Survey on Computer Worms

Darsh Shah
Department Of Information Technology
Dwarkadas J. Sanghvi College of Engineering
Mumbai, Maharashtra
Email: Shahdarsh239@gmail.com

Vaibhav Shah
Department Of Information Technology
Dwarkadas J. Sanghvi College of Engineering
Mumbai, Maharashtra
Email:vshah2212@gmail.com

Harsh Shah
Department Of Information Technology
Dwarkadas J. Sanghvi College of Engineering, Mumbai, Maharashtra
Email:shahharsh0796@gmail.com

Professor Pratik Kanani
Department Of Information Technology
Dwarkadas J. Sanghvi College of Engineering
Mumbai, Maharashtra
Email: pratikkanani123@gmail.com

Abstract—Cyber Security is an important aspect in the field of information technology. Either it is often neglected or given a lesser priority .One of the biggest challenges that we face today is to secure information. The first thing that comes to our mind whenever we think about cyber security is 'cyber crimes', which are increasing at a very fast pace. Governments of countries, agencies and companies are taking crucial measures in order to prevent cybercrimes. Despite taking measures cyber security is still a very big concern. This paper mainly lays emphasis on the definition of worms, difference between worms and viruses, behavioural patterns of worms, major categories of worms, aspects of designing of worms, life cycle of worms, history and timeline of worms and a case study of Stuxnet.

Keywords*-worms, virus, behaviour, categories, history, life-cycle, Stuxnet.*

*****

I. INTRODUCTION

Worms are self-replicating computer stand-alone malware that are either designed to only spread or harm. The ability to rapidly spread across a network or system makes worms very much dangerous, since before the user knows what has happened much damage is already done. Spreading of worm is done with help of code referred to as "Payload". By loading payload with messages and consuming system resources like memory, they cause servers, networks, and stand-alone computers to crash. Some payloads are designed in such a way that also erase or alter files.

II. TYPE STYLE AND FONTS

A. Defination

A worm is a program that is designed to infect host machines by individually replicating itself across networks.
Computer worm is a code designed to spread quickly from one computer to another without any user interaction and intervention. Computer Worms do not need a host program or file to spread. Thus can travel alone and replicate themselves extensively. In general, worm is a type of malware that can self-propagate and/or self-replicate over a network of computers. So basically it's a malicious code that spread through either internet connection or LAN (local area network).
Example of a computer Twitter worm:

```
promoteUsButton.click(function(){
channel.postBox.val("I like this website so tweet about it !
http://TwitZap.com");
channel.postBox.focus();
return false;
});
```

B. Difference Between Virus And Worms

[28]The following are the differences between viruses and worms:

TABLE I. DIFFERENCE BETWEEN VIRUS AND WORM

	VIRUS	WORMS
#Subjects		
Definition	A Virus is a program or malware that is designed to spread from file to file on a Pc.	A worm is designed to make copies and propagate on its own from PC to PC, via networks, internet etc.
Need Of Host File	It needs a host file to move and get triggered.	A worm does not need a activator (e.g. host file) to move from system to system.
Infect	Insert itself into a file or a program and get triggered when that latter is executed.	It generally exploits the weakness in the machine and then infects by replicating itself.
Speed	It spreads less rapidly as compared to worms.	Worms spread more rapidly than viruses
Spread	Relies mostly on users for transferring infected files or programs to another machine.	It uses a network to replicate itself and spread to other machines. Doesn't require any user intervention.
Attached With	Can be attached to .EXE,.DOC, .XLS etc.	It can be attached to any attachments of email, any file on a network etc.
Example	C-Brain, Macmag, Cascade etc.	Slammer, Morris etc.

III. BEHAVIORAL PATTERN OF WORMS

Causal Connection Relationship: [2]Spreading and moving from host to host is a behaviour of worms. Before a worm attempts a connection to a host there should an incoming connection from another host that may have been infected by the worm. In order for a host to infect other hosts, the host itself needs to be infected.

Self-similarity: [2]All systems have a certain vulnerability. Worms enter the system by exploiting such vulnerabilities.The worm generally selects the same known vulnerability while attacking the system.

Greedy Destination Visiting Pattern: [2]Ultimate aim of a computer worm is to infect large volume of hosts. In order to achieve this, the hosts infected by worms will try to connect to more hosts as compared to a non-infected host would normally try to connect to.

Continuity: [2]On of the characteristic behaviour of worms is to continuously infect new hosts. Although the rate of infection is slow, more hosts of a domain become infected.

IV. CATEGORIES OF COMPUTERWORMS

[8]There is a wide range of worms varying from their infection technique, propagation method and their effects on the infected computer. We can cite 5 main categories worms, namely:

• Email Worms: A worm spreads itself as soon as an email sent to another system is opened or an attachment is downloaded.

• Instant Messaging Worms: Instant Messaging applications such as Yahoo and AOL are sources for such worms.

• Internet Worms: Worms usually move around and affect another system through network. Speed of propagation is incredibly faster on a network.

• IRC (Internet Relay Chat) Worms: IRC Worms spread through Internet chat channels by transferring infected files or malicious links.

• File-sharing Networks Worms: Worms spread by placing a replica of itself in a shared folder.They spread via P2P network.

V. ASPECTS OF DESIGNING COMPUTER WORMS

In order for a worm to cause maximum amount of damage, various areas for its design need to be kept in mind. The extent to which these aspects are implemented by the worm, directly decides the success of the worm. Inability to design a worm properly may render it useless.

1. Finding Vulnerabilities in a system:

[9]The weakness of the system is the first thing every worm writer must identify. While talking about vulnerability of a system, we often ask, "What job can a worm do in the system with minimal actions?" The effectiveness of the worm depends on the lines of code it requires to complete one operation. More lines of code will use more logic, which means more ways to counter a worm. Worms should be designed such that minimum lines of code and maximum damage is caused, an ideal scenario may be a single line of code rendering the entire system useless.

Example :. A worm could affect all the hosts it encounters if it can change the permissions on the file, or use an unprotected system function to do the same. Worm designers do not write worms on simple bugs in the system. A worm needs to cause maximum damage. So, looking for holes or vulnerabilities in the system that would cause maximum damage or render the system useless is essential for worm writers. System components like, Remote Procedure Calls , Buffer Overflows , Remote Command Execution etc, provide the worm designers the ability of doing multiple things with only one worm. If we had a loophole, where all the files on the system could be deleted by a system component, the worm writers could use this to design a worm that would hibernate till a specified date and execute in all systems at the same time. This would lead to substantial damage to users across the network.

The worm writers will try to find the most secure way into the system, discretely install a back door and terminate itself, after it has made a copy of itself on another host. These types of worms are carefully crafted to slip through holes in the antivirus software, firewalls and operating system components. In order for the hacker to get the most out of the system, these worms keep the system intact till the attack is complete.

2.Speed of propagation:

[9]This is one of main aspects worm writers need to take care of when designing a worm. Worm writers need ensure that the worm can propogate from one host to another at a very fast pace because they have very little life span before they are discovered and curbed.

Earlier, emails were used to propogate worms, which has the slowest rate of propagation. The worms have to move intensively from the host system to the repective mail server and then will be sent to the next host where the email has to be opened by the user to infect the machine. Incase, the mail server itself is flooded by the worm, the worms' speed of propagation is reduced by a great extent due to the damage caused by the worm.

More speedy worms instead of relying on emails, directly interact with the network. These worms follow a root-to-branch approach for propagation. Here, they attack the first host (root) and propagate to its neighbours. Network services like TCP and UDP are used the most. TCP uses dual root topology (one host and one server) and UDP uses single root topology (one host). Worms designed to utilize TCP connects are slower as compared to the ones using UDP. The speed of propagation is three times slower than UDP considering a best case scenario. The TCP connection depend on network traffic. On a network with a lot of data traffic, they will fail to propagate fast.

Worms using UDP are the quickest. The worm is put as a

payload load on the UDP packet and forwarded to the next host. UDP packets are connectionless; enabling them to be three times faster than TCP worms. The speed of propagation of UDP worms is only dependent on the speed of network.
Example: Slammer Worm
It consists of an IP scanner and the fact that it transmits via UDP, a connectionless protocol, eliminates much of the overhead . The worm payload is contained in a UDP packet that is created by an infected system. This packet is forwarded to randomly generated IP addresses; if the destination contains an unsecured version of MSSQL, it will be infected by the worm via buffer overflow. It then affects the other hosts with the same process repeated again.

[9]Stealth:

A worm can go undetected for a longer time if it is stealthier. Hence, this is the next factor that is brought into consideration, after Vulnerability and Speed of propagation. Longer the worm remains, it can infect more number of hosts. Many of the worms cannot resist the securities built by Antivirus Software and the Operating System. Most of the worms are detected and countered within hours. Various techniques such as disabling the firewall and the antivirus software are advised.
Example: W32/Bagle-AU worm is capable of turning off the firewall built into Microsoft's recent Windows XP Service Pack 2 update.
The best way is to use a trusted process to do the job. First we need to compromise a trusted system process and then use it for the attack. A trusted process is one that meets a certain standard of security. A trusted process usually has minimal blockage by firewalls and anti-virus programs and full considerable access to the system. If the worm attaches itself to such trusted process it shouldn't trigger any alarm or take any steps to disable the security. Stealth of the worm lies in going undiscovered.

[9] Propagation Vectors:

Propagation vector is defined as the number of distinct ways a worm can spread. For example, some of the propagation vectors are port scanning and emails. The medium through which the worm will propagate is decided in this area. The speed of propagation of a worm also depends on choosing a right medium of propagation at the right time. For example, if Email and UDP is used for propagation of worm, the speed of propagation is ten fold.Initially the worm would send itself in the form of email, addresses of which are in the users address book. Next, it would spread throughout the local network. On a global scale the worm spreads across computers in matter of hours , the reason being the distant reach of internet and the pace and the speed of UDP. If a single propagation vector is used it will reduce the speed of propagation of worms. The speed at which the worms can spread is directly proportional to the number of propagation vectors.

VI. COPYRIGHT FORMS AND REPRINT ORDERS

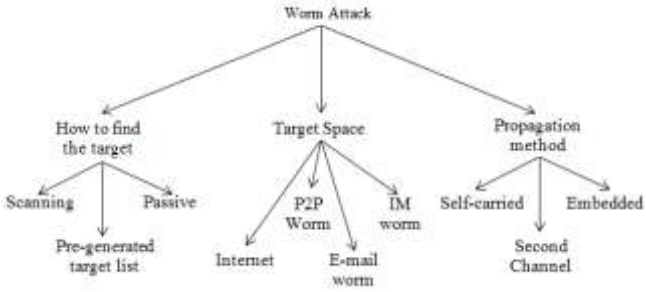


FIGURE I. WORM LIFE CYCLE AND ATTACK

1.TARGET LOCATION:

[38]The worm needs to keep finding new targets in order to keep spreading. Most of the worms search the user's system for the email addresses. Then they create a replica or copy of themselves and copies are sent to those addresses.
Corporations give the attackers an easy penetration point for their worms by allowing e-mail messages across corporate firewalls.

2.EXPLOITING THE SYSTEM:

[38]Worm uses a particular strategy to transfer itself to a new system and get control of that remote system. First they assume what kind of system must be running. According to the kind of system discovered, they forward a worm compatible with such systems. e.g. the creator of the worm may use scripting language or binary code or in-memory code to attack your system.

3.PAYLOAD:

[38]Malicious information might be present in the payload of the worm. The worm may be designed in such a way that it might remove all the files on the hard disk (if it has enough permissions for that). The malicious action is achieved when the worm engine executed the payload. There are no explicit malicious payloads found even in the most dangerous worms.

4.REMOTE CONTROL AND UPDATION:

[38]Remote controlling using a communication module is one of the important components of a worm. This is the module through which the creator or the author of the worm controls the worm .It is through this module that author sends control messages to worm copies. The worm can be used as a DDoS (distributed denial of service) tool on the zombie network against several unknown targets through remote control

5.CLONING AND PROPAGATION:

[38]Once the victim has been exploited the worm needs to get a copy of itself on the victim such that those created copies spread to another host. The process of creating copies continues till all hosts on the network are affected.

VII. History And Timeline Of Computer Worms

TABLE II. TIMELINE OF WORMS

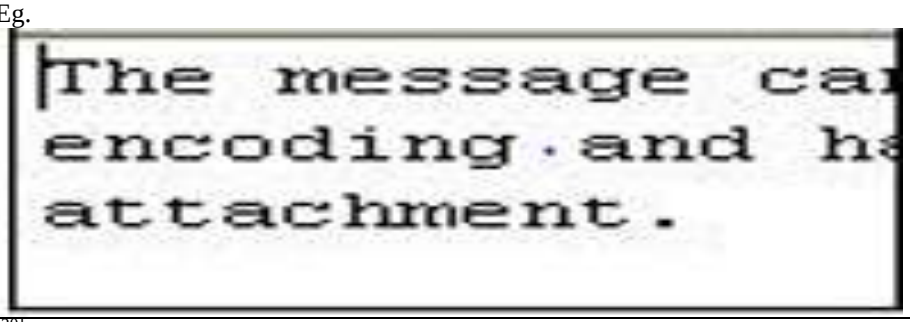
NAME	YEAR	PLATFORM	DESCRIPTION
CREEPER	1971	TENEX(O.S.)	[37]Author: Bob Thomas " The Creeper program will start printing a file and after sometime it will stop suddenly. The program will then search for another Tenex system, open a connection and along with all the external files, state, etc. it will transfer to another machine and continue running on new machine. The program generally "jumps" from one system to another system and only sometimes the program actually replicates itself. Infected systems display the text "I'M THE CREEPER: CATCH ME IF YOU CAN."

WABBIT	1974	LOCAL COMPUTER (DO NOT REPLICATE OVER NETWORK)	[37]It is a self-replicating worm that makes multiple copies of itself on a computer until the system is degraded to such an extent that system performance is reduced to nil and the computer eventually crashes. This virus was named wabbit because of the speed at which it was able to replicate.
			E.g.: Fork Bomb
			Notepad :
			%0|%0 and save it as fork.bat
			C++ version:
			#include <unistd.h>
			int main(void)
			{
			while(1)
			fork();
			return 0;
			}

ANIMAL	1974	UNIVAC	[37]Author: John Walker This type of worm would present the end user with a game known as "ANIMAL". In this game, the user is asked to guess as to what animal the user was thinking of. At the same time, another program known as "PERVADE" would make a copy of itself as well as the ANIMAL and it would spread out to each and every directory where the user has access to.
MORRIS	1988	Unix	[15]Author: Robert Tappan Morris This worm was originally made to measure the size of the Internet. However, due to some error in the program, this worm turned out to be extremely damaging. This program would not share any resources with another program and it had the capacity of bogging down a computer system by infecting the computer multiple times.
HAPPY99	1999	Propagation through Email ,USENET newsgroup postings.	[16]Author: Spanska This worm was able to reach to the end user in 2 ways. One way to reach was from an email attachment and another way to reach was from newsgroup posting. The name of the attachment was "Happy99.exe". When the attachment was executed, the worm would open up a window and display a title named "Happy New Year 1999 !!" and a few animations to conceal its install. When the infected computer is online, the worm automatically sends itself to other users. The worm also does the following: Makes a copy of itself as Ska.exe Extracts Ska.dll to C:\Windows\System Modifies the Wsock32.dll file in C:\Windows\System by copying the existing Wsock32.dll to Wsock32.ska
MELISSA	1999	Having MS Word and Outlook	[31]Author: David L. Smith Melissa is one of the fastest spreading macro virus that is reached to the end users via an email attachment. Attachment when opened would disable some safeguards in Word 97 or 2000. However, if the user's computer had Microsoft Outlook e-mail program, then the virus would be sent to the first 50 people in each of the user's address books. This virus does not kill any other resources but it has the ability to disable corporate and other mail servers. Melissa arrives in an attachment named as "LIST.DOC". The subject line of the email was "Important Message from [the name of someone]" and the body of the email read as "Here is that document you asked for...do not show anyone else ;-)". If the receiver clicks on the attachment, the infecting file is read to computer storage.

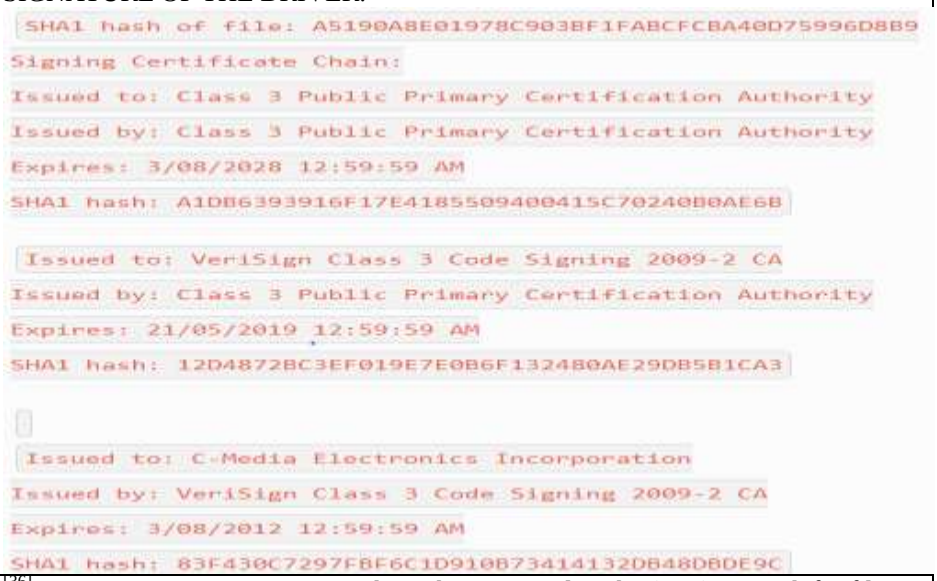
EXPLOREZIP	1999	Windows	[30]Explore Zip which is also known as I-Worm.ZippedFiles, is one of thedestructive computer worm which attacks machines running Microsoft Windows. This type of worm contains a malicious payload. It makes use of Microsoft Outlook, Outlook Express, or Exchange. This worm will start replying to all the unread messages in a user's inbox by mailing to itself. The mail consisted of an attachment named as "Zipped_files.exe". Apart from this, it also searches for the mapped drives and networked computers for windows installations. If found, it makes a copy of itself on the remote computer in the folder named as \Windows and then modifies the Win.ini file of the infected computer.
KAK	1999	Windows	[18]Kak is written in JavaScript and it works on both English and French versions of Windows 95/98 if Outlook Express 5.0 is installed. It does not work in a typical Windows NT installation.
I LOVE YOU	2000	Windows	[32] This virus comes in an e-mail. The email comes with an attachment as well as there is a note in the subject line which is read as "I LOVE YOU". When the attachment is opened, the message is sent to each and everyone in the recipients address book and will also result in deletion of every JPEG, MP3, and few of the other files on the reciever's system. The ILOVEYOU virus changes the victim's Internet Explorer start page in a way that may cause more issues, spreads itself through Internet Relay Chat (Internet Relay Chat) and also resets few Windows registry settings.
Anna Kournikova	2001		[17]Author: Jan de Wit This worm comes in an email. The email comes with an attachment named as "AnnaKournikova.jpg.vbs.". It also contained a note in the subject line which is read as "Here you have, ;0)". When the file is launched it does not show the picture of Anna Kournikova but it actually runs a VB Script that forwards the mail to each and every person in the recipients address book.
CODE RED	2001	Windows	[19] Code Red Worm, which is also known as W32/Bady.worm from Symantec Antivirus Research Centre and I-Worm.Bady is a self-duplicating code that exploits a known vulnerability in IIS servers. As soon as this worm has infected the system, it not only replicates itself but also starts scanning random IP addresses at TCP port number 80 for other IIS servers to attack. It also damages the home page of the infected machines. It also leads to denial of service attack on specific IP address.
SIRCAM	2001	Windows	[21]First appeared on July 19, 2001, this bulk mailing E-mail worm used Microsoft's Outlook program and also had the ability to distribute itself through Windows Network shares. "The worm previously contained two deadly payloads, but due to a program"
NIMDA	2001	Windows (95,XP)	[29]NIMDA's origin comes from the reversed spelling of "admin". Nimda is a file infecting computer worm. This worm made use of various propagation techniques and because of this, NIMDA became the Internet's most widespread worm within the span of 22 minutes. It affected both client's and server's workstation running on various Operating systems like Windows 95, 98, NT, 2000 or XP for client and Windows NT and 2000 for server. This worm was the first to have its own email program so it did not depend on any host's email to spread.
KLEZ	2001	Windows	[20]This worm is one of the most destructive worms which has caused about $19.8 billion in damage. This worm is famous because of its ability to disguise email address in sender line. It could infect the victim's system from simply opening or previewing the message without actually executing or downloading it.The worm utilizes bogus email IDs for the "From" line, which may be one of the following: super@21cn.com flag@21cn.com king@21cn.com A Klez email may have one of twelve possible subject lines: How are you? Can you help me? We want peace Klez has the ability to deactivate on-access virus scanners. It looks for running processes and gives the "Terminate Processes" command to processes with the following names: _AVP32

 ISSN: 2321-8169
184 – 194

			_AVPCC _AVPM
SQL SLAMMER	2003	Windows	[24]This worm is basically a computer virus (technically, a computer worm) that was responsible for causing Denial of Service(DoS) on some Internet hosts and it drastically slowed down general Internet traffic, starting at 05:30 UTC on January 25, 2003. It spreads at a very fast rate and infects most of its 75,000 victims within a span of 10 minutes. Although the title of worm is "SQL slammer worm", the program did not use the SQL language; it exploited two buffer overflow bugs in Microsoft's flagship SQL Server database product. Example: Warhol Worm
Sobig	2003	Windows	[20] This worm was considered as one of the most destructive worms. When executed, it makes a copy of itself to the windows folder named as Winmgm32.exe. It made use of the concept of Mutex named as Worm.X just for making sure that it is the only copy running on that system. This worm arrived in email with the sender's address as "big@boss.com". There are four possible subjects: • Re: Here is that sample • Re: Movies • Re: Document • Re: Sample And these possible attachment names: • Untitled1.pif • Document003.pif • Movie_0074.mpeg.pif
BLASTER	2003	Windows (XP and 2000)	[25]This Worm is also called MSBlast or Lovesan. This virus mainly targeted Microsoft platforms. The virus entered the system by exploiting the security flaw with Microsoft remote procedure call (RPC) process using TCP port number 135. It propagates automatically by transmitting itself with the help of email and several other methods.
MYDOOM	2004	Windows	[20]This worm/virus is reportedly considered to be the most dangerous worm ever released.The main reason why it got so much attention was for its spreading ability. This worm arrived in an email where the sender address is not legitimate. The subject lines of the email were as follows: • test • hi • hello The worm was designed in a way such that either the emails would be undeliverable or if they were to be sent they would be sent as binary. Eg. 
WITTY	2004	Windows	[20]This worm is similar to the CodeRed and Slammer worms in that it did not write any worm code to the hard drive, instead of staying completely in memory. It arrives on UDP source port 4000 posing as an ICQ packet. It exploits buffer overflow vulnerability in the Protocol Analysis Module (PAM). The worm sends copies of itself to 20,000 random IP addresses. The worm then selects one of the first eight hard drives and overwrites 128 sectors (64 kilobytes) with data from memory. Anything on those sectors will be destroyed and beyond recovery. The process of sending the copies of itself and then overwriting the sectors is repeated until the computer is rebooted or the worm overwrites something important that causes the computer to crash.

Sasser	2004	Windows	[26] This worm mainly targets computers running on various operation systems like Windows XP and 2000. It identifies a vulnerable network port and then it transmits itself from one computer to another computer. The main advantage is that it does not require any interface for transferring. It belongs to a family of self-executing worms known as W32.Sasser. The TCP port number 445 is used by Sasser worm to attack a computer. (However, some researchers also say that the worm may also use port 139.)
ZOTOB	2005	Windows	[34]Zotob is a worm that allows the attacker to gather personal and financial information from targeted computers and networks by exploiting Windows buffer overflow vulnerability. In addition of obtaining important information stored in personal or business computers, it also has the ability to convert infected computer into a so-called zombie just for the sake of spreading spam. Some Zotob variants have the ability to disable firewall, anti-virus programs etc. Most Zotob variants targets operating system running on windows 2000. But some variants affect computers running any Windows operating system.
NYXEM	2006	Windows	[35]The Nyxem worm is spread by mass-mailing. The payload of this worm activates on the third of every month, starting from February 3, attempts to disable security-related and file sharing software, and destroy files of certain types, such as Microsoft Office filesVariant: Blackworm.E
STORM	2007		[22]Discovered on January 17th 2007, this is a worm that is different from traditional worms such that it hides in email attachments with the typical line that states “230 dead as storm batters europe”. It is a worm that can be described by the following line: Storm= Worm + Trojan horse + Bot.The payload is designed in such a way that it changes or morphoes in a time of 25-30 minutes thus making it difficult to be tracked by an anti virus or any other protection systems.Also another striking feature of the worm is that the subject line changes everytime.The examples of the worms’s subject lines are as follows: "A killer at 11, he's free at 21 and ...,", “Strongest earthquake hits Beijing” etc.
KOOBFACE	2008		[37]Social networking websites like Facebook, MySpace, hi5, Bebo, Friendster and Twitter are the major targets of the Koobface worm. Koobface is designed to infect various operating systems like Windows and Mac OS ,Linux. It mainly propagates using social networking sites such as Facebook and hence it aims the login information of users on Facebook etc. But if it doesn’t find any reference to social networking sites then it simply discards itself and then loads pop-up messages like “Error installing code please contact support”. The personal information is obtained through cookies. It then uses the personal information to send information to people over social media in the form of download links. For eg. It may be a flash link that may contain .exe file. But the exe file is not the installer of the flash but the installer of the worm itself.
DAPROSY	2009		[23] The worm mainly spreads through the removable devices like USB and LAN’s.The worm maybe classified as risk level 2(low) worm. It is also known as W32/Autorun-APL. The worm belongs to the mass mailer category but the characteristic of the worm is that it intercepts the addresses from the keyboard .Even in the safe mode the worm is very much active and is difficult to remove manually. Problem associated with the worm is of key logging; sensitive information about the user can be sent back to the author using worm’s mailing system. Other problems associated include stalling of OS due to bug generation, stealing of online passwords , threats to E-commerce applications.
MORTO	2011		[37]It is a traditional old fashioned worm which targets windows systems. The system is compromised through Remote Desktop Protocol or RDP connections. The more the number of infected workstations in your local area network, more is the amount of traffic generated by the worm. The worm maintains a library of password such that a weak password found and the system is easily exploited. Eg.

 ISSN: 2321-8169
184 – 194

			
DUQU	2011		[33]The DUQU worm is similar to Stuxnet. The only difference is that while Stuxnet was used to target industrial systems but it rather targeted the driver files. This procedure gave the worm the the ability to download additional components and malicious files.Industrial sabotage was not the target of the worm although the driver used was similar to that used by Stuxnet. SIGNATURE OF THE DRIVER: 
NGRBOT	2012		[36]NGRBot is a worm propagates through internet relay chat(IRC) network for file transfer, chat messangers, social networking sites etc.It is the IRC network that acts as a communication medium between the attackers's server and the zombie machines.The infection by this worm mainly leading to DDOS and flooding attacks.This is mainly designed to infect HTML pages with inline frames ([HTML element#Frames|[iframes]] causing redirections, blocking victims from getting updates from security/antimalware products, and killing those services. On social networking sites it uses a microblogging service to spread itself. 

WELCHIA	2013	Windows	[20]The worm is also known as "Nachi". It exploits the vulnerabilities of RPC (microsoft's remote procedure calls).It is similar to a blaster worm in exploiting the RPC vulnerabilities. However it deletes the blsster worm if it finds it. It then proceeds to download the security patches that would further help to prevent any blaster worm infection. Thus this worm is classified as a HELPFUL worm.
WIN32.IRCBOT	2014		[3]It is a worm that belongs to WIN32/IRCbot.It is a backdoor worm that initially allows access to system without any authorization. It then allows the attacker to take control of the affected system through IRC. It spreads through removable devices. For e.g. sample location of the removable device *<targeted drive>:\dfgdfjjjjdfjdfjgfdjturturutjjf\dfg-2352-26235-2322322-624621221-2622255\usbblock.exe* In some cases it was also observed that the worm created executable autorun.inf files, which is then utilized in order to spread from machine to machine. Attacker may perform the following action after the worm has affected a particular machine : download and upload files, modify system setting , steal and delete the data, get the sensitive data through keylogging et.

VIII. CASE STUDY ON STUXNET

INTRODUCTION:

[10]Stuxnet is a sophisticated computer worm that targets the types of ICS(industrial control systems).
;ultimate goal being to reprogram the programmable logic controllers (PLC's) and thus letting the creators of the worm to operate them as they intend to.
ICS are commonly used in industrial facilities such as Power Plants, Water treatment Plants, factories, Manufacturing units etc.
[11]Stuxnet was a 500-kilobyte computer worm that infiltrated and attacked number of computer systems. This virus operated in three steps:

I. First , it analysed and targeted Windows networks and computer system. Once it entered these systems, it continuously replicated itself.
II. Then the siemens step7 software in the windows system was infiltrated.This Siemens software system is mainly used in ICS such as nuclear facilities.
III. Lastly, after infiltrating the Step7 software, the worm gained access to the PLC's. This gave the attackers access to confidential information.Also it gave them the ability to operate various machines at the industrial sites.

OPERATIONS:

The windows computers which are affefcted are not the actual targets.What Stuxnet looks for PLC's made by Siemens. These are small embedded ICS that are responsible for running of all sorts of automated processes in industries ,factories, power plants etc. These PLC's are often controlled by computers, and Stuxnet looks for Siemens Step 7 controller software.If it doesn't find the software, it does nothing. But if it does, it infects it using vulnerability in the controller software. Then it reads and changes particular bits of data in the controlled PLCs. These changes are so specific that it leads many into believing that these worm is either targeting a specific PLC or group of PLC's performing a specific function in a particular location.

WAY OF INFECTING:

1.Via USB flash drives
The ultimate destination of Stuxnet is the computers that control the centrifuges i.e basically the PLC's. Computers control and monitor the PLC's but PLC's are not connected to internet. Since there is no option of spreading through internet , Stuxnet uses vectors such as USB Flash drives for propagtion. Different versions of Stuxnet use different ways to do this: newer versions exploit LNK file vulnerabilities on windows ; Older version used vulnerabilities in the INF files which are most commonly used for installing device drivers for hardware components.

2.[12]Infected Removable Media:
• Use either the .lnk files or autorun.inf files to spread

3.[12]LAN Communications:
• Copies itself to accessible shared resources
• Copies itself to printer servers
• Uses certain vulnerabilities in RPC

4.[12]Application Data Files:
• Installs in Siemens WinCC SQL Server database with the help known credentials
• Copies into Siemens STEP7 Project files

All Windows Hosts:
• Installs rootkit and loader.It Creates configuration and data files.Then propagates to other potential hosts

5.[12]Siemens STEP7 Hosts:
• Infects Siemens S7 Device OS driver
• Looks for specific PLC models – Infects S7 Project files
• Infects WinCC SQL Server database files (Siemens WINCC hosts)

6.[12]Target System:
• Payloads which consisted of information of host OS, host computer name and a flag(which indicated whether WINCC or Siemens Step7) were installed.
[26]Stuxnet also sets a registry value of "19790509″ .This is

done so as to convey to the new copies that the current compuer has already been affected.One of the number's found in Stuxnet is 0xDEADF007. Perhaps it means "Dead Fool" or "Dead Foot," indicating that Stuxnet is in process to fail the target system.

UPDATE:

Stuxnet updates itself in 2 ways :
1.It checks back to two control servers, one in Malaysia and the other in Denmark
2.uses a peer-to-peer update system: When two copies of this worm infections encounter each other, they compare their versions to make sure they both have the most recent one. These worms have a particular kill date i.e. the date on which the worm will stop spreading by deleting itself.
EFFECTS ON COUNTRIES:
[13]A study of the spread of Stuxnet by Symantec is shown in the following table :

TABLE III. COUNTRIES AFFECTED BY STUXNET

COUNTRIES	SHARE OF INFECTED COMPUTERS
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Other countries	9.2%

EFFECT ON IRANIAN NUCLEAR PROGRAM:

[11]Total of fifteen Iranian facilities were attacked by the Stuxnet worm. It was the code present in one of the worker's USB drive that started the attack. Natanz nuclear facility was the one that was affected. It was in 2010 that the first signs of problems in facility's computer system came up. Inspectors from the International Atomic Energy Agency observed that a number of uranium enriching centrifuges were breaking. The cause of breaking was unknown. It was later in 2010, that security specialists from Belarus were contracted to examine the same. The security firm then found out multiple hostile and harmful files on the Iranian computer systems, the files were from Stuxnet worm. Estimates say over 984 uranium enriching centrifuges were destroyed thus leading to 30% decrease in enrichment facility.

IX. CONCLUSION

In this paper, we studied the history, the timeline of evolution,lifecycle, categories, behavioral patterns and various aspects of computer worm .Also along with this ww studied a case study on Stuxnet : its operation, ways of infecting a machine ,its effect on various countries and specifically its effect on Natanz Nuclear facility in Iran. Thus summarizing the work we conclude that computer worms are very dangerous and despite all the research progress made situation is far from perfect.

REFERENCES

[1] Computer Worm. (2016, November, 18) Wikipedia. [Online]. Available: https://en.m.wikipedia.org/wiki/Computer_worm
[2] Computer Worms Characteristics. (2016, November,20). Hubpages. [Online]. Available: https://hubpages.com/technology/Computer-Worm-Characteristics.
[3] B. Rajesh, Y.R. Janardhan Reddy And B. Dillip Kumar Reddy, "A Survey Paper on Malicious Computer Worms," International Journal of Advanced Research in Computer Science & Technology, 2015.
[4] Craig Fosnock," Computer Worms: Past, Present, and Future," vxheaven.org. [Online].
[5] Vishrut Sharma," An Analytical Survey of Recent Worm Attacks," IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.11, November 2011.
[6] Ravinder Nellutla, Vishnu Prasad Goranthala And Fasi Ahmed Parvez, "Classification of Different Computer Worms with Dynamic Detection Using Victim Number Based Algorithm," International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.803-812.
[7] Information-Computer Worms. (2017, January, 13). Virusall. [Online]. Available:http://virusall.com/computer%20worms/worms.php
[8] Computer Worms, different types of computer worms. (2017,January ,18). Omnisecu. [Online]. Available:http://www.omnisecu.com/security/worms.php
[9] Farhan Syed, "Understanding Worms, Their Behaviour and Containing Them," April 2009. Available:http://www.cs.wustl.edu/~jain/cse571-09/ftp/worms.pdf
[10] Marry Landesman, "Stuxnet Worm Computer Virus," (2017, March ,16). Lifewire. [Online]. Available: https://www.lifewire.com/stuxnet-worm-computer-virus-153570
[11] Michael Holloway , Submitted as coursework for PH241, Stanford University, Winter 2015 Available:http://large.stanford.edu/courses/2015/ph241/holloway1/
[12] Joel "SCADAHacker" Langill, "How Stuxnet Spreads : A look at Infection Path in Best Practice Systems," osisoft. [Online]. Available : http://cdn.osisoft.com/corp/en/media/presentations/2011/vCampusLive2011/PDF/vCL2011_SCADAhacker_Langill_Stuxnet.pdf
[13] Stuxnet. (2017, March, 20). Wikipedia. [Online]. Available : https://en.wikipedia.org/wiki/Stuxnet#Discovery
[14] Simplest Virus- The Fork Bomb. (2017, March,23). Pro Hack. [Online]. Available:http://www.theprohack.com/2009/02/simplest-virus-fork-bomb.html.

[15] Top 10 Worms Of All Time. (2017, March,23). SECPOINT. [Online]. Available:https://www.secpoint.com/top-10-worms.html.

[16] Happy99.Worm. (2017, March,24). Symantec. [Online]. Available:https://www.symantec.com/security_response/writeup.jsp?docid=2000-121812-3151-99&tabid=2

[17] Anna Kournikova. (2017, March,24). Wikioedia. [Online]. Available:https://en.wikipedia.org/wiki/Anna_Kournikova_(computer_virus)

[18] Kak-threat description. (2017, March,25). F-Secure Corporation. [Online]. Available: https://www.f-secure.com/v-descs/kak.shtml

[19] What is Code Red Worm. (2017, March,26). Sans. [Online]. Available: https://www.sans.org/reading-room/whitepapers/malicious/code-red-worm-45

[20] Welcome To Virus Encyclopedia. (2017, March,27). The Virus Encyclopedia. [Online]. Available: http://virus.wikidot.com/

[21] Sircam. (2017, March,26). Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Sircam

[22] Storm Worm. (2017, March,27). Snopes. [Online]. Available: http://www.snopes.com/computer/virus/storm.asp

[23] Daprosy Worm. (2017, March,28). ComputerSafetytpsp. [Online]. Available: http://computersafetytpsp.weebly.com/daprosy-worm.html

[24] Study Guide-What is Slammer Worm.SQL Worm/Sapphire Worm. (2017, March,28). [Online]. Available:https://ethics.csc.ncsu.edu/abuse/wvt/Slammer/study.phpl

[25] Blaster Worm. (2017, March,29). Techopedia. [Online]. Available: https://www.techopedia.com/definition/27295/blaster-worm

[26] Bruce Schneier, "The Story behind the stuxnet virus," 10/7/10@6 am Forbes. [Online]. Available :https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html

[27] Sasser Worm. (2017, March,29). Techopedia. [Online]. Available: https://www.techopedia.com/definition/27296/sasser-worm Nicolas Falliere, Liam O Murchu and Eric Chien, "W32.Stuxnet Dossier," Symantec. Version 1.4,Feb. 2011.

[28] Devika Rangnekar, "Difference Between virus And Worm," (Dec.4,2010).

[29] Nimbda. (2017,April,3). Wikipedia. [Online].

Available: https://en.wikipedia.org/wiki/Sircam

[30] ExploreZip. (2017, April, 3). Wikipedia. [Online].

Available: https://en.wikipedia.org/wiki/ExploreZip

[31] Melissa Virus. (2017, April, 4). SearchSecurity. [Online].

Available: http://searchsecurity.techtarget.com/definition/Melissa-virus

[32] ILOVEYOU virus. (2017,April, 4). SearchSecurity. [Online].

Availability: http://searchsecurity.techtarget.com/definition/ILOVEYOU-virus

[33] Duqu(Win32.Duqu). (2017,April, 5). SeearchSecurity. [Online].

Available: https://nakedsecurity.sophos.com/2011/10/19/duqu-son-of-stuxnet-raises-questions-of-origin-and-intent/

[34] Zotob. (2017,April, 7). SearchSecurity. [Online].

Available: http://searchsecurity.techtarget.com/definition/Zotob

[35] Nyxem. (2017, April, 7)

http://malware.wikia.com/wiki/Nyxem

[36] Analysis Of ngrBot. (2017,April,8) botnets.fr. [Online].

Available: https://www.botnets.fr/wiki/Analysis_of_ngrBot

[37] Timeline of Computer Worms And Viruses. (2017,April,12).

Wikipedia. [Online].

Available: https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

[38] The Generic Structure of Computer Worms. (2017,April,24).

Pearson-InformIT. [Online].

Available: http://www.informit.com/articles/article.aspx?p=366891&seqNum=2