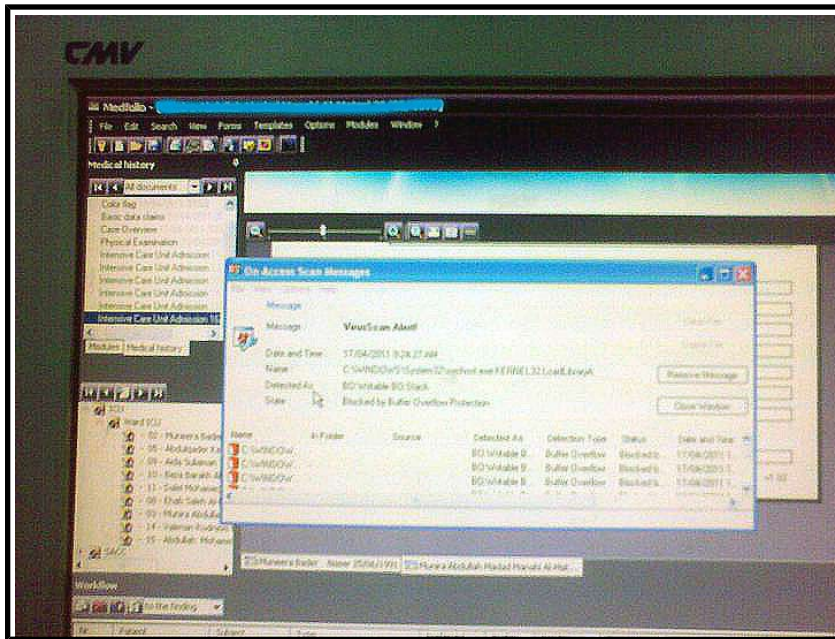


When Viruses attack ICU

By **Hussein**

Created **04/22/2011 - 22:43**



Intensive Care Units (ICU) are places in hospitals where people with special care are placed. Those people need continuous monitoring for their condition. These units are normally equipped with high tech patient monitor machines, ECGs, and ventilators.

Furthermore, ICU's normally keep higher standard of infection control to make them invulnerable to all kinds of infections due to the critical condition of its patients.

e-Infection !

Last week I was in Al-Amiri hospital, Kuwait. I was doing maintenance to a portable xray machine. There, I was struck with a view on all PC screens. Those PC's were running Critical Care Information system.

In fact, all screens were showing a Mcaffee Virus Alert. The list; as you see above, is showing multiple virus infections.

Even though ICU was equipped with high-tech patient monitors, ventilators and looked very clean and dis-infected, but it was; actually, infected with a special infections. These infection have no direct harm to the patient but they eventually do a harm !

How does a computer virus threatens life?

In these days, patient monitoring is not done at each bed. Each patient is monitored centrally by nurses & medical staff; i.e., at the nurse station. Thus, *interruption in flow of clinical data* between patient monitors and central monitoring system will *definitely interrupt monitoring the vital signs* of critically ill patient's .

Second; at critical care stations, physicians make electronic requests; i.e., for lab or imaging procedures. Virus infections can make those PC's slow or make them completely down by corrupting some files. In fact, *delay in exam requests is definitely a life threatening.*

Third, at critical care stations, physicians write there reports, notes or prescribe patient's medication. Virus threats on those stations; again, will delay the whole process at the ICU. Delay is not a good sign of a good ICU.

On the ground..

Frankly speaking, this ICU was not the only place in Ministry of Health where I have seen such virus attacks. Many places like *neonatal ICUs*, Radiology Departments, Cardiology, and Nuclear Medicine had the same issue.

In 2008, one year after world-wide attacks of a well know electronic worm (special viruses). the worm (or Trojan) with different names such as (DownaDop, Conficker, etc...) have hit most of ministry's information systems in a mater of a week. Moreover, xray and ultrasound machines were also hit by this worm specially those with MS-Windows XP were badly hit. Around 6

Xray machines went totally down due to network problems.

Finally, we have to admit that hospitals in Kuwait are in trouble ! In near Future we might see a crisis due to the fact that the no. of medical equipment getting connected using TCP/IP networks is exponentially growing.

Problem and Solution !

The problem is not actually the "virus attacks", virus attacks happen every day and everywhere, the problem is lack of network security , and maintaining that ! In fact, If you are connected to the outside world then you are at risk ! you don't have to be connected to the internet, allowing use of removable storage devices (i.e. USB sticks) is the biggest source of invulnerability.

The solution is not easy but affordable and better to start now than never. Effort to set standards for security in eHealth and for medical devices is going on. HIPAA is one example of such standards. HIPAA is a governmental act in USA to assure security and privacy of patient's health records. Some of these requirements are securing health records from viruses.

Moreover, an effort was taken by U.S department of veteran affairs to design a model for secure network of medical devices. See Excellent readings. Another effort was taken by Society of Hospital Information Management Systems (HiMSS) to encourage a medical device security disclosure like DICOM conformance statement. See Excellent Reading below.

In Kuwait, the gap is very huge. We should immediately start somewhere. Neither we have IT team in hospital nor Biomedical Engineering departments have experience or a say in this.

Thus a very rough plan should be divided into three stages.

- **Stage 1.** Putting IT security standards on our list of priorities.

-

Stage 2

. Forming an independent IT support team in the hospital independent from medical device vendor. If MOH claims that they don't have enough resources, IT team doesn't have to be through local staff, IT can be outsourced just like electrical maintenance or waste Management.

-

Stage 3. To Include IT support, Network management, and network security in medical device RFP, and the service contract (service level agreement.)

Excellent Readings..

- [When medical-device gets sick. Ellen Messmer, NetworkWorld.com, 2004](#)^[1]
- [Medical Device Isolation Architecture Guide, Department of Veteran Affairs, USA. 2004](#) ^[2]
- [Trends in Medical Device Security. HiMSS.org \(Bibliography\)](#) ^[3]
- [Cybersecurity for](#)