

Cybercriminal Connected to Multimillion Dollar Ransomware Attacks Sentenced for Online Fraud Schemes

[justice.gov/opa/pr/cybercriminal-connected-multimillion-dollar-ransomware-attacks-sentenced-online-fraud-schemes](https://www.justice.gov/opa/pr/cybercriminal-connected-multimillion-dollar-ransomware-attacks-sentenced-online-fraud-schemes)



Press Release

Friday, March 25, 2022

For Immediate Release

Office of Public Affairs

An Estonian man was sentenced today to 66 months in prison for his years-long role in furthering and facilitating computer intrusions, the movement of fraudulently obtained goods and funds, and the monetization of stolen financial account information. He also participated in ransomware attacks causing over \$53 million in losses and was ordered to pay over \$36 million in restitution.

According to court documents, Maksim Berezan, 37, of Estonia, who was apprehended in Latvia and extradited to the United States, pleaded guilty in April 2021 to conspiracy to commit wire fraud affecting a financial institution and conspiracy to commit access device fraud and computer intrusions. Berezan was an active member of an exclusive online forum designed for Russian-speaking cybercriminals to gather safely and exchange their criminal knowledge, tools, and services. From 2009 through 2015, Berezan not only furthered the criminal aims of the forum, but he also worked closely with forum members and other cybercriminals for purposes of obtaining and exploiting stolen financial account information.

“This case is a prime example of how the Department of Justice can leverage its traditional tools – criminal investigations and prosecutions – to combat ransomware,” said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department’s Criminal Division. “Many of the world’s ransomware players began as fraudsters engaged in other types of online crimes, and this case demonstrates that their crimes will catch up to them. The United States is committed to working with its international partners to hold cybercriminals accountable.”

“Cybercrime has become increasingly more sophisticated, but so have our methods for combatting it,” said U.S. Attorney Jessica D. Aber for the Eastern District of Virginia. “Ransomware attacks are devastating to people and organizations alike, and we have honed our strategies and techniques to target both the individual actors who perpetrate these attacks and the networks that support them. This case is just one example of how EDVA and the Justice Department are tackling this threat.”

“The Secret Service remains committed to ensuring that modern conveniences of today that facilitate our lawful transactions and economic health are not leveraged by criminals for illicit activity and personal gain,” said Special Agent in Charge Matthew Stohler of the U.S. Secret Service. “While we have long been in the business of protecting money, from the earliest days of coins and paper, to plastic, and today’s more accessible and commonplace digital currencies, we also remain in parallel footprint to the evolution of criminal behavior into cyberspace. Ransomware thieves are not safe in any dark corner of the internet in which they may think they can hide from our highly trained investigators and law enforcement partners worldwide. Together with our critical partners we are dedicated to protecting the public and securing every iteration of our money and every part of our national financial infrastructure.”

According to court documents, following Berezan’s arrest, investigators uncovered within his electronic devices evidence of his involvement in ransomware activities. The post-extradition investigation determined that Berezan had participated in at least 13 ransomware attacks, seven of which were against U.S. victims, and that approximately \$11 million in ransom payments flowed into cryptocurrency wallets that he controlled. Berezan used his ill-gotten gains to purchase two Porsches, a Ducati motorcycle, and an assortment of jewelry. In addition, authorities recovered from Berezan’s residence currency worth more than \$200,000 and electronic devices storing passphrases to bitcoin wallets that contained bitcoin worth approximately \$1.7 million, which has been forfeited.

Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department’s Criminal Division; U.S. Attorney Jessica D. Aber for the Eastern District of Virginia; Special Agent in Charge Matthew Stohler of the Washington Field Office of the U.S. Secret Service and Special Agent in Charge Jason Kane of the Criminal Investigative Division of the U.S. Secret Service made the announcement.

Senior Trial Attorney Laura Fong and Trial Attorney Alison Zitron of the Criminal Division’s Computer Crime and Intellectual Property Section, and Assistant U.S. Attorneys Alexander P. Berrang, Jonathan Keim, and Zoe Bedell of the Eastern District of Virginia prosecuted the case.

The Justice Department’s Office of International Affairs provided vital assistance. The Department of Justice extends its gratitude to authorities in Estonia and Latvia for their significant cooperation and assistance, in particular, the Latvian State Police and Estonian Police.

Updated March 25, 2022

Topic

Cybercrime

Press Release Number: 22-290