ORIGINAL FILED

JUN 6 2006

MADELINE COX ARLEO
U.S. MAG. JUDGE

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**CRIMINAL COMPLAINT**
-v-	:	Mag. No. 06-8093 (MCA)
EDWIN ANDRES PENA, a/k/a "David Hauster," a/k/a "Renato Moreno," a/k/a "e_andres55"	:	

I, Barbara Farrington, being duly sworn, state the following is true and correct to the best of my knowledge and belief. From in or about November 2004 to in or about May 2006, in Essex County, in the District of New Jersey and elsewhere, defendant EDWIN ANDRES PENA did:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached page and made a part hereof.

Barbara Farrington, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
June 6, 2006, in Essex County, New Jersey

HONORABLE MADELINE COX ARLEO
UNITED STATES MAGISTRATE JUDGE

Madeline Cox Arleo
Signature of Judicial Officer

ATTACHMENT A

COUNT 1

On or about July 25, 2005, in Essex County in the District of New Jersey and elsewhere, defendant

EDWIN ANDRES PENA

for the purpose of executing and attempting to execute a scheme and artifice to defraud and to obtain money and property from N.T.P., a Newark, New Jersey voice over internet protocol telephone service provider by means of materially false and fraudulent pretenses, representations, and promises, did knowingly and willfully cause writings, signs, signals, pictures, and sounds to be transmitted by means of wire communications in interstate commerce, in that he caused the electronic transfer of a customer's voice over internet protocol telephone call to be routed over the internet from a computer network router of O.H., located in or around Ryebrook, New York, to a computer network of N.T.P., located in or around Newark, New Jersey, without authorization, for the purpose of sending the call over N.T.P.'s calling network.

In violation of Title 18, United States Code, Sections 1343 and 2.

COUNT 2

On or about July 25, 2005, in Essex County in the District of New Jersey and elsewhere, defendant

EDWIN ANDRES PENA

did knowingly and with intent to defraud, access a protected computer of N.T.P., a Newark, New Jersey voice over internet protocol telephone service provider, without authorization, and exceeded authorized access, in that he caused a voice over internet protocol telephone call of a customer to be routed over the computer network of N.T.P., located in or around Newark, New Jersey, without the authorization of N.T.P.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 2.

ATTACHMENT B

I, Barbara Farrington, a Special Agent of the Federal Bureau of Investigation, have knowledge of the following facts based upon (a) an analysis of subpoenaed records; (b) information obtained via pen register and trap and trace orders; (c) information obtained from the execution of search warrants; (d) information obtained through surveillance; and (e) discussions with witnesses and other law enforcement agents. Since this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a complaint and arrest warrant, I have not included each and every fact known by the government concerning this investigation.

BACKGROUND

1. At various times relevant to this complaint:

a. **Edwin Andres Pena**: The Defendant, Edwin Andres Pena ("Defendant Pena"), was a citizen of Venezuela, and resided in Miami, Florida as a permanent resident alien. Defendant Pena held himself out as a telecommunications security expert, capable of identifying and addressing security vulnerabilities of computer networks of United States telecommunications businesses. Defendant Pena also controlled and operated two telecommunications companies known as Fortes Telecom, Inc. ("Fortes Telecom") and Miami Tech & Consulting, Inc. ("Miami Tech") out of two residences located in Miami. When transacting business on behalf of Fortes Telecom and Miami Tech, Defendant Pena communicated via e-mail, using the address "e_andres55@hotmail.com" ("Defendant Pena's E-Mail Address").

b. **Fortes Telecom Inc.**: Fortes Telecom, incorporated in the State of Florida on or about September 14, 2004, purported to be a legitimate wholesale provider of voice over internet protocol ("VOIP") telephone call service. Through Fortes Telecom, Defendant Pena offered and sold millions of minutes of VOIP telephone call service to various telecommunications companies with whom he contracted at steeply discounted below market rates.

c. **Miami Tech & Consulting, Inc.**: Miami Tech, incorporated in the State of Florida on or about September 27, 2005, purported to be in the business of providing VOIP auditing and security consulting. According to its web-site, http://www.miamitac.com, Miami Tech provides "VOIP Security Auditing." Defendant Pena also used Miami Tech to contract with various telecommunications companies for the sale of millions of minutes of VOIP telephone call service at steeply discounted below market rates.

d. **O.H.:** A hedge fund identified as O.H., with offices located in or around Ryebrook, New York, had a network router that was connected to the internet. Defendant Pena hacked O.H.'s router so that his customers' VOIP calls could be sent through it to disguise the origin of the calls, making it appear as if O.H. had initiated the calling traffic. From the O.H. router, Defendant Pena then directed the calls, without authorization, to the calling networks of legitimate VOIP telephone service providers, including N.T.P.

e. **N.T.P.**: A VOIP telephone service provider identified as N.T.P., with offices located in or around Newark, New Jersey, accepted VOIP telephone calls from other telecommunications businesses and transmitted those calls to the intended recipients' local telephone carriers. Defendant Pena used N.T.P.'s networks, without authorization, to transmit his customers' calls. N.T.P. was subsequently billed for the call traffic that appeared to be generated by O.H.

f. **VOICE OVER INTERNET PROTOCOL**:

i. The majority of today's telephone calls are transmitted through the public switched telephone network (the "PSTN"). Originally, the PSTN was an international telephone system based on copper wires carrying analog voice data. Today, the PSTN is almost entirely digital and handles fixed, as well as mobile, telephone calling traffic.

ii. A growing sector of telephone calls is now transmitted using a method other than the PSTN. Voice over internet protocol, or VOIP, is the routing of voice telephone calls over the internet or other internet protocol based networks.

THE SCHEME TO DEFRAUD

2. From at least as early as in or around November 2004, to in or around May 2006, in Essex County, in the District of New Jersey, and elsewhere, Defendant Pena did knowingly and willfully devise and intend to devise a scheme and artifice defraud N.T.P, and other VOIP telephone service providers.

3. Beginning at least as early as November 2004, Defendant Pena solicited telecommunications companies to enter into contracts with Fortes Telecom and, subsequently, Miami Tech for the wholesale purchase of VOIP telephone service minutes at discounted rates, sometimes as low as four tenths of a cent per minute (the "Telecom Customers"). The contracts provided that Defendant Pena's businesses were to be paid for what amounted to a significant volume of minutes of VOIP telephone traffic purportedly traveling over legitimate calling routes. Through these contracts with the Telecom Customers, Defendant Pena sold more than 10 million minutes of VOIP telephone service.

4. Between in or about November 2004, and in or about May 2006, unbeknownst to the Telecom Customers, rather than purchase VOIP telephone routes for resale, Defendant Pena created what amounted to "free" routes by surreptitiously hacking into the computer networks of unwitting legitimate VOIP telephone service providers (the "VOIP Telecom Providers") and routing the Telecom Customers' calls in such a way so as to avoid detection.

Avoiding Detection: Hacking Computers of Intermediaries, Establishing Decoy Servers, and Using IP Eliminator

5. In order to avoid detection when establishing the "free" calling routes, Defendant Pena recruited at least one professional computer hacker located in or around Spokane, Washington (the "Spokane Hacker") who was using a high-speed internet account registered to an individual bearing the initials R.G. The Spokane Hacker performed an exhaustive scan of computer networks of unsuspecting companies and other entities in the United States and around the world, searching for vulnerable ports to infiltrate their computer networks (the "Unsuspecting Intermediaries"). According to records obtained from AT&T, between in or about June 2005 and in or about October 2005, for example, more than 6 million scans were initiated by the Spokane Hacker in search of vulnerable Unsuspecting Intermediaries' network ports. During the same period, AT&T records reveal only two users with a greater number of scans on its entire global network.

6. After vulnerable computer networks of Unsuspecting Intermediaries were identified, the Spokane Hacker delivered to Defendant Pena's E-Mail Address information pertaining to the types of routers used, as well as corresponding usernames and passwords, necessary to infiltrate their networks.

7. After receiving the information from the Spokane Hacker, Defendant Pena reprogrammed the Unsuspecting Intermediaries' networks and hardware to accept VOIP telephone call traffic. He then routed the VOIP calls of his Telecom Customers over the Unsuspecting Intermediaries' networks. In this manner, Defendant Pena made it appear to the VOIP Telecom Providers that the calls were coming from the Unsuspecting Intermediaries' networks.

8. Defendant Pena also used other methods to avoid detection. On or about August 28, 2005, providing the name "David Hauster," Defendant Pena arranged to use a computer server hosted at FDCServers, a computer server provider located in or around Chicago, Illinois (the "Chicago Decoy Server"). In order to conceal his connection to the Chicago Decoy Server, Defendant Pena also set up the e-mail address david.haust@gmail.com to communicate with FDCServers, and paid FDCServers via money orders so as to obscure the source of the funds. After establishing the Chicago Decoy Server, Defendant Pena routed VOIP calling traffic of his Telecom Customers through it, thereby further misleading the VOIP Telecom Providers concerning the origin of the calls.

9. In similar fashion, in or about June 2005, Defendant Pena arranged to establish at least one additional server in the name of "Renato Moreno" at Netsonic, a computer server provider located in or around Green Bay, Wisconsin (this server and the Chicago Decoy Server collectively, the "Decoy Servers").

10. Defendant Pena also attempted to avoid detection by subscribing to a service known as IP Eliminator. On or about July 7, 2005, Defendant Pena subscribed to, and paid for, the IP Eliminator service, which conceals identifying data corresponding to the location of a particular computer used to connect to the internet.

Sending the Calls: Hacking into VOIP Telecom Provider Networks

11. Through a practice known as a "Brute Force" attack, Defendant Pena and others working with him acquired the proprietary codes established by VOIP Telecom Providers to identify and accept authorized calls entering into their networks for routing. These codes, known as "prefixes,"are part of the call data that must be transmitted with each VOIP telephone call.

12. Defendant Pena executed a "Brute Force" attack by flooding VOIP Telecom Providers with a multitude of test calls, each carrying a different prefix. The "Brute Force" attack progressed by continuously cycling through a volume of possible prefixes until a proprietary prefix match was identified and a test call sent by Defendant Pena succeeded in penetrating the corresponding network. For example, in or about April 2006, computer logs reveal that Defendant Pena performed a "Brute Force" attack against the networks of GTT, a VOIP Telecom Provider located in or around Miami, Florida.

13. Having penetrated the networks of VOIP Telecom Providers, Defendant Pena

programmed the Unsuspecting Intermediaries' networks, as well as Decoy Servers, to insert the illegally obtained proprietary prefix into calls of the Telecom Customers of Fortes Telecom and Miami Tech for routing.

14. By sending calls to the VOIP Telecom Providers through the Unsuspecting Intermediaries' networks and/or the Decoy Servers, the VOIP Telecom Providers were unable to identify the true sender of the calls for billing purposes. Consequently, individual VOIP Telecom Providers incurred aggregate routing costs of up to approximately $300,000 per provider, without being able to identify and bill Defendant Pena, Fortes Telecom or Miami Tech.

Hacking O.H. and N.T.P. to Route Calls

15. In or about May 2005, Defendant Pena hacked into the external router of O.H., one of the Unsuspecting Intermediaries. Defendant Pena then reprogrammed the router to accept VOIP telephone calls and direct them to the VOIP Telecom Providers that he had previously infiltrated. According to evidence obtained during the investigation, over fifteen VOIP Telecom Companies were programmed to receive the calls sent through the O.H. router. One such VOIP Telecom Provider was N.T.P.

16. Between on or about July 10, 2005 and on or about July 25, 2005, Defendant Pena caused his Telecom Customers' VOIP telephone calls to be transmitted via the internet through routers operated by O.H., located in or around Ryebrook, New York, to N.T.P., located in or around Newark, New Jersey. Records provided by N.T.P. demonstrate that Defendant Pena obtained, without authorization, the valid proprietary prefix that N.T.P. used to identify authorized calls. With an identified N.T.P. proprietary prefix and the hacked O.H. router, in the approximately three-week period Defendant Pena was able to send approximately 500,000 calls through N.T.P.'s VOIP telephone network, making it appear as if O.H. was sending the calls.

Concealing Profits from Scheme

17. As a result of Defendant Pena not having to pay N.T.P. or the other VOIP Telecom Providers through which he routed calls, the revenue he generated from his Telecom Customers was virtually all profit. In an effort to conceal the profit he derived from the scheme, Defendant Pena directed that his Telecom Customers wire transfer payments to a number of different bank accounts held in various names and subsequently depleted the accounts in short order after the payments were received.

18. Between in or about November 2004, and in or about May 2006, six identified accounts maintained at Bank of America and Atlantic Bank received more than $1 million in proceeds from Defendant Pena's Telecom Customers. Typically, within weeks from when the Telecom Customers' payments were received via wire transfer, the funds were withdrawn in the form of cash. In some instances during this period, Defendant Pena also directed that payments be made out of the bank accounts to finance the purchase of assets in the name of another

individual, identified as A.G. Assets purchased in the name of A.G. included residential real estate located in or around Miami, Florida; a forty-foot Sea Ray Mercruiser Model 300DA260 motor boat; and luxury automobiles, including a 2004 BMW M3 automobile, a 2005 BMW 325 automobile, and a 2005 Cadillac Escalade EXT sport utility vehicle.