Assessment of Brian Mottershead's Report on Faked Usenet Postings Regarding the US Chess Federation

Robert Jones, Craic Computing LLC

5th December 2007

Introduction

On 21st November 2007 Mike Curtis, a member of the US Chess Federation (USCF), sent me an email requesting my assistance in reviewing a report on the abuse of several Usenet groups that cover the game of chess.

Since 2005 a large number of messages have been posted to the Usenet group rec.games.chess.politics, amongst others, that appear to come from well known participants in these groups but which have been faked. These messages are typically very offensive and could damage the reputation the supposed author.

Abusive messages are common in many Usenet groups, but these examples were of particular concern as they involved people who were standing for election to the Executive Board of the United States Chess Federation. Concern about this led Brian Mottershead, a systems administrator for the USCF, to investigate the source of these faked messages and to prepare a report on his findings. That report was released in October 2007. In the report, Mr. Mottershead details his analysis of the Internet Protocol (IP) addresses that are recorded in the Usenet messages and correlates those over time with addresses recorded in the logs for USCF internal message boards. He draws the conclusion that one named individual was responsible for many of the offensive posts.

In response to that claim, one of the people that were impersonated has filed a lawsuit against several parties and the public rancor between some of the individuals involved has even been covered in an article in the New York Times. This issue is clearly very damaging to the reputation of the USCF and the US chess community. Mr. Curtis is a concerned member of that community. He asked me to review the Mottershead report and assess the validity of its conclusions as independent party removed from the personalities and strong opinions that are apparent within the USCF.

I work as a software developer and computer consultant and have a long standing interest in the field of Internet Forensics, the discovery of information that can identify the source of harassing emails, spam and Internet scams. I am the author of the book 'Internet Forensics', published in 2005 by O'Reilly Media, which details technical approaches that can be used in this field.

Based on an initial review of the issue and the available data, I agreed to prepare this assessment of Mr. Mottershead's analysis. Given that Mr. Curtis is making a personal

request for assistance, no fee will be charged for this assessment. This report is a service of my company, Craic Computing LLC, and is authored by myself.

I have no known conflict of interest in preparing this report. I have had no contact with Mr. Curtis prior to his request. I have had no contact and no affiliation with the USCF, any of the individuals involved in this dispute or with the Chess community in general. I have not had any contact with Mr. Mottershead and have based this report solely on the data that are available to anyone on the Internet. It is my understanding that a second independent assessment of the Mottershead report in being prepared. I have had no contact with the person preparing that review.

Methods

I have limited my analysis to only those data that publicly available and that are associated with the report by Mr. Mottershead. Specifically these datasets are contained in the zip archive file available at this URL:
http://rapidshare.com/files/62649719/mottershead.zip.html

This URL has been widely posted on chess related Usenet groups and web logs. The zip archive contains five files:

full-mottershead-report.txt
: This is the text of Mr. Mottershead's report detailing the steps he took in his analysis and his conclusions, including the name of the individual he believes in involved in the fake Usenet posts.

fake-sam-sloan.txt
: This file contains the full text and headers of a number of the offending Usenet messages that purport to be from Sam Sloan but which are not.

fake-sam-sloan-hdrs.txt
: This file contains a subset of data extracted from the headers of these messages.

chesspromotion-uscf-posts.txt
: This file contains the dates and IP address from which legitimate messages were posted to a USCF internal message board from the user with the nickname 'chesspromotion'.

chesspromotion-joomla-bridge.log
: This file is an extract of a log file for the software running the USCF internal message boards and details the accesses made by user 'chesspromotion' in September 2007.

The central argument in the Mottershead report is that the user posting to USCF internal boards is the same as the person making the fake Usenet posts. The report correlates the

identifiable legitimate activity of 'chesspromotion' with that of the Usenet impersonator, the so-called 'Fake Sam Sloan'. This is done using correlations between specific IP addresses or sets of addresses at specific times, the Internet service provider from which access was made, the approximate geographic location of the user based on network topology and other information in the various server log files, such as the 'User Agent' string that can describe the type of computer and web browser being used to access a server.

Based on the limited amount of data available in the above files, I am not able to comment on certain aspects of the Mottershead report. In particular, I cannot and do not make any statement as to the identity of the person posting as 'chesspromotion'.

In my review of the data I have limited myself to assessing any correlation between the IP address of the computer from which legitimate 'chesspromotion' messages were sent and that from which the fake Usenet posts were sent. I am reliant on the subset of data that is available in the publicly available zip archive.

The first step in my analysis was to write small computer programs ('scripts') that parse the various data files and extract the IP addresses and timestamps associated with each record. These scripts can be made available for review if needed. Running these scripts on the two 'chesspromotion' logs and the 'fake-sam-sloan-hdrs.txt' produced lists of the IP addresses involved in each and timelines of events in each log. Scripts were also written to identify IP addresses in common between the logs and to merge the different timeline files so as to provide a coordinated view of events over time.

Analysis of the subset of IP addresses common to 'chesspromotion' and 'fake sam sloan' postings was done using the UNIX utilities 'dig' and 'whois'. These allow one to lookup the Internet provider and domain owner of particular IP addresses and in some cases to determine the approximate geographic location of that address.

There are certain limitations to the datasets available for this analysis. The 'chesspromotion-uscf-posts.txt' file is the output from a SQL command on a database table that lists the date and time each message was entered into the database and the IP address of the computer that sent the message. I cannot determine the time zone used with that timestamp and do not know which of perhaps multiple internal USCF boards the data relates to. I would need to know more about the message board software to resolve that.

This has some significance as the Joomla log entries for 'chesspromotion' should line up with those in the SQL output. The Joomla log shows 'chesspromotion' viewing USCF internal boards in September 2007 and accessing the message board script '/forums/posting.php', which I presume provides the user with a way to post messages. In correlating accesses of this script with actual postings recorded in the database I see that not all accesses gave rise to recorded postings. This may reflect something of the software user interface, the activity of the user or possibly the use of multiple database tables for different message boards. What I do see for a subset of recorded postings is an

offset of one hour between the Joomla logs and the recording of the posting in the database. I believe this reflects either a difference in the way daylight saving time is handled in two pieces of software or on two distinct server computers. Either way, the correlation is so tight that I have added one hour to each of the Joomla log entries in order to align them with the SQL output.

I do not have the information needed to unambiguously align those times with those recorded in the Usenet postings. Access to the USCF servers or information about them would resolve that question. However given the information available to me here, I have to allow for plus or minus one hour in aligning the times of events on USCF forums and on the Usenet groups. I do not believe the times are out by any more than that.

If the analyses of these logs were to be used in legal proceedings then it would be important to resolve this ambiguity. However, I do not think this issue has a material impact on the overall conclusions given below.

Results

Comparing the list of unique IP addresses from the legitimate 'chesspromotion' postings and USCF board accesses with those from the faked Usenet postings produced a set of 10 unique addresses, shown in the table below:

IP Address	Internet Provider
24.90.223.35	RoadRunner, NY
75.111.194.9	Suddenlink, TX
75.111.199.177	Suddenlink, TX
201.134.236.150	Uninet S.A. de C.V., Mexico
152.163.100.67	America Online
152.163.100.132	America Online
152.163.101.14	America Online
205.188.116.199	America Online
207.200.116.5	America Online
207.200.116.66	America Online

6 of these are within ranges of addresses managed by America Online (AOL) and indicate access to the servers from an AOL account. It is not possible to identify this without access to AOL logs, which would certainly require some form of subpoena. It may well be possible to correlate activity on certain these IP addresses over time between the USCF and Usenet servers and that may provide circumstantial evidence of a linkage. The Mottershead report includes this type of analysis but I have not done so for my review and cannot comment on that.

The address 24.90.223.35 maps to the Internet Service Provider (ISP) 'RoadRunner' and specifically to a subnet of addresses that appears to cover New York City (subnet ROADRUNNER-NYC-2)

75.111.194.9 and 75.111.199.177 map to Suddenlink Communications, specifically a subnet identified with a Suddenlink office in Tyler, Texas, based on the response to the Unix command 'whois 75.111.199.177'.

201.134.236.150 maps to Uninet, a brand name of Telmex, a leading ISP in Mexico.

Here I describe my analysis of each of these four addresses.

24.90.223.35
The SQL output showing legitimate USCF postings from 'chesspromotion' shows that ALL of these came from this IP address in the time period 07/21/2006 through 08/02/2007. RoadRunner is a division of Time Warner Cable and provides residential Internet service via cable modem. These devices are often assigned IP addresses that rarely change over a period of time and that is consistent with what we see here.
A number of fake Usenet messages have this same IP address. The timestamps for these are:

```
2006-03-13 11:09:27
2006-06-20 15:07:44
2006-12-24 07:26:46
2007-04-15 22:03:18
2007-04-15 22:04:01
2007-04-15 22:11:42
2007-04-15 22:12:12
```

The first two of these precede the use of this address for legitimate posts. The other instances all lie between timestamps for legitimate messages. This pattern strongly suggests that the same residential Internet connection was used by 'chesspromotion' and the sender of these fake Usenet messages.

75.111.199.177
This address was used briefly from 26/08/2007 through 06/09/2007 and was the source of 3 fake Usenet posts and 3 legitimate posts. On 09/06/2007 the address was the source of one fake Usenet post at 8:18 and 3 legitimate posts later the same day beginning at 17:29. The location of the ISP places this address in Texas.

```
2007-08-26 19:56:07 fake Usenet post
2007-08-27 07:59:45 fake Usenet post
2007-09-06 08:18:42 fake Usenet post
2007-09-06 17:29:35 chesspromotion post to USCF
2007-09-06 21:13:35 chesspromotion post to USCF
2007-09-06 21:59:59 chesspromotion post to USCF
```

75.111.194.9

This address was used from 09/10/2007 through 09/20/2007 and was the source of 19 legitimate messages from 'chesspromotion'. This period was covered by the Joomla logs on the USCF server and show that 'chesspromotion' was active visiting the USCF message boards for the period 09/16/2007 through 09/20/2007. The discrepancy in the start date is a result of the Joomla logs not recording IP addresses prior to that date. In this period 19 fake Usenet posts were submitted from this address. Their timestamps are:

```
2007-09-10 21:18:10
2007-09-10 21:19:28
2007-09-10 21:20:14
2007-09-10 21:20:52
2007-09-11 20:52:42
2007-09-13 21:57:01
2007-09-15 12:40:38
2007-09-15 20:21:37
2007-09-16 17:30:53
2007-09-16 21:28:07
2007-09-16 21:28:42
2007-09-16 21:30:20
2007-09-19 09:01:43
2007-09-19 09:10:08
2007-09-19 09:10:56
2007-09-19 15:33:50
2007-09-19 15:42:34
2007-09-19 15:43:27
2007-09-19 19:05:42
```

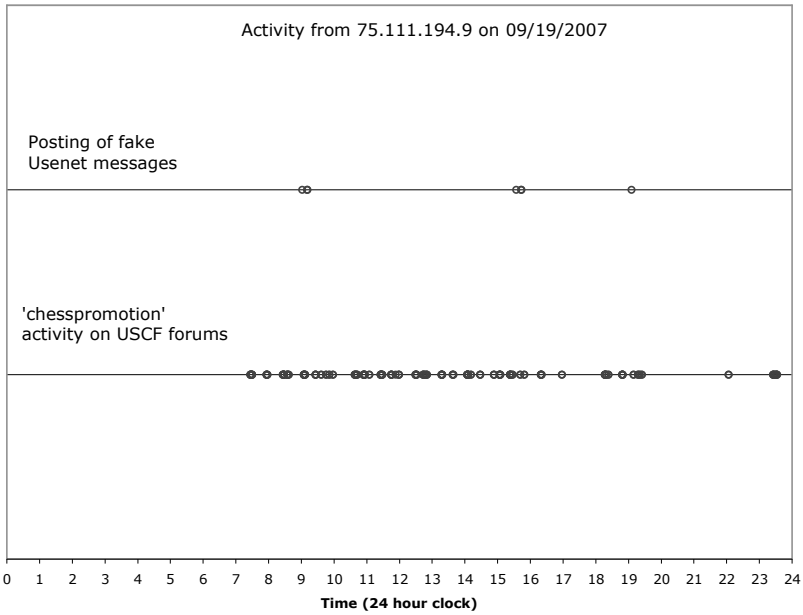
As described in the Methods section, I have been able to align the timestamps of the creation of legitimate USCF posts and activity on the USCF forums. The 'alignment' of these with the Usenet timestamps may be correct or it may be off by plus or minus one hour due to ambiguity in the time zone settings on different servers. With that caveat in mind, there are two very clear instances where the fake Usenet posts were sent during extended periods of legitimate activity by 'chesspromotion' on the same IP address.

The evening of 09/16/2007 shows the following closely timed events:

```
2007-09-16 17:30:53  fake Usenet post
2007-09-16 21:28:07  fake Usenet post
2007-09-16 21:28:42  fake Usenet post
2007-09-16 21:30:20  fake Usenet post
2007-09-16 21:39:24  chesspromotion activity on USCF forums
2007-09-16 21:39:26  chesspromotion activity on USCF forums
2007-09-16 21:39:36  chesspromotion activity on USCF forums
2007-09-16 21:39:56  chesspromotion activity on USCF forums
```

The activity on 09/19/2007 is even more pronounced. 'chesspromotion' was active on the USCF forums multiple times from 7:26 am through 11:32 pm. During this period 7 fake Usenet messages were posted. The following graph shows the times at which these events took place in the 24 hours of 09/19/2007.

It is clear that the 7 fake messages were posted from this IP address during an extended period of time when 'chesspromotion' was active on this same address. Even with the potential ambiguity in aligning Usenet and USCF timestamps this observation remains valid.



201.134.236.150
This address in Mexico was used from 09/21/2007 through 09/30/2007 and was used multiple times to access the USCF forums by 'chesspromotion'.

Use of this IP address and the 75.11.194.9 address in Texas are mutually exclusive. The last use of the Texas address was logged at 11:06 am on 09/20/2007 and the first use of the Mexico address was at 1:25 am on 09/21/2007, suggesting that 'chesspromotion' traveled between these two locations at that time.

On 09/25/2007 three fake Usenet posts were submitted from this address:
2007-09-25 14:38:26
2007-09-25 14:39:29
2007-09-25 20:59:03

On that day 'chesspromotion' visited the USCF forums at multiple times between 08:02 through 23:48. The fake Usenet postings were sent within this timeframe.

Conclusions

I conclude that the fake Sam Sloan Usenet postings that are listed above were sent from the same Internet connection as the legitimate USCF activity of user 'chesspromotion'. The close correlation in time with some of the activity, most notably on 09/19/2007, combined with the correlation in space, as both activities moved from Texas to Mexico on 09/20/2007, leads me to the clear conclusion that **a single individual is responsible for legitimate postings under the nickname 'chesspromotion' and for sending certain fake messages to Usenet groups that appear to come from Sam Sloan**.

The scope of my analysis was intentionally limited to activity on IP addresses that appeared in both legitimate and fake postings. It demonstrates a clear linkage between user 'chesspromotion' and the fake Usenet posts. Based solely on the data used in my analysis I cannot draw any conclusion as to who that individual might be.

The majority of the fake Usenet messages originate on other IP addresses, most notably those from America Online. My analysis does not draw any conclusions about those. Deeper analysis might uncover patterns of usage and circumstantial evidence that might prove or disprove any hypothesis about the source of these messages.

The analysis of Mr. Mottershead is much broader than mine, dealing with the IP addresses of many Usenet postings. The techniques that he has applied are largely identical to those that I have used and he seems to have performed his technical analysis carefully and methodically. My primary conclusion from my analysis fits perfectly within his broader set of conclusions and in no way contradicts those.

The major difference with is analysis is that he applies his knowledge of people involved in the USCF and the Usenet groups to identify and name one individual that he believes is responsible for the fake Usenet posts. I do not have that knowledge and based on the analysis described here I cannot comment on that conclusion.

Confirmatory Evidence

Definitive prove of the identity of the person or persons making the fake Usenet posts really requires the involvement of Internet service providers. Under subpoena they may be able to provide detailed logs that link a specific IP to a specific individual at a specific date and time. In the absence of that detailed information, it may be possible to confirm an identity using an additional source of data.

Specifically, if an individual suspected of involvement has sent direct email messages to other people, regarding USCF business for example, then those messages may allow specific IP addresses to be linked to an individual. This is similar evidence to the login of 'chesspromotion' to the USCF internal forums but is additional and independent.

The data associated with the Mottershead report deals only with fake 'Sam Sloan' messages but it appears from that report that other users were impersonated. Broadening and repeating Mottershead's analyses with a larger dataset might well uncover additional evidence that supports or refutes the conclusions of that report.

Caveats

Definitive conclusions about identity in Internet forensics can be difficult as there are ways in which computers can be hijacked and information disguised. Some of the arguments that might be raised with this sort of analysis are as follows:

More than one computer might share the IP address

> This is certainly possible. Multiple computers forming an 'internal' subnet behind a router or firewall may well appear to the external Internet as having the same external IP address. If this is the case it broadens the conclusion to one or more computers or individuals in the same household or organization.
> For this to hold true in this case, it would have to apply to all the IP addresses included in my analysis and that is unlikely.

More than one person might use a given computer and/or account.

> This is a common occurrence in many homes. If this applies to the current case then it broadens the conclusion to family members, but not beyond.

The computer might allow remote access

> Software such as 'PC Anywhere' and 'VNC' allow remote users to control computers attached to the Internet. These require the permission of the computer owner to install and operate. I cannot tell if such software is in use on the computer or computers used in the USCF postings. The pattern of usage on 09/19/2007 argues strongly that no remote access took place without explicit permission from the owner of the computer.

The computer might have been hijacked

> The infection of PCs by 'Trojans' is a major source of Internet spam and many computers have been compromised by such software. The majority of these trojans are focused on spam distribution or capturing credit card information and passwords. It would require considerable sophistication for someone to hijack the 'chesspromotion' computer and use it to interact with remote web sites without the real user being aware of it. I do not view this as a likely scenario.

The IP address might have been 'spoofed'

> Taking control of an IP address requires technical sophistication and access to the physical local network where that address is located. I do not believe that to be at all likely in this case where multiple locations have been involved. Again, the interleaved pattern of activity on 09/19/2007 is a very strong argument against this.

The server logs may have been tampered with

> It is certainly possible to alter server logs. Typically this would require 'root' access to the systems. However, the same information can appear in multiple log

files and those files can be backed up to tape or other permanent storage. That makes it very difficult to tamper with the data while keeping the logs consistent and risks discovery if backup copies of the logs are studied. With regard to Usenet postings, these files can be replicated to multiple servers, cached by search engines and saved to local disks. That makes it very difficult to tamper with the data. I do not believe any logs have been manipulated in this case.

IP addresses can be disguised using Internet Proxies

In these cases a message from the originating IP address can be passed through one or more intermediate computers, appearing to come from the last in the chain. Proxies are effective at disguising the real source IP but it is easy to recognize when a proxy is in use. There is no sign of their use in this case.

Summary

To summarize this review

1. The technical approach taken by Mr. Mottershead in his analysis is valid and it appears to have been carried out professionally and correctly.
2. The technical conclusion of that report that, in some cases, the same IP address was used to post legitimate USCF messages and fake 'Sam Sloan' Usenet messages is valid and I agree with that conclusion.
3. I also conclude that user 'chesspromotion' is responsible for the subset of fake Usenet messages detailed here. This is an important component of the conclusions of the Mottershead report.
4. That report is a broader analysis of the available data than mine and draws much broader conclusions that I am able to neither prove nor disprove based on my limited review. In particular, I am not able to identify the real person behind user account 'chesspromotion'.

This analysis has been performed to best of my ability given the datasets associated with the Mottershead report and given the limited time that I have been able to contribute to this analysis.

-- Robert Jones --

President, Craic Computing LLC
911 East Pike Street, Suite 231
Seattle, WA 98122