

1 December 2008

By: Lucian Constantin, Web News Editor



U.S. military networks targeted by Chinese and Russian hackers
Defense Tech

[Cyber-Attack Cripples Critical U.S. Military Networks](#)

A military base in Afghanistan was seriously affected

After the U.S. Strategic Command [banned](#) the use of removable media on the army's networks last week, new details about the incidents that might have triggered this drastic decision surfaced. The networks of the U.S. Central Command, which oversees the operations in Iraq and Afghanistan, have been crippled, while 75% of the computers in major military base in Afghanistan have been infected with a worm that spreads through such external devices.

According to [U.S. News and World Report](#), the cyber-attack at the base in Afghanistan is believed to have originated in China, and was not the first of its kind. These attacks aim at extracting secure information from the military computers, and have been successful into copying details about troop and convoy movements before. It is still not clear what and how much information was leaked out, as a result of this last incident.

According to the same source, there is still no indication whether the Chinese hackers were sponsored by the government in Beijing or if they were working independently. This seems to be a recurring question that never gets its answer, even though it is not the first time that attacks on U.S. government systems originate in China. Recent such incidents include the penetration of Pentagon computer systems, the hacking into the election campaigns' networks of both Barack Obama and John McCain, and the compromise of the White House unclassified network.

All these security breaches resulted in data being leaked out, even if it was not necessarily vital or classified in nature. An U.S. official explained that the Chinese intelligence service was known for an information gathering technique called the "grain of sand," which involved analyzing huge chunks of what might look as low security level data, in order to discover just a small piece of vital information.

At the same time, the [Los Angeles Times](#) reported that at least one highly classified network at the U.S. Central Command was compromised by a similar computer worm. The seriousness of the incident prompted the senior leaders in the military to brief President Bush on the security breach, and, at the same time, to raise the level of the INFOCON alert condition. INFOCON (Information Operations Conditions) is the military computer security equivalent to DEFCON. According to the yet scarce details, this attack is believed to originate in Russia.

Russia is no stranger to cyber-war, proving the effectiveness of such tactics back in 2007 when a Russian attack effectively crippled the network of the Estonian government. A wave of attacks from Russia resulted in over 300 websites in Lithuania being [defaced](#) after the Lithuanian government banned the display of the old soviet red flag or other communist symbols. More recently, attacks originating in Russia have [targeted](#) the Georgian government computers during the armed conflict between the two countries. The involvement of the Russian government in the attacks has yet to be proven.

Military officials expressed concern, because, according to them, these attacks were not random. Instead, the malware detected on their networks, was particularly designed to target military computer systems. The hackers "learn a lot from these attacks, [⋯] like

how our logistics and other systems work," warned an U.S. intelligence official.