The Bulgarian Computer Virus Factory

By Gordon Young

Bulgaria was the world's computer virus hot spot between 1988 and 1993, when a set of educational, technical, political, and economic conditions supported the creation and spread of computer viruses. Virus programmers became more organized, concentrated, and active in Bulgaria than anywhere else in the world.

Among a well-educated, badly under-employed and socially discontented class of computer programmers, creating computer viruses became a popular hobby.

Eastern Bloc High-Tech Capital

In the early 1980s, Bulgaria's president, Todor Zhvkov, decided his country should become the high-tech capital of the Eastern Bloc countries. High-tech products would be traded for needed raw materials. Universities and technical colleges geared up to train computer programmers.

The country's first computer products were slow and shoddy clones of IBM and Apple machines. Though quality improved through the late 1980s, Bulgaria's businesses were not modern enough to have much use for computer technology. The new computers often ended up uselessly decorating the desks of senior bureaucrats—a symbol both of the bureaucrats' social status and the useless futility of the bureaucratic administrative system that made the machines.

The breakup of the Soviet Union made things worse. Economic conditions deteriorated and unemployment soared, even among the highly skilled.

The Bulgaria-Virus Connection

The story of the Bulgarian computer virus factory begins around November 1988. The Vienna virus, originating in Austria, was the first specimen Bulgarian hackers captured. They soon had their hands on copies of the virus, and quickly developed new and improved versions that were smaller, faster, and more efficient. The first Bulgarian-produced virus was the harmless Vacsina, written by a 27-year-old engineer, Teodor Prevalsky, who developed both virus and anti-virus software as an intellectual hobby. Though he did not intend it, his creation escaped his control. It was the first Eastern virus to jump the Iron Curtain to the West.

Bulgaria's most notorious virus vandal was a skillful, talented, and clever programmer who used the alias Dark Avenger.

The common Cascade and Ping Pong viruses invaded the country next. From Ping Pong, the pirate programmers learned about boot sector viruses. Quickly, virus programming caught on across the country. Totally new viruses soon surfaced.

Bulgarian Pirates

There were so many pirate programmers in Bulgaria because their government trained them for it. Bulgarian government policies made cracking Western software copy protection schemes a standard part of a computer student's education. As a nation entering the computer age, Bulgaria chose to equip itself by pirating and reverse-engineering Western software and hardware. Hacking and cracking were not only tolerated, they were part of national policy.

Justified as anti-capitalistic, this choice also served the cash-strapped small country well by slashing spending on expensive Western software. As part of this policy, inside Bulgaria's borders there were no laws protecting computer information. Virus vandalism was not illegal. No matter how much damage virus hackers did to others' work and property, programming and spreading computer viruses was not a crime.

The fight against computer viruses in Bulgaria was weakly organized. Because few could afford them, personal computers were not common in Bulgaria. Most computers were shared. This allowed virus infections to spread between users, their disks, then on to other shared computers.

Dark Avenger

Bulgaria's most notorious virus vandal was a skillful, talented, and clever programmer who used the alias Dark Avenger.

Dark Avenger surfaced in the spring of 1989. A contagious new virus, the first "fast infector," infected targeted files as soon as they were opened. The virus contained the message, "This program was written in the city of Sofia, 1988–89—Dark Avenger." (Sofia is the capital of Bulgaria.)

Dark Avenger uploaded computer viruses to European BBSs (Bulletin Board Systems). Sometimes he packed viruses in Trojan Horse booby traps. When the Trojan Horse programs triggered, they spread the viruses through the victim computer system.

One could call Dark Avenger a "technopath," in that he used technology to indiscriminately harm society. Along with the vicious, destructive desire evident in his virus designs, he has said that, for him, "destroying data is a pleasure," and he "just loves to destroy other people's work."

Dark Avenger left enough clues in his handiwork to lead virus sleuths to a good guess at his identity: a young programmer working for a small, private software firm in Sofia. But there was no point in trying to turn him in—despite the damage he did, he was breaking no law by doing it.

Virus-Spreading BBS

In November 1988, a computer phone-in BBS that spread viruses started up in Sofia.

Run from the home of sysop Todor Todorov, a young computer science student, the BBS uploaded and downloaded both anti-virus resources and active viruses and virus source code. Named the “Virus Exchange BBS,” it described itself as, “A place for free exchange of viruses and a place where everything is permitted!” It boasted a zoo of more than 300 live computer viruses.

The price of membership on the BBS was an upload of one new virus to the collection. Creating a new virus was the easiest way to do this. Uploading it then gave access to downloading all the others. Running on a “no-questions-asked,” basis, the BBS let virus hackers use aliases. Electronic conferences spread “how-to” virus-building information.

Worse than live viruses, spreading virus program source code gave hackers what they needed to make endless new viruses. Changing the program code by, for example, adding new code for new functions, created a new, unique virus.

Hacking and cracking were not only tolerated, they were part of national policy.

The End of an Era

In 1993, virus activity in Bulgaria subsided as swiftly as it began. The BBS shut down, Dark Avenger disappeared, and other virus programmers struggled on with careers in the corrupt, destitute Bulgarian economy, or left to work in the West.

A costly legacy lives on: Computers never again can be seen as totally safe or secure. Technology and techniques developed then are used today, and the ongoing virus threat takes its toll in time and money.

One postscript: In January 1997, someone using the alias Dark Avenger—perhaps the original, perhaps an imitator—hacked into the Sofia University computer system, taking complete control for two days. Masquerading as a legitimate sysop, he managed to fool systems in both Bulgaria and the United States into allowing him access. ❏