Computer worms are a self-replicating form of malware and often contain a malicious payload[1]. The payload is what the worm does after installation, it can range from allowing a backdoor into the infected machine, to keyloggers, or complete system takeover. Often worms will target vulnerabilities in out-of-date software or rely on social engineering to install themselves. Preventing them involves both keeping your systems up-to-date, using antivirus software, and being conscious of anything downloaded onto a system[1].

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[2].” 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[2].

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[2]. 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[2]. 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[4].”

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[5]E. It was created by Reonel Ramones and Onel de Guzman out of the Philippines[5].

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[6]. The worm affected billions of computers, including the Pentagon, CIA, and British Parliament. It is estimated to have cost $15 billion in damage[7].

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 Address 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”[7]. 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[6]

Code Red is a computer worm that reached it’s peak infections in July of 2001. It was named that by Ryan Permeh and Marc Maiffret because "Code Red Mountain Dew was the only thing that kept us awake while we disassembled this exploit [9].” if affected Microsoft IIS Servers that had not received a recent update. The creator of the worm is unknown.

The worm replaced affected webpages with the text "Hacked by Chinese” and had a cycling payload. Based on the day of the month it would perform different actions. On days 1 through 19 it would search random IP addresses for more computers to infect. On days 20 through 27 it would DOS a set series of IP addresses, including the White House. Finally, on day 28 the worm would sleep[8]. Because the worm used a static seed for the IP address generation each instance of the worm would check the same list of IP addresses, and each would infect the susceptible machines, leading to many instances per infected machine[9].

Code Red used a buffer overflow attack on vulnerable servers. It sent a long series of “N” characters followed by the actual payload. The worm only existed in RAM and rebooting removed it, however if the server was not patched, it was likely to be reinfected[9].

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 usually known as anti-worms. Many of these worms are created to study the spread of worms by researches, usually using cross site scripting. It allows researchers to observe how worms are spread without causing harm to the host systems. Other anti-worms are created to prevent or to cure infection from other worms.

Code Green is an anti-worm that was created to combat Code Red. It was created in 2001 by someone using the name Herbert HexXer[10]. The worm used the same exploit as Code Red and Code Red 2, a variation. After overloading the buffer, the worm would download the latest patch from Microsoft’s servers and install it. After installing the patch, the worm would find and remove Code Red from infected machines. It would then attempt to spread to other infected machines[10].

It was heavily criticized by security experts for a number of reasons. Part of the installation required a reboot of the host machine, and this could cause loss of data. The update procedure was also not always successful and had a chance to crash the hosts, causing more damage than it fixed [11]. The worm also occupied computing time and bandwidth on infected machines, and could slow down the network[10].

Computer worms are only one form of virus that can have widespread impacts costing millions or billions of dollars in both repair and prevention. They can exploit many different protocols and have wide impacts spanning normal users, businesses, and governments.

**Works Cited**

[1] <http://www.bbc.co.uk/webwise/guides/internet-worms>

[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>