Survey on Cyber Attacks and Initial methods for its avoidance

S. Swapna
Sr. Asst. Professor, M. Tech,
Aurora's technological and Research Institute
vooreswapna205@gmail.com

Farhana Begum
Asst. Professor
M. Tech., Auroras technological and Research Institute

Girija Rani S
Asst Professor, M. Tech
Auroras technological and Research Institute

Abstract: A survey paper on the cyber crime which effected so many digital systems as we are very much depending upon internet for so many things in our daily life. It describes about the various cyber attacks around the world.In the early days of personal computing, malware threats like the infamous Brain virus, was distributed using floppy disk and were easily localized and handled. But after long time because of the Internet the cybercrime was massively distributed. From there we have seen methods of attacking increased drastically which became more prevalent. One of the most difficult things to counter about all of these cyber threats is that they are now truly personal. The one such example is ransomeware which will attack the victim's system and demand him to pay money called ransome. Unless until he pay's the attacker will not resume the system from his control. Recently we had heard that so many banking systems were hacked due to this cyber threat ransome, In this paper I am giving some of the examples of different kinds of cyber attacks.

Keywords: *Cyber crime, cyber attacks, Brain virus, Ransomware, Electronic voting systems, Electronic health records*

*****

I. INTRODUCTION

Cybercrime really became very personal when people started using email and the Internet. The Internet was like a big open book for the cybercriminal. These people could simply create an email, add an attachment in itwhich contains malware and send out to all, even using a person's own email address list to do it for them[1]. Some person would will open that attachment will auto-run a piece of executable code which is infected with malware. This type of attempt at mass infection via email came into its own in the late 90s with the Melissa email worm[1]. The trouble with this type of attack is that it gets old quickly.

Human beings will learn things and over the years, we learnt not to trust attachments in emails as much and we also set up effective spam filters. This meant that cybercriminals had to up their game.The result of this game has become more personalized approach to cybercrime with the use of 'social engineering' as the cybercriminal weapon of choice. Social engineering is a technique uses our own behavior against us. It uses psychological tricks to get us to perform actions that we really shouldn't, like opening attachments, clicking on links in a possibly suspicious email. This type of behavior manipulation is nothing new. Confidence tricksters have been using this since human beings came into existence.

One of the successful method used in social engineering and responsible for some of the cyber attacks is spear phishing which uses old malware tricks as the hackers uses but they will target perfectly. Spear phishers will also know the person who was attacked. They will check all the websites the victim is using and also check the line manager details. These people will create mails with correct logos , signatures such that the victim can feel that the mail is an authorized and open it easily.

II. BACKGROUND STUDY AND RELATED WORK

Ransomware:

Ransomware became very popular because of U.S. businesses and consumers approximately $209 million during the first quarter of 2016[1]. Topics aboutprivacy with the legal and very public battle between Apple and the FBI. The strike down of the Safe Harbor Act by a European High Court and its replacement with the EU-U.S. Privacy Shield framework has focused businesses to re-examine the impact of privacy going forward[1]. After usage of internet,therequirement of cyber security wasincreased by as more connections between the physical and the digital worlds. But companies and government agencies did not followed guidelines which left everyone vulnerable. Due to the innovative approaches of research scientists and the policy leadership of elected officials, we feel that together we can identify bold, new technologies and strategies to ensure the safety and security of government, industry and each other[1].

According to previous surveys ransomware different companies in the first five months of 2016 are more than all of 2015. Based on these facts we can sayransomwarein 2016 would be very high. Ransomware attackers will use different means to attack users by focusing on phishing attacks and drive-by downloads, use bespoke hacks to target potentially well-paying targets, such as hospitals which were locked data can mean the loss of life. Once they enter in, malware encrypts important files using a key known to the operator. Unless the use made frequent backups, the only choice is to lose data or pay the ransom. It has evolved from locking up one machine to steal data, wiping it from company machines, to sometimes destroying servers and networks in the process. Wiper malware, which has the destructive potential of ransomware but not the financial motive, it's easy to see how ransomware gets more and more attention.[1]

Ransomware is a Malware, in which people Ran scam is an example of how sloppy but effective low-rent hacking can be. Once the computer is infected with malicious code, files are deleted, but it demands a payment after the fact, with no hope for the victim of actual data recovery. Even though it's cheap and easy to obtain on the dark web, there's little chance for hackers to suddenly shift to widespread use of ransomware. If victims knows that the data which was hacked is already available with him as backstore or it was deleted by attacker , he will simple ignore it and refuse to pay the money.Ransomware also shows which file has been effected and but some of the maleware are very dangerous because it will do silently without out any information.It can also trace signatures, logo's, letterheads like other malicious software.

The only precaution the user can take is to secure data by using algorithms which can encrypt data in such a way that though the attacker attacks the data he can't use it. The second thing the user has to remember that backstore each and every file which is confidential and personal. The tadvice for companies is to usebackup servers, stored offline, ready to test restoration capability, which is paramount[1]. Protocols have to be more secured by implementing many security policies at each and every layer of transportation. The authorization of new user entered in the network have to be properly verified .To address the ever-changing nature of malware, companies need to have visibility into anomalies on their networks and should implement a multi-layered defense.

In February 2016, the FBI obtained a court order requiring Apple to engineer new access to iPhone data left by one of the massacre shooters . Apple refused, stating that doing so would undermine consumer privacy for the shortterm benefit of government access to communications by just two suspected criminals . The incident underscored that privacy-enhancing technologies in devices or services help bad actors hide[1]. Encryption is an important tool against hackers, because though the attacker gains the access on data he cannot read or use that data without decryption. In order to decrypt one has to use the key which is available only with the user . The key should be protected very carefully and should not disclosed easily. The fundamental thing here to remember is that the security of the key and the type of algorithm used by the user and strength ok breaking the key.By using the above considerations the user can protect the system from the attacker without demanding by hacking.

Mobile Applications:

One of the problems faced by the cyber users is because of drastic increase in the usage of mobile phones. With the emerging trends and technologies in Android systems with many mobile apps , the cyber attacker can generate a link which will attract the user with free download of mobile apps. Once the user clicks on the link, the virus behind the app is executed on the victims systems and results in abnormal working of user system or the attacker can silently use or check the information stored on the victims system. Some of games will attract the children and by playing continuously, it will hack the personal information or sometimes hack some of the properties of the mobile.

Electronic Voting Systems

In online businesses and technology firms will encrypt data while communicating. Some companies will encrypt customer web traffic to their sites by default and approximately 50 percent of web traffic is now encrypted[1]. International companies will use the encrypted communication channels at each and every point so the cyber attacker cannot hack the data travelling through the communication channel. But newelectronic voting systems have better features and records can be verified. These also provide secured voting systems. This information have not reached to all the countries and they were using the old voting machines. A watchdog group of scientists and government experts focused on election technology. Hacks of political IT systems put election safety in crosshairs Voting security is critical because a variety of attackers already have targeted election information.[1]

One of the hacker hacked the voting machine and changed the count of the party who bribed him.This was done at United Nations University Computing and society lab. Election accuracy is a huge issue. Research in Focus Election integrity matters for confidence in new leadership and future democratic participation. One the research scholar developed a software system to help combat intimidation at the polls and keep elections honest. How long were lines? Were people turned away? Were voting machines in a secure place? [1]

Electronic Health Records:

The Most of the problems were also faced by the hospitals due the electronic medical records as everything has made online and the doctor who is giving treatment to the patient have become online, because of this the person whom the patient is consulting sometimes became a tragedy. Some of the hackers are hacking the database of hospitals to get the reports of other patients and modify them as theirs and claim for insurance as everything became online.

But electronic health records (EHRs) are making it easier for various doctors to broadly access one's medical history, EHR systems also make it easier for data thieves to steal personally identifiable information data that is more difficult to correct than a stolen credit card number[1]. Healthcare data is 'the whale' for hackers Electronic medical records hold out the promise of better and cheaper healthcare, an important goal considering that the U.S. healthcare system is the world's most expensive by a large margin but fails to make the top 10 in terms of successful outcomes.[1]

The Complexity of the system invites fraud since every patient data is digitized and securing that became very complex.As the users are making data access more accessible and increasing the speed of access, creating different hacking problems. Adding to this each healthcare databases are exposed to so many people all over the world, which is giving a chance to an attacker to easily access and use for the different activities from which they can get benefits.The technology should be enhanced but it should not create harm to the society. Simply saying as there is a vast growth in usage of internet and advanced technologies the complexity to provide the security is increasing drastically. Overall the problems faced by the users are due to the increased technology which is completely depending upon network.

III. SOLUTION TO THE PROBLEM

After observing so many problems faced by the users who are connected to the network, to avoid such problems the government should provide a central location where the information can be stored securely. The government agency providing security should act as an interface to each and every node connected in the network. But the maintenance of the interface is very difficult.

The nodes connected to that interface should be authenticated perfectly as we can't justify the user connected that interface is a correct person or not. After that every time the user should be monitored for each and every interaction with other node or other user. Sometimes in spite of taking many measures the user may be a hacker.

The second problem discussed was Ransom ware which can be eradicated by making more secure channels. Each layer in the network should be secured perfectly. The easy and securable method to avoid it is to make the operating system of each and every node in the network most secured in such a way that no hacker can hack any system connected in the network.

The another solution is to design an antivirus software which can detect the threat perfectly and stop before entering the network. Though we have strong firewall for security the hacker is getting the information from the network. So there is a huge requirement to make the gateway more secure.

Nation-states are experimenting with information modification the control of data flows – and the content of that information – continues to be a major area of research and development for most nations, whether using Global information manipulation by nation-states now widespread blunt tools such as censorship or more refined and subtle modifications, such as filtering search results or social media campaigns. Social media and search-based information flows have made information manipulation and disinformation much easier. Nation-states have used this type of attack in the past. [1]

In the past, things were isolated and we had the security advantages of a natural firewall,But as we become more interconnected and the Internet becomes more pervasive, we increase the risk for hacking or ill will or malevolent attack. Security must be added to communications to prevent hacking .Devices must be able to manage themselves and verify the state of others nearby. Any system must be able to manage itself and verify the state of any sensors and device to which it is connected.

Tackling trust between autonomous cars sharing the road, within a naval fleet, or swarms of unmanned aircraft requires multiple layers of security. Machines need to prove they are trustworthy at the hardware level, at the network layer, and the application layer. "Before, machines were invited to work by themselves. "As soon as you communicate, there is a risk of manipulation[1]."

If society is moving toward driverless cars and hybrid ground-and-air vehicles, those machines need to research in Defense Advanced Research Projects Agency (DARPA) could lead to development of a new technique for wirelessly monitoring Internet of Things (IoT) devices for malicious software without affecting the operation of the ubiquitous but low-power equipment. The technique will rely on receiving and analyzing side-channel signals, electromagnetic emissions that are produced unintentionally by the electronic devices as they execute programs. These signals are produced by semiconductors, capacitors, power supplies and other components, and can currently be measured up to a half-meter away from operatingIoT devices. By comparing these unintended side-channel emissions to a database of what the devices should be doing when they are operating normally, researchers can tell if malicious software has been installed. “We will be looking at how the program is changing its behavior.If an Internet of Things device is attacked, the insertion of malware will affect the program that is running, and we can detect that remotely.”

CAMELIA: Monitoring Side-Channel Signals for IoT Trust know how to talk to each other. Encryption does not work in these scenarios, instead the solution demands multiple sensors or multiple kinds of sensors[1] .

Different ways of disclosing have different impacts in 2017, information sharing will continue to be a major issue for both companies and governments. Security researchers who find vulnerabilities typically disclose the issues in one of two ways:

Waiting for the company to fix the software flaw before releasing any information or releasing the information to force the company to quickly patch the issue. Each approach has benefits and drawbacks. Fully disclosing the vulnerability, along with exploit code, generally results in an increase in attacks up to six orders of magnitude more but also speeds the user community’s response to the vulnerability. “The lifecycle of the vulnerability is much shorter. With limited disclosure, the attacks start much later, but it extends for a longer period of time.” Both government and business see information sharing as a gamble despite an executive order and legislation, information sharing especially between the government and private sectors is weak. Numerous hurdles bar the way for most businesses to participate. While a large number of threat-intelligence services exist, the provided information frequently contains large number of false positives, making security professionals’ jobs harder.We are seeing more threat intelligence services, but the challenge is the fidelity of the information [1]

Conclusion:

We can conclude that whatever emerging technologies are coming in the society not only providing advantages but creating many disadvantages. One thing we can say that security plays an important role in each and every new inventions as well as using technologies.

REFERENCES:

[1] 2017 Emerging Cyber threats and trends & technology Report-Georgia Institute for Information security.