The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Ex-Soviet Hackers Dominate Cyber Crime World

August 25, 2013

An employee of the cyber security firm Kaspersky Lab working at a computer in the company’s Moscow office. **Sergei Karpukhin**

If you want to hack a phone, order a cyber attack on a competitor's website or buy a Trojan program to steal banking information, look no further than the former Soviet Union.

The breadth and sophistication of services sold on Russian-language websites such as Forum.zloy.bz or Forum.evil offer a small window onto a Russian criminal underground that is costing Western firms billions of dollars in credit card and online banking fraud as well as "phishing" attempts to lure people into downloading malware or disclosing passwords.

"If you look at the quantity of malware attacks, the leaders are China, Latin America and then Eastern Europe, but in terms of quality then Russia is probably the leader," said Vitaly Kamluk, a cyber security researcher in Moscow.

Two of the five most wanted men in the U.S. for cybercrime are Russian, and one is from Latvia, which used to be part of the Soviet Union.

Russians were also behind the biggest cybercrime case in U.S. history. Federal prosecutors named four Russians and a Ukrainian in a banking-card fraud spree that cost companies including J.C. Penney, JetBlue Airways and French retailer Carrefour more than $300 million.

The risk of being prosecuted is so low that it does little to dissuade highly educated and skillful but underemployed programmers from turning to illicit hacking for profit or fun.

In a country where wages are lower than in the West and life is expensive, and one that has long produced some of the world's best mathematicians, the temptation to turn to crime is great. And the hackers are generally ahead of the people trying to catch them.

"People think: 'I've got no money, a strong education and law enforcement's weak. Why not earn a bit on the side?'" said Alexei Borodin, a 21-year-old hacker.

As long as these hackers target victims abroad, experts say, the Russian authorities are willing to sit back and let them develop tools to burrow into computer vulnerabilities, which they can in turn use for their own cyberespionage.

Two of the Russian suspects in the banking-card fraud case were arrested while in the Netherlands, but two others — Alexander Kalinin, 26, and Roman Kotov, 32 — are still at large and thought to be in Russia, where experts doubt they will be caught.

Moscow's decision to harbor Edward Snowden, wanted in the U.S. for leaking details of government surveillance programs on the phone and Internet, is likely to freeze already slow-moving cross-border police cooperation with Washington, they said.

"They have been doing this in Russia for many years now," said Misha Glenny, an expert and author on cyber crime.

"Russian law enforcement and the FSB [Federal Security Service] in particular have a very good idea of what is going on and they are monitoring it, but as long as the fraud is restricted to other parts of the world they don't care."

Several e-mail requests for comment and calls over three weeks to the special Interior Ministry unit tasked with policing the web — Department K — went unanswered.

No Boundaries

The pool of talent churned out by top-tier institutes excelling in hard sciences across the former Soviet Union is indisputable.

A trio of students from the St. Petersburg National Research University, for instance, won the oldest and most prestigious world programming competition, the ACM International Collegiate Programming Contest, four times in the last six years.

Three Russian teams, one from Belarus and one from Ukraine were also among the top ten finalists this year in the contest, which featured teams from 2,322 universities in 91 countries.

But in a 2013 survey, only 51 percent of IT specialists in Russia polled by HeadHunter, a recruiting website, found jobs in the country's burgeoning IT sector. It said average salaries in Moscow for work in information security was 65,000 rubles ($2,000) a month, far less than Western counterparts would earn.

Hacking is not a crime in and of itself. So-called white-hat hackers, who access computers to bolster security defenses, face off on the front lines of a virtual battleground with criminals, known as crackers or black-hat hackers, who break in with ill intent.

Hackers on both sides of that divide are mostly aged 22 to 30 and, in Russia, many may have been university classmates.

Borodin, who works on startups involved in Bitcoin, the virtual currency, describes web security as his hobby. Known as ZonD80, he began exploring computer vulnerabilities at the age of 12, and made waves last year by publishing a hack allowing iPhone users to avoid paying for in-app upgrades — a system loophole it took him about a week to find.

He says he has never broken the law.

"I hacked Apple and Google systems, but I've been working on the other side for ages. ... Now it's fun to design defenses against all the hacks I used to do myself," he said in an interview via instant messenger.

"There aren't really any boundaries. Someone can go over to the bad side or suddenly become a protector. In any event, if you're caught, then you were in the wrong place at the wrong time."

Weapons Race

At the Moscow headquarters of Kaspersky Lab, a Russian rival to U.S. security firms Symantec and McAfee, sweatshirt-clad youths sit silently tapping away in an ultra-sleek workspace.

"Stealing money from behind a screen is incomparably easier psychologically than attacking someone in the street," Kamluk, 29, said in a round, glass room known as the Virus Lab. Here client data on millions of suspicious programs is parsed by analysts sitting at a circle of screens that looks like a spaceship control room.

"Using technical means, you can fight cyber crime endlessly, but it is a non-stop weapons race: We make security systems and they find ways around it."

The soft-spoken Belarussian, who sports a Mohawk and a t-shirt printed with green-on-black computer code, was hired in 2005 and is now part of an elite team chosen by CEO Eugene Kaspersky to investigate new or exotic cyber threats.

The Global Research and Expert Analysis Team, or GREAT for short, discovered the Stuxnet cyber weapon, which is believed to have been used by the U.S. and Israel to attack Iran's nuclear program a few years ago.

This year Kamluk and other GREAT prodigies uncovered a Russian-speaking cyberespionage gang, Red October, operating a complex data-hijacking system used to steal intelligence from government, military and diplomatic targets worldwide.

GREAT was not able to identify who was behind the gang. But the manpower and expense needed to wield such a network is believed by some experts to point to the involvement of a state intelligence agency, possibly Russian.

Advice Forums

On the Blackhacker.ru forum, threads offer advice on which countries have the most crime-friendly laws and sell cyber tools such as bullet-proof hosting from which to launch attacks.

In a feeble nod to the law, some sellers post disclaimers, denying responsibility if their service is put to criminal use.

Such forums played a crucial role in the criminal baptism of a generation of programmers who emerged on the job market in the 1990s when the Soviet Union was unravelling and have served as hacker incubators popularizing cyber crime in Russia.

"In 2008, you needed to buy a Botnet [network of infected computers] and set it up; it was quite sophisticated. Nowadays, every schoolboy can do this by ... using forums and reading," said Maxim Goncharov, a researcher at security firm Trend Micro.

The amount of cash flowing to this underground industry is hard to quantify, as many companies do not report losses. Moscow-based cyber forensics firm Group-IB estimated that the Russian cyber crime market was worth $2.3 billion in 2011 and far more today.

Some of the cash, it says, goes to pay off corrupt police, who then tip off the criminals.

Andrei Komarov, head of international projects at Group-IB, said cyber criminals are winning in the war against the world's law enforcement agencies.

"It is like the battle between a fly and an elephant," Komarov said. "Some cyber criminals have very close contacts with corrupted law enforcement agencies, and during our investigations some disappeared and were not arrested."

Original url:
https://www.themoscowtimes.com/2013/08/25/ex-soviet-hackers-dominate-cyber-crime-world-a27060