Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Malicious Computer Worms and Viruses: A Survey

[1]B. Rajesh, [2]P. Praveen Yadav and [3]C. V. Chakradhar,
[1,2,3]Assistant Professor , Department of Computer Science and Engineering, G. Pulla Reddy Engineering College,Kurnool, Andhra Pradesh, India.

***Abstract*—**Now a day's computer worms and viruses are playing major role in the destruction of computer world. Computer worms and viruses drawing attention of kinds of computer users with their malicious intentions. They can attack any one's computer like computer scientist, computer pioneers, and computer inventers. Computer worms and viruses can do a lot of damage in research area of computer science and information technology and also on networking. to understand the adverse impacts posed by computer worms and virsues it is necessary to understand the classes of computer worms and viruses. This survey explains about computer worms and their inception, lifecycle, history, timeline. Classification of Computer Worms based on scanning and also based on their behavior, life cycle of Computer worms and viruses.

Keywords— Computer Worms Computer viruses.

I. INTRODUCTION

Computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes i.e., computers on the network and it may do so without any user involvement. Viruses are need to be attached to the system files belongs to the operating system it requires some kind of user action to assist their propagation.

Computer virus is a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. Viruses tends to propagate more slowly They also have more mature defenses due to the presence of a large anti-virus industry that actively seeks to identify and control their spread. Unlike a virus computer worms does not need to attach itself to an existing program. Computer worms almost and always cause harm to the network if only by consuming bandwidth where as viruses almost always corrupt or modify files on a target computer. Computer worms are hated because they consumes more Bandwidth and also they might crash computers if they are infected with computer worms. Infected computers may also used for other attacks such as DDos, phishing attacks etc.. Computer worms are one form of malware along with viruses and Trojans. A person typically installs worms by inadvertently opening an email attachment or message that contains executable scripts. Once installed on a computer, worms spontaneously generate additional email messages containing copies of the worm. They may also open TCP ports to create networks security holes for other applications, and they may attempt to "flood" the LAN with spurious Denial of Service (DoS) data transmissions

II. DEFINITION OF COMPUTER WORM

Definition1: Computer worms are malicious software applications designed to spread via computer networks.

Definition2: A computer worm is a evil-intentioned program that can replicate and run itself.

III. BRIEF HISTORY OF COMPUTER WORM

The first ever program that could be called a Worm, as per definition, was developed for the assistance of air traffic controllers by Bob Thomas in 1971. this worm program would notify air traffic controllers when the controls of a plane moved from on computer to another. This worm named "Creeper" would travel from one computer screen to another on the network showing the message "iamreeper! Catch me if you can! "The difference from most worms was that this creeper did not reproduce itself.

The first Internet infection that required no human intervention to propagate was the Morris Worm, discovered in 1988 and released by Robert Morris. It spread very quickly, infecting a number of vulnerable computers in a matter of hours. The Morris Worm infected various machines and also used multiple exploits including buffer overflows, debugging routines in mail components, password sniffing, and other streams of execution to improve its ability to attack other computers. Although released on accident, the benign concept doesn't really apply tothe Morris Worm, as ithad a significant amount of impact because of the bug in its code. When re infecting a computer, there remained the possibility that the new infection would be persistent, allowing other worms to run and terribly impact system performance. However, this caused the worm to be noticed instantly, and therefore, quickly contained. **Modern Worms:** Active computer worms have returned to prominence in recent times. The first one to cause an eruption was Code Red. This infection proved how quickly a simple self-replicating program could spread via the internet's current infrastructure. Code Red exploited a buffer flow condition in the Microsoft IIS (Internet Information Server). It was able to propagate quickly because of the "always on" nature of IIS and many versions of the Windows operating system. Code Red was also equipped with scanning capabilities that improved its throughput and gave it the ability to elude numerous IP address security features.

IV. LIFE OF COMPUTER WORM

Once the worm enters in any one of the host computer. The life of the worm contain the following phases .they are

A. Scanning for a victim
B. Exploiting the victim
C. Payload
D. Cloning itself onto the victim
E. Stealth techniques used to hide itself.

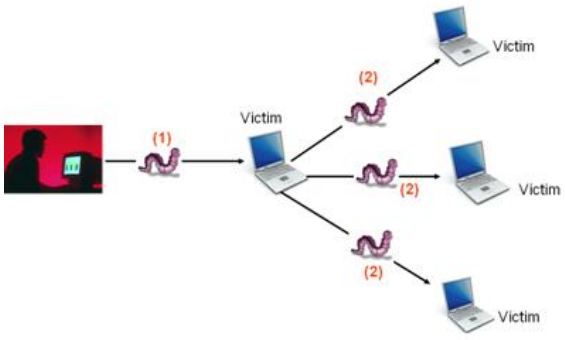

Fig. 1: Figure indicates the life of a malicious computer worms

Once the worm is created the intruder sends it in to the network. Once the worm is released into the network it will first searches for a vulnerable host i.e., victim. If victim is found it will exploit in to the victim host and then it clones itself onto the victim.

This process will continues to spread the worm to entire network without any human intervention.

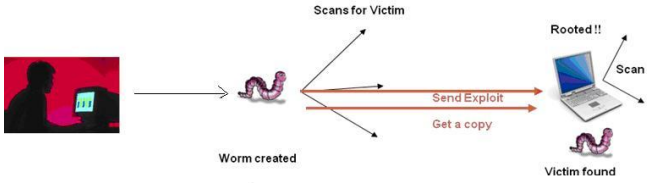

Fig. 2: Figure indicates spreading of a malicious computer worms

A. Scanning for a victim.

Scanning for a victim means target discovery. It represents the mechanism by which discovers a new target to infect. scanning requires searching a set of addresses to identify vulnerable hosts. Two simple form of scanning are sequential scanning and random scanning. The other from of scanning include full scan, subnet scan, divide and conquer scan. scanning worms spread comparatively slowly compared with a number of other spreading techniques, but when coupled with automatic activation, they can still spread very quickly in absolute terms.

B. Exploiting the victim.

Exploiting the victim means gaining access on the victim computer. A small piece of code provides access to a victim computer by utilizing some flaws in the logic of a program running on the victim computer. Gaining the access means the ability to run commands/programs on the host computer.

C. Payload.

During this phase the worm can create backdoors in the host machine, alter or destroy files, transmit passwords, or leave copies of itself. Worms use operating system facilities that are often automatic and invisible to the users. Often, worm activity remains invisible until their uncontrolled replication consumes system resources; worm's attacks include slowing or halting the system, denial of services by flooding the network with useless packets. Worms can also sends sensitive information to cause confusion, collect sensitive data, or damage data in the host machine.

D. Cloning itself on to the victim.

Once the victim has been exploited the worm needs to get a copy of itself on the victim. Once the copies of itself are created they will be spread to another targeted host computer. This process will continues in each host, until the entire host computers in the network are attacked with the worms.

E. Stealth techniques used to hide itself.

Worms uses some stealth techniques to hide itself on the host machine when ever any antivirus programs are running on that machine. Worms can also hide the process running on the machine. Worms can also hide the user files and also it can delete the logs.

V. CLASSIFICATION OF COMPUTER WORMS

A. Classification based on behavior

- **Stealth worms:**This worm doesn't spread in a rapid fashion but instead they spread in a stealthy. They are very difficult to detect.
- **Polymorph worms:**To make the signature based detection more complicated these worms can change themselves during the propagation.
- **File worms:**These worms are modified version of viruses but unlike viruses this worms does not connect their presence with any executable files. They simply copy their code to some other disk or directory hoping that these new copies will someday be executed by the user.
- **Multi-vector worms:**This type of worms use different type of propagation methods in order to make more hosts vulnerable for attack and effectively propagate behind firewalls.
- **Email worms:**Email themselves to other email addresses and make the user execute emailAttachments with malicious code or use bugs in the email programs to get attachments executed automatically.

B. Classification based on scanning

- **Random scanning:**Random Scanning worm will generate a random IP addresses using a pseudorandom number generator. Thus every host on the network is equally likely to be scanned. CodeRed v^2 and SQL Slammer are the random scanning worms.
- **Localized scanning:**Localized scanning is a simple technique used by computer worms to search for the vulnerable hosts. Localized scanning trades off between the local and the global search of vulnerable hosts and has been used by Code Red II and Nimda worms
- **Sequential scanning:**Sequential scanning worms' scans IP addresses sequentially. After the worm compromises a vulnerable host, it checks the host next to this vulnerable host. Blaster worm employed sequential scanning.
- **Topological scanning:** Topological scanning worms rely on the local information contained in the compromised hosts to locate new targets. Local information includes /etc/hosts file, email addresses etc. Topological scanning was used by Morris worm.
- **Hit list scanning:** The worm writer gathers a list of potentially vulnerable hosts beforehand, which are targeted first when the worm is released. This speeds up the spread of the worm at an initial stage. Hit list scanning was used by Slammer worm.

VI. TIMELINE OF COMPUTER WORMS

Year	Worm Name	Worm Description
1971	**Creeper**	**Author:** Bob Thomas at BBN Technologies The Creeper virus, an experimental self-replicating program, Creeper infected DEC PDP-10 computers running the TENEX operating system. Creeper gained access via the ARPANET and copied itself to the

		remote system where the message, "I'm the creeper, catch me if you can!" was displayed. The Reaper program was later created to delete Creeper.
1974	**Wabbit**	The Wabbit virus, more a fork bomb than a virus, is written. The Wabbit virus makes multiple copies of itself on a single computer (and was named "Wabbit" for the speed at which it did so) until it clogs the system, reducing system performance, before finally reaching a threshold and crashing the computer.
1975	**Animal**	**Author:** John Walker for the UNIVAC 1108. Animal asked a number of questions to the user in an attempt to guess the type of animal that the user was thinking of, while the related program PERVADE would create a copy of itself and ANIMAL in every directory to which the current user had access. It spread across the multi-user UNIVACs when users with overlapping permissions discovered the game, and to other computers when tapes were shared. The program was carefully written to avoid damage to existing file or directory structure, and not to copy itself if permissions did not exist or if damage could result. Its spread was therefore halted by an OS upgrade which changed the format of the file status tables that PERVADE used for safe copying. Though non-malicious, "Pervading Animal" represents the first Trojan "in the wild".
1988	**Morris worm**	**Author:** Robert Tappan Morris The Morris worm infects DEC VAX and Sun machines running BSD UNIX connected to the Internet, and becomes the first worm to spread extensively "in the wild", and one of the first well-known programs exploiting buffer overrun vulnerabilities.
1999	**Happy99**	First found inJanuary 20 It invisibly attaches itself to emails, displays fireworks to hide the changes being made, and wishes the user a happy New Year.It modifies system files related to Outlook Express and Internet Explorer (IE) on Windows 95 and Windows 98.
	Melissa	First found in March 26, 1999, using holes in Microsoft Outlook, Melissa shut down Internet mail systems that got clogged with infected e-mails propagating from the worm. Once executed the original version of Melissa used a macro virus to spread to the first 50 addresses in the user's Outlook address book. However, if Internet access or Outlook were not available, it would copy itself to other word documents and attempt to E-mail those documents, Revealing potentially confidential information. Further, it would modify existing documents by inserting quotes from the Simpson's television show. (Henry, 2003) **Estimated damage:** $1.1 billion.
	ExploreZip	First found in June 6 TheExploreZip worm, which destroys Microsoft Office documents, was first detected.
	Kak worm	First found in December 30 The Kak worm is a JavaScript computer worm that spread itself by exploiting a bug in Outlook Express.
2001	**"Anna Kournikova Virus"**	First appearing in February 2001 it was produced by a "scrip kiddie," and is well known only for its social engineering attachment that appeared to be a graphic image of Russian tennis star Anna Kournikova. However, when the file was opened, a clandestine code extension enabled the worm to copy itself to the Windows directory and

		then send the file as an attachment to all addresses listed in your Microsoft Outlook e-mail address book. The "Anna Kournikova Virus" worm although famous was just a nuisance as it did little to no damage **Estimated damage:** $166,827
2001	**Code Red**	First found on July 13, 2001 this worm exploited vulnerability in Microsoft's Internet Information Server (IIS) web servers to deface the host's website, and copy the command.com file and rename it root.exe in the Web server's publicly accessible scripts directory. This would provide complete command line control to anyone who knew the Web server had been compromised. It also waited 20-27 days after it was installed to launch denial of service attacks against the White House's IP address. Code Red spread at a speed that overwhelmed network administrators as more than 359,000 servers became compromised in just over 14 hours. At its peak, more than 2,000 servers were being compromised every single minute. Estimates are that Code Red compromised more than 750,000 servers. (Henry, 2003) **Estimated damage:** $2.6 billion
	Sircam	First found on July 19, 2001 this mass mailing E-mail worm not only exploited Microsoft's Outlook program it had the ability of spreading through Windows Network shares. The worm had two deadly payloads, but due to a program error they did not work. **Estimated damage:** $1.03 billion
	NIMDA	First appearing in September 2001, NIMDA, which is admin spelled backwards was not as malicious in nature as previous worms, but its advanced features and its different means of propagation which included from client to client via email, from client to client via open network shares, from web server to client via browsing of compromised web sites, from client to web server via active scanning for and exploitation of various Microsoft IIS vulnerabilities, and from client to web server via scanning for the back doors left behind by the "Code Red II" and "sadmind/IIS" worms, allowed it to spread faster than any preceding worm. NIMDA also the first worm that contained its own Email program so it did not depend on the host's E-mail program to propagate. **Estimated damage:**$645 million
	Klez	First appearing in October 26, 2001 Klez, and it variants were still considered a problem late in 2003, making Klez one of the most persistent viruses ever. Klez was a hybrid worm that took advantage of a flaw in Outlook that allowed it to be installed simply by viewing the E-mail in the preview panel. As a hybrid threat it could behave like a virus, a worm and at other times even like a Trojan horse. Klez also incorporated a technique we saw in the Christmas Exec worm as it selected one Email address from the host's address book to use as the "from" address, then sending the worm to all the other addresses. In this manner, the E-mail often appeared to have been sent from someone the addressee actually knew. **Estimated damage:** $18.9 billion
2003	**SQL Slammer**	Appearing January 25, 2003, and taking advantage of two buffer overflow bugs in Microsoft's SQL Server database product, it

		spread rapidly, with a doubling time of 8.5 seconds in the early phases of the attack allowing it to infecting most of its victims within 10 minutes. SQL Slammer was the first example of a "Warhol worm." A Warhol worm was first hypothesized in 2002 in a paper by Nicholas Weaver, and it is an extremely rapidly propagating computer worm that spreads as fast as physically possible, infecting all vulnerable machines on the entire Internet in 15 minutes or less. The term is based on Andy Warhol's remark that "In the future, Everybody will have 15 minutes of fame." (Computer Worm, 2005) **Estimated damage:** $1.2 billion.
	Sobig	Originally put together in January 2003 to spread a proxy server Trojan, its variant Sobig.F set a record in sheer volume of e-mails. Sobig like Nimda used a built-in SMTP engine so it did not depend on the host's E-mail program to propagate. Then emulating Klez, it selected one E-mail address from the host's address book to use as the "from" address, then sending the worm to all the other addresses. It also attempted to create a copy of itself on network shares, but failed due to bugs in the code. **Estimated damage:**$36.1 billion
	Blaster	Appearing August 11, 2003 Blaster exploited a Microsoft DCOM RPC vulnerability to infect systems running Windows 2000 and Windows XP, and cause instability on systems running Windows NT, and Windows Server 2003. Filtering of virus activity by Internet service providers (ISPs) worldwide greatly reduced the spread of Blaster. **Estimated damage:** $1.3 billion
2004	**Mydoom**	Appearing January 26, 2004 and primarily transmitted via E-mail to appear as a transmission error, Mydoom's rapid spread becomes the fastest spreading email worm ever. It slowed overall Internet performance by about 10%, and average web page load times by about 50%. **Estimated damage:** $38.5 billion
	Witty	Appearing March 19, 2004, the Witty worm was the fastest developed worm to date as there was only 36 hours between the release of the advisory to the release of the virus. Witty infected the entire exposed population of twelve thousand machines in 45 minutes, and it was the first widespread worm that destroyed the hosts it infected (by randomly erasing a section of the hard drive) without significantly slowing the worm's expansion. **Estimated damage:** $11 million
	Sasser	Appearing on April 30, 2004 and spreading by exploiting a buffer overflow in the component known as LSASS, (Local Security Authority Subsystem Service) it hit the Internet a little more than two weeks after Microsoft warned users of this flaw. Although it caused infected Windows XP and Windows 2000 computers to repeatedly reboot, Sasser did little damage, as was merely designed to spread and carried no payload. **Estimated damage:** $14.8 billion
2005	**Zotob**	Zotob is a computer worm which exploits security vulnerabilities in Microsoft operating systems like Windows 2000, including the MS05-039 plug-and-play vulnerability. This worm has been known to spread on Microsoft-ds or TCP port 445."The Zotob

		worm and several variations of it, known as Rbot.cbq, SDBot.bzh and Zotob.d, infected computers at companies such as ABC, CNN, The Associated Press, The New York Times, and Caterpillar Inc." **Estimated damage:** $97,000
2006	**Nyxem**	The Nyxem worm was discovered. It spread by mass-mailing. Its payload, which activates on the third of every month, starting on February 3, attempts to disable security-related and file sharing software, and destroy files of certain types, such as Microsoft Office files
2007	**Storm**	The Storm Worm is a backdoor Trojan horse that affects computers using Microsoft operating systems, discovered on January 17, 2007. The worm is also known as: Troj/Dorf and Mal/Dorf (Sophos) Trojan.DL.Tibs.Gen!Pac13 [3] Trojan.Downloader-647 Trojan.Peacomm (Symantec)
2008	**Koobface**	Koobface worm targets users of the social networking websites Facebook, MySpace, hi5, Bebo, Friendster and Twitter. Koobface is designed to infect Microsoft Windows and Mac OS X, but also works on Linux in a limited fashion. Koobface ultimately attempts, upon successful infection, to gather login information for FTP sites, Facebook, and other social media platforms, but not any sensitive financial data. It then uses compromised computers to build a peer-to-peer botnet. A compromised computer contacts other compromised computers to receive commands in a peer-to-peer fashion. The botnet is used to install additional pay-per-install malware on the compromised computer as well as hijack search queries to display advertisements. It was first detected in December 2008 and a more potent version appeared in March 2009. A study by the Information Warfare Monitor, a jointcollaboration from SecDev Group and the Citizen Lab in the MunkSchool of Global Affairs at the University Toronto, has revealed that the operators of this scheme have generated over $2 million in revenue from June 2009 to June 2010.
2009	**Daprosy Worm**	Daprosy Worm is a malicious computer program that spreads via LAN connections, spammed e-mails and USB mass storage devices. Infection comes from a single read1st.exe file where several dozens of clones are created at once bearing the names of compromised folders. The most obvious symptom of Daprosy infection is the presence of Classified.exe or Do not open - secrets!.exe files from infected folders. The worm belongs to the “slow” mass mailer category where copies of which are attached and sent to addresses intercepted from the keyboard. The e-mail consists of a promotion of and installation instruction for an imaginary antivirus product purported to remove unknown infections from the computer. While infection cannot occur until attached worm is renamed and opened, it could spread to system folders in a matter of seconds! Also, it is known to shutdown or hang Windows Vista and Windows 7 when its attempt to write on the system drive is denied. Also, the worm hides folders and makes them "super hidden" so that data contained in them cannot

		be easily accessed.
2010	**Stuxnet**	First found in June 17 Stuxnet, a Windows Trojan, was detected. It is the first worm to attack SCADA systems.[55] There are suggestions that it was designed to target Iranian nuclear facilities.[56] It uses a valid certificate from Realtek.
2011	**Summer**	Summer The Morto worm attempts to propagate itself to additional computers via the Microsoft Windows Remote Desktop Protocol (RDP). Morto spreads by forcing infected systems to scan for Windows servers allowing RDP login. Once Morto finds an RDP-accessible system, it attempts to log into a domain or local system account named 'Administrator' using a number of common passwords. A detailed overview of how the worm works—along with the password dictionary Morto uses—was done by Imperva.
	Duqu	First found in September 1 Duqu is a worm thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab)[64] of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu. Duqu gets its name from the prefix "~DQ" it gives to the names of files it creates.
2012	**NGRBot**	First found in September 20NGRBot is a worm that uses the IRC network for file transfer, sending and receiving commands between zombie network machines and the attacker's IRC server, and monitoring and controlling network connectivity and intercept. It employs a user-mode rootkit technique to hide and steal its victim's information. This family of
		bot is also 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. The bot is designed to connect via a predefined IRC channel and communicate with a remote botnet.
2013	**Welchia worm**	W32.Welchia.Worm is a worm that exploits multiple vulnerabilities, including: The DCOM RPC vulnerability (first described in Microsoft Security Bulletin MS03-026) using TCP port 135. The worm specifically targets Windows XP machines using this exploit. Users are recommended to patch this vulnerability by applying Microsoft Security Bulletin MS03-039. The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80. The worm specifically targets machines running Microsoft IIS 5.0 using this exploit. As coded in this worm, this exploit will impact Windows 2000 systems and may impact Windows NT/XP systems.
2014	**Win32. IRCBot**	Win32.IRCBot is a backdoor computer worm that is spread through MSN Messenger and Windows Live Messenger. Once installed on a PC, the worm copies itself into a Windows system folder, creates a new file displayed as "Windows Genuine Advantage Validation Notification" and becomes part of the computer's automatic startup.[2] In addition, it attempts to send itself to all MSN contacts by offering an attachment named 'photos.zip'. Executing this file will install the worm onto the local PC. The Win32.IRCBot worm provides a backdoor server

		and allows a remote intruder to gain access and control over the computer via an Internet Relay Chat channel. This allows for confidential information to be transmitted to a hacker.
2015	**BASHLITE**	The Bashlite malware is leaked leading to a massive spike in DDoS attacks.
	Linux.Wifatch	Linux.Wifatch is revealed to the general public. It is found to attempt to secure devices from other more malicious malware
2016	**RansomwareLocky**	First found in February, 2016. RansomwareLocky with its over 60 derivatives spread throughout Europe and infected several million computers. At the height of the spread over five thousand computers per hour were infected in Germany alone. Although ransomware was not a new thing at the time, insufficient cyber security as well as a lack of standards in IT was responsible for the high number of infections. Unfortunately even up to date antivirus and internet security software was unable to protect systems from early versions of Locky.
	Tiny Banker Trojan (Tinba)	Found in February, 2016 Tiny Banker Trojan (Tinba) makes headlines. Since its discovery, it has been found to have infected more than two dozen major banking institutions in the United States, including TD Bank, Chase, HSBC, Wells Fargo, PNC and Bank of America. Tiny Banker Trojan uses HTTP injection to force the user's computer to believe that it is on the bank's website. This spoof page will look and function just as the real one. The user then enters their information to log on, at which point Tinba can launch the bank webpage's "incorrect login information" return, and redirect the user to the real website. This is to trick the user into thinking they had entered the wrong information and proceed as normal, although now Tinba has captured the credentials and sent them to its host.
	Mirai	First found on September, 2016. Mirai creates headlines by launching some of the most powerful and disruptive DDoS attacks seen to date by infecting the Internet of Things. Mirai ends up being used in the DDoS attack on 20 September 2016 on the Krebs on Security site which reached 620 Gbit/s. ArsTechnica also reported a 1 Tbit/s attack on French web host OVH. On 21 October 2016 multiple major DDoS attacks in DNS services of DNS service provider Dyn occurred using Mirai malware installed on a large number of IoT devices, resulting in the inaccessibility of several high-profile websites such as GitHub, Twitter, Reddit, Netflix, Airbnb and many others.The attribution of the attack to the Mirai botnet was originally reported by BackConnect Inc., a security firm.
2017	**WannaCryransomware attack**	First found on May, 2017. The WannaCryransomware attack spreads globally. Exploits revealed in the NSA hacking toolkit leak of late 2016 were used to enable the propagation of the malware. Shortly after the news of the infections broke online, a UK cybersecurity researcher in collaboration with others found and activated a "kill switch" hidden within the ransomware, effectively halting the initial wave of its global propagation. The next day, researchers announced that they had found new variants of the malware without the kill switch.

	Petya	First found on june, 2017. The Petya (malware) attack spreads globally affecting Windows systems. Researchers at Symantec reveal that this ransomware uses the EternalBlue exploit, similar to the one used in the WannaCryransomware attack
	Xafecopy	First found on September, 2017. The Xafecopy Trojan attack 47 countries affecting only android operating systems. Kaspersky Lab identified it as a malware from the Ubsod family, stealing money through click based WAP billing systems.
	Kedi RAT	First found on September, 2017. A new variety of RAT Trojan, Kedi RAT (Remote Access Trojan) distributed in a Spear Phishing Campaign. The attack targeted Citrix users. The Trojan was able to evade usual system scanners. Kedi Trojan has all characteristics of a common Remote Access Trojan and it could communicate to its Command and Control center via gmail using common HTML, HTTP protocols

CONCLUSION

In this paper, the study on how the computer worms are came in to this world and how they evolved and how much amount of damage they have caused to the networks and their lifestyle, classification, code analysis are done. By summarizing this work it will clear that, they are very dangerous. We can also understand that computer worms have caused a massive damage to the computer world.

References

[1] Sarah H. Sellke, Ness B. Shroff, SaurabhBagchi, Modeling and Automated Containment of Worms", Journal IEEE Transaction on Secure and Dependable Computing, Vol 5, No 2, Published on April-June 2008.

[2] Cliff Changchun Zou, Weibo Gong, Don Towsley, "Code red worm propagation modeling and analysis" Conference on Computer and Communications Security, Proceedings of the 9th ACM conference on Computer and communications security

[3] Nicholas Weaver, Vern Paxson, Stuarts Staniford, Robert Cunningham, "A Taxonomy of Computer Worms" First Workshop on Rapid Malcode (WORM), 2003.

[4] "Timeline of Computer Worms and Viruses " [online] Availableat http://en.wikipedia.org/wiki/Timeline_of_ computer_viruses_and_worms.

[5] CraigFosnock,"Computer Worms: Past, Present, and Future"- East Carolina University, Published in 2005

[6] Pankaj Kohli, "Worms - survey and propagation"MS by Research - Computer Science and Engineering International Institute of Information Technology Hyderabad, India [online] Available at http://www.pank4j.com/research/worms.pdf

[7] Simon Byers, Aviel Rubin, and David Kormann.Defending against internet-based attack on the physical world, http://www.avirubin.com/ scripted.attacks.pdf.

[8] Modern Worms [online] Available at http://www.spamlaws.com/history-of-worms.html.

[9] MChristodorescu "Static analysis of executables to detect malicious patterns" Proceedings of the 12th conference on 2003. [online] Available at portal.acm.org

[10] Moriss Worm "history of computer worms [online] Available at http://www.spamlaws.com/history-of-worms.html

[11] Phases of Computer Worm Nicholas Weaver, Vern Paxson, Stuarts Staniford, Robert Cunningham, "A Taxonomy of Computer Worms" First Workshop on Rapid Malcode (WORM), 2003.

[12] Puja Bajaj, Arjun Guha Roy, Department of Computer Science St. Cloud State University, St. Cloud MN 56301, Classification based on behavior.