* In computing a worm is defined as “a program that duplicates itself many times in a network and prevents its destruction. It often carries a logic bomb or virus”
* A subset of viruses
* Destructive
  + The Morris Worm released in 1988 is credited as the first Internet worm. It was created by Robert Tappan Morris to “demonstrate the inadequacies of current security measures on computer networks[102].” Robert Morris was a graduate student at Cornell University, however he released the worm at MIT to hide its origin. The worm exploited a number of vulnerabilities in the computer systems that led to the worm infecting many universities and government departments. It exploited a bug in the UNIX sendmail protocol, the finger protocol, trusted hosts, and simple passwords[102].
  + To prevent multiple instances of the worm slowing down a machine, Robert Morris had the worm check if another copy was on the machine already. This would have made the worm difficult to detect but simple to defeat. A single instance would not take up much space or resources so it may not be noticed, however once it was, simply telling the system to respond “yes” when asked if the system had the worm would have prevented it from spreading further. To counteract this Robert Morris had the worm duplicate it on every seventh “yes” it received[102]. This meant that on any network with more than seven computers, some of them would receive multiple copies of the worm, that would each continue asking the other computers on the network. This created a spiral that lead to the worm multiplying until the system crashed.
  + Thankfully the Morris Worm carried no hostile payload. It only took up computing power and memory. The worm did not persist through shutdown, so removal was easy, the difficult part was preventing reinfection. With numerous infection vectors there was no easy way to patch all the system’s vulnerabilities, so even if a machine was cleaned, it could be reinfected[102]. Because of this the Internet had to be partitioned for several days as each local network removed the worm from their individual computers.
  + The worm is estimated to have infected 6000 computers and it is estimated to have cost anywhere from $200 to $53,000 for each site affected[102]. However, this number is extremely uncertain because according to Paul Graham, “I was there when it [the estimated 6000 computers] was cooked up, and this was the recipe: someone guessed that there were about 60,000 computers attached to the Internet, and that the worm might have infected ten percent of them[104].”
    - UNIX
    - Notable info
      * MIT release [102]
      * Demo bad security [102]
    - Time, creator,
      * Nov 2, 1988
      * Robert Tappan Morris
    - Payload
      * Killed on shutdown
      * Ask every computer it could
    - Damage
      * Computers, recovery
      * 6000 computers [105]
      * 200-53,000 per computer [102]
    - Exploits [102](finger)
      * Send mail bug
      * finger demon
      * Trusted hosts
      * Password cracker
    - Fun shit[102]
      * 1/7 reinfection
    - How caught
  + The ILOVEYOU email worm of May 2000 was the fastest spreading email worm to date. It affected millions of windows computers from Windows 95 to Windows M[105]E. It was created by Reonel Ramones and Onel de Guzman out of the Philippines[105].
  + This worm was harmful to the host systems. It overwrote many files with copies of itself, and some versions installed a trojan for password theft[106]. The worm affected billions of computers, including the Pentagon, CIA, and British Parliament. It is estimated to have cost $15 billion in damage[107].
  + The worm did not use any technological vulnerabilities, instead it relied on social engineering. The worm would send an email to every contact in the infected computer’s Windows Adress Book titled “ILOVEYOU” and it relied on the recipient of the email opening up an included "LOVE-LETTER-FOR-YOU.txt.vbs" that, thanks to Outlook’s default settings, appeared as either "LOVE-LETTER-FOR-YOU.txt” or "LOVE-LETTER-FOR-YOU”[107]. When the email recipient opened the file it would launch the Visual Basic Script that altered the Windows Registry data. This would add itself to startup so that it could run even after a reboot.
  + Because the worm was written in Visual Basic Script, anyone who received the email could view and edit the source, leading to many variations in the worm[106]
    - Windows 95,98,NT,2000,ME
    - Notable info
      * Largest Email worm seen then??
    - Time, creator,
      * May 2000
      * Reonel Ramones and Onel de Guzman[105]
    - Payload
      * Overwrite many files[106]
      * Password-stealing trojan[106]
    - Damage
      * Computers, recovery
      * $15 billion [107]
      * Pentagon, CIA, British Parliament
    - Exploits
      * Social engineering
      * Email
        + Hidden extensions
      * Emailed from Windows address book
      * Microsoft Outlook weaknesses
    - Fun shit
      * VBS can be modified
        + 25 variations
    - How caught
      * ISP pinpointed, folowed to them[105]
  + Code Red jul2001
    - Microsoft IIS Server
    - Notable info
    - Time, creator,
      * July 2001
      * Unknown creator
    - Payload[108]
      * Day 1-19 Random search for more computers
      * Day 20-27 DOS set IP
      * Day 28 sleep
    - Damage
      * Computers, recovery
      * 250,000[108]
    - Exploits
      * Buffer overflow[108]
    - Fun shit
      * Named after what discoverer was drinking[109]
    - How caught
* Good????
* Some worms have been created for reasons other than causing damage to the systems they infect, however many security experts still consider them harmful overall. These are known as anti-worm
  + Code Green
    - Notable info
      * Created to combat code red
    - Time, creator,
      * Herbert HexXer[110]
      * 2001
    - Payload
      * Downloads microsoft patch[111]
    - Damage
      * Computers, recovery
    - Exploits
      * Same as code red
    - Fun shit
      * Heavily discouraged
    - How caught
  + Welchia/Nachi 2003
    - Win XP
    - Notable info
      * Created to fix Blaster worm
    - Time, creator,
    - Payload
      * Deletes blaster
      * Download security patches from microsoft
    - Damage
      * Computers, recovery [112]
    - Exploits [112]
      * Microsoft remote procedure call
      * buffer overflow
    - Fun shit
    - How caught
* XSS Worms
* [1] <http://www.dictionary.com/browse/worm?s=t>
* [2] <http://www.loundy.com/CASES/US_v_Morris2.html>
* [3]<http://www.foo.be/docs-free/morris-worm/worm/>
* [4]<http://www.paulgraham.com/submarine.html#f4n>
* [5]<https://web.archive.org/web/20080206114348/http://www.acpf.org/WC8th/AgendaItem2/I2%20Pp%20Gana%2CPhillipine.html>
* [6]<https://www.symantec.com/security_response/writeup.jsp?docid=2000-121815-2258-99>
* [7]<https://web.archive.org/web/20111027131918/http://tech.ca.msn.com/photogallery.aspx?cp-documentid=27611570&page=1>
* [8]<https://www.cert.org/historical/advisories/CA-2001-19.cfm>
* [9]<https://web.archive.org/web/20110722192419/http://www.eeye.com/Resources/Security-Center/Research/Security-Advisories/AL20010717>
* [10]<https://www.geek.com/news/code-green-kills-code-red-547117/>
* [11]<https://www.theregister.co.uk/2001/09/05/code_red_busting_code_gets/>
* [12]<http://www.internetnews.com/ent-news/article.php/3065761/Friendly+Welchia+Worm+Wreaking+Havoc.htm>