TOP 5 MOST DANGEROUS COMPUTER VIRUSES EVER

By Gaidenraih Evald

SQL Slammer

Code Red

Sobig F

ILOVEYOU

My Doom

SQL SLAMMER

SQL Slammer, a standalone malicious program also known as "Sapphire" appeared at the starting of the year 2003 and was the first fileless worm which rapidly infected more than 75000 vulnerable hosts within10 minutes on 25thJanuary. Through a classic denial of service attack, it dramatically slowed down global internet traffic and brought down South Korea's online capacity on knees for 12 hours. Sapphire mainly targeted on the servers by generating random IP addresses and discharging the worm to those IP addresses. The abrupt release of infected network packets had a huge impact on the significant services provided by Bank of America's ATMs, Seattle's 911 emergency response systems and Continental airlines. All in all, the worm caused between $950 million and $1.2 billion in lost productivity which is not much compared to what would have happened if it erupted on a week day and not on a Saturday.

CODE RED

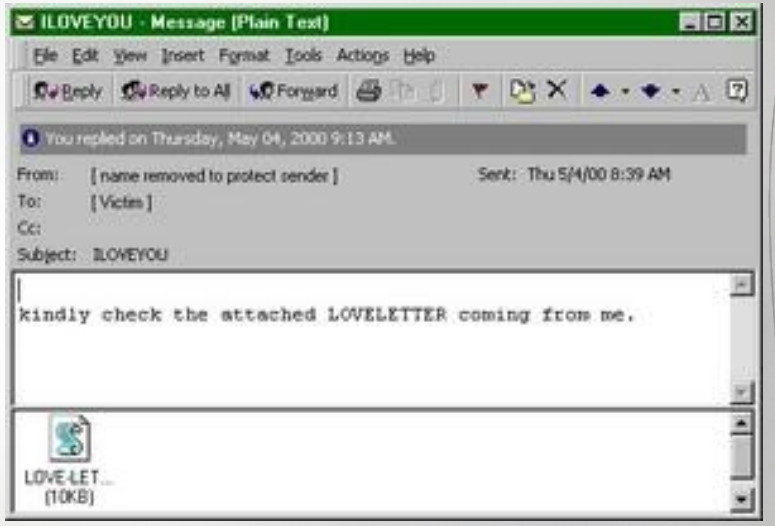
In the summer 2001, a computer worm most commonly referred to as "Code Red" was unleashed on the network servers on July 13. It was a very sneaky virus which took advantage of a flaw in Microsoft Internet Information Server. This virus was for the first time detected by two of the eEye Digital Security employees and at the time when they found out about the virus, they were drinking Code Red Mountain Dew; hence the name "Code Red." The interesting thing about this deadly virus is, it did not require you to open an e-mail attachment or run a file; it simply needed an active internet connection with which it defaces the webpage you open and display a text string "Hacked by Chinese!" In less than a week "Code Red" brought down more than 400,000 servers including the White House web server. It's estimated that the total damage was of approximately $2.6 billion dollars with as many as one million computers hit by the virus.

SOBIG F

August 2003 turned out to be the miserable month for corporate and domestic computer operators around the world as the sixth and most destructive deviant of Sobig series hit the internet. Sobig F infected host computers by fooling the users that the corrupt e-mail they received is from a legitimate source. If the user opens the attachment it exposes a security hole in the system allowing the intruder to send messages via the trapped user's e-mail address. Within 24 hours, Sobig F set a record of replicating more than one million copies of itself which later was broken by yet another mass mailer worm – My Doom. However, Sobig F caused an extensive damage of $3 billion – $4 billion leaving infections in over 2 million PCs worldwide.

ILOVEYOU

Back in 2000, one of the trickiest computer malware ever was detected on May 4 in Philippines. Around 10% of the internet users committed a huge mistake by going on the name of this hazardous worm. The virus played on a radical human emotion of the need to be loved because of which it became a global pandemic in only one night. The bug was transmitted via e-mail having a subject line "ILOVEYOU" – a notion appealing to many of us with an attached file to it which reads as – Love-Letter-For-You.TXT.vbs. As soon as the file was opened, the virus took the liberty of e-mailing itself to the first 50 contacts present in the Windows address book and also infected the multimedia files saved in the system causing damages that amounted to $5.5 billion.



MY DOOM

My Doom explored its way to the malware world on 26th January 2004 and sent a shockwave around the world as it scattered exponentially via e-mail with random senders' addresses and subject lines. My Doom also known as "Novarg" is reported to be the most dangerous virus ever released, breaking the previous record set by the Sobig F worm. My Doom swiftly infected some two million computers and instigated a huge denial of service attack which smashed the cyber world for sometime. It transmitted itself in a particularly deceitful manner through e-mail as what receiver would first reckon to be a bounced error message as it reads "Mail Transaction Failed." But, as soon as the message is clicked upon, the attachment is executed and the worm is transferred to e-mail addresses found in user's address book. The damage caused by this fastest-spreading mass mailer worm was a whopping $38 billion.