

Matt N. Wyman  
2903 Prospect Pkwy  
Durham, NC 27703  
Phone (919) 678-0823  
Email matt@northcarolinapcs.com

## **Technology Alliance - Article 2**

### **Viruses & Hackers**

#### **Keeping Systems Running Fast & Clean**

Back in the early 1980's I encountered my first case of a virus stricken computer. The virus was called "Scores" and it was on a Macintosh system. It is commonly believed that Macintosh computers don't get viruses, however back then Macs were on an equal footing with PCs and were thus equally targeted for infection by virus writers. These viruses tended to be more of an annoyance than a real threat and were fairly easily cured. However, viruses have since evolved into highly malicious programs that can evade detection, steal passwords, credit card numbers, online banking information and highly sensitive personal identifiers like Social Security numbers. Add to that the ability of viruses to take down and even wipe out computers, networks and personal data and you have a world of hurt that can be unleashed with a simple mouse click. The reason for the massive growth in the production of viruses is multifold. Some viruses are created to enrich their maker, they are launched or released and by design go out into the world harvesting sensitive monetary related information to be transmitted back to the

virus writer. This type of virus has been reported coming from Russia in the last few years. Perhaps this is because the collapse of the USSR left many talented programmers out of work and desperate for a means of income. Whatever the reason, Russia is tied to some of the 'nastiest viruses the technology world has ever experienced: Bagel, Mydoom, and Netsky, to name just a few' ([http://www.crime-research.org/analytics/Viruses\\_Russia/](http://www.crime-research.org/analytics/Viruses_Russia/)). The current world cup worst virus/worm is the "Storm Worm that dwarfs the world's top supercomputers" in its search processing power. Currently the FBI has investigated its source to the door of a Russian Web Server/Hosting company, but Russian Government officials have refused any further investigation. The Storm Worm has the additional nasty habit of attacking networks with a massive Distributed Denial of Service Attack when researchers investigated its origins.

Side bars aside, another common function of the modern computer virus is that of information theft. Not just Credit Card or Banking information (which is common) but company documents that contain key design data and concepts. These viruses like the "Myfip" worm, steal PDF, MS Word and AutoCAD files among others and are overwhelmingly of Chinese origins in recent years. It would appear that these viruses are aimed at targeting American companies Intellectual Property. Forbes magazine put it like this "The Middle Kingdom isn't just trying to buy American companies on the open market. It's also stealing industrial secrets by taking over corporate computers" (<http://www.forbes.com/global/2005/0725/022.html>).

Couple these information stealing viruses with the Hackers and you have a national security threat on your hands. For example, in 1994 hackers attacked computers at the Air Force's Rome Laboratory in New York, and stole data relating to the attack instructions that would be given to US warplanes in battle. While in September of 2007 the Financial Times, reported that hackers with the 'People's Liberation Army of China, broke into computer systems in the office of Defense Secretary Robert Gates - the Pentagon itself. The attack forced officials to take down the network for more than a week, the report said.'

Why do virus writers and hackers do these things? The reasons are many; one of them is *Greed* of a quick (stolen) buck. Another is *Power*; many of these viruses will cause the infected computer to report back to the virus writer, joining any number of other infected computers to create a 'Bot' army. These armies are powerful weapons that can be used to knock down websites, attack whole networks or even blackmail internet dependent businesses. Control & Self Aggrandizement are still other reasons virus writers and hackers do what they do. Virus writes and hackers have traditionally worked for themselves, but of late it seems more and more reports are surfacing of government sponsored hacker activity.

So there we have the problem, the rewards for this criminal behavior are many and catching these criminals is difficult. When the Pentagon gets hacked and some where in the neighborhood of 40 new viruses are created each day, security it seems is a hard thing to find. However, necessity is still the mother of invention. As such, solutions abound when you've done your homework. The number one solution for viruses is antivirus software. More than antivirus software however, it's knowing which antivirus software to use. To understand this we need to look at the facts regarding viruses and anti virus programs. It is an arguable fact that somewhere between 90 and 95 percent off all the computers sold in America come with either Norton or McAfee installed on them. Usually they have a 90 free trial period that most people pay for after the trial is up. This has been found to be the case in both East Coast & West Coast computer users and is passionately proclaimed by Norton's adds of most sold/trusted antivirus in the world today. What this means is that some 99% of the worlds virus writers write their infectious code to counter or penetrate the defenses of both Norton & McAfee antivirus software.

The simple logic is that if you, the virus writer, know that you will have a 90% chance encountering a "Sherman Tank" called McAfee or Norton then you will only be successful if you carry "Anti-Sherman Tank" weapons. This fact has been proven by our virus labs in past years, where the virus was found to disable Norton and actually hide in the Norton Program folder.

Norton and McAfee are both aware that the virus writers and hackers target their products and have worked hard to fix the weakness exploited by these criminal elements. Problem number two comes in here, the “fix” involves a heavy amount of program patching and extra code. We can use the analogy of the Sherman Tank to describe what is happening. Every time a virus writer or hacker creates a way to break Norton & McAfee, Norton & McAfee respond by putting a piece of “metal plate” code over the hole. This has gone on for such a long time that the whole tank is covered with patches and is completely weighed down by these extra armor fixes.

The result is that every time Norton or McAfee run through the downtown of your computers business sector all your business stops... Who knows maybe the “shop owners” of Quickbooks, MS Word & other programs are out on the street waving to Norton or McAfee’s tank as it goes by?! What’s the solution, use antivirus, but don’t use the slowest, heaviest, most targeted antivirus programs money can buy! Switch to something like Panda, Bitdefender or AVG. Each of these programs is sleeker, runs more quickly and causes less slowdown of your system. They are proven to be just as effective & in our studies were actually found to be more effective than Norton or McAfee in catching and removing viruses.

The Technology Alliance Newsletter Articles are brought to you by North Carolina PCs online at [www.northcarolinapcs.com](http://www.northcarolinapcs.com)