ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Cyber Security Attacks and Countermeasures

[1] Pratyush Kumar Deka

[1]Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1] pratyush.deka@galgotiasuniversity.edu.in

Abstract: Internet usage is increasing exponentially and apps are expanding in our everyday lives. Whether it is for household purposes or for use by governmental organizations, Internet is important regardless of what the individual is or what job he does. It is also essential to have protection in applications such as shopping, banking transactions, education, public services etc. Internet is also considered to have insecurity problem with wider use. This insecurity issue includes various cyber-attacks occurring these days, such as fraudulent banking transactions known as phishing, HTML injections, SQL Injections etc. Cyber security is a major concern because the complexity of the security threat is increasingly and constantly growing. Controlling access, encrypting a file, detecting intrusion, etc. will overcome these issues. It could be hacked to encrypt information and then its sensitive information can be removed, only making sure that it is updated before someone actually knows about it. Researchers have provided with a range of defensive systems to prevent such attacks. The techniques used by cyber-attackers for carrying out attacks are currently synonymous with manipulating humans.

Keywords: Attack Taxonomy, Cyber Security, Cyber-Attacks, Data Breach.

INTRODUCTION

Everything about shopping of daily items, education related searching for banking transactions and booking reservations is now carried on the internet. Each part of a human's daily life is now connected to the Internet and therefore the sensitive information must be secured against cyber-attacks. Any type of unethical activity conducted by individuals or entire organizations related to computer IS, computer networks, and/or personal computer devices utilizing numerous and malignant actions usually starting from an unknown source is called a cyber-attack [1]. By hacking into a device it either steals, changes or ends a goal. Cyber-security also referred to as IT security: defense of IS from theft or vandalization of the information, hardware and software contained therein, as well as from intrusion or target of the services rendered [2]. This monitors the physical access to the equipment and protects it from any harm passing through the network, data leakage, any device malpractice, unintended or unintentional, or bluffing into distracting and deviating from safe and secure procedures. With the growth of smart devices, televisions and networks the need for protection arises. And with private data networks growing, Ethernet, Wi-Fi and other wireless networks also growing [3]. Data security implies sensitive security, or any important data from unauthorized use and even access. Computer security is the security that is provided to computers and the information it carries by fraudulent access. Mechanisms and devices are combined as a solution. Cyber security is a collective responsibility and is the responsibility of everyone who uses the Internet for whatever purpose. Internet companies can help by making their networks and payment processes more effective. The State must pave the way for public awareness and education. It should also have anti-cybercrime laws enforced. On the other hand, companies will inculcate strong security procedures like employee knowledge about using unique and secure passwords. Attackers attempt to steal, harm, kill or monitor critical information from individuals, organizations, companies and even governments[4].

CYBER ATTACKS TRENDS

Root Kit:

It is a set of computer software that facilitates the acquisition of a computer or software that is not normally allowed to hide its presence and the existence of its software. The term rootkit is the integration of "root" (from Unix OS) and the word "kit" (components that implement the tool). This term has bad connotations as it relates to malware. Rootkit can be installed or enabled, or the user will have access to the root or administrator. When mounted, the invasion hides and even retains privileged access. It's difficult to detect Rootkit because it kills tools designed to find it. Nonetheless, detection methods use an alternative, robust operating system, behavior-based techniques, signature scanning, difference scanning, and memory dump analysis[5].

Botnet:

The botnet is a set of computers connected online and interacting with other similar devices to perform the same tasks. It is used to send spam emails and to take an active part in the transmission of denial of service attacks. The word robot and the network combine to form this word. But the word has a negative connotation[6].

Scareware:

It's used in social engineering. This causes tension or danger and allows users to buy unnecessary apps. It does not help consumers, but it is driven by unethical practices. Spyware and adware are using a scareware tactic. It can also be said that the virus is being introduced to create panic. You can also change the context of the user's desktop; add icons on your screen.

SQL Injection:

Here, data-driven systems are targeted by code injection.The malicious SQL statements are mounted in the entrance for execution. Often known as the website attack vector, it is capable of attacking any SQL database. It allows the identity to be spoofed, data to be changed, issues of repudiation to be generated, allows full access to, destroys or makes all data on the network inaccessible.

Phishing:

It is a constant threat to social networking. They can create an exact duplicate of the website and ask for personal information, which is then sent to them via email. This is more likely for the corporation, individual homes, and even the public to access personal and security information that affects the consumer or the business. Phishing is achieved in the presence of the user's confidence that the website being viewed is the one with legitimacy. Hacker will access every information that user enters[7].

Kido:

Often known to as Conficker, Downup and Downadup, it is a kind of code worm that points to Microsoft Windows OS. Using vulnerabilities in Windows operating system software and using dictionary attacks on the administrator's passwords, it is achieved by creating a botnet, incorporating the use of many sophisticated malware techniques and therefore difficult to combat. The worm relies on networking sites like Facebook, Yahoo Messenger, GMail, Yahoo Mail, and AOL Mail. It also applies to other networking sites, such as MySpace which Facebook, and may impact other users on the same local network.

Advanced Persistent Threat:

This is an intrusion on a network in which an individual steals a network and accesses sensitive and highly confidential information rather than doing any actual damage to the network or organization.

Code Injection:

It is unethical to use a bug (error) when processing invalid data. A compromised computer program is inserted (introduced) with a code and the execution mechanism is modified. The outcome could have been catastrophic. It could also lead to loss of data or delinquency, lack of accountability or denial of access. It can lead in a complete takeover of the host. Most of the examples are lighting errors. The need for this attack arose from the need to hack or break a system to gain entry, privilege upswing.

HTML Injection:

Hypertext Markup Language (HTML) Injection, called as virtual defacement, monitors any bugs in web applications and attacks. Attacker will add its own content and the program is unable to manage the data used by the user by defining a specific HTML parameter.
It's used for social engineering.

VARIOUS TYPES OF CYBER ATTACKS

Cyber-attack is the fastest growing challenge to the interconnected world of information technology. These are computer-based attacks that target human vulnerabilities rather than machine vulnerabilities. Webpage and email phishing is a type of cyber-attack in which victims are sent emails or fake webpages with links that trick them into disclosing sensitive information such as account numbers, passwords or other personal information to an attacker. Gathering information about targets may make phishing more plausible and allow it to connect falsely to a reputable business where victims may have an account. Victims are guided to a spoofed website operated by an intruder where sensitive information such as credit card numbers is entered. Drive-by-download is harmful software that operates by leveraging web browser bugs, plug-ins, or other elements that function inside browsers to spread malware without the knowledge of the user. The downloaded ransomware can use the actions of the victim or perform malicious actions automatically, such as stealing personal identification or password of users, joining a botnet to send spam, hosting a phishing site or starting distributed denial of service attacks. Social engineering is also a kind of attack that utilizes people's behavior to act on malicious intent: on social networking sites in particular. Furthermore, more cyber-attacks are currently associated with manipulating humans than previously recorded, and these are more difficult to detect and track. Protecting the confidentiality, honesty, and availability of information is an important global challenge for information security. Cyber-attack taxonomy and classification will help users participating in a security process not only to identify threats, but also to identify cyber threat detection, mitigation and remedy steps. Several researchers have contributed to the development of cyber-attack taxonomy and classification to help users become aware of online threats / risks. In this section, author gives a holistic view of some documented computer security cyber-attacks. This includes information about attacker styles and potential cybercrime attacks, motivations and drivers, goals and consequences[8].

COUNTER MEASURES AGAINST THREATS

Virus:

A malicious program inserted in the memory without interfering with the program of the user and its execution to damage system resources by creating, transferring and erasing files against the commands of the user is called a virus. It may be memory exhausting. It replicates and propagates via network-based software by making copies of itself. It may confuse the program's execution[9].

Worms:

Worm is a standalone virus that can replicate itself to spread to the computers in order to deceive program execution.

Trojan horse:

A Trojan horse is a malicious code that behaves as one thing but works differently. They create a hidden route for attackers to access secure and confidential information.

Hacker, attacker or intruder:

These are the person who tries to make use of flaws in structures to their own benefit. They enter other places without permission. While not always harming the location, sometimes they are only conducted as a means of satisfying curiosity; their acts are usually unethical to the structures they manipulate. From less vulnerable to more vulnerable, the results may vary.

CYBER CAPABILITIES BY COUNTRY

United States:

First move was taken by the President in 2002 for cyber warfare strategies. Among many other organizations, there are four main actors that are USCYBERCOM "to schedule, organize, integrate, synchronize and carry out activities to: direct the operations and protection of the designated Department of Defense Information Networks and; plan and, when directed, conduct full-spectrum military cyberspace operations to allow action in all domains, guarantee US / Allied freedom of action in cyberspace and deny the same to our adversaries," NSA / CSS (National Security Agency / Central Security Service) "to lead the United States; Government in cryptology containing both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and allowing Computer Network Operations (CNO) to achieve a decision advantage for the State and our allies in all circumstances[10].

China:

China has noticeable IT infrastructure and advanced cyber weapons, according to the National Computer Network Emergency Response Technical Team Coordination Center of China (CNCERT or CNCERT / CC) annual report. China is playing an active role in cyber-and cyber-attacks. Online attacks on China and Russia have increased significantly in recent years. A Chinese Ministry of Defense and People's Liberation Army (PLA) spokesperson says cyber war and cyber-attacks are as serious and important as other wars are. The announcement was made by the National Defense of the People's Republic of China on 20 July 2010 concerning the creation of an Information Protection Base within the General Staff Department.

North Korea:

North Korea has more than 5,000 hacker units, based on reports from South Korea. In 1998, a new unit was initially set up by the North Korean Military focusing exclusively on modern warfare. From that point on, the unit, called Program 121, has steadily grown in size and capability. They have done everything from more ballistic rocket launches, another nuclear test, withdrawal from the cease-fire of 1953 that ended the dangers of the Korean War (there is no peace settlement) and cyber warfare is no exception.

CONCLUSION

Everybody wishes to be safe and secure while using the internet but due to evolving cyber-attacks, times have come to make that sure of them. With online shopping and services increasing regular, the need for these countermeasures has become a mandatory necessity and is growing as the scams and attacks increase. Mobile devices are also becoming vulnerable to cyber-attacks. It's easy to access and change or quiet easy to break their open source software or claim easy to develop apps. In terms of security, pirated software and fake websites are also advertising about their apps which are not up to the mark.

REFERENCES

1. M. Sonntag, “Cyber security,” in IDIMT 2016 - Information Technology, Society and Economy Strategic Cross-Influences - 24th Interdisciplinary Information Management Talks, 2016, doi: 10.2478/hjbpa.
2. K. K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” Comput. Secur., 2011, doi: 10.1016/j.cose.2011.08.004.
3. N. Ben-Asher and C. Gonzalez, “Effects of cyber security knowledge on attack detection,” Comput. Human Behav., 2015, doi: 10.1016/j.chb.2015.01.039.
4. W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges,” Computer Networks. 2013, doi: 10.1016/j.comnet.2012.12.017.
5. S. Gupta, S. Vashisht, and D. Singh, “A CANVASS on cyber security attacks and countermeasures,” in 2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016, 2016, doi: 10.1109/ICICCS.2016.7542335.
6. L. Zhang, S. Yu, D. Wu, and P. Watters, “A survey on latest botnet attack and defense,” in Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011, 2011, doi: 10.1109/TrustCom.2011.11.
7. B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, “Fighting against phishing attacks: state of the art and future challenges,” Neural Computing and Applications. 2017, doi: 10.1007/s00521-016-2275-y.
8. A. M. Shabut, K. T. Lwin, and M. A. Hossain, “Cyber attacks, countermeasures, and protection schemes - A state of the art survey,” in SKIMA 2016 - 2016 10th International Conference on Software, Knowledge, Information Management and Applications, 2017, doi: 10.1109/SKIMA.2016.7916194.
9. S. Purkait, “Phishing counter measures and their effectiveness - Literature review,” Information Management and Computer Security. 2012, doi: 10.1108/09685221211286548.
10. K. N. Seviş and E. Seker, “Cyber warfare: Terms, issues, laws and controversies,” in 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016, 2016, doi: 10.1109/CyberSecPODS.2016.7502348.

11. V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data in Cloud" , International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
12. P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, "Investigations on Evolution of Strategies to Preserve Privacy of Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.

13. Bishwajeet Pandey, Vishal Jain, Rashmi Sharma, Mragang Yadav, D M Akbar Hussain, “Scaling of Supply Voltage in Design of Energy Saver FIR Filter on 28nm FPGA”, International Journal of Control and Automation (IJCA), having ISSN No. 2005-4297, Vol. 10, No. 12, December, 2017, page no. 77 to 88.

14. Gaurav Verma, Harsh Agarwal, Shreya Singh, Shaheem Nighat Khinam, Prateek Kumar Gupta and Vishal Jain, “ Design and Implementation of Router for NOC on

FPGA", International Journal of Future Generation Communication and Networking (IJFGCN), Vol. 9, No. 12, December 2016 page no. 263 – 272 having ISSNo. 2233-7857 .