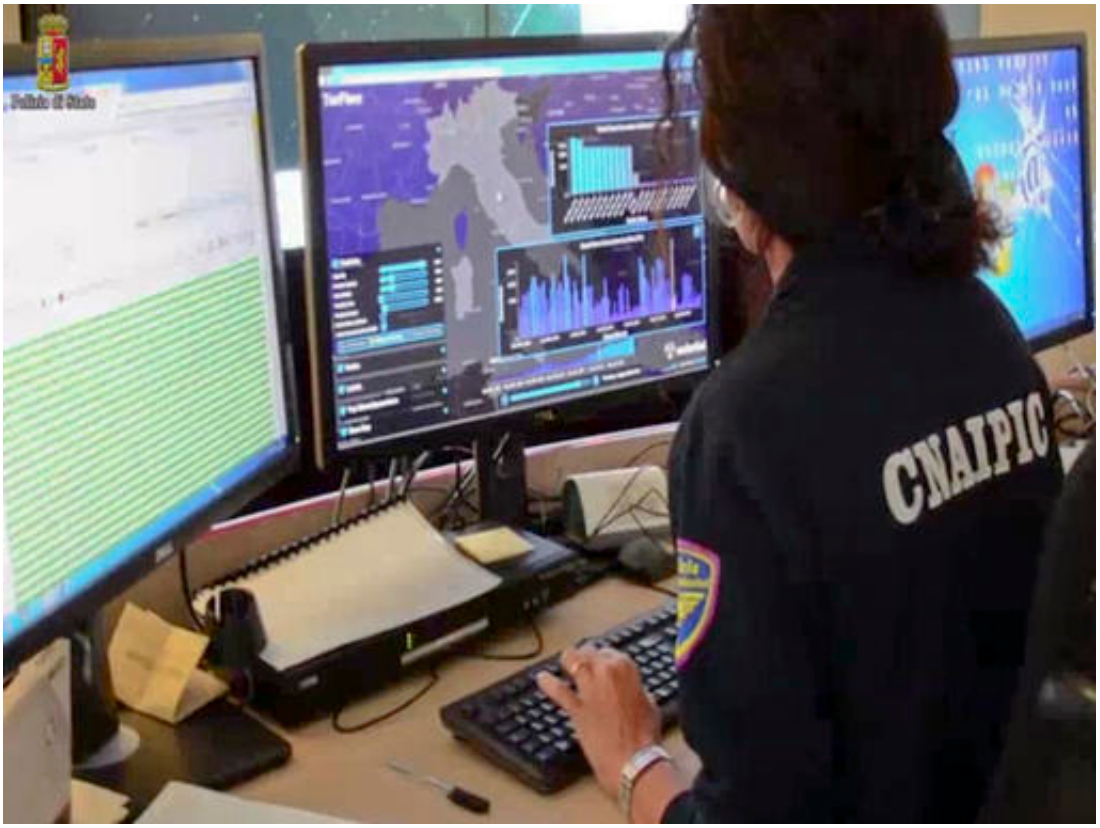
Italy arrests siblings accused of huge VIP hacking campaign (Update)

January 10 2017, by Frances D'emilio And Raphael Satter



This undated image taken from video and made available by the Italian Police on Tuesday, Jan. 10, 2017, shows an officer of Italy's National Anti Cybercrime Center and Critical Infrastructures Protection (CNAIPIC) working at a computer station. Italian police say they have arrested two suspects, a brother-and-sister team, for trying to hack the personal email accounts of leading public figures, including reportedly those of former premier Matteo Renzi and European Central Bank chief Mario Draghi (Polizia di Stato HO via ANSA)

Police have arrested a brother-and-sister team suspected of conducting an ambitious, years-long campaign of hacking that targeted thousands of accounts belonging to some of the leading political and business figures in Italy.

The motive of the sprawling campaign, which carried Masonic overtones, remains a mystery. But those in the crosshairs included Matteo Renzi when he was Italian premier, European Central Bank chief Mario Draghi and much of the cream of Italy's elite.

"In the eight months we have been investigating, we haven't registered any evidence of extortion activity, or attempts to (use hacked data) to obtain influence," Roberto Di Legami, who directs the Italian national police division that specializes in combatting internet and other communications network crimes, told The Associated Press in a telephone interview Tuesday.

Police said Tuesday that it was an assist from the FBI that helped cracked the "cyberespionage headquarters" and led to Monday's arrests of Giulio Occhionero, 45, and his 49-year-old sister Francesca Maria Occhionero. They are being kept in isolation in two different jails in Rome, police said.

The two live in the Italian capital, where they are reportedly well known in the world of high finance. They also have a legal residence in London, where at one point they registered a securities company, Di Legami said.

Prosecutors' requests for the arrest warrants alleged that the duo tried to hack into Renzi's personal email twice in June, when he was still premier, and into Draghi's email account once in June and again in July.

A person familiar with the matter said there was no indication any European Central Bank account was successfully breached. The person

spoke on condition of anonymity due to the sensitive nature of the matter.

Italian police were generous with praise for the FBI's help. Di Legami said the FBI found the servers despite the suspect's use of the online anonymity tool Tor to mask their electronic movements.

The FBI did not return a message seeking comment on the nature of its assistance, confirming only that it had helped with the investigation through the U.S. Embassy in Rome.

All but one of the servers the Occhioneros allegedly used in their scheme were located in the United States, Di Legami said. He added that, until the Americans hand the servers to Italian investigators, it will not be known if any of the hacking attempts succeeded and if so, what data might have been extracted from the targeted accounts.

Police said investigators would be analyzing "an enormous mound of sequestered material" in the United States.

The motive for the hacks was unclear, although lines of code in the software—including the English-language string "Pyramid Eye"—suggest a Masonic connection.

Giulio Occhionero was a high-ranking member of a Masonic lodge, Di Legami said.

An email sent to Giulio Occhionero's personal address was not immediately returned; a LinkedIn message left with Francesca Maria's account also was not returned.

Other prominent Italians whose accounts allegedly were targeted include Fabrizio Saccomanni, a former Italian economy minister who also served

as a top official of Italy's central bank; a Catholic cardinal holding Vatican posts; Mario Monti, an economist who wrestled with Italy's financial crisis as premier from 2011 to 2013; former top officials of the Italian tax police squad; and Italian politicians from across the political spectrum.

This undated image taken from video and made available by the Italian Police on Tuesday, Jan. 10, 2017, shows two police officers working at a computer station. Italian police say they have arrested two suspects, a brother-and-sister team, for trying to hack the personal email accounts of leading public figures, including reportedly those of former premier Matteo Renzi and European Central Bank chief Mario Draghi (Polizia di Stato HO via ANSA)

Politicians expressed relief that a cyber-spy operation had been unmasked and demanded investigators get to the bottom of it.

"Everything must be rapidly cleared up, avoiding news leaks," Debora Serracchiani, a top official with Renzi's Democratic Party, said. "Certainly, a criminal plan has been uncovered upon which many hypotheses can be made."

The alleged hacking operation came to light as Italian politics already are roiled over Renzi's stepping down as premier last month after a referendum defeat and maneuvering ahead of likely early elections that could come this year.

Ignazio La Russa, a right-wing lawmaker who was among the cyber-spies' targets, was quoted by the Italian news agency ANSA as saying that he did not feel anguished about information of his that may have been taken.

"A member of Parliament must be transparent. If they asked me, I would have given them the info gratis," La Russa said.

La Russa added: "I'd be sorry however, if they spied on my private life, entering in the accounts of my wife or children."

Giulio Occhionero co-founded a boutique Roman investment firm named Westlands Securities SpA, according to his LinkedIn profile and a former employee of the company who didn't want to be identified in connection with the investigation.

Di Legami said investigators think the firm might have been set up largely as a cover for criminal activities, although they found evidence Westland Securities provided legitimate financial advising, including for construction at a southern Italian port, and also had some dealings in stocks and bonds.

Giulio Occhionero was the main force in the duo, drawing on his

background as an engineer—he has a degree in nuclear engineering—as well as formidable talent as a quantitative analyst, the police official said.

Francesca Maria Occhionero, whose LinkedIn page shows she served as Westland Securities' managing director, mainly helped with support logistics, Di Legami said.

Di Legami said the investigators' big break came when a security manager at a government office dealing with computer security received an email from a law office he didn't recognize.

Alarmed, the manager asked a security firm to trace the IP address. When the IP address didn't match the one used by the law office, police investigators picked up the trail.

Di Legami said the hackers used sophisticated and complex malware and were able to access their victims' networks for long periods of time, remotely harvesting emails, communications and other documents from targeted computers.

In all, the suspects allegedly obtained some 18,000 usernames and nearly 1,800 passwords.

The suspects created numerous folders to divide up their targets. Among the more creatively named ones was a folder dubbed "Bros" that included persons who supposedly belong to a Masonic lodge and another folder dubbed POBU—for politicians and business—in which various individuals from high-level politics and business were listed.

Investigators moved to have the suspects arrested because of the "concrete danger" they could flee abroad, police said.