Russia's hackers pose growing global threat

December 30 2008, By Alex Rodriguez

Not long ago, the simple, anonymous thrill of exposing chinks in American software was enough of a payoff for a Russian hacker.

Today it's cash. And almost all the targets are in the United States and Europe, where Russia's notorious hackers pilfer online bank accounts, swipe Social Security numbers, steal credit card data and peek at e-mail log-ins and passwords as part of what some estimate to be a $100 billion-a-year global cyber-crime business.

And when it's not money that drives Russian hackers, it's politics - with the aim of accessing or disabling the computers, Web sites and security systems of governments opposed to Russian interests. That may have been the motive behind a recent attack on Pentagon computers.

A new generation of Russian hacker is behind America's latest criminal scourge. Young, intelligent and wealthy enough to zip down Moscow's boulevards in shiny BMWs, they make their money in cyber-cubbyholes that police have found impossible to ferret out.

From behind the partition of anonymous online hacking forums, they boast about why they use their programming savvy to spam and steal, mostly from the West.

"Why should I take a regular job after graduating and exert myself to earn just $2,000 a month, rather than grab this chance to make money?" says a Russian hacker on a cyber-crime forum that specializes in credit card fraud. "It makes sense to get as much as you can, as quickly as

possible, rather than wasting time working for someone else."

Cybercrime, by some estimates, has outpaced the amount of illicit cash raked in by global drug trafficking. Hackers from Russia and China are among the chief culprits, and the threat they pose now extends far beyond spam, identity theft and bank heists.

Besides the recent attack on computers at the U.S. Defense Department, which may have originated in Russia, according to military leaders in Washington, Russian hackers also are believed to be behind highly coordinated attacks that brought down government Web sites in Estonia in 2007 and in U.S.-allied Georgia when war broke out between Russian and Georgian forces in August.

They're even suspected of hacking into the computer systems of Barack Obama and John McCain during the presidential campaign; technical experts hired by Obama's campaign suspected the attacks may have come from Russia or China, according to Newsweek.

So far there has been no evidence of a link between the Russian government and any of the attacks on American, Georgian and Estonian Web sites and computers. Russian authorities denied any involvement in the Georgian and Estonian attacks, and they recently said that speculation about a Russian link to the attack on U.S. Defense Department computers was "groundless" and "irresponsible."

Nevertheless, the need to ramp up security of American cyberspace is being discussed with greater urgency in Washington. Earlier this month, a commission on cyber-security delivered a report to Congress calling for the creation of a new White House office that would gird the United States against computer attacks from hackers and foreign governments.

According to the commission, "unknown foreign entities" in 2007

hacked computers at the Departments of Defense, Homeland Security and Commerce, as well as NASA. Hackers broke into Defense Secretary Robert Gates' unclassified e-mail and probe Defense Department computers "hundreds of thousands of times each day," said the commission, a panel of leading government and computer industry experts.

A senior State Department official told the commission that the department had lost thousands of gigabytes of data due to computer attacks, and among the Homeland Security divisions reporting computer break-ins was the Transportation Security Administration, which provides airport security. Hacking attacks compromising intellectual property have cost U.S. companies billions of dollars, the report stated.

"The damage from cyber attack is real," the report continued. "Ineffective cybersecurity, and attacks on our informational infrastructure in an increasingly competitive international environment, undercut U.S. strength and put the nation at risk."

After the Soviet collapse in 1991, Russian hackers were primarily motivated by mischief. They crafted viruses and worms simply for the delight of revealing weaknesses in security systems and software.

"Back then, it was simple hooliganism," said Vladimir Dubrovin, a hacker in the late 1990s and now a Russian computer security expert.

Today, however, most hackers in Russia are in it strictly for the money. Cyber-crime gangs approach computer programming graduates from Moscow's technical universities with offers of making sums of $5,000 to $7,000 a month, a far cry from Russia's average monthly salary of $640, says Nikita Kislitsyn, editor of Hacker, a glossy Russian magazine with how-to information for budding hackers.

Yevgeny Kaspersky, chief executive of Moscow-based Kaspersky Lab, one of the world's leading computer security firms, says Russian hacking flourishes as "a cyber-criminal ecosystem" of spammers, identity thieves and "botnets," vast networks of infected computers controlled remotely and used to spread spam, denial-of-service attacks or other malicious programs. A denial-of-service attack floods a Web site with inquiries, forcing its shutdown.

To ply online bank accounts, Russian hackers rely on viruses that record keystrokes as customers type log-ins and passwords. Russian-made viruses are believed to be behind several major online heists, including the theft of $1 million from Nordea Bank in Sweden in 2007 and $6 million from banks in the United States and Europe that same year.

The huge amount of money cyber-crime generates has created a vast underworld market that so far has proved to be virtually impregnable by Russian police. Viruses and other types of so-called "malware" are bought and sold for as much as $15,000, Kislitsyn says. Rogue Internet service providers charge cyber-criminals $1,000 a month for police-proof server access.

Botnets relied on for cyber-crime can also be used to lash out at political enemies, computer security experts say. Most analysts agree that criminal botnets were used by Russian hackers to shut down Estonian government and banking Web sites after the tiny Baltic republic angered Russians by moving a Soviet war memorial from downtown Tallinn in 2007.

In countries such as Russia and China, where criminal botnets are highly developed, such a resource could evolve into a potent cyber-warfare weapon, experts say.

"The Internet can now be used to attack small countries," Kaspersky

said. "There are Russian and Chinese hackers that have the power to do that."

Russian police departments have cyber-crime divisions, but arrests of major cyber-criminals are rare.

"It comes down to a question of volume," said Steve Santorelli, investigations director at Team Cymru, a Burr Ridge, Ill.-based Internet security research firm. "In Russia, there simply aren't the resources."

___