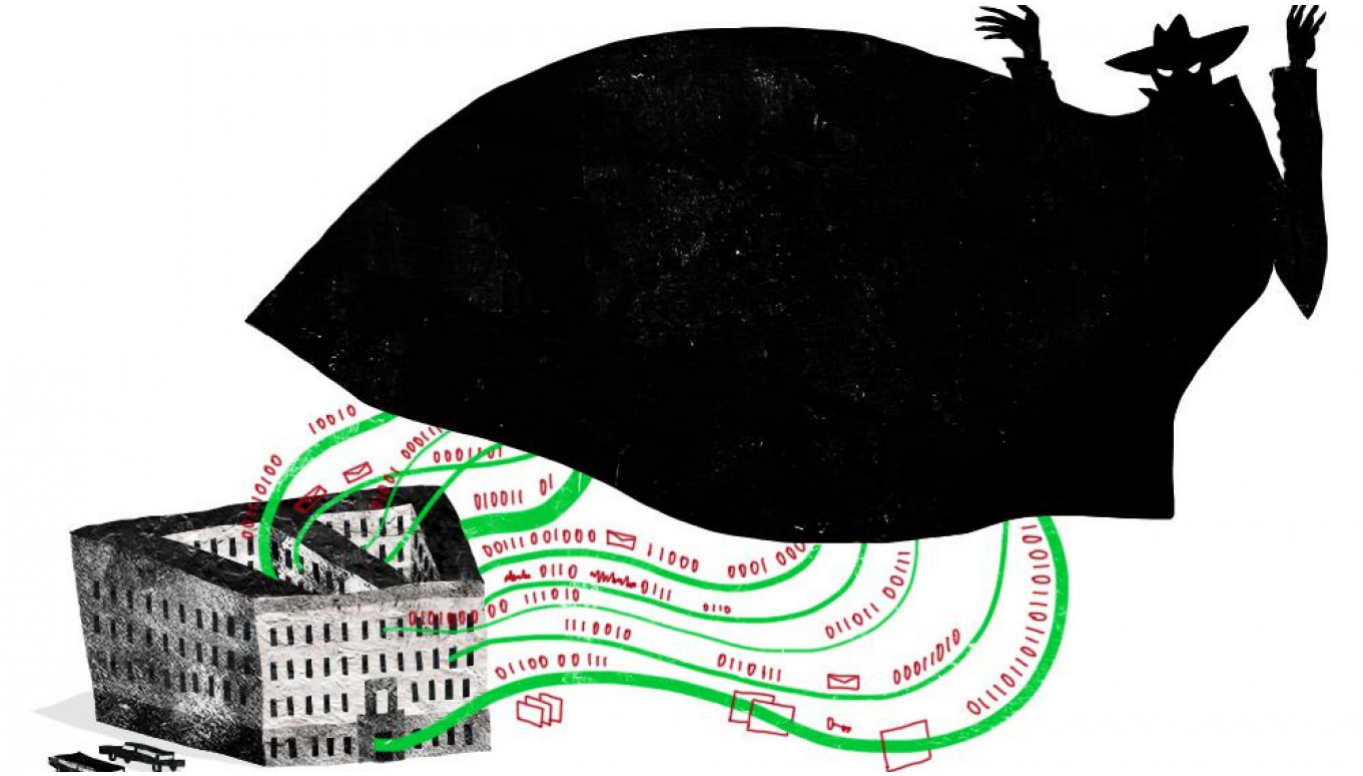
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

The Specter of Kaspersky Looms Over Russian Cybersecurity Firms

How the controversy embroiling Kaspersky Lab could spoil its competitors' chances abroad

By Evan Gershkovich

January 11, 2018



Ilya Kutoboy

Garry Kondakov speaks quickly, especially when he is upbeat. So when he says that business is good and that there seems to be no end in sight to his company's growth, his words spill out at an ever faster clip.

Kondakov is responsible for expanding Group-IB, a Russian cybersecurity firm, into foreign markets. The firm has offices in Dubai, London and New York — and, according to Kondakov, it does business with some of the world's largest companies.

"I can't give you the names," he says, citing confidentiality clauses in the deals, "but we have

contracts with several Fortune 500 companies." He can share one, though — his firm signed an information-sharing agreement with Interpol last month.

Group-IB is selling its ability to hunt down Russian hackers, a service that is increasingly coveted. In the past 18 months alone, a single Russian-speaking hacking cell reportedly stole up to $10 million from U.S. and Russian banks.

Related article: Kaspersky Lab Sues U.S. Over Federal Agency Ban on Software

Russian hackers have also struck fear in Western governments and voters. U.S. authorities have accused them of breaking into the servers of the Democratic National Committee and the emails of Hillary Clinton's campaign staff.

U.S. intelligence agencies concluded that the hacks were aimed at tipping the 2016 presidential election in favor of President Donald Trump. What's worse, their perpetrators allegedly acted on the orders of Russian intelligence.

In the United States, the breaches have come under intense scrutiny, and as the story has unraveled, the lines between hacker and cybercrime investigator have become increasingly blurred.

Kaspersky Lab, Russia's most successful cybersecurity firm and the only one to have established a firm presence abroad, has been accused of cooperating with Russia's Federal Security Service (FSB) — one of the intelligence agencies accused of directing the hacks.

Link:
https://themoscowtimes.com/news/embattled-russian-cyber-firm-kaspersky-teams-up-with-interpol-59261?src=ilaw

In response, the U.S. government has begun purging itself of Kaspersky software, and retailers have also pulled it off their shelves. Other Western governments may follow suit.

Group-IB's push into international markets, then, comes just as the West is growing more wary of Russian cyber-espionage capabilities. In a world where the cyberdefender is also a potential hacker or Russian spy, the thinking goes, the Kremlin is always watching.

Ties that bind

Kaspersky is primarily known for its antivirus software. According to Forbes, the company boasts 400 million users of its software products in more than 30 countries around the world. It is particularly popular in the West, which accounted for more than half of the firm's $633 million in sales in 2016, Bloomberg has reported.

As a large cybersecurity firm, Kaspersky is a natural ally of Russian intelligence agencies in catching cybercrooks. It is a role that Eugene Kaspersky, the co-founder of the company that carries his name, has welcomed. As the billionaire has put it, his goal is not to earn money, but "to save the world."

That the company has a relationship with intelligence agencies is not unusual, says Mark Galeotti, the coordinator of the Center for European Security at the Institute of International Relations Prague.

" *“The main thing here is that Kaspersky staff acted not as experts, but as participants in an FSB operation.”*"

“Any major cybersecurity company will have a relationship with the intelligence agency in its country,” he says. “If Kaspersky was based in Manchester, it would have a connection with British intelligence.”

The difference with Kaspersky and Russian intelligence, Galeotti says, is in the “nature” of the relationship.

Emails obtained this summer by Bloomberg from 2009 revealed that a project led by Igor Chekunov, Kaspersky Lab’s chief legal officer and a former member of the KGB, had developed security technology for the FSB.

The relationship was also on display in court documents published this year on the Facebook page of a Russian hacker, Konstantin Kozlovsky. One document, from April 2015, revealed a joint-operation between Kaspersky Lab and the FSB to ferret out cyber criminals that, damningly, was run on Kaspersky premises.

“The main thing here is that Kaspersky staff acted not as experts, but as participants in an FSB operation,” says Andrei Soldatov, a Russian journalist and co-author of “The Red Web.”

A cold wind

Until recently, Kaspersky’s close connection with the FSB was not a major worry in the United States.

As Soldatov explains, prior to allegations that it interfered in the 2016 U.S. presidential elections, the FSB was well regarded in the West. In the war against terror, the agency was viewed as an ally, especially after it tried to warn the United States about the Boston bombers.

That changed after Russia’s annexation of Crimea from Ukraine in 2014 and relations with the West spiraled.

“What we have seen, especially since 2014, is a vastly more confrontational global situation as Russia takes on the West, and with that, the increasing importance of cyber-espionage,” Galeotti says.

Eugene Kaspersky, too, has addressed that shift. “We felt a cold wind started to blow in 2014,” he said in October of his business in Western Europe and the United States.

As Russia was gearing up to launch its cyberwar ahead of 2016, U.S. authorities now worry that Kaspersky — whether by choice or not — helped the Kremlin prepare.

In September, The Wall Street Journal reported that, in 2015, Russian hackers obtained National Security Agency (NSA) hacking tools. According to The New York Times, Israeli hackers had breached Kaspersky Lab and, finding the NSA code, alerted the agency.

Although it is not publicly known how Russian hackers obtained the NSA information, investigators believe they exploited the Kaspersky antivirus software installed on an NSA employee's home computer.

This month, Trump signed a bill into law banning Kaspersky products from U.S. government machines. The move followed a U.S. Department of Homeland Security's (DHS) warning that the Russian government could — acting independently or in concert with the cybersecurity firm — "capitalize on access provided by Kaspersky products."

Kaspersky denies that the firm has helped the FSB in cyber-espionage. In a statement to Bloomberg this summer, the company said it "does regularly work with governments and law enforcement agencies around the world with the sole purpose of fighting cybercrime."

Structural impediments

Whether or not Kaspersky believes his company has helped the FSB spy, however, might be besides the point.

There are legal structures in Russia that render the work of cybersecurity companies transparent to the FSB, says Soldatov. As he puts it, for cybersecurity firms based in the country, the agency is "impossible to escape." That's because encryption developers are required to procure a license from the FSB that "allows the agency access to everything they do."

There are also laws that allow the Russian government to surveil the country's internet service providers through a system called the System of Operative-Investigative Measures, or SORM. In October, an American industry official who was briefed by the FBI on Kaspersky Lab pointed to that system as a key concern.

Related article: Head of Kaspersky Lab to Testify Before U.S. Congress

"Whether Kaspersky is working directly for the Russian government or not doesn't matter; their internet service providers are subject to monitoring," he told the Washington Post. "So virtually anything shared with Kaspersky could become the property of the Russian government."

And a lot is shared with Kaspersky. Because, by definition, antivirus software is invasive. When users download it to their computers, they give the software free reign to rifle through their data for malware. What is recognized as malware is then sent back to Kaspersky headquarters in Moscow, where it is analyzed for threats.

There are also informal structures in Russia the firms must navigate, says Soldatov. These are

the so-called *siloviki* — officials from the country's military and security agencies, like the FSB, who have their own interests to satisfy.

The agency could have easily planted its own people in the company, says Michael Kofman, a researcher at the Washington-based Wilson Center focusing on security in Russia. "The most effective resource is an organization that doesn't know it's being used," he says.

In effect, Galeotti says, there is simply not much a cybersecurity firm in Russia can do to maintain its autonomy. "If you're operating in Russia," he says, "you have to accept all the rules of the game."

Geographic concerns

As a result, Russian antivirus software is under scrutiny.

Last month, the BBC reported that the United Kingdom's National Cyber Security Centre (NCSC), a government agency, warned all British government departments against using Kaspersky software.

In an emailed statement to The Moscow Times, the NCSC clarified that its warning applies to any antivirus software sold by a company operating in Russia.

"We advised that where it is assessed that access to the information by the Russian state would be a risk to national security, a Russia-based antivirus company should not be chosen," a spokesperson wrote.

" *"U.S. Congress singled out Kaspersky Lab based solely on the location of its headquarters."*"

One of Britain's biggest banks, Barclays, announced in response it would no longer offer its customers free Kaspersky software as a "precautionary decision."

Eugene Kaspersky has decried the "geographic-specific approach to cybersecurity," and in an email to The Moscow Times, again said politics, not evidence, was the primary culprit of his predicament.

"U.S. Congress singled out Kaspersky Lab based solely on the location of its headquarters, although by all accounts we are an international company," he wrote.

Getting out

At a presentation titled "Cybercrime and Cyberpunishment" held fittingly at Moscow's Fyodor Dostoevsky Library in Moscow last November, one of Group-IB's leading specialists, Vesta Matveyeva, said the prevalence of Russian hackers means the company's services are in high demand abroad.

"As Russian experts, we understand the language they are using and so we can find them more easily," she said.

Another Group-IB specialist, Pavel Krilov, pointed to antivirus software as a key difference between his company's recent success and Kaspersky's difficulties in an interview with The Moscow Times. "We can't collect any data," he said.

Eugene Kaspersky has previously said he expects to lose as much as 8 percent in revenue from North America this year. Nonetheless, he has also tried to play off the purges of his products as a minor bump in the road, saying that he still expects his revenue to grow overall, noting growth in Asian and Latin American markets.

Related article: U.S. Bans Kaspersky Lab Products Over Security Concerns

At the very least, the Kremlin's foreign policy goals seem to have changed the atmosphere for Russian cybersecurity firms. For some, like Group-IB, it might mean more business because of the increasing prevalence of Russian hackers. For others, it could result in a shrinking market.

One Russian cybersecurity insider working for a large company in the field in Moscow claims that Russian cybersecurity companies across the board hoping to expand into Western markets started facing difficulties after sanctions were imposed on Russia.

"Security regulators started scaring off both investors and clients," he said on the condition of anonymity because he was discussing sensitive information. "It became more difficult for those companies."

Young cybersecurity entrepreneurs have taken notice of the changing atmosphere, says Galeotti, the coordinator of the Center for European Security, and have started considering distancing themselves from the Russian government.

Those who have a smart idea and want to do something with it are "looking elsewhere," he said.

After a beat, he put it more bluntly: "They are looking to get the hell out."

Original url:
https://www.themoscowtimes.com/2018/01/11/are-russian-cybersecurity-companies-still-welcome-in-the-west-a60164