A BRIEF HISTORY OF MALWARE

Since the Brain virus first hit in 1986, worms and trojans have continued to attack and infect our devices. But of all the threats faced by users, each year can be defined by one significant virus.

1986 — PAKISTANI BRAIN

First virus for the IBM PC platform and the first to use stealth mechanisms. Pakistani Brain infected the boot sector of floppy disks, spreading globally in a matter of weeks.

1987 — STONED

Early boot sector virus initially propagated across New Zealand and Australia. Infected computers would display pro-drug slogans on start-up, including "Your PC is now Stoned" and "Leagalise Marijuana". The Stoned virus had many variants and remained very common in the early 1990s.

1988 — MORRIS WORM

Developed by Robert Tappan Morris Jr., son of a former NCSC scientist. Often cited as the first worm, the virus spread across thousands or perhaps tens of thousands of minicomputers and workstations running VMS, BSD and SunOS.

1989 — DISK KILLER

One of the earliest destructive viruses, this boot sector infector would slowly corrupt disks. It's sometimes referred to as the Computer Ogre, which is the message that would flash on the screen of infected PCs.

1990 — WHALE

A pioneer in anti-debugging technology, though as viruses go, it was grotesquely bloated and awfully inefficient. One researcher at the time described Whale's main replication method as "anti virus researchers sending specimens to each other." Unfortunately, malware authors have learned a lot since then.

1991 — MICHELANGELO

Most notable for the media firestorm leading up to its March 6 trigger date, this variant of the Stoned virus infected the boot sector on floppy diskettes and MBR on hard disk drives. Spending most of its time dormant, infected computers could go years without detection if not booted on March 6.

1992 — TRIDENTS POLYMORPHIC ENGINE (TPE)

A polymorphic engine can transform a program to a new version using different code but keeping the original functionality. This can be used by viruses in an attempt to avoid detection.

1993 — DARK ANGEL'S MULTIPLE ENCRYPTOR (DAME)

Another polymorphic engine, published by a Canadian virus group Phalcon/SKISM. It was distributed as commented source code.

1994 — ONEHALF

OneHalf can be called the first Ransomware virus except that there was no ransom amount or deactivation code. It was encrypting the first series of sectors on the harddisk. If you would use FDISK / MBR, the infected MBR would be replaced with a clean one and the system would become unbootable.

1995 — WM/CONCEPT

The first Macro Virus to spread through Microsoft Word – WM/Concept caused many problems. Microsoft did not initially release the format of the Office Files (OLE2) and the streams (WordDocument). At an EICAR Conference in Linz, CARO members sat down to reverse engineer the formats together to make a proper detection and remediation.

1996 — LAROUX

Although not the first spreadsheet virus, WM/Laroux was the first Excel macro virus seen in the wild. The actual virus code consists of two macros, "Auto_Open" and "Check_Files", hidden in a datasheet named "laroux".

1997 — AOL TROJANS

1997 could be said to have seen the real beginning of the trend away from self-propagating malware and towards Trojans. The craze for stealing AOL passwords took a number of forms that foreshadowed the phishing phenomenon that has dominated the 21st century.

1998 — AUTOSTART

AutoStart 9805 was arguably not a virus, but a worm; that is, it replicated by copying itself, but didn't attach itself parasitically to a host program. The original variant took hold rapidly in Hong Kong and Taiwan in April 1998, and was soon reported on at least four continents.

1999 — MELISSA

Mass mailing worm with widespread impact, infecting Microsoft and Intel networks through the MS Outlook email client. The virus was delivered via an MS Word attachment that would forward to the victim's first 50 Outlook contacts when clicked.

2000 — LOVELETTER

Another email worm that is said to have attacked tens of millions of Windows PCs. Sometimes referred to as ILOVEYOU, The virus would arrive as an attachment disguised as a love letter, capable of accessing the operating system, secondary storage, system and user data of the unfortunate victim.

2001 — NIMDA

This computer worm was particularly effective for using several different methods of attack, including email, open network shares and compromised websites. Nimda was initially linked to Al Qaeda in the media due to its closeness to September 11th, but this theory was never proven.

2002 — KLEZ

A mass-mailer worm propagating a polymorphic virus. Once executed on an infected computer, it sends itself to addresses found in the system. It was notable for its "sender forging" technique, replacing the email address of the original sender with an alternative but real address. Many misunderstandings and false accusations followed.

2003 — SQL SLAMMER

Basically a self-replicating network packet, this worm exploited a vulnerability in Microsoft SQL Server and spread rapidly – infecting most of victims within just ten minutes. The entire Internet became very slow that day.

2004 — MYDOOM

One of a rash of mass-mailer worms that spread during the first decade of the 21st century. The original version was noted for its rapid spread, but is probably best remembered for carrying out DDoS (Distributed Denial of Service) attacks on SCO Group and Microsoft – which both offered $250,000 for information leading to the author's arrest.

2005 — COMMWARRIOR

The first mobile phone virus able to spread via MMS messages and Bluetooth, Commwarrior targeted Symbian Series 60 smartphones. Its impact was small, but its implications to AV experts were great.

2006 — VB.NEI

Also known as Nyxem, Blackmal or Mywife, it received a lot of attention because it used a counter which allowed researchers to track the number of infected hosts. VB.NEI was also notable because it deleted files – a throwback to the earlier days of data-destroying viruses what were now a rarity.

2007 — STORM

Detecting by ESET as Nuwar, the infamous Storm worm began infecting computers across Europe and the United States, propagated through an email claiming to be about a recent weather disaster, and later detected in fake emails with subjects ranging from Saddam Hussein to Fidel Castro. Infected computers became part of a botnet.

2008 — CONFICKER

Did ever a botnet spread so wide, for so long, and attract so much media attention, without actually doing very much? Even so, its use of fluxing algorithms in order to hamper tracing was a pointer to future developments.

2009 — TDL3

Innovative, adaptive, TDL3 rootkit and its successors (TDL3+, TDL4) have proved irritatingly successful in terms of persistence. It has also introduced new twists on old ideas like P2P networks and hiding malware – just as previous malware has used sectors marked as bad, slack space, or streams, TDL has made effective use of a hidden file system.

2010 — STUXNET

The first military grade worm that really hit the news big while the affecting a relatively low volume of systems. It targets industrial control systems and it was used against Iranian nuclear facility.

2011 — KELIHOS

A likely successor of the Storm worm, this botnet was primarily used to run spam campaigns and steal information.

2012 — MEDRE

An information stealing virus stealing AutoCAD documents. ESET's team discovered and analyzed this threat to find out that it was developed to steal blueprints from private companies mostly based in Peru.

2013 — HESPERBOT

This advanced trojan targeted online banking users with very credible-looking phishing-like campaigns related to trustworthy organizations. Attackers obtained login credentials by luring their victims to run the malware.

2014 — WINDIGO

Cybercriminal campaign that has seized control over 25,000 Unix servers worldwide that sent millions of spam emails every day. Sophisticated malware components were designed to hijack servers, infect computers that visit them and steal information.

2015 — POTAO

This espionage malware was detected mostly in Ukraine, Russia, Georgia and Belarus. Stealed passwords and sensitive information in order to offer them to the attackers' remote computer.

ESET — ENJOY SAFER TECHNOLOGY™