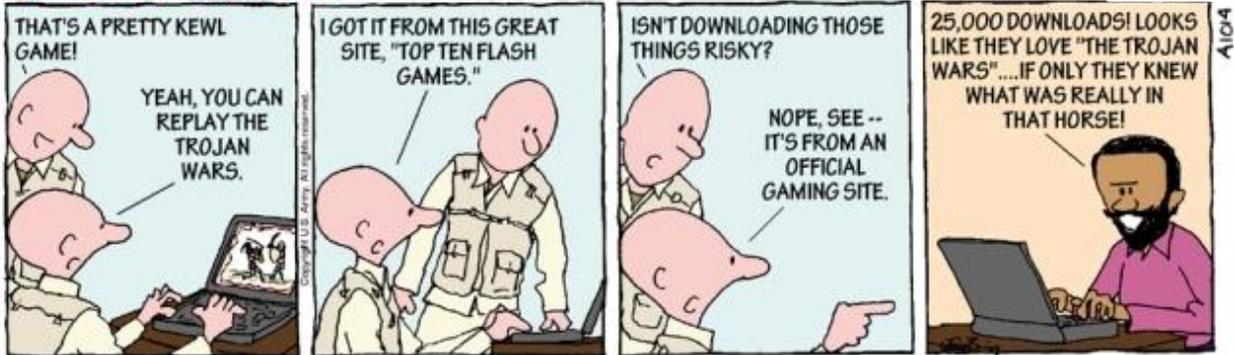


Lessons From the Past Make Good Horse Sense

November 2006



ON CYBER PATROL



Military strategists still study Alexander the Great's tactics against the Persians at the Battle of Issus. It is an excellent example of the tactical feint and illustrates the value of cutting off command and control. The tactics of the past still work today, even in cyber space. For example, the computer attack known as a Trojan Horse derives its name from the mythological battle for the city of Troy where the Greeks, frustrated by years of war, employed tactical deception by building a massive wooden horse that they left at the gate to the city as they sailed away apparently in defeat. Unfortunately for the Trojans, inside was the Greek version of a Special Ops team. The gullible Trojans dragged the horse inside the city walls and at night the Greeks climbed down, opened the gates for the returning Greek army that sacked Troy with extreme prejudice.

In tech talk, a Trojan Horse is malicious or destructive code embedded in a seemingly innocent program. Trojan Horses are often found in "free" content on the web and are usually introduced to the computer when downloading seemingly innocent software. While Trojan Horses do not spread like viruses, they are often spread by users who are sending applications to their family and friends.

Trojan Horses come with a wide array of attack strategies and can do a great deal of damage if they end up on your computer. Some are extremely destructive and will corrupt or erase valuable files, possibly making your computer useless. Others will disable your protection software leaving your computer completely vulnerable to cyber attacks. A proxy Trojan can use your computer for criminal activities such as launching cyber attacks or committing credit card fraud. Some will collect your data, IDs and passwords and send it to the attackers. A File Transfer Protocol (FTP) Trojan opens your computer and lets someone have access to all of your files via FTP. All the data on your computer can be easily transferred to a thief or the enemy. Some Trojans can give remote users access to your computer as if they were at the keys themselves.

Many Trojans are difficult for anti-virus software to detect and can easily slip by typical defenses, especially when they are voluntarily introduced to the machine. The defense is simple. Don't bring a horse into the city or your computer. Computers that have access to any military resources or contain any information that could compromise Army operations and personnel must be protected. Downloading any unauthorized software, no matter how innocent it may seem, puts the entire contents of a computer at risk. Even computers that have no military use could give up data that will give hackers and our enemies' access to personal information. This could put your loved ones, friends and yourself at significant risk.

So beware what you download. The game of the month could become the headache of the year. Compromised data or security information makes you vulnerable to the common criminal or the fanatic insurgent. It could put your family in danger. Even worse, it could cost fellow soldiers their lives.