Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas

justice.gov/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas

THE UNITED STATES
DEPARTMENT
of JUSTICE

Press Release

Wednesday, March 9, 2022

For Immediate Release
Office of Public Affairs

A man charged with conducting ransomware attacks against multiple victims, including the July 2021 attack against Kaseya, made his initial appearance and was arraigned today in the Northern District of Texas.

According to an August 2021 indictment, Yaroslav Vasinskyi, 22, accessed the internal computer networks of several victim companies and deployed Sodinokibi/REvil ransomware to encrypt the data on the computers of victim companies.

“When last year I announced charges against members of the Sodinokibi/REvil ransomware group, I made clear that the Justice Department will spare no resource in identifying and bringing to justice transnational cybercriminals who target the American people,” said Attorney General Merrick B. Garland. “That is exactly what we have done. The United States, alongside our international partners, will continue to swiftly identify, locate, and apprehend alleged cybercriminals, capture their illicit profits, and bring them to justice.”

“Just eight months after committing his alleged ransomware attack on Kaseya from overseas, this defendant has arrived in a Dallas courtroom to face justice,” said Deputy Attorney General Lisa O. Monaco. “When we are attacked, we will work with our partners here and abroad to go after cybercriminals, wherever they may be.”

According to the indictment, Vasinskyi was allegedly responsible for the July 2, 2021, ransomware attack against Kaseya. In the alleged attack against Kaseya, Vasinskyi caused the deployment of malicious Sodinokibi/REvil code throughout a Kaseya product that caused the Kaseya production functionality to deploy REvil ransomware to “endpoints” on Kaseya customer networks. After the remote access to Kaseya endpoints was established, the ransomware was executed on those computers, which resulted in the encryption of data on computers of organizations around the world that used Kaseya software.

Through the deployment of Sodinokibi/REvil ransomware, the defendant allegedly left electronic notes in the form of a text file on the victims’ computers. The notes included a web address leading to an open-source privacy network known as Tor, as well as the link to a publicly accessible website address the victims could visit to recover their files. Upon visiting either website, victims were given a ransom demand and provided a virtual currency address to use to pay the ransom. If a victim paid the ransom, the defendant provided the decryption key and the victim then was able to access their files. If a victim did not pay the ransom, the defendant typically posted the victim’s stolen data or claimed they sold the stolen data to third parties, and victims remained unable to access their files.

Vasinskyi is charged with conspiracy to commit fraud and related activity in connection with computers, damage to protected computers, and conspiracy to commit money laundering. If convicted of all counts, he faces a total penalty of 115 years in prison. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

Vasinskyi, a Ukrainian national with ties to a ransomware group linked to Russia-based actors, was taken into custody in Poland where he remained held by authorities pending proceedings in connection with his requested extradition to the United States, pursuant to the extradition treaty between the United States and the Republic of Poland. Vasinskyi was transported to Dallas by U.S. law enforcement authorities where he arrived on March 3. He made his initial court appearance and was arraigned today in the Northern District of Texas.

The FBI’s Dallas and Jackson Field Offices are leading the investigation. Substantial assistance was provided by the Justice Department’s Office of International Affairs and the National Security Division’s Counterintelligence and Export Control Section.

Assistant U.S. Attorney Tiffany H. Eggers for the Northern District of Texas and Senior Counsel Byron M. Jones of the Criminal Division’s Computer Crime and Intellectual Property Section are prosecuting the case.

The U.S. Attorney’s Office for the Northern District of Texas, the FBI’s Dallas and Jackson Field Offices and the Criminal Division’s Computer Crime and Intellectual Property Section conducted the operation in close cooperation with Europol and Eurojust, which were an integral part of coordination. Investigators and prosecutors from several jurisdictions, including Romania's National Police and the Directorate for Investigating Organised Crime and Terrorism; Canada’s Royal Canadian Mounted Police; France’s Court of Paris and BL2C (anti-cybercrime unit police); the Dutch National Police; Poland’s National Prosecutor’s Office, Border Guard, Internal Security Agency, and Ministry of Justice; and the governments of Norway and Australia provided valuable assistance.

The U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN), the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA); Germany's Public Prosecutor's Office Stuttgart and State Office of Criminal Investigation of Baden-Wuerttemberg; Switzerland's Public Prosecutor's Office II of the Canton of Zürich and Cantonal Police Zürich; the National Police of Ukraine and the Prosecutor General's Office of Ukraine; the United Kingdom's National Crime Agency; the U.S. Secret Service; the Texas Department of Information Resources; BitDefender; McAfee; and Microsoft also provided significant assistance.

For more resources on ransomware prevention and response, visit www.StopRansomware.gov.

An indictment is merely an allegation, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated March 9, 2022

Topics

Cybercrime

National Security

Press Release Number: 22-210