

Iranians indicted in Atlanta city government ransomware attack

Enlarge / The message posted to social media by the city of Atlanta in the wake of an apparent ransomware attack.

City of Atlanta

reader comments

6 with 6 posters participating

Share this story

The US Attorney's Office for the District of Northern Georgia announced today that a federal grand jury had returned indictments against two Iranian nationals charged with executing the March 2018 ransomware attack that paralyzed Atlanta city government services for over a week. Faramarz Shahi Savandi and Mohammed Mehdi Shah Mansouri are accused of using the Samsam ransomware to encrypt files on 3,789 City of Atlanta computers, including servers and workstations, in an attempt to extort Bitcoin from Atlanta officials.

Details leaked by City of Atlanta employees during the ransomware attack, including screenshots of the demand message posted on city computers, indicated that Samsam-based malware was used. A Samsam variant was used in a number of ransomware attacks on hospitals in 2016, with attackers using vulnerable Java Web services to gain entry in several cases. In more recent attacks, including one on the health industry companies Hancock Health and Allscripts, other methods were used to gain access, including Remote Desktop Protocol hacks that gave the

attackers direct access to Windows systems on the victims' networks.

The Atlanta attack was not a targeted state-sponsored attack. The attackers likely chose Atlanta based on a vulnerability scan. According to the indictment, the attackers offered the city the option of paying six Bitcoin (currently the equivalent of \$22,500) to get keys to unlock all the affected systems or 0.8 Bitcoin (about \$3,000) for individual systems. "The ransom note directed the City of Atlanta to a particular Bitcoin address to pay the ransom and supplied a web domain that was only accessible using a Tor browser," a Department of Justice spokesperson said in a statement. "The note suggested that the City of Atlanta could download the decryption key from that website." But within days of the attack, the Tor page became unreachable, and the City of Atlanta did not pay the ransom.

Savandi, 27, of Shiraz, Iran, and Mansouri, 34, of Qom, Iran, have been charged under the Computer Fraud and Abuse Act (CFAA) for "intentional damage to protected computers... that caused losses exceeding \$5,000, affected more than 10 protected computers, and that threatened the public health and safety," the Justice Department spokesperson said. They are also charged in a separate indictment in the US District Court for the District of New Jersey in connection with another ransomware attack, in which a ransom was apparently paid.

<https://arstechnica.com/?p=1423681>