FCWCOM

Cyber officials: Chinese hackers attack 'anything and everything'

BY Josh Rogin

Published on Feb. 13, 2007 NORFOLK, Va. -- At the Naval Network Warfare Command here, U.S. cyber defenders track and investigate hundreds of suspicious events each day. But the predominant threat comes from Chinese hackers, who are constantly waging all-out warfare against Defense Department networks, Netwarcom officials said.

Attacks coming from China, probably with government support, far outstrip other attackers in terms of volume, proficiency and sophistication, said a senior Netwarcom official, who spoke to reporters on background Feb 12. The conflict has reached the level of a campaign-style, force-on-force engagement, he said.

“They will exploit anything and everything,” the senior official said, referring to the Chinese hackers’ strategy. And although it is impossible to confirm the involvement of China’s government, the attacks are so deliberate, “it’s hard to believe it’s not government-driven,” the official said.

The motives of Chinese hackers run the gamut, including technology theft, intelligence gathering, exfiltration, research on DOD operations and the creation of dormant presences in DOD networks for future action, the official said.

A recent Chinese military white paper states that China plans to be able to win an “informationized war” by the middle of this century. Overall, China seeks a position of power to ensure its freedom of action in international affairs and the ability to influence the global economy, the senior official said.

Chinese hackers were responsible for an intrusion in November 2006 that disabled the Naval War College’s network, forcing the college to shut down its e-mail and computer systems for several weeks, the official said. Forensic analysis showed that the Chinese were seeking information on war games in development at NWC, the official said.

NWC was vulnerable because it was not part of the Navy Marine Corps Intranet and did not have the latest security protections, the official explained. He said this was indicative of the Chinese strategy to focus on weak points in the network.

China has also been using spear phishing, sending deceptive mass e-mail messages to lure DOD users into clicking on a malicious URL, the official said. China is also using more traditional hacking methods, such as Trojan horse viruses and worms, but in innovative ways.

For example, a hacker will plant a virus as a distraction and then come in “slow and low” to hide in a system while the monitors are distracted. Hackers will also use coordinated, multipronged attacks, the official added.

Chinese hackers gained notoriety in the United States when a series of devastating intrusions, beginning in 2003, was traced to a team of researchers in Guangdong Province. The program, which DOD called Titan Rain, was first reported by Federal Computer Week in August 2005. Following that incident, DOD renamed the program and then classified the new name.

That particular set of hackers is still active, the Netwarcom official said. He would not confirm whether the Titan Rain group was linked to the NWC attack or any other recent high-profile intrusions.

Other senior military officials have spoken out recently on U.S. cyber strategy, saying the country urgently needs to develop new policies and procedures for fighting in the cyber domain.

Current U.S. cyber warfare strategy is dysfunctional, said Gen. James Cartwright, commander of the Strategic Command (Stratcom), in a speech at the Air Warfare Symposium in Orlando, Fla., last week. Offensive, defensive and reconnaissance efforts among U.S. cyber forces are incompatible and don’t communicate with one another, resulting in a disjointed effort, Cartwright said.

Gen. Ronald Keys, commander of Air Combat Command, told reporters at the conference that current policies prevent the United States from pursuing cyberthreats based in foreign countries. Technology has outpaced policy in cyberspace, he said.

The United States should take more aggressive measures against foreign hackers and Web sites that help others attack government systems, Keys said. It may take a cyber version of the 2001 terrorist attacks for the country to realize it must re-examine its approach to cyber warfare, he added.

Netwarcom officials described their approach as an active defense, in which monitors build defenses around the perimeter of DOD systems, work to mitigate the effects of attacks and restore damaged parts of the network.

Meanwhile, the consolidation of DOD's cyber resources is ongoing. Netwarcom works directly with the Joint Task Force for Global Network Operations, DOD's lead agency on network defense and operations, a component of Stratcom.

Netwarcom, the Navy's lead cyber agency, is moving from monitoring the networks to full command-and-control capabilities. The Air Force announced in October 2006 that it will create a Cyber Command, based on the infrastructure of the 8th Air Force under Lt. Gen. Robert Elder, at Barksdale Air Force Base, La., to coordinate its cyber warfare efforts.

In the end, the cyberthreat is revolutionary, officials said, because it has no battle lines, the intelligence is intangible, and attacks come without warning, leaving no time to prepare defenses. Education and training of computer users, not enforcement, are the most effective defense measures, officials said.