Individual Pleads Guilty to Participating in Internet-of-Things Cyberattack in 2016

Press Release

Wednesday, December 9, 2020

For Immediate Release
Office of Public Affairs

An individual, formerly a juvenile, pleaded guilty to committing acts of federal juvenile delinquency in relation to a cyberattack that caused massive disruption to the Internet in October 2016.

Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division, U.S. Attorney Scott W. Murray of the District of New Hampshire, and Special Agent in Charge Joseph R. Bonavolonta of the FBI's Boston Division made the announcement.

According to the plea agreement, the individual conspired to commit computer fraud and abuse by operating a botnet and by intentionally damaging a computer. Because the individual was a juvenile at the time of the commission of the offense, the individual's identity is being withheld pursuant to the Juvenile Delinquency Act, see 18 U.S.C. § 5031, et seq. The guilty plea took place in a closed proceeding before Chief Judge Landya B. McCafferty in the District of New Hampshire. Judge McCafferty scheduled the individual's sentencing for Jan. 7, 2021.

According to unsealed court documents, from approximately 2015 until November of 2016, the individual conspired with others to create and operate one or more online botnets to launch cyberattacks against victim computers (specifically targeting those belonging to online gamers or gaming platforms) in order to take those computers offline altogether or otherwise significantly impair their functionality. These attacks are often referred to as "Distributed Denial of Service" or "DDoS" attacks.

In general, a DDoS attack is a type of cyberattack in which a malicious actor directs a large volume of Internet traffic to a victim computer or network, overwhelming it and rendering it unable to function as intended. Successful DDoS attacks can take individual computer users, websites, or entire computer networks offline altogether or otherwise slow their performance. DDoS attacks are often conducted through the use of botnets (short for "robot networks"), that is, large numbers of compromised computers under the control of an individual or group of actors.

According to court documents, in September and October of 2016, the individual and others created a botnet, which was a variant of the so-called "Mirai" botnet, for use in launching DDoS attacks. Mirai infected "Internet-of-Things" devices, such as Internet-connected video cameras and recorders, and turned them into bots to be used to launch DDoS attacks.

According to court documents, on Oct. 21, 2016, the individual and others used the botnet they created to launch several DDoS attacks in an effort to take the Sony PlayStation Network's gaming platform offline for a sustained period. The DDoS attacks impacted a domain name resolver, New Hampshire-based Dyn, Inc., which caused websites, including those pertaining to Sony, Twitter, Amazon, PayPal, Tumblr, Netflix, and Southern New Hampshire University (SNHU), to become either completely inaccessible, or accessible only intermittently for several hours that day. As a result of the individual's DDoS attacks, Dyn, Sony, SNHU, and other entities and individuals suffered losses including lost advertising revenues and remediation costs. Sony estimated that its resultant losses included approximately $2.7 million in net revenue.

This case was investigated by the FBI with assistance from the National Crime Agency and Police Service of Northern Ireland. The case is being prosecuted by Senior Trial Attorney Mona Sedky of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Georgiana MacDonald of the District of New Hampshire. Former Assistant U.S. Attorney Arnold H. Huftalen provided substantial assistance.

The year 2020 marks the 150th anniversary of the Department of Justice. Learn more about the history of our agency at www.Justice.gov/Celebrating150Years.

Updated December 9, 2020

Topic

Cybercrime

Press Release Number: 20-1325