基于发电厂控制系统的工控蜜罐设计与实现

姚 旭[1],王 钢[2],任秀勤[3],张立芳[1],孙 叶[1]
(1. 内蒙古工业大学 信息工程学院,内蒙古 呼和浩特 010051;
2. 内蒙古工业大学 信息化建设与管理中心,内蒙古 呼和浩特 010051;
3. 北方联合电力海勃湾发电厂,内蒙古 乌海 016000)

摘 要:工业控制蜜罐区别于普通蜜罐的主要标志是使用蜜罐的场景不同,在工业控制蜜罐中,使用场景为工业控制系统,工业控制设备进行通讯时所采用的工控协议不同于普通的互联网协议。工业控制蜜罐诱捕能力主要依靠其仿真交互水平,模仿协议通讯交互情况决定了诱捕环境的真实性。通过对真实发电厂控制系统的考察,提出结合沙盒技术,将发电厂控制系统置于沙盒中以还原蜜罐高仿真度。采用协议逆向分析技术,深度解析 EGD 工控协议掌握协议特征,及时感知异常工控流量数据和异常协议数据包。使用开源 cuckoo 沙盒框架,在部署蜜罐的同时采用主客机部署机制,防止因攻击者识别蜜罐借此为跳板而逃逸或其他破坏行为。然后将蜜罐捕获的所有疑似攻击数据进行分析并提交至 cuckoo 主机端进行二次分析,最后对认为是攻击的数据采取相应处理措施。为网络安全管理员提供可靠数据,为发电厂提供更安全的主动防御网络环境。

关键词:蜜罐;工业控制系统;网络安全防护;cuckoo;随机森林
中图分类号:TP302 **文献标识码**:A **文章编号**:1673-629X(2022)10-0114-06
doi:10.3969/j.issn.1673-629X.2022.10.019

Design and Implementation of Industrial Control Honeypot Based on Power Plant Control System

YAO Xu[1], WANG Gang[2], REN Xiu-qin[3], ZHANG Li-fang[1], SUN Ye[1]
(1. School of Information Engineering, Inner Mongolia University of Technology, Hohhot 010051, China;
2. Information Construction and Management Center, Inner Mongolia University of Technology, Hohhot 010051, China;
3. Northern Union Power Haibowan Power Plant, Wuhai 016000, China)

Abstract: The difference between industrial control honeypot and ordinary honeypot is mainly marked by the different scenes of using honeypot. In industrial control honeypot, the scenes are industrial control system, and the industrial control protocol used for communication of industrial control equipment is different from ordinary Internet protocol. The trapping ability of industrial control honeypot mainly depends on its simulation interaction level, and the simulation protocol communication interaction determines the authenticity of the trapping environment. Based on the investigation of the control system of real power plant, we propose that the control system of power plant is placed in sandbox to restore the high fidelity of honeypot. Using protocol reverse analysis technology, in-depth analysis of EGD industrial control protocol to master protocol characteristics, timely sense abnormal industrial control traffic data and abnormal protocol packets. The open source Cuckoo sandbox framework is used to deploy honeypots with the main aircraft deployment mechanism to prevent escape or other sabotage if an attacker identifies the honeypot as a springboard. Then all suspected attack data captured by honeypot are analyzed and submitted to cuckoo host for secondary analysis. Finally, corresponding processing measures are taken for the data considered as attacks, which provides reliable data for network security administrators and a more secure active defense network environment for power plants.

Key words: honeypot; industrial control system; network security protection; cuckoo; random forests

收稿日期:2021-11-02 **修回日期**:2022-03-03
基金项目:内蒙古自治区教育基金(NJZZ18077)
作者简介:姚 旭(1992-),女,硕士研究生,通讯作者,研究方向为工业控制系统网络空间安全;王 钢,硕士,正高级工程师,研究方向为网络空间安全;任秀勤,硕士,正高级工程师,研究方向为电力系统自动化。

0　引　言

随着互联网、物联网、5G 等网络技术的不断发展,工业控制系统(Industrial Control System,ICS)[1]网络已经由相对独立封闭的网络环境逐步接入通用互联网。当前工业控制系统结合多种新型信息技术已成为近年来的发展趋势。同时也为工业控制系统网络安全防护工作带来新任务、新挑战。

电力行业作为工业控制领域的重要组成部分,生产环境一旦被破坏或失去控制不仅对经济和公共安全问题造成影响,还会造成国家安全隐患。电力系统安全关系着国计民生,其网络安全问题不容小觑[2]。由于工业网络逐步介入互联网,通用互联网的信息安全威胁逐步渗透到传统的电力系统中[3]。早年工控网络环境以物理防护为主,设计研发的工控协议并没有考虑通用互联网威胁,很多工控协议缺乏安全机制。从 2010 年伊朗曝出震网病毒(Stuxnet)事件[4]开始,国外频频曝出各类工控网络安全事件[5]。2015 年末,乌克兰电力系统遭受恶意软件攻击导致大规模的停电事故[6]。2019 年委内瑞拉发生两次大面积停电事件[7]。2021 年 5 月美国大型成品油管道运输公司遭受了勒索软件的攻击[8]。目前发电厂的网络防护还是以物理隔离为主,但早在 2013 年,斯诺登事件中已经曝光了一组美国国家安全局的物理隔离攻击技术。有证据表明利用声波、电磁波、电磁辐射可以成功入侵一台物理隔离计算机[9]。

由于国外电力系统黑客入侵事件频发,电力系统网络安全防御一直是国外各大工业控制实验室的研究热点。Proceedings of the IEEE 在 2012 年就对电力控制系统的网络攻击的实现模式与安全防护体系进行深入研究[10]。目前在增强智能电网的应用程序和基础架构安全性的研究上也有突出成果[11]。中国近年没有发生网络攻击导致的电力事故,但常有对电力系统扫描嗅探行为。

国内一些研究机构已经开始注意到电力系统中的信息安全问题。清华团队深入研究智能电网信息系统。南瑞集团已深入研究电网恶意攻击的辨识方法以及电网侧主动防御策略[10]。工控蜜罐的交互方面研究主要集中在工控协议解析和交互能力方面。现在大多工控蜜罐实现了西门子和施耐德设备的相关协议,如 S7 相关协议和 Modbus 协议,对于其他工控协议涉猎较少。

基于以上研究,该文设计并实现了基于发电厂控制系统的蜜罐系统,主要工作如下:

(1)使用蜜罐的思想,结合沙盒技术,实现一个基于沙盒技术的发电厂蜜罐。经过对内蒙古地区发电厂实地考察,深入了解 DCS(分散控制系统,Distributed Control System)网络拓扑结构,通过结合沙盒完成高“甜度”蜜罐。

(2)系统依照 cuckoo 设定客户机和分析机,将采用对客户机部署沙盒捕获到的恶意文件、恶意流量等信息上传分析机,采用 cuckoo 的分析机制进行分析。

(3)通过逆向协议分析技术,主要对发电厂 DCS 系统使用的工控协议进行逆向解析,完善工控蜜罐的 EGD 私有协议仿真,深度分析其协议内部数据,分析在发电厂正常数据的协议包内容情况并学习。

系统通过捕获操作系统层面数据和协议通讯数据两方面来监控发电厂控制系统,实现一个蜜罐系统。该蜜罐系统将捕获数据对比发电厂实际操作层面数据以及实际流量分布情况来确定攻击数据,从主动防御方面保护发电厂控制系统网络。

1　EGD 协议解析

EGD 协议,即 Ethernet Global Data 以太网全球数据。EGD 协议是应用于电子控制器上的一种通用语言[12]。

1.1　EGD 协议通讯

EGD 协议和大多数工控协议一样是应用层协议,EGD 数据是由一台 PLC 周期性地发送给另一台(组)PLC。在 EGD 通讯方式下,通讯节点分为 Producer 和 Consumer。EGD 协议是基于 UDP/IP 的协议,占用 UDP 端口 18 246[13]。

EGD 协议支持单播(Unicast)和多播(Multicast)的模式,可以以点对点或点对多点的方式进行数据交互。EGD 协议使用的是生产者-消费者(Producer-Consumer)模型。Producer 和 Consumer 之间以 Exchange(交换数据包)进行数据交互,一个 Exchange 最多可以包含 1 400 个字节的数据[14]。

1.2　EGD 协议的解析

研究对象 EGD 协议通过协议逆向技术解析,EGD 协议是基于 UDP 的应用层协议数据包,由 EGD 协议打包原始数据后,使用通用数据协议对协议数据单元(PDU)进行封装,由 UDP/IP 封装后进行连接和传送,由于 UDP 的无连接、最大交付性,而 EGD 协议结构简单,通讯中也会一定程度依赖软件配置。

EGD 数据消息会按照要求从生产者发送到消费者,每个 EGD 消息主要分成两部分:固定标头和数据消息,标头具有固定的格式共 32 字节组成。具体协议解析见图 1 和表 1。

结合发电厂控制系统和逆向协议分析技术,使用抓包工具并调整参数,采用单一变量通过分析对比不同操作时数据包的异同点。由于 EGD 协议使用以太网结构协议,使用抓包工具 Wireshark 等网络协议分析

工具。探测输入数字量、输出数字量、输入模拟量、输出模拟量等。

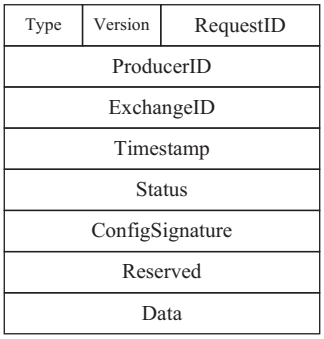

图 1 EGD 协议格式

表 1 EGD 字段解析

字段名称	字节	作用及含义
Type	1	类型,固定值为 13
Version	1	版本号,固定值为 1
RequestID	2	按每个 Exchanged ID 的数据包发送的数量共 16 位
ProducerID	4	发送方的 IP 地址指的是出数据的设备 IP
Timestamp	8	时间戳,自 1970 年 1 月 1 日起,两个秒和纳秒的 32 位数字
Status	4	状态默认值为 1
Config Sigature	4	组态签名
Reserved	4	保留字段,设为 0
Data	最大 1 400 字节	数据内容

逆向分析得知,该发电厂控制系统通信协议没有进行加密传输,采用明文传输,只是在建立连接时通过认证来实现数据的安全。

经过分析,在 EGD 数据消息部分此系统协议结构又分为值和品质两个字段。其中品质内容共 4 个字节,其数据长度由品质内容中的字符类型字段决定数据长度。具体分析见表 2。

表 2 EGD data 字段解析

品质字段名称	描述
第一字节高 4 位	固定值为 1
第一字节低 4 位	数据类型
第二字节高 4 位	品质状态
第二字节低 4 位	GTW 软件共享点设置
第三字节高 4 位	广播周期
第三字节低 4 位	测点名
第四字节高 4 位	测点描述
第四字节低 4 位	报警状态

2 发电厂控制系统蜜罐架构设计

由于工控蜜罐的诱捕能力主要决定因素是蜜罐的仿真能力,针对现有工控蜜罐,高交互蜜罐成本高,低交互蜜罐诱捕能力不足等问题,该文基于发电厂控制系统仿真提出引入沙盒技术,将发电厂控制系统放入沙盒中运行作为一个蜜罐,完成蜜罐高仿真的同时防止因攻击者识别蜜罐转而攻击真实设备。

如图 2 所示,设计的高交互工控蜜罐总体架构分为数据捕获模块、数据控制模块、数据分析模块。

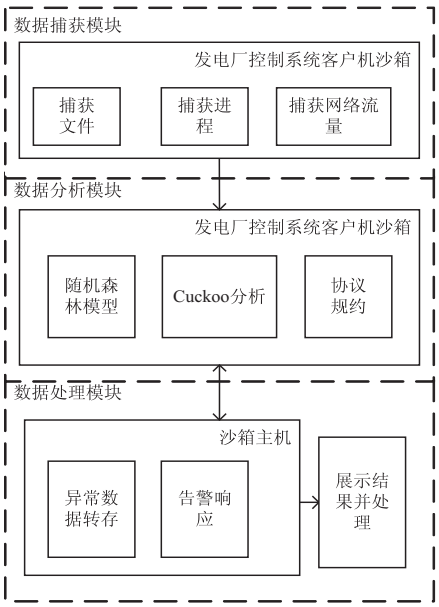

图 2 系统总体架构

系统采用 cuckoo 沙盒分析机制,数据捕获模块为了提高工控蜜罐的诱捕能力,系统仿真采用将真实发电厂控制系统放入沙盒中,形成一个高真实度的交互场景。对沙盒内部信息进行监控并捕获异常数据,主要监控正常的进程、文件路径、网络流量等,捕获可能因攻击产生的异常数据,满足工控蜜罐的捕获需求。

针对网络流量监控,除去正常的通信协议外,主要对发电设备采取的私有通讯协议 EGD 进行解析,并以此为基础开发实现了对 EGD 协议正常规约刻画,识别非规约协议。

数据控制模块,用来将蜜罐捕获到的异常信息进行转储并输出,告知系统安全管理用户并及时阻断。

蜜罐的分析机制主要在数据分析模块上,对蜜罐捕获的文件、恶意代码、异常流量数据进行分析,采用已有的开源沙盒分析工具 cuckoo,将获得的样本通过 xmlRPC 远程过程调用,使用 http 协议进行传输。由 cuckoo 进行分析并将结果输出。

3 发电厂控制系统蜜罐的实现

该文构建的发电厂控制系统蜜罐以开源沙盒架构 cuckoo 为基础,基于发电厂通讯协议 EGD 私有协议进

行开发和发电厂控制系统业务仿真,采用将发电厂控制系统置于 cuckoo 沙盒内,形成高交互仿真程度蜜罐。整个蜜罐系统使用 Django 框架进行开发。

3.1　数据捕获模块

工控蜜罐的仿真程度决定着蜜罐诱捕能力的第一环,采用将发电厂控制系统置于沙盒中营造真实环境,提高蜜罐“甜度”,满足了攻击者针对 EGD 私有协议进行攻击的场景构建。将真实发电厂控制系统部署在沙盒内,不仅使真实系统置于受控范围内,同时沙盒原有的防逃逸功能可以有效防止攻击者,因识别蜜罐借助蜜罐为跳板转而攻击其他设备。而蜜罐最基本的功能是在使攻击者毫无察觉的情况下,捕获攻击者对工控系统发起整个攻击过程的全部信息。系统采用 python3 语言编写来完成工控蜜罐的捕获工作。主要对系统的访问文件路径、进程以及网络流量进行监控和捕获攻击信息。

进程数据监控以及文件数据监控调用的核心库是 psutil。对整个发电厂运行环境进行进程、文件监控,并通过机器学习训练出的模型来优化原有的进程白名单,解决传统的白名单过滤机制单一而且需要经常维护的难题。主要监控进程创建的相关信息,以及进程对文件的操作信息。

对于网络流量信息捕获使用 python 中的 scapy 库抓取系统数据包并保存为 pacp 文件。scapy 已经在内部实现了大量的网络协议如 DNS、ARP、IP、TCP、UDP 等等,可以用它来编写。通过该第三方库将捕获的流量信息转储至数据库中。使用上述方式完成发电厂蜜罐系统的捕获功能。

3.2　数据控制模块

发电厂蜜罐系统针对识别攻击行为主要在进程、文件、网络数据包及其流量上对攻击者采取一定的控制措施。将捕获的进程文件信息通过训练好的模型,判断是否为异常进程,并索引到该异常进程,对非法进程及时发现并告警,客户端可以采用是否阻断进程对异常进程进行处理。对于疑似病毒文件调用 cuckoo 接口,提交至 cuckoo 进行分析并将分析结果页面转回。

具体流程见图 3。

采集网络数据包,在数据链路层解析以太网协议、点对点等协议,识别源 mac 地址和目的 mac 地址等数据链路层基本信息。在网络层解析 IP 协议相关内容,确定源 IP 地址和目的 IP 地址。传输层解析 TCP、UDP 等报文协议内容,并识别出源端口号目的端口号等信息。应用层根据发电厂通讯协议报文特征,识别出工控协议报文,并将其报文格式进行识别。具体流程见图 4。

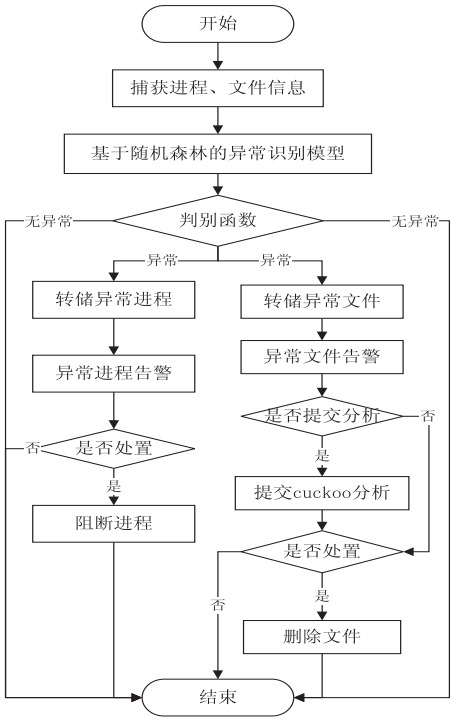

图 3　进程、文件监控流程

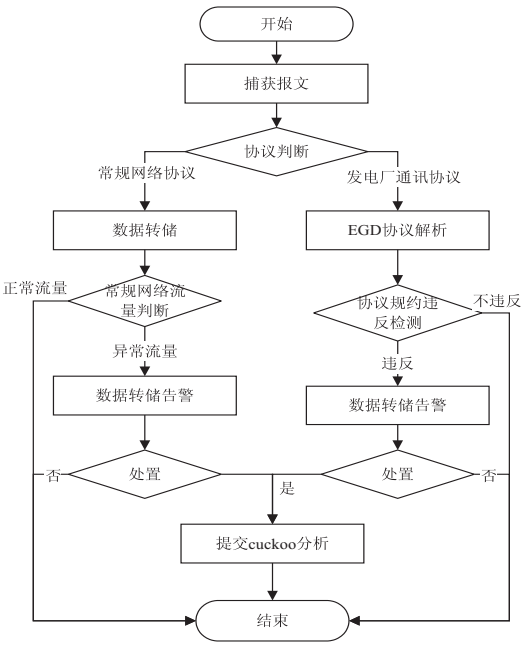

图 4　网络监控流程

3.3　数据分析模块

3.3.1　cuckoo 分析机制

cuckoo 是一个开源的自动化恶意软件分析系统[15]。它用于自动运行和分析文件,并收集全面的分析结果,概述了恶意软件在隔离的操作系统中运行时的行为[15]。整个 cuckoo 分为两部分:

Cuckoo Host:cuckoo 的核心服务端,负责分析任务的启动和分析结果报告的生成,还要负责管理多个虚拟机。

Analysis Guest:分析客户机,这里采用蜜罐将作为

分析的客户机,负责提供虚拟环境供目标样本运行,检测目标的运行情况,并将检测到的数据汇报给 Cuckoo Host。

Cuckoo 总体架构,host 主要接收分析任务,启动作为分析机的蜜罐,将样本和一些必要的分析代码通过 http 协议传输给 client 端。cuckoo 通过其内部分析代码来获取样本的行为,然后待分析完毕,将分析结果通过 tcp 传输给 host 端,将 client 回复到样本执行的状态。

3.3.2 异常进程及文件的识别

发电厂蜜罐系统捕获系统数据以及网络流量数据,可以对其数据通过机器学习识别攻击,将可能存在安全隐患的数据信息转存数据库后,做进一步处理。监控主要文件以及关键访问路径,将进程关联对文件操作的相关数据,将可疑数据调用训练完毕的检测模型接口对其进行判断,并将结果显示。

计算机攻击通常会造成进程对文件的操作异常比如对关键文件的读、写、打开、等;同时攻击时常伴有高 CPU 利用率占用资源以及对内存资源占用、磁盘空间占用、文件的操作时长等,通过进程执行时触发文件的操作对应的时间序列等信息来判断是否为异常数据。

(1)数据的提取。

通过进程捕获工具和蜜罐捕获的进程文件模块,提取电厂系统运行时的正常进程、文件数据的正常数据。攻击数据的获取主要从网站中下载永恒之蓝病毒和震网病毒样本,另一种是从 Honeynet Project(蜜网项目)网站中下载真实攻击恶意软件样本。对捕获的数据进行特征筛选、数据降维、数据归一化处理后得到样本情况:正常数据 3 710,攻击数据 2 490,共计 6 200。

(2)最优分类模型筛选。

将捕获的进程数据提取进程行为的特征向量,建立计算机正常进程的信息模型,通过进程对文件重要层级的操作,进程对磁盘文件活动的监控等,使用机器学习训练模型来判别异常进程。由于识别攻击问题属于二分类问题即是否受到攻击。该文主要采用以下机器学习进行建模训练:KNN、逻辑回归、随机森林、KVM、决策树。主要选取的评价指标有:精确率(precision)、召回率(recall)、F1 度量(F1-score)、准确率。详细评价指标见公式(1)~公式(4)。

$$\text{precision} = \frac{TP}{TP + FP} \tag{1}$$

$$\text{recall} = \frac{TP}{TP + FN} \tag{2}$$

$$\text{F1 - score} = \frac{2TP}{2TP + FP + FN} \tag{3}$$

$$\text{Acc} = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

现将分类算法的评价结果展示在表 3 中。

表 3 模型评价结果对比

模型	P	R	F1	Acc
KNN	0.948	0.906	0.931	0.931
逻辑回归	0.784	0.889	0.833	0.864
随机森林	1	0.997	0.998	0.999
KVM	0.985	0.914	0.953	0.962
决策树	1	0.896	0.945	0.954

上述 5 种分类器均采用同样的数据集进行训练,通过对比上述 5 个经典分类模型在 4 个评价指标上的结果可知,5 种算法中精确率较高的是决策树和随机森林分类器都达到了 1,但是在召回率等其他度量上,并没有随机森林高,因此采用随机森林分类器对进程相关数据进行分析并判定异常。

3.3.3 异常网络流量的识别

将识别出的异常数据分为两类,第一类是普通网络数据,将捕获到的将异常数据包进行转储并告警,同时将形成的 pacp 文件可以选择提交 cuckoo 进行处置。第二类是工控数据包,主要指 EGD 报文,分析工控协议的报文长度,工控协议报文的数据单元标识信息是否完整且正确。根据报文解析结果对报文进行分流,工控协议报文进行进一步的深入解析,将解析后的 EGD 协议对报文进行违反规约检测。

4 发电厂控制系统蜜罐测试与分析

4.1 实验环境部署

根据发电厂控制系统环境网络结构,系统主干网络采用 TCP/IP 工业以太网结构设计,采用标准 EGD 协议,构成发电厂控制系统的基本网络架构,组成单元机组数据高速网络(Unit Data Highway,UDH),负责实现系统各控制器与人机接口单元(HMI)的互联及数据共享。

控制器与 IO 模块间通讯网络通过总线连接设备与冗余控制器构成串行环网结构,实现 IO 模块与控制器的实时数据交互。

基于发电厂原有环境,现将发电厂蜜罐部署如下。将发电厂蜜罐系统接入真实系统以太网中形成闭环,通过沙盒客户机机制将真实系统放入沙盒中,模拟一个或多个真实的工程师站或网关工具。并将多个客户机与分析管理主机相连。

4.2 发电厂控制系统蜜罐系统功能测试

针对发电厂控制系统的工控蜜罐系统进行业务逻辑测试,主要任务是检验蜜罐系统在捕获数据以及识别攻击两方面。在虚拟机内以上述方式部署该蜜罐系

统,运行数据转储模块主程序和数据捕获模块主程序。

4.2.1　测试识别 EGD 协议数据

测试系统识别 EGD 协议信息,查看系统对 EGD 协议分析的能力。图 5 是系统捕获的日志信息。

```
0::c::29::f2::a2::32,ff::ff::ff::ff::ff::ff,192.168.59.128,
192.168.59.255,18246,18246,d,1,0,78.0.0.0,1::0::0::0,f1::f1
::c::61::80::28::97::1f::0::0::1::0::0::1::0::0::5e::aa::b0
::60::0::0::10::28::0::0::0::0::0::0::11::28::0::0::0::0::0
::0::12::28::0::0::0::0::0::0::0::0::0::13::28::0::0::0:
:0::14::28::0::0::0::0::0::0::15::28::0::0::0::0::0::0::0::
15::28::0::0;
0::c::29::f2::a2::32,ff::ff::ff::ff::ff::ff,192.168.59.128,
192.168.59.255,18246,18246,d,1,1,78.0.0.0,1::0::0::0,f1::f1
::c::61::40::52::64::22::0::0::1::0::0::1::0::0::5e::aa::b0
```

图 5　EGD 协议捕获日志

通过包捕获工具对比可知,本蜜罐系统可以捕获并解析出需要的数据包信息。

4.2.2　测试异常进程告警

测试系统捕获关联文件的异常进程信息。通过后台日志显示抓取到的异常日志,实时监控系统进程异常,如图 6 所示。

```
2021/10/31 12:52,wemeetapp.exe,--pipename=4341d_740AA3E2CC28,running,70,64944,48.649 MB,2
2021/10/31 12:52,wemeetapp.exe,D:\txhy\WeMeet\wemeetapp.exe,running,17,99048,1.112 MB,0.0
2021/10/31 12:52,wemeetapp.exe,--pipename=4341d_740AA3E2CC28,running,68,32960,16.261 MB,0
2021/10/31 12:52,wemeetapp.exe,--pipename=4341d_740AA3E2CC28,running,73,32960,28.434 MB,1
2021/10/31 12:52,wemeetapp.exe,--pipename=4341d_740AA3E2CC28,running,75,32960,44.088 MB,1
2021/10/31 12:52,wemeetapp.exe,--pipename=4341d_740AA3E2CC28,running,75,32960,44.699 MB,1
2021/10/31 12:53,wemeetapp.exe,--pipename=4341d_740AA3E2CC28,running,74,32960,44.699 MB,1
2021/10/31 12:53,wemeetapp.exe,--pipename=4341d_740AA3E2CC28,running,74,32960,44.718 MB,1
2021/10/31 12:53,EXCEL.EXE,C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE,runn
2021/10/31 12:53,@WanaDecryptor@.exe,@WanaDecryptor@.exe,Process Start,70,5000,48.649 MB,
2021/10/31 12:53,@WanaDecryptor@.exe,@WanaDecryptor@.exe,Thread Create,70,5000,48.649 MB,
2021/10/31 12:53,@WanaDecryptor@.exe,C:\Users\vera\Desktop\wcry\wcry2.0\@WanaDecryptor@.e
2021/10/31 12:54,@WanaDecryptor@.exe,C:\Windows\System32\ntdll.dll,running,68,4152,1192,3
```

图 6　异常进程信息捕获

5　结束语

主动防御技术中,蜜罐技术在工控领域的应用日渐成熟,针对不同的工业系统使用的工控协议,该文解析了 EGD 通讯协议,深度分析其协议内部数据,分析在发电厂正常数据的协议包内容情况并做出攻击识别。同时使用蜜罐的思想与沙盒技术的结合,完成蜜罐的高仿真环境。通过监控网络流量、工控协议包和进程关联文件等相关信息, 识别异常。进而提升整个工业控制系统网络环境安全。

参考文献:

[1] 李沁园,孙　歆,戴　桦,等. 工业控制系统设备指纹识别技术[J]. 网络空间安全,2017,8(1):60-65.

[2] 靳　敏,刘　萧. 一体化“国网云”安全防护体系设计[J]. 电力信息与通信技术,2019,17(1):78-82.

[3] 董良遇,赵　冉. 我国工业信息安全态势分析与思考[J]. 信息技术与网络安全,2019,38(12):37-41.

[4] STEVENS C. Assembling cybersecurity:the politics and materiality of technical malware reports and the case of Stuxnet [J]. Contemporary Security Policy,2020,41(1):129-152.

[5] 李　东. 震网病毒事件浅析及工控安全防护能力提升启示[J]. 网络安全技术与应用,2019(1):9-10.

[6] 弭相辰. 从“震网病毒”与乌克兰停电事件看电力企业信息安全[J]. 大众用电,2016(S2):50-56.

[7] 朱朝阳. 委内瑞拉大停电事故的背后[J]. 国家电网,2019(5):72-74.

[8] 刘绪尧. 美输油管道遭“黑”或带来涟漪效应[ER/OL]. 2021-05-12. http://www. xinhuanet. com/.

[9] 胡　汉. 物理隔离也会被跨网入侵[N]. 中国航天报,2020-10-15(003).

[10] 黄　鑫,陈德成,孙　军,等. 网络攻击下电力系统信息安全研究综述[J]. 电测与仪表,2017,54(23):68-74.

[11] SIDDHARTH S,ADAM H,MANIMARAN G. Cyber-physical system security for the electric power grid[J]. Proceedings of the IEEE,2012,100(1):210-224.

[12] GE Energy. GE Fanuc 网络及通讯用户手册[EB/OL]. 2013. https://www. docin. com/p-1925734744. html.

[13] 姬胜凯,刘仁辉,董　伟,等. 协议安全测试在工业 DCS 系统测评中的应用[J]. 微型机与应用,2017,36(20):10-13.

[14] 臧振胜. 工业气相色谱仪数据网关的研究与实现[J]. 中国仪器仪表,2020(6):36-39.

[15] 秦　鹏. 基于 Cuckoo 的恶意程序行为分析及检测系统研究[D]. 西安:西安电子科技大学,2017.