Sodinokibi/REvil Affiliate Sentenced for Role in $700M Ransomware Scheme

Published: 2024-05-01 · Archived: 2026-04-02 10:37:10 UTC

A Ukrainian national was sentenced today to 13 years and seven months in prison and ordered to pay over $16 million in restitution for his role in conducting over 2,500 ransomware attacks and demanding over $700 million in ransom payments.

“As this sentencing shows, the Justice Department is working with our international partners and using all tools at our disposal to identify cybercriminals, capture their illicit profits, and hold them accountable for their crimes,” said Attorney General Merrick B. Garland.

“Deploying the REvil ransomware variant, the defendant reached out across the globe to demand hundreds of millions of dollars from U.S. victims,” said Deputy Attorney General Lisa Monaco. “But this case shows the Justice Department’s reach is also global—working with our international partners, we are bringing to justice those who target U.S. victims, and we are disrupting the broader cybercrime ecosystem.”

“Today, the FBI’s close collaboration with our worldwide partners has again ensured that a cybercriminal who thought he was beyond our reach faces the consequences of his actions,” said FBI Director Christopher Wray. “We will continue to relentlessly pursue cyber criminals like Vasinksyi wherever they may hide, while we disrupt their criminal schemes, seize their money and infrastructure, and target their enablers and criminal associates to the fullest extent of the law.”

According to court documents, Yaroslav Vasinskyi, also known as Rabotnik, 24, conducted thousands of ransomware attacks using the ransomware variant known as Sodinokibi/REvil. Ransomware is malicious software designed to encrypt data on victim computers, allowing bad actors the ability to demand a ransom payment in exchange for the decryption key. The co-conspirators demanded ransom payments in cryptocurrency and used cryptocurrency exchangers and mixing services to hide their ill-gotten gains. To drive their ransom demands higher, Sodinokibi/REvil co-conspirators also publicly exposed their victims’ data when victims would not pay ransom demands.

“Yaroslav Vasinskyi and his co-conspirators hacked into thousands of computers around the world and encrypted them with ransomware,” said Principal Deputy Assistant Attorney General Nicole M. Argentieri, head of the Justice Department’s Criminal Division. “Then they demanded over $700 million in ransom payments and threatened to publicly disclose victims’ data if they refused to pay. Although the conspirators attempted to cover their tracks by laundering the payments from victims, Vasinskyi could not hide from law enforcement. Vasinskyi’s sentence today should serve as a reminder to ransomware actors everywhere: we will track you down and bring you to justice.”

“Using ransomware, malicious actors from around the globe can paralyze U.S. companies in a matter of minutes,” said U.S. Attorney Leigha Simonton for the Northern District of Texas. “But as cybercriminals work together to

deploy these attacks, law enforcement throughout the United States stands ready to dismantle their criminal enterprises. The dedicated prosecutors from the Northern District of Texas and the skilled agents at the FBI Dallas Field Office proved once again today to ransomware actors everywhere: When you hit targets in the United States, the Justice Department and its partners will come after you."

Vasinskyi previously pleaded guilty in the Northern District of Texas to an 11-count indictment charging him with conspiracy to commit fraud and related activity in connection with computers, damage to protected computers, and conspiracy to commit money laundering. He was previously extradited to the United States from Poland.

Relatedly, in 2023, the Department obtained the final forfeiture of millions of dollars' worth of ransom payments obtained through two related civil forfeiture cases, which included 39.89138522 Bitcoin and $6.1 million in U.S. dollar funds traceable to alleged ransom payments received by other members of the conspiracy.

The FBI investigated the case.

Senior Counsel Frank Lin of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Tiffany H. Eggers for the Northern District of Texas prosecuted the case. Assistant U.S. Attorney Dimitri N. Rocha for the Northern District of Texas assisted with the related civil forfeiture cases.

The Justice Department's Office of International Affairs worked with Polish authorities to secure the extradition of Vasinskyi.
