IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. V (Sep.- Oct. 2017), PP 01-04
www.iosrjournals.org

A General Study on Cyber-Attacks on Social Networks

M. Sreenu[1], Dr V. Anantha Krishna[2], Devender Nayak.N[3]
[1]*Assistant Professor , Department of Computer Science & Engineering, S R Engineering College, Ananthasagar, Warangal, India.*
[2]*Professor Department of Computer Science & Engineering, Sri Devi Women's Engineering College, Vattinagulapally, Hyderabad, India.*
[3]*Assistant Professor Department of Computer Science & Engineering, Sri Devi Women's Engineering College, Vattinagulapally, Hyderabad, India.*

Abstract: *A cyber attack is any type of offensive man-oeuvre employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a cyber campaign, cyber-warfare or cyber-terrorism in different context. Cyber attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. User behaviour analytics and SIEM are used to prevent these attacks. Social platform attacks target websites with large user bases, such as Face book, LinkedIn, Twitter and Instagram. A majority of current attacks simply use the social platforms as a delivery mechanism, and have been modelled after the older koobface malware. Most often, social platform attacks are able to breach user's accounts by stealing their authentication credentials upon login. This paper deals with the different kind of attacks on social networks and their issues.*
Keywords: *Cyber attacks, false flag, Social networks.*

Date of Submission: 07-10-2017 Date of acceptance: 27-10-2017

I. Introduction

Social networking is the practice of expanding the number of one's business and/or social contacts by making connections through individuals, often through social media sites such as Face book, Twitter, LinkedIn and Google+.

Based on the six degrees of separation concept, social networking establishes interconnected online communities that help people make contacts that would be good for them to know, but that they would be unlikely to have met otherwise. Depending on the social media platform, members may be able to contact any other member. In other cases, members can contact anyone they have a connection to, and subsequently anyone that contact has a connection to, and so on. Some services require members to have a pre-existing connection to contact other members.

While social networking has gone on almost as long as societies themselves have existed, the unparalleled potential of the web to facilitate such connections has led to an exponential and ongoing expansion of that phenomenon. In addition to social media platforms, the capacity for social interaction and collaboration is increasingly built business applications.

There are basically two types of Social networks, those are Egocentric and Sociocentric. The egocentric focuses on the individual and studies an individual's as personal network and its affects on that individual. The Socio centric focuses on large groups of people and quantifies the relationships between people in a group in and studies patterns of interactions and how these patterns affect the group as a whole.

1.1. SOCIAL NETWORKING SERVICE:-Social networking service: A social networking service is an online platform that is used by people to build social networks or social relations with people who share similar personal or career interests, activities, backgrounds or real-life connections. The variety of stand-alone and built-in social networking services currently available in the online space introduces challenges of definition.
The common features are

1. Social networking services are Internet-based applications.
2. User-generated content (UGC) is the lifeblood of SNS organisations.
3. Users create service-specific profiles for the site or app that are designed and maintained by the SNS organization and,

4. Social networking services facilitate the development of online social networks by connecting a user's profile with those of other individuals or groups. Most social network services are web-based and provide means for users to interact over the Internet, such as by e-mail and instant messaging and online forums. Social networking sites are varied and they incorporate a range of new information and communication tools such as availability on desktop and laptops, mobile devices such as tablet computers and smart phones, digital photo/video/sharing and "web logging" diary entries online (blogging). Online community services are sometimes considered a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, digital photos and videos, posts, and inform others about online or real world activities and events with people in their network. While in-person social networking, such as gathering in a village market to talk about events has existed since the earliest developments of towns, the Web enables people to connect with others who live in different locations, ranging from across a city to across the world. Depending on the social media platform, members may be able to contact any other member. In other cases, members can contact anyone they have a connection to, and subsequently anyone that contact has a connection to, and so on. LinkedIn, a career social networking service, generally requires that a member personally know another member in real life before they contact them online. Some services require members to have a pre-existing connection to contact other members.

The main types of social networking services are those that contain category places, mean to connect with friends, and a recommendation system linked to trust. Social network services can be split into three types: socializing social network services are primarily for socializing with existing friends networking social network services are primarily for non-social interpersonal communication and social navigation social network services are primarily for helping users to find specific information or resources.

1.2.A CHALLENGE OF DEFINITION:-The variety and evolving range of stand-alone and built-in social networking services in the online space introduces a challenge of definition. Furthermore, the idea that these services are defined by their ability to bring people together provides too broad a definition. Such a broad definition would suggest that the telegraph and telephone were social networking services – not the Internet technologies scholars are intending to describe. The terminology is also unclear, with some referring to social networking services as social media.

1.3.ATTEMPTING DEFINITION:-A recent attempt at providing a clear definition reviewed the prominent literature in the area and identified four commonalities unique to current social networking services:
(1) Social networking services are interactive Web 2.0 Internet-based applications,
(2) User-generated content (UGC), such as user-submitted digital photos, text posts, "tagging", online comments, and diary-style "web logs" (blogs), is the lifeblood of the SNS organism,
(3) users create service-specific profiles for the site or app that are designed and maintained by the SNS organization, and
(4) Social networking services facilitate the development of online social networks by connecting a user's profile with those of other individuals or groups.

II. Network Security Benefit

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

2.1.PREVENTING THE CYBER-ATTACKS IN SOCIAL NEWORKS:

2.1.1. 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.

2.1.2. 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.

2.1.3. 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.
2.1.4. 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.
2.1.5. 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.
2.1.6. 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…
2.1.7. 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.
2.1.8. 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.
2.1.9.. 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).
2.1.10. Trust: The common thread across almost all of these threats is 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.

III. Conclusion

All Social networking sites are part of life today. People love using them according to their needs and stay in contact with friends, share pictures and even just to pass the time. Social media contains a vast amount of data spread all over servers wrapped under different layer of security. Companies have also discovered social media as a effective way to target their customers with information present in it. There are several groups with hundred and millions of members & there are always some black sheep with malicious intent. We have seen many malwares, worms and others attacks spread through social networks. It is human tendency to find out some unknown thing which causes the malware spread after clicking the unknown malicious link, without knowing who is behind it. Social media now acting as a new vector of attacks and causing multiple cases where the privacy of user is breach. It is done by inherent trust on messages coming from already compromised friends accounts and it is easy for attacks or high possibility to succeed. Hence, it is necessary to understand, implement and engage in more productive discussion of sharing best practices to mitigate social media security risks.

References

[1] Communication Networks: Fundamental Concepts and Key Architectures by Alberto Leon-Garcia, Indra Widjaja Published July 16th 2003 by McGraw-Hill Education (first published January 15th 2000)
[2] Computer Networks, 5e (5th Edition) by Andrews Tanenbaum,David J.Wetherall by Pearsons Edition.
[3] Computer Networking: A Top-Down Approach by Kurose James F. (Author), Ross Keith W. Pearsons Edition.
[4] Data Communications and Networking by Forouza Indian Edition.
[5] Network Processor Design: Issues and Practices: 1 (The Morgan Kaufmann Series in Computer Architecture and Design) by Mark A. Franklin, Patrick Crowley ,Haldun Hadimioglu. Prentice Hall India Learning Private Limited; 5 edition (2006)

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

M. Sreenu. "A General Study on Cyber-Attacks on Social Networks." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 5, 2017, pp. 01–04.