For discussion
on 28 January 2003

<div align="center">

Legislative Council Panel on
Information Technology and Broadcasting

Issues Relating to the Computer Worm "SQL Slammer"

</div>

PURPOSE

This paper briefs Members on the situation in Hong Kong in respect of the global outbreak of the computer worm commonly known as "SQL Slammer".

THE OUTBREAK OF SQL SLAMMER

2.   SQL Slammer is a computer worm that started massive spreading globally on 25 January 2003 (Saturday).   The worm exploits a known vulnerability in a database software. This vulnerability was first identified in July 2002 and the vendor of the software had made publicly available a software patch to rectify the problem.   Users of this software can prevent the attack of this worm by installing the patch.

3.   The worm is a small computer program that quickly copies itself and sends rapid data requests in search of other vulnerable server computers over the interconnected network. The damage caused by the worm came from the way it overwhelmed networks by quickly cloning itself and spreading to other computer servers.

4.   The impact of the worm was first reported by international news sources when worldwide Internet traffic experienced slow performance for hours on 25 January. According to some news reports, the worm crashed almost all Internet services in South Korea. South Korea's largest web access provider KT Corp. was reportedly brought down and other web sites were taken offline.   In the United States, Bank of America Corp. was reported to have

said that customers were unable to process transactions at the majority of its automated teller machines as a result of attacks by the worm. It was also reported that significant slowing down of Internet network traffic was detected in India, Japan and the Mainland of China. According to a news report in the Mainland, the Internet Society of China had taken emergency measures after detection of the worm and brought the situation under control by close of 25 January. Official sources from India and Japan said that no major problem had been detected.

IMPACT IN HONG KONG

5. Upon notification of the incident, both the Information Technology Services Department (ITSD) and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT/CC)[1] have published relevant information on their web sites on 26 January to alert members of the public about the worm and provide information on preventive measures.

6. As of 27 January 2003 (Monday), HKCERT/CC has received a total of eight reports from the public either on infection by the worm or the slowing down of Internet connections. Some local universities also experienced network slowdown in the afternoon of 25 January but the problem was rectified in the evening. Major local banks and Internet service providers have not reported any impact of the worm on their operations.

7. As regards the situation within the Government, the ITSD had already issued security alert of the vulnerability and distributed the related software patches to Government bureaux and departments in July 2002, when it first received information from the respective sources. A reminder had also been issued to all computer users in the Government to draw their attention to the worm. We have not received any report that Government departments have been affected by the worm in this incident.

---

[1] HKCERT/CC is a not for profit organization funded by the Innovation and Technology Fund and was established by the Hong Kong Productivity Council in February 2001 as the focal point to coordinate the reporting and response to computer security incidents for local enterprises and individuals, facilitate information dissemination, provide advice on preventive measures against information security threats and promote computer security awareness.

8.   According to the preliminary assessment of the HKCERT/CC, the impact of the worm on Hong Kong is under control.

LINKAGE OF THE WORM WITH HONG KONG

9.   As the worm attack started at around midnight of US Eastern Time (0500 GMT) on 25 January, some computer security experts suspected that the worm might have been "seeded" in a number of machines by someone in the US, while some other experts suspected that the worm might have originated from Asia.

10.   One overseas news report linked the worm with Hong Kong, alleging that it originated from here. However, the statement was removed from the web site of that news agency shortly afterwards. So far there is no evidence suggesting that the worm is associated with Hong Kong.

PUBLIC EDUCATION ON IT SECURITY

11.   The Government attaches great importance to strengthening information security and providing a secure environment for the conduct of e-business in Hong Kong.   To develop a secure and reliable e-community, public education plays a key role and the ITSD has undertaken a wide range of initiatives to enhance the awareness and knowledge of businesses and the general public to protect their computing assets. In the present case, if users had adopted the best practice of applying relevant software patches soon after they were issued by the vendor, infection by the worm could have been prevented.

12.   The ITSD's public education and publicity programmes include organization of exhibitions and seminars in collaboration with industry support bodies, and production and distribution of promotional and reference materials for businesses and the general community. It has also set up the INFOSEC web site (www.infosec.gov.hk), a one-stop portal providing resources and updates on information security targeting at specific needs of different groups such as students, youngsters, parents, teachers, IT professionals, and small and medium enterprises (SMEs), etc.   A new announcement in the public interest on

information security has also been produced and broadcast on television since December 2002.

13.　　　In addition to continuing with these initiatives in 2003-04, the ITSD is producing a series of short radio programmes to educate the public and raise their awareness of information security and prevention of computer crime. The programme is scheduled to be aired from March till the end of 2003.　The ITSD is also producing an Information Security Handbook for local SMEs and the general public to raise their awareness and knowledge of information security, in collaboration with the Police and the HKCERT/CC.　This handbook will be available in the first quarter of 2003.

Information Technology Services Department
January 2003