Ukrainian Arrested and Charged with Ransomware Attack on Kaseya

justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

November 8, 2021

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, November 8, 2021

Justice Department Seizes $6.1 million Related to Alleged Ransomware Extortionists

The Justice Department announced today recent actions taken against two foreign nationals charged with deploying Sodinokibi/REvil ransomware to attack businesses and government entities in the United States.

An indictment unsealed today charges Yaroslav Vasinskyi, 22, a Ukrainian national, with conducting ransomware attacks against multiple victims, including the July 2021 attack against Kaseya, a multi-national information technology software company.

The department also announced today the seizure of $6.1 million in funds traceable to alleged ransom payments received by Yevgeniy Polyanin, 28, a Russian national, who is also charged with conducting Sodinokibi/REvil ransomware attacks against multiple victims, including businesses and government entities in Texas on or about Aug. 16, 2019.

According to the indictments, Vasinskyi and Polyanin accessed the internal computer networks of several victim companies and deployed Sodinokibi/REvil ransomware to encrypt the data on the computers of victim companies.

“Cybercrime is a serious threat to our country: to our personal safety, to the health of our economy, and to our national security,” said Attorney General Garland. “Our message today is clear. The United States, together with our allies, will do everything in our power to identify the perpetrators of ransomware attacks, to bring them to justice, and to recover the funds they have stolen from their victims.”

“Our message to ransomware criminals is clear: If you target victims here, we will target you,” said Deputy Attorney General Monaco. “The Sodinokibi/REvil ransomware group attacks companies and critical infrastructures around the world, and today’s announcements showed how we will fight back. In another success for the department’s recently launched Ransomware and Digital Extortion Task Force, criminals now know we will take away your profits, your ability to travel, and – ultimately – your freedom. Together with our partners at home and abroad, the Department will continue to dismantle ransomware groups and disrupt the cybercriminal ecosystem that allows ransomware to exist and to threaten all of us.”

“The arrest of Yaroslav Vasinskyi, the charges against Yevgeniy Polyanin and seizure of $6.1 million of his assets, and the arrests of two other Sodinokibi/REvil actors in Romania are the culmination of close collaboration with our international, U.S. government and especially our private sector partners,” said FBI Director Christopher Wray. “The FBI has worked creatively and relentlessly to counter the criminal hackers behind Sodinokibi/REvil. Ransomware groups like them pose a serious, unacceptable threat to our safety and our economic well-being. We will continue to broadly target their actors and facilitators, their infrastructure, and their money, wherever in the world those might be.”

“Ransomware can cripple a business in a matter of minutes. These two defendants deployed some of the internet’s most virulent code, authored by REvil, to hijack victim computers,” said Acting U.S. Attorney Chad E. Meacham for the Northern District of Texas. “In a matter of months, the Justice Department identified the perpetrators, effected an arrest, and seized a significant sum of money. The Department will delve into the darkest corners of the internet and the furthest reaches of the globe to track down cyber criminals.”

According to court documents, Vasinskyi was allegedly responsible for the July 2 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 defendants 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 amount, the defendants provided the decryption key, and the victims then were able to access their files. If a victim did not pay the ransom, the defendants typically posted the victims' stolen data or claimed they sold the stolen data to third parties, and victims were unable to access their files.

Vasinskyi and Polyanin are charged in separate indictments with conspiracy to commit fraud and related activity in connection with computers, substantive counts of damage to protected computers, and conspiracy to commit money laundering. If convicted of all counts, each faces a maximum penalty of 115 and 145 years in prison, respectively.

The $6.1 million seized from Polyanin is alleged to be traceable to ransomware attacks and money laundering committed by Polyanin through his use of Sodinokibi/REvil ransomware. The seizure warrant was issued out of the Northern District of Texas. Polyanin is believed to be abroad.

On Oct. 8, Vasinskyi was taken into custody in Poland where he remains 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. In parallel with the arrest, interviews and searches were carried out in multiple countries, and would not have been possible without the rapid response of the National Police of Ukraine and the Prosecutor General's Office of Ukraine.

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 of the U.S. Attorney's Office for the Northern District of Texas and Senior Counsel Byron M. Jones from the Justice Department'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, who 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); 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), 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; United Kingdom’s National Crime Agency; U.S. Secret Service; Texas Department of Information Resources; BitDefender; McAfee; and Microsoft also provided significant assistance.

This case is part of the Department of Justice’s Ransomware and Digital Extortion Task Force, which was created to combat the growing number of ransomware and digital extortion attacks. As part of the task force, the Criminal Division, working with the U.S. Attorneys’ Offices, prioritizes the disruption, investigation, and prosecution of ransomware and digital extortion activity by tracking and dismantling the development and deployment of malware, identifying the cybercriminals responsible, and holding those individuals accountable for their crimes. The department, through the task force, also strategically targets the ransomware criminal ecosystem as a whole and collaborates with domestic and foreign government agencies as well as private sector partners to combat this significant criminal threat.

For more information about the Ransomware and Digital Extortion Task Force, read the Deputy Attorney General’s recent guidance memo on related investigations and cases. For more resources on ransomware prevention and response, visit 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.