FEDERAL BUREAU OF INVESTIGATION
SITUATIONAL INTELLIGENCE REPORT

Charlotte Division

(U) Administrative Note: This product reflects the views of Charlotte Division and has not been vetted by FBI Headquarters.

(U) The situational intelligence report (SIR) has been developed to facilitate timely communication of relevant, localized intelligence from the Charlotte Division FIG to state and local law enforcement.

28 July 2009

(U) Computer Intrusions into Voice over Internet Protocol Servers Targeting North Carolina Financial Institutions and Businesses

(U//FOUO) This SIR has been produced in an effort to alert federal, state, and local law enforcement agencies of criminal activity with a nexus to North Carolina. The Charlotte Division has observed two similar occurrences of compromised Voice over Internet Protocol (VoIP) servers used to facilitate vishing attacks. Vishing attacks, a deviation from the term phishing attacks, use voice and text messages rather than email in attempts to trick victims into providing personal and financial account information. The following is a summary of the two identified intrusions:

- (U//FOUO) In March 2009, the Charlotte Division was notified of an intrusion into a VoIP server located at an undisclosed corporation in Greenville, South Carolina. It was determined that the intruder, using a Romanian based IP address, first conducted a port scan and determined port 5060 was utilized on the compromised server. Port 5060 is the standard port used for Session Initiation Protocol (SIP). SIP is responsible for the setup, modification, and

termination of sessions in an IP-based network and is typically the protocol used for VoIP servers. Then the hacker conducted a brute force attack and was able to crack the passwords to two extensions on the VoIP server due to weak passwords. The logs show several password attempts per second, indicating a script was used by the hacker. The hacker then proceeded to make 1,376 calls from the compromised phone extensions attempting to trick victims into providing their bank account information.

- (U//FOUO) In February 2009, a non-profit organization located in Charlotte, North Carolina, experienced a computer intrusion into their VoIP server. A review of the server logs revealed IP addresses resolving to France and Florida as being responsible for the intrusion. The intrusion took place through port 5060 and compromised SIP on a server running Trixbox Community Edition. After gaining access, the hackers made approximately 1,850 calls from the compromised system. The calls were made to customers of small regional banks soliciting credit card information via touchtone phone. After victims provided their account information, "money mules" across the country made ATM withdraws using the compromised accounts and sent a portion of the proceeds to Romania.

(U//FOUO) In both examples, the compromise of the VoIP servers occurred through port 5060 and they were used in furtherance of vishing schemes. As part of the compromise, intruders set up additional extensions on the compromised VoIP servers. They then notified victims of a problem with their financial accounts through automated phone calls or mass text messages to cell phones. The calls and text messages targeted an area code served by small regional banks, including two banks headquartered in North Carolina. The messages and calls solicited customers of the banks to call a toll free number and provide their credit or debit card information through an automated system. Once the victim provided their financial account information, it made them vulnerable to having money stolen and potentially made them a victim of identity theft.

(U//FOUO) Additional investigation by the Charlotte Division revealed that companies across the United States have recently had similar compromises of their VoIP which were linked to Romanian criminals.

(U//FOUO) To report instances of this crime and other Internet fraud, please visit the Internet Crime Complaint Center at www.ic3.gov.

(U) This bulletin has been prepared by the Charlotte Division of the FBI. Comments and queries may be addressed to the Charlotte Field Intelligence Group at 704-377-9200.

Distribution

Deputy Assistant Director, Directorate of Intelligence
National Security Analysis and Production Branch
Production Services Unit, Directorate of Intelligence
Criminal Intelligence Section
Financial Crimes Intelligence Unit
FBI Intranet
Columbia FIG
LEO – North Carolina Field Intelligence Group SIG
LEO – North Carolina Information Sharing & Analysis Center SIG
North Carolina State and Local Law Enforcement and Public Safety Agencies

FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our intelligence product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance.

Return to:
Federal Bureau of Investigation
400 South Tryon Street
Suite 900
Charlotte, NC, 28285

Customer and Product Information

Intelligence Product:
Title: Computer Intrusions into Voice over Internet Protocol Servers Targeting North Carolina Financial Institutions and Businesses
Dated: 28 July 2009
Customer Agency: _____

Relevance to Your Intelligence Needs

1. The product increased my knowledge of an issue or topic. (Check one)

___5. Strongly Agree
___4. Somewhat Agree
___3. Neither Agree or Disagree
___2. Somewhat Disagree
___1. Strongly Disagree

PSU INTERNAL USE ONLY

Product Tracking #: _____

Return To: _____

Actionable Value

2. The product helped me decide on a course of action. (Check one)

___5. Strongly Agree
___4. Somewhat Agree
___3. Neither Agree or Disagree
___2. Somewhat Disagree
___1. Strongly Disagree

Timeliness Value

3. The product was timely to my intelligence needs. (Check one)

___5. Strongly Agree
___4. Somewhat Agree
___3. Neither Agree or Disagree
___2. Somewhat Disagree
___1. Strongly Disagree

Comments (if any):