The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Inside A Hacker's Mind

He was a leading player in Russian-language cyber-crime. Today, he suggests electoral systems are ripe for abuse.

By Howard Amos

February 20, 2017

Olya Khaletskaya

Belarusian-born cyber-criminal Sergei Pavlovich was earning $100,000 a month by the age of 20.

A leading figure in the cyber-underworld of the early 2000s, Pavlovich surrounded himself with the best Russianlanguage hacking talent. He bought credit card details from them before using so-called cash mules to convert the stolen data into money.

"You don't think of it as criminality: it's a game," Pavlovich, whose online nickname was Policedog, said in an interview in Moscow.

Pavlovich, 33, went on to serve 10 years in prison in Belarus for cyber-crime offenses. He

retains a detailed knowledge of how criminals operate in the Russian-speaking online world, and knows many of the most successful hackers in the business.

His story is a rare glimpse into the Russian-language cybercriminal community, which many experts suggest has been used by the country's security services to enhance its aggressive cyber-operations. According to U.S. intelligence agencies, Russia used hacking as part of a cyber-campaign to support Donald Trump during the U.S. presidential elections last year.

Pavlovich was what is known as a "carder," a profession that sprang up to coordinate the complex task of turning stolen credit card information into cash.

"Carders should be good at organizing. You need to know people," Pavlovich said. "Hackers very rarely resell, its more advantageous for them to have a few regular clients."

Pavlovich is fast-talking and articulate. While behind bars, he wrote a book called "How to Steal a Million," describing his prison life and the cyber-crime scene. Since being freed in 2015, he has set up several businesses, including a fish delivery service, an online cashback scheme and a company that sells souvenir mock-ups of U.S. dollar bills.

He admits his own hacking skills would only have allowed him to break into relatively minor, or poorly-defended, organizations. Instead, he used his communication and management skills and leveraged connections in the cyber underworld.

This is not unusual. The most important people in the cyber-criminal community today are often those with no programming skills, according to Alexander Gostev, chief security expert at the cyber security firm Kaspersky Lab. "To create and manage a group demands a brain and ability," he said.

Pavlovich, who lived in the Belarussian capital of Minsk, first got involved in cyber-crime aged 13. His family had a computer at home, but his step-father "was a businessman who drank away all the money."

Related article: How Russia Became a Hacking Superpower

He began by buying credit card details online—for about $1 per card—and using them to make purchases from internet stores, a practice known as stuff-carding.

Pavlovich focused on stealing computer parts, TVs and other electronics that were scarce in former Soviet countries. The hardest part was reselling the goods: "companies in Minsk found out about their origin and would only pay 30— 40 percent of the market price," he recalled in "How to Steal a Million."

Just like hackers and cyber-criminals today, Pavlovich expanded his knowledge of his chosen profession through online forums, particularly one known as carderplanet.com, set-up in Ukraine in 2001. In his book "Spam Nation," U.S. cyber-security journalist Brian Krebs describes carderplanet. com as "the most brazen collection of carders, hackers and cyber-thieves the Internet had ever seen."

While studying for a journalism degree at Belarus State University, Pavlovich discovered so-

called “dumps,” a slang term for a full package of credit card details, including PIN codes, that can be used to create counterfeit cards. With connections to talented hackers, Pavlovich bought and sold dumps and used money mules scattered across the globe to cash out.

“No-one told us that stealing was a sin, and even if they did, no-one bothered to explain why it was,” Pavlovich writes in his book.

Almost all the stolen credit card details they used belonged to people in the United States, according to Pavlovich. Not only did this reduce the likelihood of police attention in Belarus, but it also made crimes appear victimless—particularly as insurance covered customer losses.

“There are enough well-off westerners to go by. Call it being patriotic, if you will. I don’t remember when we adopted the rule, but it was a rule everyone respected: never steal from your people,” said Pavlovich.

At the peak of his earning power in 2003, he only needed to work three hours a day to bring in $100,000 a month. Pavlovich spent his money on exotic holidays, restaurants, women and expensive purchases like cars.

“Almost all our income was scattered in the wind,” he said.

His luck ran out. He was arrested and convicted in 2004 and served almost three years in jail. In 2008, he was arrested and convicted again. This time, he was jailed for seven years. His second conviction was hailed at the time by the FBI as part of one the largest hacking and identity theft cases ever prosecuted by the U.S. Department of Justice. They said Pavlovich’s group had stolen over 40 million credit and debit card numbers.

Throughout his career, Pavlovich said he worked with Russian hackers because they were able to break into almost anything.

“Russian hackers and Russian programmers are the best in the world because they don’t work by instructions or according to the rules: they have an unusual approach and they find a way to hack things very quickly,” he said.

Online marketplaces, banks or payment centers that contain financial details are the most heavily protected sites on the Internet, Pavlovich added.

“It’s much easier to hack an electoral system than e-Bay or Citibank,” he said.

Related article: An American Cover Story for Russia's Undercover Hackers

Original url: https://www.themoscowtimes.com/2017/02/20/inside-a-hackers-mind-a57200