Alleged Hacker Indicted in New Jersey in Data Breach Conspiracy Targeting Government Agency Networks

U.S. Attorney's Office **District of New Jersey**
October 28, 2013 (973) 645-2888

NEWARK, NJ—The New Jersey U.S. Attorney's Office has charged an alleged hacker in the United Kingdom with breaching thousands of computer systems in the United States and elsewhere—including the computer networks of federal agencies—to steal massive quantities of confidential data, U.S. Attorney Paul J. Fishman announced.

The federal indictment, filed in Newark federal court, charges Lauri Love, 28, of Stradishall, England, with one count of accessing a U.S. department or agency computer without authorization and one count of conspiring to do the same. An investigation led by the U.S. Army Criminal Investigation Command-Computer Crime Investigative Unit and the FBI in Newark revealed that Love allegedly illegally infiltrated U.S. government computer systems—including those of the U.S. Army, U.S. Missile Defense Agency, Environmental Protection Agency, and NASA—resulting in millions of dollars in losses.

Law enforcement authorities in the United Kingdom, including investigators with the Cyber Crime Unit of the National Crime Agency (NCA), announced today that they arrested Love at his residence Friday, October 25, 2013, in connection with an ongoing investigation by the NCA. Love was previously charged in New Jersey by federal complaint, also unsealed in connection with his arrest. He also is charged in a criminal complaint in the Eastern District of Virginia with alleged conduct related to other intrusions.

"According to the indictment, Lauri Love and conspirators hacked into thousands of networks, including many belonging to the United States military and other government agencies," said U.S. Attorney Fishman. "As part of their alleged scheme, they stole military data and personal identifying information belonging to servicemen and women. Such conduct endangers the security of our country and is an affront to those who serve."

According to the indictment unsealed in Newark federal court:

Between October 2012 and October 2013, Love and fellow conspirators sought out and hacked into thousands of computer systems. Once inside the compromised networks, Love and his conspirators placed hidden "shells" or "back doors" within the networks, which allowed them to return to the compromised computer systems at a later date and steal confidential data. The stolen data included the personally identifying information (PII) of thousands of individuals, some of whom were military servicemen and servicewomen, as well as other non-public material.

"Computer intrusions present significant risks to national security and our military operations," said Daniel Andrews, director of the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit. "The borderless nature of Internet-based crime underscores the need for robust law enforcement alliances across the globe. We appreciate the bilateral support of the National Crime Agency in bringing cyber criminals to justice."

"This investigation shows the necessity and value of strong partnerships among law enforcement agencies worldwide in the fight against cyber criminals," said FBI Special Agent in Charge Aaron T. Ford. "Cyber crime knows no boundaries, and without international collaboration, our efforts to dismantle these operations would be impossible."

Love and his conspirators planned and executed the attacks in secure online chat forums known as Internet relay chats, or IRC. They communicated in these chats about identifying and locating computer networks vulnerable to cyber attacks and gaining access to and stealing massive amounts of data from those networks. They also discussed the object of the conspiracy, which was 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.

To gain entry to the government victims' computer servers, Love and conspirators often deployed what is known as an SQL injection attack. SQL, or Structured Query Language, is a type of programing language designed to manage data held in particular types of databases; the hackers identified vulnerabilities in SQL databases and used those vulnerabilities to infiltrate a computer network. They also exploited vulnerabilities in a web application platform that some of the targeted agencies used known as Coldfusion. Like SQL Injection attacks, this method of hacking allowed the conspirators to gain unauthorized access to secure databases of the victims. Once the network was infiltrated, Love and his conspirators placed malicious code, or malware, on the system. This malware created a back door or shell, leaving the system vulnerable and helping Love and the conspirators maintain access to the network.

Love and his conspirators took steps to conceal their identities and illegal hacking activities. To mask their IP addresses, the conspirators used proxy and tor servers to launch the attacks. They also frequently changed their nicknames in online chat rooms, using multiple identities to communicate with each other.

If convicted, the defendant faces a maximum potential penalty of five years in prison and a $250,000 fine, or twice the gross gain or loss from the offense, on each of the two counts with which he is charged.

U.S. Attorney Fishman credited special agents of the U.S. Army Criminal Investigation Command-Computer Crime Investigative Unit, under the direction of Director Andrews, and the FBI in Newark, under the direction of Special Agent in Charge Ford, with the investigation leading to the indictment. Fishman also recognized the important work of the U.S. Department of Defense, Office of Inspector General Defense Criminal Investigative Service, under the direction of Special Agent in Charge Jeffrey Thorpe, Cyber Field Office; EPA Office of Inspector General, under the direction of Michael Daggett, Deputy Assistant Inspector General for Investigations; the NASA Office of Inspector General, Computer Crimes Division; and U.S. Department of Energy, Office of Inspector General, Deputy Inspector General for Investigations under the direction of John Hartman, in this case.

The government is represented by Assistant U.S. Attorney Nicholas P. Grippo of the U.S. Attorney's Office Criminal Division in Trenton.

The charges and allegations contained in the indictment are merely accusations, and the defendant is presumed innocent unless and until proven guilty.

Information on the charges in the Eastern District of Virginia can be obtained from the U.S. Attorney's Office for that district at 703-842-4050 or by e-mail at usavae.press@usdoj.gov.

This content has been reproduced from its original source.

Twitter (5) Facebook (12) Share

Newark Division Links

Newark Home

Contact Us
- Overview
- Territory/Jurisdiction

News and Outreach
- Press Room | Stories
- In Your Community

About Us
- Our People & Capabilities
- What We Investigate
- Our Partnerships
- Newark History

Wanted by the FBI - Newark

FBI Jobs