Maryland Man Sentenced to Prison for Intentionally Damaging the Computers of His Former Employer

Press Release

Thursday, September 24, 2020

For Immediate Release
Office of Public Affairs

A Maryland man was sentenced by U.S. District Judge Catherine C. Blake today to 12 months and one day in federal prison, followed by three years of supervised release, for illegally accessing and damaging the computer network of his former employer. Judge Blake also entered an order requiring Stafford to pay restitution in the amount of $193,258.10 to his former employer.

Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division, U.S. Attorney Robert K. Hur for the District of Maryland; Special Agent in Charge Jennifer C. Boone of the FBI's Baltimore Field Office and Deputy Inspector General Richard K. Delmar of the Department of the Treasury, Office of Inspector General made the announcement.

According to court documents and evidence presented at his four-day trial, from Jan. 5, 2004 through Aug. 6, 2015, Shannon Stafford, 50, of Crofton, Maryland, was employed in the information technology (IT) department at Business A, a global company with thousands of employees and offices around the world, including in Maryland and Washington, D.C. Stafford was employed in the Washington office and provided IT technical support to employees based at, or visiting, the Washington, McLean, Virginia, or Baltimore offices. As part of his duties, Stafford had access to the system login credentials of other employees and was authorized to use them in the course of performing his technical support duties. Stafford was also responsible for disabling company users' network access credentials at the end of their employment. In 2014, Business A provided Stafford with a laptop to use for his work.

Witnesses testified that in 2014, Stafford was promoted to the managerial role of technical site lead for the Washington office. In March 2015, Stafford was demoted back to an IT support role, due to performance issues in his management position. Stafford's performance issues continued and he was fired on Aug. 6, 2015. Stafford did not return the laptop he was previously provided by Business A.

The evidence proved that on the evening of Aug. 6, 2015, Stafford repeatedly attempted to remotely access Business A's computer networks from his residence, using the company laptop. Stafford unsuccessfully attempted to access the company's network approximately 10 times, using his own credentials and the credentials of a former co-worker, whom he had previously assisted. In the early morning hours of Aug. 8, 2015, Stafford successfully used the co-worker's credentials and the company laptop to access, without authorization, the computer in the Washington office that had been located under his desk. Stafford used the Washington IT computer to execute demands to delete all of the file storage drives used by the Washington office, then changed the password to access the storage management system. The deletion of the files caused a severe disruption to the company's operations and the loss of some customer and user data. Changing the password hindered the company's efforts to determine what happened and restore access to its remaining files. As a result of the deletion of the network file storage drives, Washington users were unable to access their stored files for approximately three days, until the data could be restored from backups. Customer and user data that was not included in the most recent backup prior to Stafford's deletion of the files was permanently lost.

On Aug. 11, 2015, Stafford unsuccessfully attempted to remotely access the company's computer network from his home approximately 13 times, using credentials that were not his. On Aug. 13, 2015, a company representative spoke to Stafford and demanded that he cease and desist his attempts to unlawfully access Business A's computer systems. The evidence showed that despite the Company's demand, between Aug. 21 and Sept. 9, 2015, Stafford attempted to access the company's network from his home approximately 17 times, using credentials that were not his. On Sept. 14, 2015, Stafford used the credentials of another former co-worker to access a network file storage system computer that he had been responsible for maintaining in the IT department of the company's Baltimore office, intending to cause the same type of damage he did when he deleted the Washington office's stored files. However, Stafford's attempt failed because Business A had changed the password after Stafford's attack on the Washington files.

The actual loss to Business A resulting from Stafford's damage and attempted damage to their computer systems, including the cost of restoring the deleted systems, investigating what happened, and responding to the intrusion is at least $38,270. In addition, Business A incurred legal fees totaling $133,950.60 and a fee of $21,037.50 for a forensic investigation.

The FBI and Treasury OIG conducted the investigation. Trial Attorney S. Riane Harper of the Criminal Division's Computer Crime and Intellectual Properties Section and Assistant U.S. Attorney Zachary A. Myers prosecuted the case.

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 September 24, 2020

Topic

Cybercrime

Press Release Number: 20-998