

Jackson Lowen for The New York Times

The austere bedroom of a Chinese hacker. Legions of hackers are pilfering information from individuals, corporations and government.

<http://www.nytimes.com/2010/02/02/business/global/02hacker.html?pagewanted=2&em?partner=yahoofinance>

Published: February 1, 2010

CHANGSHA, China — With a few quick keystrokes, a computer hacker who goes by the code name Majia calls up a screen displaying his latest victims.

“Here’s a list of the people who’ve been infected with my Trojan horse,” he says, working from a dingy apartment on the outskirts of this city in central China. “They don’t even know what’s happened.”

As he explains it, an online “trapdoor” he created just over a week ago has already lured 2,000 people from China and overseas — people who clicked on something they should not have, inadvertently spreading a virus that allows him to take control of their computers and steal bank account passwords.

Majia, a soft-spoken college graduate in his early 20s, is a cyberthief.

He operates secretly and illegally, as part of a community of hackers who exploit flaws in computer software to break into Web sites, steal valuable data and sell it for a profit.

Internet security experts say China has legions of hackers just like Majia, and that they are behind an escalating number of global attacks to steal credit card numbers, commit corporate espionage and even wage online warfare on other nations, which in some cases have been traced back to China.

Three weeks ago, Google blamed hackers that it connected to China for a series of sophisticated attacks that led to the theft of the company’s valuable source code. Google also said hackers had infiltrated the private Gmail accounts of human rights activists, suggesting the effort might have been more than just mischief.

In addition to independent criminals like Majia, computer security specialists say there are so-called patriotic hackers who focus their attacks on political targets. Then there are the intelligence-oriented hackers inside the People’s Liberation Army, as well as more shadowy groups that are believed to work with the state government.

Indeed, in China — as in parts of Eastern Europe and Russia — computer hacking has become something of a national sport, and a lucrative one. There are hacker conferences, hacker training academies and magazines with names like Hacker X Files and Hacker Defense, which offer tips on how to break into computers or build a Trojan horse, step by step.

For less than \$6, one can even purchase the “Hacker’s Penetration Manual.” (Books on hacking are also sold, to a lesser extent, in the United States and elsewhere.)

And with 380 million Web users in China and a sizzling online gaming market, analysts say it is no wonder Chinese youths are so skilled at hacking. Many Chinese hackers interviewed over the last few weeks describe a loosely defined community of computer devotees working independently, but also selling services to corporations and even the military. Because it is difficult to trace hackers, exactly who

is behind any specific attack and how and where they operate remains to a large extent a mystery, technology experts say.

And that is just the way Majia, the young Chinese hacker, wants it. On condition that he not be identified by his real name, Majia agreed two weeks ago to allow a reporter to visit his modest home in a poor town outside Changsha, and watch him work.

Slim and smartly dressed in black, Majia seemed eager to tell his story; like many hackers, he wants recognition for his hacking skills even as he prizes anonymity to avoid detection. The New York Times found him through another well-known hacker who belongs to a hacker group and vouched that Majia was skilled at what he did.

While Majia's claims, of course, cannot be verified, he is happy to demonstrate his hacking skills. He met a journalist at a cafe one night just over a week ago, and then invited him to his home, where he showed how he hacked into the Web site of a Chinese company. Once the Web site popped up on his screen, he created additional pages and typed the word "hacked" onto one of them.

Majia says he fell in love with hacking in college, after friends showed him how to break into computer systems during his freshman year.

After earning a degree in engineering, he took a job with a government agency, largely to please his parents. But every night after work, he turns to his passion: hacking.

He is consumed by the challenges it presents. He reads hacker magazines, swaps information with a small circle of hackers and writes malicious code. He uses Trojan horses to sneak into people's computers and infect them, so he can take control.

Skip to next paragraph Add to Portfolio  
Google Inc

Go to your Portfolio »

"Most hackers are lazy," he says, seated in front of a computer in his spare bedroom, which overlooks a dilapidated apartment complex. "Only a few of us can actually write code. That's the hard part."

Computer hacking is illegal in China. Last year, Beijing revised and stiffened a law that makes hacking a crime, with punishments of up to seven years in prison. Majia seems to disregard the law, largely because it is not strictly enforced. But he does take care to cover his tracks.

Partly, he admits, the lure is money. Many hackers make a lot of money, he says, and he seems to be plotting his own path. Exactly how much he has earned, he won't say. But he does admit to selling malicious code to others; and boasts of being able to tap into people's bank accounts by remotely operating their computers.

Financial incentives motivate many young Chinese hackers like Majia, experts say. Scott J. Henderson, author of "The Dark Visitor: Inside the World of Chinese Hackers," said he had spent years tracking Chinese hackers, sometimes with financial help from the United States government. One Chinese hacker who broke into a United States government site later lectured on hacking at a leading university, Mr. Henderson said, and worked for China's security ministry. But recently, many have been seeking to profit from stealing data from big corporations, he said, or teaching others how to hijack computers.

“They make a lot of money selling viruses and Trojan horses to infect other people’s computers,” Mr. Henderson said in a telephone interview. “They also break into online gaming accounts, and sell the virtual characters. It’s big money.”

Majia lives with his parents, and his bedroom has little more than a desktop computer, a high-speed Internet connection and a large closet. The walls are bare.

Most of his socializing occurs online, where he works from about 6:30 p.m. to 12:30 a.m., starting every evening by perusing computer Web sites like cnBeta.com.

Asked why he doesn’t work for a major Chinese technology company, he sneers at the suggestion, saying that it would restrain his freedom.

He even claims to know details of the Google attack. “That Trojan horse on Google was created by a foreign hacker,” he says, indicating that the virus was then altered in China. “A few weeks before Google was hijacked, there was a similar virus. If you opened a particular page on Google, you were infected.”

Oddly, Majia said his parents did not know that he was hacking at night. But at one point, he explained the intricacies of computer hacking and stealing data while his mother stood nearby, listening silently, while offering a guest oranges and candy.

Majia and his fellow hackers keep secret their knowledge of certain so-called zero-day vulnerabilities — software flaws — for future use, he says.

“Microsoft and Adobe have a lot of zero days,” he said, while scanning Web sites at home. “But we don’t publish them. We want to save them so that some day we can use them.”

When asked whether hackers work for the government, or the military, he says “yes.”

Does he? No comment, he says.