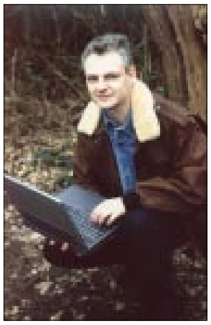
FEATURE

# Virus Hunting in Saudi Arabia

*Eddy Willems,*
*Data Alert International, Belgium*



In my work as WildList reporter, EICAR Director Information/Press and as a Senior Anti-Virus Security Consultant for Data Alert International and Network Associates, I receive a large number of virus samples. For this reason I make sure that I maintain a good secure structure on the hard disks of my computers. I consider this particularly important on my notebook because there is always a chance that it could be stolen and because I rarely use any anti-virus product on my notebook (which would interfere with my analysis of virus samples).

As part of my work I visit many clients (companies) who have been infected with different kinds of viruses in order to perform cleanup operations. In these situations I copy samples of the viruses onto a floppy disk and transfer these straight onto my notebook. Once they have been transferred to my notebook I use the PGP package to encrypt the viruses to prevent accidental access – you never know who might get their hands on my notebook!

Later, I copy the viruses to one of the PCs on my lab network so that I can replicate the samples and send them to the WildList Organization or to other virus labs. Any new viruses I find are PGP-encrypted and burned onto CD-ROM which is stored in a special safe for which there are only two key holders.

When I'm very busy, it might not be possible for me to transfer the viruses from floppy disk immediately. In this case I carry the disks with me in a protected sealed bag. On each of the disks itself is a clear fluorescent yellow label with the text ‘Virus Infected diskette … Attention – Dangerous … Don't access this diskette’.

I always try to keep ahead of potential problems and this has worked well for over ten years now. Sometimes people say to me, ‘Times are changing,’ and tell me that everyone is aware now of the measures necessary to protect against viruses. Maybe so, but allow me to share with you an incident that happened a few weeks ago.

## Arabian Night

Part of my job as Anti-Virus Security Consultant seems to be accumulating ‘air-miles’. Recently, a very large company in Saudi Arabia asked me to scope the anti-virus project for them.

After a long flight to Saudi Arabia, I stepped off the plane with the distinct feeling that it could be the start of a long evening (it was already 10.30pm). However, after passing through passport control everything appeared to be going smoothly. I was visiting the country for only three days, so I did not have much luggage with me: just one large case and one small computer bag containing my notebook, PDA, software and some magazines.

It occurred to me that there was an unusual queuing system in place. I was waiting in line with about 25 people when I was asked to step to another queue in which there were only seven people. Shortly afterwards they asked me to change queue again, this time there were only two people ahead of me. So far so good – I thought I was very lucky!

## Bag Search

When it came to my turn, the officials asked me to open my large carrying case. I opened it. The officer on duty proceeded to throw around my personal things. After about a minute of browsing he asked me to close my suitcase. Then I was asked to open my notebook bag.

By this time it was obvious that the officials were searching for something in particular. Evidently my notebook was not considered a suspicious object as it was not inspected. My pack of CDs were given a cursory glance, but the officer's eye fell upon a sealed red bag. Suddenly, seeing that there were some floppy disks inside the bag, he called loudly to another officer.

Both my bag of floppy disks and my passport were ripped out of my hands and carried away under the guard of an armed security officer.

I was horrified to realise that the previous day I had visited a company with outbreaks of W32/Magistr@mm, W32/Funlove.4099 and W32/SirCam@mm, and there were samples of each of these on the disks. I was completely astonished by what was happening and I tried to warn the airport officials politely: ‘Please attention, I am a computer anti-virus consultant, there could be some viruses on the diskettes. Please take care when accessing the files on the diskettes.’ The only response from the officer was: ‘No problem Sir’.

I tried to ask how to get my passport back but received no response other than ‘Keep ahead.’ So I followed the advice and found myself in the arrivals hall of the airport.

After a few minutes I found the ‘pickup’ who had been arranged to bring me to my hotel. I told him what had happened, and he informed me that the customs officials are constantly on the lookout for drugs and pornography. So I concluded that customs must have been searching for

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

pornography on my floppy disks. My driver told me that I would get everything back.

### No Problem

I was directed by some airport staff to a room which was surrounded by armed security guards. Inside was a man who appeared to be doing nothing other than checking diskettes and CD-ROMs. I arrived just in time to warn this guy just as I had done before. Nevertheless, he didn't seem worried about viruses. I tried again, asking him whether he had an anti-virus package installed on his system. Another a 'No problem Sir' was fired at me.

From the corner of my eye I couldn't see anything resembling an on-access scanner on this man's computer system. He continued trying to access the files on my disks, ignoring the fluorescent labels 'virus-warnings' on each of them. Again I warned him against touching the files, especially if he was connected to a network. And I warned him not to check any other disks subsequently as they also could become infected by his probably already contaminated system. It seemed that I really was talking to a (fire)wall and nearly nothing came from the mouth of this humble man.

I even asked him if he completely understood the consequences of his actions and my explanations. I received one final 'No problem Sir', together with my disks and my passport. A little disconcerted by the surrounding armed security guards I hurried away from the room with a bad feeling.

### Recommendations

Could I have prevented this? Maybe, but if someone says in clear English: 'Attention, your system may be infected or damaged by use of these diskettes', and if they choose to ignore this, what more can you do? Even my fluorescent yellow labels with 'Danger Viruses' did nothing to prevent this person from accessing my 'dangerous' files.

In my opinion, if you are in a position where you must monitor diskettes and CD-ROMs, you should have a good anti-virus protection in place. Better tools should be used to search for the things these people are looking for instead of just 'clicking' on everything – using the current system, simply altering the file name or extension would mean that the files couldn't be opened.

I wrote a letter to the airport authorities after my trip to explain this incident, and recommending that their officials be more cautious the next time. I have not received a response, but I hope things will change.

This tale demonstrates that even anti-virus experts can be beaten, even when the most secure measures have been put in place to prevent outbreaks like this one.

I hope that my next trip abroad will be less eventful – especially for the airport I am visiting!

VIRUS BULLETIN **©2001 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /2001/$0.00+2.50**
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.