Sanctioned Russian IT firm was partner with Microsoft, IBM

https://apnews.com/article/business-europe-hacking-russia-dd8c331ff30d366ea4f5d828e788c307

By FRANK BAJAK and MATT O'BRIEN | April 15, 2021

President Joe Biden leaves after speaking about Russia in the East Room of the White House, Thursday, April 15, 2021, in Washington. (AP Photo/Andrew Harnik)

The Treasury Department on Thursday slapped six Russian technology companies with sanctions for supporting Kremlin intelligence agencies engaged in “dangerous and disruptive cyber attacks.”

But only one of them stands out for its international footprint and partnerships with such IT heavyweights as Microsoft and IBM.

That company, Positive Technologies, claims more than 2,000 customers in 30 countries, including major European banks Societe Generale and ING, as well as Samsung, SK Telecom of South Korea and BT, the British telecommunications giant.

Its clients also include the FSB, a successor to the KGB that “cultivates and co-opts criminal hackers” who carry out ransomware and phishing attacks, the Treasury Department said. The U.S. said big conventions hosted by Positive Technologies are “used as recruiting events” by the FSB and the GRU, Russia’s military intelligence agency.

GRU agents are the swashbucklers of Russian intelligence. The agency stands accused of spearheading the hack-and-leak operation that interfered in the 2016 U.S. presidential election to favor Donald Trump. Its agents also conducted the most damaging cyberattack on record, the runaway 2017 NotPetya virus that did more than $10 billion in global damage, its victims including the shipping giant Maersk and pharmaceutical company Merck.

The CEO of the software industry-supported Internet Research Institute in Moscow, Karen Kazaryan, said he was not familiar with most of the Russian IT companies sanctioned on Thursday. But Positive Tech is well-known in the industry for its annual Hack Days conference, which is scheduled for May 20-21 at a Moscow hotel.

Former CIA analyst Michael van Landingham applauded the naming and sanctioning of Russian IT companies known to have aided and abetted malign government activity.

“Naming specific companies can create incentives for educated and skilled Russians who might be able to obtain jobs elsewhere where they don’t support Russian state hacking,” he said.

Positive Tech’s specialty is identifying vulnerabilities in popular software such as Microsoft’s Windows operating system. The world’s intelligence agencies regularly lean on companies like it not to disclose potent vulnerabilities publicly when they find them but to instead quietly share them for hacking adversaries’ networks.

The U.S. did not accuse Positive Technologies of any such behavior and the Treasury Department declined to answer questions about the company’s activities beyond a press release.

Microsoft would not offer details on the the company’s business relationship with Positive Tech but did say it would comply with the sanctions. Spokesmen also said the company was removing Positive Tech from a list of more than 80 security software providers to which it gives early access to vulnerability information so they can make sure their customers get patches quickly. IBM also lists Positive Technologies as a security partner, offering customers one of its scanning tools.

IBM didn’t respond to requests for comment Thursday. Neither did U.S. tech companies HP and VMware, which Positive Technologies lists as technology partners.

On its website, Positive Technologies lists Russia’s Defense Ministry as among its first major clients, in 2004 when it was two years old with just 11 employees. It claimed more than 800 employees in 2018.

Russia's biggest business database lists the company's CEO and founder as Yury Maximov, about whom little is known other than he graduated from Moscow State University. The company did not respond to questions sent to press contacts on its website.

Positive Tech's website boasts of a number of accomplishments, such as providing cybersecurity for the 2018 soccer World Cup hosted by Russia and publishing data that same year on 30 high-risk vulnerabilities. It said it opened its first international office in London in 2010 and its first U.S. office in 2012.

The company has sometimes used Framingham, Massachusetts, as its U.S. location in news releases, though it's not recorded in city or state records as a business by that name. An office building with an address linked to the company is a co-working space that can be rented on flexible terms for "one person or more."

Market research firm IDC listed Positive Technologies as one of the fastest-growing companies in security and vulnerability management in 2012, in part because it was so small at the time, growing nearly 82% year-over-year to $30 million in worldwide revenue. Nearly all that revenue came from assessing vulnerabilities. But by 2015, its worldwide revenues fell 37.6% to $26.5 million, according to IDC, which eventually stopped tracking the company.

###