

# OT: Quebec Health Care Virus

---

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2007-02/msg01175.html>

---

- *From:* JF Mezei <[jfmezei.spamnot@xxxxxxxxxxxxxxx](mailto:jfmezei.spamnot@xxxxxxxxxxxxxxx)>
  - *Date:* Wed, 21 Feb 2007 15:31:06 -0500
- 

This came to me from an untrusted source, but appears legit. Last week, the Quebec health care system came to a grinding halt due to a virus infection. (Hey Cerner, time to start taking government ministers to lunch to get the contract to rebuild this). This has been fairly hush hush in terms of details because we are just going into an election.

Notes: because of separatist philosophy, Quebec now uses "national" instead of "provincial".

But it does give some insight on how a large network of Windows Pcs cane come to a grinding halt.

####

First excuse my English, this is not my native language.

As some people want the inside of the story, here what really happened and is still happening as the situation is still not in control.

First some topology.

The Quebec health computing network (RTSS) has a pyramid structure. At the top of the pyramid there is what is called the "technocentre national" it can see all ip addresses in the network. Each administrative area in Quebec as a "technocentre regional" that can see all the ip addresses of their area.

Each hospital can not see other hospital as they are at the bottom of the pyramid. For an hospital to see another hospital ip address, forms has to be filled and an explicit route has to be configure for the two ip addresses to be able to see each others. The good thing of this architecture is that every hospital (and other services provider) is isolated.

The bad thing is if a virus gets up to the technocentre notional it can affect the entire network and make big damage.

Now some history

The RTSS has been around for now almost ten years, it is still based on old technology and the network link are not good (lots of 128, 256

and 512 kbps). Which means it is hard to do remote work, like deploying patches updates and other things.

There have been promises for the last five years to update the network but as it is an exclusive contract sign between the GTQ and the Quebec ministry of Health it is hard to have things moving before the end of the contract.

During the past 4 years, the health ministry has put a lot of pressure on the hospital to address security in the IT, but no new money has been injected. Therefore hospitals prefer to diminish the waiting list than investing on IT that still work.

Another move is for the ministry to rationalise the IT departments. That means that whenever possible software should be installed in the Technocentre regional or national instead of the hospital. This is supposed to bring scale fund saving. (This has an important part to play in this virus attacked).

The Quebec health network is composed by 90 000 pcs and more than 2000 servers. The average technician per pc ration is 1/200. That explains a lot on why there are still some windows 95, 98, NT workstations. There is no specific funding for the IT and hospital have to decide either to give services or to replace PCs. And as the waiting list are closely watch by the ministry, guess what they choose.

The virus attack

The virus (worm) was effectively the WORM.RINBOT.C worm. The attacked started two weeks ago in a hospital somewhere in Quebec.

The thing to do would have to remove this hospital from the network until the hospital has been cleaned and therefore the hospital would have been the only one contaminated.

But as they are more and more application that are housed at the technocentre regional, therefore disconnecting the hospital would have mean no radiology, no lab results,...

So the hospital was left on the network, has contaminated the technocentre regional that has contaminated the technocentre national that has contaminated all areas of Quebec.

The worm started spreading without control in the night of the 13th of February. On the 14th of February, a national security alert has been raised. But at that time most of the routers were already out of order because that one of the thing that the worm does is a DOD attack. The security alert asked us to clean all the infected servers, windows 95, 98 and NT workstation.

The virus doesn't attack XP workstations (with SP2).

On the 15th the situation got really completely out of control because more and more workstations get infected and some hospitals lost

completely their network connectivity. (despite the official announcement that stated that everything was fixed issued on the 13th of February).

So on the 15th of February desperate measures were taken.

First the internet access was closed (it is only at that point that we can be sure that no information was transmitted by the virus). We still do not know what information has been transmitted by the virus during the days it was active on the network. One thing is sure is that information was exchanged and that the virus was trying to contact an external site to exchange information.

Second the technocentre national asked that the 90 000 pcs were rebooted during a 6 hours window from 3pm to 9pm.

The measures were efficient for some areas and on the 16th the virus was less active and almost eradicated in some areas. Mail services were restored.

On the 19th the internet connection to the outside world has been restored for areas that did not show virus activity. A proxy has been put in place to manage the internet traffic because up to that time internet traffic was not monitored.

And we are waiting for the situation to be in control in the entire province.

As for the router logs, the logs have been turned on only after the facts and when the traffic was less because it was unmanageable.

What is upsetting is that the media just relay the information given but the ministry without investigating.

This was a major failure in the health network as some hospitals were not able to work during three days. They had to go back to paper. Areas that had put the VOIP did not have phones. But the government is going into election and therefore nothing has to be said as it looks really bad.

Hopes this will give you the information you were seeking.

#####

.