

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 6/6/2011

To: Los Angeles
Sacramento

Attn: CY-3 SSA Smollanoff
Attn: Sacramento ELSUR
Attn: CY-1 SST Linda Frazier

From: Sacramento
CY-1

Contact: SA John M. Cauthen

Approved By: Osborne Tom F

Drafted By: Cauthen John M;jmc 0606jmc01.ec

Case ID #: 288A-SC-44639 (Pending)

Title: CHANGED
Unsub, aka Sharpie;
Tribune Media -Victim;
CIP ;

Synopsis: Change case title and transfer investigation to Los Angeles.

Previous Title: Title marked "Changed" to reflect new subject. Title previously carried as
"Matthew Keys
Foxnews.com -Victim;
CIP;"

Reference: 288A-SC-44639 Serial 16
288A-SC-44767 Serial 46

Reference: Telcall from SA John M. Cauthen, SC, CY-1, to SSA Jason Smolanoff, LA, CY-3 on 6/6/2011.

Details: Re telcall, this case to be transferred to Los Angeles. The case involves a subject believed to be a resident of the United Kingdom who hacked into a computer in Los Angeles and damaged data affecting Tribune Media Corporation. Specifically, the subject hacked into a server called P2P and affected databases used by the Los Angeles Times and FOXNews40; both entities owned by Tribune Media.

UNCLASSIFIED

UNCLASSIFIED

To: Los Angeles From: Sacramento
Re: 288A-SC-44639

Sacramento opened the investigation, issued four subpoenas the results of which are part of the case file. Also, Sacramento conducted one consensually recorded telephone call, the results of which were placed into evidence 1D1. (A copy was also placed into 1A evidence.)

Due to venue issues, the investigation will not be pursued in Sacramento.

Case Background

Re serial 16, on about 11/7/2010, Unsub, aka Sharpie, logged into IRC chat channels associated with the hacking group called "Anonymous." The IRC channels on which Sharpie participated included #internetfeds and #operationpayback.

Re serial 16, on about 11/15/2010, chat on IRC #operationpayback suggested sharpie was UK based.

Re serial 46, Sharpie was a hacker with the group Anonymous and was involved in "Operation Payback".

On about 12/01/2010, the television station KTXL FOX40 located in Sacramento, CA learned it's e-mail contact list had been exfiltrated from the company's server in Los Angeles. The server is called the "P2P Server." The exfiltration appeared to have been accomplished via a compromised account on the P2P server.

After the P2P server was compromised, the manager of the news station began to receive emails from the person who purportedly hacked the server. The news station's customers, whose emails were part of the contact list, also began to receive e-mails from the person who purportedly hacked the server.

The majority of the e-mails carried the theme of making disparaging remarks about Fox 40 business practices. As determined by header information, the e-mails appeared to come from proxy servers in Europe.

It appears the hacker also created a fake e-mail account called cybertroll69x@hotmail.com and pretended to be Joseph Huerta, a FOX40News employee. As further discussed below, the subject later sent an e-mail using the name "Cancer Man" to the FOX40 station manager and included an attachment image called "cyber bullying." The e-mail also referenced Matthew Keys who was a former employee of FOX40 News. The email suggested the hacker may have visited Huerta's Facebook page.)

The name "Matthew Keys" also surfaced in an email from the hacker using the moniker "Cancer Man" further described below. (By way of background, Matthew Keys was a former FOX40 News employee who was terminated in about November 2010.)

On 12/3/2010, FOX40 News received an email from the hacker with the subject line "Re: Donating." The e-mail said "watch yourselves fox 40" and contained a forwarded e-mail which had been sent from the American Cancer Society to "Cancer Man." The e-mail appeared response from the American Cancer Society to Cancer Man. Based on the response, it appeared the person purporting to be Cancer Man had sent an e-mail to the American Cancer Society from the e-mail address cancerman4099@yahoo.co.uk and provided a contact name of Matthew Keys. This e-mail appeared to be in the form of a press release and described news coverage of a story by reporter Shawn Bennett. The e-mail referred to the station manager's Facebook page - www.Facebook.com/Brandon.Mercer/Posts/173241182694599, which suggested the hacker had visited the station manager, Brandon Mercer's, Facebook page.

On 12/12/2010, Mathews Keys, using e-mail address matthew@sactownmedia.com, sent an unsolicited e-mail to FOX40News stating he has infiltrated the hacking group "Anonymous." Keys sent Brandon Mercer, the station

UNCLASSIFIED

UNCLASSIFIED

To: Los Angeles From: Sacramento
Re: 288A-SC-44639

manager, a list of user names and passwords he claims he "obtained by a high authority within the 'conscious' hactivist organization Anonymous." The list pertained to a hack involving the website "Gawker." Keys also stated he had access to future operations, including operations against Paypal, Amazon, the Los Angeles Times, Fox News, and others.

On 12/12/2010, Mercer engaged Keys in a consensually recorded telephone conversation. They discussed the Gawker hack. Keys said he had entered a chat room with 2,000 plus members. In this chat room, Keys said he met someone who invited him into a private chat room populated by 15 highly skilled hackers. Keys discussed the Gawker attack, but claimed he did not know how it was done. Keys said he had limited technical knowledge, but did have computer records of his interaction with the group over the past week. In communicating with the hackers, Keys has discussed his past journalism experience. He believed that the hackers were using him for these skills. It was not clear in these discussions whether Keys was acting as a journalist to collect this information. In any case, it was clear he was sharing the information he obtained with a journalist from PBS. Keys claimed no knowledge about e-mails being sent to FOX40.

(FBI Note: Based on the conversation, it appears Keys' Twitter account may have been compromised by Anonymous members.)

In the conversation, Key stated one of the upcoming targets of Anonymous was the Los Angeles Times. Keys had no specifics about what was being planned.

The Los Angeles Times and Fox40 News are both owned by the same parent company, Tribune Media, based in Chicago, IL. They both use the server called P2P, discussed above, which is located in Los Angeles, CA.

As predicted by Keys, within two days, on 12/14/2010, LA Times server hosting the public facing website was compromised. The website was defaced by someone purporting to be Chippy1337. The hack originated from IP 188.165.6.178 which appeared to be a European proxy server (Ireland). The hack appeared to have been accomplished via a compromised account on the P2P server.

Tribune Media conducted an internal investigation regarding the intrusion performed against the Los Angeles Times on 12/14/2010 wherein the hacker used the tag, "chippy1337." According to Tribune Media management, the cost of the intrusion and the resulting time spent resolving it, cost the company over \$500,000. (A spreadsheet showing time and expenses was prepared by the investigators and is included in the investigative report on DVD in a 1A envelope)

Following the website hack, one of the Tribune Media employees accessed an IRC channel called #thegibson, hosted at a server called skidsr.us. According to the chats on this channel, a person using the moniker, sharpie, claimed to be involved in the LA Times hack and used the tag "chippy1337.". Other persons involved in hack appeared to include a person called Nikon.

Based on the information above, it appears that Keys was involved with the group "Anonymous" and members of this group hacked the P2P server on two occasions. The intrusion may have been accomplished by socially engineering someone to providing a user passwords. Keys did have access to P2P. His Twitter account may have been compromised. Keys therefore may have unwittingly been the vector used to by the hackers to perform the attacks. Or, he may have been a willing conspirator.

The person using the moniker sharpie, appears to be behind the Los Angeles Times hack on 12/14/2010.

The connection of Sharpie to the hack into the P2P server affecting FOX40News is unclear. The only connection appears to be the fact that both hacks apparently involved a compromised user account.

UNCLASSIFIED

UNCLASSIFIED

To: Los Angeles From: Sacramento
Re: 288A-SC-44639

Writer contacted Matthew Keys 4/27/2011 and asked him to bring records in his possession relating to the hacking group Anonymous. Keys has not responded to this request.

Writer contacted AUSA Matthew Segal, Eastern District of California on 5/31/2011. Writer expressed the opinion that Keys probably did not directly hack into the P2P server although he may facilitated the hack into the P2P server by members of Anonymous, albeit unwittingly. AUSA Segal listened to all the information, but was unconvinced that Keys was not knowingly involved. AUSA Segal advised that a subpoena, or search warrant, for data in the possession of Keys relating to criminal acts by the group Anonymous was feasible, but would require Attorney General concurrence. However, insomuch as the P2P server was located in Los Angeles, venue in the Eastern District of California was weak. AUSA Segal advised he would decline prosecution based on this fact alone, and recommended transferring the investigation to Los Angeles.

Writer believes the Anonymous member "Sharpie," is in the United Kingdom and is known to police officials there for his involvement in the Anonymous group.

The logical course of action is to request information from investigators in the United Kingdom to see if they have information regarding Sharpie.

The other logical step, would be to retrieve data from Matthew Keys regarding his information re Anonymous, - in particular the Anonymous member "Sharpie." To do this, assuming Keys remains uncooperative, would require a subpoena or search warrant. Insomuch as Keys considers himself a journalist, and appears uncooperative, this approach could require Attorney General concurrence. It is the opinion of Sacramento that Los Angeles has solid jurisdiction on the hack into the P2P server and which would permit investigators to compel Keys to provide the information he has about Anonymous.

The final approach would be to seek records from the companies hosting the proxy servers. This seems to be the avenue of least potential.

The only venue in Sacramento lies with the person and computer of Matthew Keys. The following things point to Keys criminal culpability:

- a) Keys had recently been terminated from FOX40 News and therefore, he may have borne resentment.
- b) Keys had previously held access to the P2P server and certainly knew how to access it. (However, it not known which account on P2P was used to hack the FOX40 News emails, and the account used to hack the Los Angeles Times did not appear related with Keys.)
- c) After being let go from FOX40, Keys had accessed and altered other social media websites belonging to FOX40 News resulting in loss of data.
- d) Keys' name was referenced in two emails by the person who purported to hack the FOX40 News P2P server.
- e) One of the e-mails sent referencing Keys appeared to originate in the Sacramento area.

However, the writer does not believe that Keys knowingly hacked the P2P server for the following reasons:

- a) While Keys name was mentioned in two emails, it seems illogical that the real hacker would identify himself so obviously while going to such lengths to avoid detection through the use of proxy servers.

UNCLASSIFIED

UNCLASSIFIED

To: Los Angeles From: Sacramento
Re: 288A-SC-44639

b) In the consensually recorded telephone call, Keys appears genuinely baffled by allegations he perpetrated the intrusion. Keys was otherwise candid about his involvement with the hacking group Anonymous and other targets of the group.

c) Keys, by the account of the FOX40 News station manager, as well as by his statements in the telephone call, did not appear to be technically sophisticated in the area of computer intrusions. Keys interest appears to be solely in the realm social media usage on the Internet. His involvement with Anonymous is likely only a journalistic interest.

Keys, according to his webpage, has left the Sacramento area and now works for KGO Television in San Francisco. His residence is unknown. Keys will not answer his phone, nor return phone calls or emails sent by the writer.

Based on the lack of venue in the Eastern District, it is recommended this case be transferred to Los Angeles. The above information, as well as other case data, can be packaged in the form of a Letterhead Memorandum (LHM) and sent to London by Los Angeles.

LEAD(s):

Set Lead 1: (Action)

LOS ANGELES

UNCLASSIFIED

UNCLASSIFIED

To: Los Angeles From: Sacramento
Re: 288A-SC-44639

At LOS ANGELES, CA

Receive results of investigative efforts in Sacramento and pursue logical investigation.

Set Lead 2: (Action)

SACRAMENTO

AT SACRAMENTO, CA

CY-1 SST to mail main case file, to include 1A, to Los Angeles, CY-3 attention SSA Jason Smolanoff, telephone 310-996-3805.

Set Lead 3: (Action)

SACRAMENTO

AT SACRAMENTO, CA

ELSUR to mail 288A-SC-44639 evidence item 1D1 to Los Angeles, ELSUR for further attention of SSA Jason Smolanoff, telephone 310-996-3805.

UNCLASSIFIED