



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



Indian
Cyber
Crime
Coordination
Centre

**NATIONAL CYBERCRIME THREAT ANALYTICS UNIT
TAU – 115 | Telecom Intelligence Report**

Abuse of ‘SMS Headers’ in Transnational ‘Stock Market Investment Fraud’

Prepared By
Indian Cyber Crime Coordination Centre (I4C)
Ministry of Home Affairs
New Delhi

18th April 2024



@cyberdostI4c



@CyberDostI4c



@cyberdostI4c



@cyberdost



@cyberdostI4c



@cyberdost.I4c



@cyberdostI4c



@cyberdost



@cyberdost

Table of Contents

1. Introduction.....	3
2. Executive Summary.....	3
3. Observations	4
4. Recommendations.....	5
5. Details of SMS Headers being Misused.....	6
6. Screenshots of SMSes	7
7. Confirmation from Entities.....	9

1. Introduction

The Ministry of Home Affairs, Government of India has established the **Indian Cyber Crime Coordination Centre (I4C)** to provide a framework and eco-system for Law Enforcement Agencies (LEAs) to deal with cybercrime in a comprehensive and coordinated manner. The **National Cybercrime Threat Analytics Unit (NCTAU)** is one of the vertical of I4C which is instrumental in issuing alerts, advisories, and carrying out analysis of cyber threats and sharing the reports with various Ministries / Department, and other stakeholders for the prevention of cybercrime in the country.

2. Executive Summary

National Cybercrime Threat Analytics Unit has observed a sharp rise in a new pattern of transnational cyber enabled financial fraud. During analysis of National Cybercrime Reporting Portal complaints and inputs from State Police, a new pattern of transnational investment scam is observed where the cyber criminals are impersonating stockbrokers, financial advisors, or company executives of capital investment companies majorly through fake mobile apps, websites, and WhatsApp / Telegram. Fraud WhatsApp groups are learnt to be operated from Cambodia / Hong Kong.

At the early stage, these apps were learnt to be circulated through Google Playstore, Apple App store and via web links that are sponsored majorly through Instagram and Facebook Advertisements targeting users with 'interest' in 'Stock Market'.

Recently, it has been observed that the cybercriminals have started abusing A2P SMS by sending bulk SMSes to the potential victims with

luring messages and a link which redirected to a WhatsApp group where further crime takes place.

3. Observations

- It is observed that there is potential takeover / misuse of SMS Header, Entity and Template ID from either Telemarketer end or through DLT platform.
- These Identifiers are being used to send SMSes by cyber fraudsters without consent / knowledge of Entity / Header Owner which is a serious cause of concern as victims believe the SMS is coming from genuine entity and proceeds with the messages.
- Fraud SMS containing link to join WhatsApp group are being sent through **V-CON Mobile & Infra Private Ltd. (VM IPL)** and **Bharti Airtel**.
- NCTAU has confirmed from some of the entities that they have not sent the SMS and header / template has been mis-used.
- It is also found that the SMS Header Entity as well as template are totally different, and the SMS being sent relating to Stock Market through these headers.
- A report on misuse of SMS Headers related to similar threat actor / modus operandi had also shared with TRAI vide report no. **TAU-042**.

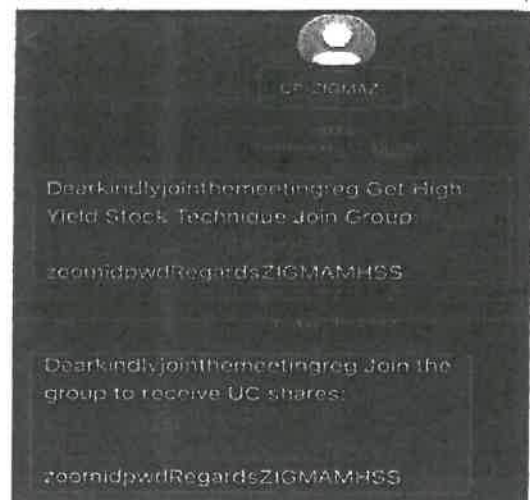
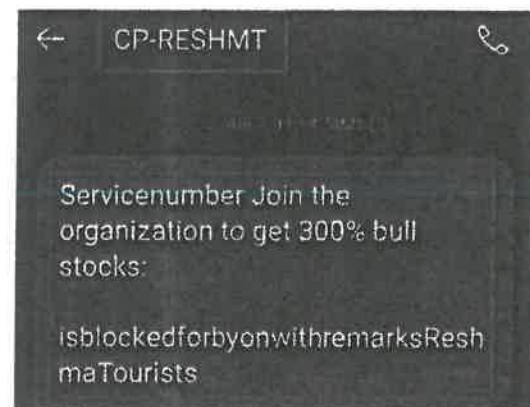
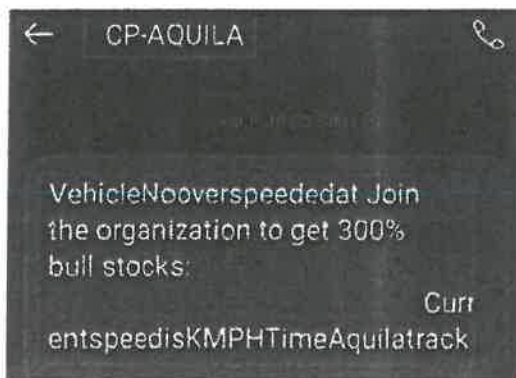
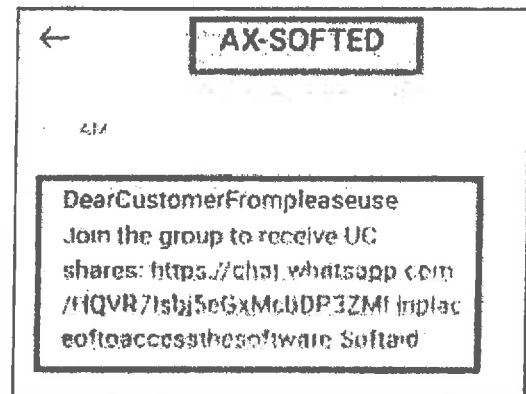
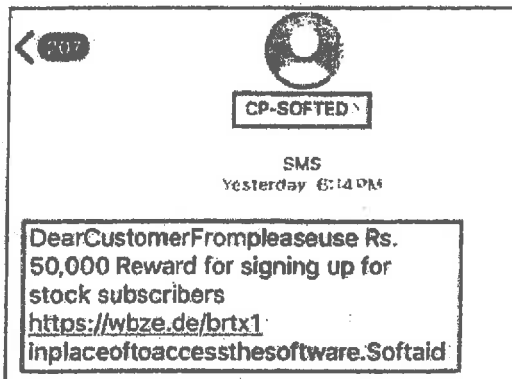
4. Recommendations

- Identify the root cause of the misuse / hacking of Entity ID, Header ID and Template ID.
- Identify the Tele-marketer involved in sending the messages shared in the report.
- Gauge the scale of abuse and number of SMS sent along with the source of phone numbers used by TM to send SMS.
- Telecom operators may implement AI based detection mechanism to detect WhatsApp group links and redirecting web links.
- Explore option to put additional authentication mechanism which will ask for re-authorization in case of Tele-Marketer change.

5. Details of SMS Headers being Misused.

Sr.No.	Prefix	Header	Principal Entity and Address	Purpose
1.	CP	SOFTED	SOFT AID COMPUTER 18/2, Ramdas Colony, M J College Rd JALGAON, Jalgaon, Maharashtra, 425001	Transactional/Service
2.	CP	RESHMT	Reshma Tourists Shop No 17, S.NO 124 1 A, Rajeev Gandhi Vanijya Sankeerna, Marpady Village, Mudbidri, Dakshina Kannada, Karnataka	Transactional/Service
3.	CP	AQUILA	Zeliot Connected Services Private Limited 803/1, 803/A-1-3, 76th A Cross, West of Chord Road, 6th Block, Rajajinagar	Transactional/Service
4.	CP	OCNSTK	OCEAN STOCKS 606, Golden Traengal, Opp Stediam, Post Navjivan, Ahmedabad	Transactional/Service
5.	CP	ZIGMAZ	Meenakshi Ammal Educational Trust, No.81/82, Veerabathra Nagar, Medavakkam, Chennai, Kancheepuram, Tamil Nadu, 600100.	Transactional/Service
6.	CP	PSRDFM	PSR Dairy Farm 77/3 Near Rto Office, Peruvangur Village, Kallakurichi, Kallakurichi, Tamil Nadu, 606213	Transactional/Service
7.	CP	TRAMCO	The Ramco Cements Limited, Ramamandiram, Rajapalayam, Rajapalayam, Tamil Nadu, 626117	Transactional/Service
8.	AX	DBSJNP	Smt dhanraji devi shri bhuleshwar singh inter college, kadipur, ramdayalganj, jaunpur, uttar pradesh, 222105.	Transactional/Service

6. Screenshots of SMSes



188

CP-ZIGMAZ

SMS
Today, 11:39 AM

Dearkindlyjointhemeetingreg Join the group to receive UC shares: <https://api.whatsapp.com/gend?phone=919725337938>
zoomidpwdRegardsZIGMAMHSS

CP-PSRDFM

SMS
Today, 11:21 AM

PSRDAIRYFARMDIAMLtr Professional Stock Analysis Link:
PiMLtr

210

AX-DBSJNP

SMS
Today, 1:52 PM

DearParentsAdmissionsareopenfor Professional Stock Analysis Link: chat.whatsapp.com/ISV4QyW4IG1AMk8ibUsf1A
toFROMDBSINTERCOLLEGE

CP-TRAMCO

SMS
Today, 11:07 AM

CementdespMTQdtMtd Blackstone recommended fine stock, click to get it now!
<https://wa.me/916899793186>
RamcoCements

Today, 12:06 PM

CementdespMTQdtMtd Professional Stock Analysis Link:<https://chat.whatsapp.com/1xQTrYudPSzL8iCodAmdwC>
RamcoCements

Today, 1:01 PM

CementdespMTQdtMtd Blackstone recommended fine stock, click to get it now!<https://wa.me/911979197919>
RamcoCements


7. Confirmation from Entities

Email Communication to Softed Computers

softaid computer April 15, 2024 11:04 AM


Good Morning.

As discussed over telephonically, please see the following SMSes being forwarded through your registered SMS Header with TPAI and requested to kindly confirm that whether these SMSes are being sent through your company or not.


CP-SOFTED

SMS
Yesterday, 7:12 AM


DearCustomerFrompleaseuse Rs. 50,000 Reward for signing up for stock subscribers
<https://wbze.de/rtx1>
inplaceoftoaccesssoftware.Softaid


AX-SOFTED

DearCustomerFrompleaseuse
Join the group to receive UC shares: <https://chat.whatsapp.com/HQYB7t8bj5eGxMcbDPJZMI> inplac
eoftoaccesssoftware.Softaid

Response from Softed Computers

Request for confirmation - reg 2 messages


 From: softaid computer April 15, 2024 1:30 PM

Dear sir,
After reviewing the messages forwarded to us, we can confirm that they were not sent by our company.

Regards,
Suresh Wankhede
www.softaidcomputers.com | softaid.computer@gmail.com

Email Communication to Zeliot

Request for confirmation - reg 2 messages

 From: akshay@zeliot.in April 15, 2024 12:44 PM

To: akshay@zeliot.in

Good Afternoon,

As discussed telephonically, please see the following SMS being forwarded through your registered SMS Header with TRAI and requested to kindly confirm that whether this SMSes are being sent through your company or not.


← CP-AQUILA 📞

VehicleNooverspeededat Join
the organization to get 300%
bull stocks. Curr
entspeediskMPHITimeAquilatrack

An early response in this regard will be highly appreciated.

Response from Zeliot

Request for confirmation - reg 2 messages

 From: akshay@zeliot.in April 15, 2024 5:10 PM

To:

Cc: sumeet@zeliot.in anup@zeliot.in

Hi

These SMSs are not being sent by us. We are not into this business case. This seems to be a case of hacking and on this suspect, we have blocked the this header through our gateway partner.

Kindly let me know if any additional action needs to be taken.



भारतीय दूरसंचार विनियामक प्राधिकरण
TELECOM REGULATORY AUTHORITY OF INDIA
भारत सरकार / Government of India



Dated : 16th February, 2023

DIRECTION

Subject: Direction under section 13, read with sub-clauses (i) and (v) of clause (b) of sub-section (1) of section 11, of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) regarding measures to curb misuse of Headers and Content Templates under Telecom Commercial Communication Customer Preference Regulation, 2018 (6 of 2018).

F. No. RG-25/(6)/2022-QoS - Whereas the Telecom Regulatory Authority of India (hereinafter referred as the "Authority"), established under sub-section (1) of section 3 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) (hereinafter referred to as "TRAI Act"), has been entrusted with discharge of certain functions, inter alia, to regulate the telecommunication services; ensure technical compatibility and effective inter-connection between different service providers; lay-down the standards of quality of service to be provided by the service providers and ensure the quality of service and conduct the periodical survey of such services provided by the service providers so as to protect the interest of the consumers of telecommunication service;

2. And whereas the Authority, in exercise of the powers conferred upon it under section 36, read with sub-clause (v) of clause (b) and clause(c) of sub-section (1) of section 11, of the TRAI Act, made the Telecom Commercial Communications Customer Preference Regulations, 2018 (6 of 2018) dated the 19th July, 2018 (hereinafter referred to as the "regulations"), to regulate unsolicited commercial communications;

3. And whereas regulation 3 of the regulations provides that every Access Provider shall ensure that any commercial communication using its network only takes place using registered headers assigned to the sender for the purpose of commercial communication;

4. And whereas regulation 5 of the regulations, inter alia, provides that every Access Provider shall develop or cause to develop an ecosystem to regulate the delivery of the commercial communications as provided for in the regulations and to comply with any other directions, guidelines and instructions issued by the Authority in this regard;

5. And whereas regulation 8 of the regulations, inter alia, provides that every Access Provider shall, before allowing any commercial communication through its network, develop Codes of Practice (hereinafter referred to as "CoPs") for

महानगर दूरसंचार भवन, जवाहरलाल नेहरु मार्ग / Mahanagar Doorsanchar Bhawan, Jawahar Lal Nehru Marg
(ओल्ड मिंगो रोड), नई दिल्ली-110002 / (Old Minto Road), New Delhi-110002
फैक्स / Fax : +91-11-23213294, ईपीबीएक्स नं. /EPBX No. : +91-11-23664145

"प्रभावी विनियमन - सुगम संचार"
"Effective Regulation - Ease of Communication"

75
आजादी का
अमृत महोत्सव

Jai Prakash

Entities of ecosystem (CoP- Entities) as per Schedule-I and develop CoP for Unsolicited Commercial Communications Detection (CoP-UCC_Detect) as per Schedule-IV, register entities as provided for in the CoP for Entities and register Senders and assign the headers/ header roots;

6. And whereas sub-regulation (3) of regulation 12 of the regulations provides that Access Providers shall deploy, maintain and operate a system, by themselves or through delegation, to register persons, business entities or legal entities in making Commercial Communication through its network involved from origination, transmission or delivery and have adequate documentary evidence in support to provide their identities;

7. And whereas item 4 (1) of Schedule I to the regulations provides that every Access Provider shall carry out Header Registration functions as provided in the regulations and the relevant provisions of the said item reads as under-

"4. Every Access Provider shall carry out following functions: -

1. Header Registration Function (HRF)

....

(b) carry out pre-verifications of documents and credentials submitted by an individual, business entity or legal entity requesting for assigning of the header;

(c) bind with a mobile device and mobile number(s), in a secure and safe manner, which shall be used subsequently on regular intervals for logins to the sessions by the header assignee;

....

(f) carry out additional checks for look-alike headers which may mislead to a common recipient of commercial communication, it may also include proximity checks, similarity after substring swaps specifically in case of government entities, corporate(s), well-known brands while assigning headers irrespective of current assignments of such headers, and to follow specific directions, orders or instructions, if any, issued from time to time by the Authority;"

Jain P.S.

8. And whereas item 4 (3) of Schedule I to the regulations provides that every Access Provider shall carry out Content Template Registration functions as provided in the regulations and the relevant provisions of the said item reads as under-

"4. Every Access Provider shall carry out following functions: -

....

(3) Content Template Registration Function (CTRF)

(a) to check content of the template being offered for registration as a transactional template and service message template;

(b) to identify fixed and variable portion(s) of the content in the offered transactional template and service message template with identification of type of content for each portion of variable part of the content, e.g. date format, numeric format, name of recipient, amount with currency; reference number, transaction identity;

(c) to estimate the total length of variable portion, viz. total length of fixed portion for a typical transactional message, service message for offered template;

(d) to de-register template or temporarily suspend use of template;

....

(f) to check content of the template being offered for registration as a promotional from perspective of content category;"

9. And whereas item 5 (1)(c) of Schedule I to the regulations provides that every Access Provider shall set up functional entities like Header Registrar for keeping record of headers throughout its lifecycle, i.e. free for assignment, assigned to an entity, withdrawn, surrendered, re-assigned etc.;

10. And whereas item 2 of Schedule VI to the regulations, inter alia, provides that in preparation of migration plan, the Access Provider shall stop assigning headers without verification of identity and scope of senders and they shall register the existing assignee of headers after verification of identity and scope documents of Unsolicited Commercial Communications senders;

Jai P. S.

11. And whereas, the Authority has noticed that-

(a) Headers and Content templates of Principal Entities (hereinafter referred to as "PEs") are being misused by some telemarketers due to failure of authentication of data of PEs and there is an urgent need to re-verify the authenticity of all headers and templates approved on Distributed Ledger Technologies (hereinafter referred to as "DLT") platform and cleanse the data within a definite time frame, and that the process of cleansing DLT data requires periodical actions by the Access Providers;

(b) look-alike headers are being registered by Access Providers on names of different Principal Entities and many times, such headers create confusion among recipients of message or even misused by some entities for their benefit; and

(c) the number of variables in a template is not defined in CoPs which leads to misuse of the same and moreover, the promotional content is being passed in the variable portions of content templates and therefore, in order to minimize the said misuse, number of variables allowed in content template needs to be limited in a way that not only gives PEs enough flexibility to phrase their content but at the same time, there are reasonable restrictions on number and placement of variables;

12. And whereas regulation 17 of the regulations provides that Authority may direct Access Providers to make changes, at any time, in the CoPs and Access Providers shall incorporate such changes and submit revised CoPs within fifteen days from the date of direction issued in this regard;

13. And whereas regulation 18 of the regulations provides that every Access Provider shall comply with submitted CoPs provided that any provision in CoP shall not have effect to the extent of being inconsistent with these regulations;

14. And whereas regulation 19 of the regulations provides that the Authority reserves the right to formulate a standard CoP in case the formulated CoP is deficient to serve the purposes of these regulations;

15. And whereas regulation 20 of the regulations provides that every access provider shall comply with the provisions of Standard CoPs;

16. And whereas the Authority is of the view that the above mentioned provisions of the regulations pertaining to Headers and Content Templates are

Jait Singh

not strictly being followed, and that there is a need to make changes in the CoPs so as to curb the misuse of Headers and Content Templates;

17. Now, therefore, the Authority, in exercise of the powers conferred upon it under section 13, read with sub-clauses (i) and (v) of clause (b) of sub-section (1) of section 11, of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), and the provisions of the Telecom Commercial Communications Customer Preference Regulations, 2018 hereby directs all the Access Providers to:

- (a) Ensure re-verification of all Headers registered on DLT platform within thirty days from the date of issue of this direction and blocking of unverified headers;
- (b) ensure to develop, within sixty days from issue of the direction, a system to –
 - (i) temporarily deactivate all headers which remain unused in last thirty days;
 - (ii) reactivate headers by PEs through an online process; and
 - (iii) ensure that PE shall classify every header at the time of registration as 'temporary' or 'permanent' header, as the case may be, and that the 'temporary' header shall be deactivated after the time duration for which such 'temporary' header has been registered;
- (c) ensure that each Header is distinct and shall reject, during registration, such Headers which are similar by virtue of combination of small case or large case letters;
- (d) ensure re-verification of all content templates within sixty days of issue of this direction and blocking of unverified templates ;
- (e) incorporate procedure for quarterly re-verification of Headers and content templates in their respective CoPs;
- (f) limit the number of variable portions in content template of messages to two variables only provided that, for the reasons to be recorded, a third variable may be allowed in case of exigency; and
- (g) ensure that variables in the content templates are non-contiguous and not separated with space, comma and/or any other special characters.

Jait Singh

18. All the Telecom Service Providers are directed to comply with the above directions and forward updated status on actions taken, including updating of CoPs, within thirty days from date of issue of this direction.

Jaipal Singh 16/02/2023
(Jaipal Singh Tomar)
Advisor (QoS)

To
All Access Providers (including BSNL and MTNL)