(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311054818 A

(19) INDIA

(22) Date of filing of Application :16/08/2023

(43) Publication Date : 15/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR REAL-TIME DETECTION OF MALICIOUS ATTACKS IN A KERNEL MODE

(51) International classification	:G06F0021560000, G06F0021550000, H04L0045000000, G06F0021530000, A61B0005000000
(86) International Application No	:NA
Filing Date	:NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number	:NA
Filing Date	:NA
(62) Divisional to Application Number	:NA
Filing Date	: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 :

Embodiments of the present disclosure relates to a system (100) and method (300) for real-time detection of malicious attacks in a kernel mode. In an aspect, the present disclosure discloses a system (102) for real-time detection of malicious attacks in a kernel mode. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to intercept one or more network calls in real-time. Further, the processor (202) is configured to extract patterns of malicious attacks from the one or more intercepted network calls. Next, the processor (202) is configured to compare the extracted patterns of malicious attacks to known patterns of malware and steganography in a database (220). In the end, the processor (202) is configured to block the detected patterns of malicious attacks.

No. of Pages : 24 No. of Claims : 10