

By ~~October 2008~~ Constantin, Web News Editor

[South Korean Military Equipment Development Secrets Compromised by Hackers](#)

Spyware was identified on the networks of two critically important manufacturers

The South Korean defense industry is at great risk as the National Security Research Institute announced that malicious spyware applications had been detected on the networks of two major manufacturers of military equipment. The LIGNex1 and Hyundai Heavy Industries produce critical defense weapons valued at tens of billions of dollars.

LIGNex1 is the manufacturer of several types of guided missiles, like Hyunmoo (surface-to-surface), Haeseong (ship-to-ship) and the Shingung (ground-to-air) portable weapon. The exact amount of money invested in the development of such weapons is not public knowledge but, for example, each Hyunmoo is said to be valued at over \$1.6 million. LIGNex1 were the first to discover that their network was compromised with complex malware which, according to them, was installed back in March.

The other manufacturer, Hyundai Heavy Industries, is building naval vessels like destroyers and submarines. The company is also building the country's first ever AEGIS ships, the King Sejong the Great class of destroyers. The lead ship, which has undergone one and a half years of tests since its launch, is expected to be commissioned in 2008 and its cost is estimated at a whopping \$923 million. The company discovered the presence of the malicious applications on their network last month.

The Koreans suspect that their less democratic neighbors are responsible for these incidents. "The research institute suspects the culprits are Chinese or North Korean hackers but doesn't know specifically what information they stole," noted an official. "In the worst case, the blueprints of missiles and Aegis ship could have been stolen," he added.

This is not the first time that South Korea is accusing the North Koreans of [cyber attacks](#) against them, or the use of the Internet infrastructure for espionage. Earlier last month, South Korean officials claimed that their communist neighbors had attempted to hack into the computers of several military officers by sending them an e-mail which contained a data collecting spyware program.

Also, earlier this year, a North Korean woman was arrested in a Mata Hari-like spying investigation. She was accused of providing classified information to the North Koreans after posing as a defector since she moved to South Korea in 2001. Apparently, she used the opportunity of giving anti-communist lectures in military units in order to gather secret information from army officers, to which she was offering "personal services" in exchange.

"It's shocking that our major defense industries are open to attacks from hackers and that our missiles are vulnerable to theft by cyber terrorists. A general review of our cyber security system is needed," is noted in a official statement.