The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

How Russia Became a Hacking Superpower

Moscow has finally got the geopolitical respect it demanded for years, but only after spooking Washington.

By Matthew Bodner

December 30, 2016

Katerina Lobanova

Since the beginning of his first presidency, Vladimir Putin has made it a national priority to convince the West, and particularly the United States, to take Moscow seriously. This goal is largely to blame for the last decade of Russian foreign policy, which has grown more assertive, and militarized. For the longest time, Russia seemed incapable of breaking through Americans' sense of invulnerability.

When Moscow annexed Crimea from Ukraine in 2014, the Kremlin's boldest aggressive trends were on full display, but Russia remained a distant concern for most people in the U.S. Even Washington refused to view Russian intransigence as a direct threat to American national

security. Yes, the Kremlin was creating problems for allies in Europe, went conventional thinking, but the United States was safe.

It was only this year that Vladimir Putin finally captured the American mind, and he owes the feat not to flashy images of Russian missiles and tanks parading through Red Square, but to the quiet actions of people armed with computers.

Not So Newfangled

Lost in the debate about Russian influence in the U.S. presidential election is the fact Russian hackers have been active for a long time. Littering the illicit pages of the dark web, Russian hacking programs today make possible most of the world's financial-sector break-ins. Increasingly, Russian hackers have acted with political motivations, but their bread and butter is and has always been theft and corporate espionage.

As programmers, Russian-speaking hackers are pioneers in their fields.

Despite some diplomatic turbulence over the last two decades, police in Russia and the U.S. have, at times, cooperated to track and arrest major cyber criminals. Even in the middle of the hacking scandal, Russian officials recently handed over notorious criminal Joshua Samuel Aaron — a man wanted by U.S. state prosecutors for "security fraud on cyber steroids."

Aaron is one of several high-profile Russian-speaking hackers arrested in recent years, and he was far from the first to get caught. These criminals belong to a community that emerged in the 1990s, when the collapse of the USSR abandoned many trained and capable technicians to lives without reliable or sustainable work.

"A lot of these people had access to computers, and they knew how to explore the possibilities," says Alexei Kruchenok, a software developer in Belarus. "If you didn't have economic opportunities, you looked at the gray Internet market for money."

Skills and Opportunity

Russian hacking came of age as the Internet economy developed in the 1990s. It was a time when capabilities outpaced security. Shopping and banking were early online growth areas, and hackers saw Western banks and consumers using credit cards as easy targets.

For Russians with the necessary skills, preying on these services was an attractive way to make money in stormy times. While rocket scientists and weapons experts found government and international support, programmers were largely overlooked.

"The U.S.S.R. had the largest engineering community in the world," says Andrey Soldatov, author of The Red Web and an expert on cyber security and the Russian security services. "They existed to support the Soviet military-industrial complex, and after its collapse, many of these experts and their children, found themselves left high and dry."

And so, in the 1990s and early 2000s, the Russian-speaking hacker community flourished.

"In the early 2000s, lots of people who had access to computers knew how to hack — and they did it, even just to get access to the Internet," Kruchenok says. "A lot of people worked on the

so-called ‘gray Internet’ in the businesses of spam, malware, and porn. Groups would hire talented people to write the code for these industries.”

Vladimir Levin, a mathematician trained as a biochemist, was the archetypal early Russian hacker. In 1994, he led a hack on Citibank, gaining access to its systems, and transferring $10 million to his own accounts. Levin was later arrested, but he would not be the last Russian amateur to hack the systems of a major Western bank.

The Community

Beyond raw technical skill, the secret behind the success of the Russian-speaking hacker community is informationsharing, says Dmitry Volkov, an expert in cyber forensics at the Moscow-based Group IB cyber security firm. Compared to other large hacker communities, such as the German and Spanish-speaking ones, the Russian community has been the most open.

Fifteen years ago, an aspiring hacker needed simply to join a forum and ask questions.

“You could ask anything,” Volkov says. “For example: which type of program should I use to steal money from a bank? And if I am targeting a specific Western bank, what kind of additional security measures does that bank have in place, and how do I get around them?”

For such specific questions, seasoned hackers would often provide very detailed answers — sometimes, they would even share step-by-step instructions.

And the activity was not limited to banks. Knowhow for other hacking techniques, like DDoS, spam, and related activities, was and still is readily available on the Russian Internet. The answers to any query were open and available to everyone in a forum, making Russian hackers’ approach to exchanging knowledge particularly effective.

Over time, these online communities became digital bazaars for all kinds of malicious software developed by hackers for personal use, and traded or sold to other hackers, as part of a fast-growing black market software industry.

“On other forums, in other languages, I never saw anything like it,” Volkov says.

Russia’s hacker community soon emerged as a powerhouse in the global malware market, producing highly specialized toolkits for hacking techniques. Talented Russian-speaking developers would band together to hack a particular target, or they might simply create cutting-edge tools for other hackers to buy and use.

Remarkably, these hacker groups resemble both organized crime syndicates and legitimate businesses.

“The best cyber criminal gangs will have one very strong leader,” Volkov says. “He won’t necessarily be a superstar hacker. Instead, he’ll have good contacts with money-laundering teams. Usually they’ll split the profits sixty-forty from hacking a bank or corporate account, and they can cause a lot of damage.”

Volkov recalls one incident two years ago, when a Russian hacker group infiltrated a trading

terminal at the Moscow Exchange and — for 14 minutes — was able to conduct transactions. They moved about $400 million worth of shares, Volkov says, influencing the ruble-to-dollar exchange rate by about 10 rubles. The bank they hacked lost 200 million rubles (almost $4 million at the time).

Given the skill of groups capable of infiltrating banks, identifying an attacker is no easy task. Volkov describes his work as "forensic investigation" focused on mapping out the vectors of attack, and the tools used. Over time, this can help identify the source.

Every now and then, people like Volkov make a major breakthrough, when the trail leads to the malware's original developer.

In 2012, Russian authorities caught the individual behind a Trojan horse virus known as "Black Hole." Used by up to 70 percent of hackers targetting banks, this exploit kit was infamous. "Most hackers across the globe were buying software from the guy who developed Black Hole," Volkov says.

Going Legit

Russian hackers still lead the pack today, but the community is thought to be smaller now than it was at its peak 15 years ago. The open online forums of old have largely fallen silent, experts say, and those who remain in the game are more professional and discreet than the amateurs who once dominated the landscape.

There are several reasons for the change. For starters, talented programmers from the former Soviet Union - who once hacked for financial, rather than ideological reasons - now have more opportunity in the legitimate information-technology market. The skills of firms like Group IB and law enforcement have increased, as well, leading to more arrests.

This is especially true in neighboring Belarus, says Kruchenok. Once a hacking haven, Belarus has used a carrot-andstick method to push its programmers into legitimate activities. A decade ago, the government opened a technology park to stimulate software developers, and many saw an opportunity for stable and legitimate salaries.

Not everyone in the black market turned to private enterprise for legitimacy, however, and some hacker groups succeeded in forging relationships with the state.

One of the most famous Russian hacker collectives, known as the "Russian Business Network," first cozied up to the government in the mid-2000s. Around this time, the group is believed to have earned roughly $150 million annually, and at one point it may have been responsible for 60 percent of all major cybercrime.

Investigators have determined that the hackers who launched several large-scale cyber attacks on Estonia and Georgia in 2007 and 2008 were using toolkits designed and sold by the Russian Business Network. State officials and researchers in these countries say the attacks were politically motivated and conducted "in service" to the Russian government.

The apparent interaction between Russian criminal hackers and the Russian government presents a challenge to cyber security in the West. While the two sides have demonstrated an

ability to work together to catch dangerous criminals who threaten the world's financial infrastructure, the existence of criminal groups for hire makes it much harder to attribute a particular attack to the state. Such complications fuel mistrust.

Data trails still exist, and the intrigue and paranoia they're capable of generating have confounded and terrified the American political establishment. The Kremlin has Russia's rich hacker tradition to thank for that.

Original url: https://www.themoscowtimes.com/2016/12/30/russia-hacker-superpower-a56704