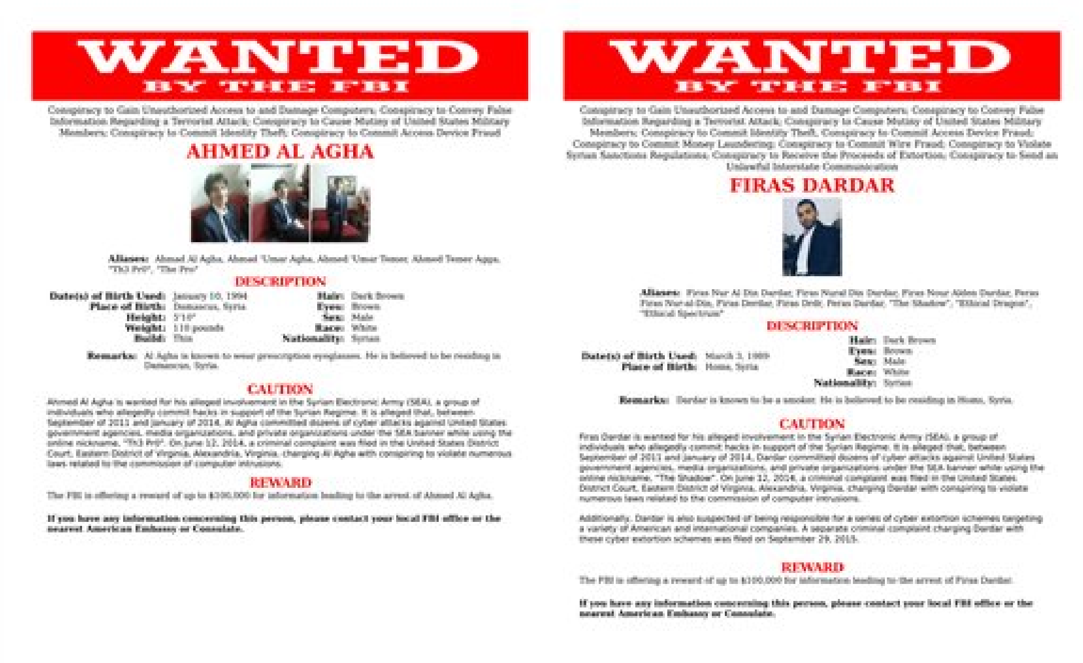
US charges 3 it ties to Syrian Electronic Army for hacking (Update)

March 22 2016, by Tami Abdollah



WANTED
BY THE FBI

Conspiracy to Gain Unauthorized Access to and Damage Computers; Conspiracy to Convey False Information Regarding a Terrorist Attack; Conspiracy to Cause Mutiny of United States Military Members; Conspiracy to Commit Identity Theft; Conspiracy to Commit Access Device Fraud

AHMED AL AGHA

Aliases: Ahmad Al Agha, Ahmad 'Umar Agha, Ahmed 'Umar Temer, Ahmed Temer Agga, "Th3 Pr0", "The Pro"

DESCRIPTION

Date(s) of Birth Used: January 10, 1994 **Hair:** Dark Brown
Place of Birth: Damascus, Syria **Eyes:** Brown
Height: 5'10" **Sex:** Male
Weight: 110 pounds **Race:** White
Build: Thin **Nationality:** Syrian

Remarks: Al Agha is known to wear prescription eyeglasses. He is believed to be residing in Damascus, Syria.

CAUTION

Ahmed Al Agha is wanted for his alleged involvement in the Syrian Electronic Army (SEA), a group of individuals who allegedly commit hacks in support of the Syrian Regime. It is alleged that, between September of 2011 and January of 2014, Al Agha committed dozens of cyber attacks against United States government agencies, media organizations, and private organizations under the SEA banner while using the online nickname, "Th3 Pr0". On June 12, 2014, a criminal complaint was filed in the United States District Court, Eastern District of Virginia, Alexandria, Virginia, charging Al Agha with conspiring to violate numerous laws related to the commission of computer intrusions.

REWARD

The FBI is offering a reward of up to $100,000 for information leading to the arrest of Ahmed Al Agha.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

WANTED
BY THE FBI

Conspiracy to Gain Unauthorized Access to and Damage Computers; Conspiracy to Convey False Information Regarding a Terrorist Attack; Conspiracy to Cause Mutiny of United States Military Members; Conspiracy to Commit Identity Theft; Conspiracy to Commit Access Device Fraud; Conspiracy to Commit Money Laundering; Conspiracy to Commit Wire Fraud; Conspiracy to Violate Syrian Sanctions Regulations; Conspiracy to Receive the Proceeds of Extortion; Conspiracy to Send an Unlawful Interstate Communication

FIRAS DARDAR

Aliases: Firas Nur Al Din Dardar, Firas Nural Din Dardar, Firas Nour Aldeen Dardar, Feras Firas Nur-al-Din, Firas Derdar, Firas Drdr, Feras Dardar, "The Shadow", "Ethical Dragon", "Ethical Spectrum"

DESCRIPTION

Hair: Dark Brown
Eyes: Brown
Date(s) of Birth Used: March 3, 1989 **Sex:** Male
Place of Birth: Homs, Syria **Race:** White
Nationality: Syrian

Remarks: Dardar is known to be a smoker. He is believed to be residing in Homs, Syria.

CAUTION

Firas Dardar is wanted for his alleged involvement in the Syrian Electronic Army (SEA), a group of individuals who allegedly commit hacks in support of the Syrian Regime. It is alleged that, between September of 2011 and January of 2014, Dardar committed dozens of cyber attacks against United States government agencies, media organizations, and private organizations under the SEA banner while using the online nickname, "The Shadow". On June 12, 2014, a criminal complaint was filed in the United States District Court, Eastern District of Virginia, Alexandria, Virginia, charging Dardar with conspiring to violate numerous laws related to the commission of computer intrusions.

Additionally, Dardar is also suspected of being responsible for a series of cyber extortion schemes targeting a variety of American and international companies. A separate criminal complaint charging Dardar with these cyber extortion schemes was filed on September 29, 2015.

REWARD

The FBI is offering a reward of up to $100,000 for information leading to the arrest of Firas Dardar.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

This two-picture combo of wanted posters provided by the FBI shows Ahmed al-Agha, left, and Firas Dardar. The Justice Department has indicted current or former members of the Syrian Electronic Army for computer hacking-related conspiracies. Prosecutors allege that 22-year-old Agha and 27-year-old Dardar used spear-phishing to steal usernames and passwords to compromise government, media, and private-sector computer systems. FBI via AP)

Three current or former members of the so-called Syrian Electronic Army have been charged with computer hacking-related conspiracies that targeted the U.S. government, media and private-sector companies, the Justice Department announced Tuesday.

The criminal charges against three Syrians were unsealed in U.S. Eastern District Court of Virginia. None are in custody.

Prosecutors allege that Ahmad Umar Agha, 22, and Firas Dardar, 27, tricked email users into revealing their usernames and passwords to compromise domestic and international computer systems from 2011 through 2014. They used a common technique known as spear-phishing, in which they forged convincing-looking emails baiting the recipient to click on an included link and reveal their passwords.

The government said Agha, known online as "Th3 Pr0," and Dardar, known as "The Shadow," are members of the special operations division of the Syrian Electronic Army, a group of hackers responsible for computer intrusions intended to punish perceived detractors of Syrian President Bashar al-Assad and publish pro-Assad propaganda.

A $100,000 reward is being offered for information leading to their arrests and they're believed to be in Syria.

In April 2013, they allegedly sent a tweet from the Associated Press account on Twitter falsely claiming a bomb had exploded at the White House and injured the president. The message caused the stock market to dip significantly before the tweet was quickly determined to be a hoax.

They allegedly altered Harvard University's website home page, substituting an image of Syrian President Bashar al-Assad, with a message saying "Syrian Electronic Army were Here."

They are accused of creating a false online post on the Washington Post;

unsuccessfully targeting members of the Executive Office of the President; defacing a blog and Twitter account belonging to Microsoft; sending false news tweets from Reuters' Twitter account and posting a false report on a journalist's blog; and posting messages on Human Rights Watch criticizing its own reports on Syria as "false."

Other media the two allegedly compromised in spear-phishing efforts include National Public Radio, CNN, The Onion, E! Online, the Daily Dot, New York Post, Time magazine and Vice. They also allegedly managed to take down the New York Times website after compromising its technology vendor.

They also allegedly redirected the U.S. Marine Corps recruiting website to an online page controlled by them encouraging marines to "refuse your orders" and inviting them to fight alongside the Syrian Army and attempted to access NASA's network.

Pierre Romar, 36, was also charged separately for his role in an extortion hacking scheme from 2013 through 2014. He was believed to be in Germany.

Romar allegedly was inspired by the hacking activities perpetrated by Agha and Dardar and wanted to join the Syrian Electronic Army, reaching out to Agha for help with a cyberattack he was planning against targets in Sauidi Arabia, Turkey and Qatar. According to the complaint, Agha connected him with Dardar on Facebook and the two worked together on an extortion scheme targeting U.S. and international computers and send victims threats to pay up after gaining access to their system through a spear-phishing attack.

Romar's location, in Germany, helped facilitate transferring the money to Syrian Electronic Army members in Syria because of U.S. sanctions.

John Carlin, the Justice Department's top national security attorney, said the allegations show the "increasingly blurry" line between criminal hackers and "potential national security threats."

Dardar allegedly demanded more than a total of $500,000 from 14 victims but ultimately accepted smaller amounts in many circumstances. Victims included an online gaming company, an online entertainment service, a Swiss web hosting provider, a United Kingdom-based web hosting company, a Europe-based web hosting company, a California-based web hosting company. In the last case, the company and some of its clients' Internet traffic was redirected to a site that said they had been hacked, alleged to have downloaded all their data and threatened to sell the databases for $100 to other hackers if it failed to comply.

The California-based company, which was not identified, ultimately paid about $1,500 to "Peter Romar in Germany" through Western Union after their bank denied the transfer to Syria—despite an initial demand of 105,000 euros.

Citation: US charges 3 it ties to Syrian Electronic Army for hacking (Update) (2016, March 22) retrieved 26 June 2024 from https://phys.org/news/2016-03-ties-syrian-electronic-army-hacking.html