NW3C
National White Collar Crime Center

The Briefing

February 2015

Contact NW3C

NW3C Website
www.nw3c.org

Member Services
(800) 221-4424, ext. 3309
membership@nw3c.org

Investigative Support
(800) 221-4424, ext. 3328
krinker@nw3c.org

Training
(877) 628-7674, ext. 2234
training@nw3c.org

Find us on Facebook

Cybercop 101 – Basic Data Recovery and Acquisition (BDRA)

Learn the fundamentals of computer operations and hardware function and how to protect, preserve and image digital evidence.

Find out more:
www.nw3c.org/training/Computer-Crime/4

Online Chat Rooms and What Law Enforcement Should Know About Them

By Kim Williams

Chat rooms have existed on the Internet for years, but social media and technological innovations have added a new dimension to them in recent months. *Fast Company*, a magazine that focuses on technology and business, has labeled the chat room as the hot social media trend for 2015 ("Why Chat Rooms are Hot"). In the past, a chat room simply provided a space where people, usually with similar interests, could share ideas or "chat" online in real time. With improved technology, people in Internet chat rooms may now see each other via webcams and also share documents. However, they may still maintain their anonymity, which adds to the allure of these rooms for criminals.

The anonymous nature of participation in these rooms also makes them a good place for law enforcement to gather intelligence. Investigators can hang out and monitor activity without divulging their identities. A 45-year-old pedophile may pretend to be a 15-year-old Justin Bieber look-alike, but a law enforcement officer can pretend to be the child this pedophile would like to exploit.

Cyber-stalking is just one of the crimes taking place in chat rooms. Other criminal activities include:

- *Facilitation of drug dealing.* Buyers may request to see the goods before paying for narcotics.
- *Gang violence.* Gang members have been known to demonstrate dominance over a rival gang by torturing or even killing one of its members in a chat room.
- *Child pornography.*
- *Exploitation of children.* Online predators "groom" children by showing interest in and supporting them online. Their aim is to get the children to trust them enough to meet them so they can then sexually abuse them.
- *Facilitation of terrorism.* Terrorist groups, such as ISIS, use chat rooms to recruit new members, solicit money and provide instructions to would-be terrorists, such as how to make bombs.
- *Hate crimes.* Similar to terrorists, hate groups use chat rooms to recruit new members and promote crimes against those they dislike.
- *Hacking.* Through social engineering or by exploiting computers already infiltrated by botnets or other malware, hackers in chat rooms may obtain passwords and user names, access files, and control computers, either for mischief or to perpetrate fraud, such as identity theft.

Like other social media applications, the number and variety of chat rooms is constantly expanding. Below is a list of some of the chat rooms currently available:

- *Banter*^{TM} - Founded in 2014, Banter is a free mobile app that allows users to join or create rooms. Public rooms are open to all and messages left in them will be available

Continued on page 2

72 hours after posting. Private rooms are used for confidential messages, which will be available for six months after posting.

- *Rooms®* - Launched by Facebook in October 2014, Rooms is a free app that allows users to create chat rooms for shared interests. It is separate from Facebook and doesn't require details such as a real name or location. Chat room entry requires codes that "can be shared on social media, email or even posted on paper in public spaces." (http://time.com/3534690/facebook-anonymous-app-rooms/)
- *Tinychat®* - Tinychat is designed to facilitate streaming real-time audio and video among a group of up to 12 individuals. Participants may remain anonymous.
- *ooVoo™* - For use on the PC, Mac or mobile devices, ooVoo allows participants to video chat with up to 12 people. Users can also send video messages and instant messages and record and upload videos to YouTube.
- *Buzz50* - Buzz50 offers chat rooms targeted to people over the age of 50, although anyone may participate.
- *Slack®* - Boasting over 250,000 users, Slack provides a central chat room for employees to share messages, photos and company updates.
- *Google Hangouts®* - Hangouts may be used for live video conversations with up to 10 people.

In the same way that child predators "groom" children in these chat rooms, law enforcement can "groom" the criminals.

- *MeowChat* - MeowChat is a mobile app that allows users to send text, images or audio clips and participate one-on-one or in group chats with strangers near their location.
- *Chatroulette®* – Chatroulette is an online chat site that pairs random people worldwide for webcam-based conversations. If unhappy with a particular chat, users can choose to go to the next chat, stop the chat or report it.
- *FireChat™* – FireChat allows smartphones to connect without an Internet connection. It became popular in Iraq following government restrictions on Internet use and in Hong Kong during recent civil protests.
- WhatsApp™ - WhatsApp Messenger is a mobile messaging app that allows users to create groups and send images, video and audio media messages.
- *TagsChat* - Currently in its beta version, TagsChat calls itself the "interest-based social network," It allows users to build a profile with a nickname and "tags," which represent interests. Users login anonymously and chat live with people with the same tags.
- *WeChat™* – WeChat (known in China as Weisin) boasted 468 million monthly active users (most in China) at the end of the 2013 third quarter.

How Law Enforcement May Gather Information in Chat Rooms

Even though many chat rooms allow their participants to remain anonymous, there are numerous methods to find out about the people within them. One of the primary ways investigators gather intelligence is simply by visiting these rooms and taking part in discussions. NW3C Computer Crimes Specialist Norm Gibson previously served as a Deputy Sheriff with the Wayne County (MI) Sheriff's Office and he provided insight for this article. As part of his work with the Sheriff's Office, he investigated pedophiles and spent time tracking them in chat rooms. His work led to the arrests of 30 men who thought they were talking to a 13-year-old girl, not the Deputy Sheriff. Gibson noted that in the same way that child predators "groom" children in these chat rooms, law enforcement can "groom" the criminals. By acting the part of a pre-teen, the investigator can build trust and rapport with the pedophile. If all goes well, a meeting can be set, and then the arrest can be made.

Gibson said he would enter an online chat room using a girl's name and just sit there. Invariably, someone would approach him and start a conversation. He noted that he would simply answer questions, without adding a whole lot to the dialogue. When the man found out he was talking to a 13-year-old girl, often he stopped the conversation, but sometimes he didn't. The men who were undeterred by the fact that they were speaking with an underage girl were the likely pedophiles. Sometimes Gibson would ask for a picture, name, etc. If the man refused, Gibson would say "bye" or "go away." Surprisingly, many of the men would then come back into the room and provide the picture or information requested, allowing the investigation to progress.

Gibson noted that a lot of information may be gathered through the chat room dialogue. In one instance, he screen captured a picture of the man he was talking with via webcam. He found out through his conversation that the man went to a local high school. Gibson went to the library, found the high school yearbook and matched the photo the man provided with a photo in the yearbook. He then knew the man's name and was able to find out where he lived and eventually make an arrest.

Law enforcement may also gather information by following conversation threads, looking through the archives—if kept—to review conversations the suspicious person has had with others. A pattern pointing to illegal activity may reveal itself.

In addition, intelligence may be gathered in chat rooms via other surveillance techniques. For instance, if a "direct connect" has been established, the investigator can see who is connected to his or her computer by downloading and using Sysinternals™ software (which is free). A one-on-one chat often allows the suspect's Internal Protocol (IP) address to be visible. A website, such as www.Arin.net, will provide more information about an IP address, such as the network administrator. Then the investigator will be able to obtain a search warrant and access more information.

NW3C's Social Media 201 course (Cyber Investigation 201 – Social Media & Technical Skills) includes hands-on instructions about how to resolve IP addresses. For more information, please visit http://www.nw3c.org/training/Computer-Crime/100.

Sources

- *General chat room Info: www.mediasmarts.ca/backgrounder/are-you-web-aware-chat-rooms*
- *The Briefing, September 2013: www.nw3c.org/News/the-briefing/page/2*
- *Why Chat Rooms are Hot: www.fastcompany.com/3040220/elasticity/why-chat-rooms-are-the-hot-social-media-in-2015*
- *ISIS uses chat rooms for recruitment: www.timesofindia.indiatimes.com/india/Radicalized-on-net-chat-room-given-Mosul-contact-ISIS-man/articleshow/45322203.cms*

Anonymous and Ephemeral Apps Pose Challenges for Users and Law Enforcement Alike

by Ty Bowers

In recent years the rise of so-called "anonymizing" or "ephemeral" applications has presented a number of challenges for citizens and law enforcement alike. The appeal of smartphone apps like Snapchat®, Yik Yak® and Whisper, especially among teenagers and twentysomethings, is rooted in an alluring blend of personal anonymity and wide-ranging social interaction. The fact that few adults or authority figures truly understand how these applications work only adds to their growing popularity.

Anonymous applications, like Yik Yak and Whisper, for instance, allow users to post and share information anonymously with others in a particular geographic area or as part of a larger social group. Apps like Snapchat deliver content with built-in expiration dates, meaning a "snap" (what posts in the app are called) will disappear after being opened by the intended recipients, or if it remains unopened for a pre-determined period of time. Many experts suggest the rise in popularity of these types of applications stems from online users' privacy concerns in an age of unprecedented digital surveillance by individuals, companies and governments. "For one, teens have been listening to adults who have warned them for years about the potential permanence of their digital footprint (digital tattoo, really), and they are looking for ways to interact with others without the stress of having to worry about how a future employer or mother-in-law might judge them based on previous online indiscretions," cyberbullying researcher Justin W. Patchin wrote in December 2014. "Apps like Yik Yak, Ask.fm, Snapchat, and numerous others, can fill this role."

The wide-open, virtually authority-free ecosystems these anonymous networks and content streams provide, however, have many parents, educators and law enforcement professionals worried. "Critics maintain that anonymity is a double-edged sword. While it lets the public frankly discuss issues they might not otherwise in an open forum, cloaking one's identity leads some to believe they can tease and troll others at will," the publication Adweek posited in its September 2014 Social Media Issue. "This is especially true among kids, teens and adults in their early 20s—groups not known for their restraint and self-control."

Incidents of threats and bullying have dogged the rise of these applications almost from the start. One app, After School, was pulled from Apple's App Store in December 2014 (less than two months after it first became available for download) after numerous reports of cyberbullying at schools. Similar complaints followed the release of Yik Yak as well, which led the company to create a mechanism that allows elementary, middle and high schools to request that a "geofence" be erected to prevent the app from working on school grounds.

While many of these applications offer the promise of anonymity – most do not require a name or other identifying personal information to function – they do track location data, store images and other content on their servers and retain registration information, all of which law enforcement personnel can obtain via search warrant when investigating threats and other potential criminal acts. Furthermore, the apps themselves, like any other type of software, can be compromised. "The risk you take when you trust these apps with your sensitive data or information is that you can't really be sure of complete privacy, or that private data is actually going to stay private," infosecurity firm Trend Micro™ wrote on its Security News blog in November 2014. "When people start to believe that the data they shared will be gone or will remain hidden forever, who cares about secure passwords or a patched device? Truth is: Anonymity is not that simple or easy, especially not on the internet."

Due to potential security concerns and a desire to demonstrate they value users' safety, many of these apps have developed specific protocols for law enforcement seeking evidence of wrongdoing. The terms and conditions of each service usually spell out what kind of information can be made available to law enforcement through legal process.

- For Yik Yak, legal information is available via www.yikyakapp.com/legal/. The company cannot provide a phone number, name or email address for its users because it does not collect that data. The company can provide law enforcement with the locations of where a person has posted to the network, which may help in terms of identification of suspects or witnesses.

- Snapchat's Community Guidelines feature an entire section on abuse and safety: https://support.snapchat.com/a/guidelines. Of note to law enforcement, however, is the fact that once a "snap" is opened by all of its recipients, it is deleted from the company servers. Deleted photos may be recoverable from some smartphone models. Access to unopened "snaps" may also be obtained via warrant under the requirements of the federal Electronic Communications Privacy Act (ECPA). Time is of the essence, though. The company only retains unopened "snaps" for a period of 30 days.

- Whisper has developed a detailed Law Enforcement Response Guide: www.whisper.sh/legal.

Each app has its own processes and terms, its own technological quirks and limitations. Understanding how each of these applications works and how they are typically used is the best way for adults and law enforcement to determine how best to safeguard young people.

NW3C Analyst Nikki Black contributed to this report.

Notes:

1. *"Yakety Yak: What's Up With Yik Yak?" by Justin W. Patchin, Cyberbullying Research Center, December 19, 2014: www.cyberbullying.us/yik-yak-revisited/.*
2. *"Anonymous Apps Like Whisper and Secret Have a Dark Side: Abusive language and bullying have brands proceeding with caution," by David Gianatasio, Adweek, September 15, 2014: www.adweek.com/news/advertising-branding/anonymous-apps-whisper-and-secret-have-dark-side-160107.*
3. *"After School Is The Latest Anonymous App Resulting In Student Cyberbullying And School Threats," TechCruch, December 3, 2014: www.techcrunch.com/2014/12/03/after-school-is-the-latest-anonymous-app-resulting-in-student-cyberbullying-and-school-threats/.*
4. *Yik Yak Geofence request form available via the company's support page: www.support.yikyakapp.com/.*
5. *"Instant Anonymity: Are Ephemeral Apps Really Safe?" Trend Micro Security News, November 4, 2014: www.trendmicro.com/vinfo/us/security/news/online-privacy/instant-anonymity-are-ephemeral-apps-really-safe.*
6. *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22: https://it.ojp.gov/default.aspx?area=privacy&page=1285.*

NW3C Featured Course: Cyber Investigation 201 – Social Media & Technical Skills

This two-day course, funded by the Bureau of Justice Assistance (BJA), is intended for law enforcement personnel who want to further their education about social media investigative techniques and best practices for conducting an online investigation. It aims to provide law enforcement with the technical skills and training needed to utilize information found on popular social media platforms.

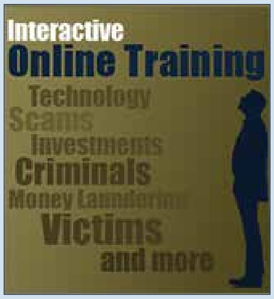
It provides hands-on instruction, walking investigators through many of the sometimes highly-technical details involved when working cyber investigations.

Topics include:

- Basic Internet investigations
- Popular social media sites
- Social media intelligence
- Online investigative tools
- Resolving Internet Protocol (IP) addresses
- Understanding the URL address
- Building an undercover online profile

There are four courses scheduled from May through October 2015. Find out more and register at: www.nw3c.org/training/Computer-Crime/100.

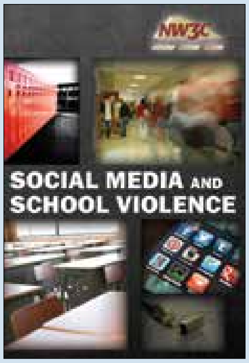
Overview of White Collar Crime



This new online class covers a variety of topics related to white collar crime. Find out more:

www.nw3c.org/training/online-training/114

Social Media & School Violence



This six-part video series provides information about social media trends and other material designed to help law enforcement who work with youth.

www.nw3c.org/training/specialty-training/social-media-and-school-violence

On Demand Training

NW3C offers free online classes to law enforcement.

Find out more at: www.nw3c.org/training/online-training

This project was supported by Grant No. 2012-MU-BX-4004 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.. The National White Collar Crime Center (NW3C) is the copyright owner of this document. This information may not be used or reproduced in any form without express written permission of NW3C. For questions or additional information, please contact Kimberly Williams, Communications Manager, at 1-800-221-4424 ext. 3320 or kwilliams@nw3c.org. NW3C ™ is a trademark of NW3C, Inc. and may not be used without written permission.

Photo Credits: 193316678 Copyright Andrey_Popov, 2015 Used under license from Shutterstock.com; 226114804 Copyright Vdovichenko Denis, 2015 Used under license from Shutterstock.com; 231888469 Copyright Mathias Rosenthal, 2015 Used under license from Shutterstock.com