(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :09/08/2023

(21) Application No.202311053324 A

(43) Publication Date : 01/09/2023

(54) Title of the invention : AUTOMATIC IDENTIFICATION OF MALICIOUS BUDGET CODES AND COMPROMISED WEBSITES EMPLOYED IN PHISHING ATTACKS

(51) International classification	:G06F0021550000, G06F0021560000, G06F0021570000, H04L0051000000, H04W0012122000
(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 :

The system (100) for automatic identification of malicious budget codes and compromised websites in phishing attacks consists of several interconnected modules. The Traffic Analysis module (102) continuously monitors incoming traffic using techniques like packet inspection, behavioral analysis, and machine learning algorithms to identify potential phishing attacks. The Budget Code Detection module (104) analyzes the traffic to identify suspicious budget codes, comparing them against a database of known codes. The Compromised Website Detection module (106) identifies compromised websites by comparing them against a database of known compromised sites. The Alert Generation module (108) promptly generates alerts to notify system administrators about detected potential phishing attacks. The Reporting module (110) generates comprehensive reports on the number and type of attacks detected, aiding in trend analysis and vulnerability identification. With the use of machine learning algorithms and comprehensive databases, the system provides real-time detection, scalability, and the ability to identify emerging threats, enhancing phishing attack identification compared to traditional methods.

No. of Pages : 22 No. of Claims : 10