(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :05/10/2023

(21) Application No.202311066860 A
(43) Publication Date : 20/10/2023

(54) Title of the invention : METHOD FOR DETECTING FILE ALTERING MALWARE IN A VIRTUAL MACHINE-BASED ANALYSIS ENVIRONMENT

(51) International classification	:G06F0021560000, G06F0021550000, G06F0021570000, G06N0020000000, G06F0009455000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
2)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The system (100) for detecting file altering malware is a comprehensive cybersecurity solution. It features a robust virtual machine environment (102) supported by high-performance processors and ample memory capacity, ensuring efficient analysis of potentially malicious files. This system combines a Behavioral Analysis Module (104) that monitors file activity within the virtual machine, including file modifications, network connections, and system resource access, with a Signature Analysis Module (106) that compares file attributes against a database of known malware signatures. A Risk Assessment Module (108) assigns risk scores, dynamically adjusting sensitivity based on behavior and signature analysis. The Response and Mitigation Module (110) takes appropriate actions, while an Updating Mechanism (112) keeps the signature database current. Detailed reports are generated, and a Machine Learning Module (116) continuously enhances detection capabilities, making it a robust defense against file altering malware.

No. of Pages : 25 No. of Claims : 10