Social Media & Social Networking: A Security Threat

Divya Dwivedi
Senior Research Fellow
Department of Defence & Strategic Studies
University of Allahabad, Allahabad, India

Abstract: In the most recent decade, with no uncertainty, web-based social networking i.e. informal organization stages that are basically made so as to collaborate with each other, for example, Facebook, Twitter, LinkedIn, Google +, Tumblr, Instagram, Flickr, Myspace, Blogs, YouTube, or any user generated content sites increased tremendous access in everyday life including people and associations. These informal organization stages, particularly Facebook, Twitter, YouTube, were developed in such quick pace way that even the big companies including Microsoft, Google, and so forth has changed their procedures, and adjusted social network platforms exceptionally well. That was the time when individuals, and little associations who did not have stage for client created content, needed to pay expense to transfer their substance over Internet. The vast majority of little organizations were utilizing privately bought platform to disseminate and share their substance; though, people were restricted to post their substance; Emails and IMs were utilized as often as possible to share their content, pictures, recordings, and so on.

By the year 2004, openly/free social network platforms turned out to be so normal/simple to utilize and were enormously effective. Platforms could give clients to share content effortlessly. Independent companies began utilizing social networks to advance their business. Veterans were effortlessly associated with their clients and followers to give assistance and data they are searching for. Upon such fast development of these online social media platforms; benefits, rewards and openings are uncountable, be that as it may, it likewise accompanied dangers and security issues.

Keywords: Cyber warfare, Cyber terrorism, Security, Social media, social networks, security risks, threats, Cyber Security, Hacking.

I.INTRODUCTION

Social Networks are an intrinsic piece of the present Web and used by in excess of a billion people around the world. They enable individuals to impart thoughts and associate to other individuals, from old friends to strangers. This communication uncovers a ton of data, frequently including ipersonal data noticeable to any individual who needs to see it. Thus security is frequently a key worry by the users. Since a huge number of people are willing to interact with others, it is additionally another assault ground for malware creators. They are spreading noxious code and sending spam messages by exploiting the users inborn trust in their relationship network. This paper will show and talk about the most pervasive issues and dangers focusing on various social networks today.[1]

Online networking and its impact have huge effect on worldwide populace incorporating individual and associations in a decade ago. As per Ashford, a greater amount of individual and organizations are exploiting web-based social networking to reach the majority and connect globally. With such points of interest, there are additionally expanding security challenges and threats to the users of online networking and social media. A large portion of these dangers connected with social networking are privacy concerns and spreading of false data. Aside from individual's personal life privacy, business security concern makes the association more helpless; as employees can unveil the organisation's private data via web-based networking media. In support of this claim, Cisco 2013 Yearly Security Report proposes that the highest concentration of online security dangers is on mass audience sites, including web-based social networking. The report additionally uncovered that online promotions are 182 times more inclined to convey noxious substance than pornography sites. (Ashford, 2013)

Sharing information with an audience and connecting globally is at the heart of the particular challenge that social media presents to businesses, because this way they give away the power to disseminate commercially sensitive information. The other drawback of social media is that it gives similar power to spread false information, which can be just as damaging. This claim is further supported by World Economic Forum in its Global Risks 2013 report, according to the report, the rapid spread of false information through social media is among the emerging risks.[2]

II.CURRENT SCENARIO

The level of human connectivity has reached extraordinary levels with over1 billion people using one or more online social networks including Facebook, Twitter, YouTube, Instagram, LinkedIn, Flickr, Myspace, Tumblr, WhatsApp, Viber, Hike and Google+.

The enormous amount of data provided and shared on these social networks may include the following data about a user: personal details, current address, hometown, email addresses, messenger usernames, activities, interests, favourite sports, groups, favorite athletes, favorite music, television shows, games, languages, his religious views, political views, inspirations, favorite quotations, service users history, education history, relationship status, family members, and software applications. The users likewise give update as status information or Tweets, which could include: an idea, a demonstration, a link they need to contribute a video. This data admits a considerable information about the user, which will hold interest to many different groups.

Social Networks, because of numerous such horrible episodes, have been blamed for breaching the privacy of their users, most recent example is the Facebook data breach that came in limelight in second week of March'2018. Both in the scholarly community and in the media, the significance of users' confidentiality has been seldom talked about. Notwithstanding some proposed technical solutions, there have been an enormous number of initiatives to teach users with the goal that they don't give an unreasonable amount of personal information.

Besides, social network information is currently being connected with user physical locations, permitting data about users' inclinations and social relationships to communicate progressively with their physical condition. This combination of online social networks with real world mobile computing has made a fast-developing group of applications that have one of a kind prerequisites and special ramifications that are not yet completely comprehended. LAMSN frameworks, for example, WhozThat [3] and Serendipity[4] give the foundation to use social networking context within a local physical proximity using mobile smart phones. Be that as it may, such frameworks pay little regard to the security and privacy concerns related with uncovering one's personal social networking preferences and friendship information to the ubiquitous computing environment.

Recently the news broke about Facebook data breach by Cambridge Analytica (CA), a data analytics firm that worked with Donald Trump's election campaign, had extracted Facebook data from 50 million user accounts. This news brought world to a wakeup call, as there are billions of Facebook users around the world and this news was an alarm to the human security experts as well as to International Security scenario too.[5]

III. COMMON SOCIAL NETWORKING THREATS

1.) Social networking worms: Social networking worms include Koobface, which has become, according to researchers, "the largest Web 2.0 botnet." While a multi-faceted threat like Koobface challenges the definition of "worm," it is specifically designed to propagate across social networks (e.g., Facebook, mySpace, Twitter, hi5, Friendster and Bebo), enlist more machines into its botnet, and hijack more accounts to send more spam to enlist more machines. All the while making money with the usual botnet business, including scareware and Russian dating services.

2.) Phishing bait: Remember FBAction? The e-mail that lured you to sign into Facebook, hoping you don't pick up on the fbaction.net URL in the browser? Many Facebook users had their accounts compromised, and although it was only a "tiny fraction of a percent," when you realize Facebook has over 350 million users, it's still a significant number. To its credit, Facebook acted quickly, working to blacklist that domain, but lots of copycat efforts ensued (e.g., fbstarter.com). Facebook has since gotten rather adept at Whack-A-Mole.[6]

3.) Trojans: Social networks have become a great vector for trojans -- "click here" and you get:

* Zeus -- a potent and popular banking Trojan that has been given new life by social networks. There have been several recent high-profile thefts blamed on Zeus, notably the Duanesburg Central School district in New York State late in 2009.

* URL Zone -- is a similar banking Trojan, but even smarter, it can calculate the value of the victim's accounts to help decide the priority for the thief.

4.) Data leaks: Social networks are all about sharing. Unfortunately, many users share a bit too much about the organization -- projects, products, financials, organizational changes, scandals, or other sensitive information. Even spouses sometimes over-share how much

their significant other is working late on top-secret project, and a few too many of the details associated with said project. The resulting issues include the embarrassing, the damaging and the legal.

5.) Shortened links: People use URL shortening services (e.g., bit.ly and tinyurl) to fit long URLs into tight spaces. They also do a nice job of obfuscating the link so it isn't immediately apparent to victims that they're clicking on a malware install, not a CNN video. These shortened links are easy to use and ubiquitous. Many of the Twitter clients will automatically shorten any link. And folks are used to seeing them.

6.) Botnets: Late last year, security researchers uncovered Twitter accounts being used as a command and control channel for a few botnets. The standard command and control channel is IRC, but some have used other applications -- P2P file sharing in the case of Storm -- and now, cleverly, Twitter. Twitter is shutting these accounts down, but given the ease of access of infected machines to Twitter, this will continue. So Twitter will become expert at Whack-A-Mole too…

7.) Advanced persistent threats: One of the key elements of advanced persistent threats (APT) is the gathering of intelligence of persons of interest (e.g., executives, officers, high-net-worth individuals), for which social networks can be a treasure trove of data. Perpetrators of APTs use this information to further their threats -- placing more intelligence gathering (e.g., malware, trojans), and then gaining access to sensitive systems. So while not directly related to APTs, social networks are a data source. Less exotic, but no less important to individuals is the fact that information on your whereabouts and activities can give more run-of-the-mill criminals an opportunity.

8.) Cross-Site Request Forgery (CSRF): While it isn't a specific kind of threat -- more like a technique used to spread a sophisticated social networking worm, CSRF attacks exploit the trust a social networking application has in a logged-in user's browser. So as long as the social network application isn't checking the referrer header, it's easy for an attack to "share" an image in a user's event stream that other users might click on to catch/spread the attack.[7]

9.) Impersonation: The social network accounts of several prominent individuals with thousands of followers have been hacked (most recently, a handful of British politicians). Furthermore, several impersonators have gathered hundreds and thousands of followers on Twitter -- and then embarrassed the folks they impersonate (e.g., CNN, Jonathan Ive, Steve Wozniak, and the Dalai Lama), or worse. Twitter will now shut down impersonators attempting to smear their victims, but at Twitter's discretion. Admittedly, most of the impersonators aren't distributing malware, but some of the hacked accounts certainly have (e.g. Guy Kawasaki).

10.) Trust: The common thread across almost all of these threats are the tremendous amount of trust users have in these social applications. Like e-mail, when it hit the mainstream, or instant messaging when it became ubiquitous, people trust links, pictures, videos and executables when they come from "friends," until they get burned a few times. Social applications haven't burned enough people yet. The difference with social networks is that the entire purpose of them is to share -- a lot -- which will result in a steeper learning curve for users. Translation -- you'll have to get burned a few more times.[8]

IV. SECURITY THREATS

National Security is of prime significance for any country to keep up peace and amicability. Nations confront various internal security challenges and threats and Online networking and social media go about as the stage for that. Social media and social networking isn't security risk in itself yet the users of these services can represent the threats by their anti-social efforts.

With constrained government oversight, industry models or motivations to educate users on security, privacy and identity protection, users are open to identity theft and fraud. Also, these platforms have enormous confidential user data, and are likely vulnerable to outside or inside attacks which is impeding to Internal Security. [9]

Different Internal Security threats due to Social Media are:

1.) Cyber Terrorism: The biggest challenge for internal security of nation through social networking site is cyber terrorism. Today terrorists select Social Media as a practical alternative to disturb the function of nations and other business activities because this technique has potential to cause huge damage. It poses enormous threat in international system and attracts the mass media, the security community, and the information technology corporation.
At the same time, due to the convenience, affordability and broad reach of social media platforms like YouTube, Facebook and Twitter, terrorist groups have increasingly used social media to further their goals and spread their message.

Social Media became a platform for coordination of plans of attack, communication with cells, or propaganda and information and spread of hate campaign or messages that can hurt the sentiments of people.
These groups now have their own websites where they can convey their propaganda and, for most of them, they advise their readers and followers not to trust the media which are seen as the enemy.
The chat service like Skype, which includes voice and video capabilities, has become particularly popular with terrorist cells. Chat rooms and electronic forums enable the insurgent and extremists groups to communicate with members and supporters all over the world, to recruit new followers and to share information at little risk of identification by authorities.[10]
Youths are especially targeted for propaganda, incitement and recruitment purposes by terrorist groups.

2.) Fraud: Social networking sites also invite fraudsters to take excellent opportunity to become wealthy by applying deceiver schemes.

3.) Criminal Activity and Money laundering: Internet Media is a major resource for developing serious crime. As Internet is growing explosively, online criminals try to present fraudulent plans in many ways. Social networking sites also pose major challenge in financial and organized crime which destabilizes the system. It creates threat to a company's security because of what employees might disclose and they are on prime target for cyber criminals.

4.) International users: The other national and international users such as the political parties, NGO's, hackers pose a serious threat using the social media. For example, during the civil turmoil in the Arab Spring Uprising, the various governments were threatened through the social media.

5.) To Bring Revolution: Some countries in the world feel threatened by the fact that social media can bring the people together and thus, create a revolution. This in turn can cause political instability.

6.) Communal Violence and Fanning Tensions: Importantly, social media also seems to be playing a significant role in polarising different communities in India and compounding India's Security challenges. The viral videos and false updates of communal clashes, riots and terrorists attack have created a massive impact in the life of public.
The power of media and the process of public opinion formation in a free society had undergone radical change due to Internet and faster means of communications like SMS, whats app, viber and simplified mobile internet. The chain of events beginning with the clashes in our North-east and which caused very serious and mass exodus of North-east population from several Indian cities has revealed the fragility of our national Cohesion.

7.) Virtual Community: Popular social networking websites are another means of attracting potential members and followers. These types of virtual communities are growing increasingly popular all over the world, especially among younger demographics. This can build Anti-National Sentiments among Society.

8.) Hacking: Hackers write or use ready-made computer programs to attack the target computer. By using Social Media hackers breach the national security and steal important data of defence or other strategic sectors. This can kneel the whole country without using Arms and Ammunition.
Although social media has the potential to be a threat to national security, it also has the opportunity to strengthen National Security and to be used to benefit the Government. [11]
One of the fastest growing ways that Governments are using social media is as a warning or trend prevention tool. As a monitoring tool, the government is able to recognize the first signs of any hostile or potentially dangerous activity by collecting and analyzing messages in order to try to predict events that could be a danger to National Security.
Another important use of social media by the government is as an institutional Communication Tool. Social Media provides a medium that creates cohesion between federal agencies by increasing both communication and transparency.

VI. CONCLUSION

Online social networks offer exciting new opportunities for interaction and communication, but also raise new privacy concerns. If online social networks are not carefully used then instead of bringing the blessings to the users, it will be appeared as a dangerously powerful tool for spammers, unscrupulous marketers, cyber criminals and cyber terrorists who may do the serious harms to the users

and being a biggest threat to Human security as a whole. Social networking sites have become a potential target for attackers due to the availability of sensitive information, as well as its large user base. Therefore, privacy and security issues in online social networks are increasing.

In a globalised society, social media becomes a lethal weapon against the enemy, and the populace as well. Information, as an element of soft power, is a strategic instrument within the context of grand strategy. There should be judicious use of social media. But we will have to mull steps to check its misuse for creating Internal security threat to Nation. Social Media, with all its benefits and the potential for more, is definitely a boon to our world, however misuse or irresponsible usage can have negative effects on Internal security. We need to guard against the negative impact of the social media, which ought to be used in the correct manner for creative or productive purposes so that it is progressive to mankind and society at large, rather than regressive.

From leaking debit card details to influencing the US Presidential Election, cyber-attacks have become a significant part of our political and social discourse. Cyber threats via social networking sites exists 24/7 and manifests along the full spectrum starting from cybercrime to cyber espionage to cyber terrorism and cyber war.

Cyber-crimes are a real threat today and are increasing very rapidly both in intensity and complexity with the spread of internet and smart phones. About eighty percent of cyber-attacks are related to cybercrimes and the information is collected through social media and social networking sites. More importantly, cyber-crimes have changed the nature of conflict by blurring the line between state and non-state actors. Dark net and Deep web are already being exploited for sale of vulnerabilities, weapons, recruitment of people in terrorist groups, drugs and so on. Other sectors high on the priority list of cyber criminals are banking, energy, telecom and defence, which along with the government, account for three-fourths of all cyber-attacks. The emergence of new services and apps, cloud and cognitive technologies, has made cyber security more challenging even as the value of data and its applications in commerce grows by the day, making cyber security a major task.

REFERENCES:

1. Candid Wuest, ‘Risks of Social networking’, Symantec, Security Response, Cupertino, USA.

2. Warwick Ashford: Social media: A security challenge and opportunity. Retrieved November 5, 2013 from http://www.computerweekly.com/feature/Social-media-a-securitychallenge-and-opportunity (Internet article), February 2013.

3. A. Beach, M. Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan, B. Surendar, M. Terada, and R. Han, “Whozthat? evolving an ecosystem for context-aware mobile social networks,” IEEE Network, vol. 22, no. 4, pp. 50–55, July-August 2008.

4. N. Eagle and A. Pentland, “Social serendipity: Mobilizing social software,” IEEE Pervasive Computing, vol. 4, no. 2, April-June 2005.

5. Aja Romano, ‘The Facebook data breach wasn’t a hack. It was a wake-up call’, Vox Blog (Internet Article) 20 Mrach 2018.

6. J. N. J. M. M. F. Jagatic, T. Social phishing. In Communications of the ACM Forthcoming (2006), 2006. www.indiana.edu/\~phishing/ social-network-experiment/ phishing-preprint.pdf

7. G. Hogben. Security Issues and Recommendations for Online Social Networks. Position paper, ENISA, European Network and Information Security Agency, October 2007. http://www.enisa.europa. eu/doc/pdf/deliverables/enisa_pp_ social_networks.pdf.

8.Staying safe in the Cyber world, Mass.gov blog, 24 Oct 2013, http://blog.mass.gov/blog/safety/staying-safe-in-the-cyber-world/

9. Ibid.

10. Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, ‘On Cyber Warfare’, A Chatham House Report, November 2010.

11. Mahmood, S., Desmedt, Y.: Online social networks, a criminal's multipurpose toolbox (poster abstract). In: Balzarotti, D., Stolfo, S.J., Cova, M. (eds.) Research in Attacks, Intrusions, and Defenses, vol. 7462 of Lecture Notes in Computer Science, pp. 374–375. Springer, New York.