Cyberstalking and Law Enforcement: Part 2

Wed, 10/12/2011 - 5:29am

J. A. Hitchcock

A step by step guide to handling a cyberstalking investigation.Part one of this article discussed how to recognize cyberstalking and the initial contact with the victim.

The Preliminary Investigation

After the law enforcement officer determines this is indeed a cyberstalking case, he or she should initiate a preliminary criminal investigation. It is important to obtain from the complainant a detailed description of the harassing behavior, including any personal contacts, such as telephone calls or being followed.

Step 1: Ask the complainant if he or she knows who is sending the harassing messages. If so, obtain the standard investigative information about the suspect: name, age, address, telephone number, vehicle information, and relationship to victim. Obtain a copy of the messages for the case file showing the e-mail address, Web site URL, nickname, screen name, and the content(s) of the message(s).

Step 2: Ask the complainant if he or she knows why he or she is being harassed. If so, record the complainant's explanation in as much detail as possible in the narrative portion of the report. Knowledge of the reason can help lead to the identification of an unknown harasser.

Step 3: Establish when and how the harassment began. Has the contact been solely via the Internet (e-mail messages, chat rooms, mailing lists, instant messages, Web site) or has there been other harassment such as telephone calls, cell phone calls or texts, postal letters, or contacts at the complainant's workplace or other locations, and whether any of the complainant's relatives or friends have also been subjected to the harassment.

Step 4: Determine whether the complainant has been threatened with physical harm or physically attacked. Often, the electronic messages will threaten violence, rape, and even death. The law enforcement officer will need to establish the details of how these threats were communicated. If the complainant has been attacked, it is apparent the threat has escalated beyond electronic threats. Details of the attack and results of the subsequent investigation of that incident become part of the case file.

Step 5: The law enforcement officer needs to secure any physical evidence available and start the chain of custody to protect the evidence. The material should be saved in both paper printouts and electronic files on an electronic medium such as a disk or CD/DVD-ROM. Ask the complainant if he or she has any material evidence. Items to request include:

E-mail messages

Chat room messages

Instant messages

Web page images

Social networking messages/wall posts

Mailing list messages

Message board messages

Telephone/cell phone conversations or answering machine messages

Text messages

Postal letters

Photographs

Step 6: What communication has the complainant had with the harasser? Did the complainant respond to the messages? Copies of the responses are necessary for the investigation. The law enforcement officer needs to describe and assess the amount and nature of communication between the two parties to understand if the incident escalated or if the threats occurred without migrating factors.

Step 7: Although cyberstalking is a secretive, individualized crime, law enforcement officers always need to ask if there are any witnesses. Often the victim will alert friends and relatives to the messages received and the law enforcement officer needs to determine whether others can contribute information to the case.

Step 8: Determine what steps, if any, the complainant has taken to stop the harassment. Has the complainant reported the harassment to anyone else, notified the ISP about the messages, filed any court actions, or sought legal advice? In order to develop a clear understanding of the case, law enforcement officers must make a record of any action by the complainant.

Step 9: Assess the steps the complainant has taken to protect himself or herself. Of prime concern are the physical protective steps of appropriate security for their person. In addition, recommendations in this article for protecting against the online abuse should be followed.

Once the initial complaint has been filed, an assessment of the case for continued investigation is appropriate.

Some Shortcuts

Many cyberstalkers who send threatening e-mail messages send them from free e-mail accounts available from such Web sites as Yahoo!, Gmail, and Hotmail. Such e-mail service providers can supply the IP logging information, which includes IP addresses used to access the account and the dates and times of that access. The IP addresses usually resolve back to a legitimate ISP. Sometimes a law enforcement officer's telephone call to that ISP will prompt the ISP to shut down the harasser's account and send information about the harasser to the police department; other times, law enforcement will need a subpoena or search warrant to get the information associated with the harasser's account. If the harasser accesses e-mail from a location that offers free Internet access (such as libraries), identification is more difficult but not impossible.

If the investigation has uncovered more than one e-mail address associated with the harasser, the law enforcement officer could conduct a search using a search engine such as www.yahoo.com or www.google.com to see if the harasser has any type of Internet presence. For example, the Maryland State Police had a case where the suspect was sending harassing e-mail messages to a female using a free e-mail account at different county libraries. The harasser's established e-mail address came from a library and therefore had no originating IP address. There seemed to be no way to determine who the harasser was. Nevertheless, a newsgroup search using the harasser's e-mail address revealed a message posted to a mountain biking group where the suspect actually gave his real first and last name and the city he lived in.

If the law enforcement officer develops an address or telephone information on the harasser, an interview with the harasser usually ends the harassment. If the harasser is in another state, it is recommended to contact the local law enforcement agency to conduct the interview. If the harassment has escalated to cyberstalking or real-life stalking, proceed from there by filing charges, getting protective orders, or helping the victim find a lawyer to file a civil suit.

There are two other forms of cyber crime that may come to the attention of law enforcement officers as they respond to these calls for services. One is when someone has been impersonating the complainant online (forging names on posted messages, e-mail messages, and chat room messages). The other cyber crime occurs when someone forges the victim's name to procure services or buy products. The investigative steps outlined will serve to develop these cases as well.

It is important to acquire as much information as possible about the Web site or message board or forum in question, including the URL. Whenever someone accesses a Web site, the Web site captures, at a minimum, the IP address used to access it at a particular date and time.

By contacting the Web site administrator by e-mail or telephone with the date and time of the harasser's activity on the administrator's site, law enforcement officers can often persuade administrators to provide the IP address without the need for a subpoena or other legal process since they are not releasing any type of subscriber records or other information that would suggest an identity. However, in some jurisdictions, officers may need to file either a search warrant or a subpoena to get the subscriber information. AOL has different procedures; they are available at http://www.haltabuse.org/cops/aolguidelines.doc.

Anonymity through the Internet

Currently the Internet provides opportunities for anonymity that are complicating cyberstalking investigations. The cyberstalker can thwart an investigation by using different ISPs and adopting different screen names. Perhaps the most difficult situation is when the cyberstalker uses an anonymous remailer service that strips identifying information from the e-mail header and erases any transactional data from servers, thus removing the tracing evidence of a message back to the author.

Cyberstalkers using anonymous remailing services will remain virtually undetectable. Fortunately, the anonymous remailers are currently being used in only a small percentage of the cyberstalking incidents. The appropriate resolution to anonymous remailing services is the development of a technological solution that will block anonymous communication and thus offset the availability of the technique to cyberstalkers.

Tracing the Suspect

Although the Internet eliminates some physical barriers to interaction with another person, and although it provides the perception of anonymity, it does leave evidence that can be traced to the cyberstalker.

The first identifying evidence is found in the headers. The headers contain the entire path and route the message took and is vitally needed when tracing a harasser ("How to Show Full Headers on Newsreaders/E-mail Programs" is available at http://www.haltabuse.org/help/header.shtml).

Here is an example of what a person usually sees when receiving an e-mail:

To: netcrimes@netcrimes.net

From: questloans@qwest.net

Subject: FOX NEWS: End of war sure to cause rate hikes soon

Date: Wed, 30 Apr 2011 00:28:01 -1900

To determine where the message really originated, activate the full headers, which will look something like this:

Received: from ns5.eleconinfotech.net [202.160.172.226] by odin.larp.com with ESMTP (SMTPD32-7.07) id ABFB80700D4; Wed, 30 Apr 2011 02:23:55 -0400

Received: from mail2.uswest.net ([211.136.104.133]) by ns5.eleconinfotech.net (8.11.6/linuxconf) with ESMTP id h3U4cij17870; Wed, 30 Apr 2011 10:08:50 +0530

Message-ID: <000060936d3a$000072c8$00005151@gateway.attbi.com>

To: netcrimes@netcrimes.net

From: questloans@qwest.net

Subject: FOX NEWS: End of war sure to cause rate hikes soon

Date: Wed, 30 Apr 2011 00:28:01 -1900

MIME-Version: 1.0

Content-Type: text/html; charset="iso-8859-1"

Headers: Mailman v2.0.4

X-RCPT-TO:

Working from the bottom up, go to the first "Received: from line" and look at the IP address there—in this case, 211.136.104.133.

An IP address consists of four sets of numbers with one to three numerals per set. This is the server the message originated from. Once the IP address is known, the officer can find out who owns it and contact the owner for more information about the account holder.

Translating IP Addresses with WHOIS

WHOIS is the registry of all the domain names that have been registered. A good resource for translating IP addresses is available at http://www.whois.sc/. Enter the IP address or hostname in the blank text box, then click “lookup” to find out who owns that domain and their contact information.

Using the IP address from the e-mail header sample, 211.136.104.133, reveals the following about its owner:

person: Jinxia Sun

```
address: China Mobile Communications Corporation

address: 29, Jinrong Ave., Xicheng District, Beijing, 100032

country: CN

phone: +86-10-66006688-1755

fax-no: +86-10-66006012

e-mail: sunjinxia@chinamobile.com

nic-hdl: JS686-AP

remarks: ------------------------------

remarks: Please send abuse e-mail to

remarks: abuse@chinamobile.com

remarks: Please send probe e-mail to

remarks: security@chinamobile.com

remarks: -------------------------------
```

Other resources for a registry of domain names and translating IP addresses are http://www.whois.net/, http://network-tools.com/, and http://www.fr2.cyberabuse.org/whois/?page=whois_server.

Before using this contact information, go to the ISP contact list at http://www.haltabuse.org/cops/isplist.php (the password is cops); this is for law enforcement only and may provide better contacts. All ISPs are in alphabetical order.

If you don't find the ISP you're looking for there, then use the WHOIS information to contact the ISP.

Once the header code is deciphered it will lead investigators to the ISP, then to the owner of the e-mail address, and thus the cyberstalker. At this point, standard investigative procedures are followed.

Advice for the Public

Always select a gender-neutral username as an e-mail alias or chat nickname. Don't pick something cute, such as misskitty@isp.com, or use a first name if it's obviously female and never use your first and last names. Most online victims are female; and female identifiers are what some harassers look for.

Keep your primary e-mail address private. Use this only for people you know and trust.

Get a free e-mail account through someplace like Hotmail, Gmail, or Yahoo and use that for all your other online activity. Select a gender-neutral username that is nothing like anything you've had before.

Do not fill out profiles, or fill out as little as possible unless you want the whole world to know everything about you. When you sign up for your e-mail account, whether it's through your ISP (such as AOL) or a free one (such as Yahoo!), supply as little information as possible. You do not need to fill out everything they ask for. When you hit the submit button, you will be told what information is absolutely necessary to get your account opened. The same goes for profiles in IM programs such as ICQ, Messenger, AOL, and chat rooms.

Block or ignore unwanted users. You should always check what options and preferences are available and take advantage of the feature that blocks all users except those on your buddy/friend list, and be sure to add unwanted usernames to an Ignore list, if that is available. If anyone bothers you and won't go away, put them on block or ignore.

Don't defend yourself. Most people naturally want to defend themselves against inflammatory remarks, but a reaction is just what the harasser wants. She or he is fishing for someone to latch onto and harass. No matter how hard it is, ignore these people. When they realize they can't bother you, they'll go on to the next chat room or newsgroup and try to find another target.

Lurk (that is, read messages and don't respond or post) on message boards, groups, mailing lists, chat rooms, and so on, before posting messages.

Watch what you say online. When you do participate, be careful. Type only what you would say to someone's face. If you wouldn't say it to a stranger standing next to you in an elevator, why would you “say” it online?

Ego surf. Put your first name and last name in quotation marks in a search engine such as Yahoo! or Google and see if there are any results regarding you. You might be surprised at what you find. Also put in the names of your spouse, loved ones, and children. Remember to put their names in quotations to refine the search results.

Online Resources for Investigators

A complete list is available at http://www.haltabuse.org/cops/links.html.

Net Crimes & Misdemeanors

www.netcrimes.net

Sam Spade

www.samspade.org

SpamCop

www.spamcop.net

Google Groups Adanced Search

http://groups.google.com/advanced_search?q=&

Yahoo!

www.yahoo.com

Yahoo! Chat

http://chat.yahoo.com/

Yahoo! Groups (newsgroups)

www.yahoogroups.com

Yahoo! Member Directory Search

http://search.profiles.yahoo.com/

Yahoo! Personals

http://personals.yahoo.com/

What victims should do if they've been harassed.

www.haltabuse.org/help/respond.shtml

Current cyberstalking-related laws

www.haltabuse.org/resources/laws/

Victim questionnaire

www.haltabuse.org/help/question.shtml

Myths and legends of the Internet

www.snopes.com

J. A. Hitchcock is a cyber crime expert and the author of Net Crimes & Misdemeanors (netcrimes.net).

Topics

- Computer Forensics
- Network Forensics

Share this Story

Share on reddit Follow on Google+

3

Comments

Trending

Gingrich Declares First US Cyberwar Lost

2 comments · 6 days ago

Black Friday, Cyber Monday for Crooks, Too!

1 comment · 2 weeks ago

Ethical Decision Making

1 comment · 3 weeks ago

Exclusives

10 Inspiring Leadership Quotes to Live By in 2015

December 23, 2014 8:13 am | by Debbie Fletcher

Streamlining the Digital Forensic Workflow: Part 3

December 17, 2014 8:49 am | by John J. Barbara

Some DFIR for Sony Cybersecurity

December 16, 2014 9:56 am | by Ernie Austin, Newsletter Editor

Questioning North Korean Sony Breach Involvement

December 15, 2014 10:29 am | by Ernie Austin, Newsletter Editor

View More Exclusive Content

Current Issue

Fall 2014

September 25, 2014 5:19 pm

Blogs

Tips

There are still many unanswered questions about the recent attack on Sony Pictures Entertainment, such as how the attackers broke in, how long they were inside Sony’s network, whether they had inside help, and how the attackers managed to steal terabytes

The Case for N. Korea's Role in Sony Hack

December 24, 2014 9:25 am | by Editor

As retailers are in the grips of the last few shopping days of Christmas, they may not even know that cyber criminals quite literally have their eyes on their stores.

Backoff Malware Validates Targets through Infected IP Cameras

December 24, 2014 9:18 am | by Ericka Chickowski

An easy way to browse the internet in anonymity and privacy? Not so fast. 2014 made privacy into a business model — and spawned an overwhelming amount of unscrupulous charlatans eager to capitalize on a frightened public.