

---

# CBC TECHNOLOGY REVIEW

---

Issue 2 - June 2006

www.cbc.radio-canada.ca

## Computer Security: A Broadcaster's Challenge

By Paul Rouleau  
Director, IT Architecture  
CBC Technology

---

### ABSTRACT

During the Torino Olympics, CBC/Radio-Canada had to face one of the toughest challenges a broadcaster's information technology (IT) support group could face: fighting a computer infection in production systems while covering a major live event. Fortunately, the emergency response team managed to keep the infection out of the systems used for the Olympics coverage. No impact was ever visible on-air. But the lessons remain. Computer security is not a technology one can implement. It is a process that requires active participation from all players: IT operations, media maintenance and suppliers. In particular, suppliers of broadcast software must understand that security is a requirement for their systems; without it, their customers are vulnerable to attack.

### INTRODUCTION

The XX Olympic Winter Games were held in Torino, Italy, from February 10<sup>th</sup> to February 26<sup>th</sup> 2006. While covering this event, CBC had to struggle with a computer infection that lasted for about a month from the first incident detected on February 15<sup>th</sup> 2006 to the last reported infection on March 14<sup>th</sup>. It put great stress on the IT support and media maintenance teams. Fortunately, it did not affect the programming and no impact was visible to the audience. But the alert was serious enough to highlight the importance of security.

### Why Security Matters to Broadcasters

Security professionals sometimes say that security is a triangle with three components: availability, integrity and confidentiality.

- **Availability** refers to the fact that computer systems are working and available for use. One purpose of computer security is to make sure the systems will be resistant to attacks and disasters and remain able to perform their functions.

- **Integrity** refers to the ability of systems to function properly with accurate data. For example, lack of integrity could cause an on-air event to occur out of schedule or to have the wrong content aired.
- **Confidentiality** refers to the ability to restrict access to data to authorized persons only. For example breach of confidentiality may result in copyrighted material being leaked on a peer-to-peer network on the Internet.

This triangle makes it clear that computer security has direct ties to heart of broadcasters' operations. The importance of security is reinforced by a phenomenon called Metcalfe's law<sup>1</sup>:

*The value of a network equals approximately the square of the number of users of the system ( $n^2$ )*

This law is sometimes explained using fax machines as an example. One single fax machine is useless. If there are two fax machines, then their use is limited because they can only talk to each other. If you have millions of devices connected to the public phone network, then faxes become a very convenient technology. The usefulness is approximately proportional to the number of possible connection pairs, which is approximately proportional to the square of the number of devices—hence the formulation of the law.

Metcalfe's law applies to every network of devices, be they faxes, telephones, Internet or corporate data networks. It implies that the more devices there are in a network, the more useful the network is. It also implies that one large network that includes every device is more useful than several smaller, isolated networks.

This last sentence is where computer security hits broadcasters hard. Broadcast systems have a history of being stand-alone islands not connected to anything else. Therefore, it was difficult for them to become infected. However, many stand-alone islands are less useful than a large, all-encompassing network. Over time, these islands get integrated and connected. Isolation stops being a viable security strategy. Examples of requirements that forced the interconnection of networks at CBC are:

- IT systems need to exchange schedule and as-run logs information with broadcast systems.
- Some broadcast systems are distributed across Canada and must use the WAN to integrate their components.
- Journalists need to access the Internet for news preparation.
- Journalists on the road need to file content using the Internet, including text, audio and video material.
- Support staff, maintenance technician and vendors need to log in to our broadcast systems from the Internet for remote access and support purposes.

The downside of this integration is that broadcast systems are more exposed to computer infections than ever before. But what is a computer infection? People who are uneducated in computer security call all infections “viruses” and believe that if they have anti-virus software, they are protected. This is not true. There are several types of infections. Countermeasures that are effective against one type will not work against another type. A comprehensive security strategy requires countermeasures against all types.

## Infection Types and Trends

Here are some of the major types of infection:

- **Virus:** this infection attaches some executable code to a file. Once the file is opened, the virus executes and infects more files. When an infected file is copied from one computer to another via file transfer, email attachment, Internet download or other means, the infection propagates.
- **Worm:** unlike a virus, this infection does not need to attach to an existing file. Worms propagate through the network hopping directly from computer to computer. Some worms use network applications like email and Instant Messaging for propagation.
- **Trojan:** this is shorthand for “Trojan horse”. This infection propagates through **social engineering** which is another way of saying techniques of deception. Trojans pretend to be useful programs you can innocuously execute or install on your computer. Users who are deceived by Trojans will manually infect themselves.
- **Backdoor:** this is a kind of infection that opens a path to the system bypassing all security. Backdoors allow remote unauthorized access over the network and make the computer vulnerable to further intrusions.
- **Downloaders:** a kind of backdoor that checks certain sites on the Internet for files to download. When the attacker puts a new file on the site, the downloader will install it on the infected computer, thereby allowing more infections to occur. Downloaders are insidious because they open the way to more infections of any type on the attackers' whim.
- **Rootkit:** this is an infection that alters the operating system, causing troubleshooting and diagnostics tools to report false data. The point of a rootkit is to hide other infections present in the system and make security countermeasures ineffective.
- **Spyware:** this infection examines the user's habits and the files installed on the computer, and reports the data to the infection originator. This is often used by shady marketing outfits to spy on the user's web surfing habits in order to send more targeted ads.
- **Adware:** this pesky infection often works in collaboration with spyware. Its purpose is to deliver unsolicited ads in the form of pop-ups or other means.

What happens when a computer is infected? This depends on the **payload**. Infections can be compared to containers. They can carry with them some other code that can do many other things. Some payloads put a heavy burden on the computer resources and make it unusable. Other payloads are meant to distribute advertising and pester the user with unwanted pop-up windows. A few years back, payloads were often pranks, sometimes destructive ones like deleting random files on the hard disk. Now we find payloads meant for monetary profit, like **keyloggers** that attempt to steal credit card numbers and banking account passwords.

Today a frequent use of payloads is the establishment of **botnets**. A botnet is a network of infected computers that is controlled remotely by the attacker at the source of the infection. Botnets can be used for a variety of purposes like sending spam emails and orchestrating DDoS attacks<sup>2</sup>. Access to botnets can be sold or rented on the black market for monetary profit.

The market has recently observed a change of trends related to infections. A few years ago, infections were often motivated by a dubious desire to achieve fame. The worm was designed to spread fast and wide. Once the infection occurred, it was easy to diagnose and the fix was obvious once you had the proper diagnostic. Newer infections are often designed to have a lower profile and propagate slowly but be hard to diagnose and hard to remove. In our adventures fighting the infection that occurred during the Olympics, we found it had the following characteristics:

- The infection involved a cocktail of several malicious software types, including two worms and several trojans, downloaders, spyware and adware.
- It was impossible to get a complete picture by doing forensics on a single PC because no single PC had the full cocktail of infections.
- One week after massive analysis and forensics, we were still having surprises. It took over two weeks to have a reasonably complete picture of what we were fighting and to develop effective countermeasures. Thorough cleaning required two additional weeks.
- The infection used multiple vectors of attacks. Filtering known vectors at switches and firewalls was not always sufficient because the infection would fall back on alternative vectors. New CBC locations were infected after being fenced with Access Control Lists (ACLs) to stop known vectors of attacks.
- The infection used multiple downloaders from multiple sources. It also included keyloggers and was reporting information to multiple sites on the Internet.
- Some downloaders were designed to reinstall themselves after they were cleaned.
- The infection was attempting communication on TCP (Transmission Control Protocol) ports dedicated to the Internet Relay Chat (IRC) protocol. IRC is often used by attackers for remote control of botnets.
- The infection included a worm that resisted our anti-virus software.
- The anti-virus vendor was unable to find the new infection and that kept saying he found only infections known to him in the sample we sent

This is in line with trends reported by security professionals. Modern infections often occur for monetary profit. The goal is to create a botnet and sell access to the infected computers for sending spam email or for other purposes.

Fortunately, the cocktail of infections did not include a rootkit. This would have made the infection even more difficult to diagnose and clean. Had a rootkit been used, complete reformatting and reimaging of all suspicious PCs' hard drives would probably have been the

only effective solution.

## Infection Propagation and Prevention

How can an infection get onto a computer? Three components are needed: a vulnerability, an exploit and an attack vector.

- A **vulnerability** is a weakness in a system or process that an attacker can use to infect the system. It can be a bug in the software, or a failure in a process, like a human being falling for a social engineering attack.
- An **exploit** is trick or technique designed to take advantage of a vulnerability. If the vulnerability is a software bug, then the exploit is something that will trigger the bug and use it to cause the software do something it was not intended to do.
- An **attack vector** is some kind of method that can be used to send an exploit where it can take advantage the corresponding vulnerability. Examples of possible attack vectors are email attachments, malicious web sites or network protocols.

There are three main methods of blocking infections:

1. One can make sure there is no vulnerability. For example, patching operating systems is a procedure that eliminates known vulnerabilities by fixing the bugs that cause them.
2. One can rely on the absence of exploits. This method is risky and short-lived because one never knows when the exploit will be developed.
3. One can rely on the absence of usable attack vectors. Keeping systems disconnected from the main network is an example of this technique. In this age when all networks tend to be connected, this approach has limited practical use.

An enhanced version of method 3 is to put filtering devices in the network, such as access control lists, firewalls, intrusion prevention systems and various types of security gateways. The attack vectors are present but hard to use for attack purposes. This works up to a point. But attackers are intelligent people who develop ways to bypass security measures. They develop attack schemes that use legitimate applications and protocols. Note that if the filters are too aggressive, they will disable legitimate applications as well.

This is an example of security being a process and not a technology. It is not sufficient to purchase and install filtering devices to block infections. One needs to examine the applications and configure the filters so that legitimate applications are allowed while providing the lowest probability of successful infection. This is an exercise in finding the right balance between network usability and security. It is also a continuous process because the filters need to be revised when new applications are deployed and new types of attacks are discovered.

Of the three main methods to block infection, preventing vulnerabilities is often the most effective. The current trend among attackers is to examine the security patches as they are released and then design an exploit for the corresponding vulnerability. They count on the fact that many people don't patch their systems; therefore, it's plain to see that not patching the systems is dangerous. Once a vulnerability is known, exploits will be written and attacks will

occur.

This is another example that security is a process and not a technology. There is a need for monitoring software vendors' patch releases, testing to ensure the patches won't disrupt the systems with new bugs, and installing them as soon as possible. When this process fails, computer systems are wide open to infections.

This is what happened during the infection that occurred during the Olympics. CBC has a strong practice of patching the Windows operating system whenever Microsoft releases new patches. This is done very systematically. But there were two kinds of cases where it didn't happen:

- a) In a few instances, the software that updated the computer was supposed to be there, but for unknown reasons wasn't activated. A critical patch that would have corrected the vulnerability used by the infection was not installed. It is not sufficient to install a patching process. There is also a need to check that it remains in place afterward.
- b) In a much larger number of cases, the infected systems were running broadcast applications that were incompatible with patches and anti-virus software. Unfortunately, several broadcast system vendors refuse to support their own software if it is installed on a computer with anti-virus protection or where the operating system is patched to the most recent level. In many cases, not only do these basic security measures invalidate the support agreement, but the anti-virus or security patches interfere with the proper operation of the broadcast software and cause either bugs or performance problems.

The infection would have been a minor problem if only the first problem occurred, because only a few non-critical computers were in this category. But the problem outlined above in point "b" did hurt. Vendors that won't support and make their software run on fully protected computers are behaving irresponsibly. Historically, this attitude was tolerable because it was viable to keep broadcast systems in an isolated environment, but this is no longer possible, at least not without foregoing the tremendous possibilities offered by modern networking.

## CONCLUSION

Unprotected broadcast systems create a paradoxical situation. Broadcast professionals see their networks as safe havens that must be guarded from all the problems that occur on enterprise data networks with filtering devices such as ACLs, firewalls and intrusion prevention systems. When infections like the one CBC faced during the Olympics occur, the opposite is true. The enterprise network is fully protected and immune from the infection while the unprotected broadcast systems remain at risk.

Countermeasures exist to mitigate the risk and protect the broadcast operations from infections. However, this is a reactive process that relies on the rapid intervention of the emergency response team. It is much preferable to proactively protect the broadcast systems with proper anti-virus and patch management.

Vendors are part of the security process. When they don't play their part, their customers' security is seriously weakened.



Paul Rouleau is CBC/Radio-Canada's Director of IT Architecture. He holds a Bachelor of Social Communications from University of Ottawa (1979), as well as a master's degree in computer science from Concordia University (1988). He began working at CBC/Radio-Canada in 1984 as a technical support programmer/analyst. Throughout his career with the Corporation, he has consistently held positions related to planning, setting up and supporting CBC/Radio-Canada's IT infrastructures and data transmission networks.