Original Research Paper

Volume-9 | Issue-5 | May-2019 | PRINT ISSN No 2249 - 555X

Computer Science

# REVIEW ON THE HISTORY OF MALICIOUS OBJECTS ATTACKS IN NETWORK

**Malti Kumari** — Research Scholar, University Department of Computer Applications, Vinoba Bhave University, Hazaribag, Jharkhand, India

**Bimal Kumar Mishra*** — Principal Markham College of Commerce, Vinoba Bhave University, Hazaribag, Jharkhand, India *Corresponding Author

**ABSTRACT** In this paper we have discussed about the different types of malicious objects (Virus,Worms, Trojan Horse etc.) in Network. The behavior and nature of worms and virus from 1980 to 2019 is also critically analysed. Development of anti-virus software over the last 3 decades as per the attacking behavior of worms in the Network is also analysed.

**KEYWORDS :** Virus; Worms; Network; Anti-virus Software; Attacking behavior

***A.* Virus*:***
A self-replicating program. Some definitions also add the constraint saying that it has to attach itself to a host program to be able to replicate. Often Viruses require a host, and their goal is to infect other files so that the virus can live longer.

***B.* Worms*:***
Worms are insidious because they rely less (or not at all) upon human behavior in order to spread themselves from one computer to others. The *computer worm* is a program that is designed to copy itself from one computer to another, leveraging some network medium: e-mail, TCP/IP, etc. The worm is more interested in infecting as many machines as possible on the network, and less interested in spreading many copies of itself on a single computer (like a computer virus).

Some categories that come under worms are:
i.Mailers and Mass-Mailer worms
ii.Octopus
iii.Rabbits

***C. Trojan Horses:***
Trojan Horse is a one which pretend to be useful programs but do some unwanted action. Most trojan activate when they are run and sometimes destroy the structure of the current drive (FATs, directories, etc.) obliterating themselves in the process. These does not require a host and does not replicate. A special type is the backdoor trojan, which does not do anything overtly destructive, but sets your computer open for remote control and unauthorized access.

- ***D. Other Malicious objects :***

There are other types of malicious programs apart from Viruses, Worms and Trojan Horses. Some of them are described below.

***I.Logic Bombs:***
A logic bomb is a programmed malfunction of a legitimate application. These are intentionally inserted in otherwise good code. They remains hidden with only their effects are being visible. These are not replicated. Bugs do everything except make more bugs.

***ii.Germs:***
These are first-generation viruses in a form that the virus cannot generate to its usual infection process. When the virus is compiled for the first time, it exists in a special form and normally does not have a host program attached to it. Germs will not have the usual marks that the most viruses use in second-generation form to flag infected files to avoid reinfecting an already infected object.

***iii.Exploits:***
Exploit is specific to single vulnerability or set of vulnerabilities. Its goal is to run a program (possibly remote, networked) system automatically or provide some other form of more highly privileged access to the target system.

**iv.Effectiveness –**
Many of the computer viruses have far-reaching and catastrophic effects on their victims, including total loss of data, programs, and even the operating systems.

**v.Functionality –**
A wide variety of functions has been demonstrated in virus programs. Some virus programs merely spread themselves to applications without attacking data files, program functions, or operating system activities. Other viruses are programmed to damage or delete files, and even to destroy systems.

**vi.Persistence –**
In many cases, especially networked operations, eradication of viruses has been complicated by the ability of virus program to repeatedly spread and reoccur through the networked system from a single copy.

- The following are some of the characteristics of Viruses:

**I.Size-**
The sizes of the program code required for computer viruses are very small.

**ii.Versatility-**
Computer viruses have appeared with the ability to generically attack a wide variety of applications.

**iii.Propagation-**
Once a computer virus has infected a program, while this program is running, the virus is able to spread to other programs and files accessible to the computer system.

- Here we define three categories of worms

i.E-mail (and other Client application) worms
ii.Windows file sharing worms
iii.Traditional worms.
i.E-mail worms- Email worms are programs that, when executed on a local system, take advantage of user's email capabilities to send themselves to others.
ii.Windows file sharing worms take advantage to the Microsoft Windows Peer-to- Peer service that is enabled whenever windows determines networking hardware is present in a system.
iii.Traditional worms are worms that do not require user intervention and /or Worms that use other methods of propagation.

Most often the propagation uses direct connections over TCP/IP based protocols to exploit vulnerabilities in OS applications.

**History of Malicious attacks in network:**
The first computer worm program was created at XEROX PARC for some maintenance purpose [1]

The year of 1980's some incidents which came to light due to cyber-crime are AT&T Long distance Breakdown, several glitches aboard the shuttle Columbia, other a on Airbus A 320 crashes etc.[2]

On December 1987 Christmas Tree was the first malicious code to use e-mail to propagate through it did trick the user into opening a fake Christmas card like a Trojan horse [3].

In 1993 (after Share Fun Virus) one new virus was found in both e-mail

and IRC to propagate known as Antimare [3].
After 4 years in 1997 month of Feb was found the first known virus to use e-mail to spread in the network was properly known Sharefun. [3]

In 1998, several dozen-computer systems in U.S military installations and government agencies were successfully breached [4].

In December 1999, the owners and operators of the Napster web site were sued by the Recording Industry Association of American for "illegally" distributing copy righted music (in the form of MP3 files) on the Internet [4].

In March 1999 first mass mailer, E-Mailed itself to the first 50 entries in the user address book, causing a widespread epidemic Melissa was found. [3]

In February 2000, various websites like Amazon, eBay, CNN, Yahoo, and others were owned illegally by criminals [4]

And March 2000 LoveLetter virus was Introduced hidden double extensions. used the prospect of a secret admire to entice users to execute it [4].

In May 2000 'I LOVE YOU" virus also known as lovebug infected many computers in Europe, U.S., and Asia [4]

Few other Email worms discovered in year 2000 like "stages "in May 2000 and" VBSWG Toolkit "June 2000 and other one is windows File sharing worm in Feb. 2000 is "NetLog"[3].

Year 2001 was declared as the "Year of worms" as many of the worms like self – replicating code, fast moving worms like Magistr, Sircam, PeachyPDF,Nimda, Klez, Goner is Email worms, and Few others are shorm &.Nimda are Windows File sharing worms.

Some other Traditional worms are detected in 2001 is 'Ramen', Jan 2001, Lion Ma 2001, Box Poison May 2001 cheese Jun 2001, code Red Jul 2001, walk Aug 2001, Nimda Sep. 2001 [3].

Year 2002 some windows file sharing worms are detected like Ladex Jul 2002, Opasery Sept. 2002, Goabot Oct. 2002. [3]

In 2003 was not a silent year about malicious objects. various worms were activated like Bibrog, Netspree, Slammer, W32/Sobig, etc. [5],[6],[7]

All these events were due to the worm propagation or generating bogus messages. These are some events, which because a matter of concern to the persons related to the cyber defense world.

A good taxonomy has been provided by Nicholas Weaver and his team, to understand the threat posed by computer worms, to understand the classes of worms, to know the attackers who may employ them, and the potential payloads. Malicious objects first discover the computer machine whether it is exists or not, it can be done by pre-generated target list or externally generated target list[8].

After that, activation is carried out by some means like human activity based, scheduled process activation or self-activation, a large payload is generated on Data servers, Proxy servers HTML servers, E-mail Servers or at some worm detection mechanisms and cause an information loss[8].

What are the reasons behind these destructive events? Who motivate and promote them? Who are the real attackers? Answers of these questions may be due to experimental curiosity. Pride and power, commercial advantage, extrusion and criminal gain, random protest, political protest or terrorism [8].

current Internet system having more than 233 million of computers till Jan-2004[9], are prone to threat from various malicious objects, may be of any type like-worm, virus, Trojan horse, etc and they can spread over the Internet through-

Secondary memory (Floppy, Hard-disk, CD-ROM etc)
E-mail (Attachments)
Instant Messaging (FTP, Text Messaging, Chat etc.)
Malicious Boot Programs [10]

In year of 2004 some E-mail worms are discovered like w32/Bangle.gen 18th Jan 2004 W32/MyDoom@mm 26th Jan2004. W32/Netsky.J@MM8th March 2004 and some other Internet worms are W32/sasser.worm.a 30th April 2004, Perl/Santy.worm 21st Dec.2004.[5],[6],[7]

In year 2005 the worm type is Internet /IRC worm name is W32/IRCboot.worm/MS05-039 in 16th Aug 2005.[5][6][7]

In year 2006 the worm type is Email/File-sharing Networm worm Name is W32-Nyxem.e 16th Jan 2006 and some other Email worm is W32. Rontokbro.AN@m22nd April 2006.[5],[6],[7].

Year 2008 some Internet worms are W32/Koobface.worm 3rd Aug2008.and 2009 W32/conficker.worm 13th Jan 2009 W32.stuxnet 13th July 2010, In year 2011 W32.Morto 28th Aug 2011 Internet worms are discovered.[5,6,7]

**2011:-**
Spy Eye and Zeus merged code is seen [15] New variants attack mobile phone banking information [16]

Anti-Spyware 2011, a Trojan horse that attacks windows 9x,2000,xp,Vista, and Windows 7,posing as an anti-spyware program. It actually disables security related process of anti-virus programs, while also blocking access to the Internet, which prevents updates [17]. July 13th: The Zero Access rootkit (also known as sirefef or max ++) was discovered.

September 1st : Duqu is a worm thought to be related to the stuxnet worm. The laboratory, of cryptography and system security (CrySyShab)[18] 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.[19],[20] Duqu gets its name from the prefix '~DQ" it gives to the names of files it creates.[21].

**2012:-**
- May: Flame also known as Flamer, sky Wiper, and Sky Wiper a modular computer malware that attacks computers running Microsoft Windows. Used for targeted cyber espionage in Middle Eastern countries. Its discovery was announced on 28 May 2012 by MAHER Center of Iranian National **Computer Emergency Response Team (CERT)**, Kaspersky Lab and CrySyS Lab of the Budapest University of Technology and Economics. CrySyS stated in their report that "sKyWIper is certainly the most sophisticated malware[22]

**2013**
- September: The CryptoLocker Trojan horse is discovered. CryptoLocker encrypts the files on a user's hard drive, then prompts them to pay a ransom to the developer in order to receive the decryption key. In the following months, a number of copycat ransomware Trojans are also discovered.
- December: The Gameover ZeuS Trojan is discovered. This type of virus steals one's login details on popular Web sites that involve monetary transactions. It works by detecting a login page, then proceeds to inject a malicious code into the page, keystroke logging the computer user's details.
- December: Linux.Darlloz targets the Internet of things and infects routers, security cameras, set-top boxes by exploiting a PHP vulnerability.[23][24]

**2014**
- November: The Regin Trojan horse is discovered. Regin is a dropper that is primarily spread via spoofed Web pages. Once downloaded, Regin quietly downloads extensions of itself, making it difficult to be detected via antivirus signatures. It is suspected to have been created by the United States and United Kingdom over a period of months or years, as a tool for espionage and mass surveillance.[25]

**2015**
- The BASHLITE malware is leaked leading to a massive spike in DDoS attacks.[26]
- Linux.Wifatch is revealed to the general public. It is found to attempt to secure devices from other more malicious malware.[27][28][29][30]

**2016**

- February: Ransomware Locky 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.[31]
- February: Tiny Banker Trojan (Tinba) makes headlines.[32]
- September: 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 Sept. 2016 on the Krebs on Security site which reached 620 Gbit/s.[33]

**2017**

- May: The WannaCry ransomware attack spreads globally. Exploits revealed in the NSA hacking toolkit leak of late 2016 were used to enable the propagation of the malware.[34] Shortly after the news of the infections broke online, a UK cyber security researcher in collaboration with others found and activated a "kill switch" hidden within the ransomware, effectively halting the initial wave of its global propagation.[35] The next day, researchers announced that they had found new variants of the malware without the kill switch.[36]
- June: The Petya (malware) attack spreads globally affecting Windows systems. Researchers at Symantec reveal that this ransomware uses the Eternal Blue exploit, similar to the one used in the WannaCry ransomware attack.[37][38][39]
- September: 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.[40][41]
- September: 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.[42][43].

**Survey table for Virus, Worms and Antivirus:**

| SN. NO | Year | Virus/Worms | Antivirus |
|---|---|---|---|
| 1 | 1980-1986 | | Avast , Norman Safeground, Sophos, Atari |
| 2 | 1987 | Christmas tree | McAfee,Avira |
| 3 | 1988 | | TrendMicro |
| 4 | 1990 | | Panda Security |
| 5 | 1991 | | TrustPort |
| 6 | 1992 | | F-Secure |
| 7 | 1993 | Antimare | |
| 8 | 1997 | Sharefun | Webroot,Kaspersky |
| 9 | 1998 | Antimare | |
| 10 | 1999 | Melissa | LavaSoft Security |
| 11 | 2000 | Love Letter, I Love You,Stages,NetLog | Zone Alarm Antivirus |
| 12 | 2001 | Magister,Sircam,PeachyPDF ,Nimda,klez,Gonner,Box Poison,cheese,CodeRed | Bitdefender |
| 13 | 2002 | Ladex,Opasery, Goabot | Bullguard |
| 14 | 2003 | Bibrog,Netspree,Slammer | |
| 15 | 2004 | W32/Bangle.gen W32/MyDoom@mm W32/Netsky.J@MM8th W32/sasser.worm.a Perl/Santy.worm. | |
| 16 | 2005 | W32/IRC boot.worm/MS05-039 | F-Secure |
| 17 | 2006 | W32-Nyxem.e, W32. Rontokbro.AN@m | |
| 18 | 2007 | --- | McAfee, Cyber Defender Antivirus |
| 19 | 2008 | W32/Koobface.worm | McAfee |
| 20 | 2009 | W32/conficker.worm | AVG, Bitdefender |
| 21 | 2010 | W32.stuxnet | McAfee, AVG |
| 22 | 2011 | SpyEye and Zeus,Sirefef or Max++,Duqu | Total Defense Antivirus, Zone Alarm Antivirus, Cyber Defender Antivirus,Microsoft Security Essential (MSE) |
| 23 | 2012 | Flamer,SkyWiper | Sophos |
| 24 | 2013 | CryptoLocker Trojan horse,GameoverZeuS Trojan | F-Secure, Avira |
| 25 | 2014 | Regin Trojan horse | Avast, Norton ,McAfee ,Norman |
| 26 | 2015 | BASHLITE | Total Defense Antivirus , Zone Alarm Antivirus |
| 27 | 2016 | RansomewareLocky, Tiny Banker Trojan(Tinba),Mirai | Panda Cloud, Bitdefender ,Avast, AVG |
| 28 | 2017 | WannaCryransomware,Petya,Xafecopy Trojan,Kedi RAT (remote Access trojan) | AVG, Total Defense Antivirus |
| 29 | 2018 | WannaCry ransomware, CBTLoker, Jigsaw | Vipre, Kaspersky, Norton, TrendMicro,Webroot |
| 30 | 2019 | | Bitdefender-secure |

**CONCLUSIONS:**

We have found different types of worms/Virus/Malicious Signals in the network and its behavior according to the nature of viruses/worms/ Malicious Signals we also need patches for update the anti-virus software.

**REFERENCES:-**


[1]. Shoch J.F., Hupp, J.A. The "Worm" programs early experience with a distributed computation. Communications of the ACM, ACM press New York, NY, USA, volume-25, Issue-e, 1982, PP. 172-180.

[2]. Neumann P.G. Risks to public in computers and related systems. 1990 ACM press New York, NY, USA, Volume – 15, Issue-2, 1990, PP.3-22.

[3]. Darrel M.Kienzle, Matthew C.Elder."Recent worms, A Survey and Trends". WORM 03 Proceeding of the 2003 ACM. Desktop on Rapid malcode.ACM Press New York, NY, USA,2003, PP.1-10.

[4]. Tavani H.T. Defining the boundaries of Computer crime: piracy, break-ins.and sabotage in cyberspace, ACM Press New York, NY, USA, Volume-30, Issue-3, 2000, P.3-9.

[5]. Threat Expert. http://www.threatexpert.com

[6]. McAfee Threat Library. http://www.mcafee.com/ threatintelligence/ malware/ latest. aspx.

[7]. Symantec security Response.http://www.symantec.com/security-response

[8]. Weaver N.Paxson V.stainform S.Cunningh am R.A. taxonomy of computer worms. Proceedings of the 2003 ACM workshop on Rapid malcode. ACM Press New York, NY, USA, 2003, PP.11-18.

[9]. Im G.P., Baskerville R.L. A Longitude sudy of information system threat categories the enduring problem of human error. ACM SIGMIS Database, ACM Press New York, NY, USA, Volume – 36, Issue-4, 2005, PP. 68-79.

[10]. Geer D. Malicious BOts Threaten Network Security, IEEE computer, IEEE Computer Society Washington, DC,USA, Vol.38, Issue,1,2005, PP.18-20.

[11]. Antrosio J.V., Fulp E.W. Malware Defence using Network Security Authentication, iwiq, Third IEEE International Workshop an Information Assurance (IWIA'05). IEEE Computer Society Washington, DC,USA, 2005, PP.43-54.

[12]. Sheng Y., Phoha V.V., Rovnyak S.M.A Parallel Decision Tree – Based Method for user Authentication Based on keystroke Patteruss. IEEE Transactions on systems, man, and cybernetics – Part B: CYBERNET-ICS, IEEE Computer Society Washington, DC, USA, Volume-35, Issue-4, 2005, PP.826-833.

[13]. Geeta Kumari G., Negi A.,Sastry V.N.Dynamic, Delegatio Approach for Access control in Grids, e-science, first International conference one – science and Grid Computing (e-Science'05) IEEE Computer Society Washington, DC, USA, 2005, PP.387-394.

[14]. Qiang W.,Jin H., Shix., Zou D.Joint Management of Authorization for Dynamic Virtual Organisation, cit, The fifth International conference on Computer and IT(CIT05),2005, IEEE Computer Society Washington DC, USA, 2005, PP. 375-381.

[15]. "Bastard child of SpyEye/ZeuS merger appears online" (http://www.theregister.co.uk/2011/01/25/spyeye_zeus_merger/).The Register. 2011. Retrieved April 11, 2011. "Bastard child of SpyEye/ZeuS merger appears online"5/27/2017 Timeline of computer viruses and worms Wikipedia https://en.wikipedia.org/wiki/ Timeline_of_computer_viruses_and_worms 13/14

[16]. "SpyEye mobile banking Trojan uses same tactics as ZeuS" (http://www.theregister.co.uk/2011/04/05/spyeye_mobile_trojan/). The Register. 2011. Retrieved April 11, 2011. "SpyEye mobile banking Trojan uses same tactics as ZeuS"

[17]. "XP AntiSpyware 2011 Virus Solution and Removal" (http://www.precisesecurity.com/rogue/xpantispyware2011/).Precisesecurity.com. Retrieved 20120329.

[18]. "Laboratory of Cryptography and System Security (CrySyS)" (http://www.crysys.hu/). Retrieved 4 November 2011.

[19]. "Duqu: A Stuxnetlike malware found in the wild, technical report" (http://www.crysys.hu/publications/files/bencsathPBF 11duqu.pdf) (PDF). Laboratory of Cryptography of Systems Security (CrySyS). 14 October 2011.

[22]. "sKyWIper: A Complex Malware for Targeted Attacks" (http://www.crysys.hu/skywiper/skywiper.pdf) (PDF). Budapest University of Technology and Economics. 28 May 2012. Archived (http://www.webcitation.org/682bQ4f6J) from the original on 30 May 2012. Retrieved 29 May 2012.

[23]. Goodin, Dan (20131127)."New Linux worm targets routers, cameras, "Internet of things" devices" (http://arstechnica.com/security/2013/11/ newlinuxwormtargetsrouters camerasinternetofthingsdevices/).Ars Technica. Retrieved October 24, 2016.

[24]. Sterling, Bruce (20140129)."Linux.Darlloz, the InternetofThings worm" (https://www.wired.com/2014/01/spimewat chlinuxdarllozinterne tthingsworm/).Wired. Retrieved 24 October 2016.

[25]. "Attack of Things!" (http://blog.level3.com/security/attackofthings /).Level 3 Threat Research Labs. 25 August 2016.Retrieved 6 November 2016.

[26]. "Attack of Things!" (http://blog.level3.com/security/attackofthings/). Level 3 Threat Research Labs. 25 August 2016.Retrieved 6 November 2016.
[27]. Ballano, Mario (1 Oct 2015). "Is there an Internet of Things vigilante out there?" (https://www.symantec.com/connect/blogs/there internet things vigilante out there).Symantec. Retrieved 14 November 2016.
[28]. Das, Samburaj (October 2, 2015). "Linux.Wifatch: Vigilante Hacker Infects Routers with Malware to Fight Bad Malware" (https://hacked.com/ linuxwifatchvig ilantehack erinfectsroutersmalwarefightbadmalware/).hacked.com.Retrieved 14 November 2016.
[29]. "linux.wifatch" (https://gitlab.com/rav7teif/linux.wifatch). The White Team. October 5, 2015. Retrieved 15 November 2016.
[30]. Cimpanu, Catalin (Oct 7, 2015). "Creators of the Benevolent Linux.Wifatch Malware Reveal Themselves" (http://news.softpedia.com/news /creators of the benevolent linux wifatch malware reveal themselves493938.shtml). Softpedia.Retrieved 14 November 2016.
[31]. "Ransomware: Erpresserische Schadprogramme" (https://www.bsifuerbuerger.de/ BSIFB /DE/Service/Aktuell/Informationen/ Artikel/Ransomware.html), bsifuerbu erger.de, 9 February 2016. Retrieved 10 March 2016.
[32]. http://www.massivealliance.com/2014/09/19/tinybankermalware attemptedcus tomersusbanks.
[33]. The Economist, 8 October 2016, The internet of stings (http://www. economist.com /news/scienceandtechnology/21708220 electronic tsunamicrashesd ownsolitaryjo urnalistinternet)
[34]. Wong, Julia Carrie; Solon, Olivia (20170512)."Massive ransomware cyber attack hits 74 countries around the world"(https://www. the guardian. com/technology /2017/may/12 /global cyber attack ransomware nsauknhs).The Guardian.ISSN 02613077(https://www.worldcat .org/issn/02613077).Retrieved 20170512.
[35]. Solon, Olivia (20170513)." 'Accidental hero' finds kill switch to stop spread of ransomware cyberattack"(https://www.theguardian.com/technology/2017/may/13/ accidentalherofindskillswitchtostopspreadofransomwarecyberattack).The Guardian. ISSN 02613077(https://www.worldcat.org/issn/02613077).Retrieved 20170513.
[36]. Khandelwal, Swati. "It's Not Over, WannaCry 2.0 Ransomware Just Arrived With No 'KillSwitch'" (http://thehackernews.com/2017/05/ wannacryransomwa recyberatt ack.html). The Hacker News. Retrieved 20170514.
[37] "Petya ransomware outbreak: Here's what you need to know". Retrieved 10 September 2017.
[38] "Ransom.Petya - Symantec". www.symantec.com. Retrieved 10 September2017.
[39] "Petya' Ransomware Outbreak Goes Global — Krebs on Security". krebsonsecurity.com. Retrieved 10 September 2017.
[40] "New malware steals users' money through mobile phones: Report". 10 September 2017. Retrieved 10 September 2017 – via The Economic Times.
[41] "Xafecopy Trojan, a new malware detected in India; it disguises itself as an app to steals money via mobile phones". Tech2. Retrieved 10 September 2017.
[42] "Kedi RAT can steal your information and send it through Gmail".
[43] "Beware the Kedi RAT pretending to be a Citrix file that Gmail home".