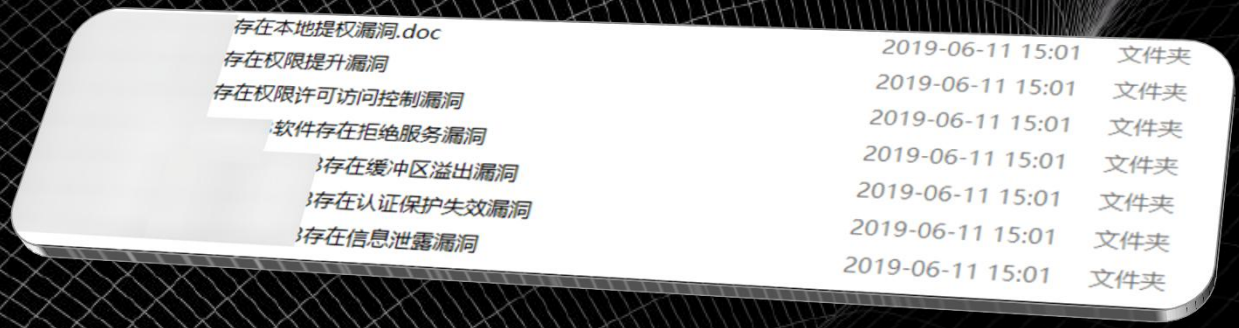
漏洞修复前

国内某工控厂商后门漏洞—发现第2次

```
.text:006761CA                add     eax, 0F8h
.text:006761CF                push    eax
.text:006761D0                call    ??8@YG_NABVCString@@PBD@Z ; operator==(CString const &,char const *)
.text:006761D5                and     eax, 0FFh
.text:006761DA                test    eax, eax
.text:006761DC                jnz     short loc_6761FB
.text:006761DE                push    offset a68860426_6 ; "68860426"
.text:006761E3                mov     ecx, [ebp-1Ch]
.text:006761E6                add     ecx, 0F8h
.text:006761EC                push    ecx
.text:006761ED                call    ??8@YG_NABVCString@@PBD@Z ; operator==(CString const &,char const *)
.text:006761F2                and     eax, 0FFh
.text:006761F7                test    eax, eax
.text:006761F9                jz      short loc_676277
.text:006761FB
.text:006761FB loc_6761FB:                            ; CODE XREF: .text:006761DC↑j
.text:006761FB                push    3ECh
.text:00676200                mov     ecx, [ebp-1Ch]
.text:00676203                call    ?GetDlgItem@CWnd@@QBEPAV1@H@Z ; CWnd::GetDlgItem(int)
.text:00676208                mov     ecx, eax
.text:0067620A                call    ?IsWindowEnabled@CWnd@@QBEHXZ ; CWnd::IsWindowEnabled(void)
.text:0067620F                test    eax, eax
.text:00676211                jnz     short loc_676277
.text:00676213                call    ?AfxGetApp@@YGPAVCWinApp@@XZ ; AfxGetApp(void)
.text:00676218                mov     [ebp-10h], eax
.text:0067621B                push    ecx
.text:0067621C                mov     esi, esp
.text:0067621E                mov     [ebp-14h], esp
.text:00676221                push    offset asc_8153B4 ; """
.text:00676226                mov     edx, [ebp-1Ch]
.text:00676229                add     edx, 134h
```

漏洞修复后

国外--国内工控厂商PC漏洞



木星安全实验室--工控小组

- 工程师站、操作员站移动端
  - 签名破解
  - 组件攻击
  - 逻辑漏洞
  - 跨站请求伪造
  - 路径穿越
  - 越权攻击
  - 明文存储
  - ...

国外--国内工控厂商移动端漏洞

电站监控系统存在验证码绕过漏洞	2019-11-07 9:39	文件夹
电站监控系统（专业版）存在重置任意企业电站密码漏洞	2019-11-07 9:39	文件夹
电站存在不安全账户密码明文存储漏洞	2019-11-07 9:39	文件夹
)A工业组态监控系统存在越权漏洞	2019-11-07 9:39	文件夹
)A工业组态监控系统存在遍历目录漏洞	2019-11-07 9:39	文件夹
用电云平台存在未授权任意访问漏洞	2019-11-07 9:40	文件夹
SCADA工业控制系统存在弱口令漏洞	2019-11-07 9:40	文件夹
供水调度SCADA系统存在目录遍历漏洞	2019-11-07 9:40	文件夹
供水调度SCADA系统存在任意文件上传漏洞	2019-11-07 9:40	文件夹
报警系统存在SQL注入漏洞	2019-11-07 9:44	文件夹
统移动端存在签名破解漏洞	2019-11-07 9:45	文件夹

木星安全实验室--工控小组

- 工程师站、操作员站WEB端
  - 目录遍历
  - 拒绝服务
  - 跨站脚本
  - 未授权访问
  - SQL注入
  - 弱口令
  - 命令注入
  - 信息泄露
  - ...

国外--国内工控厂商部分WEB漏洞

缺陷编号	漏洞起因	漏洞标题
wooyun-2015-132010	弱口令	工控安全之华润燃气敏感环境竟然未走专线可导致内网渗透（监控/配置/阀门可控未测）
wooyun-2015-129388	注入	华润化工控股有限公司信息门户设置缺陷/sql 注入
wooyun-2015-125651	弱口令	某地有线电视内网沦陷可能修改推送广告内容等
wooyun-2015-125399	注入	中华工控网SQL注入导致全网数据沦陷90W会员数据#打包
wooyun-2015-122677	弱口令	某工控系统配置不当危及船只安全
wooyun-2015-117227	弱口令	某水库工控系统存在弱口令(成功渗透)
wooyun-2015-116558	配置不当	某电厂监管系统缺陷可导致整个工控网络沦陷（DCS/PLC 可被操控执行任何命令）
wooyun-2015-107326	注入	某油田开发公司工控系统 sql 注入
wooyun-2015-96729	配置错误	VA 弱密码致华北工控内网远程桌面服务器/内网穿透/涉及敏感信息
wooyun-2014-87708	弱口令	温州市管道燃气公司 SCADA 系统弱口令
wooyun-2014-86726	逻辑漏洞	中国工控网任意用户密码重置漏洞
wooyun-2014-83839	弱口令	大量外网 web 监控系统后台存在弱口令(涉及两款监控产品，涵盖宾馆、车间、仓库、企业内部等)
wooyun-2014-71890	弱口令	某财政信息网系统管理系统密码泄露
wooyun-2014-58681	配置不当	对电厂生产控制网络的一次漫游（针对工控网络的小型APT 攻击）
wooyun-2013-42212	目录遍历	北京市一工控系统多处漏洞可内网渗透（已经发现 webshell）
wooyun-2013-22961	网络未授权访问	301 基础设施系列-国外基础设施 1（鲍里斯波尔国际机场地面照明控制和监测系统）暴漏
wooyun-2013-21848	弱口令	从对某电厂 DCS 控制系统的实体控制谈谈工控安全（可控制电厂实体设备）

木星安全实验室--工控小组

- 工程师站、操作员站网络端
  - DOS攻击
  - 中间人攻击
  - 协议校验绕过
  - 启停攻击
  - 服务端攻击
  - 寄存器攻击
  - CPU存储器清除
  - …

工控漏洞挖掘环境

木星安全实验室--工控小组

➢ 工控安全漏洞挖掘需要的技能如下：

- 会自动化工程师技能
- 会电工技能
- 会PC逆向安全技能
- 会WEB渗透师技能
- 会移动端安全技能
- 会协议分析师技能
- 会嵌入式安全技能
- ...

网络安全创新大会
Cyber Security Innovation Summit

PART 04

工控安全防护

工控安全防护误区：

- 工业控制系统是与外界隔离的
- 没有人会攻击工业控制系统
- 黑客不懂工控协议和系统，系统非常安全
- 单向通信可以保证100%的安全

➢ 工控安全对抗形式：

工控系统防御必须具有全球性视角

1、各国网军不断扩大，对抗升级

2、明间黑客组织水平的不断提升

3、背后巨大的商业利益驱动

4、针对工业控制网络的恐怖袭击

工业控制系统防护要点：

- 用户与帐号管理
- 授权和访问控制
- 边界保护
- 系统监控管理
- 系统资源管理
- 身份认证
- 文件与数据保护
- 入侵检测
- 恶意代码防护
- 系统安全增强
- 网络安全审计

- 工业系统可用性监控：

- 工业系统行为监控：

➢ 工控防护演变过程：

强调隔离	物理隔离的变种，隔离背后是脆弱的，现代高端持续性攻击都是针对隔离系统的
纵深防御	由传统信息安全厂商提出的，大多数项目演变为信息安全产品的简单堆砌，网关、网闸已不能完全适应工业网络安全的特点
工业控制系统持续性防御体系	适应工业控制网络的特点，通过基础硬件创新来实现，低延时，高可靠，可定制化，持续更新，简单化的实施和操作等
以功为守的战略	以美国、以色列为代表，在国家层面注重攻击技术的研究、实验、突破和攻防演示实验的建设，以攻击技术的提高，带动防御技术的提高，以攻击威慑力换取安全性

中国网安·三零卫士·木星安全实验室

CIS 网络安全创新大会 Cyber Security Innovation Summit

THANKS

➢ 国家漏洞库原创漏洞证书（部分）

CNVD-YCGA-201******085 CNVD-YCGA-201******472 CNVD-YCGA-201******269 CNVD-YCGA-201******607 CNVD-YCGA-201******956 CNVD-YCGA-201******439
CNVD-YCGA-201******298 CNVD-YCGA-201******966 CNVD-YCGA-201******350 CNVD-YCGA-201******991 CNVD-YCGA-201******165 CNVD-YCGA-201******882
CNVD-YCGA-201******478 CNVD-YCGA-201******764 CNVD-YCGA-201******112 CNVD-YCGA-201******682 CNVD-YCGA-201******558 CNVD-YCGA-201******781
CNVD-YCGN-201******058 CNVD-YCGA-201******865 CNVD-YCGA-201******231 CNVD-YCGA-201******370 CNVD-YCGA-201******266 CNVD-YCGA-201******095
CNVD-YCGI-201*******461 CNVD-YCGA-201******270 CNVD-YCGA-201******495 CNVD-YCGA-201******948 CNVD-YCGA-201******244 CNVD-YCGA-201******697
CNVD-YCGA-201******579 CNVD-YCGA-201******172 CNVD-YCGA-201******410 CNVD-YCGA-201******689 CNVD-YCGA-201******154 CNVD-YCGA-201******916
CNVD-YCGA-201******532 CNVD-YCGA-201******511 CNVD-YCGA-201******684 CNVD-YCGA-201******506 CNVD-YCGA-201******875 CNVD-YCGA-201******815
CNVD-YCGW-201******882 CNVD-YCGA-201******851 CNVD-YCGA-201******692 CNVD-YCGA-201******190 CNVD-YCGA-201******143 CNVD-YCGA-201******798
CNVD-YCGA-201******043 CNVD-YCGA-201******756 CNVD-YCGA-201******596 CNVD-YCGA-201******285 CNVD-YCGA-201******872 CNVD-YCGA-201******860
CNVD-YCGA-201******453 CNVD-YCGA-201******130 CNVD-YCGA-201******451 CNVD-YCGA-201******738 CNVD-YCGA-201******783 CNVD-YCGA-201******840
CNVD-YCGA-201******144 CNVD-YCGA-201******174 CNVD-YCGA-201******021 CNVD-YCGA-201******083 CNVD-YCGA-201******377 CNVD-YCGA-201******855
CNVD-YCGW-201******723 CNVD-YCGA-201******360 CNVD-YCGA-201******060 CNVD-YCGA-201******588 CNVD-YCGA-201******884 CNVD-YCGA-201******864
CNVD-YCGA-201******739 CNVD-YCGA-201******010 CNVD-YCGA-201******455 CNVD-YCGA-201******685 CNVD-YCGA-201******064 CNVD-YCGA-201******637
CNVD-YCGA-201******830 CNVD-YCGA-201******570 CNVD-YCGA-201******515 CNVD-YCGA-201******002 CNVD-YCGA-201******053 CNVD-YCGA-201******367
CNVD-YCGA-201******642 CNVD-YCGA-201******187 CNVD-YCGA-201******957 CNVD-YCGA-201******184 CNVD-YCGA-201******166 CNVD-YCGA-201******063
CNVD-YCGA-201******002 CNVD-YCGA-201******565 CNVD-YCGA-201******168 CNVD-YCGA-201******405 CNVD-YCGA-201******276 CNVD-YCGA-201******848
CNVD-YCGA-201******447 CNVD-YCGA-201******851 CNVD-YCGA-201******195 CNVD-YCGA-201******708 CNVD-YCGA-201******267 CNVD-YCGA-201******164
CNVD-YCGA-201******528 CNVD-YCGA-201******908 CNVD-YCGA-201******916 CNVD-YCGA-201******386 CNVD-YCGA-201******110 CNVD-YCGA-201******265
CNVD-YCGA-201******931 CNVD-YCGA-201******952 CNVD-YCGA-201******389 CNVD-YCGA-201******392 CNVD-YCGA-201******009 CNVD-YCGA-201******471
CNVD-YCGA-201******039 CNVD-YCGA-201******192 CNVD-YCGA-201******717 CNVD-YCGA-201******068 CNVD-YCGA-201******100 CNVD-YCGA-201******541
CNVD-YCGA-201******262 CNVD-YCGA-201******738 CNVD-YCGA-201******480 CNVD-YCGA-201******214 CNVD-YCGA-201******201 CNVD-YCGA-201******369
CNVD-YCGA-201******570 CNVD-YCGA-201******179 CNVD-YCGA-201******314 CNVD-YCGA-201******024 CNVD-YCGA-201******983 CNVD-YCGA-201******017
CNVD-YCGA-201******671 CNVD-YCGA-201******028 CNVD-YCGA-201******213 CNVD-YCGA-201******999 CNVD-YCGA-201******290 CNVD-YCGA-201******178
CNVD-YCGA-201******129 CNVD-YCGA-201******269 CNVD-YCGA-201******704 CNVD-YCGA-201******134 CNVD-YCGA-201******391 CNVD-YCGA-201******568
CNVD-YCGA-201******785 CNVD-YCGA-201******821 CNVD-YCGA-201******809 CNVD-YCGA-201******765 CNVD-YCGA-201******492 CNVD-YCGA-201******793
CNVD-YCGA-201******071 CNVD-YCGA-201******798 CNVD-YCGA-201******919 CNVD-YCGA-201******839 CNVD-YCGA-201******852 CNVD-YCGA-201******894
CNVD-YCGA-201******511 CNVD-YCGA-201******616 CNVD-YCGA-201******883 CNVD-YCGA-201******470 CNVD-YCGA-201******953 CNVD-YCGA-201******106
CNVD-YCGA-201******958 CNVD-YCGA-201******464 CNVD-YCGA-201******607 CNVD-YCGA-201******774 CNVD-YCGA-201******910 CNVD-YCGA-201******401
CNVD-YCGA-201******371 CNVD-YCGA-201******293 CNVD-YCGA-201******415 CNVD-YCGA-201******099 CNVD-YCGA-201******204 CNVD-YCGA-201******697
CNVD-YCGA-201******139 CNVD-YCGA-201******220 CNVD-YCGA-201******581 CNVD-YCGA-201******457 CNVD-YCGA-201******002 CNVD-YCGA-201******721
CNVD-YCGA-201******410 CNVD-YCGA-201******122 CNVD-YCGA-201******516 CNVD-YCGA-201******572 CNVD-YCGA-201******046 CNVD-YCGA-201******394
CNVD-YCGA-201******001 CNVD-YCGA-201******275 CNVD-YCGA-201******153 CNVD-YCGA-201******776 CNVD-YCGA-201******147 CNVD-YCGA-201******617
CNVD-YCGA-201******319 CNVD-YCGA-201******839 CNVD-YCGA-201******780 CNVD-YCGA-201******941 CNVD-YCGA-201******136 CNVD-YCGA-201******140
CNVD-YCGA-201******027 CNVD-YCGA-201******103 CNVD-YCGA-201******296 CNVD-YCGA-201******673 CNVD-YCGA-201******237 CNVD-YCGA-201******207
CNVD-YCGA-201******091 CNVD-YCGA-201******998 CNVD-YCGA-201******279 CNVD-YCGA-201******973 CNVD-YCGA-201******282 CNVD-YCGA-201******241
CNVD-YCGA-201******814 CNVD-YCGA-201******680 CNVD-YCGA-201******443 CNVD-YCGA-201******223 CNVD-YCGI-201*******562 CNVD-YCGA-201******342

姓名：伍智波
ID：SkyMine
职务：木星安全实验室 负责人

姓名：周坤
ID：曲终人散
职务：高级安全研究员
团队：破晓团队核心成员
团队：IRT工控红队联合创始人