

The Journey, So Far: Trends, Graphs and Statistics

Martin Overton, IBM Global Technology Services, UK

Email: *overtonm@uk.ibm.com*

WWW: *http://www.ibm.com/uk*

Tel: *+44 (0) 2392 563442*

Abstract:

This paper will discuss the observed trends that have emerged since the start of the malware problem on DOS and Windows and how things have changed over the years.

The paper will discuss examples of the following:

- Malware types.
- Targets; file formats and operating systems.
- Obfuscation and related tricks and counter techniques.
- The use of social-engineering by malware authors.
- The cat and mouse game between the malware authors and vendors.
- The challenges of classification of malware.
- Changes in motivations.

The paper will discuss the changes witnessed in the malware/anti-malware arena seen since the start of it all with Brain. This will cover the emergence of stealth, polymorphism, macro and script malware and go on to cover the growth of mass-mailing worms, bots and the rebirth of stealth as rootkits.

This paper will include clear trend analysis showing the major shifts in malware over the years using a consistent data source which I have compiled. Key shifts from both sides of the problem will be covered, such as polymorphism [including TPE and DAME] and the resulting move to emulation and generic decryption to counter the threat. The growth in the use of packers, compressors and social engineering will also be covered.

Finally, the paper will cover the change in motivation for the malware authors, not just covering the excuses/reasons that they offer, but also the real reasons. It will also cover the changing landscapes of types or malware used and the now often confused classification situation.

Disclaimer:

Products or services mentioned in this paper are included for information only. Products and/or services listed, mentioned or referenced in any way do not constitute any form of recommendation or endorsement by IBM or the papers author.

This paper was written for, and presented at, the 2007 Virus Bulletin conference at the Hilton Hotel, Vienna, Austria between September 19th – 21st 2007.

I would welcome any constructive feedback on this paper and its content.

1 Introduction

This paper has been written for the corporate stream of the conference and therefore it will not delve into very technical details of malware and anti-malware. However, links will be used [where possible] to point the reader to more details on a topic.

This paper will not attempt to cover the complete history of the malware or anti-malware arena as this is not possible in the time and size limits imposed by the conference organisers (even though this paper has greatly exceeded them). Furthermore, to cover these arenas in sufficient depth would require hundreds [if not thousands] of pages, and it would no longer be a paper but a book [or a series of them].

I will also not be discussing spam, scams, spyware or adware in detail, as again that would only make the paper even longer.

2 Malware History

2.1 Pre-Main-Stream-Malware-History

As mentioned in the abstract of this paper I will cover *“the observed trends that have emerged since the start of the malware problem on DOS and Windows and how things have changed over the years.”*

Please notice the mention of ‘DOS’ as the starting point, I will not be covering malware which preceded the appearance of DOS, in depth. I will however, quickly cover the key points and dates of what came before as it is important to understand that malware is not just a ‘DOS’ or ‘Wintel’ issue.

Although this papers main purpose is to mainly discuss ‘DOS’ and ‘Wintel’ malware I will cover key events on other operating systems when the need arises.

Let me first kick off this paper with a little techno-archaeology, so that you can understand where things really started and how they developed over the years before the first real IBM PC virus arrived in 1986.

Trying to excavate the details of the early days of computer virus development has been both frustrating and immensely interesting, however I safely believe that we can say that the very first computer designed by Charles Babbage was not bothered by them as neither of his difference engines were completed in his lifetime.

It is claimed that the basic idea of self-producing mathematical automata which discussed ways for creating such 'Self-Reproducing-Machines' is down to John Von Nuemann. He proposed the idea in the 1948 and 1949 timeframe and by 1951 he had progressed from the idea to methods for demonstrating how such automata could be created.

The next person to get involved is believed to be Lionel Penrose, a British mathematician, who presented his own view on automated self-replication in an article which was published in 1959 in Scientific American entitled 'Self-Producing Machines'. If you think this sounds like the same idea as John Von Nuemann then you are correct, up to a point, as Penrose used a simple two dimensional structure as his basis, this model could be activated, multiply, mutate and attack. Sounds like the building blocks of a computer virus to me. A little later after the article was published it is claimed that Frederick G. Stahl actually reproduced Penrose's model in machine code on an IBM 650, in other words he created a self-producing computer program that included the functions laid out by Penrose.

I should make one thing very clear at this point, these early studies were not intended to be the 'foundations' for developing what became known as computer viruses. In fact these experiments were used to help scientists understand life and many of these techniques led to the foundation of artificial intelligence and robotics.

Moving on to the 1960s, in 1962 we find a group of engineers from the Bell Telephone Labs of America had created a game which they called 'Darwin' [later, widely known as Core Wars]. According to the data I've managed to extract from one documented source [Kaspersky],

"The game consisted of a so-called umpire in the memory of the computer that determined the rules and order of battle between competing programs created by the players. The programs could track and destroy opponents' programs and, more importantly, multiply. The point of the game was to delete

your opponent's programs and gain control over the battle field."

The engineers credited with the creation of 'Darwin' are V. Vyssotsky, G. McIlroy, and Robert Morris.

The problem was, as with most things in the real world, the techniques and games which had been created by these engineers and scientists, could unfortunately, be used for a completely different and less mundane purposes. The world was about to find this out as we started to see the other uses for these self-reproducing techniques.

The 1970s was when the seeds of the other uses for self-reproducing techniques for computer programs started to sprout:

It is believed that during the early 1970s a computer virus was detected on the predecessor to what would later become the Internet. This network was the property of the US military and known as ARPANET. The virus was known as 'Creep' and was written for operating system that ARPANET relied on, this being the then-popular Tenex operating system. Creep was able to move from system to system by gaining access through a modem, it then copied itself to the remote system. Systems that became infected displayed the message, *'I'M THE CREEPER : CATCH ME IF YOU CAN.'* You could call this the proto-type of what would become known as computer worms. Interestingly, shortly after Creep was found a new program was anonymously created and released to hunt down and delete the Creep virus; this new program was known as Reaper. But, Reaper was not an anti-virus program, but another virus itself. No one has come forward or been outed as the author/authors of both Creep and/or Reaper. Was Reaper designed by the same author as an anti-dote for Creep, or by someone else?

In 1974 another virus was found which was called Rabbit as it didn't do anything but reproduce and spread to other machines. Rabbit replicated so many copies of itself on the infected system that it seriously affected system performance; eventually this would cause an infected machine to crash.

Just a year later in 1975 another game was created, this time for the Univac 1108; this one was known as Pervading Animal, To this day, analysts argue about whether this was another virus or the very first Trojan. According to Kaspersky:

"The rules of the game were simple: the player would think of an animal and the program asked questions in an attempt to identify it. The game was equipped with a self-correction function; if the program was unable to guess the animal, it would update itself and enter new questions. The new modernized version overwrote the old version but, in addition to this, copied itself to other directories. After some time, as a result, all directories would contain copies of 'Pervading Animal.' It is unlikely that engineers appreciated this because the combined volume of the game's copies occupied a significant amount of disc space."

To combat Pervading Animal Univac programmers attempted to use a similar technique that had been successfully used against the Creep virus. They created a Reaper-like program, this was a new version of the game which hunted for older versions of the game and destroyed them. This however was just a stop-gap as the problem was completely resolved when a new version of the operating system; Exec 8, was released. As part of this OS upgrade, the file system was modified making Pervading Animal unable to replicate any longer.

By the beginning of the 1980s as computers started to turn up in schools, universities, business and in homes, we also saw another advancement in telecommunications and the rise of BBS [Bulletin Board Systems] which used modems to allow other computers to connect to the BBS and either chat in real-time with the SYSOP or other users connected to the system, post and read messages, both personal and in discussion groups and upload and download data and software. This was the time when Trojans started to appear in quantity; programs that claimed to do one thing, but when run often did something that wasn't expected. These didn't self replicate, but they did do lots of damage.

By 1981 Apple computers were in widespread use, at this time it was the Apple II and it was attracting the attention of virus authors. Because of this, according to Kaspersky:

"It is not surprising that the first large-scale computer virus outbreak in history occurred on the Apple II platform."

This outbreak was the virus that is often mentioned as the first 'in-the-wild computer virus'; known as Elk Cloner which was authored by Rich Skrenta. This is how Kaspersky describes it:

"Elk Cloner spread by infecting the Apple II's operating system, stored on floppy disks. When the computer was booted from an infected floppy, a copy of the virus would automatically start. The virus would not normally affect the running of the computer, except for monitoring disk access. When an uninfected floppy was accessed, the virus would copy itself to the disk, thus infecting it, too, slowly spreading from floppy to floppy.

The Elk Cloner virus infected the boot sector for Apple II computers. In those days, operating systems were stored on floppy disks: as a result the floppies were infected and the virus was launched every time the machine was booted up. Users were startled by the side effects and often infected friends by sharing floppies, since most people had no idea what viruses were, much less how they spread.

The Elk Cloner payload included rotating images, blinking text and joke messages:

*ELK CLONER:
THE PROGRAM WITH A PERSONALITY
IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES, IT'S CLONER
IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM, TOO
SEND IN THE CLONER!"*

Meanwhile at Xerox PARC in 1982 two researchers were studying programs which would later be considered computer worms. More details about early worms can be found here:

<http://momusings.blogsome.com/2004/12/13/the-only-good-worm/>.

However, it wasn't until 1983, according to Kaspersky, that the use of the word 'virus' was used in connection with self-replicating computer programs. This first use of the term is attributed to Fred Cohen who used it on November 10th, 1983, during a seminar on computer safety at Lehigh University.

During that seminar he [Fred Cohen] demonstrated a virus-like program on a VAX11/750 computer system. The virus-like program was, it is claimed, able to install itself to other system objects.

Dr. Frederick Cohen introduced the term 'computer virus' on the recommendation of his advisor, Professor Leonard Adleman, who it is claimed, picked the name from science fiction novels. I wonder from which novel he borrowed it from, or was it from a film as Wikipedia suggests¹:

"The term "virus" was first used in an academic publication by Fred Cohen in his 1984 paper Experiments with Computer Viruses, where he credits Len Adleman with coining it.

However, a 1972 science fiction novel by David Gerrold, When H.A.R.L.I.E. Was One, includes a description of a fictional computer program called "VIRUS" that worked just like a virus (and was countered by a program called "VACCINE").

The term was also used in Michael Crichton's 1973 movie "Westworld" to describe the problems "infecting" the robots in the parks as they failed.

The term "computer virus" with current usage also appears in the comic book Uncanny X-Men #158, written by Chris Claremont and published in 1982. Therefore, although Cohen's use of "virus" may, perhaps, have been the first "academic" use, the term had been used earlier."

Fred Cohen's original definition of a computer virus as of 1983 was: "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself." He updated this definition a year later in 1984 in his paper entitled: "Computer Viruses – Theories and Experiments".

¹ Source: http://en.wikipedia.org/wiki/Computer_virus#Etymology

So if you use the dates given above 2007 is the:

- 58th or 59th Anniversary of Von Neumann's idea [1948-49]
- 48th Anniversary of the first self-producing computer program [1959]
- 36th Anniversary of Creeper and Reaper, first computer worms? [1971]
- 33rd Anniversary of Rabbit, first real computer virus? [1974]
- 32nd Anniversary of Pervading Animal, first computer Trojan? [1975]
- 25th Anniversary of Elk Cloner, first 'in the wild' computer virus? [1982]
- 21st Anniversary of Brain, first IBM PC and compatible virus, also the first stealth virus. [1986]

See, before 1986 not a single DOS or IBM PC or compatible virus in sight and no anti-virus software either!

If you want to learn more about these early years, then I would suggest getting hold of the books, and reading the many articles and papers mentioned in the references section of this paper. It should only take you a few months to get through all of them.

2.2 The Eighties

The 1980s was where it all began for the IBM PC and compatibles as far as malware is concerned...however it didn't start until after the first half of that decade, in 1986 to be exact.

2.2.1 1986

So, back to the main focus of this paper, DOS and Wintel based malware:

It all started for the IBM PC and clones back in January 1986.

It is claimed that two brothers from Lahore, Pakistan, Basit and Amjad Alvi realised that the boot sector of a floppy diskette contained executable code; this code, if present, is automatically executed whenever you start or reboot a computer with a floppy disk in drive A. In their case the floppy disks in widespread use at that time were 5.25 inch 360KB.

According to some sources, they decided to write some code to replace this boot code and they made this code memory resident. They also included in the replacement code a function which enabled a copy to be made of their code and install it on each and every unprotected floppy diskette that the computer accessed, not just in the A drive, but any floppy disk drive. As part of the infection of the floppy disk they changed its label to '(c) Brain'. They also included a copyright message in their code, which is show below:

```
Welcome to the Dungeon (c) 1986 Brain & Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0
Dedicated to the dynamic memories of millions of viruses who are no longer with us
today - Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching program
follows after these messages....$#@%$@!!
```

They also included their address and three phone numbers in a message that informed the user that their machine was infected and for vaccination the user should contact them:

```
Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730
NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of
this VIRUS.... Contact us for vaccination...
```

This floppy disk boot sector 'virus' was also known by the following names: *Lahore, Pakistani, Pakistani Brain, Brain-A, UIUC* and *Pakistani flu*.

In fact, not only was Brain the very first malware written for the IBM PC [and clones]², it was also the first computer virus that used 'stealth' techniques to hide its presence.

Brain, when it infected a 360KB floppy disk moved the real boot sector to another part of the disk and marked those sectors as bad. Disks infected by Brain usually were found to have 3KB of bad sectors.

Here is a short extract from the description of Brain from F-Secure explaining how the stealth function it used

² It has been suggested by some sources that another Boot Sector Infector was created before Brain, this being Ashar, which seems to be an earlier version of what would be later known as Brain.

works:

“The Brain virus tries to hide from detection by hooking into INT 13. When an attempt is made to read an infected boot sector, Brain will just show you the original boot sector instead. This means that if you look at the boot sector using DEBUG or any similar program, everything will look normal, if the virus is active in memory. This means the virus is the first "stealth" virus as well.”

So, although Brain was the first stealth virus, it didn't hide its presence very well due to the use of bad sectors and the change of label to (c) Brain.

By December 1986 another programmer, called Ralf Burger, this time in Germany, had found out that a file could be made to make a copy of itself, and attach that copy to another existing file. In his case he was focussing on DOS executable files that used the COM file format. He called this program he had created ‘Virdem’ and presented it at a meeting of the German underground Chaos Computer Club, where the theme was viruses. Virdem was the first program which could replicate a copy of its code to executable DOS files, as with Brain the payload was essentially harmless.

Not content with creating the first DOS COM file infector, because of the interest Virdem had generated he was asked to write a book. But let me not get ahead of the timeline, more on that in the next section.

According to Joe Wells *"Two other demo viruses have 1986 copyright notices. These are the Burger virus (Program Virus ver. 1.1 by R. Burger) and the Rush Hour virus by B. Fix."*

By the end of 1986 we knew of at least three computer viruses.

2.2.2 1987

Although Brain has been written and released into the world 'in-the-wild' it wasn't until October of 1987 that it really was noticed, by then the University of Delaware realised that they had this virus, when they started seeing the label "(c) Brain" on floppy diskettes.

In 1987, a program was circulating called Charlie that Franz Swoboda believed contained a virus. So, when he analysed the file and found out that it did indeed contain a virus, he decided to call it the Charlie virus. There are several claims about this incident, some sources claimed that Swoboda got the virus from Ralf Burger and others claim it was the other way round, some even claim that one or the other was the author of it, yet others claim that it was created by an Austrian high school student. Whatever the truth, Vienna, as the virus eventually became known, was something different to what had so far been seen as it had a payload that did something bad; if you ran an infected file there was a one in eight chance of it causing the computer to reboot. Like Virdem it only infected COM files.

Even more notably, Burger gave a copy of Vienna to Bernd Fix, who then disassembled the file; this was the first time that anyone had done this with a computer virus, and Fix sent a copy of the disassembly back to Burger. This disassembly was modified slightly, 5 bytes were zeroed out, and this disassembly was published in Burger's book. The 5 bytes that were zeroed out were the 5 bytes that would normally reboot the computer in the original Vienna code; the change meant that instead of rebooting the computer it caused it to hang instead.

As mentioned in the previous section, Ralf Burger had been asked to write a book about computer viruses, this book first published in 1987, was called: 'Computer Viruses - A High-Tech Disease'. Not only did Ralf include the source code [modified] for the Vienna virus, but he also included source code for the Number One virus, the Burger virus and the Rush Hour virus, he also includes the source code for the first known virus detection programs; however they were limited to detecting a single virus each.

The impact of the publishing of the source code for Vienna would be felt by computer users the world over as the number of viruses based on it quickly multiplied over the next few years.

During the fall of 1987 a new virus which targeted only the DOS Command Processor [COMMAND.COM] was found at the University of Lehigh. Not surprisingly, at that time, it was called the LeHigh virus. Like Vienna, it too also did something bad, in Lehigh's case this was once it had infected the first four disks it came into contact with. At that point, it then triggered a payload that would overwrite the File Allocation Table [FAT] of all the disks currently available to the system. However, the programmer of LeHigh had made several errors

that meant that even though the size of the host file 'COMMAND.COM' didn't change when infected, the date stamp of the file did change. If it hadn't changed the file date stamp then the computer staff at Lehigh would not have been able to get on top of the outbreak as quickly as they did. Although the virus did cause a lot of damage to the Universities computer disk library. One thing of note with Lehigh, is that since 'COMMAND.COM' remains resident, it was technically the first memory resident file infector.

Kaspersky has this to say on the outbreak:

"In 1987, Cohen was at Lehigh, as was Ken van Wyk. So was the author of the Lehigh virus. Lehigh was an extremely unsuccessful virus - it never managed to spread outside its home university, because it could only infect COMMAND.COM and did a lot of damage to its host after only four replications. One of the rules of the virus is that a virus that quickly damages its host, cannot survive. However, the Lehigh virus got a lot of publicity, and led to van Wyk setting up the Virus-L newsgroup on Usenet. Lehigh was nasty. After four replications, it did an overwrite on the disk, hitting most of the File Allocation Table. But a virus that only infects COMMAND.COM, isn't very infectious."

1987 seemed to be the time when academia was at the forefront of virus outbreaks and creation. Not only did Lehigh get infected, but also Yale got infected by a new boot sector virus that was named Yale; it only copied itself when you booted from an infected floppy, then put another floppy in to continue the boot process. No subsequent diskette was infected. If the boot continued from a hard disk instead then there was no infection at all. The other side of the world was not immune to outbreaks either as seen by the creation by a student at the University of Wellington in New Zealand of a new boot sector virus. This caused an outbreak and the virus was called 'Stoned'. It was the first MBR infector; previously Boot Sector Infectors had only used the DBR. One time in eight, when attempting to boot from floppy disk that was infected floppy it displayed the message 'Your PC is now Stoned'.

In October a new and previously unknown virus appeared at the Hebrew University of Israel, it was found by Yisrael Radai. What made this one different was that this was the first file infector designed to go memory-resident. It was later called the Jerusalem virus. However, as was common at this time, it seems that Jerusalem was the third in a series of viruses by the same author, the other two being Suriv 1 [TSR COM infector], 2 [TSR EXE infector], and 3 [TSR COM and EXE infector, later known as Jerusalem]. Just in case you didn't notice, Suriv is Virus spelled backwards. Jerusalem was also the first virus discovered that infected DOS executable files with either .COM or .EXE extensions. It was also the first virus to contain a bug which made it re-infect EXE files that it had already infected, making them grow and grow and grow. The bug seems to have been unintentional and it may be that the virus escaped rather than being placed in to the wild as it wasn't a finished project as can be seen from the debug code found in it.

Jerusalem's payload was to destroy all executable files on the infected system on Friday the 13th of any year (except Friday the 13th Nov 1987 making its first trigger date actually May 13th 1988). Interestingly, Jerusalem avoided infecting command.com, so that it wouldn't be detected so quickly.

After the viruses we'd seen so far in the 1980s, a new trend started, this trend was the inclusion of some animated payload, rather than the static ones we had seen with Stoned, etc.

One of the first of these new breed of virus was a floppy disk boot sector infector commonly known as Ping Pong [aka Italian] which was found at the University of Turin in Italy during 1987. Ping Pong derived its name from the graphical payload it contained; it put a bouncing ball up on the screen, but only if the disk was accessed exactly on the half hour. Due to a major programming error by its author the virus would not work on anything except computers that used Intel 8088 or 8086 processors.

Also in 1987, a very competent German programmer had written a virus, like Suriv1 it infected COM files and went resident in memory, unlike Suriv1, it contained an animated payload from which its name is derived; if the system date is between October and December 1988, then at random intervals the characters on the screen will cascade down to the bottom of the screen as if someone has detached them from their original column and row position.

Cascade also used another new idea that had not been seen before. It encrypted most of its code, leaving only a small stub of clear static code for decrypting the rest [encrypted part] of the virus. The affect of this encryption of the virus was not only to obfuscate the main body, but to use a different key each time so that it appeared different in every infected file, up to a point. When an infected file, was executed, control was transferred to the

encryption routine which decoded the virus body and transferred control to it, once that was done the file was run as normal. In many ways Cascade is seen as the forerunner of what would become known as polymorphic viruses. Unlike polymorphic viruses, Cascade only encoded the main body of the virus, not all of itself. Cascade used the size of the infected file as the decryption key.

The author of Cascade included a routine to look at the computers BIOS, if it found an IBM copyright message it was supposed to not infect files. Unfortunately, this routine didn't work and to try and fix the problem the author released another version of the virus; the original Cascade was 1701 bytes, the new one was 1704 bytes long instead. However, the fixed version still didn't detect IBM BIOSes correctly.

1987's virus creations were not just targeting DOS, there were also a number of viruses created for other operating systems: In November a boot sector virus was found which infected Amiga, this was known as The SCA virus, and this was followed up by the author with a new, and more destructive virus known as the Byte Bandit.

At the very end of 1987, we also saw the first major local network epidemic. This occurred on the Bitnet network on the 9th of December. Bitnet used the VM/CMS-9 operating systems, and the worm was written in a scripting language called REXX. The worm was known as the Christmas Tree Worm (aka CHRISTMA EXEC), is reported to have been released on to the Bitnet network from a West German university through a European Academic Research Network (EARN) portal and from there it got into IBM's Vnet. By December 13th (just 4 days after it was released), it had flooded the network. Upon loading, the worm displayed a Christmas tree on-screen and sent copies of itself to all network users whose addresses were listed in the NAMES and NETLOG system files. An unintentional side effect was that this was the effectively the first denial of service [DoS].

By the end of 1987 we knew of at least eight computer viruses.

2.2.3 1988

1988 was really the year when anti-virus software started to appear, not just freeware and shareware products but also some companies' actually trying to sell commercial anti-virus software to a generally uninterested or rather sceptical computing world. Probably one of the things I remember most about 1988, apart from the number of outbreaks, is that 1988 is the year that a certain Peter Norton made the following statement as part of an interview for Insight:

"Viruses are an 'Urban Myth', just like the alligators said to inhabit the sewers of New York."

This was interesting as quite a few well-known people had also claimed that computer viruses didn't exist and that those who believed in them were suffering from sort of mass-hysteria, or as Kaspersky stated: *"One UK expert claimed that he had a proof that viruses were a figment of the imagination."*

This 'head-in-the-sand' attitude meant that many people dismissed the threat of computer viruses, and few were inclined to actually find out if their systems were infected, using the free or shareware virus scanners. Even fewer were actually willing to pay for software to detect something that may be a figment of an a few over-active imaginations.

However, there were several outbreaks that really woke people up to the threat and these are worthy of a mention here:

The Jerusalem virus which was created and found in 1987, caused a major epidemic as it was detected on numerous computers in many companies, government offices, and last but not least academia. It was mainly discovered because on Friday, May 13th all the systems that had been infected since its release the previous year had suffered from the destructive payload; Jerusalem destroyed all loaded files on infected machines when the trigger date arrived. The virus struck all over the world, but the US, Europe and the Near East were hit hardest, so hard in fact that May 13th 1988 came to be known as Black Friday.

The second major outbreak effected IBM, and potentially their customers:

This was not because of the well-known Christma Exec worm which hit them the previous year; no it was due to an outbreak of Cascade at the Le hulpe site. This put IBM in an embarrassing position of having to inform their customers that they might have passed on the virus to them. As it turned out this was not the case, the

fallout of this 'near-miss' was that from then on, IBM took viruses very seriously indeed, and gave responsibility for virus/anti-virus research to the High Integrity Computing Laboratory in Yorktown.

There were other sporadic, smaller outbreaks of Stoned, Cascade, Brain and Ping-Pong during the year.

Then there was Scores, another virus written for the Apple Macintosh, which according to one source was intended to target a particular company; this being EDS. This is first case of a targeted attack using malware that I'm aware of.

Although not a DOS/Wintel threat, I better include a quick summary of what became known as 'The Morris Worm' or 'The Internet Worm'

November 2nd 1988 and a new worm written by Robert Morris Jr. 23 from Cornell caused a world-wide network epidemic. The worm is believed to have infected over 600 computer systems in the US alone (including the NASA research centre) bringing some to a complete standstill. Other estimates claim that over 6,000 systems were infected, bear in mind that the fledgling Internet at that time is believed to have consisted of around 600,000 systems. Paul Graham has claimed that he was there when the 6,000 infected system claim was cooked-up as it was estimated that about ten percent of systems had become infected.

In order to multiply, the Morris Worm exploited vulnerabilities in the UNIX operating systems on VAX and Sun Microsystems platforms. It used known vulnerabilities in sendmail, finger and rsh/rexec. As well as exploiting the UNIX vulnerabilities, the worm used several innovative methods to gain system access such as harvesting passwords. So, in many ways this was the first time malware had exploited known vulnerabilities in an operating system or harvested passwords.

The overall losses attributed to the 'Morris Worm' were estimated at US \$96 million dollars - a very significant sum of money at the time.

Interestingly Robert Morris Jr. had earlier in the year started a virus hoax claiming that over 300,000 computers had been infected in under 12 minutes in the Dakotas, he claimed that the "*virus was spreading over networks and changing port and drive configurations*".

There were several positive things that happened for the fledgling anti-virus research community, during 1988:

On April 22nd, the first electronic forum devoted to antivirus security was opened; this was the Virus-L forum on Usenet which was created by Ken van Wyk, a university colleague of Fred Cohen's.

Towards the end of 1988 a certain Dr. Solomon launched his own anti-virus, called 'Dr. Solomon's Anti-Virus Toolkit'.

The year ended with quite a different perspective that it had begun with; few people now doubted that computer viruses did indeed exist, and most were now starting to look at tools to detect viruses. Others were starting to believe the hype that viruses were invisible and invincible, paranoia was starting to grip all but the most level headed.

More worryingly, the media had now taken a very serious interest in Viruses, as can be seen from this list [courtesy of Joe Wells] of just some of the many magazines who published articles on viruses during the later half of 1988:

- *Business Week, Aug 1*
- *Byte, Jul*
- *Changing Times, Sep*
- *Compute!, Jun, Jul, Aug, Oct, Dec*
- *Datamation, Sep 15, Oct 15*
- *Design News, Dec 19*
- *Fortune, Dec*
- *Futurist, Sep/Oct*
- *Industry Week, Aug 15*
- *Newsweek, Nov 14, Nov 28*

- *PC-Computing, Nov, Dec*
- *PC Magazine, Feb 29, Jun 14, Jun 28*
- *Personal Computing, Jul*
- *Science, Apr 8, Nov 25*
- *Time, Feb 1, Sep 26*
- *US News and World Report, Oct 3*
- *Working Woman, Sep*

In addition, PC Week had over 20 articles on viruses during the year.

One more thing I ought to mention before I finish off 1988 is a boot sector virus known as DenZuk. It is worthy of note because of as part of its infection routine it would check to see if the floppy disk in the drive is infected with either an earlier version of itself or Brain, if found it would remove them and place a copy of itself on the floppy disk instead.

By the end of 1988 we knew of at least twelve computer viruses.

2.2.4 1989

In 1989, the first Friday 13th was in January. Yes it was Jerusalem time once more. By the end of 1988, it was clear that Jerusalem was widespread in Spain and the UK in both academia and commercial organisations. Because of the destructive payload in the virus, Dr. Solomon felt that if he didn't send out some sort of warning, to wake up people to the risk, then he would be seen as acting negligently. However he needn't have worried as the media grabbed the story and milked it; the predictability of the trigger day, together with the feature of it being Friday 13th, caught their imagination, and the first virus media hype-fest was born.

Dr Solomon had this to say about the media circus that ensued:

"On the 13th of January, we had dozens of phone calls, mostly from the media wanting to know if the world had ended yet. But we also had calls from a large corporate site, a small vendor of PC hardware, and a couple of single users. We were invaded by TV cameras in droves, and had to schedule them carefully to avoid them tripping over each other. In the middle of all this, the PC Support person from the infected corporation arrived. The TV people wanted nothing better than a victim to film, but the corporate person wanted anonymity. We pretended that he was just one of our staff. Also, at that time, British Rail contacted us; they also had an outbreak of Jerusalem, and they went public on it. Later, they regretted that decision, because for a long time afterwards, their PC Support person was badgered by the media seeking interviews."

A second media storm happened in 1989, this being the one surrounding DataCrime!

In March of 1989, a new virus was written in Holland, we know this because a Dutchman who said his name was Fred Vogel contacted a UK virus researcher, informing that he had found a virus called Datacrime all over his hard disk and he was worried that it would trigger on the 13th of the next month.

Now comes the fun part, when a sample was disassembled, it was found that on any day after October 12th, the virus would trigger a low level format of cylinder zero of the hard disk. So, Mr Vogel had got the month wrong when it would trigger. He did get the correct day of the month it would start to trigger; on any day between the 13th of October and December 31st. As part of its payload it would display its name: Datacrime virus. A simple technical write-up of this virus was published concluding that it was another non-memory-resident virus, and highly unlikely to spread or be a big threat.

The write-up was reprinted by a magazine and then another magazine repeated the story, another modified it, and so on. Not surprisingly, by June the fictionalised version of the write-up was being treated as fact. The details now said the virus would trigger on October 12th and that it would low level format the whole hard disk.

The embellishments continued, once the story got to America, the press started calling it "Columbus Day virus" (October 12th) and it was suggested that it had been written by Norwegian terrorists, angry at the fact that Eric the Red had discovered America, not Columbus.

IBM who had their own internal-use-only anti-virus software for checking computer disks, which they had

developed after the LeHulpe incident with Cascade the previous year, decided that it might be in their own and their customers interests if they made their in-house antivirus available to customers, what with the hype surrounding Datacrime. Failure to make this software available to customers might be seen as they didn't care about them.

So, in September 1989 IBM decided to bite the bullet and they sent out copies of IBM Anti-Virus 1.0 to their customers, along with a letter telling them what it was and more importantly why they had sent it out. As someone said, "*When you get a letter like that from IBM, and a disk, you would be pretty brave to take no notice*". So, lots of IBM customers started to scan their systems and they found viruses, the usual suspects, hardly anyone is reported to have found Datacrime.

Meanwhile back in Holland, the Dutch police had decided to take action themselves, so they commissioned a programmer to write a virus detector for Datacrime. They offered it for sale at Dutch police stations for \$1 and it sold really well and it also suffered from false alarms. So, they recalled it and replaced it with an updated version. Not surprisingly because of the hype the media had stirred up, there were long queues outside the police stations in Holland as well as a certain amount of confusion about whether anyone's computers were really infected with Datacrime; the false alarms caused by the detector didn't help.

Here is a list of just some of the many, many stories published about DataCrime, once more courtesy of Joe Wells:

- "*Rumors abound of Columbus Day virus attacking MS-DOS nets*" - *Federal Computer Week*, August 28, 1989
- "*Experts warn of DataCrime virus, plan prevention*" - *PC Week*, September 11, 1989
- "*Virus outbreak rumored*" *MIS Week*, September 18, 1989
- "*NIST fears virus attack after holiday*" - *Government Computer News*, October 2, 1989
- "*Friday the 13th: a virus is lurking*" - *New York Times*, October 8, 1989
- "*Computer virus doesn't cause much lost sleep*" - *Wall Street Journal*, October 13, 1989
- "*Computer Virus Cases Called Rare*" - *The Washington Post*, October 14, 1989
- "*Virus Week finds sites ready, still waiting for infections*" - *Computerworld*, October 16, 1989
- "*DataCrime fizzles in U.S.*" - *Newsbytes*, October 17, 1989

As October 13th 1989 actually fell on a Friday it meant that it was a day when either Jerusalem or Datacrime would trigger, and cause significant damage to the infected computer. In the end there were reports of systems being affected by Jerusalem, but there were no confirmed reports of systems that felt the bite of Datacrime. So, Datacrime turned out to be a damp squib, and the over-hyping by the media once more led many people to believe that computer viruses were not a widespread and dangerous as they had been led to believe.

October 16th saw the appearance of another new worm, this time targeting VAX/VMS computers on the SPAN network. The worm spread via the DECNet protocol and changed system messages to read, 'WORMS AGAINST NUCLEAR KILLERS' accompanied by the message, 'Your System Has Been Officially WANKed.' WANK also changed system passwords to random symbols and sent them to a user by the name of GEMPAK on the SPAN network. Not surprisingly, it used techniques learnt from the 'Morris Worm' the previous year.

Also in October Fredrik Skulason, the founder of Frisk Software [maker of F-Prot] found a new virus in Iceland which he named Ghostball, what was unique about it was that it could infect boot sectors and COM files making it the very first multipartile virus. However, it appears that all Ghostball did on floppy disks was drop a non-viable variant of Ping-Pong to the boot sector.

Other notable viruses found during 1989 included:

The Dark Avenger.1800 [aka Eddie] virus which was reportedly written by someone calling himself 'Dark Avenger' in the city of Sofia in Bulgaria in January of 1989. This virus marked a new phase in the virus and anti-virus arms race. Not only that, but little did we realise at that time how much we'd be hearing from 'Dark Avenger'.

This virus introduced two new and worrying payloads. Firstly, it was a data-diddler; designed to do slow, insidious damage to the system rather than sudden obvious damage. To do this it wrote a sector that starts with the text "Eddie lives...somewhere in time!" to random sectors of the drive, slowly corrupting the data held on

the disk, and even backups, if the corrupted data was backed-up.

Also, it was found to be what we called a fast-infecter. Memory resident viruses previously would only infect programs as they were run. Dark Avenger also infected programs if they are opened. This meant that if the virus was resident in memory and you ran an anti-virus scanner to scan the system for viruses, the virus would follow behind the scanner and infect every program the scanner opened to scan for viruses. So, unless your virus scanner already knew about Dark Avenger.1800 and could detect its presence in memory, it would be actually helping to further infect your computer.

The Frodo virus was found in Haifa, Israel in October. What made Frodo different was that it was the first full-stealth file infecter. The payload for Frodo was meant to damage the hard disk if run on or after the 22nd of September of any year. In reality, due to programming errors, Frodo simply hangs the system instead.

The book published by Ralf Burger was responsible for the 405 virus, which was a modified version of the overwriting virus in his book. Unknown to most of us was that the Bulgarians had become interested in viruses and the Russians were coming to the party too, as shown a number of new variants that appeared. These included: two variants of Cascade, several variants of Vacsina, Yankee, Jerusalem, Vienna, Eddie, and Ping-Pong.

Quickly going back to April; something rather important was happening in the anti-virus field, this being the first antivirus publications being founded: Sophos sponsored Virus Bulletin, whereas Dr. Solomon's founded Virus Fax International. Virus Fax International was first renamed as Virus News International and eventually metamorphosed into Secure Computing.

Both Secure Computing and more importantly Virus Bulletin are still published today, although Virus Bulletin is the only one of these publications which still focuses mainly on malware research and testing of anti-malware tools.

1989 also saw another book written on the subject of viruses: *'Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats'* written by Eugene H. Spafford, Kathleen A. Heaphy, and D. J. Ferbrache'.

From an anti-virus company view, it was a good year as not only did Eugene Kaspersky find his first virus in October, this being Cascade, which led Eugene to devote his life to antivirus research, a month later he detected the Vascina virus using the first version of the -V antivirus program he had just written. Much later, -V turned into AVP Antiviral Toolkit Pro. The following anti-virus companies also sprung up: F-Prot, ThunderBYTE, and Norman Virus Control.

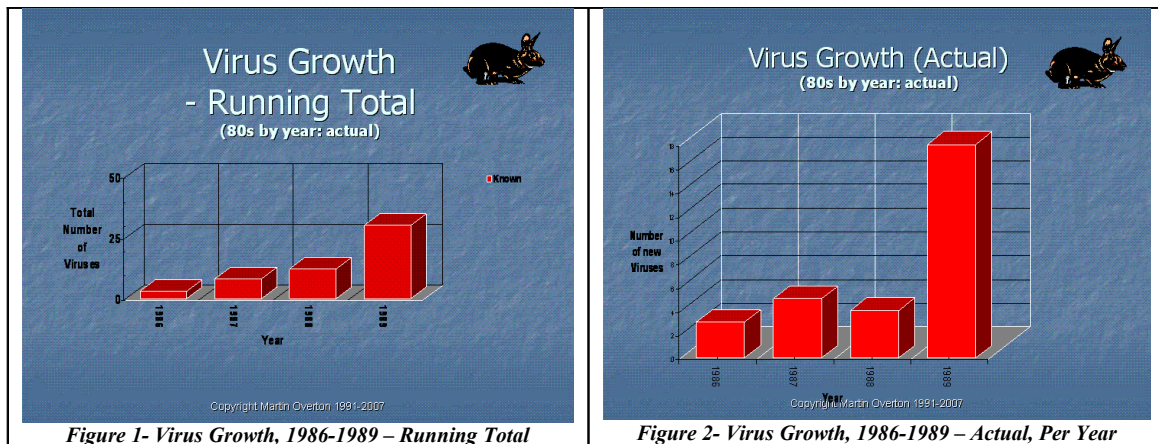
A leading researcher, Dr. Harold Highland, created the very first macro virus during 1989, this used Lotus 123 macros. He showed the macro virus during a demonstration at a conference, and managed to scare the living daylight out of the audience. According to various sources, he immediately destroyed the virus after the conference and that was the last we saw of macro viruses until the 1990s when they resurfaced.

The year ended with another first:

December saw the Aids Information Diskette incident. This involved 20,000 discs which contained a Trojan being sent to addresses in Europe, Africa, Australia and the WHO. The addresses that the disks were sent to had been stolen from the database of PC Business World. The disk came with installation instructions. If you install the program on the disk it would automatically create its own concealed files and directories and modified the autoexec.bat. After 90 loads, the operating system encoded the names of all files, rendering them invisible and leaving only one file accessible. This file was an invoice for \$189 to be sent to PO Box 7 in Panama. The Trojan's author was discovered to be Joseph Popp.

The main issue was that so many people had installed the software that PC Business World decided to create a program to decrypt the files and directories and undo the other changes made by Dr. Popp's Trojan. Yes it was a Trojan, in fact the first trojan that appeared 'in-the-wild' and a warning to those that took note that this sort of cyber-extortion could be made to work, although in Dr. Popp's case it flopped.

By the end of 1989, and the end of the 80's we knew of at least thirty computer viruses.



2.3 The Nineties

2.3.1 1990

By 1990, it was clear that the game was changing; no longer could you get by with running a couple of dozen search simple strings on each file to detect viruses.

To make this absolutely clear to the anti-virus researchers and companies several things happened:

A researcher called Mark Washburn, from the US, took the Vienna virus, and created the first polymorphic virus. This was a step up in the viral arms race as Cascade had only used encryption.

Mark's viruses (1260, V2P1, V2P2 and V2P6) used a new idea in that the whole virus would be variably encrypted, and there would be a decryptor at the start of the virus (like Cascade). There the similarity ended as the decryptor in Mark's new viruses could take a very wide number of forms. In his first few viruses that used this technique, the longest possible simple search string was just two bytes; V2P6 got this down to just a single static byte. A number of anti-virus vendors couldn't make the transition and gave up as it wasn't simple to write new algorithms to handle this move; others saw it as just another challenge.

As Dr Solomon confirms:

"The three main sources of search strings were a newsletter called Virus Bulletin, the IBM scanner, and reverse engineering a competitor's product. But you can't detect a polymorphic virus this way (indeed, two years after these viruses were published, many products were still incapable of detecting these viruses)"

To counter this move towards the use of polymorphic code required a completely different approach to what had been used before, no more simple hex strings and patterns. Dr. Solomon decided the best way to deal with this new technique was:

"it was necessary to write an algorithm that would apply logical tests to the file, and decide whether the bytes it was looking at were one of the possible decryptors."

Other researchers came up with other solutions to detecting polymorphic code, some worked better than others. Most of these worked fairly well.

However, many of these new techniques to detect viruses using polymorphic technique were prone to false alarms. It wasn't until 1992 that the problem with polymorphic techniques was fully addressed.

The award for the first multipartite virus should probably go to Flip, which got its name from the payload it used; on the second day of any month between the times of 16:00 and 16:59 it flips the screen display horizontally by switching to a special character set, Flip is also polymorphic. There were several multipartite viruses that were created before Flip. They include Ghostball (often regarded as the very first multipartite virus), Anthrax and V1; however, none of these were very successful.

On May the 16th Robert Tappan Morris was convicted of violating the computer Fraud and Abuse for releasing

the worm he created. An appeal was denied in March of 1991. He was sentenced to three years probation, a \$10,000 fine and 400 hours of community service. This was the first time anyone had been charged and successfully prosecuted for this type of computer crime.

The bad guys (at this time there were no known female malware writers) started to get organised:

First we saw the so-called 'Bulgarian Virus Writing Factory'³ who were responsible for many viruses during 1990, these include Number-of-the-Beast (full stealth in a file virus) and Nomenklatura (with an even nastier payload than Dark Avenger), Murphy and new versions of Eddie. Many of the most advanced, and ones using new ways to hide from anti-virus came from a certain person using the pseudonym "Dark Avenger". He usually wrote and released several viruses each year, which incorporated new infection and techniques to hide from anti-virus tools. He was the first virus author to employ a technique where the virus, if detected, would automatically infect all files in the computer, even if the file was opened for read-only purposes.

Secondly we saw the birth of and rapid growth of Virus Exchange Bulletin Board Systems [VX BBSes]. Interestingly the first VX BBS is believed to have been started by the author that would cause so much hard work for the anti-virus researchers; this person was the Dark Avenger. According to Joe wells:

"These boards had huge virus collections for download. But to download viruses, the user had to upload viruses first. This resulted in hundreds of viruses being created just for upload. Moreover, many hacked viruses, non-viruses, attempts at viruses, and completely innocent programs were being uploaded. In turn, these unwieldy conglomerate masses made their way into antivirus research collections. Worse still, such horrific "test collections" fell into the hands of product reviewers."

To further exacerbate the problem these VX BBSes often also offered source code and disassemblies of viruses, which only encouraged more virus variants to be written. Just what the world needed more viruses!

In July, PC Today inadvertently created a viral first, they sent out 50,000 copies of their magazine which had a free floppy disk infected with DiskKiller [aka Ogre].

During the second half of the year a new virus appeared that caused a rather intense storm in the anti-virus camp, this virus was called Whale. Whale was a beast of a virus, over 9KB of highly armoured, oligomorphic code. It was memory resident and used stealth. It would infect both COM and EXE files [but only if you were really 'lucky']. Steve White of IBM is credited with saying the following at virus conference in early 1991:

"I could give the Whale virus to everyone in the audience and it still wouldn't spread."

I remember Whale very well, although Steve White indicated that it was unlikely to spread, I did actually managed to get Whale to run on a test system and it did infect other files, but what I remember most about Whale was that you couldn't mistake when it actually went resident as the response of the infected computer was so silloowwww....

Much analysis was wasted on Whale, meanwhile other viable, and destructive viruses, were spreading unchecked in-the-wild.

According to Kaspersky, the first Russian viruses also appeared during 1990, these were Peterburg, Voronezh, and LoveChild.

In December there was some good news for the anti-virus community as EICAR (the European Institute for Computer Antivirus Research) was established in Hamburg, Germany. Another group was created just for invited researchers, this group was CARO. CARO is often jokingly referred to as the virus researcher's beer drinking club, and CARO members are jokingly known as CAROtS.

Remember the guy who in 1988 was quoted in a magazine as believing that "*Viruses are an 'Urban Myth', just like the alligators said to inhabit the sewers of New York.*"? Well sometime in 1990 he obviously decided after all that they were real after all; the viruses that is (not sure if he changed his mind about the alligators), as his company released their own anti-virus. Yes, Norton Anti-Virus was now here to save the world!

³ This is more of a metaphor as the Bulgarian virus writers were not really working together, in fact according to Dr. Vesselin Bontchev, they hardly communicated with each other at all.

So, by the end of 1990 the following companies were known to be offering anti-virus products:

Iris, Certus International, Digital Dispatch, Carmel, Microcom, Parsons, Elia Shim, McAfee, S&S, Frisk Software, ESaSS, Sophos, World Wide Data, BRM, Cybec, Hunix, IBM, RG Software and Norton.

2.3.2 1991

In January Roger Riordan of Cybec in Australia discovered a new variant of the Stoned virus. When he analysed it he found that it triggered on the birthday of a Max Telfer. According to Joe Wells:

"Max, evidently not wanting the thing named after him, suggested the name of someone else born on that day. So Roger named it Michelangelo."

Little did we realise at that time how much we'd be hearing of Michelangelo.

Also in March another first happened, in this case it wasn't a virus but a Virus Construction Set, known as VCS V1.0 was discovered. VCS allowed the user to build viruses.

Dark Avenger, in another viral first for him, announced the first virus vapourware. He threatened to write and release a highly polymorphic virus capable of 4,000,000,000 different mutations. It never actually appeared until January of the following year (1992), but it wasn't just a virus he delivered. It turned out to be something that hit the anti-virus community much harder, at first.

1991 was the year that polymorphic viruses really started to impact people in the real world; normal people, rather than just researchers.

As mentioned in the previous section, Mark Washburn had written a series of polymorphic viruses based on Vienna, because of this they really weren't infectious enough to spread very far.

This all changed in April when a new polymorphic memory resident EXE and MBR infector known as Tequila was found. The virus was written in Switzerland by two brothers, and was not intended to spread. However, as these things do, in the murky world of virus writing, it was stolen from the authors by a friend, who planted it on his father's disks. As the thief's father was a shareware vendor, soon Tequila was very widespread.

Not only was Tequila polymorphic and now widespread, it also used full stealth when run from the partition sector, and in files it used partial stealth, so it was pretty hard to spot.

Also in April another company joined the ranks of anti-virus vendors, this newcomer was Central Point. Others followed; Xtree and Fifth Generation. Most of these companies were actually re-badging other company's programs; most of them were products from Israel.

During the summer of 1991 saw another new virus that did something no other virus had done before. This virus known as Dir_II caused an epidemic. It used a fundamentally new way to infect files, as Kaspersky explains:

"It actually places a single copy of itself on the disk. Then it infects by setting the cluster pointers in directory sectors to point to itself."

According to one source: "*Dir_II is still the only example of this type of virus using this infection technique detected in the wild*". However, another claims that another existed, known as Dir_III [written in South America]. The difference between them is that Dir_III hides itself in a file, rather than using an unused cluster, as is the case with Dir_II.

On the positive side: "*The inaugural VB conference took place in 1991, its objectives were to present factual information about computer viruses, to demonstrate defensive procedures, to discuss probable future virus developments and countermeasures and to attempt to harmonise research efforts.*"

By the end of 1991 there were at least 900 viruses. Although, in many ways 1991 was relatively calm; the calm before the storm that broke in 1992.

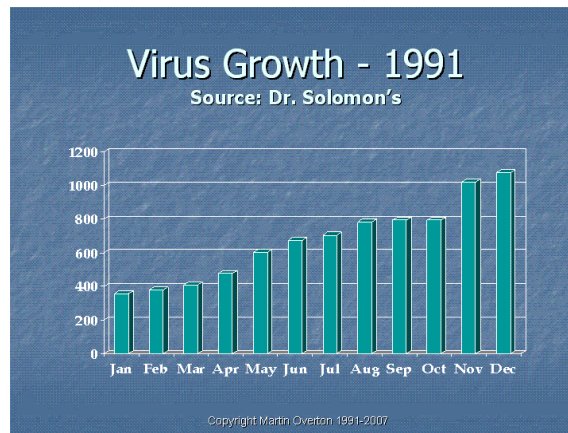


Figure 3- Virus Growth,-1991 – Running Total

2.3.3 1992

As mentioned in the previous section, Dark Avenger had promised a new and ground breaking virus, with levels of polymorphism that had never been seen before....

Joe Wells had this to say about it:

"Fridrik Skulason and Alan Solomon had wrestled with descriptions of variably modified decryption routines and coined the term "polymorphic" as it applies to computer viruses."

In January it finally arrived, but it wasn't a virus, it was something else, in many ways, something more feared by the anti-virus community. It was the Mutating Engine (MtE), the first we saw of it was in a virus called Dedicated, which used the MtE, so Dark Avenger kept his promise. Next, we saw the MtE itself.

Dr Solomon had this to say about it:

"This came as an OBJ file, plus the source code for a simple virus, and instructions on how to link the OBJ file to a virus to give you a full polymorphic virus. Immediately, virus researchers set to work on detectors for it. Most companies did this in two stages. In some outfits, stage one was look at it and shudder, stage two was ignore it and hope it goes away. But at the better R&D sites, stage one was usually a detector that found between 90 and 99% of instances, and was shipped very quickly, and stage two was a detector that found 100%. At first, it was expected that there would be lots and lots of viruses using the MtE, because it was fairly easy to use this to make your virus hard to find. But the virus authors quickly realised that a scanner that detected one MtE virus, would detect all MtE viruses fairly easily. So very few virus authors have taken advantage of the engine (there are about a dozen or two viruses that use it)."

Although, according to Kaspersky:

"Even after months of work, many antivirus companies were unable to reach 100% results in detecting well-known versions of polymorphic viruses created with the help of MTE."

So, in the end the arrival and fallout from MtE was not as bad as the anti-virus vendors had feared, but Dark Avenger was not finished yet.

A second strike from Dark Avenger left the anti-virus community reeling once more. This follow-up to MtE was called Commander Bomber. Dr. Solomon's explains why it caused such a stir:

"Before CB, you could very easily predict where in the file the virus would be. Many products take advantage of this predictability to run fast; some only scan the top and tail of the file, and some just scan the one place in the file that the virus must occupy if it is there at all. Bomber transforms this, and so products either have to scan the entire file, or else they have to be more sophisticated about locating the virus."

Commander Bomber was highly polymorphic, but interestingly it wasn't encrypted. Because of the new way it

infected files [inserting its code into the middle of a file] a new term had to be found to describe it.

During 1992 we started to see viruses that would fight back against anti-virus tools or would defeat them in novel ways, here are a couple of examples:

Starship was targeted at checksummers and avoided the protection offered by them by using a very simple technique. This was to only infect files as they are copied from the hard disk to the floppy disk; the files on the hard disk are never infected. Furthermore, Starship is a fully polymorphic virus which contains anti-debugging tricks and also infected the hard disk in a new way without changing executable code. It does this by changing the partition data, making a new partition as the boot partition. The new partition contains Starship, and this is run before it passes control on to the original boot partition.

Peach was written to target Central Point Anti-Virus's change inspector, to do this it deleted the database used by change inspector. The effect of this was that the antivirus acted as if it had been installed for the first time, and created [or in this case re-created] the database allowing the infected files to be included in the database as if they were clean. This is how Peach avoided detection, allowing it to slowly infect the entire system.

More virus construction kits followed in July and August of this year. Nowhere Man's VCL (Virus Construction Lab) had a nice Borland-like DOS interface and allowed the user to build viruses, including selecting payloads, by simply pointing and clicking. Later, Phalcon/Skism's PS-MPC also allowed viruses to be mass-produced with little or no programming skill required. By the end of the year dozens of viruses had been created using them.

Look in any anti-virus products virus list and you're sure to see lots and lots of VCL and PS-MPC viruses.

Other malware appeared that did something new, included:

- *EXEBug introduced CMOS modification to prevent clean booting.*
- *Invol was the first .SYS infector. It was also slightly polymorphic.*
- *V-Sign was the first polymorphic boot sector virus.*

All of this was only the warm-up act for what was to follow next:

Probably the greatest event of the year was the great Michelangelo media and vendor hype-fest. It is claimed that John McAfee was quoted as saying that the "*Michelangelo virus was on 5 Million PC's worldwide*"; other vendors soon joined in and jumped on to their soapboxes and predicted mass casualties. However, at that time it is doubtful that there even were five Million PC's in existence.

The result of the hype-fest caused PC users to go into a purchasing frenzy. When the dreaded date arrived, between 5,000 and 10,000 machines are actually believed to have gone down due to Michelangelo. The vendors that had been part of the hype-fest stated that this low body-count was a testament to their timely and accurate warnings. After March 6th, there were a lot of red-faced and discredited experts around.

In many ways the Michelangelo hype was a re-run, on a larger scale, of that seen with Datacrime, except that Michelangelo was actually in the wild. The fallout included the damaged credibility even to those people who were/had advocated sensible antivirus strategies. The damage cause by the excessive hyping of Michelangelo easily outweighed any gains made in awareness of the virus problem as a whole

Joe Wells made a note of the relevant headlines, just in the Los Angeles Times:

- *Michelangelo Virus Is Alive and Virulent, Waiting for March 6 - Feb 21*
- *Doomsday Nears for Infected PCs - Feb 20 Paint It Scary: Businesses, Others Scramble to Thwart*
- *Michelangelo PC Virus - Mar 4*
- *Michelangelo Virus Hits PCs at Some Firms Early - Mar 6*
- *Most Escape Brush With 'Michelangelo' - Mar 7*
- *Few Casualties From Dreaded Computer Virus - Mar 8*

He goes on to mention: "*The full extent of this media mayhem was documented by Pamela Kane in an article titled "Anatomy of a Virus Scare" (ISPNews of May/June 1992) and in her book P.C. Security and Virus*

Protection Handbook."

1992 also saw the first Windows virus, known as Win.Vir_1_4. This infected operating system executable files even though the virus was poorly coded. Furthermore, it had limited propagation ability, and had no special Windows functionality. Even so, it is still a first in computer virus history.

The author of Win.Vir_1_4 was also responsible for writing and releasing another polymorphic engine during this year (or possibly early 1993). This one was called TPE (Trident Polymorphic Engine). It is claimed that the author of TPE based it on the encryption algorithm he used in the Coffershop 3 virus. The first virus known to use the TPE engine is Giraffe.A. Dr.Solomon stated that:

"TPE is much more difficult to detect reliably than the MtE, and very difficult to avoid false alarming on."

Not to be left out, in October Nowhere Man, of the Nuke group based in the US, released the Nuke Encryption Device (NED). As expected this mutation engine was also trickier than MtE.

By now many anti-virus programs had started to use emulation and generic decryption techniques to deal with the increased use of encryption and polymorphism by malware authors.

We also saw people selling (or trying to sell) virus collections. To be more precise, these were collections of files. Some of which were actual viruses, others just were assorted clean files.

In America, John Buchanan was offering his virus collection which consisted of a few thousand files for \$100 per copy. Meanwhile in Europe, The Virus Clinic offered various options from £25. The Virus Clinic was later raided by the newly formed (at that time) Computer Crime Unit which operated out of New Scotland Yard in London, England.

On a similar theme, towards the end of year a new virus writing group had been started in England, this group was ARCV (Association of Really Cruel Viruses). The Computer Crime Unit had tracked them down and arrested them in a matter of a few months after they had first formed. All in all, ARCV flourished for about three months and managed to write a few dozen viruses, and gain members. The group's leader was called Apache Warrior. The proactive law enforcement position taken in England actively slowed, and in some cases, stopped the computer underground from getting fully established in the country.

A rather unusual VX BBS sprung up towards the end of 1992, the US Government was offering viruses to people who called the relevant BBS.

Building on the success of the inaugural Virus Bulletin conference, another was held, this time in Edinburgh, Scotland

On the antivirus vendor front, Symantec bought Certus International along with their proprietary antivirus product, Novi.

By the end of 1992 there were at least 1400 viruses known.

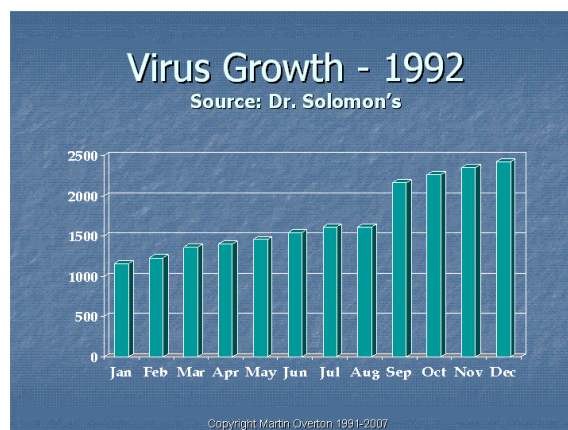


Figure 4- Virus Growth, 1992 – Running Total

2.3.4 1993

The spring of 1993 turned out to be a nerve-wracking time for many antivirus vendors: The first casualty of the commercial anti-virus business occurred early in the year. XTREE announced that they were no longer going to produce anti-virus software. The malware authors had claimed their fist scalp, and Microsoft released its own antivirus. This was known, not surprisingly as Microsoft AntiVirus (MSAV). The anti-virus was effectively based on Central Point AntiVirus (CPAV). MSAV was included in the standard delivery of both the MS-DOS and Windows operating systems.

Shortly after MSAV's launch a virus appeared in Germany that contained code to disable the resident [on-access] portion of this anti-virus product. That virus was called Tremor. It didn't help when it got included in a TV broadcast of software (received via a decoder).

Early testing conducted by independent testing laboratories indicated that the anti-virus was pretty effective⁴. The anti-virus community held its collective breath, and waited. The quality of the product and the meagre updates that Microsoft made available began to affect the effectiveness of the product and eventually the project was discontinued; the anti-virus community let out their collective breath, in an almost audible sigh of relief.

More anti-virus casualties appeared, this included Fifth Generation. On a positive note, Dr Solomon came up with the 'Generic Decryption Engine' as a solution to polymorphism becoming the de facto standard for all new malware.

In the middle of the year Joe Wells started a personal project to document exactly which viruses were being reported in the wild. He compiled a list of 100 viruses from various lists of "common viruses" and posted it to other members of CARO. In July this list became known as 'The WildList' with the intention of publishing it regularly.

As with 1992, we saw the quest for polymorphism continued as a number of new engines appeared:

Phalcon/Skism was not to be left out, in one of their 40hex electronic magazines they released their own, this was called DAME (Dark Angel's Multiple Encryptor).

Trident released another updated version of TPE [1.4]. This is more complex and difficult than previous versions and Lucifer Messiah, of Anarkick Systems had also taken version 1.4 of the TPE, modified it again [TPE 1.4b], and created a new virus called POETCODE that used it.

Trident had also been busy with other projects and this included Cruncher, the first virus that worked according to a principle first described by Fred Cohen. The Cruncher virus was a data compression virus. The virus automatically added itself to files in order to auto-install on as many computers as possible. A number of people tried to suggest that Cruncher was a "good" virus because it compressed file which gives the user more disk space.

Around the middle of the year, Trident, riding on a wave of publicity, received another sign that they were the group to be in, when Dark Ray and John Tardy decided to join them. As a sort of welcome present to Trident, Tardy released a fully polymorphic virus in just 444 bytes.

Other interesting viruses that appeared in the year include:

- The PMBS virus which worked in the secure regime of Intel 80386 processors. This was the first virus to use a processors protected mode and run DOS and other programs inside a virtual machine.
- The Strange virus which is a boot virus that exploits an undocumented bug in DOS versions, it is also the only stealth virus which is executed on the level of device interruption at INT 0Dh and INT76h.
- Carbuncle signalled a new generation of companion viruses.
- Emmie and Uruguay employed fundamentally new techniques to conceal themselves in the code of infected files.
- Monkey, which is loosely based on Stoned. However, it is full-stealth virus which stores the original master boot record (MBR) in an encrypted form. Unlike Stoned the virus does not leave the original

⁴ CPAV [which it was a re-badged version of] was never considered to be one of the best products available at the time, but it was adequate.

partition table for the infected drive in place. The end result is that the drive is effectively invisible to DOS if the system is booted from a clean floppy disk.

Just say no to FDISK/MBR!

FDISK /MBR was being touted as a "cure-all" technique to remove MBR infecting viruses. It became popular after Michelangelo hit. This supposed "cure-all" technique uses an undocumented option for the FDISK utility that is part of DOS. If you use the command FDISK /MBR, FDISK re-writes the code portion of the master boot record, but doesn't make any changes to the partition table in the MBR.

For viruses like Stoned and Michelangelo this overwrites the start of the virus code and leaves the partition information, effectively removing the virus. However, in the case of Monkey and similar viruses that don't preserve the partition information, using FDISK /MBR will still remove the virus from the MBR, but still leaves virus code in the partition table. The drive is then inaccessible to DOS.

The Virus Bulletin conference was going from strength to strength, this year it was held in Amsterdam in the Netherlands.

By the end of the year there were at least 3700 viruses known.

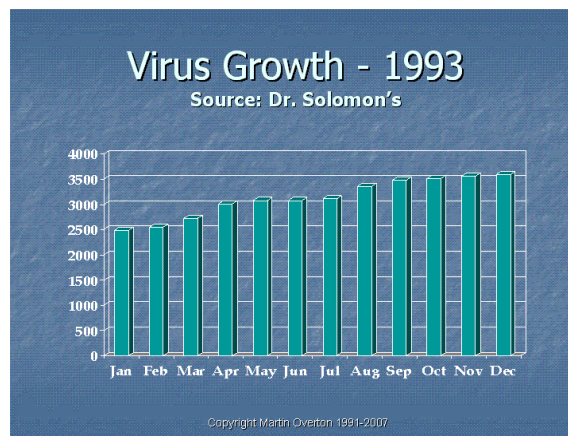


Figure 5- Virus Growth, 1993 – Running Total

2.3.5 1994

The year started with a bang, especially here in the UK as two extremely complex polymorphic viruses appeared in January. These were SMEG.Pathogen and SMEG.Queeg, both written by a British malware author known as The Black Baron. He placed the infected files on a number of BBSes, including VX ones. These viruses caused an outbreak and a fair bit of panic and hype in the media.

The viruses written by The Black Baron used yet another polymorphic engine; this one was called SMEG (Simulated Metamorphic Encryption Generator). We would be hearing more about the Black Baron before the year had ended as well as the following year.

A virus called Kaos4 was posted to the 'alt.binaries.pictures.erotica' news group in a file called Sexotica. The virus was encoded as text. It was downloaded by a number of users who decoded it back into an executable and then they executed it on their systems. In this way, visitors to this particular section of USENET caused a small epidemic. Luckily the virus was rather lame it didn't manage to cause a pandemic.

In a similar change of tactic by the virus authors, a virus known as Chill, or Chill Touch, was found to have been planted in some games offered on ZiffNet.

The first virus written for OS/2 was released by Phalcon/Skism in their latest 40hex edition. The virus called OS/2Vir_1 is a primitive overwriting virus, only groundbreaking because it was the first, and used OS/2 specific API calls.

Two notable viruses appeared during the year that became quite widespread. Both were polymorphic and multipartite. These viruses were called One_Half and Natas (Satan spelled backwards).

Natas is a memory resident stealth virus which infects the system hard disk's Master Boot Record (MBR), diskette Boot Sectors, .COM, .EXE, and .OVL files, including COMMAND.COM. The virus contains a destructive payload with a 1-in-512 probability of rewriting sections of the hard disk whenever a file or boot sector infected by the virus is accessed. This routine can also be executed by attempting to disassemble the virus. Even worse, when you got rid of the virus the hard disk's partition table may be damaged.

One_Half is an interesting multipartite stealth virus which contained a rather unusual payload. The virus would upon each reboot or boot, encrypt two unencrypted sectors on the hard disk, until it reached the half way point on the infected computers hard disk [starting from the end of the drive and working towards the middle]. At that point a message would appear stating '*Dis is one half, Press any key to continue ..., Did you leave the room?*' At which point you probably realised your computer was infected. However, simply removing the virus was not going to solve the problem, as the contents of half your hard disk are now encrypted.

A number of other viral firsts appeared during the year, these included:

3APA3A (Zaraza) was the first virus that infected the core DOS file called IO.SYS. Not only that but it is also a boot sector virus, but on floppy disks only.

Shifting Objectives targeted Object files rather than executables or boot sectors. This virus was very much targeted at software developers and if a system used by such a developer was infected then each program they compiled could contain a copy of the virus

Dichotomy was the first virus to split itself into two parts; half would be placed in one host file and the other half, in another different file.

On the anti-virus front Symantec acquired Central Point on the 4th of April and AntiViral Toolkit Pro was launched in September by Eugene Kaspersky.

I attended my first conference; EICAR's 2nd conference which was held in the UK this year. EICAR '94 was remarkable in more than one way, as that year, apart from being a very good conference; they allowed a virus writer (Tim Gaskin aka Ice9) to speak! Virus Bulletin held yet another conference, this time they revisited Jersey in the Channel Islands on the 8th and 9th of September.

The very first Microsoft Word and Excel macro viruses were allegedly created by Joel McNamara in December⁵, however, they were never found in-the-wild. Little did anyone know at the time just how significant this would be until August of the following year.

The year was also notably for the hoax that appeared, this being the Good Times hoax which caused widespread panic. GoodTimes claimed to spread via the Internet and infected computers via email. Bear in mind at this time, there were no e-mail worms.

Oh, yes The Black Baron was arrested in August of this year, but more on that in the next section.

By the end of the year at least 4500 known viruses existed.

⁵ However, the source code was not made available to the anti-virus community until after Concept was found. So, we don't really know for certain if his macro viruses were created before it, or not.

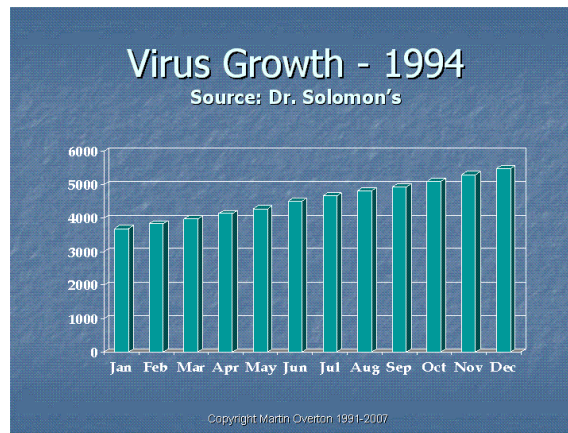


Figure 6- Virus Growth, 1994 – Running Total

2.3.6 1995

On the 16th of January, The New Scotland Yard's Computer Crime Unit took 'The Black Baron', now unmasked as Christopher Pile, 26, from Plymouth to court for writing and distributing viruses. The unemployed Pile was accused of authoring the Queeg and Pathogen viruses as well as the SMEG polymorphic generator. On the 26th of May Pile was convicted and sentenced to 18 months in prison.

The virus authors were mainly doing the same sort of thing during the year, more complex and obfuscated code as well as lots of new variants of existing viruses. However, as witnessed during the previous year, some malware authors were starting to look at new platforms to attack. This year was somewhat pivotal, both for malware and for other reasons.

On the malware front we saw the first fruits of this research, a virus in a Batch file [.BAT], this was definite first⁶. The virus was called Winstart.

However, it wasn't until August that the rug was pulled out from under the World's feet, for two reasons:

1. Windows 95 (aka Chicago) finally arrived on the 24th of the month. This caused all sorts of problems for the malware authors, as many viruses, especially complex stealth file and boot viruses, would not work correctly under Windows 95.
2. Sarah Gordon, a researcher at Command Software Systems, had found and analysed a new type of virus⁷. Jimmy Kuo suggested a name the next day; Concept. Concept was a Microsoft Word macro virus and at the time it was believed to have been the first of its kind. Within a single month it had been found all over the world.

Concept was a macro virus written in WordBASIC (which is an interpreted programming language) and this is built into the Microsoft Word environment.

The anti-virus community was quick to point out that the idea of macro viruses was nothing new. However, most of the product developers were quite unprepared for Concept and did not have any code ready; even if they did it wasn't going to be that simple.

Dealing with Concept involved more than simply releasing new signatures or an updated database. The problem was that Concept runs in the MS-Word environment. The MS-Word environment is the operating system that Concept replicates within, and that operating system was not very well understood outside of Microsoft.

Most anti-virus product developers had to make major changes to their products to deal with Microsoft Word macro viruses, like Concept. You can clearly see how much the anti-virus community were caught out by Concept, in Virus Bulletin's July, 1996 testing report: Eight out of twenty-four scanners tested still failed to

⁶ Although Ralf Burger did include an example of a batch file virus in his book, it is not known if it was found in-the-wild. It also depended on external DOS programs to work.

⁷ Another source claims that Sarah was not the one who discovered Concept as an infected file was allegedly sent out on a CD by Microsoft. So Concept effectively appeared in many countries at almost the same time.

detect Concept almost a year after it had first been found.

Once the Macro Virus stable door had been opened, the stream rapidly grew to a torrent. Other macro languages were targeted also, Green Stripe, a virus for AmiPro appeared and also spread rapidly.

The previous year (1994) saw the GoodTimes hoax appear, so what did one of the virus authors do? He, Qark of the VLAD group, created a virus which he named Good Times, however, the antivirus community spoiled his fun by calling it GT-Spoof. The virus, a COM and EXE infector, used a new polymorphic engine known as 'RHINCE' (Rickety and Hardly Insidious yet New Chaos Engine) created by another VLAD member called Rhincewind.

On the anti-virus front, during the spring ESaSS (the developer of ThunderBYTE Anti-Virus) and Norman Data Defense Systems (Norman Virus Control) announced an alliance.

The Virus Bulletin conference was held in Boston, USA from the 20th-22nd of September. This was also the year that I started to estimate virus growth and keep detailed information regarding the actual growth of viruses.

By the end of this year there were at least 7559 virus known to exist.

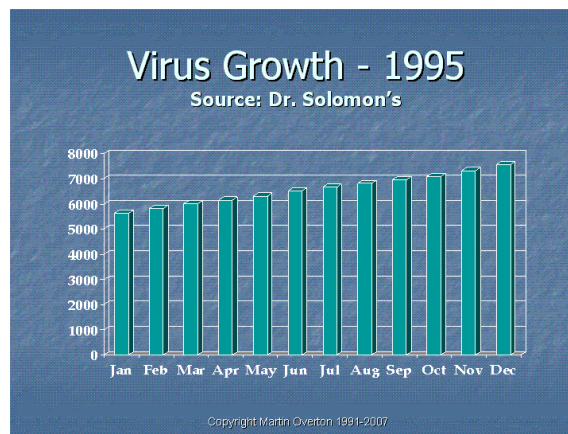


Figure 7- Virus Growth, 1995 – Running Total

2.3.7 1996

Boza, the first virus for Windows 95 virus appeared, just to start the year off on the right foot. However, it was a pitiful virus and not likely to turn up in the wild. It was, however, widely hyped by anti-virus vendors and the press as was another virus this year, that one was called Hare.

In March we saw the first virus epidemic for Windows 3.x. This epidemic was caused by Win.Tentacle and for starters it had infected a hospital computer network and several other organisations in France. This virus was also the first Windows virus detected in the wild; before this Windows viruses had been kept in collections, or as part of the electronic magazines offered by virus writing groups. Before Win.Tentacle burst onto the scene we had really only seen boot sector, DOS, and macro viruses in the wild.

In June the OS2.AEP virus appeared; this was the first virus which infected OS/2 EXE files. Before this, most OS/2 viruses had written themselves to the file location, destroyed the file, or employed the companion virus technique.

July saw the macro theme continued; Laroux became the first Microsoft Excel virus seen in the wild. However, as previously mentioned it may not have been the first Excel macro virus created. It was found in the wild in two oil drilling companies in Alaska and South Africa respectively and almost simultaneously. As with Concept the year before, Laroux was first discovered and analyzed by Sarah Gordon of Command Software Systems.

Just to drive home the fact that virus writers were now heavily focussed on Macro viruses, towards the end of the year, two virus writers known as Nightmare Joker and Wild Worker both released a construction kit each for macro viruses. These were the 'Word Macro Virus Construction Kit' and 'Macro Virus Development Kit'.

Windows 95 OSR2 (aka Windows 95B) arrived on the 26th of August, and with it a new file system, known as

FAT32. This caused all sorts of problems for not only the malware authors, as many viruses, especially complex stealth file and boot viruses, would not work on 95B. The problems caused by FAT32 also hit the anti-virus industry hard as many products were not compatible with it. Bear in mind the changes made by Microsoft for Windows 95 were not implemented to solve the virus problem.

In December the first memory resident Windows 95 virus appeared. It loaded into the system like a VxD driver, intercepted file calls, and infected them.

Throughout the year numerous viruses for Windows 95/NT were developed, and at least a hundred macro viruses appeared (including Nuclear, NOP, and Wazzu). Many of these viruses used completely new techniques and innovative methods such as stealth capability and polymorphism. Consequently, computer viruses reached a new evolutionary level, now aimed at 32 bit operating systems. However, not surprisingly; they followed the same evolutionary style of development as we had seen with DOS viruses ten years before.

Towards the end of the year, another antivirus vendor, Cheyenne Software who made InocuLAN, was bought out by Computer Associates.

This was also the year that I submitted my first abstract for a conference paper to Virus Bulletin and much to my surprise it was selected, and I was honoured to be asked to present. So, at the Virus Bulletin this year, which was held in the highly exotic location of Brighton, [about 20 miles from where I live] England from the 19th-20th September, I made my conference debut as a speaker on the corporate stream presenting a paper called 'Anti-virus in the Corporate Arena.'

By the end of this year there were at least 11241 viruses known to exist.

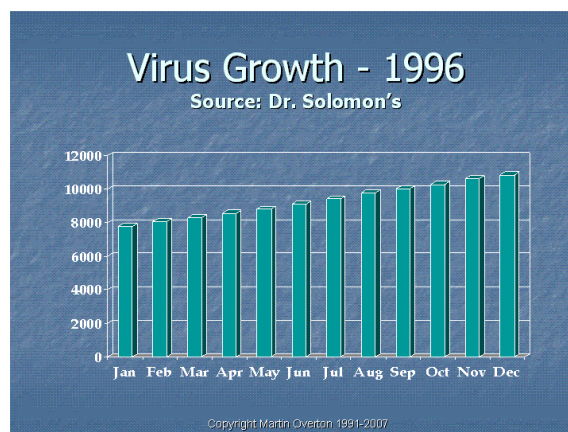


Figure 8 - Virus Growth, 1996 – Running Total

2.3.8 1997

In February, the virus authors once more showed that they were looking at other platforms to foist their malware on. The latest operating system under scrutiny was Linux. The result of this scrutiny was a virus called Bliss and it was a first for Linux.

The release of Microsoft's Office 97 during the year made sure that once more malware authors would target it, especially those whose forte was now macro viruses. Not surprisingly many of the first Office 97 macro viruses turned out to be little more than those that had come before. However, new macro viruses written specifically for Office 97 did appear. The limited payloads (or in some cases the total absence thereof) of macro viruses created for MS Word 5.0 and Excel 5.0 resulted from a new and very different version of Visual Basic for Applications; VBA 5.0, previous versions of Office had used VBA 3.0.

March arrived and so did an extra surprise; 'ShareFun'; a macro virus for MS Word 6/7 which also spread via e-mail, especially MS Mail. This started a new chapter in computer viral history, as the e-mail worm was born.

April brought us the Homer virus which was the first network worm which used FTP to propagate.

June brought us the first self-encrypting virus for Windows 95; Win95.Mad.

November brought us The 'Esperanto' virus. It was a bungled attempt to create a virus which would be able to infect DOS, Windows and (possibly) MacOS; in other words, a multi-platform virus.

The malware authors would often use IRC as a channel of communication, and not surprisingly they found that they could do other things with some of the IRC clients available at the time. Here's what Kaspersky had to say about the phenomenon:

"In December of 1997, the antivirus world publicized the appearance of a fundamentally new type of computer worm which spread via IRC channels. An analysis of mIRC, one of the more popular IRC utilities showed a dangerous security loophole. The directory for files downloaded via IRC coincided with the directory which held the SCRIPT:INI command file. The SCRIPT:INI file, which contained the body of the worm, could therefore be transferred to a remote computer, where it would automatically replace the original command file. When restarted, mIRC would activate the malicious code, and the worm would then send itself to other users. This error was quickly corrected and the rather primitive IRC worms had disappeared by summer. However, multi-component IRC worms which actively searched for SCRIPT.INI files (in mIRC clients), EVENTS.INI (in pIRCh) clients, and others. later appeared, working in a similar way to email worms; the user would receive an EXE, COM, BAT, file, which when launched, would replace the original command file."

One of the more important events of the year, as far as the anti-virus world was concerned, was the segmentation of KAMI; the anti-virus division became an independent company, to be known as 'Kaspersky Labs'. However, Kaspersky went further than this split; and in October they signed an agreement with Finnish company Data Fellows (later renamed as F-Secure Corporation) who wanted to include another antivirus engine in their latest product, FSAV (F-Secure Anti-Virus). So, FSAV would use the F-PROT, Kaspersky and another, third engine they had developed, in a single antivirus product. This was another first.

This year was a bit of an odd one as some anti-virus company's waged war on their competitors. It wasn't a pretty sight; the following comes from Kaspersky and explains the issues rather well⁸:

"1997 will also long be remembered as a year of petty squabbles. Several scandals evolved at the same time between some of the larger antivirus manufacturers. At the beginning of the year, McAfee announced that they had discovered a 'bookmark' in the programs of one of their main competitors, antivirus firm Dr. Solomon's. McAfee's announcement continued in saying that if Dr. Solomon's antivirus program discovered several viruses during a scan-check, then it completed its work in an elevated mode. In other words, if the program worked in a normal mode in normal conditions, then in testing for several viruses it switched to an intense mode (or in McAfee's words, a 'cheat mode') which allowed the detection of viruses previously invisible to Dr. Solomon's in normal scanning mode. As a result, the testing of uninfected discs showed good speed results and the scan tests of virus collections showed good detection results.

Dr. Solomon's response was not long in the waiting, and the company soon filed suit against McAfee's recent marketing campaign which claimed that McAfee was, 'The Number One Choice Worldwide. No Wonder The Doctor's Left Town'. This was an obvious reference to Alan Solomon, the founder of Dr. Solomon's who had in fact, earlier transferred control of his company to its senior management.

Perhaps even more scandalous was the affair of the Taiwanese developer Trend Micro who accused two of the leading antivirus companies, McAfee and Symantec, of violating its patent on virus scan-checking technology via Internet and electronic mail. Shortly afterward Symantec leapt into the fray with its own accusations, alleging that McAfee was guilty of using code from Symantec's Norton AntiVirus."

The year ended on a more positive note with McAfee and Network General announcing their intent to merge companies. This new company would be known as Network Associates Inc (NAI). The idea was that merging would allow both companies to explore other computer security technologies.

As with the previous year, I submitted an abstract to Virus Bulletin, and to prove that lightning can strike twice, they again accepted it. This time it was a paper called 'FAT32 - a new problem for anti-virus or viruses?' This

⁸ This wasn't really a cheat-mode; it just turned off exact identification if it found four or more different viruses on a system. However, this wasn't the case if you used it for disinfection/removal of viruses, only scanning.

time I was promoted to the Technical Stream. The conference was held in San Francisco, USA on the 2nd -3rd of October. VB2007 also broke new ground, for VB anyway, as one of 'the enemy' was to present at the conference; yes an ex-virus writer, known as Stormbringer!

By the end of this year there were at least 17238 viruses known to exist.

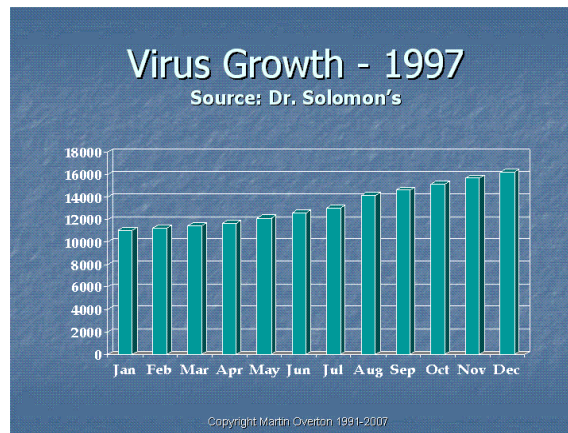


Figure 9- Virus Growth, 1997 – Running Total

2.3.9 1998

The beginning of the year brought an epidemic primarily targeted at French speaking countries. This outbreak was caused by a whole family of viruses Win32.HLLP.DeTroi which not only infected Win32 EXE files, but were also capable of transmitting information about victim machines to the author of the virus.

January also brought us a new initiative from Virus Bulletin known as VB 100%. This would entail regular testing of antivirus products against viruses known to be in the wild. Those that pass this test are awarded a VB 100% certificate for that one test. Many products now regularly achieve VB100% status, but they didn't at first.

When February arrived so did the Excel4Paix (or Formula.Paix) macro virus. This new macro virus infected Excel tables in a new way. February also brought us polymorphic Windows32 viruses, such as Win95.HPS and Win95.Marburg. The emergence of Windows32 polymorphism caused antivirus developers to develop new methods, or update existing detection methods, for polymorphic viruses which, until these two viruses had appeared had been only required for DOS viruses.

Microsoft Office applications continued to be targeted:

Access went first, in March. The first virus to infect Access files was known as Accesiv.

Powerpoint fell in December. The first virus to infect PowerPoint files was known as Attach, others quickly followed. However, scanning and disinfecting PowerPoint files caused the anti-virus vendors another headache, as Kaspersky explains:

"Files of this MS application use an OLE2 format which determines the way in which viruses can be scanned for in DOS and XLS files. However, the VBA modules in PPT format are stored in compressed format which meant that it was necessary to design new algorithms to decompress them and facilitate antivirus searches. Despite the complexity of what would seem like a simple task, almost all antivirus companies have integrated into their products the necessary functionality to defend against PowerPoint viruses."

We also saw the emergence of macro viruses which could move from one Office application to another. Cross was the first, just infecting Word and Access files, but the most complete one was called Tristate and it could infect Word, PowerPoint and Excel files.

In May, a new virus appeared, called Red Team. It was the first virus to infect Windows EXE files and distribute copies of itself using the Eudora email client.

June brought the Win95.CIH virus, which by the end of the year was responsible for a global outbreak. Some bright spark thought that the name wasn't new-worthy enough and renamed it 'Chernobyl' as the trigger date was, coincidentally, the same as that of the anniversary of the accident.

The virus was written in Taiwan by a then unknown author, we now know that CIH was written by Cheng Ing Hau. What made the virus a first was its payload: depending on the day of infection, the virus would attempt to erase the computer motherboards Flash BIOS chip. Unfortunately, many motherboards no longer used ZIF-sockets for BIOS chips, those that did, meant that the BIOS chip could be simply replaced. Otherwise you had to replace the whole motherboard.

I personally witnessed motherboards having to be replaced when the payload triggered on certain Compaq machines. These machines used Flash chips that were soldered directly on to the motherboards.

August saw first malicious executable Java module appear; known as Java.StrangeBrew.

Also in August a family of password stealing Trojans appeared, known as the PSW family. We also saw the release of remote administration utilities. BackOrifice is just one example of this, and when it arrived in August it caused more than a bit of controversy.

September brought a new threat known as AutoStart to Apple users. This was helped by its inclusion on distribution disks for Corel Draw 8.1.

November saw the release of three viruses that infected Visual Basic Script files (VBS files). VBS is often used to create active web pages and content.

Yet more changes occurred in the antivirus vendor market during this year. In May, IBM and Symantec announced their unified efforts to develop an antivirus product. The combined product was to be distributed by Symantec under the same name; IBM Anti-Virus would cease to exist. Towards the end of September, Symantec announced the continuation of its buying spree, with the purchase of the antivirus business from Intel Corporation and a few weeks later, Symantec snapped up QuarterDeck for \$65 million.

The quick growth of Symantec, mainly via acquisitions, didn't go unnoticed by its competitors, especially NAI. In a somewhat hurried fashion, on August the 13th, NAI purchased one of its main competitors; Dr. Solomon's at the cost of a \$640 million stock swap.

To complete this years buying frenzy, EliaShim, a developer of the antivirus product E-Safe was bought in December by Alladdin Knowledge Systems.

Virus Bulletin had another conference, this year it was held in Munich, Germany from the 22nd-23rd of October.

By the end of this year there were at least 39,559 viruses known to exist. Yes, the numbers had more than doubled since the end of the previous year.

Do you want to know part of the reason for this massive growth? Well, some kind hearted soul decided that the anti-virus companies were not busy enough, so they created almost 14,000 new viruses using one of the known virus creation tools; PS-MPC. They then sent these 14,000 new variants, on a CD to each of the anti-virus companies, expecting it to cause them much hair pulling and gnashing of teeth.

However, a number of vendors didn't even break sweat; after the initial shock wore off, as many vendors only needed to make a few thousand new signatures, or update a smaller number of generic (family) signatures to detect the majority of these new variants.

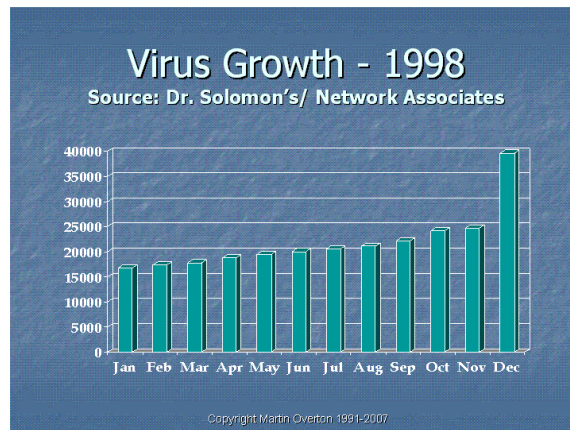


Figure 10 - Virus Growth, 1998 – Running Total

You can clearly see the spike caused by those 14,000 samples given to the anti-virus vendors in the graph in Figure 10, above.

2.3.10 1999

January of this New Year had an unwelcome start; a global epidemic of the Happy99 virus (also known as Ska) which was created by a virus author called Spanska. Many consider this to be the first modern-day worm and it opened a new chapter in the history of malware. Happy99 relied on MS Outlook to spread. It also had an interesting payload, when executed it displayed a window wishing you a 'Happy New Year 1999', and supplying a firework display. It also used USENET to spread, as well as e-mail.

Around the same time a new and interesting macro virus for MS Word was found. It was named Caligula and what was different about it was that it searched through the system registry trying to find PGP (Pretty Good Privacy) keys. If any PGP keys were found, the virus sent them to a remote server using FTP.

February brought us another first, this being SK; the first virus which infected Windows HLP files.

If January had been a bit of a rude awakening, then March was the morning after from hell.

On the 26th of March Melissa, the first macro virus for MS Word with Internet worm functionality was found. When a system was infected by Melissa, it scanned the Outlook address book and sent copies of itself to the first 50 addresses it found, via e-mail, using the e-mail address of the user on the infected system, so it appeared to have been sent by someone they already knew and possibly trusted. As a result of this, Melissa managed to cause significant outbreaks on systems across the world, these included companies like Microsoft, Intel and Lockheed Martin.

What's worse is that when Melissa sent out copies of itself, it could also use an existing Word document on the infected system, infect it, and then send that out instead. This document was chosen at random and could have contained anything including confidential or personal information.

Law enforcement agencies reacted very quickly to the outbreak caused by the Melissa virus. The author of the virus was discovered and arrested; he was a 31 year old programmer from New Jersey in the US. His name was David L. Smith.

PrettyPark arrived, and caused a flurry of outbreaks during the year. It is notable for two reasons. First, it ensured that it was invoked every time an executable was launched by making changes to the registry key used to launch Executable files on Windows. Secondly, it was able to spread via e-mail using addresses found in the address book and could also spread using IRC. It also used IRC to allow the author to connect remotely to the infected system.

May the 7th brought us a new script virus which targeted Corel DRAW. It was known as the Gala virus (aka GaLaDRieL). It was written in the Corel SCRIPT language and became the first virus capable of infecting Corel DRAW files as well as Corel PHOTO-PAINT and Corel VENTURA.

July brought us yet another script virus. This one was called Freelinks, it was unusual because it used encrypted VBS and copied itself to the root of any shared drives it found. Like Melissa it mass-mails itself, but it doesn't infect Word documents. The worm includes a copy of itself in all e-mail it sends out; the file it attached was called LINKS.VBS. Like PrettyPark it also spread via IRC.

Just to keep everyone busy, we saw yet another virus outbreak at the very beginning of the summer. This time it was ZippedFiles (also known as ExploreZip). The virus came in the form of an EXE file and once a system became infected ExploreZip would destroy data files of some of the more popular applications [.DOC, .XLS, .PPT as well as three common source code file formats]. A modified version appeared at the very end of the year. This virus was changed so that the body of the virus was compressed using the compression tool known as Neolite. At the time none of the antivirus programs available handled this compression format, so the virus managed to bypass them.

In August, an Internet worm named Toadie (or Termite) was detected. This virus was written by a very outspoken virus writer known as RaiD from the virus writing group SLAM. Apart from the usual routines to infect files in DOS or Windows, the virus attached copies of itself to emails sent via Pegasus, a popular e-mail client, and finally it attempted to spread through IRC channels.

In November, the world was once more in the grip of a new e-mail worm. What made this different from earlier worms spread via email was that this one didn't use files attached to the e-mail. Worse still, is that if you opened or even previewed the worm e-mail on vulnerable mail clients, your computer became infected. The first of these new '*just read the e-mail and get infected*' worms was Bubbleboy, and it was almost immediately followed by another; KakWorm. Viruses of this type exploited a vulnerability in Internet Explorer; Microsoft issued a patch for the vulnerability the same month.

December wasn't much better, what with more new viruses using new techniques, such as Babylonia, which according to Kaspersky:

"The very dangerous and complex Babylonia virus turned a new page in the history of virus creation. It was the first worm which was capable of remote self-rejuvenation. Every minute it would connect to a server in Japan and download a list of virus modules. If it found viruses there fresher than on the infected computer, then it immediately downloaded them."

An article written by Greg Hoglund was published in Phrack 55⁹ on the possibility of a Windows NT Kernel rootkit. He discusses a 4 byte patch which, as he describes "*removes ALL security restrictions from objects within the NT domain. If this patch were applied to a running PDC, the entire domain's integrity would be violated.*" From this article he went on to develop, as he advertises it: "*The original and first public NT ROOTKIT¹⁰*". Pandora's Windows box was now open!

And then there was Millennium Fever:

The security industry was evenly split about the Y2K problem, also known as the 'Millenium Bug'.

This meant that quite a bit of software could not handle the change in date from the 31st of December 1999 to the 1st of January 2000 properly. The effects of this could be minor, or catastrophic, depending on the affected software and how [or where] it was used. This though was not what most of the security industry was most concerned about, they were more worried about what the hackers and virus authors had up their sleeves (apart from their arms).

The suggestions ranged from '*nothing much, it's just another day*' to '*they have thousands of new viruses ready to be released on January the 1st and/or there will be major hack attacks carried out, causing untold damage*'. As a person that was volunteered to watch IDS and other security systems for this type of activity, I was sat in front of a bank of computers from 6pm on the 31st of December 1999, until 6am on the 1st of January 2000. Did the world end, were there anymore hacking attacks than usual, loads of new viruses unleashed? No. I can honestly say it was about as eventful as most days, in fact less so than we had already seen earlier in the year.

⁹ The article can be found here: <http://www.phrack.org/phrack/55/P55-05>

¹⁰ Source: <http://www.rootkit.com/project.php?id=11>

There were more acquisitions on the anti-virus vendor front, as Cybec was swallowed by Computer Associates (CA). This meant that CA had added another antivirus product to its collection, having purchased Cheyenne Software at the end of 1996.

As with the previous years, I submitted an abstract to Virus Bulletin, and they again accepted it. This time it was a paper called ‘*Viruses & Lotus Notes - Have Virus Writers Finally Met Their Match?*’ This was once more on the Technical Stream. The conference was held in Vancouver, Canada on 30th September - 1st of October. This was the anti-virus communities nearest thing to a millennium party.

By the end of this year, and the end of the 90s, there were at least 48,271 viruses known to exist.

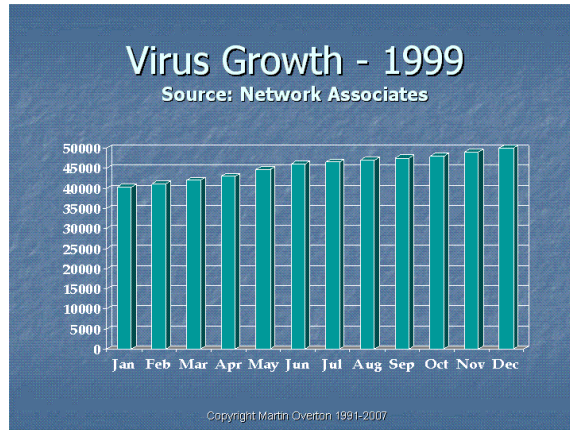


Figure 11 - Virus Growth, 1999 – Running Total

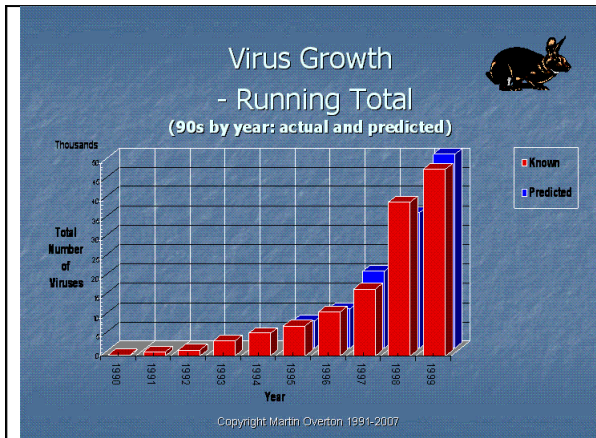


Figure 12 - Virus Growth, 1990-1999 – Running Total

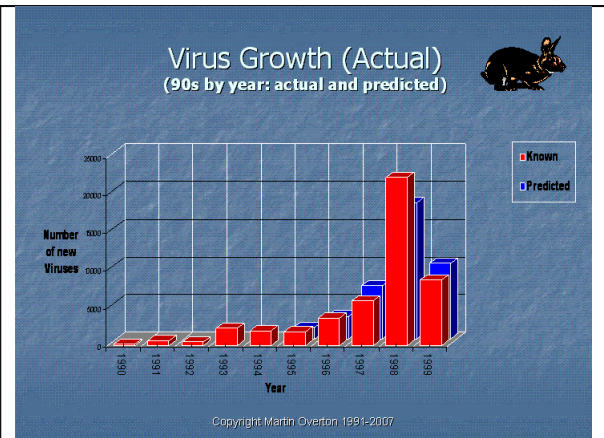


Figure 13 - Virus Growth, 1990-1999 –Actual, Per Year

2.4 The Noughties

2.4.1 2000

So, another year has started and a new Millennium too¹¹. Will it bring anything new? You bet!

The onslaught against Microsoft applications continued with Visio becoming the next target of virus authors. Kaspersky had this to say about it:

Microsoft had not even finished announcing the release of a fully functional commercial version of their operating system when members of the underground group 29A set Inta loose. The virus was the first to infect Windows 2000 files. Shortly after, two viruses emerged almost simultaneously, Unstable and Radiant which marked Visio's demise."

If we thought that script viruses were going to fade away this year, then we got a nasty wake-up call in May, when the infamous 'LoveLetter aka I LOVE YOU' virus burst onto the scene and it quickly eclipsed Melissa, BubbleBoy and KakWorm as the fastest spreading virus ever seen. Once the virus infected a new system it destroyed a range of files and then proceeded to send copies of itself to all addresses in the MS Outlook address book [not just 50 as we had seen with Melissa]. The availability of the source code, which was not obfuscated or encrypted in any way, guaranteed that new variants of the virus would appear. At least until the virus authors got sick of writing them or computer users got wise, neither happened for quite a while.

The 6th of June arrived and the Timofonica virus was detected. Timifonica was the first computer virus that employed, in a limited manner, mobile phones. As Kaspersky explains:

"In addition to spreading via email, the virus sent messages to random mobile phone numbers in the MoviStar cellular network, which belonged to the global telecommunications giant, Telefonica. The virus had no other effect on mobile phones despite the fact that many mass media outlets were quick to name Timifonica the first 'cellular' virus."

In July, the group known as the Cult of Death Cow [or CdC] produced a new version of Back Orifice virus (BO2K). It was just a prettier version of what we had seen previously with a few new features to try and get it accepted as a commercial remote access program. In other words, CdC were trying to go commercial.

Also in July we saw the appearance of two interesting new viruses, these were:

- *Star was the first virus designed to infect AutoCAD files.*
- *Dilber was extremely unusual as it contained code from five other viruses including CIH, SK, and Bolzano. Depending on the date, Dilber activated processes from one of the borrowed components, earning it the nickname, the Shuttle Virus.*

In June the media had hyped Timofonica as a mobile phone virus, which it wasn't, this may have influenced some virus authors, as in August we saw a brand new platform being targeted, this being PalmOS. The first virus for it was Liberty, but it wasn't a virus it was a trojan. Upon installation, it deleted files but was incapable of replicating. In September, Liberty was joined on the PalmOS by the first true virus for it, this being Phage. It was a classic virus-parasite program which after installing and infecting files, it proceeded to delete them and record its own code.

September brought us another new virus, using a new technique. This virus was called Stream. It was capable of manipulating the ADS [Alternate Data Streams] of the NTFS file system, used by NT and 2000. The virus itself was fairly harmless; the technique of accessing and using ADS was new. Furthermore, no antivirus was, at that time, able to scan NTFS Alternate Data Streams.

October came and brought us:

- *The first virus for PIF files (Fable).*
- *The first virus using PHP script-language (Pirus).*

¹¹ Although the new millennium didn't really start until January 1st 2001, as there wasn't a year zero!

It also brought us Hybris. This virus was written by the Brazilian virus writer Vecna, who had written Babylonia last year. In Hybris he had further developed the techniques used in Babylonia taking into account his earlier coding mistakes. The main innovation in Hybris was the use of websites and list servers (alt.comp.virus in particular) to load new modules of the virus to infected computers. If it was easy to simply take a website down, then list servers were an ideal alternative for spreading as they were less easy to take down. To make it harder for the antivirus vendors, Hybris used a 128-bit RSA key for identifying modules actually written by the author.

This was the year that email again proved itself to be the best infection vector. According to Kaspersky Labs' support statistics:

“Approximately 85% of all registered infection occurred via email.”

The virus authors hadn't given up targeting Linux either; there were 37 new viruses and Trojan programs created for the Linux operating system during this year.

And just in case you hadn't noticed, before 2000, macros viruses had been the most commonly encountered viruses by most computer users, this year saw that crown being removed from macros viruses and being given to the script viruses instead. The era of the macro virus was coming to an end, they weren't finished, but they would never recover enough to take the crown back again.

Virus bulletin held their conference in Orlando, USA from the 28th-29th September. Unfortunately, for me, I was unable to attend VB this year. However, something interesting happened during VB2000. This was the initial discussions about creating a new user group. This would be known as AVIEN [Anti-Virus Information Exchange Network]. Run for the users, by the users, no vendors allowed!

By the end of this year, there were at least 56,236 viruses known to exist.

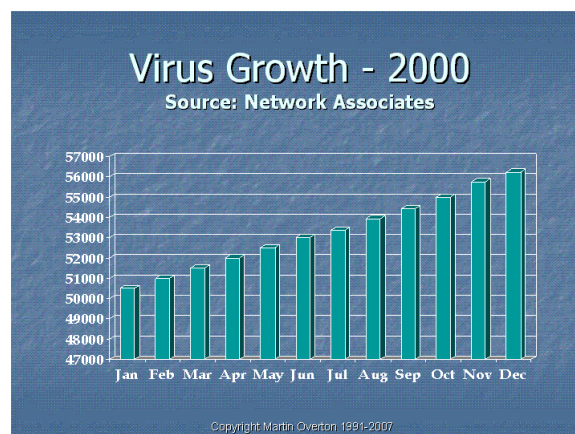


Figure 14 - Virus Growth, 2000 – Running Total

2.4.2 2001

The move from classic viruses to worms progressed rapidly during this year, driven by the massive increase in the use of the internet by both those of us that had started using the internet before it was synonymous with the world-wide-web, and the massive influx of new users aka 'newbies'.

It seems that social engineering was gaining in popularity this year, at least by the hoaxers. By March at least 10 virus hoaxes had already been seen. The malware authors were still somewhat suspicious of such a non-technical way to get their creations on to peoples systems, although some were starting to come round to the idea as you'll see.

The year started off badly, well for the Linux evangelists anyway, as during January, a worm called the Ramen [or just Ramen] started to spread, infecting Red Hat Linux machines running version 6.2 and 7. It did this simply by using three well known vulnerabilities in wu-ftpd, rpc-statd and lpd.

In February we saw a new VBS worm called OnTheFly, although most people still call it the Anna Kournikova worm. The worm spread worldwide in just a few hours by promising pictures of the tennis player.

By March we had the Magistr virus and worm as it infected files on the local machine as well as spreading like a normal mass-mailing worm. It was also a rather nasty virus as it used a similar payload to that of CIH; overwriting motherboard flash BIOSes.

On the 9th of May, we saw yet another VBS worm generated by the VBSWG virus kit, the same kit used by OnTheFly in February. This new worm was called Homepage. As part of its infection routine the worm would attempt to open one of four 'adult' web sites in the infected systems web browser.

Unix was once more the target when the Sadmin worm starting spreading in June. This worm also used known vulnerabilities, like Ramen, this time Sun Microsystems Solaris based systems were the target.

June was also the month that Macintosh users got a bit of a shock, as they too were targeted with a mass mailing worm known as the Mac.Simpsons worm.

July brought us a new threat, this being the first of the 'file-less' worms. This was the Code Red worm which exploited the vulnerability in the Index Server ISAPI Extension of Microsoft's Internet Information Services. A second version was released on August the 4th; this was dubbed Code Red II, and was a major rewrite. Both of these worms were a major problem for anti-virus software because of the way the spread, and the lack of disk I/O, as the worm was never written to the hard disk this meant that anti-virus products couldn't detect them. Most companies ended up using network sniffers/packet filters or IDS to stop it getting into their infrastructure. Unfortunately, by the time they put these defences in place it was often too late.

July also brought us Sircam, another worm which used local office documents as carriers for itself when it mass-mailed itself to another victim. Like Nimda it could also spread via network shares.

On September the 18th a new fast spreading worm was released, this was called Nimda (Admin backwards). It was different in many ways from previous Wintel worms as it spread via e-mail as an e-mail worm, open shares, including Samba shares on Linux/Unix boxes, as well as vulnerabilities in Internet Explorer, using backdoors left by Code Red II and the Sadmin worm. According to F-Secure:

"Nimda infected 2.5 million computers, taking just one day to infect local area networks and individual desktops globally."

Nimda mainly spread via the Unicode exploit allowing it to infect vulnerable web servers, which when visited by users that used vulnerable versions of Internet Explorer, Nimda was automatically installed on their computer, infecting local executables. The Nimda infected computer then searched for open shares to infect, e-mailed itself out to other victims via MAPI and then started scanning the internet for more vulnerable web servers to infect.

The mass-mailing Windows worms just keep coming: On October the 26th, we saw Klez, during November we saw Badtrans.B which contained keylogging features too, and to cap it all, in December we saw Goner which was written in Visual Basic, and it also spreads via ICQ and IRC.

We also saw numerous variants of LoveLetter (aka ILoveYou) during the year, this kept users and antivirus vendors well and truly on their toes.

File sharing networks weren't ignored either as the Internet worm Mandragore attacked the Gnutella network.

2001 was the year of the worms, especially mass-mailing and network worms for Windows, although *NIX didn't get off easy either. Macro viruses continued to decline, as script viruses increased their hold. It was also the year that everyone, Windows, *NIX, and even Mac users should have learnt that you need to install patches, if you don't, then you make your PC an easy target for the malware authors.

As with the previous years, I submitted an abstract to Virus Bulletin, and they again accepted it. This time it was a paper covering '*Hoaxes and Other Electronic Ephemera*'. This was once more on the Corporate Stream. The conference was held in Prague, Czech Republic from the 27th-28th September, just over two weeks after 9/11.

By the end of this year there were at least 59,483 viruses known to exist.

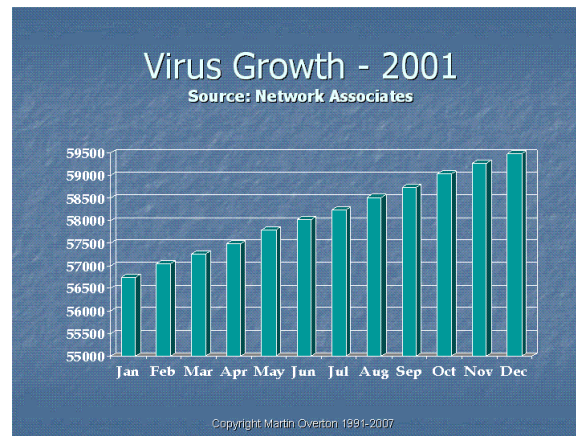


Figure 15 - Virus Growth, 2001 – Running Total

2.4.3 2002

January started off with two new worms targeting Shockwave and .NET, LFM (Shockwave worm) and Donut. Both of these worms were designed to spread in the .NET environment. Both worms were proof of concept viruses and no infections were registered.

Then Myparty arrived! This e-mail worm propagated using an attachment name resembling a web address ('www.myparty.yahoo.com'). All this time we had been telling people not to open attachments, and telling e-mail senders, that they should offer links to the file instead, and it was starting to sink in. So, what do the virus authors do? They create Myparty, an e-mail worm which sends an e-mail with an attachment named as if it were a hyperlink. The file attachment was a Windows executable, and although its extension was .com, Windows took a peek inside and saw that it was really an .exe file, and promptly executed it as such.

In February we saw a new network worm which spread via MSN Messenger, this was called Coolnow.

March saw the advent of a new e-mail worm which posed as a Microsoft software patch. This e-mail worm was called Gibe.

May brought us a Kazaa worm which was widespread on the file sharing network. This worm was named Benjamin.

We also saw SQLSpida worm which targeted Microsoft SQL servers.

Finally, in May of this year, the author of one of the previous years worms Melissa [1999] was sentenced and went to jail for 20 months.

June was pretty busy, as we saw yet more VBS script worms. A new version of the Yaha worm; Yaha.E was found and it spread quite widely.

Just to make sure that the *NIX community didn't feel left out; we also saw the Scalper worm in June. This targeted FreeBSD-based Apache web servers.

August brought another surprise, a trojan was found in the OpenSSH distribution package of the main distribution server.

September, which like August is often a busy month for the anti-virus community, brought us Bugbear; an e-mail worm which quickly spread world-wide. It also brought us Slapper another worm which targeted Apache web servers. F-Secure had this to say about it:

"The most interesting characteristic of Slapper was its ability to create a distributed peer-to-peer attack network by means of which the writer of the worm was able to take control of any infected server. This feature was probably created to launch distributed denial-of-service attacks with the help of the worm. F-Secure's specialists managed to disassemble the peer-to-peer protocol used by the worm and the threat posed by the worm was eliminated in a few days."

October came and it delivered Opaserv to us; Opaserv looked for unprotected Windows 95 and 98 computers and broke the password protection on shares. Another MSN worm appeared called Fleming. It also brought an extensive attack against the Internet's 13 master domain name servers. This was almost certainly a dry run for something big being planned.

November arrived along with more trojans being found hidden in the distribution versions of tcpdump and libcap. Again this was found on the main distribution server.

The year ended with yet another Kazaa worm; Lolol and an attempt to spread a new version of Yaha via mailing lists run by Yahoo.

Throughout the year users continued the hoax-fest from the previous year; we saw new hoaxes such as 'JDBGMGR', 'Ace-?', 'SULFNBK', and 'Virtual Card for You' as well as many of the old ones. The interesting thing about the hoaxes like JDBGMGR and SULNBK is that they managed to convince users to delete files which were part of the operating system, all by the power of social engineering.

Many of this year's e-mail worms were different than what we had seen before, no more reliance on MAPI, Outlook or other e-mail clients to send out copies of themselves. No, most of these new e-mail worms were able to send directly to SMTP servers; either local ones, or directly to ones on the Internet.

This year was also the start of the move by the computer underground to turn their hobby, into a business. As Kaspersky said:

"There was a significant increase in malicious programs designed to commit financial fraud. These programs stole passwords, confidential data, Internet access information and other data that allowed virus writers to make money by using the harvested data."

It was also the year that saw the rise of Asian virus writers and the general decline of virus writers from the US.

There were a few other odd things that occurred during the year that were throwbacks, as Kaspersky explains:

"Interestingly enough, macro viruses rose to the fore among classic viruses this year. Macro viruses for MS Word - Thus, TheSecond, Marker and Flop were the most widespread. These viruses had first appeared in the late 1990s, but they resurfaced in 2002. The most likely reason is increased numbers of Windows users who were all sure that macro viruses were a thing of the past. Inconvenient security measures were abandoned and the result was a second round of old viruses. The majority of infections were caused by Elkern, CIH, FunLove and Spaces."

As with the previous years, I submitted an abstract to Virus Bulletin, and they again accepted it. This time it was a paper covering 'When Worlds Collide'. This was once more on the Corporate Stream. The conference was held from the 26th-27th September 2002 at the Hyatt Regency, New Orleans, LA, USA.

By the end of this year there were at least 64,034 viruses known to exist.

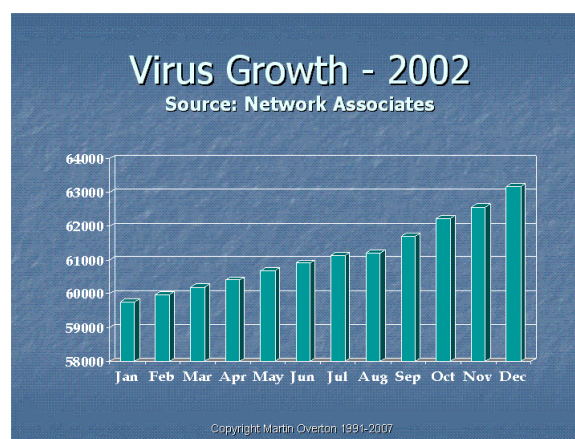


Figure 16 - Virus Growth, 2002 – Running Total

2.4.4 2003

Even before the end of January, the users of the internet got a very nasty wake-up call called Slammer. It targeted a known vulnerability in Microsoft's SQL server (again). Slammer was the first file-less worm which fully showed the capabilities of so-called flash-worms; capabilities which had been foreseen several years before.

Kaspersky explains:

"On January 25th, 2003, within the space of a few minutes, the worm infected hundreds of thousands of computers throughout the world, and increased network traffic to the point where several national segments of the Internet crashed. Experts estimate that traffic increased from 40% - 80% in a variety of networks. The worm attacked computers through ports 1433 and 1434 and on penetrating machines did not copy itself on any disk, but simply remained in computer memory. If we analyse the dynamics of the epidemic, we can assert that the worm originated in the Far East."

In fact it is known that Slammer infected over 75,000 vulnerable systems in under 10 minutes. It was able to do this as the worm itself was only 376 bytes long, and so it fitted inside a single TCP/IP packet. Added to that was the fact that the worm used UDP to send copies of itself to new IP Addresses, because it used UDP it didn't need to connect to any of the targeted systems, it was a fire and forget worm, that's why it could infect so many systems in such a short period of time.

January also brought us the first member of the Sobig virus family, Sobig. Little did we know how much trouble this family of e-mail worms would cause before the end of the year.

When May came, so did the Fizzer worm. This caused a global outbreak and the worm was heavily linked to spammers. This was another sign that the computer underground was starting to work together more closely than ever before. Normally spammers, hackers and virus writers hardly spoke to each other, except to call each other rude names and generally taunt each other.

Sobig was also back in May; variants B and C appeared and they both spread widely.

June arrived and brought us more e-mail worms including:

Another member of the Bugbear family, B, targeted at banks, spreads globally. The new variant of Bugbear exploited the well-known IFRAME vulnerability in MS Outlook to automatically launch itself from infected messages. It caused one of the most significant email epidemics of the year.

F-Secure had this to say about the new Bugbear variant:

"This virus was interesting because it tried to steal information from banks and other financial institutions. When Bugbear.B infected a computer, it checked if the affected computer was located in an internal network of a known financial institution. If this was the case, the virus gathered information and passwords from the system and sent them to ten pre-defined e-mail addresses."

To this end, the worm carried a list of network addresses of more than 1300 banks. Among them were network addresses of American, African, Australian, Asian and European banks. As soon as this functionality was discovered, F-Secure warned the listed financial institutions about the potential threat. The response time of the F-Secure Anti-Virus Research Unit was 3 hours 59 minutes from the detection of the worm to the release of an anti-virus update. F-Secure also published a free tool to clean systems affected by Bugbear.B."

More members of the Sobig clan turned up, D and E. Interestingly the D version appears to be a bit of a dud, as it failed to spread. However, E becomes the most wide spread variant so far this year.

August was a horrible month for computer users as wave after wave of new worms arrived. For those of us responsible for fighting these outbreaks, we hardly had time to catch our breath, let alone sleep, before we had to deal with yet another outbreak.

It started off fairly quietly, with a new worm called MiMail which used the latest vulnerability in Internet Explorer to activate itself. The vulnerability allowed binary code to be extracted from HTML files and executed. However after that it was downhill all the way.

Next up was Blaster (aka Lovesan) on the 12th of August. It showed just how vulnerable Windows was. Like Slammer, Blaster exploited a vulnerability in Windows in order to replicate itself. The difference was that Blaster used a vulnerability in the RPC DCOM service working under Windows 2000/XP. This led to almost every Windows Internet user being attacked by it, even if their computer wasn't vulnerable.

Barely 6 days later, on the 18th, along came Welchia (aka Nachi). This worm infected computers already infected by Blaster. Once Welchia had infected a system it destroyed Blaster and tried to download and install Windows security updates. In other words, it was an anti-virus virus. However, the cure was worse than the disease: Welchia generated far more network traffic than Blaster (the disease it was supposedly written to cure) and was the reason for most of the severe system outages in companies in mid-August.

The very next day the 19th saw the biggest and baddest of the Sobig family, Sobig.F.

Kaspersky had this say about Sobig.F:

"At the peak of the epidemic, Sobig.f, which was first detected in August, could be found in every 20th email message. The virus writers who created the Sobig family, were aiming to create a network of infected machines with the aim of conducting DoS attacks on arbitrarily selected sites and also to use the network for spam attacks."

And F-Secure had this to say about some of the functionality they found in Sobig.F:

"F-Secure's researchers continued studying the code of the worm and eventually found a functionality hidden in the virus code: computers infected by the worm were synchronized with an atomic clock to activate on Friday, August 22nd at 19:00 UTC. At this clock strike they would contact one of 20 pre-defined computers around the world and receive more specific instructions from them. When this functionality was found, F-Secure had less than 30 hours to disconnect those 20 computers from the net in order to stop the activation. By working in close co-operation with Internet operators, CERT units and the FBI, this was accomplished just in time. The last computer that needed to be disconnected was shut down only 15 minutes before the deadline."

The whole of September belonged to just one e-mail worm; Swen. It first appeared on the 18th of the month, masquerading as a patch from Microsoft. It managed to infect several hundred thousand computers throughout the world. The author of the virus exploited frightened users who were still nervous after the recent Lovesan and Sobig.f epidemics. Repeat after me "Microsoft never sends updates as e-mail attachments", lather, rinse and repeat, ad infinitum.

The anniversary of 9/11 brought the usual crop of ambulance chasing malware authors out to play. Examples of 9/11 worms included: Mimail.B and Vote.K, which contain text "WORLD TRADE CENTER, REVENGE"

October wasn't quite as quiet as September as we saw more than one worm causing problems, again. The Mimail.C worm was detected and as part of its payload it launches denial of service attacks. Sober appeared, this worm sent out infected e-mail messages, which look as if they have been sent from anti-virus companies

During November we saw ten, yes ten, new variants of the Mimail worm. The variants attacked anti-spam sites, among others, or stole users' credit card details.

The only new file format/application targeted during the year was MapInfo; the virus was found in the wild and named MBP.Kynel.

Furthermore, for all the worms we saw during the year, what most users didn't see was the slow and steady growing army of Bots, crawling from computer to computer, infecting and signing in for duty, waiting for orders to be issued. This scourge would be the one big move that the growing band of professional cyber-criminals would increasingly rely on from now on.

A paper was also published on the FU rootkit which uses what it describes as ‘Direct Kernel Object Manipulation (DKOM)’. This step is described by some as the third generation of ‘rootkit’ techniques. FU is described thus by its author: “*The FU rootkit can hide processes, elevate process privileges, fake out the Windows Event Viewer so that forensics is impossible*”. The latest version can “*even hide device drivers*”.

As with the previous years, I submitted an abstract to Virus Bulletin, and they again accepted it. This time it was a paper covering ‘*Worm Charming: Taking SMB Lure to the Next Level*’. This was once more on the Corporate Stream. The conference was held from the 25th-26th September 2003 at the Fairmont Royal York, Toronto, Canada.

By the end of this year there were at least 84,111 viruses known to exist.

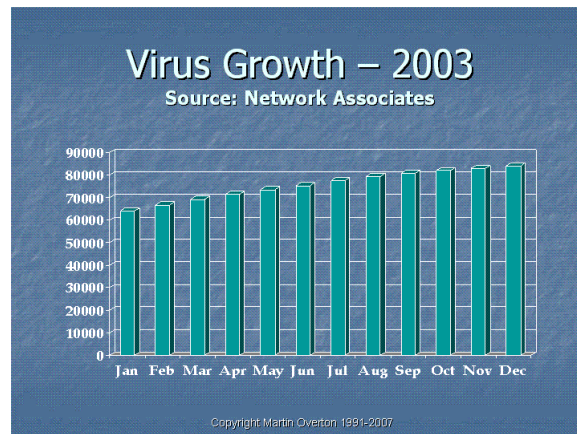


Figure 17 - Virus Growth, 2003 – Running Total

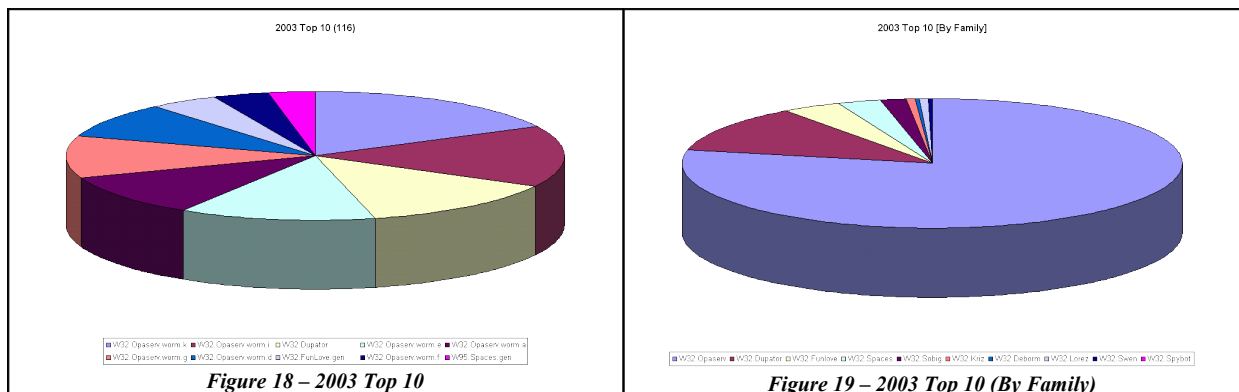


Figure 18 – 2003 Top 10

Figure 19 – 2003 Top 10 (By Family)

The graphs shown in Figure 18 and 19 are created from data using my own malware honeypots and my WormCharmer.

2.4.5 2004

2004 was a real 'game of two halves'. What do I mean by that?

The first half of the year was mainly dominated by the ‘Malware Wars’ between the authors of MyDoom, Netsky and Bagle, this resulted in dozens of variants for each family. The peak of this war was in April, by May it had started to slow and by the end of June the war had degenerated into the occasional scuffle.

The second half of the year was more dominated by the Bots and other network worms, The Agobot, Rbot, SdBot and Protoride families were particularly fecund; producing new variants with increasing frequency and features to boot. The SDbot family by the end of 2004 contained over 3,000 variants [members] in its family.

The other major shifts during 2004 were the rise of Phishing, which grew around 5,000 percent over the previous year¹². Spyware also became a major headache for home users and showed signs that it would be a headache for many companies during the year. We also saw the move from very visible 'in-your-face' malware,

¹² Source APWG (4,000% growth between November 2003 and April 2004)

to more sneaky and stealthy worms which were almost invisible, as they spread without user intervention. The methods used included: Open Windows Shares, exploiting vulnerabilities in the OS and applications and carrying password files to perform dictionary attacks on Windows shares.

The years top performers were; Netsky.P which accounted for more than a quarter of all reported virus incidents (source: SOPHOS) and it was the most prevalent threat for eight months. Furthermore four other Netsky variants also made it into the top ten. The other big worm that caused a lot of grief was Sasser. The thing to note here is that the author of Netsky and Sasser are one and the same; Sven Jaschan, an 18 year-old German who was arrested in May 2004. Ironically Jaschan was 'fingering' by one of his friends who were after the Microsoft Bounty of \$250,000 USD.

It also appears that changes in legislation in many parts of the world drove malware authors further underground and increasingly into the waiting arms of organised crime and spamming syndicates.

Spammers, scammers and organized crime syndicates were increasingly working together with malware authors. This was evident due to the rise of malware being used by organised crime to steal information, such as credit card and bank details via the use of remote-access-trojans (RATs), Phishing, key-loggers and worms, as well as cyber-extortion.

The malware problem in 2004 mainly concentrated on the Windows platform. No new major malware were detected for Linux. The Apple Mac was also targeted by a 'rootkit' during 2004. A small but growing number of viruses aimed at PDAs or mobile phones were discovered. The source code for the Cabir worm was published.

During the last few weeks in December we saw the rise of PHP worms, originally just targeted at a specific Bulletin Board package, but then extended to try and attack all PHP based websites. In all cases the worm uses a search engine to find new hosts to attack.

So, let's look at the main malware events of 2004:

Month	Malware	Comments
Jan	+MyDoom.a	The Malware war breaks out!
	Bagle.a	Both Bagle and MyDoom turn infected PCs into spam proxies.
	Netsky.a	Anti-Bagle/MyDoom worm
Feb	Doomjuice	Worm which used the MyDoom backdoor
	+#Netsky.b	
	+Netsky.c	
	+#Netsky.d	
	Vesser	Worm which used the MyDoom backdoor and also used SoulSeek P2P application to spread.
Mar	Witty worm, Blackice (ISS)	According to Joe Stewart of LURHQ "A vulnerability alert for the ISS products was released on March 18, and the worm [Witty] began spreading March 20. The writer of the worm either knew of the vulnerability before the announcement or wrote and tested the worm in less than two days."
	*+#Netsky.p	
	*#Netsky.q	
Apr	*+#Bagle.aa	
	+Netsky.z	
	#Netsky.x	
	#Lovgate.w	Used poetry and suggestive attachments as part of its social engineering.
May	+Sasser.a	Sasser arrived a mere two weeks after the vulnerability is used was patched, however most systems weren't!
	#Sober.g	Another mass-mailer with good social engineering.
	*Bagle.ab	
Jun	Korgo.a-u	Drops keylogger
	+#Zafi.b	Multi-lingual mass-mailer using social engineering.
	Cabir	First mobile phone infector (via Bluetooth)
Jul	Duts	First Windows/CE Pocket PC virus Another prevalent variant of Bagle
	*Bagle.ai	
Aug	Bradord	First PocketPC backdoor
Sep		
Oct	Linux rootkit	Spam message points users to fedora-redhat.com which downloads the rootkit to the system.
	Opener	Apple Mac malware
	*Bagle.bb	
	*Bagle.bd	

	*Netsky.ag	
Nov	Bofra	Used a vulnerability that went un-patched for 30 days. According to a number of sources, ad-servers used by many well-known companies and news services were hacked and were used to infect vulnerable systems that connected to them, or on the websites where their ads were served to. Used web-links to the malware rather than attachments.
	*MyDoom.ah	
	Skulls Trojan	Symbian OS Trojan
	*+#Sober.j	2004 part 2's biggest outbreak
Dec	Atak.a	Christmas social engineering.
	*Zafi.d	Multi-lingual mass-mailer using Christmas social engineering.
	Santy/Spyki	Worm which attacks PHP based websites

* *Top Ten Corporate Malware [McAfee]¹³ + Top Ten Malware of 2004 [SOPHOS]¹⁴ # Top Ten Malware of 2004 [F-Secure]*

Jaschan [the author of Netsky and Sasser] now ironically works for a computer security firm (SecurePoint), as does the malware author known as Benny of the 29A group (employed by the Czech company Zoner).

2004 was a very good year for malware authors being caught, not only Jaschan, but also the only known female malware author: Gigabyte (aka Kim Vanvaeck), who is well known for her 'obsession' with Graham Cluely of SOPHOS. Other arrests included: Alex G author of Agobot, the author of Blaster.B, Cabrotor, Magold, Randex, Peep and VBS/Lasku.

It was also a good year in arresting other cyber-criminals, such as scammers and spammers.

2004 saw the continuation of the trend that was born the previous year, in that organized crime had become the friend and paymaster of many malware authors. Large numbers of malware were written to make money, or steal data to make money during 2004. This includes many of the 'bots' which are herded by bot-shepherds (aka bot-herders or bot-masters) and these are sold to spammers, scammers and extortionists so that they can carry out their crimes using the bot infected.

What had become abundantly clear is that the window between a vulnerability being found and it being exploited was now smaller than ever and malware authors were increasingly including exploits in their creations, along with social engineering and multiple infection vectors to maximise their penetration potential.

Social engineering was alive and well, during 2004, and came to a PC or mobile device near you. It seems that not only were the 'Click-a-holics' alive and well but also those that lack even the slightest shred of scepticism and take everything at face value.

The data from the end of 2004 suggested that 5 percent of Phishing scam recipients actually fall for them and disclose their personal and financial data, such as credit card numbers, pins, pass phrases, account numbers, mothers maiden name, ISP, eBay and PayPal login details...the list goes on, no wonder identity theft was growing so fast during 2004.

We also saw the massive growth of Trojans, now let's be clear Trojans don't spread on their own, they are either invited guests, such as applications masquerading as useful tools, or more frequently as files dropped by other malware, such as a viruses, bots or worms.

In fact a significant proportion of malware released in 2004, carried not just Trojans, but also Spyware, Keyloggers and other uninvited guests which gate-crashed many Windows PC.

Many malware authors were regularly trying to disguise their creations using packers and compressor, such as UPX, ACE, PEX, etc. In some cases multiple packers/compressors were used, along with tools to modify the headers or other identifiers that these tools were being used.

As with the previous years, I submitted an abstract to Virus Bulletin, and they again accepted it. This time it was a paper covering 'Canning More Than Spam With Bayesian Filtering'. This was once more on the Corporate Stream. The conference was held from the 29th September – 1st October 2004 at the Fairmont Chicago, IL, USA.

¹³ All descriptions of the malware listed can be found here: <http://vil.nai.com/vil/default.asp>

¹⁴ All descriptions of the malware listed can be found here:
<http://www.sophos.com/virusinfo/topten/200412summary.html>

The number of known viruses grew by 28,327 in 2004. By the end of this year there were at least 112,438 viruses known to exist.

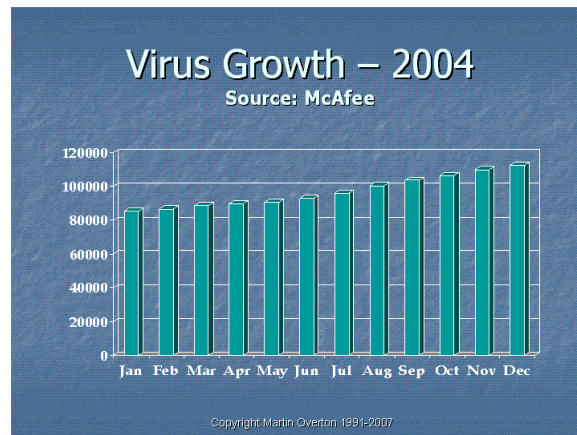


Figure 20 - Virus Growth, 2004 – Running Total

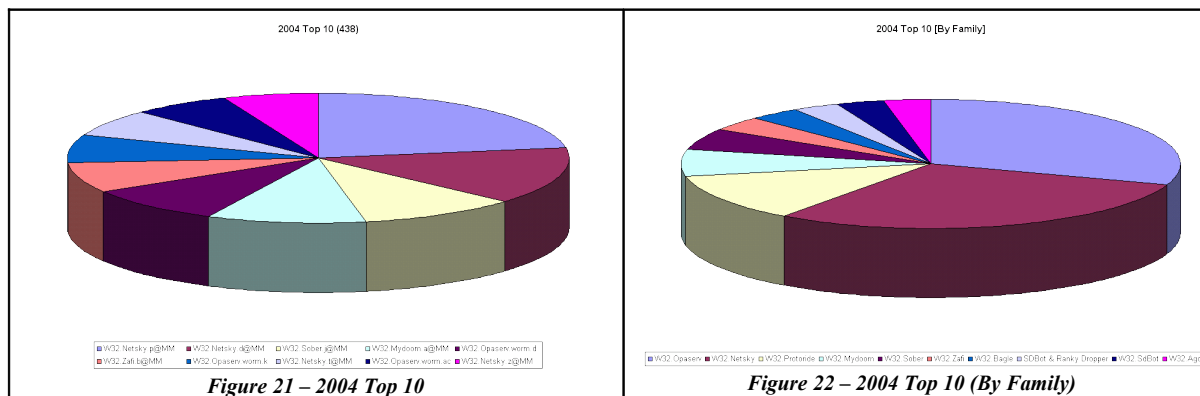


Figure 21 – 2004 Top 10

Figure 22 – 2004 Top 10 (By Family)

The graphs shown in Figure 21 and 22 are created from data using my own malware honeypots and my WormCharmer.

2.4.6 2005

January to June

According to F-Secure http://www.f-secure.com/2005/1/data-security-summary-2005_1.pdf the number of virus outbreaks almost halved during the first half of 2005 when compared to the first half of 2004. This is not that surprising as the first half of 2004 was dominated by the Mydoom, Netsky and Bagle war.

E-mail borne malware was fast becoming extinct as malware authors move to using other infection vectors or links instead of attaching malware. The other trend that was occurring was the move back towards Trojans and using social engineering to get users to infect their own computers. SOPHOS found that only 1 in 91 e-mail were viral compared to 1 in 35 for the same period the previous year.

Instant Messaging and the worms that have been created to use IM as an infection vector have been around for a number of years. However, the first half of 2005 saw a significant growth in the number of malware that uses IM as a vector to spread.

The vast majority of these IM worms were created in Visual Basic and seem to be mainly written to target users of Microsoft's MSN Messenger, although other IM clients have been targeted too during the year.

It seems that the source code for several of these worms had been made available on the Internet and this code was being actively used as a 'basis' by new malware authors; the so-called script-kiddies.

The main families that were very active include:

Name	Notes
------	-------

Bropia	More data can be found here: http://www.viruslist.com/en/viruses/encyclopedia?virusid=81593
Kelvir	More data can be found here: http://www.viruslist.com/en/viruses/encyclopedia?virusid=81593
Mytob	This is a bot with mass-mailing and IM functionality. More data can be found here: http://momusings.blogspot.com/2005/05/27/mytob-madness/

All the data during 2005 indicated that we were seeing a certain amount of evolutionary testing of IM malware. Unfortunately, this trend could indicate that we would see more aggressive and faster spreading malware via the IM clients and networks in the future.

In many ways this was a carbon-copy to what we saw in the development of peer to peer malware and we may well see the same conclusion; peer to peer malware tailed off sharply during 2004, would the same happen with IM malware?

The notable thing to mention with regard the use of IM as an infection vector is that the vast majority of malware that uses this vector tended not to send files, but links to files instead. Why this was the case is unclear, although it may have something to do with IM worms mainly being the domain of script-kiddies and the increasing security in IM clients and networks.

Data or disks being encrypted by malware is nothing new, however we seemed to be seeing a rebirth of this technique to extort money from those that get infected during 2005.

In May most anti-virus companies added detection for a new malware which encrypted files and effectively held them to ransom; this malware was known as: Virus.Win32.GpCode [Kaspersky Lab], TROJ_PGPCODER.A [Trend Micro] and Trojan.Pgpocoder [Symantec].

However, the original version was found in December of 2004 by Kaspersky and interestingly they also found the second variant later that month, so why did it taken Symantec [and other AV vendors] so long to add detection to their products?

During the first half of the year we saw the rebirth of virus technology which has been in decline for the previous 3-4 years, as worms and Trojans took over. However, it seems they may have been enjoying their own renaissance during 2005.

During 2005 we saw several new 'true' viruses including Virus.Win32.Bube and Virus.Win32.Tenga.

Bube actually injects its code into the explorer.exe system file; whereas Tenga will infect all suitable files in a given directory in one go, similar to the way Nimda worked as a file infector.

The growth in the numbers of bots, and the increase in functionality, infection vectors used and uses of bots had been nothing short of 'breathtaking' during the first half of 2005.

The Mytob family, at the end of the first half of the year, stood at 299 variants, not bad for a new family that only appeared in February of 2005. This family of bots had effectively taken over as 'top-dog', consigning both the Agobot and the SD/IRCBot family to the back seat.

July-December

In the first half of 2005 we saw a massive growth in malware authors using Instant Messaging as an infection vector for their creations. However, in the second half of 2005, this 'development' almost ceased as malware authors switched back to using known vulnerabilities as their preferred method of gaining access to a box.

In August we saw a new bot based on Mytob, but instead of spreading via e-mail or IMs, this new bot used the Plug and Play exploit code [MS05-039] as its only way to spread from system to system. Later versions also used e-mail and IM as well as other older exploits to facilitate its spread once the vast majority of vulnerable systems had been patched against the original Plug and Play hole. This new bot was named Zotob, although some anti-virus vendors have since renamed it as a Mytob variant.

More details on the Zotob variants and their capabilities can be found here: <http://momusings.blogspot.com/2005/10/13/zotob-madness/>

Several large media firms were infected by Zotob and they mistakenly believed that the scale of the infection was massive; with many millions of systems infected globally. This however turned out to be wrong. Yes Zotob was the biggest security event in 2005, but it wasn't on the scale of Blaster, Slammer or Nimda.

At the end of September a new mobile malware was found, known as Cardtrap. What was different about Cardtrap was that it didn't only target Symbian OS; it also wrote two Windows viruses [Rays and Padobot] to any memory card found, this effectively gave it the ability to infect multiple platforms. Rays also appeared pre-installed on over 4,000 MP3 players from Zen.

The second half of 2005 also saw malware authors looking at 'games consoles', such as the Sony PSP and Nintendo's DS. The results from these experiments were interesting and rather worrying as it often resulted in devices effectively turned into expensive paper-weights.

During August, we saw a new threat emerge, this being viruses using Microsoft Shell, it was still a beta project codenamed 'Monad' at the time. The malware author wasn't content with just creating one new malware, created five all targeting Microsoft MSH. The viruses were published in a virus writing zine.

Cyber blackmail and extortion came to the fore during 2005. In September we saw more developments on this theme, with the release of Krotten aka Agent.il. Instead of encrypting files and demanding a ransom, ala GPCode, this one modified the system registry to seriously restrict what users could do. This made infected systems very hard to use, as access to Regedit and the Task Manager was blocked. It also stopped the user from closing Explorer and Internet Explorer windows and blocked the ability of being able to run a command prompt. What did the author want? He requested that you sent him 25 Hryvna [Ukrainian currency, about 5 USD], and he would restore [disinfect] your system.

In November an interesting press release was published by the Bavarian police, stating that a new version of Sober might be imminent. The very next day a new Sober variant was found, this came to be known as Sober.Z. The e-mail that this Sober variant created and sent out with a copy of itself attached, often claimed that the recipient had infringed copyright or had illegal files/pictures on their system. All in all, it was very successful, not because it used any exploits, as it didn't. It relied on social engineering techniques, which were very effective in getting the recipient to open the attachment and infect their system.

Also during November a surprising discovery suddenly catapulted 'rootkits' back into the news from their relative obscurity of the last two decades. We saw the debacle of a company using 'rootkit' [stealth] techniques and software for the purposes of DRM [Digital Rights Management]. To say that once discovered this caused a storm is a massive understatement. This eventually led to the company [Sony] apologising, recalling all products that used the technology, and being hit with a number of class-action suits. These cases have now been settled. However, the impact of the use of 'malware' author tactics was significant, and the problem escalated once the real malware authors found they could use the technology to hide their creations from anti-virus and other security tools. The first malware to do this was Brepibot.

On the 26th of December strange WMF files [Windows Meta Files, graphic files] started to show up, these when analysed were found to contain executable code which would, when executed, download other files from a web site and execute them. The first wave of these malicious WMF files were placed on websites where any visitor using Internet Explorer as a browser would render these bogus graphics files and run the embedded code. In most cases these resulted in Spyware getting installed. Other versions appeared that would install bots, Trojans and other malware.

Of course Microsoft had no patch for this new vulnerability in their software at the time; luckily several security researchers stepped forward and created 'temporary' patches or workarounds for the problem. Finally on January 6th 2006 Microsoft gave in to pressure and released their own 'official' patch for the problem [MS06-001].

As with the previous years, I submitted an abstract to Virus Bulletin, and they again accepted it. This time it was a paper covering '*Bots and Botnets - Risks, Issues and prevention*'. This was once more on the Corporate Stream. The conference was held from the 5th - 7th October 2005 at The Burlington, Dublin, Ireland. I also wrote a paper for, and presented at the EICAR 2005 conference, held in Malta at the end of April. The paper was called '*Anti-Malware Tools: Intrusion Detection Systems*'.

The number of known viruses grew by 56,369 in 2005. By the end of this year there were at least 168,807 viruses known to exist.

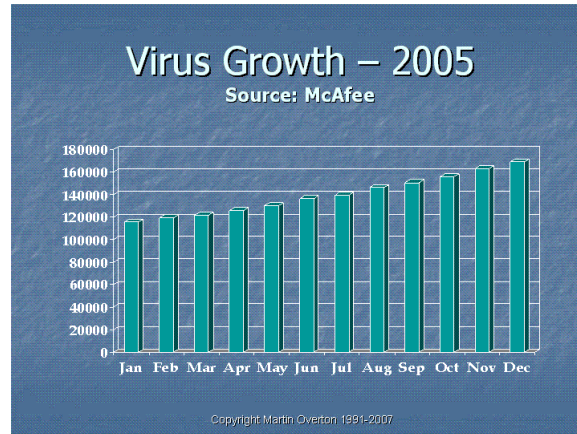
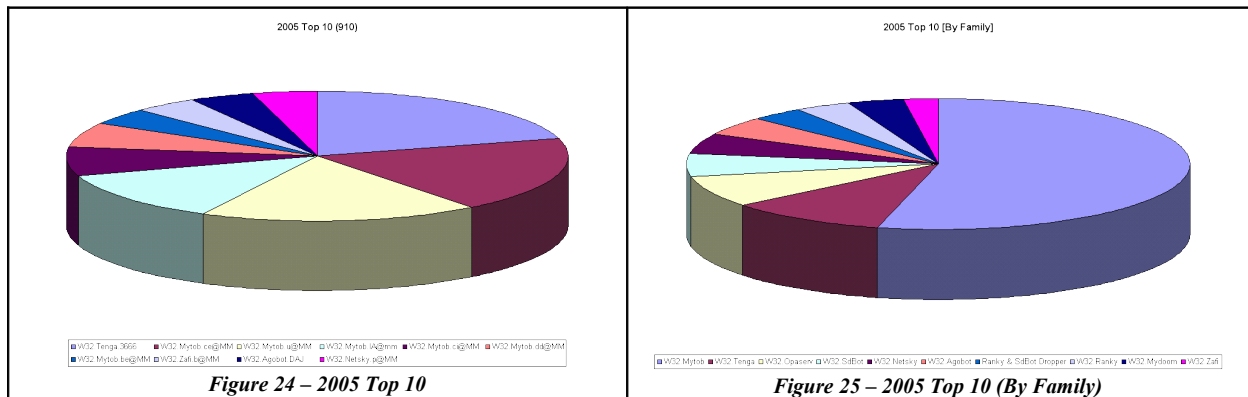


Figure 23 - Virus Growth, 2005 – Running Total



The graphs shown in Figure 24 and 25 are created from data using my own malware honeypots and my WormCharmer.

2.4.7 2006 January to June

For anyone outside the security industry the first six months of 2006 were pretty uneventful; however this was just a case of the 'Swan Principal' - All serene and smooth on top but furious activity going on beneath the surface – both in the malware and anti-malware camps.

A new worm appeared on the 17th of January which quickly became not only very widespread but also was a rarity in the sense that it would overwrite certain files, 11 file formats in all, on the 3rd of each and every month. Furthermore the worm contained a routine to connect to a website once a system was successfully infected; this caused the 'hit-counter' on the page to increase.

This worm was also known as: CME-24, Kama Sutra, Nyxem.E (F-Secure), W32.Blackmal.E@mm (NAV), W32/Grew.A!wm Fortinet), W32/Kapsler.A@mm (F-Prot), W32/MyWife.d@MM, W32/MyWife.d@MM! M24, W32/Nyxem-D (Sophos), W32/Tearec.A.worm (Panda), Win32/Blackmal.F (Vet) and WORM_GREW.A (Trend)

The worm's payload as mentioned above targets 11 files types. These files are overwritten and the contents get replaced with a text string “DATA Error [47 0F 94 93 F4 K5]”.

This meant that the only way to get the overwritten files back was to restore them from backups!

The worm incremented a counter on a website, at the 1st of February of 2006, this counter was standing at over 5 Million. However, this does not mean there were 5 Million infected hosts, as some miscreant had been using a botnet to artificially inflate the figures. It is believed that there were at that time actually around 600,000 infected hosts.

An amazing 54 percent of new malware in the second quarter of 2006 were Trojans, in the first quarter the percentage was 47 percent [source Panda-labs]. SOPHOS's own findings showed a similar, although not so large, move towards the use of Trojans. They found that Trojans outweighed viruses and worms by a factor of 4 to 1, whereas in the same period in 2005 the ratio was 2 to 1. Furthermore, they found that 50 percent of these new Trojans contained spyware components, such as key logger, data pilfering or backdoor [remote access] facilities.

This threat had grown considerably during 2006, not only with spyware hidden in or bundled with software, but also the use of botnets to deliver and install spyware, the use of exploits to do the same, and general drive-by downloads when just browsing the web.

Malicious software aimed at mobile devices, such as PDAs and SmartPhones grew quickly this year. This was not surprising as more and more of us now had SmartPhones with more computer power in our hands than a desktop computer offered a mere 10 years ago.

One of the more interesting developments we saw was a Trojan known as Redbrowser.

What was unusual about Redbrowser is that it isn't a SIS or Windows Mobile executable, but a Java based mobile malware threat. This means that in theory it will work on any mobile that contains a Java virtual machine.

Before Redbrowser unless you had a mobile based on Symbian or PocketPC [WindowsCE] then mobile malware was unlikely to bother you.

By the end of the first half of 2006 there were over 200 mobile malware strains/variants targeting mobile phones. Luckily many were Trojans, and therefore can't spread on their own, however the small number that can spread via MMS or Bluetooth were doing rather well.

The first six months of 2006 were also eventful for those that use Apple computers. We had seen growing interest by the malware authors and hackers in Mac OSX. Not only had we seen increased interest but also several PoC [Proof of Concept] malware created specifically for OSX.

Those we saw in the first half of 2006 included:

Name	How it spreads
Leap.A	Via iChat and infecting local files.
Inqtana.A	Via Bluetooth [3 variants now exist]

It is expected that more malware will be aimed at OSX in the future as we have already seen significantly increased interest from hackers, and knowing that most Mac users believe they are secure and not at risk will only make the malware authors more inclined to target OSX further.

Microsoft has long held the accolade for being the company closest to the heart of malware authors, without Microsoft malware would still exist but probably in far less numbers and varieties than they do today. Back in 1995 Microsoft Office was first targeted; this was the start of the macro-virus years, and although things were a lot quieter on the macro-virus front in 2006, it seems that the malware authors haven't forgotten their first love. We saw a number of new vulnerabilities being found in Microsoft Word and PowerPoint.

In May one of the Word exploits were used to install a backdoor, hidden with rootkit techniques on systems that opened the infected Word document on an un-patched version of the Microsoft word-processing application.

It was rather manic on the 'proof of concept' front with regard to malware, during the first half of 2006 we saw the following new targets attacked:

- *Matlab*
- *Microsoft Project*
- *Open Office*
- *Mac OSX*
- *J2ME*

2006 may have been short on major outbreaks during the first half of the year, partially because the malware authors are spending the time in investigating new attack vectors and methods.

One of the first ransomware found was Virus.Win32.GpCode [Kaspersky] which was found in December of 2004, a second variant appeared later that month. We were now seeing versions of this ransomware using strong encryption. In January 2006 variant ac was found and it used a RSA algorithm with a 56 bit key-length¹⁵. Next we saw a version using a 260 bit key, then a 330 bit key, each of these were cracked by the anti-virus firms. To top it all in June the author released a new version using a 660 bit key, this should have taken around 30 years to crack, but Kaspersky managed to crack it within 24 hours. No doubt we will see more of these Gpcode variants using larger and larger keys along with new malware that uses strong encryption techniques to hide or steal data.

If we see this technique added to bots we may well have to add a new entry to the definition of DDoS attacks, as encrypting files or whole disks without the owners knowledge is definitely a denial of service as they won't be able to use the data or disk that has been encrypted.

In one case a ransomware known as Ransom-A [Sophos] prevented users from accessing their computer until the ransom was paid via Western Union. The fee demanded was a measly 10.99 [US Dollars]. The amount may be small, but to try and ensure that the victim paid up, for every thirty minutes which passed it claimed it would delete a file. Furthermore, Ransom-A displayed pornographic images and messages on the infected systems screen which added to the pressure to pay up, especially if you were in an office or public place where your screen could be seen.

Script viruses and other malware have been around for many years, but interest in them had waned over the last few years, or so it seemed. During 2006r we saw a number of new script based malware, these include:

- *Yamanner*
- *Stardust*
- *Feebs*
- *Scano*

It seemed that we were seeing the rebirth of script-based malware, this time the target was web-based applications and the servers running these applications and sites. What was more worrying is that some of these script malware, such as Feebs and Scano were polymorphic and therefore harder to reliably detect as they mutate each time they infect.

July to December

E-mail borne malware numbers again dropped dramatically until practically the last week in December which saw a huge seeding of Tibs variants masquerading as a happy New Year message. SOPHOS found that only 1 in 337 emails contained viral payloads compared to 1 in 91 in the first half of this year.

In July the recorded numbers of viruses seen in the wild broke through the 200,000 mark – it was 100,000 just 2 years previously! This is a massive increase when you consider it took 18 years to get to 100,000.

Spammers trying to avoid having their emails trapped by mail filters continued to use image based spam although changed their routines to send out images with random colours/shapes along with quotes taken from news websites or extracts from books. The randomness of the images caused a major problem to the anti-spam vendors as they were difficult to filter.

Phishing scams continued to grow in both numbers and sophistication during the latter part of 2006 with “RockPhish” attacks becoming widespread. Bogus sites had been seen that acted as a “man in the middle” and they checked that the details being entered were genuine, with the real site. Phishers also took further advantage of hijacked VoIP telephone systems and used them as part of a phone based scam a.k.a. Vishing.

Social networking sites such as MySpace were targeted heavily with phishing scams and malware, yet more worms were released as we had first seen the previous year.

SOPHOS's figures again showed a continued move towards the use of Trojans. They found that Trojans made up over 80% of malware in 2006.

¹⁵ According to Kaspersky, although another source states that this key size is “ridiculously short” and that most key generators would refuse to create it.

The second half of 2006 also saw a resurgence of the mass mailing worm in the shape of Warezov which took just a single week to become the most widely spread email malware.

This worm propagated heavily around the internet via social engineering techniques and also by using exploits to launch when an infected e-mail was opened. The worm acted as a “spam machine” sending out millions of emails for pharmaceuticals, shares etc. causing spam traffic across the internet to rise by more than 500%. Over 1000 different variants were detected in November alone!

Once installed Warezov downloaded other payloads, modified your hosts file to stop your machine being able to connect to various anti-virus update servers and starts scanning your machine for new email addresses to send itself to.

A number of malware targeting MSN Messenger and Internet Explorer were seen in the wild, often linking off to 2 or more sites to pull down code. One of the more high profile vulnerabilities was found in the way that Windows handled VML files. This problem lead to infection just by browsing to a website or reading an infected email, Microsoft responded by releasing a patch for advisory 925568 over two weeks after.

One technique that was becoming more widely used was to spam out a small downloader program which can get past AV defences, this once installed, turns off or removes AV, personal firewalls and other security tools [lowering/disabling all the defences it can] and then connects to one [or more] of a pre-programmed list of websites where it will attempt to download another component and run/install it [let down the draw-bridge and let it's allies in to rape, pillage and take over the castle].

At this point your computer was often wide open to misuse and may well have become part of a botnet, all your financial details may have been captured and you may well have been sending spam and/or Phishing scam e-mails by the bucket-load without your knowledge!

As with the previous years, I submitted an abstract to Virus Bulletin, and they again accepted it. This time it was a paper covering '*Rootkits - Risks, Issues and prevention*'. This was once more on the Corporate Stream. The conference was held from the 11th - 13th October 2006 at the Fairmont The Queen Elizabeth hotel, Montréal, Canada. I also wrote a paper for, and presented at the EICAR 2005 conference, held in Hamburg, Germany at the end of April. The paper was called '*Spyware: Risks, Issues and Prevention*'.

The number of known viruses grew by 53,666 in 2006. By the end of this year there were at least 222,473 viruses known to exist.

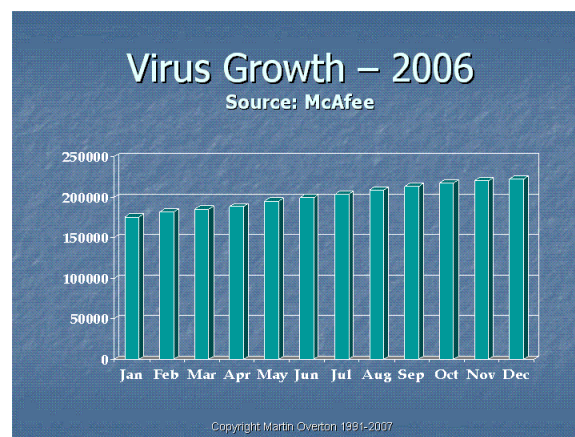
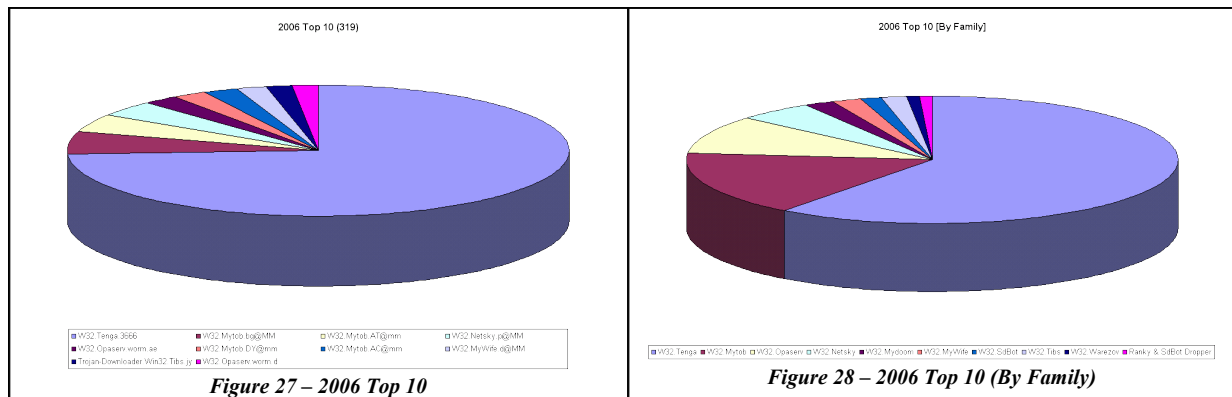


Figure 26 - Virus Growth, 2006 – Running Total



The graphs shown in Figure 27 and 28 are created from data using my own malware honeypots and my WormCharmer.

2.4.8 2007 (first-half)

Storm Worm caused many, many infections during the first half of 2007. It all started when the gang behind it launched the first version of it. This used real news events about the storms across Europe, as the hook to get users to click on an attachment in the e-mails that were spammed out by the hundreds of thousands during January.

The next wave used 'fake' news items, such as ones about World War III starting, and nuclear missiles being launched. There were many other fake stories used as the hook to get curious users to run the attachment.

The versions that appeared in May and June used a fake notification that you have received an e-card [electronic-greeting-card] from someone you know; a friend, neighbour, son, partner, worshiper and so on. Unlike the earlier versions, these e-mails do not contain an attachment; instead they supply a URL [web link] to the fake e-card.

Of course, when you click on the link you go to another site, not the one you expect to go to.

The main problem with the waves of fake e-card e-mails we saw, is that the link to the 'fake e-card' often took you to a website that contains the following payloads that could automatically infect your computer just by visiting it with a system that isn't fully patched:

- Various Browser Exploits.
- Various Windows Exploits.
- A download [fake e-card] which is actually malware.

I've often mentioned that the 'Bad Guys and Girls' seem to be using social engineering as their primary tool to try and get you to infect your own computer. The Storm Worm gang seem to excel in this area.

In March a new malware arrived, this being W32.Drum.A. This arrived as an e-mail with a graphic of IE7 Beta2 and links to a bogus 'IE7.0.exe' file on a remote web server.

Malware Wars Break-out again!

Kaspersky had this to say on the new malware war that broke out during the first half of 2007:

"War had been declared in cyberspace between the groups producing WarezoV and Zhelatin. Taking into account the size of the botnets used by both groups, and their clear aim to conduct a large number of attacks, the situations was clear: this was threatening to become one of the most serious problems on the Internet in recent years.

Until now, the best known cyber conflict was that between Mydoom, Bagle and NetSky, back in spring 2004. The network was flooded with dozens of variants of these worms: they scanned victim machines for their competitors and took their place, deleting the original worm. The war was brought to an end by the arrest of 18 year old Sven Jaschan, the author of NetSky, in Germany. However, his creations remain one of the most widespread worms in mail traffic. Out of all the malware authors involved,

only the authors of Bagle have remained active. It's true that they disappeared into the shadows for a while, and didn't react in any way to the appearance of Warezov, which is why we thought that they might have been involved in creating this worm. However, in January Bagle suddenly reappeared, and one variant of this worm became the most widespread malicious program in mail traffic."

The first half of the year has seen quite a bit of activity in the mobile phone arena, with SMS Spam, Phishing and Trojans all being seen.

The Warezov family added a new infection vector to their list, this being IM and not just any IM, but Skype.

USB drive malware started to grow during the first half of 2007, a common trick was to use 'autorun.inf' files to try and get the malware to auto-launch when the infected USB drive is attached to a computer. Could this be the new removable media threat? Two recent examples are discussed below:

LiarVB-A uses AIDS and HIV as the hook. This is what Sophos had to say about it:

"The [W32/LiarVB-A](#) worm hunts for removable drives such as floppy disks and USB memory sticks (as well as spreading via network shares), and then creates a hidden file called autorun.inf to ensure a copy of the worm is run the next time it is connected to a Windows PC. Once it has infected a system it drops an HTML file containing a message about AIDS and HIV to the user's drive"

Hairy is a new worm using Harry Potter as the hook. This is what Sophos had to say about it:

"The [W32/Hairy-A](#) worm can automatically infect a PC when users plug-in USB drives, which carry a file posing as a copy of the eagerly anticipated novel, "Harry Potter and the Deathly Hallows". If the users have allowed USB drives to 'auto-run' they will see a file called

HarryPotter-TheDeathlyHallows.doc

Inside this Word document file is the simple phrase "Harry Potter is dead." The worm then looks for other removable drives to infect."

During May we saw a new threat which was targeting OpenOffice. This new threat is known as BadBunny. It is a multi-platform worm written in several scripting languages contained in an OpenOffice document. It also uses a StarBasic macro. Sophos had this to say about it:

"SB/BadBunny-A spreads by dropping malicious script files that affect the behavior of the popular IRC programs mIRC and X-Chat, causing them send SB/BadBunny-A to other users. These malicious script files are named badbunny.py (for XChat) and script.ini (for mIRC, overwriting the existing mIRC file) and are also detected as SB/BadBunny-A.

SB/BadBunny-A drops different additional components depending on the platform on which it is running:

- On Windows, it drops a file named badbunny.js that is a JavaScript file infector also detected as SB/BadBunny-A.

- On Linux, it drops a file named badbunny.pl that is a Perl file infector also detected as SB/BadBunny-A.

- On MacOS, it drops one of two possible files named badbunny.rb and badbunnya.rb that are Ruby file infectors also detected as SB/BadBunny-A."

And I must not forget to mention MPack which turned up on lots of hacked website during the first half of 2007. Here's a clip from Wikipedia about it: "MPack is a PHP-based malware kit produced by Russian hackers. The first version was released in December 2006. Since then a new version is thought to have been released roughly every month. It is thought to have been used to infect up to 160,000 PCs with keylogging software.¹⁶"

So, the first half of 2007 was interesting, but very strange too.

¹⁶ Source: http://en.wikipedia.org/wiki/MPack_%28software%29

I had a paper accepted for the EICAR conference that was due to be held in Budapest, Hungary at the start of May, however about 6 weeks before the conference was due to be held, it was cancelled. An abstract was also sent to Virus Bulletin, and the original version of this paper was the end result of it. The conference took place from the 19th-21st September 2007 at the Hilton Vienna, Austria.

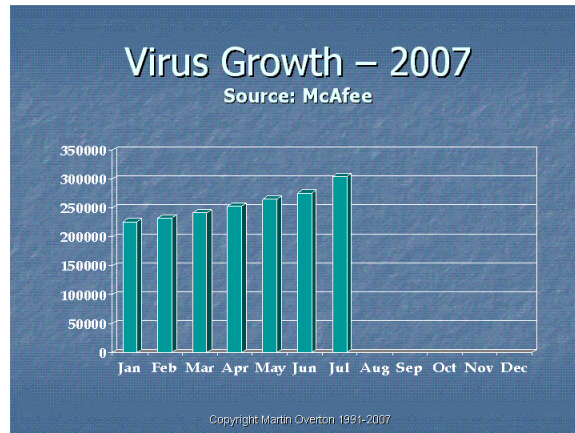


Figure 29 - Virus Growth, 2007 – Running Total

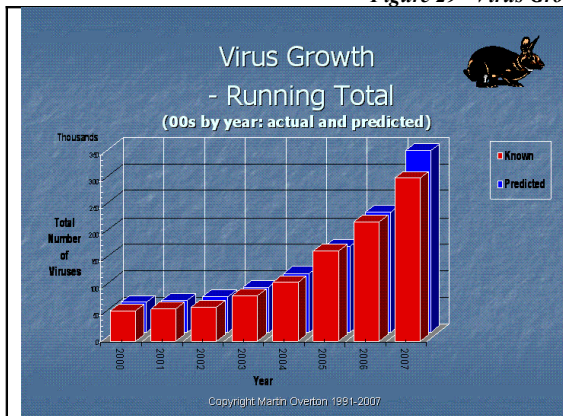


Figure 30 - Virus Growth, 2000-2007 – Running Total

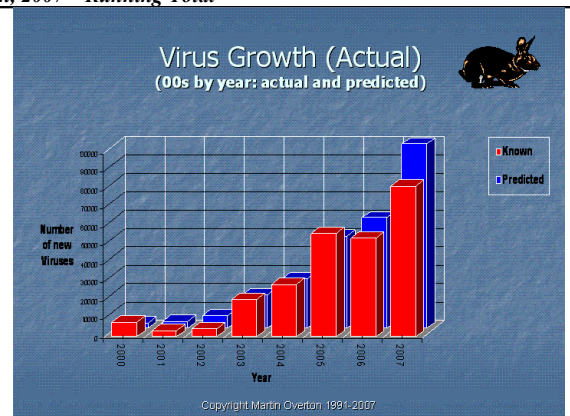


Figure 31 - Virus Growth, 2000-2007 – Actual, Per Year

2.5 Putting it all together...

So, you've now seen the events for each year, as well as the data for each of the relevant decades; 80s, 90's and 00's. Let us now quickly look at the overall patterns, trends, etc. that this shows.

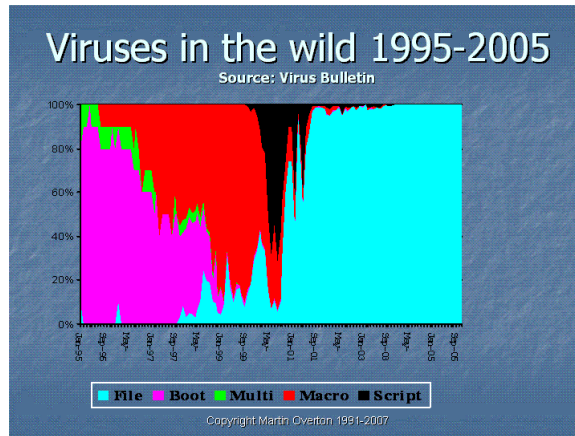


Figure 32 - Viruses in the wild 1995-2005

The graph shown in Figure 32, nicely illustrates the changes in malware type since 1995 and 2005. You can clearly see that boot sector viruses were King, until the advent of Macro viruses. These in turn very superseded by Script viruses. However, since 1997 you can see the inexorable growth of File viruses (.COM, .EXE, .DLL, .SCR and so on). By the start of 2002 almost all other virus types had shrunk to less than 5 percent of the totals seen in the wild. By 2004 that had shrunk further to around 1 percent, where it had remained almost static ever since.

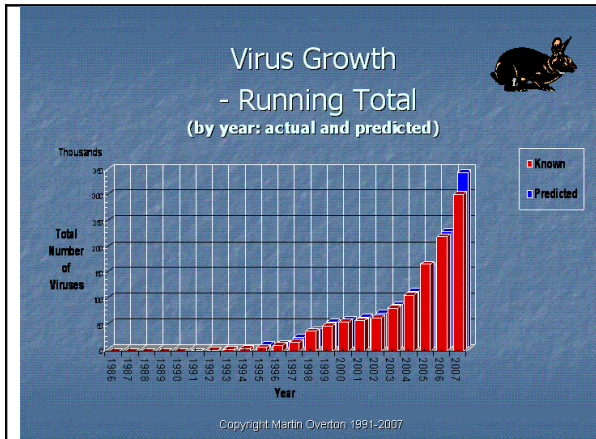


Figure 33 - Virus Growth, 1986-2007 – Running Total

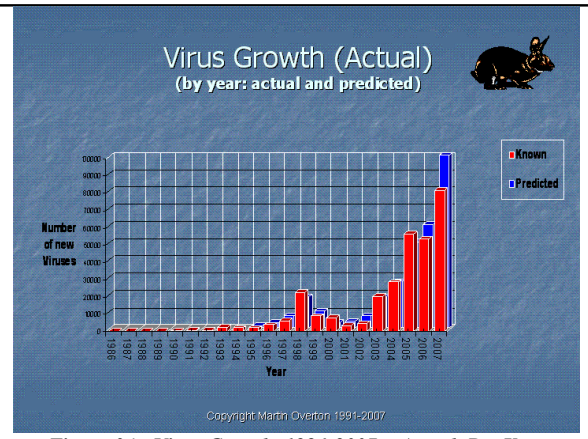


Figure 34 - Virus Growth, 1986-2007 – Actual, Per Year

The graph in Figure 33 clearly shows the growth from 1986 until July 2007. However, the more useful, and interesting way to look at the data is to see the actual yearly growth, as seen in Figure 34. Here you can clearly see the effect of the 14,000 modified variants created in 1998. It also shows the apparent drop-off in interest in creating malware which started in 1999 and which came to an apparent end in 2001. 2002 could have been seen as a slight increase in malware authoring again. However, it is clear that from 2003 to the present day, that malware authoring is a growing business. I use the word business, on purpose, as I believe that from 2002 many malware authors were looking at making money from their creations. This in turn attracted the old-style organised crime syndicates to take notice. From then on it was a sure thing that they would play an increasing role in hiring and recruiting malware authors to work for them on their own cyber-crime projects.

3 Conclusions

It has been an interesting journey, since the start of the problem with malware on the IBM PC and compatibles in 1986 with Brain.

We can see the following trends since those first tentative steps:

1986 until early nineties they were the almost exclusive domain of the DOS COM, EXE file infectors and boot viruses. They became more complex and stealthy as the years passed. We also saw viruses that would attack or disable anti-virus defences. Mostly the motivations for these creations were, in the early days, curiosity and research; later it became the electronic equivalent of graffiti, vandalism or bullying. Occasionally it would be used to get a message across, be it personal or political.

From 1995-2000 Macro viruses were King, slowly spreading at first, as people exchanged infected .doc/.xls files via floppy, CD or e-mail. Later examples would be able to propagate via e-mail by reading the Outlook or Windows address book, but only after a recipient had opened the infected attachment. Mostly the motivations for these later creations were the electronic equivalent of graffiti, vandalism or bullying. Occasionally it would be used to get a message across, be it personal or political. There were less likely to be motivated by research.

2000-2003 saw Script viruses steal the crown from Macro viruses, and we also started to see 32 bit PE files becoming dominant; multi-component malware started to appear. A large proportion of malware started to use vulnerabilities in both the OS and applications. The motivations for this period were almost the same as for those between 1995 and 2000.

2004 to the start of 2005, the mass-mailing worms were the Kings; resulting in many overloaded mail servers and worn-out anti-virus researchers and corporate security staff. However, in most cases the motivations were the same as before, although the shift towards seeing malware as a business tool had already started. Social-engineering was becoming more widely used.

2005-2007 and the new Kings, were BOTs, Trojans and Spyware. Phishing grew from almost nowhere to one of the biggest security risks, aside from malware. The motivations for writing malware changed dramatically from the start of 2005. Money was the main motivational driver, and this would grow as organised crime got into the act, and slowly took over. Many malware authors were regularly trying to disguise their creations using packers and compressor, such as UPX, ACE, PEX, etc. The use of social-engineering was very noticeable and by 2007 it had become almost the most common method used by malware authors to get their creations onto a computer, aside from using vulnerabilities.

So, what does the future hold?

I believe that we are at a tipping point, and as such there are two immediate ways things can go:

1. The security industry can use the current effective stalemate and lack of serious new malware development, to take the upper hand and take control of the problem, rather than being controlled by it, as they have been almost since the start of the malware problem. This will mean that new pro-active techniques need to be found, created, or dusted-off and updated. It will also require more consolidation and merging of security technologies than we've seen to date.
2. The malware authors take the fight back to the security industry by creating new malware or related security threats that use new techniques that side-step or defeat one of more layers of security defences. This scenario is unfortunately more likely to occur now than at any time in the past, due to the financial backing of organised criminal gangs who have staked more than money on this new digital crime-wave; their reputations are also on the line.

The problem is, it is not clear just how much time there is for the security industry to act; and act they must, or the bad guys and girls will, which will lock us in to another struggle which may well last several years or as long as a decade.

4 Thanks and Feedback

I would like to thank Joe Wells, Dr. Alan Solomon, Robert Slade, F-Secure and Kaspersky Labs for making lots of historical data available as well as articles about trends, techniques and motivation. I would also like to acknowledge Sophos, McAfee and Panda for some of the virus data I have used. Without the material they published this paper would have contained far more gaps than it does. Finally, I would like to thank Dr. Vesselin Bontchev for a number of corrections to the original published paper. The facts are theirs; any erroneous interpretations based on those same facts, are mine alone.

All constructive feedback on this paper will be warmly received as are any suggestions for things I've missed that should have been included.

I plan to update this paper at regular intervals, so that it becomes a rolling history of malware and anti-malware developments.

Further Reading/Resources

- Anti-Virus in the Corporate Arena - Proceedings of the 6th International Virus Bulletin Conference 1996 – Martin Overton – <http://momusings.com/papers/corpav.pdf>
- FAT32 - a new problem for anti-virus or viruses? - Proceedings of the 7th International Virus Bulletin Conference 1997 – Martin Overton - <http://momusings.com/papers/VB97-FAT32.pdf>
- Viruses and Lotus Notes – Have Virus Writers Finally Met Their Match? - Proceedings of the 9th International Virus Bulletin Conference 1999 – Martin Overton – http://momusings.com/papers/lotus_notes_and_viruses_101.pdf
- Hoaxes and Other Electronic Ephemera - Proceedings of the 11th International Virus Bulletin Conference 2001 – Martin Overton – http://momusings.com/papers/VB2001_Electronic_Ephemera-1.01.pdf
- When Worlds Collide - Proceedings of the 12th International Virus Bulletin Conference 2002 – Martin Overton - http://momusings.com/papers/VB2002-When_Worlds_Collide.pdf
- Worm Charming: Taking SMB Lure to the Next Level - Proceedings of the 13th International Virus Bulletin Conference 2003 – Martin Overton - http://momusings.com/papers/VB2003-Worm_Charming.pdf
- Canning More Than Spam With Bayesian Filtering - Proceedings of the 14th International Virus Bulletin Conference 2004 – Martin Overton – <http://momusings.com/papers/VB2004-Canning-more-than-SPAM-1.02.pdf>
- Anti-Malware Tools: Intrusion Detection Systems – EICAR 2005 – Martin Overton - <http://momusings.com/papers/EICAR2005-IDS-Malware-v.1.0.2.pdf>
- Spyware: Risks, Issues and Prevention – EICAR 2006 – Martin Overton - <http://momusings.com/papers/EICAR2006-Spyware-v1.0.2.pdf>
- Bots and Botnets - Risks, Issues and Prevention - Proceedings of the 15th International Virus Bulletin Conference 2005 – Martin Overton - http://momusings.com/papers/VB2005-Bots_and_Botnets-1.0.2.pdf
- Rootkits – Risks, Issues and Prevention - Proceedings of the 16th International Virus Bulletin Conference 2006 – Martin Overton - <http://momusings.com/papers/VB2006-Rootkits-1.0.2.pdf>
- A Short Course on Computer Viruses – Dr. Frederick B. Cohen – Wiley – ISBN 0-471-00768-4
- Viruses Revealed – David Harley, Robert Slade and Urs Gattiker – Osborne – ISBN 0-07-213090-3
- The Art of Computer Virus Research and Defense – Peter Szor – Symantec press – ISBN 0-321-30454-3
- Dr. Solomon's Virus Encyclopedia , October 1996
- Virus Bulletin Magazine – 1989-2007 – <http://www.virusbtn.com>

5 Appendix A – Links

Here are links to a selection of malware mentioned in the paper.

Year	Link to Description
1986	http://www.f-secure.com/v-descs/brain.shtml http://www.f-secure.com/v-descs/virdem.shtml
1987	http://www.f-secure.com/v-descs/vienna.shtml http://www.f-secure.com/v-descs/number1.shtml http://www.f-secure.com/v-descs/lehigh.shtml http://www.f-secure.com/v-descs/alameda.shtml http://www.f-secure.com/v-descs/stoned.shtml http://www.f-secure.com/v-descs/jerusalem.shtml http://www.f-secure.com/v-descs/pingpong.shtml http://www.f-secure.com/v-descs/cascade.shtml
1988	http://www.f-secure.com/v-descs/denzuk.shtml
1989	http://www.f-secure.com/v-descs/datacrim.shtml http://www.f-secure.com/v-descs/ghost.shtml http://www.f-secure.com/v-descs/eddie.shtml http://www.f-secure.com/v-descs/frodo.shtml http://www.f-secure.com/v-descs/burger.shtml http://www.f-secure.com/v-descs/vacsina.shtml
1990	http://www.f-secure.com/v-descs/flip.shtml http://www.f-secure.com/v-descs/nomenkla.shtml http://www.f-secure.com/v-descs/v1p1.shtml http://www.f-secure.com/v-descs/notb.shtml
1991	http://www.f-secure.com/v-descs/whale.shtml http://www.f-secure.com/v-descs/dir2.shtml http://www.f-secure.com/v-descs/tequila.shtml http://www.f-secure.com/v-descs/michel.shtml
1992	http://www.f-secure.com/v-descs/bomber.shtml http://www.f-secure.com/v-descs/tpe.shtml http://www.f-secure.com/v-descs/mte.shtml http://www.f-secure.com/v-descs/winvir.shtml http://www.f-secure.com/v-descs/peach.shtml
1993	http://www.f-secure.com/v-descs/cruncher.shtml http://www.f-secure.com/v-descs/tremor.shtml http://www.f-secure.com/v-descs/ste_boot.shtml http://www.f-secure.com/v-descs/monkey.shtml http://www.f-secure.com/v-descs/uruguay.shtml
1994	http://www.f-secure.com/v-descs/3apa3a.shtml http://www.f-secure.com/v-descs/one_half.shtml http://www.f-secure.com/v-descs/hoaxes/goodtime.shtml http://www.f-secure.com/v-descs/smeg.shtml http://www.f-secure.com/v-descs/natas.shtml http://www.f-secure.com/v-descs/kaos4.shtml
1995	http://www.f-secure.com/v-descs/concept.shtml http://www.f-secure.com/v-descs/gstripe.shtml
1996	http://www.f-secure.com/v-descs/boza.shtml http://www.f-secure.com/v-descs/laroux.shtml http://www.f-secure.com/v-descs/tentacle.shtml http://www.f-secure.com/v-descs/wazzu.shtml
1997	http://www.f-secure.com/v-descs/bliss.shtml http://www.f-secure.com/v-descs/esperant.shtml http://www.f-secure.com/v-descs/sharefun.shtml
1998	http://www.f-secure.com/v-descs/detroie.shtml http://www.f-secure.com/v-descs/hps.shtml http://www.f-secure.com/v-descs/marburg.shtml http://www.f-secure.com/v-descs/cih.shtml http://www.f-secure.com/v-descs/jetdb.shtml http://www.f-secure.com/v-descs/tristate.shtml
1999	http://www.f-secure.com/v-descs/calig.shtml http://www.f-secure.com/v-descs/ska.shtml http://www.f-secure.com/v-descs/melissa.shtml http://www.f-secure.com/v-descs/pretyp.shtml http://www.f-secure.com/v-descs/csv.shtml http://www.f-secure.com/v-descs/kak.shtml http://www.f-secure.com/v-descs/babylon.shtml
2000	http://www.f-secure.com/v-descs/inta.shtml http://www.f-secure.com/v-descs/love.shtml http://www.f-secure.com/v-descs/phage.shtml http://www.f-secure.com/v-descs/lib_palm.shtml

	http://www.f-secure.com/v-descs/w2kstrm.shtml http://www.f-secure.com/v-descs/hybris.shtml
2001	http://www.f-secure.com/v-descs/ramen.shtml http://www.f-secure.com/v-descs/onthe-fly.shtml http://www.f-secure.com/v-descs/macsimps.shtml http://www.f-secure.com/v-descs/bady.shtml http://www.f-secure.com/v-descs/klez.shtml http://www.f-secure.com/v-descs/nimda.shtml http://www.f-secure.com/v-descs/mandra.shtml
2002	http://www.f-secure.com/v-descs/dotnet.shtml http://www.f-secure.com/v-descs/swflfm.shtml http://www.f-secure.com/v-descs/myparty.shtml http://www.f-secure.com/v-descs/scalper.shtml http://www.f-secure.com/v-descs/opasoft.shtml http://www.f-secure.com/v-descs/benjamin.shtml
2003	http://www.f-secure.com/v-descs/mssqlm.shtml http://www.f-secure.com/v-descs/sobig_f.shtml http://www.f-secure.com/v-descs/swen.shtml http://www.f-secure.com/v-descs/msblast.shtml http://www.f-secure.com/v-descs/tanatos.shtml http://www.f-secure.com/v-descs/welchi.shtml
2004	http://www.f-secure.com/v-descs/novarg.shtml http://www.f-secure.com/v-descs/bagle.shtml http://www.f-secure.com/v-descs/witty.shtml http://www.f-secure.com/v-descs/sasser.shtml http://www.f-secure.com/v-descs/dtus.shtml http://www.f-secure.com/v-descs/cabir.shtml http://www.f-secure.com/v-descs/agobot.shtml http://www.f-secure.com/v-descs/netsky_d.shtml
2005	http://www.f-secure.com/v-descs/mytob_a.shtml http://www.f-secure.com/v-descs/gpcode.shtml http://www.f-secure.com/v-descs/tenga_a.shtml http://www.f-secure.com/v-descs/zotob_a.shtml http://www.f-secure.com/v-descs/cardtrap_a.shtml
2006	http://www.f-secure.com/v-descs/nyxem.shtml http://www.f-secure.com/v-descs/redbrowser_a.shtml http://www.f-secure.com/v-descs/leap_a.shtml http://www.f-secure.com/v-descs/yamanner_a.shtml http://www.f-secure.com/v-descs/febs.shtml
2007	http://www.f-secure.com/v-descs/small_dam.shtml http://www.f-secure.com/v-descs/worm_w32_hairy_a.shtml http://www.sophos.com/virusinfo/analyses/sbbadbunnya.html http://www.sophos.com/pressoffice/news/articles/2007/06/liarvba.html