Timeline of computer viruses and worms

From Wikipedia, the free encyclopedia

This **timeline of computer viruses and worms** presents a chronology of noteworthy computer viruses, computer worms, trojan horses, similar malware, related research and events.

Contents

- 1 1949
- 2 1970–1979
- 3 1980–1989
- 4 1990–1999
- 5 2000–2009
- 6 2010 and later
- 7 See also
- 8 References
- 9 External links

1949

- John von Neumann's article on the "Theory of self-reproducing automata" is published.[1] The article is based on lectures given by von Neumann at the University of Illinois about the "Theory and Organization of Complicated Automata" in 1949.

1970–1979

1971

- The Creeper system, an experimental self-replicating program, is written by Bob Thomas at BBN Technologies.[2] 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.[3]

1974

- The Rabbit (or Wabbit) virus, more a fork bomb than a virus, is written. The Rabbit virus makes multiple copies of itself on a single computer (and was named "Rabbit" 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.[4]

1975

- April: ANIMAL is written by John Walker for the UNIVAC 1108.[5] ANIMAL asked a number of

questions of 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 structures, 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".[6]
- The novel *The Shockwave Rider* by John Brunner is published, coining the word "worm" to describe a program that propagates itself through a computer network.[7]

1980–1989

1982

- A program called Elk Cloner, written for Apple II systems, was created by Richard Skrenta. The Apple II was seen as particularly vulnerable due to the storage of its operating system on floppy disk. Elk Cloner's design combined with public ignorance about what malware was and how to protect against it led to Elk Cloner being responsible for the first large-scale computer virus outbreak in history.[8]

1983

- November: The term 'virus' is coined by Frederick Cohen in describing self-replicating computer programs. In 1984 Cohen uses the phrase "computer virus" – as suggested by his teacher Leonard Adleman – to describe the operation of such programs in terms of "infection". He defines a 'virus' as "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself." Cohen demonstrates a virus-like program on a VAX11/750 system at Lehigh University. The program could install itself in, or infect, other system objects.[9]
- A very early Trojan Horse designed for the IBM PC called ARF-ARF was downloaded from BBS sites and claimed to “Sort” the DOS Diskette Directory. This was a very desirable feature because DOS didn’t list the files in alphabetical order in 1983. Instead, the program deleted all of the files on the diskette, cleared the screen and typed ARF – ARF. ARF was a reference to the common “Abort, Retry Fail” message you would get when a PC could not boot from a diskette.[10]

1984

- August: Ken Thompson publishes his seminal paper, *Reflections on Trusting Trust*, in which he describes how he modified a C compiler so that when used to compile a specific version of the Unix operating system, it inserted a backdoor into the login command, and when used to compile itself, it inserted the backdoor insertion code, even if neither the backdoor nor the backdoor insertion code were present in the source code.[11]

1986

- January: The Brain boot sector virus is released. Brain is considered the first IBM PC compatible virus, and the program responsible for the first IBM PC compatible virus epidemic. The virus is also known as Lahore, Pakistani, Pakistani Brain, and Pakistani flu as it was created in Lahore, Pakistan by 19 year old Pakistani programmer, Basit Farooq Alvi, and his brother, Amjad Farooq Alvi.[12]

- December: Ralf Burger presented the Virdem model of programs at a meeting of the underground Chaos Computer Club in Germany. The Virdem model represented the first programs that could replicate themselves via addition of their code to executable DOS files in COM format.[13]

1987

- Appearance of the Vienna virus, which was subsequently neutralized—the first time this had happened on the IBM platform.[14]
- Appearance of Lehigh virus (discovered at its namesake university),[14] boot sector viruses such as Yale from USA, Stoned from New Zealand, Ping Pong from Italy, and appearance of first self-encrypting file virus, Cascade. Lehigh was stopped on campus before it spread to the wild, and has never been found elsewhere as a result. A subsequent infection of Cascade in the offices of IBM Belgium led to IBM responding with its own antivirus product development. Prior to this, antivirus solutions developed at IBM were intended for staff use only.
- October: The Jerusalem virus, part of the (at that time unknown) Suriv family, is detected in the city of Jerusalem. The virus destroys all executable files on infected machines upon every occurrence of Friday the 13th (except Friday 13 November 1987 making its first trigger date May 13, 1988). Jerusalem caused a worldwide epidemic in 1988.[14]
- November: The SCA virus, a boot sector virus for Amigas appears, immediately creating a pandemic virus-writer storm. A short time later, SCA releases another, considerably more destructive virus, the Byte Bandit.
- December: Christmas Tree EXEC was the first widely disruptive replicating network program, which paralyzed several international computer networks in December 1987.

1988

- March 1: The Ping-Pong virus (also called Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A or VeraCruz), an MS-DOS boot sector virus, is discovered at University of Turin in Italy.
- June: The CyberAIDS and Festering Hate Apple ProDOS viruses spreads from underground pirate BBS systems and starts infecting mainstream networks. Festering Hate was the last iteration of the CyberAIDS series extending back to 1985 and 1986. Unlike the few Apple viruses that had come before which were essentially annoying, but did no damage, the Festering Hate series of viruses was extremely destructive, spreading to all system files it could find on the host computer (hard drive, floppy, and system memory) and then destroying everything when it could no longer find any uninfected files.
- November 2: The Morris worm, created by Robert Tappan Morris, infects DEC VAX and Sun machines running BSD UNIX that are 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.

1989

- October: Ghostball, the first multipartite virus, is discovered by Friðrik Skúlason. It infects both executable .COM-files and boot sectors on MS-DOS systems. It captures certain information entered or saved by the user, with the corresponding threat to privacy, causes the loss of information stored on the computer, either specific files or data in general, affects the productivity of the computer, the network to which it’s connected or other remote sites, decrease the security level of the computer, but does not automatically spread itself.

1990–1999

1990

- Mark Washburn working on an analysis of the Vienna and Cascade viruses with Ralf Burger develops the first family of polymorphic virus: the Chameleon family. Chameleon series debuted with the release of 1260.[15][16][17]

1992

- March: The Michelangelo virus was expected to create a digital apocalypse on March 6, with millions of computers having their information wiped according to mass media hysteria surrounding the virus. Later assessments of the damage showed the aftermath to be minimal. John McAfee had been quoted by the media as saying that 5 million computers would be affected. He later said that, pressed by the interviewer to come up with a number, he had estimated a range from 5 thousand to 5 million, but the media naturally went with just the higher number.

1993

- "Leandro" or "Leandro & Kelly"[18] and "Freddy Krueger"[19] spread quickly due to popularity of BBS and shareware distribution.

1994

- April: OneHalf is a DOS-based polymorphic computer virus.

1995

- The first Macro virus, called "Concept," is created. It attacked Microsoft Word documents.[20]

1996

- "Ply" - DOS 16-bit based complicated polymorphic virus appeared with built-in permutation engine.[21]

1998

- June 2: The first version of the CIH virus appears. It is the first known virus able to erase flash ROM BIOS content.

1999

- January 20: The Happy99 worm first appeared. 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.
- March 26: The Melissa worm was released, targeting Microsoft Word and Outlook-based systems, and creating considerable network traffic.
- June 6: The ExploreZip worm, which destroys Microsoft Office documents, was first detected.
- December 30: The Kak worm is a Javascript computer worm that spread itself by exploiting a bug in Outlook Express.[22]

2000–2009

2000

- May: The ILOVEYOU worm, also known as Love Letter, or VBS, or Love Bug worm, is a computer worm purportedly created by a Filipino computer science student. Written in VBScript, it infected millions of Windows computers worldwide within a few hours of its release. It is considered to be one of the most damaging worms ever.
- June 28: The Pikachu virus is believed to be the first computer virus geared at children. It contains the character "Pikachu" from the Pokémon series, and is in the form of an e-mail titled "Pikachu Pokemon" with the message: "Pikachu is your friend." The attachment to the email has "an image of a pensive Pikachu", along with a message stating, "Between millions of people around the world I found you. Don’t forget to remember this day every time MY FRIEND." Along with the image, there is a program, written in Visual Basic 6, called "pikachupokemon.exe" that modifies the AUTOEXEC.BAT file and adds a command for removing the contents of directories C:\Windows and C:\Windows\System at computer's restart. The affected operating systems are Windows 95, Windows 98 and Windows Me.

2001

- February 11: The Anna Kournikova virus hits e-mail servers hard by sending e-mail to contacts in the Microsoft Outlook addressbook.[23] Its creator, Dutchman Jan de Wit, was sentenced to 150 hours of community service.[24]
- May 8: The Sadmind worm spreads by exploiting holes in both Sun Solaris and Microsoft IIS.
- July: The Sircam worm is released, spreading through Microsoft systems via e-mail and unprotected network shares.
- July 13: The Code Red worm attacking the Index Server ISAPI Extension in Microsoft Internet Information Services is released.
- August 4: A complete re-write of the Code Red worm, Code Red II begins aggressively spreading onto Microsoft systems, primarily in China.
- September 18: The Nimda worm is discovered and spreads through a variety of means including vulnerabilities in Microsoft Windows and backdoors left by Code Red II and Sadmind worm.
- October 26: The Klez worm is first identified. It exploits a vulnerability in Microsoft Internet Explorer and Microsoft Outlook and Outlook Express.

2002

- February 11: The Simile virus is a metamorphic computer virus written in assembly.
- Beast is a Windows-based backdoor Trojan horse, more commonly known as a RAT (Remote Administration Tool). It is capable of infecting almost all versions of Windows. Written in Delphi and released first by its author Tataye in 2002, its most current version was released October 3, 2004
- March 7: Mylife is a computer worm that spread itself by sending malicious emails to all the contacts in Microsoft Outlook.[25]
- August 30: Optix Pro is a configurable remote access tool or trojan, similar to SubSeven or BO2K.[26]

2003

- January 24: The SQL Slammer worm, aka *Sapphire worm*, *Helkern* and other names, attacks vulnerabilities in Microsoft SQL Server and MSDE becomes the fastest spreading worm of all time (measured by doubling time at the peak rate of growth),[27] crashing the Internet within 15 minutes of release.[28]

- April 2: Graybird is a trojan horse also known as Backdoor.Graybird.[29]
- June 13: ProRat is a Turkish-made Microsoft Windows based backdoor trojan horse, more commonly known as a RAT (Remote Administration Tool).[30]
- August 12: The Blaster worm, aka the *Lovesan* worm, rapidly spreads by exploiting a vulnerability in system services present on Windows computers.
- August 18: The Welchia (Nachi) worm is discovered. The worm tries to remove the blaster worm and patch Windows.
- August 19: The Sobig worm (technically the Sobig.F worm) spreads rapidly through Microsoft systems via mail and network shares.
- September 18: Swen is a computer worm written in C++.[31]
- October 24: The Sober worm is first seen on Microsoft systems and maintains its presence until 2005 with many new variants. The simultaneous attacks on network weakpoints by the Blaster and Sobig worms cause massive damage.
- November 10: Agobot is a computer worm that can spread itself by exploiting vulnerabilities on Microsoft Windows. Some of the vulnerabilities are MS03-026 and MS05-039.[32]
- November 20: Bolgimo is a computer worm that spread itself by exploiting a buffer overflow vulnerability at Microsoft Windows DCOM RPC Interface.[33]

2004

- January 18: Bagle is a mass-mailing worm affecting all versions of Microsoft Windows. There were 2 variants of Bagle worm, Bagle.A and Bagle.B. Bagle.B was discovered on February 17, 2004.
- January 23: The L10n worm (usually pronounced "lion") was a Linux worm that spread by exploiting a buffer overflow in the BIND DNS server. It was based on an earlier worm known as the Ramen worm (commonly, albeit incorrectly referred to as the Ramen Virus) which was written to target systems running versions 6.2 and 7.0 of the Red Hat Linux distribution.[*citation needed*]
- Late January: The MyDoom worm emerges, and currently holds the record for the fastest-spreading mass mailer worm.
- February 16: The Netsky worm is discovered. The worm spreads by email and by copying itself to folders on the local hard drive as well as on mapped network drives if available. Many variants of the Netsky worm appeared.
- March 19: The Witty worm is a record-breaking worm in many regards. It exploited holes in several Internet Security Systems (ISS) products. It was the fastest disclosure to worm, it was the first internet worm to carry a destructive payload and it spread rapidly using a pre-populated list of ground-zero hosts.
- May 1: The Sasser worm emerges by exploiting a vulnerability in the Microsoft Windows LSASS service and causes problems in networks, while removing MyDoom and Bagle variants, even interrupting business.
- June 15: Caribe or Cabir is a computer worm that is designed to infect mobile phones that run Symbian OS. It is the first computer worm that can infect mobile phones. It spread itself through Bluetooth. More information can be found on F-Secure[34] and Symantec.[35]
- August 16: Nuclear RAT (short for Nuclear Remote Administration Tool) is a backdoor trojan that infects Windows NT family systems (Windows 2000, Windows XP, Windows 2003).[36]
- August 20: Vundo, or the Vundo Trojan (also known as Virtumonde or Virtumondo and sometimes referred to as MS Juan) is a trojan known to cause popups and advertising for rogue antispyware programs, and sporadically other misbehaviour including performance degradation and denial of service with some websites including Google and Facebook.[37]
- October 12: Bifrost, also known as Bifrose, is a backdoor trojan which can infect Windows 95 through Vista. Bifrost uses the typical server, server builder, and client backdoor program configuration to allow a

remote attack.[38]

- December: Santy, the first known "webworm" is launched. It exploited a vulnerability in phpBB and used Google in order to find new targets. It infected around 40000 sites before Google filtered the search query used by the worm, preventing it from spreading.

2005

- August 2005: Zotob
- Late 2005: The Zlob Trojan, is a trojan horse which masquerades as a required video codec in the form of the Microsoft Windows ActiveX component. It was first detected in late 2005.[39]
- Bandook or Bandook Rat (Bandook Remote Administration Tool) is a backdoor trojan horse that infects the Windows family. It uses a server creator, a client and a server to take control over the remote computer. It uses process hijacking / kernel patching to bypass the firewall, and let the server component hijack processes and gain rights for accessing the Internet.

2006

- January 20: 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.
- February 16: discovery of the first-ever malware for Mac OS X, a low-threat trojan-horse known as OSX/Leap-A or OSX/Oompa-A, is announced.
- Late March: Brontok variant N was found in late March.[40] Brontok was a mass-email worm and the origin for the worm was from Indonesia.
- Late September: Stration or Warezov worm first discovered.

2007

- January 17: Storm Worm identified as a fast spreading email spamming threat to Microsoft systems. It begins gathering infected computers into the Storm botnet. By around June 30 it had infected 1.7 million computers, and it had compromised between 1 and 10 million computers by September.[41] Thought to have originated from Russia, it disguises itself as a news email containing a film about bogus news stories asking you to download the attachment which it claims is a film.
- July: Zeus is a trojan that targets Microsoft Windows to steal banking information by keystroke logging.

2008

- February 17: Mocmex is a trojan, which was found in a digital photo frame in February 2008. It was the first serious computer virus on a digital photo frame. The virus was traced back to a group in China.[42]
- March 3: Torpig, also known as Sinowal and Mebroot, is a Trojan horse that affects Windows, turning off anti-virus applications. It allows others to access the computer, modifies data, steals confidential information (such as user passwords and other sensitive data) and installs more malware on the victim's computer.[43]
- May 6: Rustock.C, a hitherto-rumoured spambot-type malware with advanced rootkit capabilities, was announced to have been detected on Microsoft systems and analyzed, having been in the wild and undetected since October 2007 at the very least.[44]
- July 6: Bohmini.A is a configurable remote access tool or trojan that exploits security flaws in Adobe Flash 9.0.115 with Internet Explorer 7.0 and Firefox 2.0 under Windows XP SP2.[45]
- July 31: The Koobface computer worm targets users of Facebook and MySpace. New variants constantly

appear.[46]

- November 21: Computer worm Conficker infects anywhere from 9 to 15 million Microsoft server systems running everything from Windows 2000 to the Windows 7 Beta. The French Navy,[47] UK Ministry of Defence (including Royal Navy warships and submarines),[48] Sheffield Hospital network,[49] German Bundeswehr[50] and Norwegian Police were all affected. Microsoft sets a bounty of $250,000 USD for information leading to the capture of the worm's author(s).[51] Five main variants of the Conficker worm are known and have been dubbed Conficker A, B, C, D and E. They were discovered 21 November 2008, 29 December 2008, 20 February 2009, 4 March 2009 and 7 April 2009, respectively. On December 16, 2008, Microsoft releases KB958644 [52] patching the server service vulnerability responsible for the spread of Conficker.

2009

- July 4: The July 2009 cyber attacks occur and the emergence of the W32.Dozer attack the United States and South Korea.
- July 15: Symantec discovered Daprosy Worm. Said trojan worm is intended to steal online-game passwords in internet cafes. It could, in fact, intercept all keystrokes and send them to its author which makes it potentially a very dangerous worm to infect B2B (business-to-business) systems.

2010 and later

2010

- January: A botnet called Waledac sent spam emails. In February 2010, an international group of security researchers and Microsoft took Waledac down.[53]
- February 18: Microsoft announced that a BSoD problem on some Windows machines which was triggered by a batch of Patch Tuesday updates was caused by the Alureon trojan.[54]
- June 17: Stuxnet, a Windows trojan, was detected.[55] It is the first worm to attack SCADA systems.[56] There are suggestions that it was designed to target Iranian nuclear facilities.[57] It uses a valid certificate from Realtek.[58]
- September 9: The virus, called "here you have" or "VBMania", is a simple trojan horse that arrives in the inbox with the odd-but-suggestive subject line "here you have". The body reads "This is The Document I told you about, you can find it Here" or "This is The Free Download Sex Movies, you can find it Here".
- September 15: The virus called Kenzero is a virus that spreads online from Peer to peer (P2P) sites taking browsing history.[59]

2011

- SpyEye and Zeus merged code is seen.[60] New variants attack mobile phone banking information.[61]
- Anti-Spyware 2011, a trojan horse which 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.[62]
- Summer 2011: 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.[63] A detailed overview of how the worm works—along with the password dictionary Morto uses—was done

by Imperva.[64]
- July 13: the ZeroAccess rootkit (also known as Sirefef or max++) was discovered.
- September 1: Duqu is a worm thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab)[65] 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.[66][67] Duqu gets its name from the prefix "~DQ" it gives to the names of files it creates.[68]

2012

- May: Flame also known as Flamer, sKyWIper, and Skywiper is modular computer malware discovered in 2012 that attacks computers running Microsoft Windows. The program is being 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 we encountered during our practice; arguably, it is the most complex malware ever found".[69]
- August 16: Shamoon is a computer virus designed to target computers running Microsoft Windows in the energy sector. Symantec, Kaspersky Lab, and Seculert announced its discovery on August 16, 2012.
- September 20: NGRBot 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 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.[70][71]

2013

- April: 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, making it the first true ransomware.

See also

- Helpful worm
- Multipartite virus
- Timeline of computer security hacker history

References

1. ^ von Neumann, John (1966). Arthur W. Burks, ed. *Theory of self-reproducing automata* (http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf). University of Illinois Press. Retrieved June 12, 2010.
2. ^ Chen, Thomas; Robert, Jean-Marc (2004). "The Evolution of Viruses and Worms" (http://vx.netlux.org/lib/atc01.html). Retrieved 2009-02-16.
3. ^ Russell, Deborah; Gangemi, G T (1991). *Computer Security Basics* (http://books.google.com/?id=BtB1aBmLuLEC&printsec=frontcover). O'Reilly. p. 86. ISBN 0-937175-71-4.
4. ^ "The very first viruses: Creeper, Wabbit and Brain" (http://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/), Daniel Snyder, InfoCarnivore, May 30, 2010

5. ^ "ANIMAL Source Code" (http://www.fourmilab.ch/documents/univac/animalsrc.html). Fourmilab.ch. 1996-08-13. Retrieved 2012-03-29.
6. ^ "The Animal Episode" (http://www.fourmilab.ch/documents/univac/animal.html). Fourmilab.ch. Retrieved 2012-03-29.
7. ^ Craig E. Engler (1997). "The Shockwave Rider" (http://web.archive.org/web/20080703121956/http://www.scifi.com/sfw/issue48/classic.html). *Classic Sci-Fi Reviews*. Archived from the original (http://www.scifi.com/sfw/issue48/classic.html) on 2008-07-03. Retrieved 2008-07-28.
8. ^ "First virus hatched as a practical joke" (http://www.smh.com.au/articles/2007/09/01/1188671795625.html?page=fullpage#contentSwap2), *Sydney Morning Herald* (AP), 3 September 2007. Retrieved 9 September 2013.
9. ^ "Fred Cohen 1984 "Computer Viruses – Theory and Experiments" " (http://www.eecs.umich.edu/%7Eaprakash/eecs588/handouts/cohen-viruses.html). Eecs.umich.edu. 1983-11-03. Retrieved 2012-03-29.
10. ^ "The Arf-Arf Virus" (http://www.bloggers.nl/nalisesre/916130/The+Arf-arf+Virus+Arrived+In+1983+And+The+Trojan+Horse+Wiped+Out+The+Computers+Directory+By+Offering+To+Sort+It+Into+Alphabetical+Order!.html), Eric Peters, Eric's blog, 5 May 2013. Retrieved 9 September 2013.
11. ^ Communication of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763.
12. ^ Leyden, John (January 19, 2006). "PC virus celebrates 20th birthday" (http://www.theregister.co.uk/2006/01/19/pc_virus_at_20/). *The Register*. Retrieved March 21, 2011.
13. ^ *The Art of Computer Virus Research and Defense* (http://books.google.com/books?id=XE-ddYF6uhYC&pg=PT204), Peter Szor, Symantec Press / Addison-Wesley Professional, 2005, ISBN 978-0-321-30454-4
14. ^ ***a b c*** "Computer Virus!" (http://uanr.com/articles/virus.html), Rob Wentworth, Reprinted from *The Digital Viking*, Twin Cities PC User Group, July 1996. Retrieved 9 September 2013.
15. ^ "Virus.DOS.Chameleon.1260 - Securelist" (http://www.viruslist.com/en/viruses/encyclopedia?virusid=2008). Viruslist.com. Retrieved 2010-07-10.
16. ^ "V2PX" (http://vil.nai.com/vil/content/v_98074.htm). Vil.nai.com. Retrieved 2010-07-10.
17. ^ "What we detect - Securelist" (http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311162). Viruslist.com. Retrieved 2010-07-10.
18. ^ "Leandro" (http://about-threats.trendmicro.com/us//archive/malware/LEANDRO), *Threat Encyclopedia*, Trend Micro, 9 March 2000. Retrieved 9 September 2013.
19. ^ "Freddy Virus" (http://wiw.org/~meta/vsum/view.php?vir=529), Virus Information Summary List, December 1992. Retrieved 9 September 2013.
20. ^ "Glossary - Securelist" (http://www.viruslist.com/en/glossary?glossid=189267795). Viruslist.com. Retrieved 2010-07-10.
21. ^ "Ply" (http://virus.wikia.com/wiki/Ply), Virus Information, Wikia, 27 June 2010. Retrieved 9 September 2013.
22. ^ "Wscript.KakWorm" (http://www.symantec.com/security_response/writeup.jsp?docid=2000-121908-3951-99). Symantec. Retrieved 2012-03-29.
23. ^ "Kournikova computer virus hits hard" (http://news.bbc.co.uk/2/hi/science/nature/1167453.stm). *BBC News*. February 13, 2001. Retrieved April 9, 2010.
24. ^ Evers, Joris (May 3, 2002). "Kournikova virus maker appeals sentence" (http://www.computerworld.com/s/article/70752/Kournikova_virus_maker_appeals_sentence_). Retrieved 20 November 2010.
25. ^ "MyLife Worm" (http://antivirus.about.com/library/weekly/aa030802a.htm). Antivirus.about.com. 2002-03-07. Retrieved 2012-03-29.
26. ^ Sevcenco, Serghei (August 30, 2002). "Security Updates: Backdoor.OptixPro.12" (http://securityresponse1.symantec.com/sarc/sarc.nsf/html/backdoor.optixpro.12.html/). Symantec. Retrieved 2009-03-01.
27. ^ "The Spread of the Sapphire/Slammer Worm" (http://www.caida.org/publications/papers/2003/sapphire/sapphire.html). Retrieved 2012-12-14.
28. ^ "Slammed!" (http://www.wired.com/wired/archive/11.07/slammer.html). July 2003. Retrieved 2012-12-14.
29. ^ Sevcenco, Serghei (February 10, 2006). "Symantec Security Response: Backdoor.Graybird" (http://securityresponse1.symantec.com/sarc/sarc.nsf/html/backdoor.graybird.html). Symantec. Retrieved 2009-03-01.
30. ^ "Backdoor.Prorat" (http://www.symantec.com/security_response/writeup.jsp?docid=2003-061315-4216-99). Symantec. February 13, 2007. Retrieved 2009-03-01.
31. ^ "Threat Description: Worm:W32/Swen" (http://www.f-secure.com/v-descs/swen.shtml). F-secure.com. Retrieved 2012-03-29.

32. ^ "Backdoor.Win32.Agobot.gen" (http://www.securelist.com/en/descriptions/old61021). Securelist. Retrieved 2012-03-29.
33. ^ "W32.Bolgi.Worm" (http://www.symantec.com/security_response/writeup.jsp?docid=2003-112019-2425-99). Symantec. Retrieved 2012-03-29.
34. ^ "Threat Description:Bluetooth-Worm:SymbOS/Cabir" (http://www.f-secure.com/v-descs/cabir.shtml). F-secure.com. Retrieved 2012-03-29.
35. ^ "SymbOS.Cabir" (http://www.symantec.com/security_response/writeup.jsp?docid=2004-061419-4412-99). Symantec. Retrieved 2012-03-29.
36. ^ "Spyware Detail Nuclear RAT 1.0b1" (http://www.ca.com/securityadvisor/pest/pest.aspx?id=453078396). Computer Associates. August 16, 2004. Retrieved 2009-03-01.
37. ^ "Vundo" (http://vil.nai.com/vil/content/v_127690.htm). McAfee. Retrieved 2009-03-01.
38. ^ "Backdoor.Bifrose" (http://www.symantec.com/security_response/writeup.jsp?docid=2004-101214-5358-99). Symantec, Inc. October 12, 2004. Retrieved 2009-02-28.
39. ^ "The ZLOB Show: Trojan Poses as Fake Video Codec, Loads More Threats" (http://www.trendmicro.com/vinfo/secadvisories/default6.asp?VNAME=The+ZLOB+Show%3A+Trojan+poses+as+fake+video+codec%2C+loads+more+threats). Trend Micro. Retrieved 2009-02-28.
40. ^ "Threat Description: Email-Worm:W32/Brontok.N" (http://www.f-secure.com/v-descs/brontok_n.shtml). F-secure.com. Retrieved 2012-03-29.
41. ^ Peter Gutmann (31 August 2007). "World's most powerful supercomputer goes online" (http://seclists.org/fulldisclosure/2007/Aug/0520.html). [[Full Disclosure (mailing list)|]]. Retrieved 2007-11-04.
42. ^ Gage, Deborah (February 17, 2005). "Chinese PC virus may have hidden agenda" (http://www.seattlepi.com/business/351670_picframevirus18.html). SeatlePI. Retrieved 2009-03-01.
43. ^ Kimmo (March 3, 2008). "MBR Rootkit, A New Breed of" (http://www.f-secure.com/weblog/archives/00001393.html). F-Secure. Retrieved 2009-03-01.
44. ^ "Win32.Ntldrbot (aka Rustock)" (http://www.pr.com/press-release/84130). Dr. Web Ltd. Retrieved 2009-03-01.
45. ^ "Virus Total" (http://www.virustotal.com/analisis/a5d8b3ba9226285dd14619fd8faf12a7). virustotal.com. July 8, 2008. Retrieved 2009-03-01.
46. ^ "Koobface malware makes a comeback" (http://news.cnet.com/8301-1009_3-20002112-83.html?). cnet.com. April 9, 2010. Retrieved 2009-04-13.
47. ^ Willsher, Kim (2009-02-07). *French fighter planes grounded by computer virus* (http://telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html). London: The Daily Telegraph. Retrieved 2009-04-01.
48. ^ Williams, Chris (2009-01-20). *MoD networks still malware-plagued after two weeks* (http://theregister.co.uk/2009/01/20/mod_malware_still_going_strong). The Register. Retrieved 2009-01-20.
49. ^ Williams, Chris (2009-01-20). *Conficker seizes city's hospital network* (http://theregister.co.uk/2009/01/20/sheffield_conficker). The Register. Retrieved 2009-01-20.
50. ^ *Conficker-Wurm infiziert hunderte Bundeswehr-Rechner* (http://www.pc-professionell.de/news/2009/02/16/conficker_wurm_infiziert_hunderte_bundeswehr_rechner) (in German). PC Professionell. 2009-02-16. Retrieved 2009-04-01.
51. ^ Neild, Barry (2009-02-13). "$250K Microsoft bounty to catch worm creator" (http://www.cnn.com/2009/TECH/ptech/02/13/virus.downadup/index.html). CNN. Retrieved 2009-03-29.
52. ^ "MS08-067: Vulnerability in Server service could allow remote code execution" (http://support.microsoft.com/kb/958644). Microsoft Corporation.
53. ^ "Waledac Takedown Successful" (http://honeyblog.org/archives/52-Waledac-Takedown-Successful.html). honeyblog.org. February 25, 2010. Retrieved 16 November 2012.
54. ^ "Alureon trojan caused Windows 7 BSoD" (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fAlureon). microsoft.com. February 18, 2010. Retrieved 2010-02-18.
55. ^ "VirusBlokAda News" (http://anti-virus.by/en/tempo.shtml). Anti-virus.by. Retrieved 2012-03-29.
56. ^ Gregg Keizer (16 September 2010). "Is Stuxnet the 'best' malware ever?" (http://www.infoworld.com/print/137598). InfoWorld. Retrieved 16 September 2010.
57. ^ Stuxnet virus: worm 'could be aimed at high-profile Iranian targets' (http://www.telegraph.co.uk/technology/news/8021102/Stuxnet-virus-worm-could-be-aimed-at-high-profile-Iranian-targets.html), Telegraph, 23 Sep 2010
58. ^ "Possible New Rootkit Has Drivers Signed by Realtek" (http://threatpost.com/possible-new-rootkit-has-drivers-signed-realtek-071510). Kaspersky Labs. 15 July 2010.

59. ^ Harvison, Josh (September 27, 2010). "Blackmail virus infects computers, holds information ransom" (http://www.kait8.com/Global/story.asp?S=13220447). kait8.com. Retrieved 20 November 2010.
60. ^ "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"
61. ^ "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"
62. ^ "XP AntiSpyware 2011 - Virus Solution and Removal" (http://www.precisesecurity.com/rogue/xp-anti-spyware-2011/). Precisesecurity.com. Retrieved 2012-03-29.
63. ^ "Morto Worm Spreads to Weak Systems" (http://blogs.appriver.com/blog/digital-degenerate-2/morto-worm-spreads-to-weak-systems). *blogs.appriver.com*. 2011.
64. ^ "Morto Post Mortem: Dissecting a Worm" (http://blog.imperva.com/2011/09/morto-post-mortem-a-worm-deep-dive.html). *blog.imperva.com*. 2011.
65. ^ "Laboratory of Cryptography and System Security (CrySyS)" (http://www.crysys.hu/). Retrieved 4 November 2011.
66. ^ "Duqu: A Stuxnet-like malware found in the wild, technical report" (http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf). Laboratory of Cryptography of Systems Security (CrySyS). 14 October 2011.
67. ^ "Statement on Duqu's initial analysis" (http://www.crysys.hu/in-the-press.html). Laboratory of Cryptography of Systems Security (CrySyS). 21 October 2011. Retrieved 25 October 2011.
68. ^ "W32.Duqu – The precursor to the next Stuxnet (Version 1.4)" (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf). Symantec. 23 November 2011. Retrieved 30 December 2011.
69. ^ "sKyWIper: A Complex Malware for Targeted Attacks" (http://www.crysys.hu/skywiper/skywiper.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.
70. ^ "NGRBot" (http://www.enigmasoftware.com/ngrbot-removal/), Enigma Software Group, 15 October 2012. Retrieved 9 September 2013.
71. ^ "Dissecting the NGR bot framework: IRC botnets die hard" (http://www.virusbtn.com/virusbulletin/archive/2012/01/vb201201-NGR-botnet), Aditya K. Sood and Richard J. Enbody, Michigan State University, USA, and Rohit Bansal, SecNiche Security, USA, with Helen Martin1 (ed.), January 2012. Retrieved 9 September 2013. (subscription required)

External links

- Snopes (http://www.snopes.com/computer/virus/) — Compilation of viruses, worms, and trojan horses.
- A short history of hacks, worms and cyberterror (http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Government&articleId=9131924&taxonomyId=13&pageNumber=1) by Mari Keefe, Computerworld, April 2009

Retrieved from "http://en.wikipedia.org/w/index.php?title=Timeline_of_computer_viruses_and_worms&oldid=598413543"

Categories: Computing timelines | Malware | Computer security exploits | Trojan horses

- This page was last modified on 6 March 2014 at 16:04.