SBK/EL/2009R00080

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	
	:	Hon.
	:	
v.	:	Criminal No. 09-
	:	
	:	18 U.S.C. §§ 371 and 1349
ALBERT GONZALEZ,	:	
a/k/a “segvec,”	:	
a/k/a “soupnazi,”	:	
a/k/a “j4guar17,”	:	
HACKER 1, and	:	
HACKER 2	:	

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

COUNT 1
(Conspiracy)
18 U.S.C. § 371

1. At various times relevant to this Indictment:

The Defendants

a. Defendant Albert Gonzalez, a/k/a “segvec,” a/k/a “soupnazi,” a/k/a “j4guar17” (“GONZALEZ”), resided in or near Miami, Florida.

b. Defendant HACKER 1 resided in or near Russia.

c. Defendant HACKER 2 resided in or near Russia.

Coconspirator

d. P.T., a coconspirator who is not charged as a defendant herein, resided in or near Virginia Beach, Virginia and in or near Miami, Florida.

Methods of Hacking Utilized by Defendants

e. Structured Query Language ("SQL") was a computer programming language designed to retrieve and manage data on computer databases.

f. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.

g. "SQL Injection Strings" were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.

h. "Malware" was malicious computer software programmed to, among other things, identify, store, and export information on computers that were hacked, including information such as credit and debit card numbers and corresponding personal identification information of cardholders ("Card Data"), as well as to evade detection by anti-virus programs running on those computers.

The Corporate Victims of Computer Hacking

i. Heartland Payment Systems, Inc. ("Heartland"), which was located in or near Princeton, New Jersey and Plano, Texas, among other places, was one of the world's largest credit and debit card payment processing companies. Heartland processed millions of credit and debit transactions daily. Beginning on or about December 26, 2007, Heartland was the victim of a SQL

Injection Attack on its corporate computer network that resulted in malware being placed on its payment processing system and the theft of more than approximately 130 million credit and debit card numbers and corresponding Card Data.

j. 7-Eleven, Inc. ("7-Eleven") was the corporate parent of a convenience store chain that processed credit and debit card payments through its computer networks. Beginning in or about August 2007, 7-Eleven was the victim of a SQL Injection Attack that resulted in malware being placed on its network and the theft of an undetermined number of credit and debit card numbers and corresponding Card Data.

k. Hannaford Brothers Co. ("Hannaford") was a regional supermarket chain with stores located in Maine, New Hampshire, Vermont, Massachusetts, and New York that processed credit and debit card payments through its computer network. In or about early November 2007, a related company of Hannaford was the victim of a SQL Injection Attack that resulted in the later placement of malware on Hannaford's network and the theft of approximately 4.2 million credit and debit card numbers and corresponding Card Data.

l. Company A was a major national retailer that processed credit card payments through its computer network. Beginning on or about October 23, 2007, Company A was the victim of a SQL Injection Attack that resulted in the placement of

malware on its network.

m. Company B was a major national retailer that processed credit and debit card payments through its computer network. In or about January 2008, Company B was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.

n. Heartland, 7-Eleven, Hannaford, Company A and Company B are collectively referred to herein as the "Corporate Victims."

THE CONSPIRACY

2. Between in or about October 2006 and in or about May 2008, in Mercer and Morris Counties, in the District of New Jersey, and elsewhere, defendants

ALBERT GONZALEZ,
a/k/a "segvec,"
a/k/a "soupnazi,"
a/k/a "j4guar17,"
HACKER 1, and
HACKER 2

did knowingly and intentionally conspire and agree with each other, P.T., and others to commit offenses against the United States, namely:

(a) by means of interstate communications, knowingly and intentionally accessing computers in interstate commerce without authorization, and thereby obtaining information from those computers, namely credit and debit card numbers and corresponding

Card Data, for the purpose of commercial advantage and private financial gain, contrary to Title 18, United States Code, Section 1030(a)(2);

(b) knowingly and with intent to defraud accessing computers in interstate commerce and exceeding authorized access to such computers, and by means of such conduct furthering the intended fraud and obtaining anything of value, namely credit and debit card numbers and corresponding Card Data, contrary to Title 18, United States Code, Section 1030(a)(4); and

(c) knowingly causing the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally causing damage without authorization to computers in interstate commerce, contrary to Title 18, United States Code, Sections 1030(a)(5)(A)(i) and (a)(5)(B)(i).

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for GONZALEZ, HACKER 1, HACKER 2, P.T., and others to hack into the Corporate Victims' computer networks in order to steal credit and debit card numbers and corresponding Card Data from those networks, which credit and debit card numbers and other information was offered for sale in order to reap profits for the coconspirators.

MANNER AND MEANS OF THE CONSPIRACY

Scouting Potential Victims

4. It was part of the conspiracy that GONZALEZ and P.T. would identify potential corporate victims, by, among other methods, reviewing a list of Fortune 500 companies.

5. It was further part of the conspiracy that GONZALEZ and P.T. would travel to retail stores of potential corporate victims, both to identify the payment processing systems that the would-be victims used at their point of sale terminals (e.g., "checkout" computers) and to understand the potential vulnerabilities of those systems.

6. It was further part of the conspiracy that P.T. would also visit potential corporate victims' websites to identify the payment processing systems that the would-be corporate victims used and to understand the potential vulnerabilities of those systems.

Launching the Attacks – The Hacking Platforms

7. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would lease, control, and use Internet-connected computers in New Jersey ("the Net Access Server"), California ("the ESTHOST Server"), Illinois ("the Gigenet Server"), Latvia ("the Latvian Server"), the Netherlands ("the Leaseweb Server"), and Ukraine ("the Ukranian Server") (collectively, "the Hacking Platforms") to (1) store malware;

(2) stage attacks on the Corporate Victims' networks; and (3) receive credit and debit card numbers and corresponding Card Data from those networks.

8. It was further part of the conspiracy that GONZALEZ would provide HACKER 1, HACKER 2, and P.T. with SQL Injection Strings and malware that could be used to gain unauthorized access to the Corporate Victims' networks and to locate, store, and transmit credit and debit card numbers and corresponding Card Data stolen from those networks.

9. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would hack into the Corporate Victims' networks using various techniques, including, among others, SQL Injection Attacks, to steal, among other things, credit and debit card numbers and corresponding Card Data.

Executing the Attacks - The Malware

10. It was further part of the conspiracy that once they hacked into the computer networks, GONZALEZ, HACKER 1, and HACKER 2 would place unique malware on the Corporate Victims' networks that would enable them to access these networks at a later date ("Back Doors").

11. It was further part of the conspiracy that once they hacked into the Corporate Victims' networks, GONZALEZ, HACKER 1, and HACKER 2 would conduct network reconnaissance to find credit and debit card numbers and corresponding Card Data within the

Corporate Victims' networks.

12. It was further part of the conspiracy that once GONZALEZ, HACKER 1, and HACKER 2 hacked into the Corporate Victims' networks, they would install "sniffer" programs that would capture credit and debit card numbers, corresponding Card Data, and other information on a real-time basis as the information moved through the Corporate Victims' credit and debit card processing networks, and then periodically transmit that information to the coconspirators.

13. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would communicate via instant messaging services while the unauthorized access by them was taking place in order to advise each other as to how to navigate the Corporate Victims' networks and how to locate credit and debit card numbers and corresponding Card Data.

14. It was further part of the conspiracy that GONZALEZ, HACKER 1, and HACKER 2 would use unique malware to transmit the stolen credit and debit card information and Card Data to a Hacking Platform.

Concealing the Attacks

15. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would conceal their efforts to hack into the Corporate Victims' networks by, among other things, leasing the Hacking Platforms under false names, communicating

over the Internet using more than one messaging screen name, storing data related to their attacks on multiple Hacking Platforms, disabling programs that logged inbound and outbound traffic over the Hacking Platforms, and disguising, through the use of “proxies,” the Internet Protocol addresses from which their attacks originated.

16. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would conceal their efforts to hack into the Corporate Victims’ networks by, among other things, programming malware to be placed on the Corporate Victims’ computer networks to evade detection by anti-virus software and then testing the malware against approximately 20 different anti-virus programs.

17. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. programmed the malware to be placed on the Corporate Victims’ computer networks to erase computer files that would otherwise evidence its presence on the Corporate Victims’ networks.

OVERT ACTS

18. In furtherance of the conspiracy, and to effect its unlawful object, the coconspirators committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. On or about November 6, 2007, GONZALEZ transferred a computer file to the Ukranian Server named "sqlz.txt" that contained information stolen from Company A's computer network.

b. On or about November 6, 2007, GONZALEZ transferred a computer file to the Ukranian Server named "injector.exe" that matched malware placed on both Heartland and Company A's servers during the hacks of those companies.

c. On or about December 26, 2007, HACKER 1 and HACKER 2 accessed Heartland's computer network by means of a SQL Injection Attack from the Leaseweb Server and using the ESTHOST Server.

d. In or about January 2008, over an internet messaging service, GONZALEZ sent P.T. a SQL Injection String that was used to penetrate Company B's computer network (the "Company B SQL String"). The Company B SQL String was programmed to direct data to Hacking Platforms, including the ESTHOST Server and the Ukranian Server.

e. On or about March 13, 2008, at approximately 10:41 p.m., GONZALEZ connected to the Latvian Server.

f. On or about March 13, 2008, at approximately 10:42 p.m., GONZALEZ connected to the Ukranian Server.

g. On or about April 22, 2008, GONZALEZ modified a file on the Ukranian Server that contained computer log data stolen from Company B's computer network.

h. Between in or after March 2007 and in or about May 2008, GONZALEZ participated in a discussion over an internet messaging service in which one of the participants stated "planning my second phase against Hannaford."

i. Between in or after March 2007 and in or about May 2008, GONZALEZ participated in a discussion over an internet messaging service in which one of the participants stated "core still hasn't downloaded that [Company B] sh-t."

j. Between in or after December 2007 and in or about May 2008, P.T. participated in a discussion over an internet messaging service in which one of the participants stated "that's how [HACKER 2] hacked Hannaford."

All in violation of Title 18, United States Code, Section 371.

COUNT 2
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1349

1. The allegations contained in paragraphs 1 and 3 through 18 of Count 1 of the Indictment are realleged and incorporated as if set forth herein.

2. Between in or about October 2006 and in or about May 2008, in Morris and Mercer Counties, in the District of New Jersey, and elsewhere, defendants

ALBERT GONZALEZ,
a/k/a "segvec,"
a/k/a "soupnazi,"
a/k/a "j4guar17,"
HACKER 1, and
HACKER 2

did knowingly and intentionally conspire and agree to devise a scheme and artifice to defraud the Corporate Victims, their customers, and the financial institutions that issued credit and debit cards to those customers, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for GONZALEZ, HACKER 1, HACKER 2, P.T., and others to profit from the sale and fraudulent use of credit and debit card numbers and corresponding Card Data stolen from the Corporate Victims' computer networks.

MANNER AND MEANS OF THE CONSPIRACY

4. It was part of the conspiracy that once the coconspirators had stolen credit and debit card numbers and corresponding Card Data (the "Stolen Data") from the Corporate Victims' computer networks, GONZALES, HACKER 1, HACKER 2, and P.T. would cause the Stolen Data to be broken down into batches suitable for wholesale distribution over the Internet.

5. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would sell the Stolen Data and cause it to be available for resale.

6. It was further part of the conspiracy that those who purchased batches of the Stolen Data would further distribute the Stolen Data throughout the United States and elsewhere, where it would be used to make unauthorized purchases at retail locations, to make unauthorized withdrawals from banks and financial institutions, and to further identity theft schemes.

All in violation of Title 18, United States Code, Section 1349.

A TRUE BILL

_____
FOREPERSON

_____
RALPH J. MARRA, JR.
Acting United States Attorney