US charges 2 suspected major ransomware operators

8 November 2021, by Eric Tucker and Alan Suderman

Attorney General Merrick Garland, center, accompanied by Deputy Attorney General Lisa Monaco, left, and FBI Director Christopher Wray, right, speaks at a news conference at the Justice Department in Washington, Monday, Nov. 8, 2021. Credit: AP Photo/Andrew Harnik

A suspected Ukrainian hacker has been arrested and charged in the United States in connection with a string of costly ransomware attacks, including one that snarled businesses around the globe on the Fourth of July weekend, U.S. officials said Monday.

Yaroslav Vasinskyi was arrested last month after traveling to Poland, according to the Justice Department, which also announced the recovery of $6.1 million in ill-gotten funds from a Russian national who was separately charged and remains sought by the FBI.

Both men are alleged to be affiliated with the prolific Russia-based REvil ransomware gang, whose attacks have compromised tens of thousands of computers worldwide and yielded at least $200 million in ransom payments, said Attorney General Merrick Garland. Victims have included the world's largest meat processor, JBS SA, and a technology company called Kaseya, which was hit in a holiday weekend attack last July that the company said affected between 800 and 1,500 businesses that relied on its software.

The coordination of multiple agencies across the Biden administration amounted to perhaps the most high-profile response yet to a blitz of ransomware attacks that officials say continues to threaten national security and the economy. Deputy Attorney General Lisa Monaco appeared to foreshadow Monday's announcement in an interview with The Associated Press last week, saying that "in the days and weeks to come, you're going to see more arrests" as well as more seizures of illicit ransomware proceeds.

Speaking at a news conference Monday, she said, "We have been using every tool at our disposal and leveraging every authority we have to hunt down and hold accountable cybercriminals wherever they seek to hide."

The indictment accuses Vasinskyi, 22, of deploying REvil ransomware, also known as Sodinokibi, a broad range of victims—including the massive Kaseya attack.

Yevgeniy Polyanin, a Russian national, is charged in a separate indictment. He's accused of conducting roughly 3,000 ransomware attacks on companies and entities across the U.S., including law enforcement agencies and local governments in the state of Texas.

In this March 22, 2019 file photo, an American flag flies outside the Department of Justice in Washington. Credit: AP Photo/Andrew Harnik

The announcement of the criminal charges came hours after European law enforcement officials revealed the results of a lengthy, 17-nation operation. As part of that operation, Europol said, a total of seven hackers linked to REvil and another ransomware family have been arrested since February, including two last week by Romanian authorities.

The Justice Department has tried multiple ways to address a ransomware scourge that has exploded over the last year with attacks against critical infrastructure and major corporations. Arrests of foreign hackers are significant for the Justice Department, and rare, since many of them operate in the refuge of countries that do not extradite their own citizens to the U.S. for prosecution.

Both indictments were filed in federal court in the Northern District of Texas, a state where REvil ransomware compromised the computer networks of some two dozen local government agencies in the summer of 2019.

The U.S. is seeking Vasinskyi's extradition from Poland. Though it successfully seized $6 million in ransomware payments from Polyanin, the FBI is continuing to seek his arrest, and the State Department on Monday announced a $10 million reward for anyone with information leading to the capture of any leaders of the REvil group.

The Treasury Department, meanwhile, announced sanctions against the pair as well as a virtual currency exchange, Chatex, that it said was used to facilitate financial transactions for ransomware gangs.

President Joe Biden commended the government's actions, saying he was making good on his commitment to Russian leader Vladimir Putin that the U.S. would hold cyber criminals accountable.

He said in a statement that the U.S. was "bringing the full strength of the federal government to disrupt malicious cyber activity and actors" and to "bolster resilience at home."

Deputy Attorney General Lisa Monaco speaks to The Associated Press during an interview at the Department of Justice in Washington, Tuesday, Nov. 2, 2021. Two suspected hackers accused of ransomware attacks resulting in 5,000 infections have been arrested as part of a global cybercrime crackdown. That's according to an announcement Monday from Europol. Monaco appeared to foreshadow Monday's announcement in an interview with The Associated Press last week, saying that "in the days and weeks to come, you're going to see more arrests." Credit: AP Photo/Manuel Balce Ceneta, file

"There's lots of reasons why people travel, and I can't get into the specific reasons why Mr. Vasinskyi traveled, but boy are we glad he did," FBI Director Christopher Wray said Monday.

Even so, ransomware attacks—in which hackers seize and encrypt data and demand often-exorbitant sums to release it to victims—have been hard to curb. Monaco told the AP last week that since Biden's admonitions to Putin last summer to rein in ransomware gangs, "we have not seen a material change in the landscape."

Garland did not answer directly when asked if there was evidence that the Russian government was aware of REvil's activities, but said, "we expect and hope that any government in which one of these ransomware actors is residing will do everything it can to provide that person to us for prosecution."

The $6.1 million seizure in this case builds on a similar success from months ago.

Federal authorities in June seized $2.3 million in cryptocurrency from a payment made by Colonial Pipeline following a ransomware attack that caused the company to temporarily halt operations, creating fuel shortages in parts of the country.

Justice Department officials also used Monday's news conference to urge Congress to create a national standard for the reporting of significant cyber incidents, and to require that that information be shared immediately with federal law enforcement.

APA citation: US charges 2 suspected major ransomware operators (2021, November 8) retrieved 21 January 2022 from https://techxplore.com/news/2021-11-hackers-global-ransomware-crackdown.html