U.K. Citizen Extradited and Pleads Guilty to Cyber Crime Offenses

Press Release

Tuesday, May 9, 2023

For Immediate Release
Office of Public Affairs

A U.K. citizen pleaded guilty today in New York to his role in cyberstalking and multiple schemes that involve computer hacking, including the July 2020 hack of Twitter.

Joseph James O'Connor, aka PlugwalkJoe, 23, was extradited from Spain on April 26.

"O'Connor's criminal activities were flagrant and malicious, and his conduct impacted multiple people's lives. He harassed, threatened, and extorted his victims, causing substantial emotional harm," said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department's Criminal Division. "Like many criminal actors, O'Connor tried to stay anonymous by using a computer to hide behind stealth accounts and aliases from outside the United States. But this plea shows that our investigators and prosecutors will identify, locate, and bring to justice such criminals to ensure they face the consequences for their crimes."

"O'Connor has left an impressive trail of destruction in the wake of his wave of criminality," said U.S. Attorney Ismail J. Ramsey for the Northern District of California. "This case serves as a warning that the reach of the law is long, and criminals anywhere who use computers to commit crimes may end up facing the consequences of their actions in places they did not anticipate."

"O'Connor used his sophisticated technological abilities for malicious purposes – conducting a complex SIM swap attack to steal large amounts of cryptocurrency, hacking Twitter, conducting computer intrusions to take over social media accounts, and even cyberstalking two victims, including a minor victim," said U.S. Attorney

Damian Williams for the Southern District of New York. “O’Connor’s guilty plea today is a testament to the importance of law enforcement cooperation, and I thank our law enforcement partners for helping to bring to justice those who victimize others through cyber-attacks.”

“Today’s guilty plea is confirmation that the FBI’s strategy to counter cyber crime is working. It’s also indicative of what can be accomplished when we work closely with our partners to bring these perpetrators to justice and make the cyber ecosystem more secure,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “O'Connor's extradition is as a warning to all dangerous cyber criminals that the FBI will work tirelessly to find them and hold them accountable wherever in the world they may try to hide.”

NDCA Case

According to court documents, between 2019 and 2020, O’Connor participated in a variety of crimes associated with exploitation of social media accounts, online extortion, and cyberstalking.

In July 2020, O’Connor participated in a conspiracy to gain unauthorized access to social media accounts maintained by Twitter Inc. (Twitter). In early July 2020, O’Connor’s co-conspirators used social engineering techniques to obtain unauthorized access to administrative tools used by Twitter to maintain its operations. The co-conspirators were able to use the tools to transfer control of certain Twitter accounts from their rightful owners to various unauthorized users. In some instances, the co-conspirators took control themselves and used that control to launch a scheme to defraud other Twitter users. In other instances, the co-conspirators sold access to Twitter accounts to others. O’Connor communicated with others regarding purchasing unauthorized access to a variety of Twitter accounts, including accounts associated with public figures around the world. A number of Twitter accounts targeted by O’Connor were subsequently transferred away from their rightful owners. O’Connor agreed to purchase unauthorized access to one Twitter account for $10,000.

O’Connor also accessed without authorization one of the most highly visible TikTok accounts in August 2020, which was associated with a public figure with millions of followers (Victim-1). O’Connor and his co-conspirators obtained unauthorized access to Victim-1’s account via a SIM swap after discussing a variety of celebrities to target, and O’Connor used his unauthorized access to Victim-1’s platform to post self-promotional messages, including a video in which O’Connor’s voice is recognizable. O’Connor also stated publicly, via a post to Victim-1’s TikTok account, that he would release sensitive, personal material related to Victim-1 to individuals who joined a specified Discord server.

O’Connor also targeted another public figure (Victim-2) in June 2019. O’Connor and his co-conspirators obtained unauthorized access to Victim-2’s account on Snapchat via a SIM swap. They used that access to obtain sensitive materials, to include private images, that Victim-2 had not made publicly available. O’Connor sent copies of these sensitive materials to his co-conspirators. O’Connor and his co-conspirators also reached out to Victim-2 and threatened to publicly release the stolen sensitive materials unless Victim-2 agreed to publicly post messages related to O’Connor’s online persona, among other things.

Lastly, O'Connor stalked and threatened a minor victim (Victim-3) in June and July 2020. In June 2020, O'Connor orchestrated a series of swatting attacks on Victim-3. A "swatting" attack occurs when an individual makes a false emergency call to a public authority in order to cause a law enforcement response that may put the victim or others in danger. On June 25, 2020, O'Connor called a local police department and falsely claimed that Victim-3 was making threats to shoot people. O'Connor provided an address that he believed was Victim-3's address, which would have the result of causing a law enforcement response. That same day, O'Connor placed another call to the same police department and stated that he was planning to kill multiple people at the same address. In response to that call, the department dispatched every on-duty officer to that address in reference to an armed and dangerous individual. O'Connor sent other swatting messages that same day to a high school, a restaurant, and a sheriff's department in the same area. In those messages, O'Connor represented himself as either Victim-3 or as a resident at the address he believed was Victim-3's. The following month, O'Connor called multiple family members of Victim-3 and threatened to kill them.

The NDCA Case was transferred to SDNY pursuant to Federal Rule of Criminal Procedure 20 and consolidated with the SDNY Case.

SDNY Case

According to court documents, between approximately March 2019 and May 2019, O'Connor and his co-conspirators perpetrated a scheme to use subscriber identity module (SIM) swaps, a cyber intrusion technique, to conduct cyber intrusions to steal approximately $794,000 worth of cryptocurrency from a Manhattan-based cryptocurrency company (Company-1), which provided wallet infrastructure and related software to cryptocurrency exchanges around the world.

During a SIM swap attack, cyber threat actors gain control of a victim's mobile phone number by linking that number to a SIM card controlled by the threat actors, resulting in the victim's calls and messages being routed to a malicious unauthorized device controlled by the threat actors. The threat actors then typically use control of the victim's mobile phone number to obtain unauthorized access to accounts held by the victim that are registered to the mobile phone number.

As part of the scheme, O'Connor and his co-conspirators successfully perpetrated SIM swap attacks targeting at least three Company-1 executives. Following a successful SIM swap attack targeting one of the executives on or about April 30, 2019, O'Connor and his co-conspirators successfully gained unauthorized access to multiple Company-1 accounts and computer systems. On or about May 1, 2019, through their unauthorized access, O'Connor and his co-conspirators stole and fraudulently diverted cryptocurrency of various types from cryptocurrency wallets maintained by Company-1 on behalf of two of its clients. The stolen cryptocurrency was worth at least approximately $794,000 at the time of the theft.

After stealing and fraudulently diverting the stolen cryptocurrency, O'Connor and his co-conspirators laundered it through dozens of transfers and transactions and exchanged some of it for Bitcoin using cryptocurrency exchange services. Ultimately, a portion of the stolen cryptocurrency was deposited into a cryptocurrency exchange account controlled by O'Connor.

As part of the NDCA Case, O'Connor pleaded guilty to conspiracy to commit computer intrusion and two counts of committing computer intrusions, each of which carries a maximum penalty of five years in prison; making extortive communications, which carries a maximum penalty of two years in prison; two counts of stalking, each of which carries a maximum penalty of five years in prison; and making threatening communications, which carries a maximum penalty of five years in prison. As part of the SDNY case, O'Connor pleaded guilty to conspiracy to commit computer intrusions, which carries a maximum penalty of five years in prison; conspiracy to commit wire fraud, which carries a maximum penalty of 20 years in prison; and conspiracy to commit money laundering, which carries a maximum penalty of 20 years in prison. O'Connor also agreed to forfeit $794,012.64 and to make restitution to victims of his crimes. He is scheduled to be sentenced on June 23. A federal district court judge will determine any sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI is investigating the case.

The U.S. Attorney's Office for the Northern District of California and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) are handling the NDCA case. Assistant U.S. Attorney Andrew F. Dawson for the Northern District of California and CCIPS Assistant Deputy Chief Adrienne L. Rose are prosecuting the case.

The U.S. Attorney's Office for the Southern District of New York's Complex Frauds and Cybercrime Unit is handling the SDNY case. Assistant U.S. Attorney Olga I. Zverovich for the Southern District of New York is prosecuting the case.

The Justice Department's Office of International Affairs provided valuable assistance in securing the extradition of O'Connor.

Updated May 9, 2023

Topic

Cybercrime

Press Release Number: 23-534