Member of “The Dark Overlord” Hacking Group Extradited From United Kingdom to Face Charges in St. Louis

Press Release

Wednesday, December 18, 2019

For Immediate Release
Office of Public Affairs

Defendant Conspired to Steal Sensitive Personally Identifying Information from Victim Companies and Release those Records on Criminal Marketplaces unless Victims Paid Bitcoin Ransoms

A United Kingdom national appeared today in federal court on charges of aggravated identity theft, threatening to damage a protected computer, and conspiring to commit those and other computer fraud offenses, related to his role in a computer hacking collective known as “The Dark Overlord,” which targeted victims in the St. Louis, Missouri, area beginning in 2016.

Nathan Wyatt, 39, was extradited from the United Kingdom to the Eastern District of Missouri and arraigned on Dec. 18 before U.S. Magistrate Judge Shirley Padmore Mensah. He pleaded not guilty and was detained pending further proceedings.

A federal grand jury indicted Wyatt on Nov. 8, 2017. According to court records, beginning in 2016, Wyatt was a member of The Dark Overlord, a hacking group that was responsible for remotely accessing the computer networks of multiple U.S. companies without authorization, obtaining sensitive records and information from those companies, and then threatening to release the companies’ stolen data unless the companies paid a ransom in bitcoin. Victims in the Eastern District of Missouri included healthcare providers, accounting firms, and others. Among other things, Wyatt is alleged to have participated in the conspiracy by creating email and phone accounts that he used to send threatening and extortionate emails and text messages to certain victims, including victims in the Eastern District of Missouri.

“Today’s extradition shows that the hackers hiding behind The Dark Overlord moniker will be held accountable for their alleged extortion of American companies,” said Assistant Attorney General Brian A. Benczkowski of the Justice Department’s Criminal Division. “We are thankful for the close cooperation of our partners in the United Kingdom in ensuring that the defendant will face justice in U.S. court.”

“Cyber criminals who harm victims in the Eastern District of Missouri cannot hide behind international borders to evade justice,” said U.S. Attorney Jeffrey B. Jensen of the Eastern District of Missouri. “Today’s case demonstrates the United States’ commitment to unmasking criminal hackers and bringing them to justice, no matter where they may be located.”

“Cyber hackers may no longer use territorial borders to shield themselves from accountability,” said Special Agent in Charge Richard Quinn of the FBI’s St. Louis Field Office. “This case is another example of how the FBI successfully works with international law enforcement partners to bring alleged perpetrators to justice.”

The investigation was conducted by the FBI’s St. Louis Field Office. The FBI’s Atlanta Field Office also provided support. The Criminal Division’s Office of International Affairs coordinated the extradition of Wyatt. The department thanks law enforcement and international cooperation authorities in the United Kingdom for their substantial assistance in the investigation.

Senior Counsel Laura-Kate Bernstein of the Criminal Division’s Computer Crime and Intellectual Property Section, and Assistant U.S. Attorneys Gwendolyn Carroll and Matthew Drake of the Eastern District of Missouri are prosecuting the case.

The details contained in the charging document are allegations. The defendant is presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated January 17, 2020

Topics

Cybercrime

Identity Theft

Press Release Number: 19-1420