

Rallying For Democracy

<http://www.rallyingfordemocracy.org>

Chinese hackers: No site is safe

06/02/2010 07:50 by admin

By John Vause

ZHOUSHAN, China (CNN) -- They operate from a bare apartment on a Chinese island. They are intelligent 20-somethings who seem harmless. But they are hard-core hackers who claim to have gained access to the world's most sensitive sites, including the Pentagon.

In fact, they say they are sometimes paid secretly by the Chinese government -- a claim the Beijing government denies.

"No Web site is one hundred percent safe. There are Web sites with high-level security, but there is always a weakness," says Xiao Chen, the leader of this group.

"Xiao Chen" is his online name. Along with his two colleagues, he does not want to reveal his true identity. The three belong to what some Western experts say is a civilian cyber militia in China, launching attacks on government and private Web sites around the world.

If there is a profile of a cyber hacker, these three are straight from central casting -- young and thin, with skin pale from spending too many long nights in front of a computer.

One hacker says he is a former computer operator in the People's Liberation Army; another is a marketing graduate; and Xiao Chen says he is a self-taught programmer.

"First, you must know about the Web site you want to attack. You must know what program it is written with," says Xiao Chen. "There is a saying, 'Know about both yourself and the enemy, and you will be invincible.'"

CNN decided to withhold the address of these hackers' Web site, but Xiao Chen says it has been operating for more than three years, with 10,000 registered users. The site offers tools, articles, news and flash tutorials about hacking.

Private computer experts in the United States from iDefense Security Intelligence, which provides cybersecurity advice to governments and Fortune 500 companies, say the group's site "appears to be an important site in the broader Chinese hacking community."

Arranging a meeting with the hackers took weeks of on-again, off-again e-mail exchanges. When they finally agreed, CNN was told to meet them on the island of Zhoushan, just south of Shanghai and a major port for China's navy.

The apartment has cement floors and almost no furniture. What they do have are three of the latest computers. They are cautious when it comes to naming the Web sites they have hacked.

On camera, Xiao Chen denies knowing anyone who has targetted U.S. government Web sites. But off-camera, in conversations over three days, he claims two of his colleagues -- not the ones with him in the room -- hacked into the Pentagon and downloaded information, although he wouldn't specify what was gleaned. CNN has no way to confirm if his claim is true.

"They would not publicize this," he says of someone who hacks the U.S. Defense Department. "It is very sensitive."

This week, the Pentagon said computer networks in the United States, Germany, Britain and France were hit last year

Rallying For Democracy

<http://www.rallyingfordemocracy.org>

by what they call "multiple intrusions," many of them originating from China.

At a congressional hearing in Washington last week, administration officials testified that the government's cyber initiative has fallen far short of what is required. Most alarming, the officials said, there has never been a full damage assessment of federal agency networks.

"We are here today because we must do more," said Robert Jamison, a top official in the U.S. Department of Homeland Security. "Defending the federal system in its current configuration is a significant challenge."

U.S. officials have been cautious not to directly accuse the Chinese military or its government of hacking into its network.

But David Sedney, the deputy assistant secretary of defense for East Asia, says, "The way these intrusions are conducted are certainly consistent with what you would need if you were going to actually carry out cyber warfare."

Beijing hit back at that, denying such an allegation and calling on the United States to provide proof. "If they have any evidence, I hope they would provide it. Then, we can cooperate on this issue," Qin Gang, a spokesman for the Chinese Foreign Ministry, said during a regular press briefing this week.

But again off-camera, Xiao Chen says after the alleged Pentagon attack, his colleagues were paid by the Chinese government. CNN has no way to independently confirm if that is true.

His allegations brought strenuous denials from Beijing. "I am telling you honestly, the Chinese government does not do such a thing," Qin said.

But if Xiao Chen is telling the truth, it appears his colleagues launched a freelance attack -- not initiated by Beijing, but paid for after the fact. "These hacker groups in my opinion are not agents of the Chinese state," says James Mulvenon from the Center for Intelligence Research and Analysis, which works with the U.S. intelligence community.

"They are sort of useful idiots for the Beijing regime."

He adds, "These young hackers are tolerated by the regime provided that they do not conduct attacks inside of China."

One of the biggest problems experts say is trying to prove where a cyber attack originates from, and that they say allows hackers like Xiao Chen to operate in a virtual world of deniability.

And across China, there could be thousands just like him, all trying to prove themselves against some of the most secure Web sites in the world.