el/2012R00672

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 12-
	:	
WOLFGANG UELPENICH	:	18 U.S.C. §§ 371
	:	
	:	INFORMATION
	:	
	:	

The defendant having waived in open court prosecution by indictment, the United States Attorney for the District of New Jersey charges:

CONSPIRACY TO GAIN UNAUTHORIZED ACCESS TO PROTECTED COMPUTERS (18 U.S.C. § 371)

BACKGROUND

1. At all times relevant to this Information:

Defendants

a. Defendant Wolfgang Uelpenich was a citizen of Germany who resided in Switzerland. Uelpenich operated WU-Solutions of Cologne, Germany ("WU-Solutions") and Avant Telecom Consulting of Zurich, Switzerland ("Avant"), both of which advertised themselves on the Internet as telecommunications companies.

b. Co-Conspirator Noor Aziz, a/k/a "Noor Aziz Uddin," a/k/a "Noor Aziz Aziz Uddin," a/k/a "Aziz Uddin," was a Pakistani national who resided in Saudi Arabia and operated LinkedTel, a business purporting to provide premium telephone services.

c. Co-Conspirator Farhan Arshad was a citizen of Pakistan and served as Aziz's business manager.

d. CC1, a coconspirator who is not charged as a defendant herein, operated a purported telecommunications provider with operations in New Castle, Delaware.

e. CC2, a coconspirator who is not charged as a defendant herein, resided in the Philippines and worked for Defendant AZIZ.

Other Entities

f. AT&T was an international telephone company with headquarters in Dallas, Texas and major operating centers and a fraud detection center located in Somerset County and Middlesex County, New Jersey, respectively.

Background

g. *PBX Systems*. Large businesses and organizations commonly used private computer systems to operate their internal telephone networks. Such internal telephone networks were referred to as a Private Branch eXchanges, or "PBX." The primary functions of PBX systems included making connections for internal calls placed within the system (i.e., when one employee called another employee) and connecting internal users of the system to public telephone networks, very often for the purpose of making long distance telephone calls which were then charged to the business. PBX systems also directed calls made to a business' main number to the desired extension.

h. *PBX Hacking.* Since approximately 1999, PBX systems of corporations and entities in the United States were compromised by hackers. Hackers involved in such a scheme target the PBX systems of certain corporations and governmental entities and place calls to those

systems in an attempt to identify unassigned telephone extensions at the victim entity. Once an unassigned extension is identified, the hackers use that extension to illegally reprogram the compromised PBX system. In this way, the hackers, and their designees can make unlimited calls, incurring millions of dollars in damages, which are billed to the victim entities that own and operate the hacked PBX systems.

i. *Revenue Share Numbers* ("RSNs") are telephone numbers that connect to services which potentially receive a high volume of incoming calls. A subset of RSNs are known as are as "Premium Numbers" or "international premium numbers," which, when dialed, incur higher rates than typical long distance telephone calls. Premium Numbers often offer such services as adult entertainment, chat lines, and psychic lines on a cost-per-minute basis.

j. *Revenue Share Providers* ("RSPs" or the "Providers") are companies that lease RSNs or Premium Numbers from telephone companies that the Providers use to host high volume call sites. When a person places a call to an RSN or Premium Number, the Provider earns a portion of the per-minute revenue generated by the call. For example, if a Provider named "Provider A" leased a particular telephone number (the "Number") from a telephone company in Austria as a Premium Number, Provider A would receive a percentage of the rate that the Austrian telephone company charged for every minute of calls placed to the Number. As part of the contractual arrangement between telephone companies and the Providers, the telephone companies which lease the Numbers to the Providers receive revenues from the callers' originating telephone company, and then pay the Providers a set rate for each and every minute.

k. *Revenue Share Fraud.* Because the Providers stand to gain from increased call traffic to the RSNs and Premium Numbers that they offer, certain Providers and others have

used hacked PBX systems to generate unauthorized calls to the RSNs and Premium Numbers. The unauthorized calls made by persons or entities, sometimes known as "Dialers" or "Callers," increased call traffic to RSNs and Premium Numbers and generate additional fraudulent revenue for the Providers, Dialers and hackers. A recent telecommunications industry association report estimated $3.84 billion in annual losses attributable to Revenue Share Fraud.

l. *Calling Line Identifier* ("CLI") is a numerical identifier used by telecommunications companies to designate the source of telephone calls. Ordinarily, legitimate Providers of RSNs and Premium Numbers do not know, in advance, the originating CLI for calls to Premium Numbers.

THE CONSPIRACY

2. Between in or about 2010 and in or about January 2012, in the District of New Jersey, and elsewhere, defendant

WOLFGANG UELPENICH

did knowingly and intentionally conspire and agree with Noor Aziz, Farhan Arshad, and others to access protected computers, namely telecommunications systems used in and affecting interstate and foreign commerce and communication, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained things of value, namely telephone service from customers' accounts, contrary to Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A) .

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for Defendant UELPENICH, Aziz and Arshad and others to profit by accepting and generating unauthorized telephone calls to RSNs and Premium Numbers, including through hacked PBX systems, knowing that the telephone companies would not recover the rates for those calls.

MANNER AND MEANS OF THE CONSPIRACY

The Fraudulent Revenue Share Numbers

4. It was part of the conspiracy that Aziz, and Arshad falsely represented to telephone companies that they were providing legitimate Premium Numbers when, in fact, they knew that calls to the Premium Numbers would originate from hacked PBX systems.

5. It was further part of the conspiracy that defendant UELPENICH, Aziz and Arshad, entered into contracts and agreements with Providers and telephone companies for the use of RSNs and Premium Numbers. The contracts contained specific provisions regarding fraudulent activity, including provisions relating to unauthorized telephone calls. Aziz and Arshad signed such contracts and represented that they would meet common carrier industry standards despite knowing that there would be illegitimate calls made to their Premium Numbers. In or around 2010, UELPENICH knew that there would be calls made to the RSNs or Premium Numbers from hacked PBX systems.

6. It was further part of the conspiracy that the Premium Numbers offered by Aziz and Arshad purportedly for premium service frequently were no more than "shell" numbers containing no actual content (*i.e.*, did not have adult entertainment, chat rooms, or psychic lines) and could therefore never generate legitimate fee revenue for the Providers or telephone

companies. In many instances, calls to the RSNs and Premium Numbers resulted in nothing more than recordings of fake rings, fake password prompts, fake voicemail messages, music, or dead air. In some instances, the coconspirators did provide content, in the form of audio files with fake messages directing callers to enter a pin code or other introductory instructions, in order to mimic legitimate Premium Numbers and thereby disguise the fraudulent nature of the Premium Numbers from the telephone companies.

Access to Compromised Systems

7. It was further part of the conspiracy that Aziz negotiated with CC2 and others to use hacked (compromised) PBX systems so that telephone calls could be routed through those systems.

8. It was further part of the conspiracy that Aziz paid CC1, CC2 and the Dialers to generate telephone calls.

9. It was further part of the conspiracy that Aziz and CC1 hired others to obtain cellular telephones through the provision of fraudulent information so calls from those telephones would not be traced to the coconspirators. CC1 and the Dialers then used the cellular telephones as conduits for telephone calls to the RSNs and Premium Numbers.

10. It was further part of the conspiracy that Aziz, Arshad, CC1, CC2, and the Dialers generated telephone calls from hacked PBX systems, and other phones to the RSNs and Premium Numbers controlled by Aziz and Arshad, including, for example, RSNs and Premium Numbers leased from Defendant UELPENICH in Slovenia, Liechtenstein, Austria and elsewhere overseas ("the Stolen Calls").

Avoiding Detection by Using Stolen Identities

11. It was further part of the conspiracy that Aziz, CC2 and others used stolen identities as payment to vendors so as conceal their connection to the payments. The stolen identities consisted of names, credit card numbers, credit card expiration dates, customer verification codes, mother's maiden names, and PIN numbers.

12. It was further part of the conspiracy that Aziz transferred the stolen identity information through international e-mails to CC2 and others.

Accounting the Fraudulent Proceeds

13. It was further part of the conspiracy that Aziz and Arshad, CC1, and the Dialers shared Calling Line Identification ("CLI") numbers for telephones making Stolen Calls, so that CC1 and the Dialers could determine the number of Stolen Calls to RSNs and Premium Numbers attributable to CC1 and the Dialers and the commensurate amount that CC1 and the Dialers should be paid for originating those Stolen Calls.

Profiting from the Scheme

14. It was further part of the conspiracy that Defendant UELPENICH, even before he received payment from overseas telephone companies based on Stolen Calls placed to RSNs would wire Aziz's share of the payments to be received to accounts controlled by Aziz or other accounts designated by Aziz and Arshad.

Overt Acts

Hacked PBX Systems

15. In e-mail correspondence on or about August 24, 2009, Aziz was asked whether he could work with "hacked" calls. Aziz replied "YES, NO PROBLEM" (emphasis in original).

16. Aziz routinely received notice from telecommunications providers that call traffic to his Premium Numbers was generated through hacked PBX systems. For example, on or about August 16, 2010, September 2, 2010, October 30, 2010, April 12, 2011 and May 18, 2011, Aziz received notices from different telecommunications providers that his Premium Numbers were receiving calls from hacked PBX systems.

17. On or about March 27, 2011, after Aziz received a report from a telecommunications provider that calls to his Premium Numbers were being generated from a hacked PBX system, Aziz contacted his Dialer responsible for the calls and instructed him either to conceal that the calls that were coming from a hacked PBX, or stop the calls so the scheme would not be detected. Specifically, Aziz wrote: "[E]ither rotate the CLIs or send [call] traffic by hide CLI or stop further [call] traffic."

Controlling the Dialers

18. Aziz sought to create an appearance of legitimate calls to the Premium Numbers by controlling the Dialers and discussing with them the technical operation such as timing, length of calls and originating numbers:

a. On or about July 18, 2009, Aziz sent CC2 an e-mail asking CC2 to direct the Dialers to alter the type of traffic to avoid detection. Specifically, Aziz wrote: "As all the

traffic on this serail is generated only from one cli, may be carrier raise objection. therefore, please ask callers to send traffic from at least 2 or 3 clis to avoid any objection" (sic).

b. On or about May 7, 2010, CC1 sent Aziz an e-mail explaining that he will "start the traffic in 15 minute[s]." CC1 further asked Aziz to "please let me know how long the call must be and if you like the CLI [so] we can hire."

c. On or about May 28, 2010, Defendant UELPENICH e-mailed Aziz and stated that the issue had been fixed and asked "Can you please inform all dialers to restart?"

d. On or about February 22, 2011, Aziz and Defendant UELPENICH exchanged e-mails in which Aziz stated that he would restrict dialer activity after UELPENICH complained about the amount of activity.

Transmitting Calls Over Hacked PBX Systems

19. On or about the dates listed below, Aziz and Arshad, CC1, CC2, the Dialers, and others, caused unauthorized telephone calls to pass through hacked PBX systems identified below to Premium Numbers controlled by Aziz and Arshad, and generated the loss identified below.

Date	Hacked Entity	Approximate Loss Through AT&T
March 17, 2009	"S.H.", Livingston, New Jersey	$24,140
August 19, 2009	"B.S.P.", Englewood, New Jersey	$83,839
June 23, 2010	Township of Parsippany Troy Hills, Parsippany, New Jersey	$395,752
November 21, 2010	"H.H.C.", New Brunswick, New Jersey	$12,661
December 11, 2010	County of Burlington Board of Freeholders, Mount Holly, New Jersey	$8,065
May 19, 2011	"F.R.P.", Carlstadt, New Jersey	$78,588

In violation of Title 18, United States Code, Section 371.

FORFEITURE ALLEGATION

1. The allegations contained in Count 1 of this Information are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

2. Upon conviction of the offenses in violation of Title 18, United States Code, Section 371 set forth in Count 1 of this Information, defendant

WOLFGANG UELPENICH

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), and Title 28, United States Code 2461(c), any property which constitutes or is derived from proceeds traceable to such violation. If more than one defendant is convicted of an offense, the defendants so convicted are jointly and severally liable for the amount subject to forfeiture under this paragraph.

3. If any of the property described above, as a result of any act or omission of the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

All pursuant to Title 28, United States Code, Section 2461(c).

_____
PAUL J. FISHMAN
UNITED STATES ATTORNEY