No. 2003/01029/X1

Neutral Citation Number: [2003] EWCA Crim 2288
IN THE COURT OF APPEAL
CRIMINAL DIVISION

Royal Courts of Justice
The Strand
London
WC2A 2LL

Monday 21 July 2003

B e f o r e:

MR JUSTICE PENRY-DAVEY

and

MR JUSTICE AIKENS

R E G I N A

- v -

SIMON LEE VALLOR

Computer Aided Transcription by
Smith Bernal, 190 Fleet Street, London EC4
Telephone 020-7421 4040
(Official Shorthand Writers to the Court)

MR G VAN STONE appeared on behalf of THE APPELLANT

J U D G M E N T

(As Approved by the Court)

Monday 21 July 2003

MR JUSTICE PENRY-DAVEY:

1. On 20 December 2002, in the Bow Street Magistrates' Court, this appellant pleaded guilty to three offences of releasing computer viruses onto the internet under section 3 of the Computer Misuse Act 1990. On 21 January 2003, in the Crown Court at Southwark, he was sentenced to two years' imprisonment on each concurrent. He appeals against sentence with the leave of the single judge.

2. The offences were committed over a period of about six weeks. On each occasion the appellant wrote the virus code and sent it out to the internet where it travelled through e-mails. The first virus, subsequently named "Gokar" was detected in the internet around 5 December 2001. By the time a search warrant was executed at the appellant's home it had been detected in no fewer than 42 different countries and computer systems had been stopped 27,000 times. It was at that time the third most virulent virus in the world. There was expert evidence that the virus infected a substantial number of organisations, companies and home users around the world, and was still doing so in September 2002. Its effect was highly disruptive, but not destructive in terms of lost data.

3. The second virus known as "Redesi" also operated as a worm, arriving in an e-mail message, but like the third, known as "Admirer", its destructive capability was enormous in that it was programmed to bring the operation of computers to a stop and then, when they were re-booted, to remove all material on them which had not already been saved.

4. The appellant was traced through postings to various internet bulletin boards in the name of "Gobo". That user name was traced by the Computer Crime Unit to a BT internet access account registered to the appellant at his home address. A search warrant was obtained on 8 February 2002 and executed on 14 February.

5. The appellant was arrested and interviewed. He made full admissions.

6. It appears that the actual amount of damage caused by the Admirer virus was small because the police had moved quickly to find the appellant shortly after it was created. The extent of the damage caused by the Redesi virus is unknown, but estimated by the appellant to have affected the material on between 200 and 300 computers.

7. In passing sentence the judge identified a number of aggravating features of the offences, including the actual and potential disruption of computer use on a "grand scale". He identified the planned and very deliberate nature of the offences, calculated and intended to cause disruption, and the fact that they were not isolated offences but committed over a period of time. Equally, he indicated that he took into account the significant mitigation in the case, including the appellant's young age and previous good character, the fact that he had pleaded guilty and had co-operated with the police, and, against the background of the tragic death of the appellant's mother, that the appellant and his family had suffered a very difficult time. He pointed out that criminal conduct of this kind has the capacity to cause disruption, consternation and even economic loss on an unimagined scale which required the imposition of a deterrent sentence. He indicated that the appropriate sentence in the absence of the significant mitigation would have been four years' imprisonment.

8. On behalf of the appellant it is submitted that, having regard to the maximum sentence of five years for the single offence under section 3, the judge's starting point of four years was too high. Mr Van Stone submits that there are seriously aggravating features that are absent

from this case. He gives examples of such, including the creation of highly sophisticated viruses that are harder to detect; viruses that are created expressly to cause great economic damage, for example, to affect accounting, banking, commercial or security systems; and the creation of viruses the origins of which are deliberately difficult to trace, for example by the use of false names or by the use of corporate computers.

9. There may well be cases in which the combination of aggravating features make them more serious than this case; but in our judgment the judge correctly identified the aggravating features in this case and its element of persistence. Consequently, he was entitled to take a very serious view of this series of offences. As he pointed out, this was not an isolated occasion, but a persistent, calculated, disruptive and actually and potentially destructive course of conduct involving three offences over a period of time. In our judgment, in all the circumstances his starting point was not too high. He properly gave significant credit for the substantial mitigation in this case. In our judgment, the sentence was neither manifestly excessive nor wrong in principle. The appeal is accordingly dismissed.

10. There will be no Recovery of Defence Costs Order.