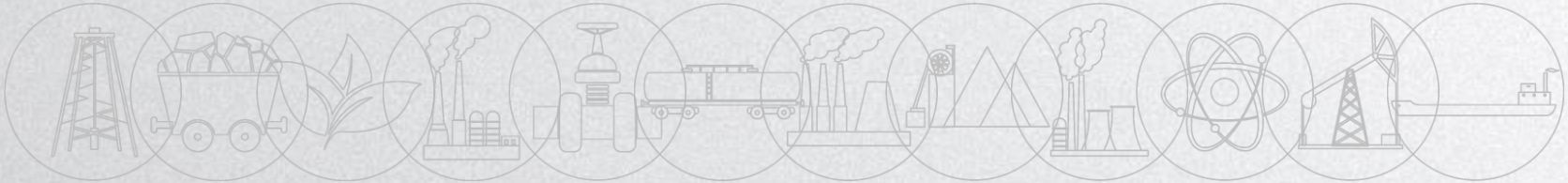
工控安全现场案例分析

北京威努特技术有限公司

公司简介

威努特
WINICSSEC

- 北京威努特技术有限公司是国内专注于工控安全领域的高新技术型企业。以研发工控安全产品为基础，打造多行业安全解决方案，提供培训、咨询、评估、建设、运维全流程安全服务。
- 国内首家提出工业网络“白环境”理念，迄今已服务电力、石油、石化、市政、烟草、化工、军工、轨道交通等行业近百家客户，落地项目遥遥领先，奠定了工控安全市场核心领导地位。



目录

典型案例分析Ⅰ：让“WannaCry”笑不出来

案例背景

2017年5月12日晚20时左右，全球爆发大规模的“WannaCry”勒索病毒事件。该病毒由不法分子利用NSA（National Security Agency，美国国家安全局）泄露的危险漏洞“EternalBlue”（永恒之蓝）进行传播，俨然是一场全球性互联网灾难，工业现场也没有幸免于难。

问题描述

威努特第一时间协助客户做病毒清理和主机加固的工作，并做出情况总结：

- 工业客户中，地域分布广的工业控制现场是重灾区。
- 办公网中毒比较严重，但是生产网也不同程度感染。
- 病毒由办公网进入生产网的趋势比较明显。

“WannaCry” 出现在工业现场的原因

问题分析

- 办公网和生产网没有物理隔离，很多是通过主机双网卡的形式做逻辑隔离，为病毒传播提供重要途径。
- 对移动存储设备使用的管控失位，进一步扩大了安全风险。
- 部分现场应用软件使用的端口和病毒利用的端口一致，难以做到端口的有效控制。
- 基于“黑名单”思路的杀毒软件在面对0Day漏洞和未知威胁时往往束手无策，被动防御。

“WannaCry”事件部分工业现场情况统计

威努特基于“白名单”思想的工控主机卫士在此次事件中表现不凡，工业现场部署了该软件的主机无一感染。

工业现场	中毒情况	操作系统	主机防护	后续措施
油田现场1	办公网：1 生产网：7	Windows XP、Windows 7 Windows server 2008 R2	办公网：北信源、360天擎 生产网：无	生产网免费试用工控主机卫士
油田现场2	办公网：30 生产网：2 （部署工控主机卫士的主机病毒未生效）	Windows XP Windows 7	办公网：诺顿 生产网：部分部署工控主机卫士	生产网全部部署工控主机卫士
油田现场3	办公网：未统计 生产网：1 （部署工控主机卫士的主机病毒未生效）	Windows 7 Windows server 2008 R2	办公网：无 生产网：部分部署工控主机卫士	生产网全部部署工控主机卫士

“WannaCry”事件部分工业现场图

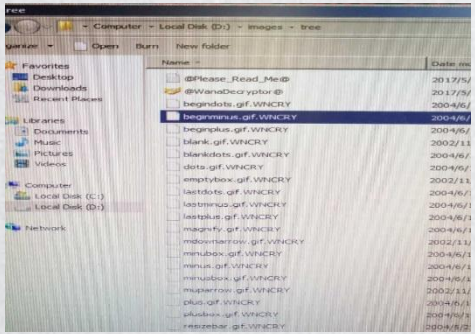


图1：病毒将文件名后缀修改

图2：病毒在办公网爆发

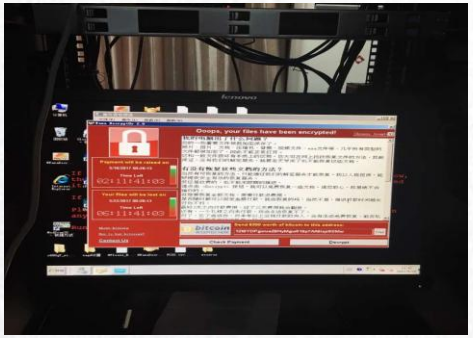


图3：生产网服务器中毒

图4：威努特工程师现场服务

图5：工控主机卫士阻断病毒执行

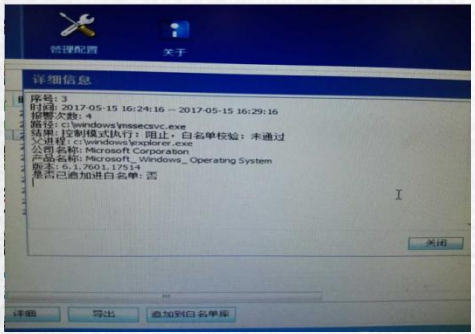


图6：阻断病毒执行的日志详情

工业主机“WannaCry”解决方案

普通解决方案

- **方案：**

已经被病毒加密了文件的主机，可以通过解密工具进行解密，但是成功概率较低。

未染毒主机打补丁、关端口。

- **问题：**

一、 端口是必须用到的端口，不能关闭怎么办？

二、 病毒变种或者新的病毒怎么办？

有效解决方案

- **方案：**

部署基于“白名单”思想的主机加固软件，如工控主机卫士，变被动防御为主动防护。

- **优势：**

一、不借助任何类型的病毒库文件，有效抵御未知威胁和0Day漏洞。

二、低开销，对工业控制软件全面兼容。

典型案例分析Ⅱ：工业现场“扫毒”记

案例背景

除了电力、石化等国家基础工业领域，与民生密切相关的市政系统也分布了大量的工业控制系统，做好这部分的安全防护工作，同样意义重大。

某石化燃气公司经过长时间技术交流和对比测试后，最终选择了成熟的工控安全解决方案来保障生产的安全与稳定。

问题描述

现场所有的操作员站和工程师站平时通过网络共享或U盘拷贝文件，但没有安装任何安全软件，在查毒过程中都发现有病毒感染，其中部分病毒（马吉斯病毒）还非常顽固。由于控制软件授权昂贵，任何情况下遭到破坏，都需要重新采购，这也给杀毒工作也带来风险。

工业现场病毒“横行”的根源分析

根源分析

工业现场的相对封闭性，使得补丁升级、病毒库升级变成一件很复杂的事情，在这种情况下，只要没出大问题，能用的东西就会一直用下去，因此从工业现场找到一个很原始的操作系统版本或者找到一个很古老的病毒样本都是一件很简单的事情。

工业控制相关的软件都是专业软件，和传统防病毒软件在兼容性方面测试不够充分，因此这也是造成工业主机爱“裸奔”的一个重要原因，甚至有部分工业控制系统生产商明确告诉客户：“如果因为安装了某某防病毒软件导致系统异常，我们概不负责。”

典型的工业主机杀毒过程

杀毒过程

技术专家在实验室内反复试验，最终找到了能彻底清除马吉斯病毒的方法，并为现场的杀毒工作制定了严密的方案：

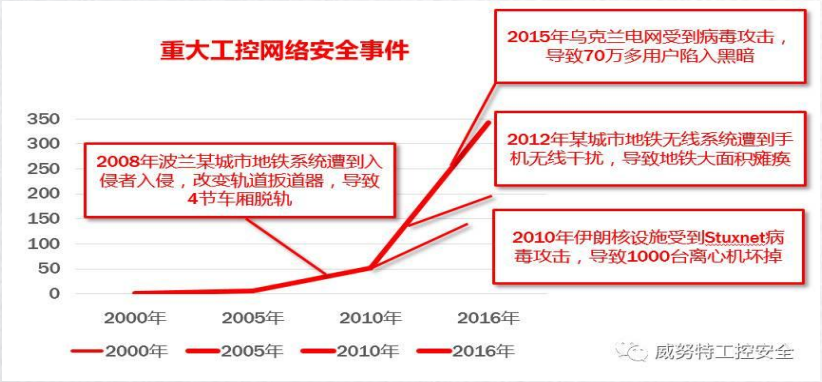
- 镜像中毒主机的硬盘，建立和现场主机一样的软、硬件模拟环境。
- 在模拟的环境上用专杀工具做病毒查杀的工作，这些工具包括：360顽固木马专杀工具、超级巡警、SRENG、瑞星专杀MagistrKiller等。
- 根据专杀工具不同而选择不同的杀毒方式，为保证彻底杀毒，多个工具交替进行。
- 杀毒结束后，测试工业控制软件的各项功能是否正常。
- 在确认工业控制软件运行无误后，在目标主机上重复同样的杀毒过程。
- 部署威努特工控主机卫士。

工业主机安全解决方案

■ 解决方案

- 基于“白名单”思想的主机防护软件是解决上述问题一剂良药，具有**低开销、全兼容、无需升级病毒库文件**等优势。
- 移动存储设备的管控功能、配套安全U盘等技术手段也能解决客户现场数据交换的需求。

长期以来，病毒问题是困扰工业主机的一个棘手问题，从大名鼎鼎的震网病毒到2015年岁末的BlackEnergy，再到现在的“WannaCry”，这些如鬼魅般游荡在工业控制系统网络中的杀手总是伺机而动。



典型案例分析Ⅲ：从“拒绝服务”到“安全稳定”

案例背景

XX油田作为国内名列前茅的油田公司，其已探明的油气储量和每年的油气产量在国内具有举足轻重的战略地位。一直以来，该公司在工业控制系统的安全方面也高度重视，力求打造油田行业的工控安全标杆项目。

在完成整体的工控系统纵深防御之后，系统也一直稳定运行。

问题描述

油田公司某分厂有一个控制器需要增加读取点数，信息中心的工程师进行加点操作，此时更改控制逻辑可以正常进行，但采集数据的动作却没有成功，通过工程师站查看数据存在坏点。工程师又通过ping控制器的方式发现控制器没有响应，对应的通道已坏死，无论如何操作都无法恢复，只能冷重启控制器。

工业控制设备安全分析

问题分析

XX油田所使用的控制器（国外品牌）安全系数较低，在 没有安全防护的情况下，且不说存在数据非法采集的问题，单就增加数据采集的点数而言，用正常速率建立会话连接，当连接数增加到2500左右时，必然导致拒绝服务，最后只能通过冷重启来释放连接，如果遭遇Pingflood之类的攻击更是毫无抵抗之力。

补充说明

从我们做实际项目的经验和漏洞挖掘的实验情况来看，工业控制设备的自身安全性问题比较多，涉及到处理能力、漏洞、后门等，工控安全中对控制设备的安全防护是一个非常重要的方面。

工业控制设备安全解决方案

■现场问题解决：

通过开启防火墙的并发连接数控制的方式来提高控制器的安全系数，并且在防火墙上配置会话老化时间，在白名单防护的同时，给原通信双方发送reset报文，在合理阻断非法的采集请求的同时，保证控制器的正常服务能力。

■问题根源解决：

这个问题是一个典型的工控设备通信健壮性不足的问题，而这恰恰也是当前工控设备普遍存在的现象。使用专门针对工控设备进行通信健壮性测试的漏洞挖掘类工具，去挖掘设备未知的漏洞，进而促使工控设备厂商去修补漏洞，这样能从根源上杜绝类似问题发生，防患于未然。越早发现问题，安全的代价就越低。

目录

西气东输

中国石油

典型SCADA工业控制系统

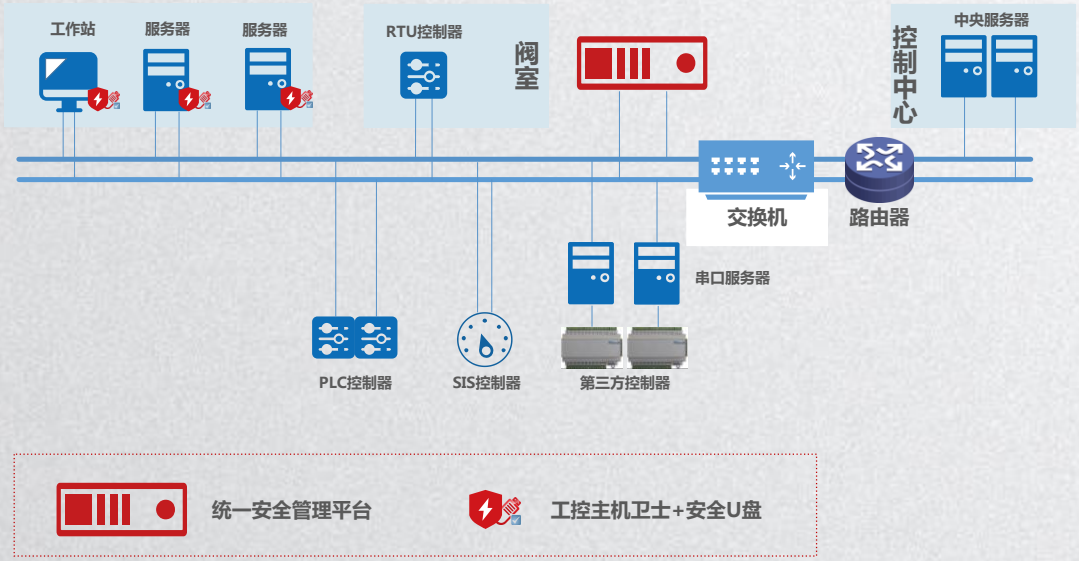
- “西气东输”是我国距离最长、口径最大的输气道管，西起塔里木盆地的轮南，东至上海。本项目是西气东输西二线湖北段，全线采用自动化控制，供气范围覆盖中原、华东、长江三角洲地区。

病毒专杀服务
jwgkvsq.vmx”蠕虫

整体解决方案
基等级保保护

核心安全产品
边界、主机等核心产品

案例说明



客户需求：

- 解决移动存储介质滥用导致的安全问题；
- 解决主机遭受病毒侵入或出现误操作而造成的宕机、运行缓慢及信息数据泄露等问题。

解决方案：

- 在站场工作站及服务器上部署网络版工控主机卫士，避免工作站受到未知漏洞威胁，同时阻止异常操作带来的安全风险；
- 在站场工作站、服务器部署安全U盘，实现移动存储介质管控。

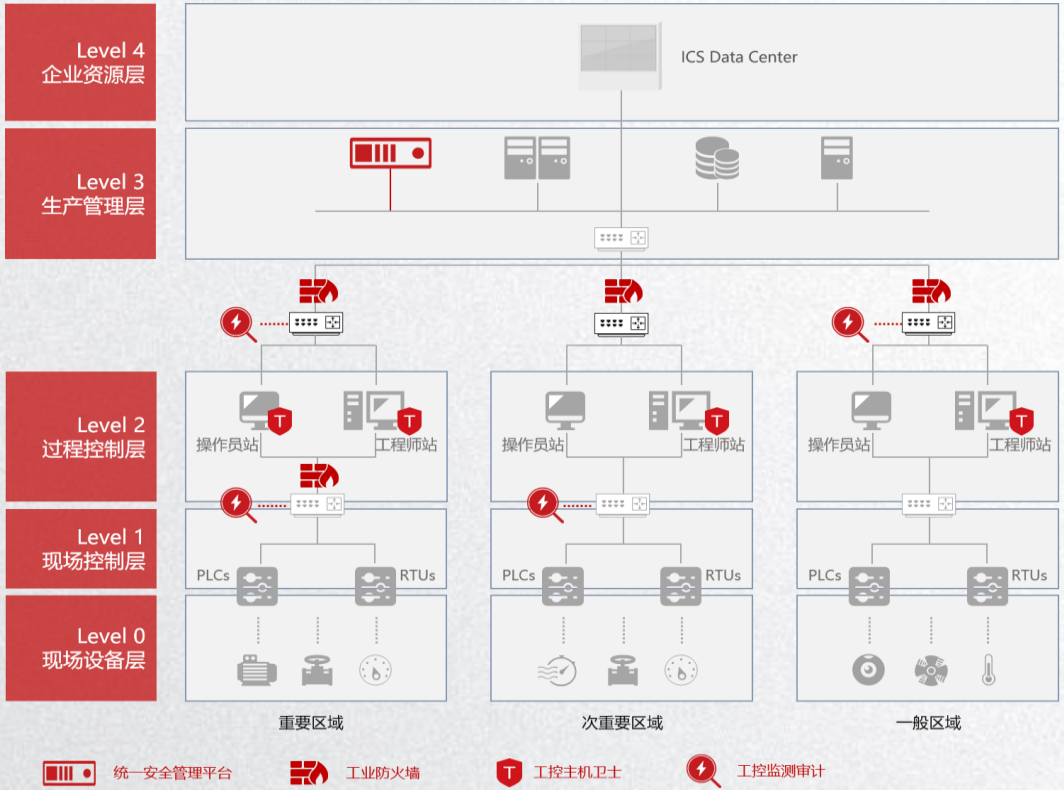
目录

工控安全“白环境”解决方案

国内首家提出工控安全**“白环境”**解决方案体系的工控安全厂商，迄今已为上百家关键行业客户建立自主可控、安全可靠的工控安全整体防护体系。

核心技术理念：

- 纵深防御
- 白名单机制
- 工业协议深度解析
- 实时监控审计
- 统一平台管理



专注工控 · 捍卫安全

工控安全“白环境”解决方案

方案
核心安全理念

创新性提出了建立工控系统的**可信任网络白环境**和**工控软件白名单**的理念为客户构筑工控系统“安全白环境”整体防护体系，保护国家基础设施安全。

技术
亮点及创新点

- 只有可信任的**设备**，才能接入控制网络
- 只有可信任的**消息**，才能在网络上传输
- 只有可信任的**软件**，才允许被执行

- 从“黑”到“白”
- 从“被动防御”到“主动防护”

产品全家福

平台类

工控统一安全管理平台

工控综合检测系统

防御类

单向隔离网关

工业防火墙

运维管理系统（堡垒机）

工业主机安全
安全U盘

检测类

工业网络监测审计

评估类

工控漏洞挖掘平台

工控漏洞扫描平台

等保工具箱

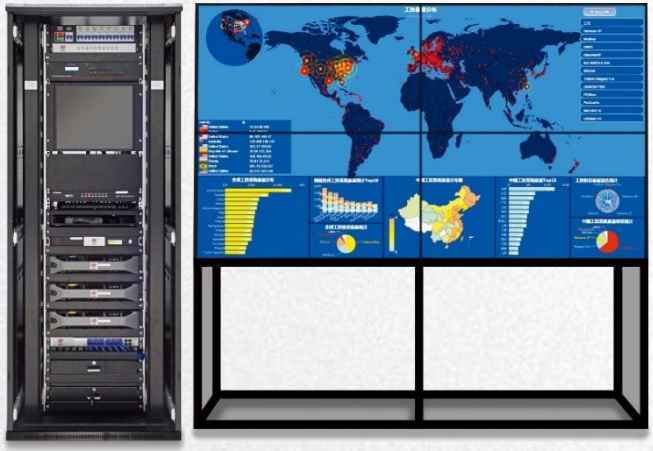
专注工控 · 捍卫安全

产品全家福

科研类

行业仿真攻防平台

漏洞挖掘平台



工业网络态势感知

威努特 WINICSSEC

专注工控·捍卫安全