Analysis of Statistical Data of Cyber Attacks in History

[1]Anmol Hariyani,[2]Harsh Shah,
[1,2]U.G.Student, SOE, Ajeenkya D Y Patil University, Pune, Maharastra, India

Abstract : With a major advancement in technology nowadays one can always see the rising number of different types of cyber attacks which are widely targeting almost all aspects of technology. So one needs to understand clearly about attacks to prevent the repercussions of cyber attack. To understand the attacks more clearly one needs to know about the cyber attacks that is from how it happened and how it started spreading rapidly with the advancement of technology. So this research paper provides one with detailed information about how different types of cyber attacks came into the picture, how the cyber attack took place, what were the outcomes of those cyber attacks and how it started spreading all over. All the detailed information of major attacks is mentioned in this paper and advancement in all types of attacks is being mentioned below statistically to get a clear picture of all types of attack.One can refer to this paper to understand the history of different types of cyber attacks.

***IndexTerms*- Stats, Cyber Attacks in history, Analysis, Virus, Worm, Ransomware, DOS**

I. Introduction

In these present days where technology has advanced so there exists a growth of fatal, disruptive and vicious cyberattacks.
This research is going to examine the problems that surround cyber-attacks and the acknowledgment of activities which are carried out over the internet. This research paper aims to demonstrate the statistics of evolution and growth of cyber attacks decade so that one can get an idea of various types of cyber attacks and gain knowledge about it.
Security expert researcher can refer to this data to for study of attacks took place in history. Authentic research papers were referred for the details of different types of cyber attacks for the statistical data. Cyber attacks used for this research paper are Viruses, Worms, DOS Attack and Ransomware.

II. Cyber Crime

Computer crime, cyber-crime, e-crime, hi-tech crime or electronic crime refers to criminal activity where a computer orca network is the primary source, tool, target or place of a crime.
Although the term cybercrime are more properly restricted to describing criminal activity in which mainly the computer or network is a very important part of the crime, these terms are used to include traditional crimes such as fraud, theft, blackmail, forgery and embezzlement, in which computers or networks are used to easily commit the criminal activity.
Cyber crime is also a major issue now a days in the world as many people are trying to get into the computer systems illegally. Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system) , data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference, misuse of devices, forgery (ID theft), and electronic fraud.

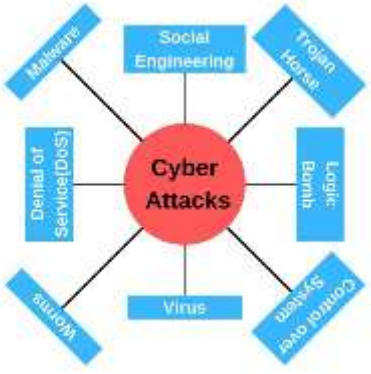

Fig. 1. Types of Cyber Attacks

DENIAL OF SERVICES ATTACK

A denial of service attack occurs when large number of requests on Internet server is flooded for web-pages, there by denying legitimate users an opportunity to access page and which results to crashing the web-server. The following is one case involving a famous series of denial of service (DoS) attacks:

2000- The Yahoo website was the target on 7 Feb 2000. The attack lasted three hours. Website was pinged at the rate of one gigabyte/second. The websites of amazon.com, buy.com cnn.com, eBay.com were under attack on Tuesday, 8 Feb 2000. According to the CNN report the attack on its website was the first major attack since its website went online in August 1995. The websites of E Trade, a stock broker and ZDNet, a computer information company, were under attack on 9 Feb 2000. It received the attention of President Clinton and the U.S. Attorney General, Janet Reno. Investigation started by the FBI about the attack. A CNN news report posted at 18:44 EST on 9 Feb 2000 quotes Ron Dick of the FBI's National Infrastructure Protection Center as saying "A 15-year-old kid could launch these attacks. It doesn't take a great deal of sophistication to do." His remark was prophetic, because, on 18 April 2000, a 15 year old pupil in Montréal Canada was arrested and charged with two counts of "mischief to data" arising from his DoS attack on CNN. Because he was a juvenile, his name cannot be publicly disclosed, so he was called by his Internet pseudonym Mafiaboy.

2007- The nation of Estonia was hit by massive DDoS attack targeted at government services as well as financial institutions and media outlets. This had a crushing effect since Estonia's government was an early adopter of online government and was practically paperless at the time; even national elections were conducted online. The attack, considered by many to be the first act of cyber warfare, came in response to a political conflict with Russia over the relocation of the 'Bronze Soldier of Tallinn', a World War II monument. The Russian government is associated with inclusion and an Estonian national from Russia was captured as the outcome, however, the Russian government has not given Estonian law authorization a chance to do any further examination in Russia. This occasion prompted the making of global laws for digital fighting.

IV. VIRUSES

2000- The "I love you" infection, otherwise called the "Love Bug" contaminates in excess of a million PCs. It sends usernames and passwords back to the individual answerable for spreading the infection. It is likewise fit for erasing arrangement of documents, for example, JPEGs, MP2, or MP3. Being exceptionally dynamic, individuals clicked into the email with paying little mind to the reality the email wasn't from anybody they knew. The malware was a worm that was downloaded by tapping on a connection called 'LOVE-LETTER-FOR-YOU.TXT.vbs'. ILOVEYOU infection overwrite framework documents and individual records and spread itself again and again. ILOVEYOU hit features far and wide and still individuals tapped on the content—possibly to test in the event that it truly was as terrible as it should be. Jabbing the hold on for a stick, to utilize a representation. ILOVEYOU was so powerful it really held the Guinness World Record as the most 'harmful' infection ever. A viral infection, apparently. Two youthful Filipino software engineers, Reonel Ramones and Onel de Guzman, were named as the culprits as there were no laws against composing malware, their case was dropped and they went with no charge.

2004- The quickest email and document sharing PC worm called MyDoom that enables programmers to get to the contaminated PCs hard drive. It holds the record for the fastest spreading mass mailer worm. MyDoom was one of the extraordinary, as it hit tech organizations like SCO, Microsoft, and Google with a Distributed Denial of Service assault. 25% of contaminated hosts of the. A form of the infection supposedly hit the SCO site with a boatload of traffic trying to crash its servers. In 2004, generally somewhere close to 16-25% of the sum total of what messages had been contaminated by MyDoom.

Cost of the malware: $38 billion.

2006- A quick spreading email spam compromising Microsoft frameworks called the Storm worm was found. In about a half year it had contaminated near 1.7 million PCs. StormWorm was an especially awful infection that made the rounds in 2006 with a title of '230 dead as tempest hitters Europe'. Interested, individuals would open the email and snap on a connect to the news story and that is the point at which the issues started. StormWorm was a Trojan horse that tainted PCs, some of the time transforming them into zombies or bots to proceed with the spread of the infection and to send a tremendous measure of spam mail. By July 2007, Storm Worm was grabbed in excess of 200 million messages. **2003**- The quickest spread worm to date called "Slammer" taints more than 75,000 PCs in only minutes. It was additionally fit for multiplying its numbers like clockwork during the primary introductory moment of contamination. Slammer is the sort of infection that makes it into films, as just a couple of moments in the wake of contaminating its first injured individual, it was multiplying itself at regular intervals. 15 minutes in and Slammer had tainted portion of the servers that basically ran the web. The Bank of America's ATM administration slammed, 911 administrations went down, and flights must be dropped as a result of online blunders. Slammer, relevantly, caused a gigantic frenzy as it had adequately figured out how to crash the web in 15 snappy minutes.

Cost of the malware: Around $1 billion.

2010- A Windows trojan called the Stuxnet was the main worm to hit the SCADA frameworks. Stuxnet is effectively the scariest infection on the rundown as it was worked by government designs in the US with the expectation of discouraging nukes from being worked in Iran. Stuxnet spread by a USB thumb drive and focused on programming controlling an office in Iran that held uranium. The infection was so powerful it made their axes fall to pieces, hampering Iran's atomic improvement and costing a ton of cash. Stuxnet is the main genuine endeavor into cyberwar and it unquestionably poses the inquiry about what will come straightaway. The possibility of advanced weaponry is truly startling.

The following figure Fig.2 shows the number of major Virus and DOS attacks from 2000 to 2010. There were no major ransomware attacks during this period.

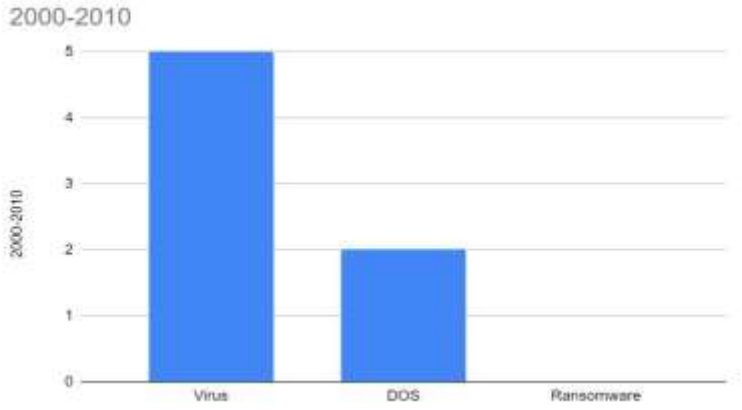

Fig. 2. Chart of Major Virus, DOS and Ransomware Attack from 2000 to 2010

V. RANSOMWARE

Ransomware is a type of malicious software that gains access to files or systems and blocks user access to those files or systems. Then, all files, or even entire devices, are held hostage using encryption until the victim pays a ransom in exchange for a decryption key. The key allows the user to access the files or systems encrypted by the program. Following are some major ransomware attack in history:

2016- Initially professing to be one of the CryptoLocker variations, this ransomware got the name TeslaCrypt and it focused on subordinate documents related with computer games like spared games, maps and downloadable substance. These documents are on the double valuable to in-your-face gamers and furthermore bound to be put away locally as opposed to in the cloud or upheld up on an outer drive. By 2016, TeslaCrypt made up 48 percent of ransomware assaults. One especially malicious part of TeslaCrypt was that it was continually enhanced. By mid 2016, it was basically difficult to reestablish records without the assistance from the malware's makers. Yet, at that point, incredibly, in May 2016 TeslaCrypt's makers declared that they were finished with their vile exercises and offering the ace unscrambling key to the world.

2015- As an ever increasing number of significant documents move to cell phones, so there become the expansion in the ransomware con artists. Android was the foundation of decision to assault, and in late 2015 and mid 2016, ransomware Android contaminations spiked practically fourfold. Many were supposed "blocker" assaults that just made it hard to get to records by keeping clients from getting at parts of the UI, yet in late 2015 an especially forceful ransomware called SimpleLocker started to spread, which was the principal Android-based assault to really scramble documents and make them unavailable without the con artists' assistance. SimpleLocker was additionally the main known ransomware that conveyed its noxious payload by means of a trojan downloader, which made it progressively hard for safety efforts to make up for lost time to. While SimpleLocker was conceived in Eastern Europe, seventy-five per cent of its unfortunate casualties are in the United States, as con artists pursue the cash. While the SimpleLocker time saw a major ascent in Android malware contaminations, the numbers, in general, are still moderately low — around 150,000 starting late 2016, which is vanishingly little level of Android clients. Furthermore, most exploited people get tainted by endeavouring to download dodgy applications and substance from outside the official Google Play store. Google is striving to guarantee clients that it's difficult to really get tainted by ransomware. Be that as it may, it's as yet hiding danger.

2017- Two significant and interweaved ransomware assaults spread quickly over the globe, closing down medical clinics in Ukraine and radio stations in California, and that was when ransomware turned into an existential danger. The first of the two significant assaults was called WannaCry, and was effectively the most noticeably awful ransomware assault ever. On May twelfth, the ransomware began grabbing hold in Europe. Only four days after the fact, Avast had recognized in excess of 250,000 location in 116 nations. In any case, WannaCry's genuine significance goes past the numbers: ReliaQuest CTO Joe Partlow brings

up that it was "the primary influx of assaults that malevolently used spilled hacking instruments from the NSA" — for this situation EternalBlue, an endeavour that exploits an imperfection in Microsoft's usage of the SMB protocol. Despite the fact that Microsoft had discharged a fix for the imperfection, numerous clients hadn't introduced it. WannaCry "aimlessly exploited," this gap, says Penn, "spreading heavily crosswise over gadgets on the system since client association isn't required for further contamination." And, Kyle Wilhoit, senior cybersecurity threat scientist at DomainTools, calls attention to that "numerous associations had the SMB port, 445, straightforwardly presented to the Internet, which engendered the worm."

2015- Attacks utilizing programming known as SamSam began showing up in late 2015, yet truly increase in the following barely any years, increasing some prominent scalps, including the Colorado Department of Transportation, the City of Atlanta, and various social insurance offices. What makes SamSam exceptional is more authoritative than specialized: it's not programming that aimlessly searches for some particular powerlessness, yet rather a ransomware-as-a-service whose controllers cautiously test pre-chosen focuses for shortcomings, with the gaps it's misused running the gambit from vulnerabilities in IIS to FTP to RDP. Once inside the framework, the aggressors obediently work to heighten benefits to guarantee that when they do begin encoding records, the assault is especially harming.

Despite the fact that the underlying conviction among security specialists was that SamSam had an Eastern European cause, the overwhelming majority of SamSam assaults focused on organizations inside the United States. In late 2018, the United States Department of Justice arraigned two Iranians that they guarantee were behind the assaults; the prosecution said that those assaults had come about in over $30 million in misfortunes. It's indistinct the amount of that figure speaks to genuine payment paid; at one point the Atlanta city authorities gave neighborhood media screen captures of payoff messages that remembered data for how to speak with the assailants, which drove them to close that correspondences entryway down, potentially keeping Atlanta from paying payment regardless of whether they needed to.

2018- Ryuk is another focused on ransomware variation that hit huge in 2018 and 2019, with its exploited people being picked explicitly as associations with little resistance for personal time; they incorporate day by day papers and a North Carolina water utility battling with the fallout of Hurricane Florence. The Los Angeles Times composed a genuinely nitty gritty record of what happened when their very own frameworks were tainted. One especially mischievous element in Ryuk is that it can impair the Windows System Restore alternative on tainted PCs, making it even more hard to recover scrambled information without paying a payment. Payoff requests were especially high, relating to the high-esteem exploited people that the assailants focused on; a Christmas season wave of assaults demonstrated that the aggressors weren't hesitant to demolish Christmas to accomplish their objectives.

Analyst believe that the Ryuk source code is to a great extent got from Hermes, which is a result of North Korea's Lazarus Group. Notwithstanding, that doesn't imply that the Ryuk assaults themselves were run from North Korea; McAfee accepts that Ryuk was based on code obtained from a Russian-talking provider, to a limited extent on the grounds that the ransomware won't execute on PCs whose language is set to Russian, Belarusian, or Ukrainian. How this Russian source obtained the code from North Korea is indistinct. **2013**- Falling simply outside our 5-year time span was CryptoLocker, which burst onto the scene in 2013 and truly opened the period of ransomware on an excellent scale. CryptoLocker spread by means of connections to spam messages, and utilized RSA open key encryption to seal up client documents, requesting money as a byproduct of the decoding keys. Jonathan Penn, Director of Strategy at Avast, takes note of that at its tallness in late 2013 and mid 2014, more than 500,000 machines were contaminated by CryptoLocker.

CryptoLocker was to some degree crude, and was eventually crushed by Operation Tovar, a white-cap crusade that cut down the botnet that controlled CryptoLocker, in the process finding the private keys CryptoLocker used to encode records. Yet, as Penn put it, CryptoLocker had "opened the conduits" to numerous different assortments of record encryption ransomware, some of which were gotten from Crypto Locker's code and some of which was given the CryptoLocker name or a nearby variation yet was composed without any preparation. The variations by and large gathered about $3 million dollars in emancipate expenses; one such them was CryptoWall, which by 2015 represented the greater part of all ransomware contaminations.

VI. Conclusion

Cyber Crimes are increasing day by day as technologies are advancing, more number of people are moving towards usage of technology for their comfortable life. So it is necessary to know what type of attacks are occuring in the cyber world and how attackers are targeting the users in the world. This research paper will give an idea about what type of major attacks were performed in history from which one can know about how it started and what was it’s cause and how dangerous it came out for the organizations. This paper also shows the statistical data of the few of attack from 2000 to 2010 in the history.

REFERENCES

[1]. Arunabha Mukhopadhyay, Samir Chatterjee, Debashis Saha, Ambuj Mahanti, Samir K. Sadhukhan "Cyber-risk decision models: To insure IT or not?" Decision support system of Elsevier May 2013, PP 11-26.

[2]. Jill Rowland, Mason Rice, Sujeet Shenoi "The anatomy of a cyber-power" international journal of critical infrastructure protection of Elsevier January 2014.

[3]. R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, S. Shenoi, "Security strategies for SCADA networks," in: Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, Mar. 19-21, 2007.

[4]. S.M.Furnel and M.J.Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?", Computers & Security, vol.18, pp.28-34,1999.

[5]. S. Karnouskos, "Stuxnet worm impact on industrial cyberphysical system security", IECON 2011 –37th Annual Conference on IEEE Industrial Electronics Society, pp. 4490- 4494, 2011

[6]."Kaspersky Lab provides its insights on Stuxnet worm". Kaspersky. Russia. 24 September 2010.

[7]. R. Shanmugavadivu, "Network Intrusion Detection System Using Fuzzy Logic", Indian Journal of Computer Science and Engineering (IJCSE), vol.2, pp. 101-111, 2011.

[8]. S. M. Bridges, and R. B.Vaughn, "Fuzzy Data Mining And Genetic Algorithms Applied to Intrusion Detection", In Proceedings of the National Information Systems Security Conference (NISSC), Baltimore, MD, 2000, pp.16-19.