Virus Hunting in Saudi Arabia – Part 2

Eddy Willems
Data Alert International, Belgium

[*Last year (see* VB*, October 2001, p.10), Eddy Willems related the terrible tale of the computer virus horrors he witnessed at the hands of Saudi customs officials. Earlier this year he returned to Saudi, where his inquisitive nature led him into trouble of a different kind.*]

Whenever I visit a new city I like to spend a day wandering around, exploring and getting a feel of the place and its people. My experience is that, by night, many places have a completely different atmosphere. People have warned me that sometimes I venture too far and that I could be putting myself in danger. But, when they advise me not to visit certain areas of the town, I am intrigued as to why. I have visited some infamously dangerous areas in cities both in the US and Europe. Now, I have felt the same atmosphere in the Middle East.

Arabian Nights

In the Middle East it is very pleasant to go out at night because that it is the only time when the climate is bearable for walking around. If you venture outside at noon you may find yourself being barbecued by the sun! In the summer the temperature can rise to about 45 ºC easily, whereas at night a slightly cooler temperature of between 20 ºC and 30 ºC is very pleasant.

All the shops in Saudi seem to stay open very late into the night. Usually when exploring a new city I try to find the electronics shops, so one evening I asked the hotel receptionist to direct me to the area of the town in which these were located. I followed his directions to a large square downtown.

The square was completely filled with small computer shops and some larger electronics shops. As I arrived, a man approached me. I assumed he was about to ask me for something and thought he must be a drug addict. But it seems that I had jumped to the wrong conclusion: 'Hi, do you want some software, CDs, music or DVDs?' he asked. A little puzzled, I replied, 'No thank you,' and walked on.

About five metres further on another man approached me with the same question. This continued until I had been offered the chance to buy software or music CDs about 50 times.

Suddenly I had an idea: what if you really wanted some software … what if you asked for anti-virus software?

Place your Orders

I began walking around the square again. Nearly every man I spoke to seemed to have some kind of anti-virus software on his list (each of these 'vendors' have lists from which you can choose the software; once they have taken your 'order' they go way and return with everything you requested copied onto one CD).

Prices seem to vary from 10 to 40 Saudi Rials (approximately 0.3 Euro = 1 SR) for one product or program. After a while I started asking for corporate anti-virus software. This was not so easy to come by. Most of the men didn't know what 'corporate' meant – the majority of them were 'illegals' (with no visa) and seemed to have no computer knowledge whatsoever.

After a while, I realized that one man was following me very closely. After the 25th man I passed this guy approached me and said that he had heard what I was searching for. He asked me to follow him and led me to a narrow alley…

Everything under the Sun

After going through a small door we entered a building where we climbed two levels up some broken stairs, then he asked me to wait in a small dark room. After a while he returned and asked me which anti-virus product I wanted.

'What do you have?' I asked the man. 'Everything!', he exclaimed as he showed me into a room containing a PC. He inserted a DVD into the machine and asked me to make my selection.

I saw every latest version of nearly every AV package I could think of – even *NAI ePO server 2.5.0* and *Symantec System Center 7.5* as well as *Trend's NeaTSuite* were on the DVD. The price was 30 SR.

I told the man that I was not really interested as I didn't find what I was looking for. It looked to me as if only one or two anti-virus packages were missing, so I told him I wanted a package (*eSafe*) that wasn't on the DVD, since I was keen to leave as quickly as possible. A little upset, the man explained that he couldn't have everything.

Surprise!

At that moment the man asked me something I was really not expecting: 'Maybe I can help you with some computer viruses?' he said, 'What do you think?'.

Taken by surprise, I asked him what he could give me. The man left the room and, after a few minutes, he returned with another DVD.

He explained that this was the best virus DVD available. 'More than 300,000 different viruses – even undetectables!' he told me. 'That's impossible,' I told him. When he realized I knew the field well, he conceded that there were about 32,000 viruses on the DVD. 'Will you take it?' he asked again.

I was horrified by this proposal, but I was quite intrigued. I asked the man how he had obtained this collection. He told me that he knew a man who wrote viruses and that this DVD had been the man's own private collection. However, since having been married, the man was no longer interested in viruses and had given the collection away.

After hesitating a while, I repeated that I was not interested in buying the virus collection. This time the man became angry and asked me to pay him 100 SR (approximately 30 Euro). Again I stated that I was not interested, but the man started shouting at me and I felt very intimidated.

A little nervous because of the strange environment and very confused, I gave the man some money. He threw the DVD at me and asked to leave immediately. Before I left he advised me to say nothing about this deal and to 'forget' him.

The Analysis

On my rapid return to the hotel I hoped that I had not been ripped off by this wretched deal. Once I reached my hotel room I very quickly booted my notebook and searched for the scanners I had brought with me. Only three of them were up to date.

First, I discovered that the DVD was at least readable, though not fully used. Nevertheless, there were 30,751 files on the disk. It seemed that the DVD was not a copy of some known CDs on the Internet like the 'old' Digital Hackers' Alliance virus CD or others and it didn't look like a collection from an anti-virus vendor either.

The DVD contained a mixture of executables, zip and rar files, docs, xls and some html files. Within most of the (few) archived files, I just found one or two other files. This brought the total up to 31,657 different files.

I used *NAI VirusScan 4.5.1 SP 1* with 4160 Engine and Dat file 4205, as well as *AVP Pro 4.0* and *Symantec NAV CE 7.6*, both with the latest (May 2002) update. It appeared that every single file was, indeed, infected – although not each with a different virus.

I found exactly 31,655 different viruses. This indicated that the DVD had been prepared properly – otherwise I would have found many more uninfected files. This is quite a huge number for such a collection.

I did not find any new, undetected viruses, although some of those I found on the disk were relatively recent (e.g. W32/Yaha.c@MM). Nevertheless, I did find viruses which don't appear frequently and are classed as Zoo viruses, such as V5M/unstable (a proof of concept virus written in VBA for *Visio 2000*). The viruses themselves were not always named or classified. In most cases the viruses were not even replicated.

Where the macro viruses were concerned, I easily located the real content inside the files. Most of the files seemed to have come from European corporates – I found it puzzling that these had appeared on this side of the world. I'm unsure whether the man was very honest about the details of his virus writer acquaintance.

The Lesson

One of the last questions I asked the man was whether there was a lot of demand for these CDs.

He told me that I was one of the first to have asked for anti-virus software. It seems that most people ask for some specific OS software like *Windows XP* or *Windows 2000*. He had come across the virus CD by coincidence. He told me that he had received only a few special requests for it, and explained that there was significantly more demand for 'good' hacker tools at the moment.

I advised the man not to sell any more of this kind of CD or software because of the trouble he could get into with the authorities. He told me that there had already been several raids that attempted to break down this illegal dealing. However, he explained that virus writing is very easy in this region, because of the lack of good laws concerning this matter.

I think that I underestimated this man when I stormed out of that dark alley at around midnight that night. He knew exactly how many viruses were on the DVD, and he gave me a detailed explanation of the laws concerning computer crime.

It seems that I had stumbled across a man who was not typical of these illegal software vendors. It occurred to me that he was the only one who seemed to have any knowledge about computers.

Later on, I contacted the local police about these practices (which was an adventure in itself!). On my next visit to the city I found out that a raid had been carried out by the police and most of the men had been arrested.

Dangerous Corners

Again I have been surprised in a land that I didn't know very well. I do not condone the sort of practice I experienced, but I couldn't prevent it – would the man have stayed calm had I not agreed to the deal?

I have learned that drug dealing, software dealing and even virus dealing lie in the same dangerous corners of our society. I hope I never have to write part three of this series – but my work will bring me back to the same region later this year, so watch this space!