INVESTIGATION REPORT

Agency	BU Cybercrime Investigation Division	**Investigator**	Katie Barnes
Address	1010 Commonwealth Avenue, 5th Floor Boston, MA 02215	**Case Number**	U1000407
		Date of Report	06/15/2021

Details of Case

On or about January 1, 2012, Michael A. Berenson and a group of co-conspirators worked together with an objective to produce child pornography in a chatroom website. Michael A. Berenson and his co-conspirators knowingly engaged in a child exploitation enterprise by violating Chapters 110 and 117

of Title 18 of the United States Code (specifically 18 U.S.C. § 2251, 18 U.S.C. § 2422(b), and 18 U.S.C. § 2252A) (*United States vs. Berenson*, 2017). As far back as 2012, Michael A. Berenson and his co-conspirators engaged in explicit conduct, as defined in 18 U.S.C. § 2256 (2), on web cameras to record sexually explicit video footage (*United States vs. Berenson*, 2017). They worked together to produce videos of minor victims engaging in sexual acts. This case is connected to a purported long-running "sextortion" ring investigated by the Federal Bureau of Investigation (FBI). As of November 1, 2015, Michael A. Berenson is under investigation for sexually exploiting children under the ages of 18 and is believed to be using sexually explicit images and/or video footage to blackmail his victims.

Actions Taken

Task 1: As an agent of the Federal Bureau of Investigations (FBI) I utilized our Internal Database to perform a keyword search for any previous cases associated with Mr. Berenson along with any possible aliases, but the search did not return any results at this time for Michael Berenson.

Task 2: I conducted a search of Michael A. Berenson through an open-source intelligence link better known as OSINT. During this search I found that an alias name listed as "Quagmire" in private chat rooms on a website named "*Chateen.com*" based in Spain and is linked to Michael A. Berenson. I discovered Mr. Berenson's name listed in the Dark Web as the result of an online hacking game where the users hack one another's real names. The tools I used to find such information through OSINT were Maltego, Recon-ng, theHarvester, Shodan, Metagoofil, Searchcode, Spiderfoot, and Babel X (Breeden, J. 2020). I have reason to believe that Michael A. Berenson is using the Dark Web for anonymity to hide his real identity and to participate in illegal activities against minors in private chat rooms.

Task 3: Following a chain of command all evidence collected in this case have been preserved and analyzed by officers with the credentials and expertise in forensic science specifically in a digital forensics background. I have reviewed the evidence through a process called hashing. The common algorithms used are called MD5 (Message Digest 5) and SHA256 (Secure Hash Algorithm 256)' this process is comparable to DNA evidence as no hash value is the same and impossible for any two files to have the same hash (Graham & Smith, 2020). This evidence can be presented in front of a judge as I have reason to believe that the Email messages linked to Mr. Berenson contain illegal audio, video, and photographs. I have also recovered deleted Emails revealed through hashing that contain threatening messages that were sent to minors under the age of 18. All hash values have been preserved and ready for digital forensic presentation in court.

Task 4: I verified the privacy levels of each of the accounts and
profiles provided through the OSINT platform that are associated with the detected criminal activity. It appears that Mr. Berenson has several accounts such as his Google home page, Facebook, Twitter, Tiktok,

Snapchat, Instagram, and LinkedIn account. All these social media platforms are private except for Google and Facebook which are public for all to see. After clicking on the suspect's Facebook profile picture there was a link provided on Mr. Berenson's timeline that led to the TOR browser. The TOR browser is an anonymous browser used to search the internet freely without any trace or connection to the user other than the installation of a TOR browser. The Onion Router (Tor) provides anonymity online to allow the user to browse cyberspace anonymously (Lee, 2021). Following the link there are instructions after installation of the TOR browser to follow an encrypted link revealing the website "*Chateens.com*" on this website are thousands of pornographic videos and pictures of underage children ranging from ages 8 to 14 years old.

Task 5: There is a forum on this website that was reported by an underage female victim who identifies the name of the man who threatened her through Email as Michael Berenson via Berenson20@gmail.com. The photograph of Michael Berenson matches the photographs on Mr. Berenson's Facebook account. Additionally, I was able to link Mr. Michael A. Berenson's personal Gmail account to his Facebook account as a match to the hash values listed in **Task 4**.

Task 6: While the forum listed under the dark web @ "*Chateens.com"* was available for chat with an alias connected to Mr. Berenson listed as "*Quagmire*" I requested permission from Chief Bradshaw to authorize placement of our undercover officer Detective Rosa to utilize his undercover profile which has been undercover for 5 years using the same screen name with other suspects in this case. The username is well known to forums and chat rooms and has sufficient history to be trustworthy of the suspect in question. Our undercover officer will begin to initiate and engage in live chat with Mr. Michael A. Berenson upon the approval of Chief Bradshaw.

Task 7: Approval from Chief Bradshaw has been provided and Detective Rosa has agreed to initiate live chat with the username *"Quagmire*" who is believed to be Michal A. Berenson. The username of our detectives is kept confidential and classified thus, I cannot provide information of the screen name of our detective however all chats are preserved and ready for use in a court of law under the approval of our department. All identities of our detectives are kept confidential to protect the well being of our detectives, their families, and our staff. Furthermore, we keep information pertaining to the case confidential to protect the case while investigation is in progress.

Task 8: I have requested a court ordered subpoena to Mr. Berenson's Verizon cell phone provider and Comcast internet provider to perform selective database searches of any wireless cell phones, landlines, and to provide any data pertaining to communications, traffic, and other data such as downloading and uploading files.

Task 9: The approval of the court order has been granted by Chief Bradshaw and I am following through with the initial request for all applicable data.

Task 10: Detective Rosa is continuing to act as an undercover agent on the case and is currently active under his classified username. He is currently preserving logs of every encounter of conversation or contact for the court report. The username of Detective Rosa is reserved for court appearance as default "JOHN1234" to represent our officer partaking in conversation. However, the actual username is for FBI use only and will not be revealed otherwise.

Task 11: Update of **Task 8** Our Bureau received cooperation from both Verizon and Comcast releasing data for communications, traffic, downloading and uploading of wireless cell phones, and landlines. Both providers have agreed to provide additional information such as GPS data and originating location of illegal internet data. However, our Bureau ran into a speed bump as "*Chateen.com*" reported by Comcast Communications is listed as originating in Spain. Chief Bradshaw granted a court order to retrieve more information of data through Spain authorities.

Task 12: Update Task 11 Spain authorities approved subpoena and access to all requested data pertaining to *"Chateen.com"*. I introduced Digital Forensic Expert Mr. Novak to our investigation team. Mr. Novak introduced a variety of different software programs but found Encase, Autopsy, FTK Imager Lite among the most useful software programs in this investigation. In our digital forensic investigation Mr. Novak was able to reveal E-Mail addresses affiliated with Mr. Berenson, originating location of "*Chateen.com"*, originating location of the computer devices used to commit the crimes.

Task 13: After reviewing all reports and evidence I was able to reveal other suspect's identities and thousands of underaged victims. I have confirmed that the website "*Chateen.com* is used as an illegal child exploitation enterprise platform. Also, the website's administrator was revealed to be Mr. Michael A. Berenson. Earlier in the investigation I used OSINT to help with the search of any aliases for Mr. Berenson and received the alias listed as "*Quagmire*", this username has been confirmed through forensic software as the alias of Michael A. Berenson used on "*Chateen.com"*. Forums and private chats logs reveal this discovery.

Task 14: I reviewed the records for time zone conversion, ISP identification, and submitted all undercover activities. Although the originating website is listed in Spain, there has been no change in time zone information.

Task 15: I have completed the investigative report and revealed the identities of Mr. Michael A. Berenson A.K.A *"Quagmire*", and several co-conspirators. I revealed the ISP addresses of the criminals involved in the case and over 1000 potential victims in hopes of bringing justice to the victims and their families.

Task 16: To be sure that I was not missing anything I performed a second search which revealed The ISP originating location of Mr. Berenson's computer device. The device was traced using forensic software to an address that was listed under Mr. Berenson's birth mothers name which has been added to the report. Additionally, it has come to my attention that Mr. Berenson has been using Skype to interact with underage girls on live webcam. Additionally, our team has discovered that there are over 100 identified victims, but the others are unknown.

Task 17: Detective Rosa recorded other interactions with another undercover agent, but the interaction was not useful to the case.

Task 18: My investigative team has confirmed factual evidence that proves probable cause in this investigation, as we have reason to believe that Mr. Michael A. Berenson and several Co-conspirators, through the periods of at least January 2012- November 2014, Mr. Berenson created an illegal website named "*Chateen.com*, to lure young teen girls using his original Facebook account and other apps in his cell phone like Tiktok and snapchat accounts to join his illegal website for private chat. This site was under the anonymity of the dark web hidden from law enforcement officials to illegally record explicit videos and photographs of underage girls. Mr. Berenson and his accomplices pretended to be teenage boys, target victims on other social media platforms, and work together to pressure victims to engage in masturbation, and other sexual acts in a web-based chatroom (United States v. Berenson, 2020). Moreover, Mr. Berenson used the Skype video web camera platform to entice and engage in live sexual encounters with underage girls. Mr. Berenson and accomplices conspired to commit at least 8 felony crimes. The felonies have been listed below as follows:

Count One- Child Exploitation Enterprise, 18 U.S.C. § 2252A (g)
Count Two- Conspiracy to produce Child Pornography, 18 U.S.C. § 2251(a), 2251 (e)
Count Three- Production of Child Pornography, 18 U.S.C. §§ 2, 2251 (a)
Count Four- Production of Child Pornography, 18 U.S.C. §§ 2, 2251 (a)
Count Five- Coercion and Enticement of a Minor 18 U. S.C. §§ 2, 2422 (b)
Count Six- Coercion and Enticement of a Minor 18 U.S. C. §§ 2, 2422 (b)

Count Seven- Conspiracy to Receive Child Pornography, 18 U.S.C. §§ 2252A(a)
Count Eight- Conspiracy Access with Intent to View Child Pornography 18 U.S.C. §§ 2252A(a)(5)(B), 2252(b)(2) (*United States vs. Berenson*, 2017).

Task 19: 11/01/2014- a search warrant and arrest warrant have been issued by United States District Court Eastern District of Michigan. The warrants allow a search to seize all electronic devices including mobile devices, documents, photographs, VCR Tapes, digital cameras, any form of web cameras, USB devices or floppy discs, or any hard drives or detachable/removable devices, or any device capable of storing images, video, or audio located inside 779 Washington St. Detroit Michigan, 48127 the home of Michael A. Berenson.

Task 20: The arrest warrant and search warrant are in place and ready for submission to the proper authorities to apprehend Mr. Michael A. Berenson so that he can stand trial and face the charges that are represented against him. All agents, detectives and forensic experts are prepared to stand trial to prosecute Mr. Michael A. Berenson for his crimes against the United States of America and all his victims.

Task 21: Despite limited funding for the case our team did a tremendous job keeping within budget guidelines, following tactical efforts in a timely manner and sticking to protocol. The members of our investigation team always remained professional and followed a chain of command to ensure the integrity of the case. Each member of our team kept daily logs of every event that contributed to every effort. We implemented strategies to take down members of the exploitation ring and succeeded in exposing many of them. What felt like endless hours of work resulted in about 600 hours of contribution that led to the arrest of Michal A. Berenson and the dismantling of the illegal website "*Chateen.com*". At the time of search and seizure we were able to retrieve enough evidence to seal the charges against Mr. Berenson, and to prosecute him and with his Co-conspirators. We were able to retrieve a computer belonging to Michael A. Berenson, digital cameras, photographs, live video footage, and text messages as proof to combine with the rest of the evidence gathered throughout the investigation.

Summary

Chief Bradshaw suggested that I take over this investigation since Detective Rosa and I have interacted with several criminals connected to this case during several interactions through various chat rooms while undercover. I completed 21 tasks for this investigation which is protocol and standard procedure for criminal investigations in the Federal Bureau of Investigations (FBI). I performed a keyword search in the beginning of the investigation through our internal database for previous crimes, or encounters with the law for Mr. Berenson. I proceeded to use other sources to conduct my investigation such as using the OSINT platform to find preserved digital evidence on various social media websites.

Our team reviewed metadata and collected hash value information from data recovered. We conducted searches on social media sites and hidden browser contents and discovered an illegal enterprise in which Mr. Berenson turned out to be the administrator of the website "*Chateen.com*". All evidence used against our suspect was completely useful and led to his arrest at his home. Our teams' budgets plans were implemented and were successful. The work of our investigation team was impeccable, and we were pleased with the results of the case. We are thankful to the victims that came forward in the case to help those who have yet to find justice for their families. This case is connected to a much larger case and that of Amanda Todd, a 14-year-old victim who was also a victim of the child exploitation enterprise. She is a victim of one of the Co-conspirators of this investigation. Unfortunately, Amanda Todd commit suicide in 2012 after dealing with bullying and depression caused by Berenson and several unnamed criminals in this case. Aydin Coban is one of Berenson's many Co-conspirators and has been indicted in the case of Amanda Todd thanks to our

courageous team of investigators who are continuing to work every day with ongoing investigations to take down this massive child exploitation ring.

References

Breeden, J. (2020 September 15). *8 Top Open Source Intelligence Tools.* IDG Communications, California.

Accessed on June 18, 2021 from https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html.

Graham R, Smith S, (2020). *Cybercrime and Digital Deviance.* Routledge, New York, NY.

Lee, H. (2021) Module 6: *Criminal Procedure and Digital Evidence*. Boston University Metropolitan College

United States vs. Michael A. Berenson, No. 16-20239 (6th Cir. Aug. 03,2017)

United States v. Berenson, No. 19-1550 (6th Cir. Nov. 10, 2020)