MyDoom:

MyDoom was a computer worm that targeted windows computers, and as of 2024, is the fastest spreading email worm ever. It was primarily spread through emails and these emails contained an attachment that resends the worm to email addresses found in the victim’s local files if the attachment is executed. Additionally, the worm can also copy itself to the shared folder of a peer-to-peer file sharing application called Kazaa as an additional attack vector. MyDoom had two variations. MyDoom.A had two payloads. The first was a backdoor to a specific port which alled remote access of the PC. The second was designed to launch a DDOS attack on a specific company at a coordinated time. The second version, MyDoom.B, in addition to the original payloads it also carried attempted to block access to Microsoft websites and popular online antivirus sites.

SoBig

SoBig, similar to MyDoom, was a computer worm that spread primarily through email attachments. There were six variants of SoBig, A through F, and at the time of its release, SoBig.F was the fastest growing computer worm on record. It is still in second place, having been topped by MyDoom a year later. When the attachment to the email is opened, SoBig replicates itself by searching for specific file extensions and scrapping any email addresses that they contain. The final version, SoBig.F, also contacted multiple IP addresses to download additional data to the victim device, though it was never discovered what the purpose of this was. One implication of this worm was that companies pushed harder for employees to only use their work computers for work activities, attempting to reduce the risk of exposure from personal activities.

Stuxnet

Stuxnet was a virus that was designed to specifically target Siemens supervisory control and data acquisition (SCADA) systems which were configured for specific industrial applications. Stuxnet spread by utilizing four separate zero-day vulnerabilities. It spreads initially via USB drives and then via peer-to-peer remote procedure calls. It also had the ability to rootkit both user mode and kernel mode in Windows and its device drivers were digitally signed using stolen private keys. Stuxnet could also be updated via websites located in Denmark and Malaysia. Once activated, Stuxnet operated as a man-in-the-middle, modifying the information passed between the SCADA controllers and Siemens Step 7 control software. This allowed the virus to subtly and invisibly alter the operations of the centrifuges, causing increased wear and eventual failure of the devices.

BredoLab

Bredolab was a Russian botnet which was mostly focused on email spam. Much like the computer worms discussed above, Bredolab mostly spread via malicious email attachments which executed on opening. Bredolab additionally utilized drive-by-downloads as an additional attack vector. Once infected by the virus, the victim machine became part of the controlled botnet. Interestingly, the services of this botnet could be rented out to third parties, with some estimating that the botnet owner was bringing in $139,000 in revenue per month. These third parties mostly utilized the botnet for spreading email spam, but it was also used to spread other malware and scareware, among other things.