Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Social Media Crime Investigation

Divya Joshi[1], Hepi Suthar[2]
Students at Gujarat Forensic Sciences University Gandhinagar, India

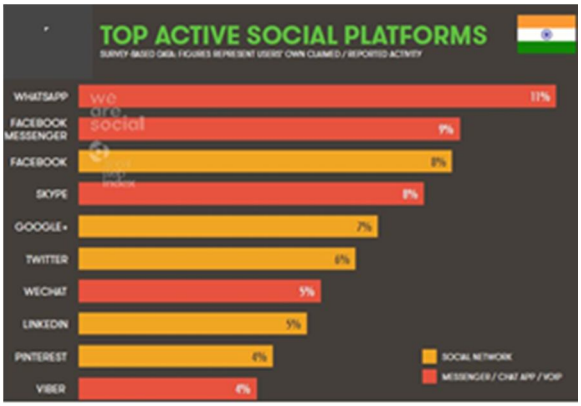
Abstract-Social networking on social media websites involves the use of the internet to connect users with their friends, family, and acquaintances. Social media websites are not necessarily about meeting new people online, although this does happen. This online social network is useful for spreading information, pictures and videos and generally staying in touch with people you wouldn't normally get to interact with all the time. Social Network is now available an application which is used in Smartphone so people now easily connected and share information, pictures, videos etc. using whatsApp, hike, Facebook, hangout, etc.In this paper, create an invisible ip logger which is sending a message using the different social networking apps and get the IP address of the receiver device.
Key words: Social Networking crimes, user's safety, IP Address, Geo Location,

I. INTRODUCTION

A social networking service is an internet based service, platform, or a site that focuses on facilitating the building of social networks or social relationships among people who, share interests, activities, backgrounds, or real-life relations. social network service consists of a representative of each user (often a profile), his/her social links, and a variety of additional services. Social media is an internet-based form of communication. Social media platforms allow users to have conversations, share information and create web content. There are many forms of social media, including blogs, micro-blogs, wikis, social networking sites, photo-sharing sites, instant messaging, video-sharing sites, podcasts, widgets, virtual worlds, and more.

Most social network services are web-based and provide a way for users to interrelate over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, the social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, activities, events, and interests.

In the realm of computer security, the term social engineering is used to describe the malicious intent of people who are trying to gain access to sensitive data and information through illegal means. The process of obtaining information through social engineering techniques implies a lack of technical skills but places a strong emphasis on social skills. However, a skilled social engineer can spend a lot of time gathering publicly available information about the targeted data and talking to eventual victims before directly requesting access to the desired information.



[Social Network usage statistics]

II. RELATED WORK

Now most of the social networking websites like Facebook, WhatsAppweb, Gmail, twitter, etc run on HTTPS protocol, which means the secure connection, but now hackers are more powerful and security is less. Hackers also easily break the HTTPS connection and sniff the chat or other information about the victim using sending any attractive messages or attachments which are

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

malicious.

In this paper, made a scenario in which create an attractive email, message, and pdf which is bound with the IP logger and sent to the social network user and when a user clicked on that link got the IP address of the user's devices and using IP address got the geo-location of that user.

III. METHODOLOGY

Nowadays terrorist targeting the people using the social networking applications or websites. When any attractive messages like online shopping discount scheme, Internet data plans scheme, free movie tickets coupons, etc. sent to the people in social networking apps and websites like Whatsapp,Facebook,hike,hangout,etc. they were easily attracted towards that schemes and hackers got the benefit of that. The Cyber terrorist group made an attractive e-mail, attractive pdf, and attractive message and all this are bounded with IP logger in this one link is provided when people clicked on that link the terrorist got the IP address of the people's digital devices and using this IP address they easily find the geo-location of that people. Many websites are available on the internet which gives the geolocation from the IP address. So terrorist using these websites easily find the geo-location as well as operating system and browser information also.

Hackers sends the malware through the email also. A new malware campaign is aiming specifically at businesses and consumers using the email mobile service. The campaign uses emails masquerading as WhatsApp content. These have an attached zip file containing a malware executable.

The emails have a variety of subject lines including, "You have obtained a voice notification," and "An audio memo was missed," each followed by a short string of random characters which are probably used to identify the recipient.

If the zip file in the email is opened and executed, the malware is installed on the PC. It's a variant of the 'Nivdort' family. When run it replicates itself into different system folders, as well as adding itself into an auto-run in the computer's registry.

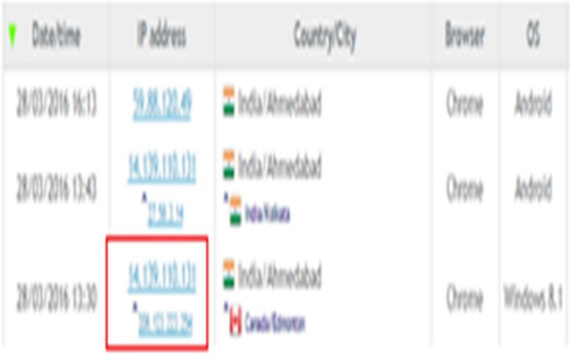
The Terrorist group creates online shopping offers attractive e-mail and sent it to the victim. In this e-mail power bank shoppingdiscount image and one link is provided for more know more about the power bank details as shown in a figure.

[Fig. 1: Attractive e-mail image]

In this image, IP logger is bounded with the link. When a user clicked on the open now links the power bank details is opened but terrorist got the IP address of the victim's device.

Many websites provides the service to bound the IP logger with an image and when that image is sent to the victim and victim clicked on that link and short the URL using the URL shorter this website gives the IP address, location, operating system and browser information about the victim. If the user uses the proxy server then also it gave the IP address of that proxy server.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



[Fig.2: Details about user's device IP address]

Hackers may send the malicious URL using the attachments like PDF, word documents, txt files, etc. now pdf documents not only sent with the e-mail attachment but also sent using the social applications like WhatsApp, Facebook, etc. so, hackers create one attractive PDF about the internet usage plans and sent to the victim. In this PDF malicious link was also added when the user clicked on the more details about the internet plan user was redirected to details of internet plan but hacker also got the ip address, geolocation and browsing information.

BROADBAND PLANS

Click on the link for more details http://goo.gl/worGBN

S.N.	Particulars	New Student CUG - 148 Prepaid Plan
1	SIM Card Charges	NIL
2	Plan Voucher (Monthly Recharge)	Rs. 148
	(i) Monthly free calls (On Net or Off Net/Both) worth Rs.	Rs. 21/-
	(ii) Monthly free Data Usage in Home LSA	1GB
	(iii) Free Number of SMS (Local/National) / Month	50 Nos.
	(iv) Validity	30 Days
3.	Call Charges	
	(i) Pulse rate for Local & STD and National Roaming Call	60 Sec.
	(ii) Within CUG	Free
	(iii) Local Calls (On Net)	Rs. 0.30 /Min
	(iv) Local Call (Off Net)	Rs. 0.50/Min
	(v) STD Calls (on Net & Off Net)	Rs. 0.50/Min.
	(vi) ISD Calls	Not Allowed
	(vii) Outgoing Call Charges while Roaming	Rs. 0.50/Min
4.	Data Usage Charges after free usage	2 Paisa /10 kb
5.	SMS Charges in Rs./SMS (max. 160 character)	
	(i) Local	Rs. 0.1/SMS
	(ii) National	Rs.0.2/SMS
	(iii) International	Rs. 5.00/SMS
6.	While on Roaming Incoming/Outgoing SMS	
	(i) Incoming SMS from any network	Free
	(ii) Outgoing SMS to any other Network	Rs.0.25/SMS
7.	Local CUG/VPN Charge	NIL
8.	Group Size	Open

[Fig. 3: Attractive PDF]

WhatsApp Web is a service that allows people to access the messaging service via a browser on a smartphone or computer, rather than the app. Hackers were sending so called vCard's to random phone numbers they had obtained, according to Check Point, a security firm that originally found the vulnerability. A vCard is an electronic contact card that you can send to another person. For example, if somebody wanted the number of someone in your phone's contact book, you could send the vCard over and the other person would have all the details. The vCard sent by the hackers contained a malicious code that would distribute bots, ransomware and remote access tools (RATs) on a person's phone or PC.

In this scenario Hackers create an attractive message and sent malicious link also in the social networking apps or websites like facebook, Whatsapp, hike, hangout, etc. when user click on that message link hacker got the IP address of the user's device. In

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

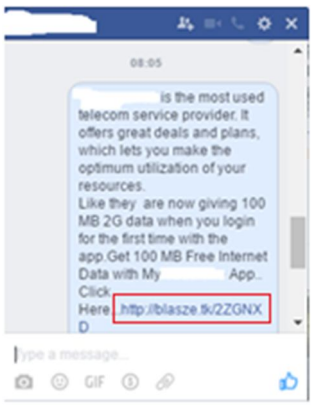
figure showed that in Whatsapp sent an attractive message with a malicious link.

[Fig.4 Attractive Message]

This attractive message sent to many users and we got the details about the user which operating system user's was used like android, mac, windows, etc as shown in the figure. In this also got the proxy server IP address also.

[Fig.5: Message IP Details]

On Facebook and other social media websites, clickjacking has been engaged in a variety of ways. For example, "likejacking", a variation of the clickjack, is a malicious technique that tricks users into unintentionally "liking" a page. Clickjacking on Facebook has also been used to infect users' computers with malicious code. Once you click a malicious link, you unwittingly download malware to your computer. Same as in this Paper As shown in below figure message sent on facebook and when user clicks on the link got the information of the user's device.



[Fig. 6: Facebook message]

The IP address which got when a user clicked on the link this IP address tracked using the IP address tracker online website and got the exact location of the user as shown in the figure.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

[Fig. 7: IP Address Geo Location Information]

IV. CONCLUSION

Social Networking websites is useful for communication as well as for information sharing also but hacker or cyber terrorist misuse this social networking websites and applications because people are not aware of hacker's malicious activities and attracted towards the discount coupons, schemes,etc and hacker got benefit of this and targeted the victim and got the details about the victim's device as well as victim's geolocation information. So, when the user using the social websites or applications never attract towards the attractive discount coupons, schemes links and don't click on that type of any link because user doesn't aware about the background process through which hackers or attacker got the information.

V. ACKNOWLEDGEMENT

This work was supported by Gujarat Forensic Sciences University, Faculty of Institute of Forensic Science that provided technical condition and machines use for the development and testing. Also guided by eSFlabs network expert.

REFERENCES

[1] M. Neela Malar Dept of Media Sciences, Anna University, Chennai “Impact of Cyber Crimes on Social Networking Pattern of Girls”- 2012
[2] [2] https://accan.org.au/consumer-info/tip-sheets/introduction-to-social-networking
[3] http://www.iptrackeronline.com/