UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | Hon. Susan D. Wigenton |
| | : | |
| v. | : | Crim. No. 13-712 |
| | : | |
| LAURI LOVE,<br>a/k/a "nsh,"<br>a/k/a "route,"<br>a/k/a "peace" | : | 18 U.S.C. §§ 371, 1030, and 2 |

**SUPERSEDING INDICTMENT**

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

**COUNT I**

**BACKGROUND**

**Defendant and Others**

1. At all times relevant to this Superseding Indictment:

a. Defendant LAURI LOVE, a/k/a "nsh," a/k/a "route," a/k/a "peace" ("LOVE"), resided in or near Stradishall, England. As set forth more fully below, defendant LOVE was a sophisticated and prolific computer hacker who specialized in gaining access to the computer networks of large organizations, including government agencies, collecting confidential data including personally identifiable information ("PII") from within the compromised networks, and exfiltrating the data out of the compromised networks.

b. Co-conspirator-1 ("CC#1"), a co-conspirator who is not charged as a defendant herein, resided in or near New South Wales, Australia.

c. Co-conspirator-2 ("CC#2"), a co-conspirator who is not charged as a defendant herein, resided in or near Australia.

d. Co-conspirator-3 ("CC#3"), a co-conspirator who is not charged as a defendant herein, resided in or near Sweden.

**Overview of the Hacking Conspiracy**

2. From at least as early as approximately October 1, 2012, through in or about October 2013, defendant LOVE and others (collectively, the "Co-Conspirators") hacked into thousands of computer systems in the United States and elsewhere. Once inside the compromised computer systems, the Co-Conspirators placed hidden "shells" or "backdoors" within the networks, which allowed the Co-Conspirators to return to the compromised computer systems at a later date and steal confidential data.

3. The Co-Conspirators' victims included the United States Army and numerous other agencies of the United States, including the United States Missile Defense Agency, Environmental Protection Agency, and the National Aeronautics and Space Administration (collectively the "Government Victims"). The data stolen from the Government Victims included the PII of hundreds of thousands of individuals, including military servicemen and servicewomen and current and former employees of the federal government. The attacks collectively resulted in millions of dollars in damages to the Government Victims.

**Definitions and Methods of Hacking Utilized by the Co-Conspirators**

4. At times relevant to this Superseding Indictment:

a. An Internet Protocol ("IP") address was a unique numeric address used by a computer on the internet. An IP address consisted of a series of four numbers, each in the range of 0-255, separated by periods and every computer connected to the internet was assigned an IP address.

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

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

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

e. "HTML" was a computer programming language used to design websites.

f. "Malware" was malicious computer software programmed to, among other things, identify, and export information from computers that were hacked as well as to evade detection by anti-virus programs running on those computers.

g. "ColdFusion" was the name of a commercial web application development platform created by Adobe and designed to make it easier to connect simple HTML pages to a back-end database.

h. "Proxy servers" were computer systems or applications that acted as intermediaries for requests from clients seeking resources from other servers. A proxy server has a large variety of potential uses, one of which is to attempt to hide one's true IP address from others, and to thereby remain anonymous.

i. An Internet Relay Chat ("IRC") was an online medium through which multiple people could gather together in a "chat room" or "channel" and discuss topics of mutual interest. Similar to a telephone conference call, it allowed multiple people to participate in and communicate within one "conversation," but words were typed not spoken.

**The Government Victims**

5. At all times relevant to this Superseding Indictment:

a. The Engineer Research and Development Center ("Engineer R&D Center") was a research organization of the U.S. Army Corps of Engineers ("Army Corps") with laboratory facilities in various locations of the United States, including Vicksburg, Mississippi and Champaign, Illinois.

b. The Plans and Analysis Integration Office ("PAIO") was an agency of the United States government, and was a component of the United States Military ("USM") responsible for gathering and analyzing data, tracking the implementation of policies and overseeing long-range plans. The PAIO maintained a Research, Development and Engineering Command located in or around Aberdeen Proving Ground, Maryland.

c. The Strategic Studies Institute ("SSI") was an agency of the United States government, and was a branch of the U.S. Army War College that published national security and strategic research and analysis. The SSI was located in Carlisle, Pennsylvania.

d. The Army Network Enterprise Technology Command ("NETCOM") was an agency of the United States government that planned, installed, integrated, protected and operated computer networks of the U.S. Army, and maintained a Network Enterprise Center located in or around Aberdeen Proving Ground, Maryland. Until in or around 2010, NETCOM maintained computer servers at Fort Monmouth in Monmouth County, New Jersey.

e. The Army Contracting Command ("ACC") was an agency of the United States government that provided contracting support to the U.S. Army throughout the United States and abroad. The ACC maintained the Army Materiel Command in or around Redstone Arsenal, Alabama.

f. The Missile Defense Agency ("MDA") was an agency of the United States government located in or around Fort Belvoir, Virginia, and was a research, development and acquisition agency within the United States Department of Defense (the "DOD") that was responsible for, among other things, establishing a ballistic missile defense system.

g. The Federal Facilities Environmental Stewardship and Compliance Assistance Center ("FedCenter") was a joint initiative of the United States Environmental Protection Agency's Office of Enforcement and

Compliance Assurance ("EPA-OECA"), the Army Corps' Construction Engineer Research Laboratory, and the Office of the Federal Environmental Executive. The purpose of the FedCenter was to create an all-services technical compliance assistance center to assist federal environmental officials in addressing environmental needs. The FedCenter was administered by the Corps' Construction Engineering Research Laboratory in Champaign-Urbana, Illinois.

h. The National Aeronautics and Space Administration ("NASA") was an agency of the United States government responsible for the nation's civilian space program and for aeronautics and aerospace research and was headquartered in Washington, D.C.

i. Human Resources Technologies, Inc. ("HRTec") was a company based in Alexandria, Virginia that provided technological solutions to government agencies, non-profit associations and the private industry. HRTec specialized in providing information technology services, including custom applications, web design, databases and web-based systems to their customers. HRTec provided several database driven web applications for the DOD, including applications that managed and stored DOD's Equal Employment Opportunity ("EEO") records such as EEO complaints, case management documents, and other records. Some of these records contained PII of DOD employees.

**THE CONSPIRACY**

6. From in or about October 2012 through in or about October 2013, in the District of New Jersey and elsewhere, defendant

LAURI LOVE,
a/k/a "nsh,"
a/k/a "route,"
a/k/a "peace,"

did knowingly and intentionally conspire and agree with others to commit an offense against the United States, that is, to intentionally access a computer without authorization, and to exceed authorized access, and thereby obtain information from a department or agency of the United States, namely, the United States Army, the Missile Defense Agency of the United States Department of Defense, the Environmental Protection Agency, and the National Aeronautics and Space Administration, the value of which exceeded $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(B) and 1030(c)(2)(B)(iii).

**OBJECT OF THE CONSPIRACY**

7. It was the object of the conspiracy for defendant LOVE and others to hack into the computer networks of the Government Victims and steal large quantities of non-public data, including PII, to disrupt the operations and infrastructure of the United States government.

## MANNER AND MEANS OF THE CONSPIRACY

8. The manner and means by which defendant LOVE and others sought to accomplish the conspiracy included, among other things, the following:

**Searching for Potential Victims**

a. It was part of the conspiracy that defendant LOVE and other Co-Conspirators would search for vulnerabilities in the websites of various United States Army installations and other government agencies to identify potential hacking victims.

b. It was further part of the conspiracy that defendant LOVE and other Co-Conspirators would use an automated process to scan IP address ranges to identify computer systems vulnerable to cyber attacks.

c. It was further part of the conspiracy that the defendant LOVE and other Co-Conspirators would share information about potential hacking victims through online IRC communications, including sharing links that could be used to access compromised computer systems. For example, in an IRC communication on or about January 3, 2013, defendant LOVE, using the online moniker "peace," stated:[1]

peace: so can pivot and scan for other vulns [vulnerabilities]

peace: we might be able to get at real confidential shit

....

peace: blow this year wide open

[1] The text of the chats is reproduced in this Superseding Indictment as it appears in the chat logs; errors in spelling and punctuation have not been corrected.

**Executing the Attacks**

d. It was further part of the conspiracy that defendant LOVE and other Co-Conspirators would hack into the Government Victims' networks using various techniques, including, among other things, SQL Injection Attacks and exploitation of vulnerabilities in Coldfusion applications, to access PII of current and former United States government employees and other information located on government victim networks.

e. It was further part of the conspiracy that defendant LOVE and other Co-Conspirators would provide each other and others with SQL Injection Strings, ColdFusion vulnerabilities and malware that could be used to gain unauthorized access to the Government Victims' networks to locate, transmit and store confidential data from those networks.

f. It was further part of the conspiracy that once they hacked into the Government Victims' computer networks, defendant LOVE and other Co-Conspirators would place malware, including backdoors and shells, on the Government Victims' networks that would enable them to access these networks at a later date. Defendant LOVE and other Co-Conspirators placed thousands of shells on computer networks.

g. It was further part of the conspiracy that defendant LOVE and other Co-Conspirators would communicate in IRC channels while their unauthorized access was taking place in order to advise each other as to how to navigate the Government Victims' networks and how to locate confidential data and other information. The Co-Conspirators also communicated in IRC

channels about how they would export or exfiltrate stolen government data, and what they could do with the data. For example, on or about July 31, 2013, defendant LOVE, using the online moniker "peace," discussed in an IRC communication the data that he had stolen during a recently-committed hack of a United States government agency:

peace: [CC#2], you have no idea how much we can fuck with the us government if we wanted to.

peace: this ... stuff is really sensitive

CC#2: ooh nice

peace: it's basically every piece of information you'd need to do full identity theft on any employee or contractor for the [government agency]

**Publicizing the Attacks**

h. It was further part of the conspiracy that defendant LOVE and other Co-Conspirators would use various forms of social media, including Twitter, to announce and publicize the attacks against the Government Victims. For example, in an IRC communication on or about January 24, 2013, defendant LOVE, using the online moniker "route," discussed the timing of disclosing through social media a cyber attack against a United States government agency:

CC#2: do it friday ngiht

CC#2: dont rush

Route: mm

CC#2: well friday night still friday

CC#2: give ur sel the extra few hours to get set

CC#2: self

route: yeah

route: aiming for 5AM EST [Eastern Standard Time] == 10AM UTC [ Coordinated Universal Time] == 9PM AUS

route: so it rolls along the morning news in US

route: and gets europe for the afternoon and evening

**Concealing the Attacks**

i. It was further part of the conspiracy that defendant LOVE and other Co-Conspirators would conceal their attacks by disguising, through the use of proxy servers, the IP addresses from which their attacks originated. Defendant LOVE and the other Co-Conspirators further used the Tor network, which was an anonymizing proxy service, to hide their activities.

j. It was further part of the conspiracy that defendant LOVE and other Co-Conspirators would communicate about their hacking activities in secure IRC channels. The Co-Conspirators would use more than one screen name ("nic" or "nicks") and would often change names to further conceal their identities. For example, in an IRC communication on or about January 24, 2013, LOVE, using the online moniker "route," discussed his efforts to conceal his identity and hacking activities, and to avoid detection:

route: consideration 1: behaviour profile should not change

route: public side i mean

route: so whatever "normal" activities we do

route: should continue

route: but we move from this irc to better system

....

route: also

route: these nicks should change

route: i think

route: when we get on new communications

route: all new names

**OVERT ACTS**

9. In furtherance of the conspiracy, and to effect its unlawful object, the Co-Conspirators committed and caused to be committed the following criminal acts, among others, in the District of New Jersey and elsewhere:

**Engineer R&D Center Attacks**

10. Beginning on or about October 2, 2012, and continuing through on or about October 6, 2012, defendant LOVE and other Co-Conspirators attacked one of the Engineer R&D Center's servers, and compromised that server, by exploiting a vulnerability in its ColdFusion application to unlawfully access an Army database.

11. After accessing these forbidden areas of the Engineer R&D Center's server, defendant LOVE and his Co-Conspirators obtained a copy of a file that

enabled them to determine the administrator password for the Engineer R&D Center's website.

12. Using the stolen administrator password, defendant LOVE and the Co-Conspirators obtained data belonging to the Army Corps, including information regarding the planned demolition and disposal of certain military facilities.

13. On or about October 6, 2012, defendant LOVE and other Co-Conspirators attacked another computer system of the Engineer R&D Center by exploiting a vulnerability in the server's ColdFusion platform and to unlawfully access several databases. In executing this attack, the Co-Conspirators used a compromised computer server located in or around Parsippany, New Jersey, to temporarily store the malware that they then used to carry out the intrusion.

**HRTec Attack**

14. Beginning on or about October 6, 2012, and continuing for several months thereafter, defendant LOVE and other Co-Conspirators carried out a large scale cyber attack against HRTec's computer systems and stole large quantities of confidential information, including confidential EEO records and the PII of hundreds of thousands of DOD employees.

15. On or about October 6, 2012, defendant LOVE, using the online moniker "nsh," and others discussed the attack in an IRC chat, including the vulnerability in HRTech's computer system that he and his Co-Conspirators exploited.

**The NETCOM Attack**

16. Beginning on or about October 6, 2012, and continuing through on or about October 9, 2012, defendant LOVE and other Co-Conspirators carried out a SQL Injection attack and unlawfully accessed and stole data from NETCOM servers which included the PII of over 1,000 individuals, including military personnel stationed at Fort Monmouth, a military installation in Monmouth County, New Jersey.

17. On or about October 6, 2012, defendant LOVE, using the online moniker "nsh," discussed this hack with CC#1 in an IRC chat, including some of the data that the Co-Conspirators had accessed from the NETCOM servers:

| | |
|---|---|
| nsh: | [CC#1] |
| nsh: | you hexing mil? |
| CC#1: | Yes |
| CC#1: | sure am! |
| CC#1: | Via my new vps |
| CC#1: | lol |
| CC#1: | hmm, have a look at some of the passwords, hmm |
| nsh: | okais |

18. Also on or about October 6, 2012, defendant LOVE stated in an IRC chat: "hacking the army." Later in the chat, the Co-Conspirators discussed other military-based computer systems that they claimed to have compromised, or "owned":

| | |
|---|---|
| CC#2: | kewl so we have a few mil dbs now |

....

CC#2: now all we need is army

CC#2: lol

nsh: well, on army site atm

**The ACC Attack**

19. Beginning on or about October 7, 2012, and continuing through on or about October 8, 2012, the ACC's Army Materiel Command located in or around Redstone Arsenal, Alabama was the victim of a SQL Injection Attack through which defendant LOVE and other Co-Conspirators unlawfully accessed nonpublic data from an ACC database, including competitive acquisition bids and related attachments.

20. On or about October 10, 2012, in an IRC chat, defendant LOVE indicated that he had hacked the ACC website.

**The Army Corps Attacks**

21. On or about October 6, 2012, defendant LOVE and other Co-Conspirators attacked an Army Corps' computer server, and compromised that server, by exploiting a vulnerability in its ColdFusion application to unlawfully access an Army database. The data exposed as a result of the intrusion included natural resource management data.

22. On or about the same date, defendant LOVE, using the online moniker "nsh," CC#1, CC#3, and others, discussed this hack in an IRC chat, including sharing the "shell" that the Co-Conspirators used to access the compromised database:

CC#1: nsh

CC#1: We can upload a shell on this .mil

CC#3: nsh

CC#1: there's lots of pdf documents here

CC#3: mmmmm

CC#3: download them all

23. Additionally, beginning on or about October 7, 2012 and continuing through October 9, 2012, defendant LOVE and other Co-Conspirators carried out a SQL Injection attack against the Army Corps in Vicksburg, Mississippi to gain unlawful access to nonpublic data from an Army Corps database and steal that data.

24. On or about October 7, 2012, defendant LOVE, again using the online moniker "nsh," discussed this hack in an IRC chat. Specifically, defendant LOVE and CC#1 discussed the data that they stole from the Army Corps database, including email addresses of military personnel:

CC#1: 400K email log?

....

CC#1: The other army one is almost completely dumped :)

nsh: nicee

CC#1: Oh

CC#1: Wow

CC#1: We're going to have 400k emails.

....

nsh: can you grab one email for curiosity

nsh: to see who from to about

**The PAIO Attack**

25. On or about October 9, 2012, defendant LOVE and other Co-Conspirators compromised a computer server owned and operated by PAIO's Research, Development and Engineering Command, located in or around Aberdeen Proving Ground, Maryland by exploiting a vulnerability in the system's ColdFusion platform. The Co-Conspirators unlawfully accessed defense program budgeting data, among other information.

26. On or about the date of the hack, defendant LOVE and others discussed the attack in an IRC chat, including the vulnerability in the PAIO's computer system that the Co-Conspirators exploited.

**The MDA Attack**

27. In or around October 2012, defendant LOVE and other Co-Conspirators unlawfully accessed a database owned and operated by the MDA by exploiting a vulnerability in the MDA's computer system's ColdFusion platform. The database that the Co-Conspirators compromised stored, among other things, PII of over four thousand individuals.

28. On or about October 9, 2012, defendant LOVE, using the online moniker "nsh," discussed this hack in an IRC chat, including the data that the Co-Conspirators stole:

nsh: got a list of emails with clearance levels

....

nsh: one table is 4k wordlist

nsh: must be codewords

nsh: this data only up til 2007

nsh: at least, that table

nsh: other tables are update 2012

Defendant LOVE then pasted into the chat log samples of the stolen data, including account user names, email addresses, and telephone numbers of various victims.

**The SSI Attack**

29. On or about January 11, 2013, defendant LOVE and the Co-Conspirators compromised a server owned and operated by SSI by exploiting a vulnerability in the network's ColdFusion platform.

30. On or about January 11, 2013, defendant LOVE, using the online moniker "peace," discussed this hack in an IRC chat. Among other things, defendant LOVE posted a link to the shell that the Co-Conspirators had used, and could continue to use, to access SSI's server.

**The FedCenter Attack**

31. On or about January 3, 2013, defendant LOVE and other Co-Conspirators compromised a FedCenter computer server that the EPA-OECA owned and operated, which was located in or around Newark, Delaware. The Co-Conspirators exploited a vulnerability in the system's ColdFusion platform to unlawfully access and steal hundreds of megabytes of personnel information relating to federal government employees, among others.

32. Defendant LOVE, CC#3 and others coordinated the attack in an IRC chat as it took place, including sharing some of the stolen FedCenter data. Defendant LOVE and CC#3 also discussed their use of a "data dumper" to exfiltrate the stolen data:

peace: fedcenter.gov

CC#3: aight, lemme fix my dumper

CC#3: lol

peace: :)

....

CC#3: my dumper is ready

CC#3: uploaded to fedcenter

peace: nice

peace: lemme try

....

CC#3: u try or me?

CC#3: seems to me it is working

....

CC#3: in 50min i have 250MB plain text data

CC#3: partitial of 2GB

**The NASA Attack**

33. On or about July 10, 2013, defendant LOVE and other Co-Conspirators unlawfully accessed a database owned and operated by NASA by exploiting a vulnerability in the system's ColdFusion platform. The database that the Co-Conspirators compromised and stole consisted of, among other things, the PII of numerous NASA employees.

34. On or about July 10 and July 11, 2013, defendant LOVE, using the online moniker "peace," discussed this hack in an IRC chat:

peace: lol NASA...

peace: ahaha, we owning lots of nasa sites

peace: including nasajobs

peace: [CC#2], we own nasa

....

CC#2: hehe

CC#2: supa

....

peace: like 10 subdomains of nasa.gov :)

peace: i think we can do some hilarious stuff with it

35. During these communications, the Co-Conspirators also discussed the importance of concealing their unlawful activities:

CC#2: but server must have no link to you or us

....

peace: :)

CC#2: when done we kill it

CC#2: for this plan

CC#2: we can reopen another one for other ongoing stuff

CC#2: but once this plan done we need to make sure they cannot all trace it back to us

36. Collectively, the hacks described herein substantially impaired the functioning of dozens of computer servers and resulted in millions of dollars of damage to the Government Victims.

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

**COUNT 2**

1. The allegations of paragraphs 1 through 5 and 8 through 36 of Count 1 of this Superseding Indictment are realleged and incorporated herein.

2. On or about October 6, 2012, in Morris County, in the District of New Jersey and elsewhere, defendant

LAURI LOVE,
a/k/a "nsh,"
a/k/a "route,"
a/k/a "peace,"

did knowingly and intentionally access a computer without authorization, and exceeded authorized access, and thereby obtained information from a department or agency of the United States, namely, the United States Army Corps of Engineers, the value of which exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and 1030(c)(2)(B)(iii), and Section 2.

**FORFEITURE ALLEGATION**

1. The allegations contained in this Superseding Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

2. Upon conviction of the conspiracy offense in violation of Title 18, United States Code, Section 371 set forth in of this Superseding Indictment, defendant LAURI LOVE shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such conspiracy offense; and

b. pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such conspiracy offense.

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

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 18, United States Code, Sections 982(b) and 1030(i).

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B), 982(b) and 1030(i), and Title 21, United States Code, Section 853.

A TRUE BILL

FOREPERSON

PAUL J. FISHMAN
United States Attorney

**CASE NUMBER: 13-712 (SDW)**

# United States District Court
# District of New Jersey

**UNITED STATES OF AMERICA**

**v.**

**LAURI LOVE**

**SUPERSEDING INDICTMENT FOR**

18 U.S.C. §§ 371, 1030 & 2

**A True Bill,**

_____

**Foreperson**

**PAUL J. FISHMAN**
*U.S. ATTORNEY*
*NEWARK, NEW JERSEY*

NICHOLAS P. GRIPPO
*ASSISTANT U.S. ATTORNEY*
*(973) 645-2915*