Department of Justice

U.S. Attorney's Office

Eastern District of Virginia

FOR IMMEDIATE RELEASE

Tuesday, March 22, 2016

Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army

ALEXANDRIA, Va. – Three Syrian nationals, all current or former members of the Syrian Electronic Army (SEA), were charged with multiple conspiracies related to computer hacking, according to two criminal complaints unsealed today here in the U.S. District Court of the Eastern District of Virginia.

Ahmad Umar Agha, 22, known online as "The Pro," and Firas Dardar, 27, known online as "The Shadow," were charged with a criminal conspiracy relating to: engaging in a hoax regarding a terrorist attack; attempting to cause mutiny of the U.S. armed forces; illicit possession of authentication features; access device fraud; unauthorized access to, and damage of, computers; and unlawful access to stored communications. Dardar and Peter Romar, 36, also known as Pierre Romar, were separately charged with multiple conspiracies relating to: unauthorized access to, and damage of, computers and related extortionate activities; receiving the proceeds of extortion; money laundering; wire fraud; violations of the Syrian Sanctions Regulations; and unlawful interstate communications. The court has issued arrest warrants for all three defendants.

"The tireless efforts of U.S. prosecutors and our investigative partners have allowed us to identify individuals who have been responsible for inflicting damage on U.S. government and private entities through computer intrusions," said U.S. Attorney Boente. "Today's announcement demonstrates that we will continue to pursue these individuals no matter where they are in the world."

According to allegations in the first complaint, beginning in or around 2011, Agha and Dardar engaged in a multi-year criminal conspiracy under the name "Syrian Electronic Army" in support of the Syrian Government and President Bashar al-Assad. The conspiracy was dedicated to spear-phishing and compromising the computer systems of the U.S. government, as well as international organizations, media organizations and other private-sector entities that the SEA deemed as having been antagonistic toward the Syrian Government. When the conspiracy's spear-phishing efforts were successful, Agha and Dardar would allegedly use stolen usernames and passwords to deface websites, redirect domains to sites controlled or utilized by the conspiracy, steal email and hijack social media accounts. For example, starting in 2011, the conspirators repeatedly targeted computer systems and employees of the Executive Office of the President. Despite these

efforts, at no time was an EOP account or computer system successfully compromised. Additionally, in April 2013, a member of the conspiracy compromised the Twitter account of a prominent media organization and released a tweet claiming that a bomb had exploded at the White House and injured the President. In a later 2013 intrusion, through a third-party vendor, the conspirators gained control over a recruiting website for the U.S. Marine Corps and posted a defacement encouraging U.S. marines to "refuse [their] orders."

"The Syrian Electronic Army publicly claims that its hacking activities are conducted in support of the embattled regime of Syrian President Bashar al-Assad," said Assistant Attorney General Carlin. "While some of the activity sought to harm the economic and national security of the United States in the name of Syria, these detailed allegations reveal that the members also used extortion to try to line their own pockets at the expense of law-abiding people all over the world. The allegations in the complaint demonstrate that the line between ordinary criminal hackers and potential national security threats is increasingly blurry."

Today, the FBI announced that it is adding Agha and Dardar to its Cyber Most Wanted and offering a reward of $100,000 for information that leads to their arrest. Both individuals are believed to be residing in Syria. Anyone with information is asked to contact their nearest FBI field office or U.S. Embassy or consulate.

"Cybercriminals cause significant damage and disruption around the world, often under the veil of anonymity," said Assistant Director Trainor. "As this case shows, we will continue to work closely with our partners to identify these individuals and bring them to justice, regardless of where they are."

According to allegations in the second complaint, beginning in or around 2013, SEA members Dardar and Romar engaged in multiple conspiracies dedicated to an extortion scheme that involved hacking online businesses in the United States and elsewhere for personal profit. Specifically, the complaint alleges that the conspiracy would gain unauthorized access to the victims' computers and then threaten to damage computers, delete data or sell stolen data unless the victims provided extortion payments to Dardar and/or Romar. In at least one instance, Dardar attempted to use his affiliation with the SEA to instill fear into his victim. If a victim could not make extortion payments to the conspiracy's Syrian bank accounts due to the Syrian Sanctions Regulations or other international sanctions regulations, Romar would act as an intermediary in an attempt to evade those sanctions.

"These three members of the Syrian Electronic Army targeted and compromised computer systems in order to provide support to the Assad regime as well as for their own personal monetary gain through extortion," said Assistant Director in Charge Abbate. "As a result of a thorough cyber investigation, FBI agents and analysts identified the perpetrators and now continue to work with our domestic and international partners to ensure these individuals face justice in the United States. I want to thank the dedicated FBI personnel, federal prosecutors, and our law enforcement partners for their tremendous efforts to ensure on-line criminal activity is countered, U.S. cyber infrastructure is safeguarded, and violators are held accountable under the law."

Dana J. Boente, U.S. Attorney for the Eastern District of Virginia; John P. Carlin, Assistant Attorney General for National Security; James Trainor, Assistant Director of the FBI's Cyber Division; and Paul M. Abbate, Assistant Director in Charge of the FBI's Washington Field Office, made the announcement after the charges were unsealed.

The case is being investigated by the FBI's Washington Field Office, with assistance from the NASA Office of the Inspector General, Department of State Bureau of Diplomatic Security and other law enforcement agencies. The case is being prosecuted by Assistant U.S. Attorneys Jay V. Prabhu and Maya D. Song of the Eastern District of Virginia, and Special Assistant U.S. Attorney Brandon Van Grack and Trial Attorneys Scott McCulloch and Nathan Charles of the National Security Division's Counterintelligence and Export Control Section.

A copy of this press release may be found on the website of the U.S. Attorney's Office for the Eastern District of Virginia. Related court documents and information may be found on the website of the District Court for the

Eastern District of Virginia or on PACER by searching for **Case Nos. 1:14-mj-292, and 1:14-mj-498.**

Criminal complaints contain allegations that a defendant has committed a crime. Every defendant is presumed to be innocent until and unless proven guilty in court.

Download sea_agha_and_dardar_complaint.pdf
Download sea_romar_and_dardar_complaint.pdf

Department of Justice
USAO - Virginia, Eastern

Updated March 22, 2016