INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 7, Issue 6 - V7I6-1281)
Available online at: https://www.ijariit.com

Famous cyber-attacks in the history of cyber security

Zaid Ahmad Rather
zaidajaz27@gmail.com
Sri Venkateswara College of Engineering and Technology

ABSTRACT

As we move forward toward technology and digitization, we have witnessed a frequent rise in Cyber Attacks resulting in various data leaks. Cyber Attackers are capable of keeping their identity hidden and staying low while gaining access to the data. To avoid all this we require to carry a full-fledged analysis of different types of cyberattacks for the purpose of educating people and making them aware of different types of cyber-attacks that exist and secure their data. In this research paper, I will analyze the most famous cyber attacks in the history of cyber-security: WannaCry Ransomware, Nasa Cyber-attack, Estonia Cyber-Attack, Sony Pictures Cyber-attack, Melissa Virus Cyber attack etc.

Keywords: Nasa Cyber Attack , Wannacry Ransomware , Melissa Virus Cyber Attack , Estonia Cyber Attack , Sony Pictures Cyber Attack

1. INTRODUCTION

The use of Technology and Cloud services has expanded largely in the past few years throughout the world. All the familiar things that a human being does every day have been made easier, faster, accurate, and safer through the use of the internet and technologies may it be Smart locks, Smart housing systems, or a simple cell phone, everything has become much easier than compared to the last decade. We can do all the time-consuming things within minutes such as shopping for clothes, Transferring money, booking airplane tickets, etc. But sadly internet and technology are just like a sword which means that it has their own pros and cons. There are people who use the internet for their own benefit, without harming others but there are also people who want to harm people by stealing their data and valuable information such as bank details, Credit card information, etc. In order to save ourselves from these harmful cyberattacks, we should be aware of these attacks and know what steps we should follow to protect our data. In this paper, we will focus on the famous cyber attacks that occurred in the history of cyber-attacks namely the NASA cyber attack, WannaCry Ransomware, Melissa Virus Cyberattack, Estonia Cyber Attack, Sony Pictures Cyber Attack, Ukraine power grid cyberattack, Sony Play-station Cyberattack, Adobe Cyber attack.

In this paper, we will discuss each of these cyber-attacks one by one starting with the WannaCry Ransomware Cyber Attack followed by all other cyberattacks and ending with Adobe cyberattack

2. WANNACRY RANSOMWARE CYBER ATTACK

The WannaCry Ransomware Cyberattack is one of the most dangerous cyber attacks in the history of cyberattacks.WannaCry Ransomware cyber attack was caused by the WannaCry Cryptoworm .It all began at 1:14 m (IST) on 12 May 2017 and within 24 hours it had already affected over 2,00,000 computers across 150 countries. The WannaCry Ransomware utilizes the vulnerabilities present in Windows Operating System(vulnerable SMB Port) which is the most commonly used Operating System nowadays, the cyber attack locked the victim out of their systems and encrypted the data from the device and then demand ransom in the form of bitcoins in exchange for data recovery. After this cyber attack Microsoft released emergency patches to halt the attack.After a certain period of time a kill switch was discovered which helped in stooping the spread of the cyptoworm. Most of the cyber security experts linked this cyber attack to a North Korean group of hackers who were also responsible for various attacks before such as the Sony Picture cyber attack in 2014, etc. There were four different variants of the WannaCry Ransomware which are :

1. WCRY
2. WCRY(+ .WCRYT for temp)
3. WNCRY (+ .WNCRYT for emp)
4. WCRY with a kill switch.

In order to protect our data from WannaCry Ransomware Cyberattacks we should make sure that our Anti-virus is up-to-date, Backing up all the data, Downloading free software from trusted websites only, and opening mails and links only from trusted people.

3. THE NASA CYBER ATTACK

The NASA Cyber Attack took place in the year 1999 which caused a three-week computer shutdown in NASA, all of the systems that were used in NASA were shut down by this Cyberattack. This attack was launched by a 15-year-old boy from Florida named Jonathan James who used the internet name "c0mrade". At first, he penetrated the US Department of Defence's computers and installed a backdoor on the servers which allowed him to intercept thousand of official government emails including usernames and passwords. The backdoor helped James steal NASA software and then crack the computers at NASA which cost NASA a loss of $41,000 as the systems were shut down for three weeks. Jonathan James was the first person to carry out a hack against NASA.
Later in 2000 James was arrested from his home in Florida and was sentenced to seven months of house arrest until he was 18. In an interview, James said that he could have easily gotten away but he didn't think he was doing anything wrong as he was just playing around. He also stated that if he was able to hack into NASA anyone else with the skills can do the same because people with skills get whatever they want. James ended his life in 2008 by committing suicide.

4. UKRAINE POWER GRID CYBER ATTACK:

The Ukraine power grid cyberattack was the first successful cyberattack on a power grid that caused a power outage in several parts of Ukraine. This cyber-attack took place on December 23rd, 2015 which caused a blackout of 1 to 6 hours affecting about 2,30,000 people in Ukraine. This attack was planned months before the real attack even began. Approximately six months before the attackers used phishing email with malware-infected Microsoft files, the hackers here used the vulnerability present in Microsoft office in order to gain access to the system at the power grid. Once the employee clicked on the malicious file a malware was installed in the system called "BlackEnergy3", this malware created a gateway for the attackers to access all the information such as usernames and passwords and, other credentials as well. Once the attacker was inside the system they reconfigured the UPS that was supposed to provide backup power if an outage took place. They also changed all the important passwords that could be used to override the attack. They also launched Denial of Service attacks to prevent calls from customers. Once all this was done they used another malware called "KillDisk" to erase all the data from the computers and crash all the systems. After the attack was successful it was said that Russian hackers were behind the attack but there wasn't any proof against them.

5. SONY PICTURES CYBER ATTACK:

Sony is one of the biggest entertainment studios in the world, which releases movies now and then. Sony pictures came into the limelight in 2014 when they decided to release a movie named "The Interview" which was a comedy storyline to assassinate the North Korean leader Kim Jong Un. Sony Pictures office in Los Angeles received a message on their computers saying "We have obtained all your internal data including your secrets and top-secrets" and were asked to obey the order otherwise the data would be leaked. This attack was done by a Korean group of hackers called"Guardians of Peace". The attackers threatened to leak the information about each employee, emails, and passwords of every employee, Scripts of unreleased movies, and more confidential data. Due to these threats, Sony Pictures canceled the release of the movie. These attackers used malware to get all the data from Sony Pictures, it is said that they used Server Message Block(SMB) worm tool to conduct the attack on Sony Pictures. They installed backdoors to listen to every crucial information and gain access to every confidential document. It is also said that the attackers stole more than 100 Tbs of data and more than fifty thousand(50,000) social security numbers from this attack . This attack is said to be one of the biggest attacks in the history of cybercrimes.

6. ESTONIA CYBER ATTACK

Estonia is a country in Northern Europe and it witnessed several cyberattacks in April 2007 for almost a week. It all started when the Estonian government decided to move a Bronze Solider Statue from the center of Tallinn(capital of Estonia) to a cemetery that was on the outskirts of the city. This decision sparked protests and riots all over Tallinn as Russian news channels spread fake news about the statue being destroyed along with the graves of Soviet soldiers. On April 27, 2007, the cyber-attacks began and various government bodies, media channels all were affected by this attack. Online services of the Estonian Bank were also affected by this attack. The attackers used botnets that send a huge amount of spam and automated online requests. The attacker also used DDOS(Distributed Denial of Service) attacks. It is believed that a group of hackers from Russia were behind this cyberattack that almost crippled an entire country but the Russian Government denies all the allegations. This attack proved that how a social issue can be used by the attackers to find the vulnerabilities in the system.Because of this cyber attack , Now Estonia is considered as one of the hotspots for Cyber Security

7. MELISA VIRUS CYBER ATTACK

In the year 1999, a macro virus took the world by surprise as it spread like a wildfire within 24 hours of being released. This mass-mailing macro virus called Mellisa Virus was released by David L Smith in March 1999. This virus targeted the outlook-based systems and the systems that used Microsoft word software and affected the system via emails. The victim would receive an email stating that it is an important email containing a word file attachment, Once the victim downloaded the attachment and opened it in Microsoft Word, the virus would disable the security measures that would let the user know about the virus. The virus was forwarded to the first 50 people that were on the contact list of the victim and this is how it spread like a wildfire within a short period. The

speed at which Mellisa Virus spread was unimaginable, in three days it had affected almost 1 lakh computers worldwide. The Mellisa virus did not steal and data or did not demand ransoms however it disrupted almost 1 million emails worldwide and in some parts, the internet speed was slowed down which caused damage of approximately 80 million dollars.

Mellisa Virus helped us understand that how easy it is to spread a virus due to the networking and connectivity we have today, it also helped us to know that the most widely used software are most vulnerable and can be used to exploit the data whenever the attacker wants.

The best way to protect your system from Mellisa Virus is to disable the macros by default.

8. ADOBE CYBER ATTACK

In the year 2013, Adobe witnessed one of the biggest data breach cyberattacks. The attackers stole the usernames and passwords of almost 30 million users and also stole 3 million credit card details, they also breached almost 150 million accounts worldwide. One of the reasons why attackers were able to steal the information so easily was the shifting of Adobe to cloud services which made adobe vulnerable. Other mistakes that led to these attacks were that Adobe used the same encryption key for a similar password which means if more than one user has the same password, obtaining the password of just one is sufficient to breach other accounts as well. The hackers also stole the source codes for Adobe Acrobat, Photoshop, and ColdFusion. The attackers used the vulnerabilities such as usage of Block cipher to get the user credentials, they also used the hints that were set by the users to steal the passwords and other confidential information from the users. In order to be safe from attacks like this, we must use different passwords for different accounts, using a combination of alphabets, numbers, and special characters to make your password stronger.

9. CONCLUSION

The purpose of this research paper is to analyze and discuss various cyberattacks that took place in the past decade. We also came across various terms such as Ransom, malware, Botnets, Server Message Block(SMB), DDOS, and macro-virus, etc. In order to avoid cyber attacks in the coming time we must learn from these past attacks and work on perfecting our cyber and network security measures.

10. REFERENCES

[1] A Study of WannaCry Ransomware Attack. Dr Supreet Kaur Sahi Asst Prof, SGTBIMIT
[2] Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US Abir Shehod Working Paper CISL# 2016-22
[3] How a cyber attack transformed Estonia from https://www.bbc.com/news/technology-24740873
[4] The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data Statement of Keith A. Rhodes Technical Director for Computers and Telecommunications Accounting and Information Management Division - GAO/T-AIMD-99-146
[5] Case Study: 2014 Sony Pictures Entertainment cyber attack Team: MORPHO-7470 Jesús Gabriel Ly Ponce Pere Garau Burguera Tahmid Quddus Adobe hack: At least 38 million accounts breached from https://www.bbc.com/news/technology-24740873

