International Journal of Multidisciplinary Conference Proceedings
editor@ijmcp.com
https://www.ijmcp.com

A Holistic Framework for Detecting and Mitigating Fileless Malware in Operational Technology Environments

1st Faheem Hussain, 2ndSyed Farman Hussain, 3rdUsman Ahmed & 4thFarayha Hydari

1st, 2nd, 3rd, 4th Dawood University of Engineering and Technology, Pakistan

KEYWORDS

Fileless Malware Operational Technology (OT), Security Memory Forensics, Behavioral Analytics, Endpoint Detection and Response (EDR)

ARTICLE HISTORY

Date of Publication:16-04-2025

Conference Organizer(s)

Research Consultancy on Social & Management Development
&
University of Karachi
DHA Suffa University

ABSTRACT

Fileless malware exists as a highly intricate and dominant security threat that shows increasing presence most strongly in Operational Technology environments. These malicious intrusions work in system memory space exclusively so they do not produce disk-based artifacts that signature-based detection methods would recognize. This document explores the essential challenge of discovering and reducing fileless malware within essential Operational Technology infrastructure that powers vital systems such as power networks and water treatment plants and industrial production facilities. Modern detection methods should focus on memory forensics along with behavioural analytics and endpoint detection response (EDR) and network traffic analysis since file-based artifacts cannot be relied upon. A new framework specifically created for operating technology environments integrates advanced detection methods which target the needs of limited resources alongside real-time operational integrity in legacy systems. The framework uses machine learning algorithms and threat intelligence integration along with anomaly detection capabilities to identify indicators of compromise (IOCs) in advance. The solution includes multiple strong protection measures which include application authorisation together with zero trust architecture and document macro restriction methods for securing users against attacks.

Corresponding Email: Fhaemali234@gmail.com

Volume-Issue-Page Number: 2(1) 21

Citation: Hussain, F., Hussain, S. F., Ahmed, U., & Hydari, F. (2025). A Holistic Framework for Detecting and Mitigating Fileless Malware in Operational Technology Environments. *Proceedings of the 1st International Conference on Innovation and Sustainability in Management and Social Sciences, *International Journal of Multidisciplinary Conference Proceedings, 2(1).*