International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Analysis of Social Media Attacks and Classify Advances to Preserve

Hardik Gohel[1], Dr. Alpana Upadhyay[2], Dr. Priyanka Sharma[3]

[1] Assistant Professor, Computer Engineering, AITS, Gujarat, India
[2] Associate Professor, MCA, Sunshine College, Gujarat, India
[3] Professor, IT, RSU, Gujarat, India

Abstract - ***The growth of Internet is increasing day by day and users of internet are also increasing regularly. The tremendous growth of internet also leads to increment in cyber attacks. Security threats and attacks are violating cyber rules and regulations. It also affects data and information available on internet and steals personal information of users who are locating their secret information online. The major problem is there when threats and attacks are affecting to financial transaction performed by user online and secret information available online on social media. The standard rules and regulation for internet and cyber security are there but not enough to protect data online available on social media and it is also not useful to get defence from threats and attacks by legitimate or unlawful users of social networking sites and applications. This leads to study of threats and attacks of social media and approaches to defend it from others. This paper presents depth study of threats and attacks available on social media webs and applications and various ways to defend it. The paper discusses characteristics of threats and attacks on social media and also discusses about vulnerable sites and applications. Paper is useful to protect their data and information to them who are providing their personal and secret data as well as information online via social media. This paper is also discusses about the case study of threats and attacks available on Facebook, largest popular site of social media, and various way to defend it.***

Keywords *Threats, Attacks, Social Media, Cyber security, Cyber protection*

INTRODUCTION

The era of digital world, in which all economy, governance and business routines depends on information solution based on computer networks. Threats and attacks are also increasing to destroy an information solution available through computer networks. According to cyber terms threat is generating possible harm to security by exploiting vulnerability and attack is to get illegal access to depiction, demolish, immobilize, modify, and lift sensitive information.

International Telecommunication Union Telecommunication (ITU-T) is a United Nations agency which developed standards known as Open Systems Interconnection (OSI). The OSI protocol architecture with RFC 2828 has been defined definition of Threat and Attacks given bellow [1]:

Threat (According to OSI RFC 2828)

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack (According to OSI RFC 2828)

An assault on system security that derives from an intelligent threat. That is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Threat based attack is a kind of attack which is using different technique to penetrate user of cyber environment. The infected file which come from spam or anyway of an internet downloading also part of thread based attack. Generally, it tries to exploit various vulnerabilities to come across with system. An attacker can exploit multiple different points of entry with single attack by parallel multiple diverse attacks.

THREATS AND ATTACKS OF SOCIAL MEDIA GENERALIZATION

History of Cyber Threats & Attack

The history of cyber threats and attack is very interesting and here we have drafted only those threats

and attack which has been reported by authorities includes government and cyber military. There is very long history of cyber threats and attack but we are going to study a single decade with versatility of attacks and threats.

In 1988 the first worm has been recognised. It has been used to affect and spreading infrastructure largely at US. This worm has been used weaknesses in UNIX operating system and simulated to itself frequently. Because of this worm the performance of system becomes very slow. It also is making system unusable. That is founded and worked of Robert Tapan Morris, and he said that he was just tyring to measure the big size of an internet was. He consequently becomes the first fellow to be crooked under US computer fraud and abuse act. He is now doing work as a senior professor at MIT.

In December 2006, NASA has been strained to block mails by means of attachments sooner than transport launches out of dread they would be attacked. The business week descript that plans for the latest US space launch vehicles would be got hold of by unidentified strange intruders.

Unknown foreigner intruder has been obtained latest US space launching plan. - reported by Business week.

In April 2007, government of china has gone through one survey in which they have found spyware in the computer of classified department and corporate leaders. There are other attacks also founded during the year of 2007 in which there were very high security requirements of sensitive data.

In August 2008, Computer network of Georgia has been hacked by unknown foreign intruders. It was not having much affection but it has created very high political pressure on government of Georgia and they had to take coordination from military of Russia.

In January 2009, near about 5,000,000 computers are affected by attack on Israel's internet infrastructure attempted by hackers. This attack focuses on government websites only.

In January 2010, Iranian cyber army has been hacked into a twitter. In April 2010, a piece of malware has been designed to crossing point with siemens industrial control systems, has been discovered in Indonesia, Iran and other places of world also.

In January 2011, Canadian government has found as well as reported many cyber attacks against its agencies including defence research and development at Canada. In July 2011, DoD (Department of Defence) at US mentioned there is a defence contractor has been hacked by someone and near about 24,000 files has been stolen from Defence.

In April 2012, Kaspersky, the Russian firm, discovered "Red April" which was functioning at since 2007. The vulnerabilities of Microsoft world and excel programmes are best source to gather information. Firstly, they have targeted to Eastern Europe countries, central Asia, Western Europe and reached up to North America as a victim. The virus and worms collected all information from embassies of government, firms of research, installations of military, and providers of energy, nuclear with other critical infrastructures.

In March 2013, Korean broadcaster YTN with South Korean financial institutions, in addition, to had their networks contaminated in an occurrence said to bear a resemblance to past cyber efforts by Korea.

In June 2013, NATO has extended protection to the networks which has owned by Alliance at cyber-defence.

In April 2013, The NCIRC (NATO Computer Incident Response Capability) improves a project in which Million euro improvements of cyber NATO ramparts, is on track for completion by April ends 2013.

SOCIAL NETWORKING SECURITY THREATS

With expose of individual's personal information extreme away from any one's group of friend and so many users any social media is target for scams. Any social media is making money from the advertisement not from users of social media so user should understand that various social media are sharing their information everywhere but not limited to your friend circle. Presently, in social media technology of face reorganization supports suggestion to users to tag their friend until and unless any user make it turn off. Threats and attacks on social media sites includes scripting of cross site, click jacking, survey rip-off and identify theft.

The first scripting of cross site means why are you tagged in this video? And the button takes you to the web page which tries to cut and then paste malicious JavaScript into your browser's address bar. Scripting of

cross sites is also kind of attack which can run hidden and allow malware to get into your system.

The second is click jacking which is also known as UI redressing. This is coming into a picture when user relieves their personal information and apparently innocently clicks on web pages. This attack is uses embedded code rather script which can execute without knowledge of user. It is having some curious messages also which attract users to click on web page like "Beautiful girl is in party" and "Funny stories related to condom". When user will try to click on link it will spear it across the friend profile within user's account.

The third one is survey rip-off which tries to install from the application which is used by user. The threat owner and attackers are trying to get advantages of recently published news related topic such as the Indian Prime Minister Mr. Narendra Modi visited US, which leads you to fake site of video and trying to get a survey. It is another way for money making from users.

In various social networking sites the Facebook is the largest risky site and according to the survey form users 81% Facebook is risky and out of them 60% says that it is a riskiest site where Twitter and MySpace received 8% for risk point of view and LinkedIn with 3%.[2]

TOPMOST SOCIAL MEDIA THREATS

According to general information available on internet 82% of employees any organization are using Facebook, 62% and 46% are using blogs and micro blogs subsequently, 69% are using GTalk and 61% are using messenger of yahoo.

Here, paper discusses methods of attacks and topmost key social media threats: [3]

Social Engineering Threat

Presently, social engineering is very famous threat for cyber criminals. It allows attacker to find out personal information of any individuals. Attackers are making this happen by using information available online or from company database, by using fake account and create trust over the time. After getting trust from user attacker is staring to collect personal information of individual by asking him/her. Information includes name of project people are doing, name of server on which they are working and go through website which drop a backdoor to their computer.

Embattled Phishing

Especially for stealing money or confidential information this attacks are carried out. The case of Hydraq attacks, in initial of 2010, compromised multinational companies' essential information. Using system vulnerability, attackers develop fright and unease instead of, to get users to part with their money and this is very specific and targeted attack and its chances are more to get success.

Bogus Accounts

The most grave social media threats gets emphasized when fake or bogus account has successful connection with so many people of various institutes, corporate and specially military, government and security firms. The best example of this when In July 2010, Robin Sage – a faked profile pressed request to people randomly and people were accepting without knowing.

Exploitation of Celebrity Names

Today, this is most popular. This is the best way to spread rumours and misinformation as well as to attack followers which can spam. There have been various occurrences when hacker is creating account by using name of celebrity. For example, Fan club of Angelina Jolie. Attacker is extracting individual's personal information to misuse it. There is no real authentication or identity check to protect against such kind of threats.

Conciliation of Websites

Compromises with any social networking site with some malicious code in which any site visitor has been attacked by attacker. Attacker or hacker have to find the way to insert such kind of malicious code into popup or advertisements by through attacker can enter in users computer to get their personal information.

Dissemination spam and Malware

Most popular social networking sites include Facebook and Twitter is most popular to spread malware. The shortened URLs have risen to various threats of social media. By masking their links, cyber criminals with short URL, making tricky for user to identify difference between legitimate or malicious site. Various social networking sites used to spread news and links within short period of time for which these kinds of threats are possible.

Reveal of confidential information

This is the very scariest drawback of social media in which individual is publishing their confidential information which is uncritical or technical. For example, status like I am fades up by configuring this server. After sometimes user status updates with technology which was helpful to get success in server configuration. This kind of status message helps attacker to find out the way to identify confidential information of any organization.

CONCLUSION

Threats and attacks on social media and different ways to defend it we have discussed above. Apart from above discussion we can give following conclusion points for above study. There are various types of threats and attacks available on social media and also different types of defences to protect personal and organizational information available on online.

References

1. William Stallings, "Network Security Essentials – Applications & Standards," in Book of Pearson Education Publication. Inc. 5th Edition, Upper Saddle River, NJ 07458, 2012.
2. Anonyms, "Social Networking Security Threats – Understand Facebook Security threats" on http://www.sophos.com, 2014, (Accessed on April 2015)
3. Shantanu Ghosh,"Top Seven Social Media Threats" in article on http://searchsecurity .techtarget.in, 2011, (Accessed on April 2015)
4. Valerie Ria Boquiron,"Spam, Scams and Other Social Media Threats", in article on http://www.trendmicro.com, 2014, (Accessed on April 2015)
5. Valerie Ria Boquiron,"Protect Your Social Medial Privacy", in article on http://www.trendmicro.com, 2014, (Accessed on April 2015)
6. Anonyms, "Social Networking Security Threats – Understand Facebook Security threats" on http://www.sophos.com, 2014, (Accessed on April 2015)
7. Shantanu Ghosh,"Top Seven Social Media Threats" in article on http://searchsecurity .techtarget.in, 2011, (Accessed on April 2015)
8. Valerie Ria Boquiron,"Spam, Scams and Other Social Media Threats", in article on http://www.trendmicro.com, 2014, (Accessed on Aprial 2015)
9. Hardik, Gohel. "Design of Intelligent web based Social Media for Data Personalization." International Journal of Innovative and Emerging Research in Engineering (IJIERE) 2.1 (2015): 42-45.
10. Hardik, Gohel. "Design and Development of Combined Algorithm computing Technique to enhance Web Security." International Journal of Innovative and Emerging Research in Engineering(IJIERE) 2.1 (2015): 76-79.
11. Gohel, Hardik. "Looking Back at the Evolution of the Internet." CSI Communications - Knowledge Digest for IT Community 38.6 (2014): 23-26.
12. GOHEL, HARDIK, and ALPANA UPADHYAY. "Reinforcement of Knowledge Grid Multi-Agent Model for e-Governance Inventiveness in India." Academic Journal 53.3 (2012): 232.
13. Gohel, Hardik, and Vivek Gondalia. "Executive Information Advancement of Knowledge Based Decision Support System for Organization of United Kingdom." (2013).

An academician and researcher, Hardik A Gohel is working on Intelligent Web Application Development and Social Intelligence. His research spans Artificial Intelligence and Business Intelligence. He has 35 publications in Journals and in the proceedings of national and international conferences

Dr. Alpana Upadhyay who is presently holding the post of Associate Professor and Head of MCA Faculty of Sunshine Group of Institutions-Rajkot, Gujarat, India, has 16 years of experience in academic and research.

Dr. Priyanka Sharma has worked in IT education field in teaching and research at Masters level for 16 years ,published more than 100 papers , carried out Funded research projects , reviewers and editors of various journals and conferences and guiding PhD students in GTU and other recognized universities. Her area of interest is Knowledge Based systems and Information system security

