NEWS RELEASE

André Birotte Jr.
United States Attorney
Central District of California

Thom Mrozek, Public Affairs Officer
(213) 894-6947
thom.mrozek@usdoj.gov
www.usdoj.gov/usao/cac

For Immediate Distribution

June 22, 2010

ORANGE COUNTY MAN SUSPECTED OF HACKING COMPUTERS ARRESTED ON FEDERAL CHARGES RELATED TO DEMANDS FOR SEXUALLY EXPLICIT VIDEOS FROM WOMEN AND TEENAGE GIRLS

LOS ANGELES – A man who claims to be affiliated with an underground gang of hackers was arrested today on federal extortion charges that allege he hacked into dozens of computers, obtained personal data about people using the computers, and then demanded sexually explicit videos from female victims in exchange for keeping their personal information private.

Luis Mijangos, 31, of Santa Ana, California, was arrested without incident at his residence by special agents with the Federal Bureau of Investigation.

The arrest of Mijangos, which was pursuant to a criminal complaint filed last week in United States District Court, follows a six-month FBI investigation into his involvement in computer hacking, identity theft and video voyeurism. FBI computer forensics experts have determined Mijangos infected more than 100 computers that were used by approximately 230 individuals, at least 44 of whom were juveniles.

The federal investigation into Mijangos resulted from a referral from the Glendale Police Department, which received a complaint from a victim and realized the matter involved a number of victims and may be the work of a sophisticated computer hacker.

“This case is another example of local police and FBI agents collaborating to solve a crime,” said FBI Assistant Director in Charge, Steven M. Martinez. “The investigation leading to the extensive network of victims in this case and culminating with today’s arrest of Mr. Mijangos would not have been possible without information

provided by the Glendale Police Department, whose detectives worked this investigation jointly with FBI agents. Mr. Mijangos is alleged to have exploited new technology to exert control over young women whom he extorted, and many who were unwitting victims."

The affidavit in support of the complaint outlines a series of schemes that all involve Mijangos using peer-to-peer networks to infect computers around the world with malicious computer code. Mijangos induced victims to download the malware onto their computers by making the files appear to be popular songs. After the victims downloaded the malware, Mijangos was able to control their computers, allowing him to send instant messages containing malware from those computers to other people in the victims' address books. These later victims thought they were receiving messages from friends or family members.

Mijangos infected victim computers for a variety of purposes, according to the complaint, that outlines several lines of criminal conduct.

Once he had control of a computer, Mijangos searched for sexually explicit or intimate images and videos of women, typically young women and girls in various states of undress or engaged in sexual acts with their partners. Mijangos contacted the female victims, informing them that he was in possession of intimate images and videos and threatening to distribute those stolen images and videos to every addressee in the victims' contact lists unless they made additional videos for him. Mijangos also told his victims that, because he controlled their computers, he would know if they attempted to contact the authorities, and he threatened to retaliate against them by releasing the images and videos if they called the police. According to the affidavit, Mijangos told one victim that she did not want to "mess" with a team of hackers.

Mijangos also installed a "keylogger" on victims' computers that allowed him to record every key that was struck on the keyboards of the infected computers. Because the users of those compromised computers were unaware that their computers had been infected, they continued to use their computers to engage in commercial and social activities. Mijangos used the keylogger to steal credit card numbers and personal identifying information that he used to engage in identity theft and to purchase merchandise, the affidavit states.

Mijangos also used stolen usernames and passwords to access victims' email and social networking sites to further his extortion scheme. After hacking email accounts belonging to victims' boyfriends, Mijangos contacted women and teenage girls and, pretending to be their boyfriends, asked them to create pornographic videos for him. Once he had those videos, Mijangos again contacted the victims, this time using an alias, to demand more pornographic videos under threats of distributing the videos previously sent to him.

With his control of the victims' computers and all of their functions, Mijangos was able to remotely access victims' webcams and to turn them on from time to time in an attempt to catch the victims in intimate situations. Occasionally he was successful.

During the execution of a search warrant at his residence, Mijangos was interviewed by FBI agents. According to the affidavit, Mijangos acknowledged that he hacked into computers, but claimed that he did so at the request of boyfriends and husbands who sought to determine whether the women were cheating on them. Mijangos acknowledged that he asked for additional sexual videos but only to determine whether the women would actually do it. Mijangos also admitted his involvement with an international network of hackers and his participation in credit card fraud.

Mijangos is expected to make his initial court appearance this afternoon in United States District Court in downtown Los Angeles.

The criminal complaint charges Mijangos with extortion, a felony offense that carries a statutory maximum penalty of two years in federal prison.

A criminal complaint contains allegations that a defendant has committed a crime. Every defendant is presumed to be innocent until proven guilty.

This case was investigated by the Federal Bureau of Investigation and the Glendale Police Department.

CONTACT: Assistant United States Attorney Mark C. Krause
Cybercrime and Intellectual Property Section
(213) 894-3493

Release No. 10-076