The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Cracks Down on Russian 'Evil Corp' Cybercrime Group

Russian hackers stole more than $100 million in eight-year operation run out of Moscow cafe basements.

By Reuters

December 06, 2019

British authorities published photos of Evil Corp ringleader Maxim Yakubets' lavish lifestyle. **National Crime Agency**

U.S. authorities took aim at a Russian cybercriminal group known as Evil Corp Thursday, indicting its Lamborghini-driving alleged leader and ordering asset freezes against 17 of his associates over a digital crime spree that has netted more than $100 million from companies across the world.

The action against Evil Corp, described by officials as one of the most damaging criminal organizations on the internet, comes with a $5 million bounty issued for information leading to the arrest of its alleged leader, Maksim Yakubets.

British authorities described the 32-year-old Yakubets as a supercar-lover who customized his Lamborghini license plate to read "Thief" in Russian and ran his operation from the basements of Moscow cafes.

"Yakubets is a true 21st century criminal," U.S. Assistant Attorney General Brian Benczkowski said. "He's earned his place on the FBI's list of the world's most wanted cyber criminals."

Related article: U.S. Sanctions Russian Cybercrime Outfit 'Evil Corp'

Evil Corp is alleged to be behind an ever-evolving family of malicious software known as Dridex, which has bedeviled banks and businesses since it first appeared in 2011. The malware works by hacking into banks and businesses and making rogue financial transfers that are eventually funneled back to the hackers. It has since also branched out into ransomware.

The Russian connection

Underlining alleged links between cybercriminals and the Russian state, U.S. Treasury officials said Yakubets worked on the side for Russia's Federal Security Service (FSB), its domestic intelligence agency, and stole classified material on Moscow's behalf. One senior U.S. Treasury official said he had even applied to the FSB for a license last year to handle secret documents.

Even so, the FBI's Bowdich said the Russian government had been "helpful to a point" in their request to track the hackers down. Bowdich and other U.S. officials declined to comment on whether either of the two men had links to the Russian government. The FSB did not immediately reply to a Reuters request for comment sent after hours in Russia on Thursday.

Dridex targeted smaller businesses and organizations that lacked the sophisticated cyberdefenses of larger organizations, U.S. officials said.

Though the indictments only mentioned incidents in Nebraska and Pennsylvania, victims spanned the United States — including a dairy company in Ohio, a luggage company in New Mexico and a religious order in Nebraska, FBI Deputy Director David Bowdich told a news conference.

Losses totaled $70 million in the United States alone, officials said.

The crackdown straddled the world of cybercrime and intelligence. The U.S. Treasury and Justice Departments worked in coordination with Britain's National Crime Agency, which published a series of photographs and video of the hacker's lavish, devil-may-care lifestyle that featured pictures of his camoflaged car streaked with fluorescent yellow.

Related article: Russia's FSB Linked to $450M Bitcoin Disappearance – BBC

The director general of the British agency, Lynne Owens, said that Yakubets and Evil Corp "represent the most significant cyber crime threat to the U.K.," a sentiment endorsed by John Shier, an expert at U.K.-based cybersecurity company Sophos.

"I'd put them in the top tier," he said of the group's operators.

American and British companies were targets of choice, according to U.S. Treasury officials, but they said France, Italy, the United Arab Emirates, India and Malaysia were also badly affected.

In addition to Yakubets, his close associate Igor Turashev, 38, was also indicted in the United States Thursday for allegedly serving as the group's technical administrator. U.K. authorities say they have already arrested and convicted eight other members of the network.

Reuters could not immediately locate contact details for Yakubets and Turashev, who have not been arrested and are believed to be still at large.

Zero chance

This is at least the second major effort by American authorities and their allies to bring down Evil Corp — whose eye-catching name appears to be more of nickname than a formal company. A 2015 indictment also charged Yakubets and Turashev with a series of fraud and hacking crimes, but they were never arrested and — following a brief disruption — Dridex went right back to stealing money.

Shier, of Sophos, said that Thursday's attempt appeared to be more robust — but he doubted that Yakubets would ever see justice.

"What are the chances this guy is going to face trial in the United States?" he said. "Probably next to zero."

Even so, officials described the charges as an important step that strips the hackers of their anonymity and makes it more difficult for them to travel internationally.

Benczkowski, head of the U.S. Justice Department's Criminal Division, said the group was carrying out crimes as recently as May. "It is fair to say they are not out of business at this point," he said. "But that is our ultimate goal."

Original url:
https://www.themoscowtimes.com/2019/12/06/us-cracks-down-on-russian-cybercrime-group-evil-corp-a68503