(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :09/10/2023

(21) Application No.202311067618 A

(43) Publication Date : 22/12/2023

(54) Title of the invention : SYSTEM AND METHOD TO DETECT AND MITIGATE TIME-BOMB MALWARE THREATS IN A NETWORK ENVIRONMENT

| | |
|---|---|
| (51) International classification | :G06F0021560000, G06F0021550000, H04W0012128000, H04L0043040000, H04L0012280000 |
| (86) International Application No<br>Filing Date | :NA<br>:NA |
| (87) International Publication No | : NA |
| (61) Patent of Addition to Application Number<br>Filing Date | :NA<br>:NA |
| (62) Divisional to Application Number<br>Filing Date | :NA<br>: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 present disclosure relates to a system (100) and method (300) includes a processor (102) and memory (104) that execute a set of instructions to detect and mitigate time-bomb malware threats in a network environment. The system (100) captures and logs one or more network activities within a network environment and analyzes the captured one or more network activities to establish behavioral baselines and detect anomalies indicative of a time-bomb malware. The system stores a set of known malware signatures associated with the time-bomb malware and compares the results of the behavioral analysis with the known malware signatures to identify potential instances of the time-bomb malware. Upon detection of the time-bomb malware, the processor (102) sends an alert to the one or more users (114) through one or more computing devices (112).

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