https://doi.org/10.48009/1_iis_2013_27-36
Issues in Information Systems
Volume 14, Issue 1, pp.27-36, 2013

THE RISE AND FALL OF CABINCR3W: HOW SIMPLE MISTAKES DOOMED A HACKING GROUP

William Stanley Pendergrass, Robert Morris University, Wspst2@mail.rmu.edu
Robert Joseph Skovira, Robert Morris University, Skovira@rmu.edu

ABSTRACT

The hacking group CabinCr3w emerged in conjunction with the Occupy Wall Street movement in late 2011. Initially they were solely involved in releasing personal information or "dox" on Wall Street investment bankers and other individuals who were involved in facilitating the "Great Recession." However in November of 2011, under an operation they dubbed Operation Pig Roast, CabinCr3w increasingly turned their attention to hacking law enforcement organizations and government institutions across the country. In March of 2012, two of the most active members of the group were arrested and charged with several high-profile hacks. An analysis of secondary data in the form of news articles and unsealed Criminal Citations reveals that both hackers made fundamental and basic mistakes in preserving their anonymity, which law enforcement officials used to connect their online identities to their physical locations.

Keywords: Hackers, Hacking, Hacktivism, CabinCr3w, Anonymous, Dox and Occupy

INTRODUCTION

2011 was a watershed year for hacktivism. Beginning in December 2010 and continuing on into 2011, the hacker collective Anonymous was involved in what they called Operation Payback. Payback had initially started in the fall of 2010 as a protest in support of pirating Bollywood videos. However with the Wikileaks release of confidential Defense and State Department communications and the government's insistence that financial institutions deny their services to WikiLeaks, thousands of Anonymous supporters participated in Distributed Denial of Service (DDoS) attacks on those institutions. The relentless bombardment of DDoS requests forced VISA, MasterCard, PayPal and others' websites offline. In the spring of 2011, a hacking group who called themselves LulzSec ran rampant for 50 days releasing data taken from a number of seemingly random websites. Later that year, Occupy Wall Street began and Occupy protests and rallies were held across the county to protest corporate greed. As all these protests sprang up over the course of the year, so too did other hacking groups with varying agendas from the larger Anonymous collective.

One such group which appeared briefly in 2011 and 2012 called itself CabinCr3w. CabinCr3w began as a support element of the Occupy Wall Street demonstration. Early on they were very successful in releasing personal information and documents, abbreviated in hacker terminology as "dox", on a number of top Wall Street investment bank Chief Executive Officers (CEO). This collaboration fit well with the Occupy movement's purpose which was to draw attention to the perceived greed and wrongful practices of Wall Street and other banks across the country. However CabinCr3w began to change their tactics and aim in late 2011 when they increasingly began to target law enforcement organizations across the country in what they called Operation Pig Roast. Finally in March of 2012 it all came to a sudden end when the two main members of CabinCr3w were arrested and charged for the computer crimes they had allegedly committed. What went wrong with their operation? How were they caught and what mistakes, if any, did they make which led to their arrests? These are some of the questions this research paper investigated.

RESEARCH METHODOLOGY

This research project was part of a larger project which studied Anonymous. Because of the nature of Anonymous and its activities, it would be problematic to be able to conduct direct observation of hacks or individuals participating in them. As such, as well as for the reason to remain clear of any legal issues, only secondary data was collected and evaluated. However the amount of secondary data collected proved to be its own unique problem; there was so much data with little consistency to it. For this reason, a case study methodology was selected as the

method for data analysis. Yin [41] posits that "case studies are the preferred method [of analysis] when (a) "how" or "why" questions are being posed, (b) the investigator has little control over events, and (c) the focus is on a contemporary phenomenon within a real-life context." [41]

Yin [41] defines three principles of data collection: use multiple sources of evidence, create a study database, and maintain a chain of evidence [41] This study used multiple sources of evidence in the form of news articles, Twitter posts, unsealed Federal Court documents, PasteBin posts and other types of secondary data freely available to the public. A timeline of events with links to the internet source both created a study database and maintained a chain of evidence. This timeline was referenced for this study and forms a diagram of events as the occurred. One method of analyzing the database was by separating the data into categories that could be further described. Yin [41] discusses a 1929 study which created descriptive bins to sort out a huge amount of data. In *Middletown: A Study in Modern American Culture* [21] descriptive categories were defined so that data taken from a small Midwestern city could be filtered to create an image of an "average" American city. Much in the way that study sorted gathered data, this study used descriptive bins to analyze the events of CabinCr3w. The descriptive categories include a brief timeline of events of the group CabinCr3w followed by a detailed analysis of unsealed Federal Court documents which detail the chain of events and evidence which led to the arrests of CabinCr3w members and Twitter users @AnonW0rmer and @ItsKahuna. This analysis allowed the following research questions to be answered: How did CabinCr3w begin and end and were there mistakes they made which facilitated the end?

RESULTS

CabinCr3w

On September 14, 2011, the @CabinCr3w Twitter account was established and CabinCr3w was born. Their first tweet was "Just DDoSed Twitter as a welcome to twitter!" [4]. From their start, CabinCr3w was very supportive of the Occupy Wall Street movement [5]. On September 24th, New York Police Department Deputy Inspector Anthony Bologna was caught on camera pepper-spraying two Occupy Wall Street protesters. The video was posted online and quickly went viral. CabinCr3w posted Inspector Bologna's personal information and documents, also known as dox, online on the 26th [20, 22]. By doxing Inspector Bologna, CabinCr3w had begun its direct collaboration with Occupy Wall Street.

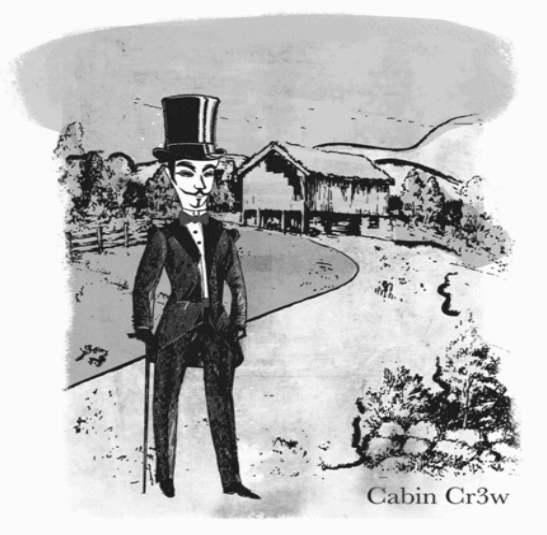

Figure 1. Twitter profile picture for @CabinCr3w

The next day, CabinCr3w released dox for Investment Bank Goldman Sachs CEO Lloyd Blankfein. CabinCr3w's Twitter account linked to a PasteBin post with Blankfein's age, recent addresses, and details of litigation he had been involved in as well as registration information for businesses [23]. Next, CabinCr3w released dox from the CEO of JP Morgan, James Dimon. Information released included addresses, family and business connections, political contributions and legal information [24]. On October 11, CabinCr3w released dox from two more Wall Street bankers, Joseph Ficalora, CEO of New York Community Bancorp and Kerry Killinger who left Washington Mutual before it collapsed in 2008. Killinger had been given more than $25 million in compensation that year, to include a $15 million severance payment [25].

After two dozen Occupy Wall Street protesters were arrested for disturbing the peace after trying to close their Citibank accounts in support of Occupy's Operation Cash Back, CabinCr3w released dox on Citigroup CEO Vikram Pandit on October 18th [7]. On October 24th they released dox on former Citigroup and Goldman Sachs executive Robert Rubin. Rubin was Treasury Secretary under President Clinton when the banking reform Glass-Steagall Act was repealed [26].

November 21st, CabinCr3w launched Operation Pig Roast with the release of dox of the Police Executive Research Forum's directors and members for their involvement in the police crackdowns of various Occupy protests across the country [33]. On November 30th, Twitter user @ItsKahuna tweeted a link to a PasteBin post which contained names, usernames, passwords and other sensitive data taken from a number of websites: four websites of the Italian and Bhutan governments, theredearsweb.com, evidalia.es, sitcomsonline.com, a real estate company in Texas and the Bishop McDevitt Catholic High School. Also, customer payment and medical information was taken and posted from a cosmetics website. @ItsKahuna claimed to have conducted the raids because he was bored but also wanted to demonstrate lax security protocols on websites [16].

On December 9th, CabinCr3w teamed with Anonymous and posted dox on more than 40 officers of the Los Angeles Police Department (LAPD); their statement explained their reasoning. "For the irresponsible posting of a crime scene photo, laughing at protesters while they were being arrested at #OccupyLA Raid, and being part of the LAPD/FBI. While you can operate in "grey" areas, so can we. Enjoy." [30]. This operation was unique in that it was the first announced pairing between Anonymous and CabinCr3w.

On December 18th, after reading about an Equal Employment Opportunity Commission ruling against G2Secure Staff which he considered insufficient, @ItsKahuna hacked into G2Secure's website and posted the details he found on the servers to act as additional punishment. Details included 63 administrative and executive email addresses, hashed passwords, names and access levels as well as the names, email addresses, addresses, and phone numbers of more than 8,000 of their employees [17].

With the start of 2012, CabinCr3w continued to shift its tactics more and more away from just releasing doxes to more traditional hacking techniques; i.e., Structured Query Language injection (SQLi) intrusions where actual server data could be accessed for release. On January 1st, the server details of the Indonesian Ministry of Trade were posted [14]. On January 19, 2012, unbeknownst to Administrators, the computer servers that hosted the Utah Chiefs of Police Association website, www.utahchiefs.org, were compromised by a SQLi hack. The names, email addresses and hashed passwords of approximately 24 Utah Chiefs of Police were posted and the link tweeted by @ItsKahnuna [35]. Later that month, on the 31st, Administrators of the Salt Lake City Police Department's (SLCPD) website, slcpd.com, noticed that three extra pages had been added to their website. After reviewing their logs, they noted over 18,000 connections from a single IP address. Administrators shut down the website while investigating the breach. Later that day, @ItsKahuna tweeted that over 1,000 usernames and passwords had been hacked from the website [27, 29, 35]. The SLCPD's hack was purportedly conducted in protest of a proposed Utah bill, SB107, which would make the possession of graffiti tools such as spray paint a misdemeanor if they were intended for the purpose of defacement [27].

CabinCr3w posted dox information of more than 150 police officers obtained from an old website for the West Virginia Chiefs of Police Association on February 6th [1]. Their posted announcement stated their reasoning for the hack.

> Database Drop - OpPiggyBank By w0rmer & @CabinCr3w #OpPiggyBank #CabinCr3w #Anonymous Dear citizens of West Virginia: As of late we have been watching cases of Police Brutality against the general pulic [sic] with a piqued interest. We have been taking notes while watching police departments across the United States become more militrarized [sic] and weaponized at our expense. The CabinCr3w has not been idle, the fire has been lit, and those in attendance are just getting warmed up. We are here to remind you that we the taxpayers pay your exorbitant salaries, and those salaries of your officers. Your job is to protect and serve, not brutalize the very people that pay your wages. Muzzle your dogs of war, or we will expose more of your sensative [sic] information. [19]

On February 9th, CabinCr3w hacked Alabama police and government websites and released dox of more than 40,000 people; CabinCr3w announced that the release was in protest of Alabama's immigration laws. In the Alabama Department of Public Safety hack, dps.alabama.gov, seven spreadsheets were posted with information on sex offenders along with limited information on the victims and the crimes, as well as a database listing offenders' automobile make, model, and license plate numbers. The post included the Twitter handles related to the crew, @ItsKahuna @CabinCr3w and @AnonW0rmer. They also hacked into the National Crime Information Center database, the Texas Department of Safety and the City of Mobile Police Department [9, 20, 28, 40]. On February 9th, CabinCr3w member W0rmer tweeted links to several pictures which showed various body parts of his girlfriend in a blue bikini top, shorts and panties. The photos had signs included which named W0rmer [9].

Figure 2. One of W0rmer's tweeted photographs of his girlfriend

On February 16th, CabinCr3w hacked the Wyoming State Troopers' website, www.wyomingstatetrooper.com. They posted names, telephone numbers, cell numbers, home addresses, city, zip codes and email information obtained from the servers [32]. On the 20th, Alabama's Houston County website, www.houstoncounty.org, was defaced by CabinCr3w. Additionally, they created fake events on the online calendar, posted images representing Anonymous and CabinCr3w, deleted all the administrator accounts except the one they created [9]. On the 21st, the official websites of the Los Angeles County Police Canine Association (LACPCA) and the Los Angeles County Sheriff's Department were hacked. CabinCr3w claimed to have released server data, email addresses, passwords, names and physical addresses belonging to more than 1,000 officers as part of Operation Piggy Bank. They also claimed to have gained access to "over fifteen thousand police warrants, hundreds of thousands of court summons, over forty thousand social security numbers of citizens proving the police lack of care for the security of the citizens, anonymous tips of criminal informants pertaining to narcotics, criminal informant information and thousands of online police reports." [34]. They claimed to have found some questionable content in one of the email accounts

which purportedly contained pictures of child exploitation. They also posted nude photos of Mechelle Thompson, an airport officer at LAX, which were allegedly found in her inbox [34, 40]. The same day @ItsKahuna hacked the website of the City of Newark, NJ and tweeted the Administrator's username and password which essentially allowed anyone access to the website servers [18].

AnonW0rmer

On March 15, 2012, Higinio O. Ochoa III, also known as @AnonW0rmer and W0rmer, of Galveston, Texas, was charged with illegally hacking into websites of the Texas Department of Public Safety, the West Virginia Chiefs of Police Association, the Alabama Department of Public Safety and Houston County, Alabama. After pleading guilty to the charges in June, on August 27th, Ochoa was sentenced to two years in federal prison and required to pay more than $14,000 in restitution [3, 6, 8, 9, 13, 31].

Figure 3. Higinio Ochoa III "@Anonw0rmer" and his girlfriend/now-wife Kylie Gardner "@MissAnonFatale"

In reviewing the Texas Criminal Complaint against Ochoa, there are a number of incidents where the FBI was able to link Ochoa, @AnonW0rmer and W0rmer. The February 9, 2012 tweet, which featured pictures of his girlfriend in a blue bikini top still contained Exchangeable Image File Format (EXIF) data which indicated that the photograph was taken with an iPhone 4 in Australia. The sign which was positioned below the woman's cleavage linked the name "W0rmer" to the group CabinCr3w. The Texas Department of Safety hack, which was announced on February 9th on @AnonW0rmer's Twitter account also featured other pictures of the woman and originated from an IP address at 4925 Ft. Crocket Boulevard, Apartment 325, in Galveston, Texas. On February 12th at 1: 54 AM (the Criminal Complaint lists the time as 4:54 AM), @AnonW0rmer posted a tweet which linked to a picture presumably of his computer screen showing an error message. In the picture, there is also a Skype session running with a username of anonw0rmer logged on and another program called KVIrc version 4 with the username @higochoa logged in [38].

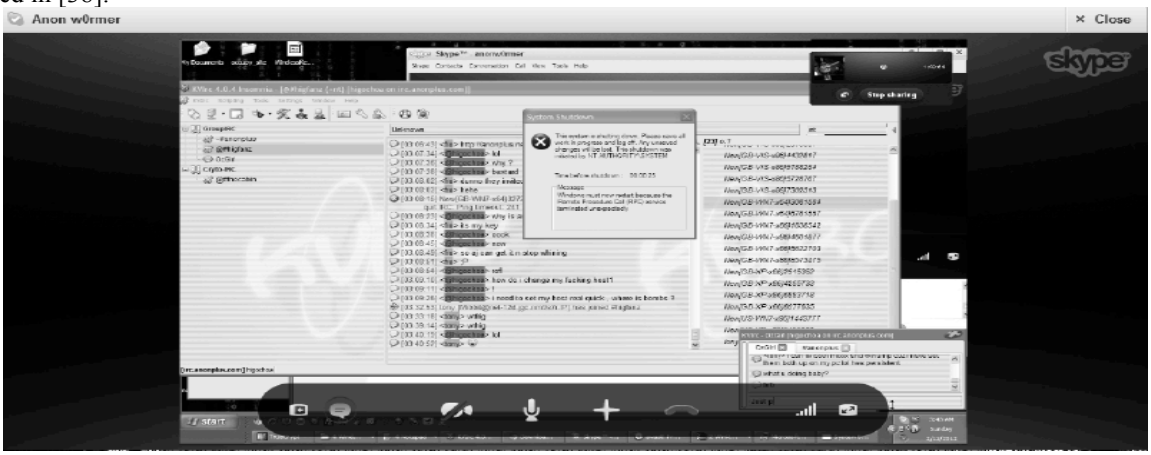

Figure 4. February 12, 2012 1:54 AM tweeted photo linking @Anonw0rmer with @higochoa

An open source search for the username w0rmer on search.gmane.org provided two hits from January 2000, one of which stated "I just signed up and am waiting to jump right in im [sic] a Visual Basic Programmer and network admin, so im [sic] ready for the challenge, cant [sic] wait. Any VB Programmers please send me some info regarding the syntax to the commands for the servers -Higino Ochoa AkA w0rmer" [38]. A search of the Texas Drivers License database for Higino Ochoa listed an address in Galveston, Texas. The Drivers License photograph was similar to a photograph on the website www.geocaching.com when the username @higochoa was searched [38].

On February 5th at 10:53 PM, Twitter user @higochoa tweeted a link to the West Virginia Chiefs of Police hack claiming credit for the hack along with @CabinCr3w and @ItsKahuna. He must have realized his mistake because the next day, Twitter account @Anonw0rmer was created and while the first login was apparently from a server in the Czech Republic, most likely anonymous through a service or The Onion Router service, the second login was from Comcast Communications in Houston, Texas. A search for Ochoa at the Galveston address of the Drivers License came up blank; he had moved to a new address in 2010. Ochoa had provided mail forwarding information to his old apartment, directing it to 925 Ft. Crocket Boulevard, Apartment 313, in Galveston, Texas. That address was one floor down and one unit over from the address which had the unsecured Wi-Fi router used in the Texas Department of Safety hack. FBI surveillance of the apartment complex visually identified Ochoa from the license photographs. A LinkedIn search for Ochoa came up with his profile, on which he indicated that he had been a Lead Administrator for Bombshellnet.org, a defunct software company, located in Houston. Finally, a search for Facebook users with Ochoa's name came up with user Galvestonman who listed that he was in a relationship with Kylie Gardner, whose Facebook profile indicated that she graduated from Dungog High School which happened to be in Dungog, New South Wales, Australia [38]. Numerous connections had been made between CabinCr3w, AononW0rmer, Ochoa and the Australian photographs of the girlfriend.

ItsKahuna

On March 16, 2012, John Anthony Borell III, also known as @ItsKahuna, of Toledo, Ohio, was charged with hacking into the websites of the Utah Chiefs of Police Association and the Salt Lake City Police Department. Borell was the second member of CabinCr3w to be charged with participation with Operation Pig Roast. After his arrest, Borell initially pled not guilty, however he agreed to plead guilty under a plea bargain on April 15, 2013 and at the time of submission of this research, was scheduled for sentencing on August 21, 2013 [2, 12, 15, 31, 36, 38].

Figure 5. John Anthony Borell III "@ItsKahuna"

The Utah Complaint notes that the investigation into the identity of @ItsKahuna began purportedly on February 15th with a search of possible aliases in unnamed IRC channels; this brought up usernames specter, anonjb, cryto667, ml5tlk and vector. Additionally, the Complaint listed posts on two FBI tip websites, tips.fbi.gov and ic3.gov. Both tips were identical, came from the same Sprint telephone and stated that John Anthony Borell III was a member of Anonymous, participant of AntiSec and used aliases specter, kahuna, TehTiger and Anonjb. The tip gave his address, phone number, email address and stated that he was a lead in the Brazilian Satiagraha hacks, that he had contacted Sabu, the LulzSec hacker who was arrested by the FBI on June 7, 2011 and that he had knowledge of the inner workings of Anonymous. The anonymous leaks were cited in the Complaint as originating from Borell stating that he was turning himself in because he was tired of running and hiding. There was no mention of who other than Borell might have actually sent in these tips in the Complaint; the FBI website does not require an informant provide a name, only the content of the tip. Most likely the tips were provided by someone who knew of Borell and wanted to expose him. It's interesting that the former-LulzSec hacker Sabu was mentioned by name in the tips. Sabu had been turned by the FBI from hacker into informant/mole the day after he was arrested and originated the AntiSec operation while under FBI control. So if Borell *was* in AntiSec, which at the time was linked to LulzSec and Anonymous, participating in operations, Sabu would conceivably have had intimate knowledge of the facts and conceivably could have made the anonymous tips to the FBI. The Satiagraha leaks investigation was in another FBI file which identified a hack generated at a Toledo, Ohio church [35].

The Complaint then notes that on February 6th, a Google search was conducted using the email address jborell3@gmail.com. However, this date was prior to the February 15th searches which provided the FBI tips and Satiagraha hack data, so it is unclear if this is a mistype or that information of Borell's activities were known prior to February 15. In any event, using the email address, the FBI was able to link to his Facebook account (Jborell) which provided a profile picture, home city (Sylvania, Ohio), Drivers License, with another photograph, a Twitter account (Jboerell3), and a YouTube profile (Jborell3) [35]. On January 29, 2012 a Pastebin post titled "Kahuna Pentagon Leak Log" contained a snippet of conversation with someone who used the alias "Presstorm" where Borell seemingly incriminates himself in the Satiagraha hack and notes his father is a lawyer. The FBI then finds two listings for an Ohio lawyer, John Anthony Borell Esq. [35].

On February 17th, the FBI subpoenaed Twitter to obtain all account IP addresses used, all tweets, all direct messages, user information and email accounts used for accounts @CabinCr3w, @Anonw0rmer and @ItsKahuna. Twitter responded on March 2nd with the information which the FBI used to subpoena Ohio Internet provider Buckeye Telesystems for several consistent IP addresses which Twitter user @ItsKahuna used. One IP address came from a neighbor's unprotected Wi-Fi, 312 feet from Borell's residence, while another address used was located at one of his friend's house, another was at Affinity Information management, Borell's workplace and one was at a church. The Complaint then goes on to detail the two hacks of the Utah Chiefs of Police and Salt Lake City Police Department websites noting from the Twitter logs that both were accessed at Borell's place of work and @ItsKahuna took credit for them [35].

On April 16, 2012, after word gets out that both Ochoa and Borell had been arrested, GardenslayerComm posts CabinCr3w's farewell video. In it, CabinCr3w identifies itself as part of Anonymous and ends with the Anonymous signoff message. While the @CabinCr3w Twitter account claims the video was not produced by CabinCr3w, every other member of the "crew" had tweeted a link to the video; apparently the person(s) who had control of the Twitter account now was not affiliated with the actual members [10, 11].

CONCLUSIONS

The hacking group CabinCr3w began with the start of the Occupy Wall Street movement in late-2011. As this was a protest against the Wall Street banking greed that was a major element in the coming of the Great Recession, the initial attacks of the group were against banking executives. By doxing Wall Street CEOs, CabinCr3w was viewed as an element of the larger protest. A sub-current to all this was the fact that in June of 2011, the rouge hacker group LulzSec had been compromised as its leader, Sabu, had been arrested and turned by the FBI into a clandestine informant in exchange for anticipated leniency in his sentencing and in order for him to be able to support his nieces. Under the FBI's tutelage, Sabu shut down the LulzSec brand and started what was called AntiSec, which was a purported movement against "The Authorities."

Many operations were started using the AntiSec banner, one being the Brazilian Satiagraha hacks which Court documents reveal, John Anthony Borell III was a lead in and undoubtedly on the FBI's radar. Borell brought this baggage and notoriety with him as he became a founder of CabinCr3w. As Sabu was still undercover in late-2011, having been arrested and charged in June of 2011 and revealed to be an FBI informant on March 6, 2012, he most likely maintained some degree of contact with Borell. Sabu might have even conceivably helped to steer CabinCr3w away from just the doxes of Wall Street executives toward the more damaging operations against law enforcement entities across the country under Operation Pig Roast, begun on November 21, 2011. While the details of the inner working of CabinCr3w may never be made available, it's clear that the group changed its focus in November 2011 and from that time forward began an aggressive campaign of SQLi attacks against law enforcement and government organizations across the country and around the world.

While doxing executives of mostly publicly-known information might be seen by some as a relatively harmless offense, hacking into law enforcement databases and posting server data to include files which might be law enforcement sensitive, was an entirely different matter. CabinCr3w decided to shift their focus and up the ante so to speak when they actively went after government and law enforcement websites. They had to know that this in and of itself would have certainly brought more scrutiny from federal officials, but the fact that at least one of their members had possibly unknowingly dragged an active FBI mole into operations certainly helped seal the group's fate and certainly Borell's fate.

But regardless of what affect or effect Sabu might have had in potentially steering the group in any direction, CabinCr3w members in the end were sloppy and careless. Both Anonw0rmer and ItsKahuna used undisguised IP addresses, a single instance of which might provide the location information that tied a Twitter account to a place of business or a neighbor's apartment. That fact was the key to their downfall; all of the other connections led to that fault. Over time, CabinCr3w most likely began to feel they were invincible enough to taunt authorities with photographs which probably unknowingly contained GPS data which helped fill in the blanks which showed relatable screen names and aliases of different accounts. In the end, their reliance on Twitter served to put the final nail in their electronic coffin. All Twitter accounts are open to subpoena if the government can establish probable cause and when certain Twitter accounts broadcast their illegal activities brazenly, probable cause is easy to establish.

CabinCr3w apparently began with a cause, support Occupy Wall Street protests by shedding light on those who participated in the downfall of the banking system; however it ended with a series of random attacks on totally unrelated law enforcement and government websites for a means which did not justify the end. In the end, their mistakes proved to be their downfall; if anyone is going to participate in any form of hacking, legal or illegal, they had better start with a totally clean identity which cannot be connected with any others, never use an undisguised IP address and watch what they say and who they say it to. This is not meant to provide a "how to" guide for those who might want to participate in illegal activities, it is the results of an investigation into what went wrong with CabinCr3w. CabinCr3w made basic mistakes and paid the price for it.

There are further research possibilities with other hacking groups, both affiliated with Anonymous, rouge groups for their own reasons, state-sponsored hacker elements and criminal groups. With our internet-interconnected electronic information system world growing ever interconnected and ever larger, elements who might wish to hijack systems and accounts are ripe for study to better understand motivation and mission.

REFERENCES

1. Associated Press. (2012a, February 8). Hackers post W.Va. police officers' personal info. *Fox News.* Retrieved February 8, 2012 from http://www.foxnews.com/us/2012/02/08/hackers-post-wva-police-officers-personal-info/cabincr3w
2. Associated Press. (2012b, April 16). Man linked to 'Anonymous' faces hacking charges. *WPVI News*. Retrieved April 16, 2012 from http://abclocal.go.com/wpvi/story?section=news/national_world&id=8622643
3. Associated Press. (2012c, August 27). Galveston man gets prison for hacking Texas DPS. *KTRK-TV News.* Retrieved August 27, 2012 from http://abclocal.go.com/ktrk/story?section=news/local&id=8787565

4. CabinCr3w. "Just DDoSed Twitter as a welcome to twitter!" 14 September 2011a, 3:42 p.m. Tweet.
5. CabinCr3w. "Good Morning #Lasers... #OccupyWallStreet" 17 September 2011b, 6:52 a.m. Tweet.
6. Cain, P. (2012, May 11). Higinio O. Ochoa III's girlfriend busts hacker (Kylie Gardner photos). *Right Entertainment.* Retrieved March 6, 2013 from http://www.rightentertainment.com/?p=2353
7. Couts, A. (2011c, October 18). Hackers leak Citigroup CEO's personal data after Occupy Wall Street arrests. *Digital Trends.* Retrieved October 21, 2011 from http://www.digitaltrends.com/computing/hackers-leak-citigroup-ceos-personal-data-after-occupy-wall-street-arrests/
8. Diaz, J. (2012, April 12). These breasts nailed a hacker for the FBI. *Gizmodo.* Retrieved April 30, 2012 from http://gizmodo.com/5901430/these-breasts-nailed-anonymous-hacker-in-fbi-case
9. Edge, J. (2012, April 17). Very revealing boobs [nsfw]. *Takedown News.* Retrieved April 20, 2012 from http://takedownnews.com/very-revealing-boobs/
10. Eördögh, F. (2012, April 17). Anonymous offshoot CabinCr3w disbands. *Daily Dot.* Retrieved April 17, 2012 from http://www.dailydot.com/news/anonymous-offshoot-cabincr3w-disbands/
11. GardenslayerComm. (2012, April 16). CabinCr3w final message. [video post]. Retrieved May 3, 2012 from http://www.youtube.com/watch?v=Gz3ibtYS47Q
12. Goodin, D. (2012a, April 17). Ohio man charged with Anonymous-sponsored attacks on police websites. *Ars Technica.* Retrieved April 17, 2012 from http://arstechnica.com/tech-policy/news/2012/04/ohio-man-charged-for-anonymous-sponsored-attacks-on-police-websites.ars?clicked=related_right
13. Guest. (2012d, March 31). Untitled. [Online forum comment]. Retrieved October 31, 2012 from http://pastebin.com/jjMRFDH6
14. J. L. (2012, January 1). Ministry of Trade Republic of Indonesia hacked and dumped by @CabinCr3w. *Cyber War News.* Retrieved March 8, 2013 from http://www.cyberwarnews.info/2012/01/01/ministry-of-trade-republic-of-indonesia-hacked-and-dumped-by-cabincr3w/
15. Jeralyn. (2012, April 16). Ohio hacker charged with Utah police website attacks. *TalkLeft.* Retrieved March 6, 2013 from http://www.talkleft.com/story/2012/4/16/223755/942
16. Kovacs, E. (2011a, November 30). Italian and Bhutan government websites hacked by Kahuna. *Softpedia.* Retrieved March 8, 2013 from http://news.softpedia.com/news/Italian-and-Bhutan-Government-Websites-Hacked-by-Kahuna-237558.shtml
17. Kovacs, E. (2011b, December 18). G2Secure hacked for discrimination against sick man (exclusive). *Softpedia.* Retrieved March 8, 2013 from http://news.softpedia.com/news/G2Secure-Hacked-for-Discrimination-Against-Sick-Man-Exclusive-241409.shtml
18. Kovacs, E. (2012, February 21). City of Newark website hacked for second time by Kahuna. *Softpedia.* Retrieved March 8, 2013 from http://news.softpedia.com/news/City-of-Newark-Website-Hacked-for-Second-Time-by-Kahuna-254051.shtml
19. Legitgov. (2012, February 5). CabinCr3w Database Drop – OpPiggyBank. Citizens for Legitimate Government. Retrieved March 2, 2013 from http://www.legitgov.org/CabinCr3w-Database-Drop-OpPiggyBank
20. Luminant Films. (2012, November 17). Hactivist timeline. *We Are Legion: The Story of the Hactivists.* Retrieved November 17, 2012 from http://wearelegionthedocumentary.com/hacktivist-timeline/
21. Lynd, R. & Lynd, H. (1929). *Middletown: A Study in Modern American Culture*. New York: Harcourt Brace & Company.
22. Mills, E. (2011a, September 26). Anonymous exposes info of alleged pepper spray cop. *CNET.* Retrieved January 23, 2012 from http://news.cnet.com/8301-27080_3-20111813-245/anonymous-exposes-info-of-alleged-pepper-spray-cop/
23. Mills, E. (2011b, September 27). Hackers leak data of Goldman Sachs CEO. *CNET.* Retrieved January 23, 2012 from http://news.cnet.com/8301-27080_3-20112400-245/hackers-leak-data-of-goldman-sachs-ceo/
24. Mills, E. (2011c, September 30). Hackers post data on JP Morgan Chase CEO. *CNET.* Retrieved January 23, 2012 from http://news.cnet.com/8301-27080_3-20113943-245/hackers-post-data-on-jp-morgan-chase-ceo/
25. Mills, E. (2011d, October 11). Digital activists release more banker data. *CNET.* Retrieved January 23, 2012 from http://news.cnet.com/8301-27080_3-20118929-245/digital-activists-release-more-banker-data/
26. Mills, E. (2011e, October 24). Hackers release data on ex-Treasury Secretary Rubin. *CNET.* Retrieved January 23, 2012 from http://news.cnet.com/8301-27080_3-20125022-245/hackers-release-data-on-ex-treasury-secretary-rubin/

27. O'Donoghue, A. (2012, January 31). Group hacks into SLCPD website over graffiti bill. *KSL.com.* Retrieved March 2, 2012 from http://www.ksl.com/index.php?nid=960&sid=19077893&s_cid=article-related-3
28. Office of Inadequate Security. (2012, February 9). Alabama and Texas law enforcement sites fall to hackers (updated). *Office of Inadequate Security.* Retrieved March 2, 2012 from http://www.databreaches.net/?p=23257
29. Reavy, P. (2012, January 20). Utah Chiefs of Police website hacked by Anonymous group. *Deseret News.* Retrieved March 2, 2012 from http://www.deseretnews.com/article/705397751/Utah-Chiefs-of-Police-website-hacked-by-ANONYMOUS-group.html?pg=all
30. Sarkar, A. (2011b, December 9). Los Angeles Police Department (LAPD) officers personal info leaked by CabinCr3w & Anonymous. *Voice of Grey Hat.* Retrieved December 9, 2011 from http://www.voiceofgreyhat.com/2011/12/los-angeles-police-department-lapd.html
31. Schwartz, M. (2012b, April 18). Anonymous hackers not smart on anonymity, feds say. *Information Week.* Retrieved April 18, 2012 from http://www.informationweek.com/news/security/government/232900479
32. Scrooby, P. (2012, February 16). Anonymous dump Wyoming State Troopers data in #OpPigRoast. *Examiner.com.* Retrieved March 2, 2013 from http://www.examiner.com/article/anonymous-dump-wyoming-state-troopers-data-oppigroast
33. Stone, M. (2011, November 22). Anonymous targets top cops: Cabin Cr3w launches #OpPigRoast. *Examiner.com.* Retrieved March 8, 2013 from http://www.examiner.com/article/anonymous-targets-top-cops-cabin-cr3w-launches-oppigroast
34. The Mad Bomber. (2012, February 22). Los Angeles police site hacked by CabinCr3w. [Web log comment]. Retrieved March 2, 2012 from http://accesstoinfo.blogspot.com/2012_02_01_archive.html
35. United States District Court for the District of Utah, Central Division. (2012, March 16). United States of America v. John Anthony Borell III. Complaint. Case No. 2:12-CR-163 DON. Salt Lake City, UT.
36. United States District Court for the District of Utah, Central Division. (2013, February 20). United States of America v. John Anthony Borell III. Trial Order. Case No. 2:12-CR-163 DON. Salt Lake City, UT
37. United States District Court for the District of Utah, Central Division. (2013, April 15). United States of America v. John Anthony Borell III. Statement by Defendant in Advance of Plea of Guilty Pursuant to Fed. R. Crim. P. 11(c)(1)(C). Case No. 2:12-CR-163 DON. Salt Lake City, UT.
38. United States District Court for the Western District of Texas. (2012, March 15). United States of America v. Higinio O. Ochoa III. Criminal Complaint. Case No. 1:12-mj-00163-DGG. Austin, TX.
39. Whitmire, K. (2012, February 10). Hacker group Anonymous targets Alabama over HB56. *Weld for Birmingham.* Retrieved February 10, 2012 from http://weldbham.com/secondfront/2012/02/10/hacker-group-targets-alabama-over-hb56/
40. Wilson, S. (2012, February 23). 'Anonymous' hacks into L.A. county police and sheriff databases; posts contact info, nude pics. *LA Weekly.* Retrieved March 2, 2012 from http://blogs.laweekly.com/informer/2012/02/anonymous_hacks_la_county_police_sheriff_contact_info_nude_pics.php
41. Yin, R. (2009). *Case Study Research: Design and Methods. Fourth Edition.* Thousand Oaks, CA: Sage.