A DAY IN THE LIFE

Viruses: A Way of Life

Eddy Willems
Data Alert International, Belgium

I remember the time when there were only 20 to 30 viruses around. I have seen old, familiar faces disappear in the last few years and new ones come along. I'm not a new one. I'm an old face who has spent a long time in the background. Some of you know me but for those who don't…

I was born in 1962. I am married to Nadine, a police officer – you could say we are both in 'security'. We have a son, Frank, who loves that I'm working with computers probably because of all the games I get! I studied Computer Sciences at IHB and VUB (University of Brussels) and was employed as a Systems Analyst in 1984. In 1987 I worked at *Vaderlandsche* (an insurance company in the internationally known *ING* group) as a System Support Engineer and Security Officer.

In those days, I programmed in languages like COBOL, assembler and C. I also did some data recovery work. I became interested in viruses at the end of 1989. It all started with a diskette which was given to me by my former employer who said 'Try and test it, it has proved quite a challenge for our company doctor.' I didn't know that this would change my life!

It Started with a Disk…

Between 8 and 12 December of that year, twenty thousand envelopes containing a 5.25-inch floppy disk were mailed to computer users all over the world. The disk was labelled 'AIDS Information diskette' and encouraged the recipient to install it on a computer. Enclosed was a leaflet with a licence agreement urging the user to send US$378 to a post office box in Panama. There was a threat in the agreement that unspecified action would be taken if the appropriate fee was not paid. I received just such a disk.

The floppy itself contained a nice questionnaire which assessed the user's exposure to the real aids virus. Once installed, the program printed an invoice giving the address in Panama to which payment should be sent. At that time the installation procedure made modifications to the AUTOEXEC.BAT with the result that every time it was executed, a counter in another file was incremented.

After about 90 (random) counts the trigger activated. The file names in the root directory of the hard disk were encrypted and marked hidden. I made a program and a procedure to reverse that process at that time. It seems that I was the first in Belgium to have a solution for the 'aids-information' diskette incident. It made me quite popular on TV and in some journals.

The writer of this Trojan had obtained mailing labels from the *PC World* circulation department. The case was solved by chance, when Dr Joseph Popp was stopped by a security guard at Schiphol Airport. He was extradited to the UK to await trial but his strange behaviour (wearing hair curlers in his beard etc) caused him to be declared unfit to be tried and he was returned to the US. He has since been found guilty of 'attempted extortion' by a court in Rome.

From that point on I began to gather information about computer viruses and anti-virus software. In 1990, by sheer coincidence, I made a modem connection straight to a US Unix-operated BBS. I was surprised when I recognized the operator's name: Sarah Gordon. In 1991 I became a member of *EICAR* and attended the *EICAR* conference along with lot of old friends. It was a strange feeling for me drinking beer (Belgium is reknowned not only for our famous chocolates but also for over 500 beers, not forgetting Belgian fries… historically not a French invention!) with all those familiar names like Alan Solomon, Vesselin Bontchev, Frans Veldman, Paul Ducklin, etc…

Over the years I have maintained a reference library of software, books and almost everything that has been published on the anti-virus field. I have also been a reporter for the well-known WildList since 1995. That same year I started writing anti-virus-related articles for Belgian magazines. I also put up my Web site specifically designed to be the index to all anti-virus related pages and Web sites (http://www.wavci.com).

In 1996 I started conducting seminars and workshops about computer viruses. At that time *Microsoft* came to me and asked to write the 'Virus Article' for the *Microsoft Encarta Encyclopedia*. Since the end of 1996 I have been working as a Technology Consultant for the largest *Benelux* distributor of the former *Dr Solomon's Software*, now *NAI TVD: Data Alert International*. In this role I am responsible, together with eight other colleagues, for anti-virus consultancy work, support, training and research. *Data Alert* specializes in all security-related products. Finally, at the start of 1999 I took on the extra job of news editor for the *EICAR* magazine.

Pick an Average Morning

My alarm clock rings at 6 am on a day in November 1999. I expect this day is going to to be like any other as I get up and hop in the shower, before running to one of my many computers. Already, my email box is filled up with over 100 new messages and that's without looking at my second (*Data Alert*) email address (which I checked at midnight). Trying to eat and read and answer the messages at the same time is not easy. I check my agenda and see two jobs for today. Two, hmm… there is definitely a third.

I jump into my car at half past seven and drive to a see a customer – a large French-speaking bank. We have three official languages here in Belgium: Dutch, French and German. My native language is Dutch. It is what I call a site-visit day. Sometimes I stay in the office to look into virus samples and problems from customers, sometimes I get out and do some training or some Virus Workshops.

My training courses are what I call really deep product training while the Virus Workshops are completely product-independent. The Workshop gives our customers (ranging from worldwide corporates to small businesses) an insight into the real threats which are around the dark corner.

I arrive at the bank in Luxembourg without a problem. It is a Virus Workshop this morning. A lot of questions are asked about the future. I explain that we are seeing a number of new problems this year and start talking about an increase of Worms, email propagation and VBS viruses. The I proceed to reiterate the importance of updating anti-virus products.

And an Average Afternoon

My mobile phone rings at lunchtime. Our support department informs me of a problem that one of our customers has with a potentially new virus. They ask me to call in on my way back. So, at 2 o'clock I arrive at – let us call this Company 3, a Dutch-speaking one this time. The IT manager tells me that they've got some email problems whereupon I open my notebook, copy some samples down and started to analyse the documents. I'm assuming at this point that it is another W97M/Melissa variant, but a few minutes later I witness some interesting things.

This particular virus hooks the system event that opens documents in *Word 97* with the 'Document_Open' subroutine, thereby running its code. Another system event is also hooked – the closing of documents due to the subroutine 'Document_close' in the global template after infection.

There is also a self-check to verify if the local system has already been infected. It's a check for existence of a certain registry key. If this key is not found, the virus code uses VBA instructions to create an *MS Outlook* email message with the subject line 'Message from' (Username) and in the body 'This document is very important and you've got to read this!!!'. The first 50 listings from all available address books are selected as the recipient.

Furthermore, that is not the only payload. If it is 25 December this virus overwrites the existing AUTOEXEC.BAT with instructions to format the hard disk.

I also saw a message box. After clicking OK on the dialog box, random coloured objects fill the document as an overlay. This reminds me of W97M/Pri. I call the Virus Lab in Aylesbury, UK. It transpires that I was the first in Belgium to run up against this one. They get an extra driver to repair it and the virus is given the name W97M/Prilissa.

Again my mobile phone rings. Rainer Fahs, Chairman of the Board of *EICAR* wants to discuss some small points concerning the upcoming *EICAR* newsletter and the next conference, to be held in Brussels in 2000. I arrive at the meeting place with Rainer at 6.30 pm. We discussed some confidential *EICAR* stuff and I start for home to have dinner with Nadine and Frank. The next two hours are dedicated to my family. I can't resist it when my son asks if I will put him to bed!

After a while I hear the sound from one my computers upstairs: 'Incoming mail'… I look into my mailbox from the downstairs PC and see about 200 new emails. I start reading and answering them. I also look at the virus samples I received today. After replicating and classifying them I start to make them ready for inclusion on the most recent WildList.

I also take a look at two new magazines which came out today. One of them appears to be the December issue of a computer publication which features an interview with me! I rush upstairs to show Nadine. She's already asleep though, probably tired after chasing after some criminals today… honestly, it's an interesting case but that's a different story. I put the magazine away for tomorrow.

Midnight. Time to sleep. After finishing a very good book concerning hacking techniques I turn to my bed. My mobile rings at 1am. Oh yes, I forgot, *Data Alert's* 24-hour emergency line was forwarded to me today. It is a desperate customer who's seen some strange behaviour on his machine. After helping him with some advice it looks to me that he is infected with VBS/BubbleBoy.

Afterwards I try to catch up on my sleep again but I am still wondering about that third thing that I had to do today. I still can't remember it. At 2.00 am I suddenly wake up… the third job: I was meant to be preparing a paper!