Germ warfare

GEOF WHEELWRIGHT INVESTIGATES THE DARK WORLD OF COMPUTER VIRUSES, ELEGANTLY DESIGNED PROGRAMS WITH A STING IN THE TAIL.

Your computer is acting strangely. It doesn't recognise your floppy drive, data on your hard drive appears to be damaged and nothing seems to be working properly. It could be that it is suffering from the effects of a 'computer virus'. But who would do such a thing? Particularly to someone as nice as you? You have no enemies that you know of, and you always clean up after your dog.

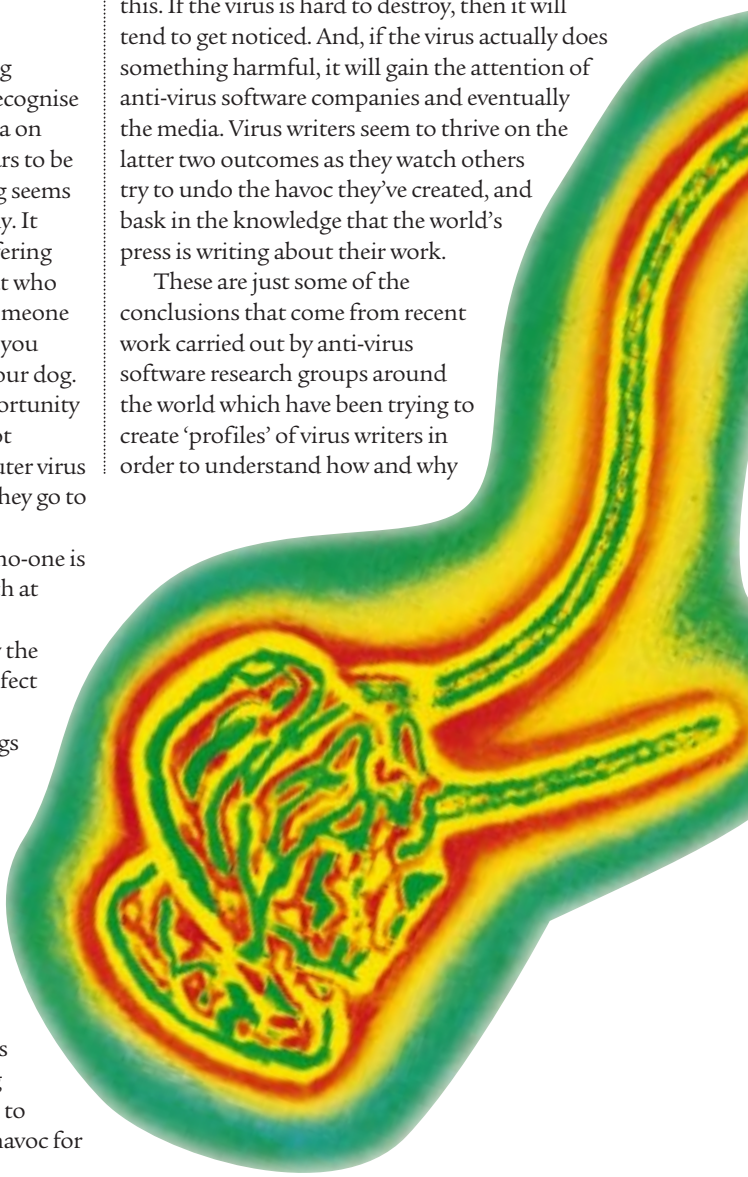
Chances are you've never had the opportunity to ask these questions, as the police do not routinely investigate incidences of computer virus infection. But they are good points, and they go to the heart of why computer viruses exist.

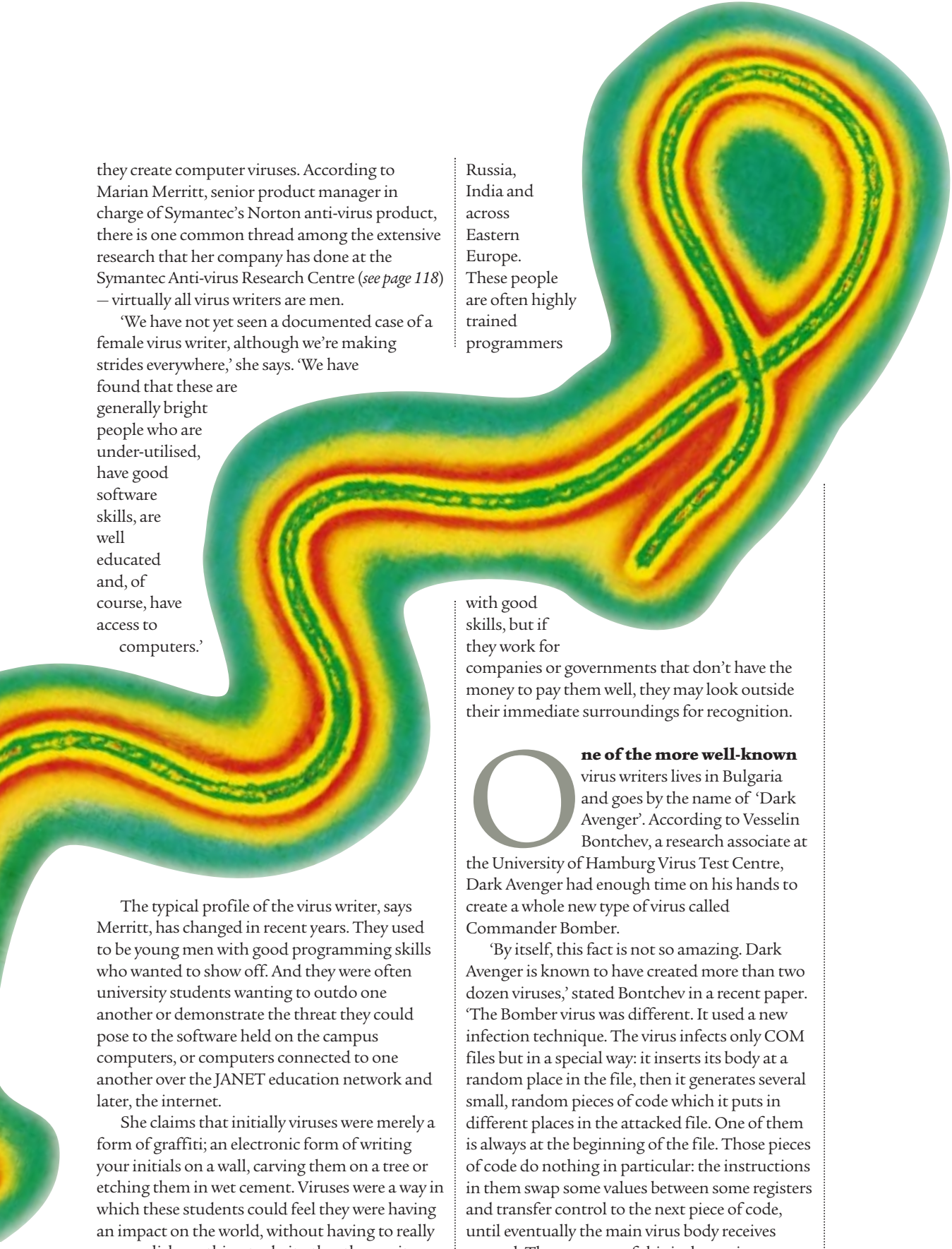
The first point is that, in most cases, no-one is doing something to you directly. Research at anti-virus labs the world over suggests in almost all cases, virus writers don't know the people whose computers the virus will infect — it would be like suggesting that people who write graffiti on the walls of buildings have some idea of the identity of those who will be offended by it — and, they often have little regard for the impact the virus will have on those whose computers suffer from it. This attitude appears to be a rather sick distortion of the idea that art should be produced for its own sake and not just to please a given audience.

In this case, the attitude is that viruses are produced simply to create something that is technically 'elegant' and very hard to crack. The fact that the virus may cause havoc for individuals appears secondary to the virus writer; the key issue for them is to produce something that will be hard for anyone to destroy.

Many secondary considerations flow from this. If the virus is hard to destroy, then it will tend to get noticed. And, if the virus actually does something harmful, it will gain the attention of anti-virus software companies and eventually the media. Virus writers seem to thrive on the latter two outcomes as they watch others try to undo the havoc they've created, and bask in the knowledge that the world's press is writing about their work.

These are just some of the conclusions that come from recent work carried out by anti-virus software research groups around the world which have been trying to create 'profiles' of virus writers in order to understand how and why





they create computer viruses. According to Marian Merritt, senior product manager in charge of Symantec's Norton anti-virus product, there is one common thread among the extensive research that her company has done at the Symantec Anti-virus Research Centre (*see page 118*) — virtually all virus writers are men.

'We have not yet seen a documented case of a female virus writer, although we're making strides everywhere,' she says. 'We have found that these are generally bright people who are under-utilised, have good software skills, are well educated and, of course, have access to computers.'

The typical profile of the virus writer, says Merritt, has changed in recent years. They used to be young men with good programming skills who wanted to show off. And they were often university students wanting to outdo one another or demonstrate the threat they could pose to the software held on the campus computers, or computers connected to one another over the JANET education network and later, the internet.

She claims that initially viruses were merely a form of graffiti; an electronic form of writing your initials on a wall, carving them on a tree or etching them in wet cement. Viruses were a way in which these students could feel they were having an impact on the world, without having to really accomplish anything to do it other than write some difficult code. 'There is often competition amongst them to see who can write the best, who can write the virus that's hardest to crack,' adds Merritt.

In recent years, viruses have moved well beyond being harmless college and university pranks. In some cases, they've become a social statement as programmers with little money and fewer prospects, but good access to computers and the internet, write and distribute viruses in Russia, India and across Eastern Europe. These people are often highly trained programmers with good skills, but if they work for companies or governments that don't have the money to pay them well, they may look outside their immediate surroundings for recognition.

One of the more well-known virus writers lives in Bulgaria and goes by the name of 'Dark Avenger'. According to Vesselin Bontchev, a research associate at the University of Hamburg Virus Test Centre, Dark Avenger had enough time on his hands to create a whole new type of virus called Commander Bomber.

'By itself, this fact is not so amazing. Dark Avenger is known to have created more than two dozen viruses,' stated Bontchev in a recent paper. 'The Bomber virus was different. It used a new infection technique. The virus infects only COM files but in a special way: it inserts its body at a random place in the file, then it generates several small, random pieces of code which it puts in different places in the attacked file. One of them is always at the beginning of the file. Those pieces of code do nothing in particular: the instructions in them swap some values between some registers and transfer control to the next piece of code, until eventually the main virus body receives control. The outcome of this is that a virus scanner has no way to determine where exactly in the file the virus is present. All "smart" scanning techniques, like entry-point tracing and top-and-tail scanning, suddenly stop working.'

American author George C. Smith described the work of Dark Avenger in his book *The Virus Creation Labs*: 'The Dark Avenger obviously knew how real computer viruses should be written,' suggested Smith. 'His Eddie virus — a.k.a Dark Avenger — had gained a reputation as a program

Seek & destroy: anti-virus research at Symantec

Santa Monica, California — palm-tree lined streets and a short drive from the Hollywood hills — is home to Symantec's Anti-virus Research Centre (SARC) which holds the largest collection of computer viruses on the planet. SARC acts as an international clearing house for the creation of software solutions to computer viruses imported from around the globe.

According to Symantec, there are over 17,000 strains of computer virus in circulation, although only a tiny proportion of that number are active viruses showing up on a significant number of computer systems with regularity. But Symantec sees them all. Corporate and retail customers of its Norton AntiVirus (NAV) software are encouraged to submit new viruses — those which cannot be handled by NAV — to SARC for inspection, detection and repair.

According to Bob Pettit, product director for Symantec's consumer products group, there is one type of computer virus that it sees more than any other: the 'macro' virus. This is a malicious computer program written in the same macro programming language that was designed to allow users of the Microsoft Word WP software and Microsoft Excel spreadsheet applications to add new functions to their software. Instead, macro-virus writers have used the macro programming language to create small programs which prevent you from carrying out simple tasks, like saving or printing files, by attaching themselves to your documents.

Since Word and Excel documents are used in the majority of offices around the world, they tend to be the kinds of document that are sent and received in electronic mail messages. And therein lies the problem. Every time someone opens an email message with a Word or Excel 'attached' document that is infected with a macro virus, it spreads to the computer on which the electronic mail message was opened. Those with newer versions of Word and Excel are less likely to suffer the problem as Microsoft Office 97, which includes the latest versions of Word and Excel, has a utility to detect unexpected viruses. But there are still many users who have older copies of Word which are prone to these kinds of virus incursions via email.

Symantec warns users to seek out virus detection utilities that inspect the contents of all files on a hard disk, as well as attached files in unopened electronic mail messages, to ensure they don't contain virus messages.

Here's a checklist of symptoms which Symantec suggests you should look out for if you suspect that your computer has a virus:

- The program takes longer to load.
- The program size keeps changing.
- The disk keeps running out of free space.
- When it runs CHKDSK it doesn't show 655360 bytes available.
- It keeps getting 32-bit errors in Windows.
- The drive light keeps flashing when it's not doing anything.
- No access to the hard drive when booting from the A: drive.
- Files appear from nowhere.
- Files have unrecognised or strange names.
- Clicking noises from the keyboard.
- Letters look like they are falling to the bottom of the screen.
- The computer doesn't remember .

to be reckoned with. It pushed fast infection to a fine art, using the very process anti-virus programs used to examine files as an opportunity to corrupt them with its presence. If someone suspected they had a virus, scanned for it, and

THE LAROUX MACRO VIRUS, DESIGNED TO CAUSE PROBLEMS IN MICROSOFT EXCEL WORKSHEETS

Eddie was in memory but not detected, the anti-virus software would be subverted, spreading Eddie to every program on the disk in one sweep.

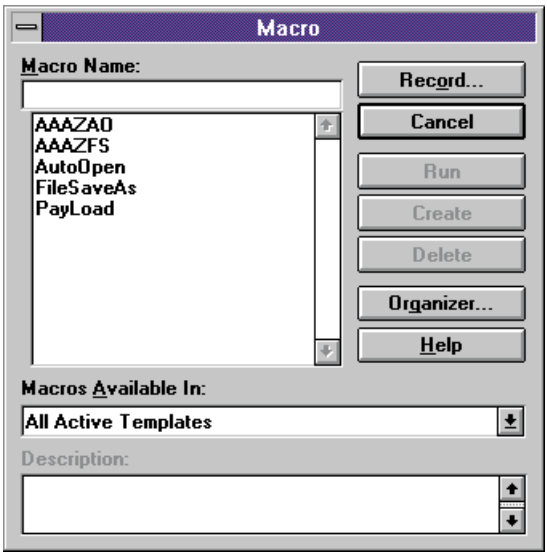
'Eddie would also mangle part of the machine's command shell when it jumped into memory from an infected program. When this happened, the command processor would reload itself from the hard disk and promptly also be infected. This put the Eddie virus in total charge of the machine. From that point on, every 16 infections the virus would take a pot shot at a sector of the hard disk, obliterating a small piece of data. If the data was part of a never-used program, it could go unnoticed. So, as long as the Eddie virus was in command, the user stood a good chance of having to deal with a slow, creeping corruption of his programs and data.'

Finding concrete information about virus authors like Dark Avenger is not an easy task, though. The authors are understandably cautious about revealing their real identities, for fear of prosecution. And anti-virus software

companies worry that giving publicity to virus writers will only glorify their nasty work.

Carey Nachenburg, chief researcher at the Symantec Anti-virus Research Centre (SARC), claims there's a big debate in anti-virus research about whether or not any understandable names should even be ascribed to viruses. Many researchers suggest they should simply be given non-descriptive combinations of letters and numbers. This not only makes the viruses easier to catalogue, but also eliminates the romantic attraction of writing a virus that bears your name, or one that you have given it.

Vesselin Bontchev echoes this concern and suggests little can be done to eliminate the attractiveness of virus writing. 'The process of virus creation is not going to stop or slow significantly in the forseeable future,' he predicts. After a few years of activity, the virus writers usually grow up and switch to other activities but many new "wannabe" virus writers, usually adolescent kids, pop up in their place.'



THIS IS THE SCREEN NO-ONE WANTS TO SEE IN MICROSOFT WORD, SHOWING THE MACROS THAT MAKE UP THE WELL-KNOWN 'CONCEPT' WORD MACRO VIRUS. IT INTERFERES WITH WORD'S ABILITY TO SAVE FILES IN STANDARD DOCUMENT FORMAT AND CAUSES THEM TO BE SAVED AS TEMPLATES INSTEAD

If the latest statistics from the Internet Computer Security Association (ICSA) are to be believed, the problem will get worse before it gets better. ICSA's 1998 Computer Virus Prevalence Survey, released in late 1998 and sponsored by Microsoft, Computer Associates, Network Associates, Intel, Price Waterhouse, Symantec, Trend Micro *et al*, suggests 'macro' viruses which run inside Microsoft Office are the biggest problem currently facing most users.

'The dramatic increase in the incidence of computer viruses is being driven by the rapid proliferation of macro viruses,' says Peter Tippett, president of ICSA. 'The primary infection vector for a macro virus is as an email attachment. Macro viruses spread easily because the infected files often exhibit few, if any, obvious symptoms. Because computer users need run time, anti-virus software needs to continuously scan email attachments for viruses.'

The ICSA survey concluded that the rate of infection in 1998 was 48 percent higher than reported in l997. The annual survey, based upon interviews with technology professionals drawn from 300 corporations and government institutions in the US, represented some 750,000 PCs and servers.

One of the most disturbing trends uncovered by the report is that despite increased use of anti-virus software, computer-virus infection rates continue to increase. Of those surveyed, almost all have anti-virus software installed and running continuously. The report suggests the main reason for the increase in prevalence appears to be 'ineffective policy management across the enterprise'. More specifically, it reveals that regular software updates, email policies, improper installation and policies governing remote computer use are major issues.

So, despite all efforts to identify virus writers, eliminate the fruits of their work and encourage users to guard against the impact of viruses, it seems that they will be with us for some considerable time to come. □

VIRUS NEWS AND VIEWS

Here is a list of sites offering utilities for virus detection, as well as news and updates on virus trends.

☛ **www.symantec.com/avcenter/index.html**
The online home of the Symantec Anti-virus Research Centre (SARC). Here you can download updates to Norton AntiVirus, a virus encyclopaedia. There's news about virus hoaxes, a virus reference area and information on how to submit virus samples for 'diagnosis'.

☛ **www.nai.com/vinfo/**
Network Associates offers free downloads, news and views on viruses. It includes an online virus information and technical documentation library, a list of new virus entries and descriptions of the ten most common viruses. There are lists of viruses by name, type and payload activation date — this last is useful, as some viruses are triggered on a certain date.

☛ **www.drsolomon.com/vircen/gallery/picture.html**
In this section of the site run by Dr Solomon's Software, you can see screenshots of what viruses look like when they're activated. This is a rather fun 'rogue's gallery' of some of the more noteworthy DOS and Windows-based viruses that have plagued computers in recent years.

☛ **www.hitchhikers.net/av.shtml**
A comprehensive site which includes a wide variety of articles, an excellent set of links to anti-virus software producers, copies of recent research papers, reviews of anti-virus products and recommendations on how to fight viruses.

☛ **http://ciac.llnl.gov/ciac/CIACHoaxes.html**
If you prefer the entertainment value of hearing about how people react to virus reports and hoaxes, you'll enjoy this site which has been put together by the US Department of Energy Computer Incident Advisory Capability.