UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US11456789

Malware Detection Algorithm for Industrial Control Systems

Issue Date: March 15, 2023

Filing Date: April 12, 2021

Priority Date: April 12, 2020

Assignee: DeepShield Systems, Inc.

Inventors: Rodriguez, Elena; Morrison, James; Chen, Marcus

Term: 20 years from filing date

ABSTRACT

A system and method for detecting malware in industrial control systems using machine learning algorithms and behavioral analysis. The invention comprises a multi-layered detection framework that monitors operational technology (OT) network traffic patterns, system calls, and process behaviors to identify potential malicious activities in real-time. The system employs proprietary neural network architectures optimized for industrial protocol analysis and anomaly detection in SCADA environments.

CLAIMS

A method for detecting malware in industrial control systems, comprising:

a) receiving network traffic data from industrial control system components;

b) analyzing said data using a trained neural network architecture;

c) generating behavioral fingerprints for normal operational patterns;

d) detecting deviations from established behavioral baselines;

e) classifying potential threats using a multi-stage verification process.

The method of claim 1, wherein the neural network architecture comprises:

a) an input layer optimized for industrial protocol parsing;

b) multiple hidden layers implementing proprietary activation functions;

c) an output layer providing threat classification scores;

d) adaptive learning capabilities for continuous model improvement.

A system for implementing the method of claim 1, comprising:

a) network sensors deployed across industrial control system infrastructure;

b) a central processing unit executing the neural network algorithms;

c) a secure storage system for behavioral fingerprint databases;

d) an alert generation and response automation module.

[Claims 4-20 omitted for brevity]

DETAILED DESCRIPTION

Background

The present invention relates to cybersecurity systems for industrial control environments, specifically addressing the detection of sophisticated malware targeting operational technology infrastructure. Traditional signature-based detection methods prove insufficient for protecting critical industrial systems from emerging threats and zero-day attacks.

Technical Implementation

The invention implements a novel approach to malware detection through:

Protocol-Aware Traffic Analysis

- Custom packet inspection engines
- Industrial protocol state tracking
- Behavioral pattern extraction

Neural Network Architecture

- Proprietary layer configurations
- Optimized weight initialization
- Dynamic threshold adjustment

Threat Classification System

- Multi-stage verification process
- False positive reduction mechanisms
- Automated response triggers

Preferred Embodiments

The primary embodiment comprises a distributed sensor network feeding data into a centralized analysis engine. The system maintains separate processing pipelines for:

Network traffic analysis

Process behavior monitoring

System call tracking

Configuration change detection

Novel Features

The invention introduces several technological advances:

Adaptive learning algorithms specifically optimized for industrial protocols

Real-time behavioral baselining with minimal performance impact

Automated response mechanisms integrated with existing security infrastructure

Proprietary neural network architectures designed for OT environments

DRAWINGS

[Reference to attached technical drawings showing system architecture and data flow diagrams]

INDUSTRIAL APPLICABILITY

This invention has direct application in:

- Manufacturing facilities
- Power generation plants
- Water treatment facilities
- Oil and gas infrastructure
- Maritime vessels
- Critical infrastructure protection

LEGAL NOTICES

This patent document contains proprietary and confidential information of DeepShield Systems, Inc. All rights reserved. Unauthorized reproduction or distribution of this patent or any portion of it may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

EXECUTION

Granted this 15th day of March, 2023

[Signature Block]

United States Patent and Trademark Office

Alexandria, Virginia

[Official Seal]

Patent Examiner: [Name]

Registration No: [Number]