

Two charged in Massachusetts for defacing websites following killing of Qasem Soleimani

Two alleged computer hackers were indicted in the District of Massachusetts on charges of damaging multiple websites across the United States as retaliation for United States military action in January 2020 that killed Qasem Soleimani, the head of the Islamic Revolutionary Guard Corps-Quds Force, a U.S.-designated foreign terrorist organization.

Behzad Mohammadzadeh (a/k/a "Mrb3hz4d"), believed to be approximately 19 years old and a national of the Islamic Republic of Iran, and Marwan Abusrour (a/k/a "Mrwn007"), believed to be approximately 25 years old and a stateless national of the Palestinian Authority, were charged in an indictment unsealed today on one count of conspiring to commit intentional damage to a protected computer and one count of intentionally damaging a protected computer. The defendants are believed to be living in Iran and the Palestinian Authority and are wanted by United States authorities.

"The hackers victimized innocent third parties in a campaign to retaliate for the military action that killed Soleimani, a man behind countless acts of terror against Americans and others that the Iranian regime opposed," said Assistant Attorney General for National Security John C. Demers. "Their misguided, illegal actions in support of a rogue, destabilizing regime will come back to haunt them, as they are now fugitives from justice."

"Foreign hackers are a persistent commercial and national security threat to the United States," said United States

Attorney Andrew E. Lelling. "Working with our law enforcement partners worldwide, we will aggressively pursue, prosecute and apprehend those who use the internet to attack American interests."

"These hackers are accused of orchestrating a brazen cyber-assault that defaced scores of websites across the country as a way of protesting and retaliating against the United States for killing the leader of a foreign terrorist organization. Now, they are wanted by the FBI and are no longer free to travel outside Iran or Palestine without risk of arrest," said Joseph R. Bonavolonta, Special Agent in Charge of the FBI Boston Division. "Today's indictment should send a powerful message that we will not hesitate to go after anyone who commits malicious cyber intrusions against innocent Americans in order to cause chaos, fear, and economic harm."

According to the indictment, Mohammadzadeh has publicly claimed to have personally defaced more than 1,100 websites around the world with pro-Iranian and pro-hacker messages, which he began in 2018 and continues through the present day. Abusrour is a self-described spammer (sender of unsolicited emails for profit), carder (illicit trader in stolen credit cards) and black hat hacker (a hacker who violates computer security for personal gain or maliciousness) who has publicly claimed to have defaced at least 337 websites around the world, which he began no later than June 6, 2016, and continued through at least July 2020.

The defendants allegedly started working together on or about Dec. 26, 2019, when Abusrour began providing Mahammadzadeh with access to compromised websites. On or about Jan. 2, 2020, the U.S. Department of Defense issued a statement that the United States military had "taken decisive defensive action to protect U.S. personnel abroad by killing Qasem Soleimani, the head of the Islamic Revolutionary Guard Corps-Quds Force, a U.S.-designated Foreign Terrorist Organization." The statement explained that the "strike was aimed at deterring future

Iranian attack plans” and described briefly General Soleimani’s past actions and future plans. The United States’ responsibility for General Soleimani’s death was widely publicized.

Following this statement, and in retaliation for it, Mohammadzadeh allegedly transmitted computer code to approximately 51 websites hosted in the United States, and defaced those websites by replacing their content with pictures of the late General Soleimani against a background of the Iranian flag along with the message, in English, “Down with America,” and other text. Some of the websites defaced were hosted on computers owned by a company with corporate headquarters in Massachusetts. No later than Jan. 7, 2020, Abusrour provided Mohammadzadeh with access to at least seven websites, which they defaced with a similar image and text. The defendants took credit online for their website defacements.

The charge of conspiring to commit intentional damage to a protected computer provides for a sentence of up to five years in prison, three years of supervised release and a fine of \$250,000 or twice the gain or loss, whichever is greatest. The charge of intentionally damaging a protected computer provides for a sentence of up to 10 years in prison, three years of supervised release and a fine of \$250,000 or twice the gain or loss, whichever is greatest. Sentences are imposed by a federal district court judge based upon the U.S. Sentencing Guidelines and other statutory factors.

Assistant Attorney General for National Security John C. Demers; United States Attorney Andrew E. Lelling; and Joseph R. Bonavolonta, Special Agent in Charge of the Federal Bureau of Investigation, Boston Field Division made this announcement. Assistant U.S. Attorney Scott L. Garland, Deputy Chief of Lelling’s National Security Unit, and Assistant U.S. Attorney David J. D’Addio of Lelling’s Securities, Financial & Cyber Fraud Unit are prosecuting this case with the assistance

of Cyber Counsel Ali Ahmad of the National Security Division's Counterintelligence and Export Control Section.

The details contained in the charging documents are allegations. The defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.