# Viruses and Worms: The Inside Story

By Tracey Losco
tracey.losco@nyu.edu

Connect Spring 2002





In today's almost completely interconnected world, it's likely that everyone reading this article has had his or her machine infected at least once. With people and companies making things more automated daily, many of our everyday transactions take place online. What does this mean? Why does this matter? Well, it means that we are spending more and more time using our computers, and it matters because this makes us more vulnerable to contracting a worm or virus.

**What are Worms and Viruses?**

Merriam Webster Online defines a worm as, "a usually small, self-contained computer program that invades computers on a network and usually performs a malicious action." They define a virus as, "a computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs and that usually performs a malicious action (as destroying data)." As you can see from these definitions, if you end up with either one, it usually results in trouble.

Those of you who have used and still do use Microsoft Word may be familiar with the macro viruses. At one point in time, if you shared a floppy disk with others, you were almost guaranteed to end up with a document that contained a macro virus. Sometimes these viruses were destructive and sometimes they were just annoying; there was one strain of the macro virus that simply converted your documents into templates...not really destructive--you only ended up with a whole bunch of documents whose symbols were a file with an arrow instead of a typical document symbol--but definitely annoying.

Viruses can also display messages and other images, as well as take up space on your computer. There have been some viruses that have gradually increased the amount of space that they take up. If you don't have a whole lot of space left on your drive this could be problematic; however in today's world of gigabyte hard drives this is less of a problem. As noted by the company Trend Micro in their Virus Primer, "If the virus doesn't contain a damage routine, it can still cause trouble by taking up storage space and memory, and downgrading the overall performance of your computer." (www.antivirus.com/vinfo/vprimer.htm).

What makes viruses and worms a big concern, however, is the fact that they can destroy files on your machine, and, in certain instances they can destroy your entire machine, leaving you with nothing to do but rebuild from scratch. Not only that, but they can use your machine as their base of operations for going out and infecting or damaging other individual computers or entire networks.

To make matters worse, there are many cases in which you wouldn't even know that you had a virus until someone told you that you had given them an infected file, or your anti-virus software all of a sudden started popping up alert screens on your computer.

**When are You Most Vulnerable to a Worm or Virus?**

This is a big concern for many people, and rightly so. In order to protect yourself, you need to know when you are vulnerable. If you are not running some type of anti-virus software, you are in the category of the highest possible risk for getting infected. If your computer is connected to a network, if you dial in to an Internet service provider, if you share files with anyone or if you surf the Web, you should definitely be running anti-virus software.

Students, faculty and staff at NYU are all entitled to free copies of Norton AntiVirus. The software is included on the NYU-NET CD--available at any of the ITS computer labs and the Client Services Center--and online at www.nyu.edu/its/software/. There is no reason why you should have a computer running without anti-virus software...in fact, to do so is downright flirting with disaster! Before installing Norton AntiVirus on your work computer, however, be sure to consult the information technology

personnel in your area.

Even if you have installed anti-virus software, you are still vulnerable if your virus definitions are not up to date. If the last time you downloaded virus definitions was on the same day you installed the anti-virus software, it's as if you don't even have the software installed. New viruses are released daily, so it's very important for you to keep your definitions current. Most anti-virus software has the ability to automatically download the definitions while still allowing you to also perform manual downloads if you want or need to, so there really is no excuse for not keeping your virus definitions up to date. (See the box below for more information.)

**What are Virus Definitions?**

Virus definitions are files that have information on certain behaviors, characteristics and signatures of various viruses. When downloaded into anti-virus software, these definitions allow the software to search the machine for specific attributes that match those contained in the definition. If found, the software is able to determine that the machine has that particular virus and either cleans it or, at least, notifies you that your machine is infected.

You may also be vulnerable to infection if your operating system is not up to date. Many viruses and worms take advantage of holes or vulnerabilities in operating systems. If you are running a Microsoft OS, you have the ability to check for updates right from the "Start" menu. All you have to do is click on "Start", then select "Windows Update", and you will be brought directly to the updates website (http://windowsupdate. microsoft.com). On the upper-left section of the page you will find a link for "Product Updates". When you click on this you will get a window telling you that Microsoft is customizing the product catalog for you.

Once you are there, you will see a section for critical updates and service packs--this is the most important section, so be sure to download and install whatever appears here. Also, keep an eye on the section for "Advanced Security Updates" and on the "Recommended Updates" for any software that you may be running.

There is a tool from Microsoft that will pop up an alert on your screen if a critical update is released. This tool is called the Windows Critical Update Notification tool. I would highly recommend downloading and installing this on your system so that you will be alerted as soon as any critical updates become available.

Historically, these updates have included fixes for many of the vulnerabilities within the OS and its components that have allowed viruses to spread. They have fixed vulnerabilities in Internet Explorer whereby malicious code included on websites using an < EMBED > directive is run when the user views the page. This vulnerability has caused buffer overflows as well as the transmission of viruses and worms. If you don't keep your OS up to date you are leaving yourself wide open to an infection.

**Who Creates These Things?**

It used to be the case that worms and viruses were created by people who had nothing better to do with their time. Most often the intent was to do some type of damage, with the possibility of bringing fame to the creator. Now they are sometimes created by your everyday programmer as a "proof of concept" project. These individuals come up with a unique new method of propagation, and just want to prove that it can be accomplished. These individuals may innocently release the code to a newsgroup or website where someone else with a less then ethical nature may then take the code and release or implement it.

The newest fear is that some sort of terrorist organization may latch on to these types of programs in an effort to do real damage. There have been many discussions about how potentially dangerous these types of programs are and could be if targeted at the right spot. A document was published in September of 2001 by the Institute for Security Technology Studies at Dartmouth College called "Cyber Attacks During the War on Terrorism: A Predictive Analysis." You can find a copy of the paper at www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf.

The paper discusses how we now have to be aware of vulnerabilities on our networks in the same way that we are aware of our physical vulnerabilities. With programs such as Code Red and Nimda, there is the potential for the destruction of key parts of an infrastructure.

**Infamous Worms**

Nimda and Code Red were the worms that really caused the everyday user to stop and take notice. These worms were so widespread that they even gained news coverage. What helped both worms achieve their claim to fame was the speed at which they were able to propagate, and their pervasive means of doing so.

Nimda's ability to propagate via shared drives, e-mail, and web pages made it almost unstoppable. As an added bonus, with its network scanning 'feature', it had the potential to go on to cripple local networks. Nimda's attacks started with a scan, in an attempt to find machines that weren't up to date with their OS patches. Once a vulnerable machine was found, it was infected. The worm then searched its new host for e-mail addresses and proceeded to mail itself out to every address it found.

As a final insult, Nimda checked for a running web server and, if one was found, added code to the web pages being served that enabled its continued propagation onto the computers of users viewing those web pages. But, again, it could only infect those machines that were not up to date with their patches. The worm also copied itself onto any network shares that were set up on the machine.

To sum up, this worm infected multiple Windows platforms, ran a denial of service attack, provided outsiders with full access to the infected machines and gave out administrator privileges, and, to top it off, it was hard to get rid of and spawned itself onto other machines in the blink of an eye. Pretty bad, huh?

The story really started, though, with another worm named Code Red and its descendent Code Red II. This worm also had a speedy rate of propagation; however, there was a timing phase coded into this worm. It would scan for a while, looking for machines to infect, and then it would perform a distributed denial of service (DDoS) attack against the www.whitehouse.gov website. It also left a back door open on the infected machines, which made it easier for the second version and Nimda to follow in its footsteps.

**How Can You Protect Yourself?**

When a virus or worm first appears, the anti-virus software developers may not yet have had time to create any protection against it. Nonetheless, the odds will still be in your favor if you have taken additional precautions to secure your machine. It's important to remember, though, that just because you are running anti-virus software doesn't mean that you are safe from all viruses.

Nonetheless, a first step in protecting yourself would be to get and install anti-virus software. You can also set up the software to perform scheduled scans of your drive in addition to automatically checking anything you download or attempt to access, such as a floppy or Zip disk. Another step to take in protecting yourself is to carefully screen the e-mail that you receive. You should always be especially careful of e-mail attachments. If you receive a message from someone you don't know and it has an attachment with it, the smartest thing to do is to delete the message without opening the attachment. This is a very common way for viruses and worms to be transmitted, so it's better to be safe than sorry.

Another way of protecting yourself is to pay attention to anomolies in your computer's behavior. Some of these programs open a virtual door to your computer, allowing others to gain access and possibly use it for nefarious purposes. A good rule of thumb would be to scan your machine on a periodic basis, and especially if you notice it acting strange. By strange, I mean if windows start opening or closing by themselves, if your machine starts to turn itself off when you've never scheduled it to do so, or if unfamiliar files or folders appear and you didn't put them there.

Your best defense is a good offense. Be careful with what you download and install on your computer. Only download shareware or other software from reputable sites such as www.shareware.com or www.versiontracker.com. Be wary of software sent to you by people you don't know, and make sure to keep updating your virus definitions. You can't be too careful nowadays, especially since more and more machines are being added to the Internet. You might want to check periodically with the anti-virus software sites to find out about the latest virus running rampant over the Internet. Symantec has a section entitled "Latest Threats" on their website (www.symantec.com) along with other useful information.

If you find that you still have a question after reading this article, we have a virus FAQ section on the security website that may already address your question: www.nyu.edu/its/security/virus-faq.nyu.

If you ever have any security-related questions, send us a message at security@nyu.edu, and we'll be happy to discuss it with you.

Surf safe!

---

*Tracey Losco is Network Security Analyst in the ITS Network Services Department.*