Minhal Aamer  
Getrude Bossmart  
Luis Ruiz

PSCS 2301 Cyber Investigation Team Paper  
George Washington University

The Rise and Fall of Albert Gonzalez

Table of Contents

Introduction: Minhal.........................................................................................................

Early Life: Trudy...............................................................................................................

Career and Crime: Luis......................................................................................................

Arrest: Minhal....................................................................................................................

Charges and Consequences: Minhal...................................................................................

Current Life: Minhal...........................................................................................................

Conclusion: Trudy...............................................................................................................

Profile: Minhal and Luis......................................................................................................

References*............................................................................................................................*

Introduction

One of the biggest computer crime cases in the United States, for its time in 2007, was known as the TJX hack which resulted in enormous amounts of consumer data loss and costed potentially millions of dollars to TJX Corporations and its affiliates and many other companies. The hack had lasting effects on both cybersecurity and the payment industry security standards, that are still present today. It was perpetuated by a group of individuals from all over the world, but the most notorious of them was the one who orchestrated and led the attack, known as Anthony Gonzalez. A hacker who had managed to breach NASA at only 14 years old, which led to a life of cybercrime, eventually culminating in a breach never before seen, and the largest sentencing received at the time as well. In this paper, we will use any and all available resources to investigate and gain information on Albert Gonzalez and his early life, hacking career, crimes, and where he is today.

Early Life

Albert Gonzalez was a Cuban-American citizen born in 1981. His father’s name was Alberto Sr, a modest landscaper who migrated to America from Cuba on a handmade raft. Albert, his parents, and his older sister settled in Miami, Florida which was where Albert spent the majority of his childhood. At age 12, Albert obtained his first computer but it was only after the computer got a virus after a download from the Internet, that his curiosity truly awakened and a hobby became a fixation. He was upset about the malware and that indignation and confusion resulted in Albert having many questions on why and how hackers did what they did so he began to learn more about computers, malware, hacking, etc. He was intelligent, determined, and a natural leader, and also known at school as a “pack leader” of other like-minded students like him.

At age 14, Albert had managed to commit several cybercrime incidents prompting FBI agents to arrive at his school and interview and investigate him. These incidents included, stealing credit card information to buy clothes and CD’s, gaining access to an Indian government site, and hacking into NASA’s servers. Although he was talked to for hours, the goal was not to press charges but to instead establish how he had committed those acts and later he was let go. Seemingly, he did not partake in any other incidents after that and graduated high school in 1999 and began attending Miami Dade College.

However, unbeknownst to the public and those around him, he was spending more time in online chatrooms conversing with other hackers, sharing tips and implementing hacks. He had cultivated online personas, the most reputable of which was “soupnazi”. He formed a group of “black hats” who implemented curiosity and rebellion driven attacks, and he later bragged about defacing government and admin sites under his soupnazi persona. After being dissatisfied with college life, and the computer classes that were offered he dropped out of college and focused on enhancing his knowledge about computers by himself. He read software manuals, and taught himself how to hack into Internet providers to obtain free broadband, and continued to chat with other hackers, some of which would aid him later in life when he moved onto bigger hacking crimes in his career.

Career and Crime

Dropping out of Miami Dade Junior College after his first semester in 1999, Albert Gonzalez was an unemployed dropout and looking for opportunity. He didn’t have a job lined up when he dropped out, but he knew he wanted to pursue a career following his lifelong obsession with computers, but like he couldn’t handle how easy and primitive college classes were, he also had a dislike for white hat hackers. Albert moved from Florida to New York in the year 2000 in the pursuit of a job at a dot-com firm. It did not take long for the firm to go bust but, he managed to secure another position at the Siemens New York office. Siemens USA was a technology-based company that focused on creating new technologies to advance power, transportation and infrastructure. However, in 2002, the company made a move from New York to Pennsylvania. Unwilling to make that move, Albert was left unemployed yet again and needed income to fuel his habit of illicit drug use. He had already been in communication with hackers through IRC chats where he was already learning the principles on how to hack and basic concepts of network security making him more developed than his peers in the cyber world. He shared the hatred of “white hat” hackers with his friend and future “business” partner Stephan Watt. They conversed about hacking and nurtured each other’s lifelong passion and obsession, so much so, that Albert Gonzalez delved deeper into hacking and cybercrime. Frustrated with his initial attempts to go straight from dropping out of college to going through two different jobs, Albert began focusing more on hacking schemes.

Albert Gonzalez began his hacking career through a messaging board called the “Shadowcrew” where he quickly rose to the rank of moderator. This was a gang of ID thieves that operated on the domain “shadowcrew.com” which was founded and further funded by Brett Johnson, “The Original Internet Godfather” but its centralized marketplace was created and lead primarily by Andrew Montavani. This was not an organized crime syndicate but was instead a place where hackers of all degree of levels could come together, most had unassuming careers during the day such as students, mortgage brokers and even the unemployed such as the case for Albert. The Shadowcrew was the perfect place where a green hat (novice) hacker such as Albert could refine their skills. Shadowcrew hosted over 4,000 members internationally and these members were identified through nicknames such as “CumbaJohnny” which Albert used. Even though the group was loosely organized from the outside, it did have a strict chain of command and at the top of the hierarchy were the three administrators: Andrew Montavani, David Appleyard and Antoly Tyukanov. Following the administrators were the moderators and then the vendors and regular members. It was made clear by the administrators that no one could give their real name and some users were punished for doing just that. Anonymity was their strength, and even though Albert was presumed to be the mastermind of the group, he was just a moderator. This is not to discredit him because in this group the moderator rank was a sign of leadership, and they had their own forums where they could share information and hacking techniques with the regular members. To obtain such a rank withing a short time and being relatively new to his hacking career is a testament to the skill that Albert displayed but, his greatest skill would not be hacking but, it would be deception.

Albert was not a great criminal in fact, it was early on in his Shadowcrew that he was detected by the police and was arrested in July of 2003. To try and avoid detection he was wearing a wig and nose ring but any person swiping multiple cards at 12 am at an ATM would seem suspicious by nature. As such, a detective in plain clothes was surveilling the area due to car thefts and came across Albert who disclosed his real identity. This quickly made its way to the Secret Service Electronic Crimes Task Force and after meeting him they found that not only was he good mannered and willing to patiently give details about how he committed fraud but, he was one of the moderators for the group that they could not infiltrate. So, instead of arresting him they used Albert as an informant for “Operation Firewall” and they began to pay for his living expenses in exchange for information. In fact, it was later accounted for by Stephan Watt that Albert was getting paid as much as $75,000 a year being an informant for the group and in cash. This was a great success for the Secret Service agents, and on October 26, 2004, they made 21 arrests in the United States and allowing them to corner the Shadowcrew group. One of those men was Andrew Montavani, a cofounder and administrator of the group, originating from the state of Arizona and it eventually led to his guilty plea and prison term. This was enough to cause the United States government to shut down the shadowcrew site in 2004 which had stolen 1.5 million credit and bank numbers and lead to over $4 million in losses. Throughout this time, Albert wasn’t just quietly watching the arrest the members of the shadowcrew, but he was also assessing the agents. He knew that they couldn’t do it without him and that gave him the validation that he wanted and that further urged his criminal behavior. Stephan Watt, longtime friend and confidant of Albert even attested that Albert told him that “*These people are fucking retarded about anything other than jumping in front of a bullet*,” regarding the other members of Shadowcrew. It’s apparent that in his mind, Albert saw himself as someone so special that he had not just deceived the shadowcrew gang but was seemingly an essential asset to the Secret Service. This type of mentality would lead to him deceiving the Secret Service and committing a cyber heist all while being considered as a professional informant for the Secret Service.

Albert Gonzalez seemed to have fostered a friendly relationship with the Secret Service and overall, the agents that had handled him all had positive remarks regarding his character. Due to those reasons, it did not come as a shock that after the government shut down the Shadowcrew site in 2004, that the Secret Service office in Miami would reach out and offer to employ him as a paid informant in 2006. An agent in the Secret Service even attested that he believed that Albert was “trying to do the right thing” as Albert had already formed close bonds with some agents. However, unbeknownst to them, it was around this time when Albert and his friend Patrick Toey, another young hacker, began to explore a new concept of hacking called wardriving. Wardriving as an exploitative technique where hackers would drive around in vans or cars loaded with Wi-Fi antennas searching for unencrypted Wi-Fi signals. During this time many businesses began the adoption of wireless networks but did not have sufficient security to protect themselves, so a hacker on the move could easily drive around searching for those signals and then gain access their servers within minutes. This was the start of Albert Gonzalez’s infamous scheme, “Operation Get Rich or Die Trying”. The operation expanded and soon Albert had hackers across the country working for him. His teams of hackers would find an open network and remain near that location, usually in a hotel, as the store would conduct legitimate business transactions and then they would forward the data to Albert who would then forward it to Patrick who would then forward it to other hackers to decrypt the data. Essentially, customer data was hopping from hacker to hacker across the nation and then Albert would receive his share though a post office drop box in Miami. Ever since his first arrest in 2003, Albert had developed new techniques to avoid being seen cashing out at ATMs and was now receiving undocumented money through the mail across the nation. However, this did not last long as it was risky for the hackers as they were waiting in the parking lot or nearby hotels with their equipment.

With a new grand idea, Albert needed to contact Stephen Watt, who was working as IT for Morgan Stanley, to create a new sniffer code. Using a sniffer code would have allowed Albert to work his way up from a store to a corporate network, greatly increasing efficiency, reducing risk and giving him access to millions of credit card numbers. Albert, having dropped out of college, did not have the technical skills to create the program he desired and relied on Stephen and Patrick to create the sniffer code, named “blabla”, that would allow them to gain access to the parent servers of a company by sniffing the data packets from the compromised store servers. At this time, the money that they were cashing out was so significant, in the hundreds of thousands, that it became too risky to even pick it up at his drop box. It was at this point that Albert began to grow an international criminal empire. Albert’s idea was that it would be safer for them to not cash out the credit and banking numbers and instead sell the numbers to buyers who then had to cash them out themselves. He assembled a new team and now had Maksym Yastremskiy, a Ukrainian cybercrime lord, and two Russian hackers working for him. Within this time frame they were laundering money, communicating through encrypted IMs, and organizing and keeping his team of hackers in check from blowing their cover. This was all done while Albert was working as a paid informant for the Secret Service. In fact, he didn’t just fool the Secret Service, but he was directly profiting from them.

Confident in how well he had fooled the Secret Service, he even introduced Stephan Watt to his handlers. The introduction led to Stephan doing a presentation for the Secret Service about malware, but he declined an offer from them. Using information from the Secret Service Albert let his friends and contacts know when they or a site they were using was being investigated and to lay low until it blew over. He would also burn out databases with stolen information and sell it to other hackers to pin the blame on them. Using this method, he was able to commit the crime and then use his position of a paid informant to blame another hacker whom he had inside knowledge that was being investigated. This worked out well for Albert until another informant told the Secret Service that he was commit cybercrimes under the nickname of “K1ngchili” to which paid another criminal to use that nickname was Albert was physically present in the Secret Service headquarters. Deceit being one of Albert’s greatest skills he was not only able to betray the shadowcrew from 2002-2004 but he also betrayed the Secret Service and other members of the hacking community.

In what would now be the final moment of “Operation Get Rich or Die Trying” they would repurpose their sniffer code, “blabla”, to use a SQL injection attack to gain access through a backdoor and then the main sniffer code to gain access to the parent servers of a company. They would then gather the data in small batches, install invisible backdoors and erase their presence to avoid tipping off the system administrators of their presence. Ultimately, Maksym had been arrested outside a Turkish Nightclub in 2007 and his computer had not only evidence of stolen card numbers but his encrypted chats with Albert. He became too ambitious and overconfident in his skills that he ignored warning signs that the Secret Service was investigating him and his contacts. This led to his arrest on May 7th, 2008, as well as the indictment of 11 members of his business, called Green Hat Enterprises, across 5 countries. While they had compromised millions of cards from major retailers like BJ’s Wholesale, Marshalls, JCPenney and even the infamous TJX breach, where half to all their transactions were stolen, it was a relatively small hack on Dave & Busters in 2007 that led to his downfall. Later, he was also indicted to the Heartland Payment Systems hack, 7-Eleven and Hannaford Brothers Co and true to their operation name, they did try to get rich or die trying.

Arrest

In late 2006, the TJX corporation became aware that a large and suspicious amount of credit cards used at their affiliate stores were stolen. Further internal investigation led to the revelation that there was a breach of 45 million credit cards, which would later double in size after further investigation. They would soon realize that they had been being hacked since 2005 and would later contact the federal government. Later another target of Albert’s, the company Dave and Busters would also contact the government for a similar breach. At the time, Albert Gonsalez and his gang were not suspects, however that changed when the investigating federal officers received a lead through the Secret Service. An undercover agent was in contact with a foreign contact who sold stolen credit card information. That contact was Maksym Yastremskiy, who Albert Gonzalez supplied. The secret service managed to copy information off of Yastremskiy’s hard drive and found messages between the Ukranian and his largest supplier, unbeknownst to them due to the anonymous usernames, Albert Gonzalez.

Yastremskiy was later arrested in July of 2007 and the Secret Service managed to obtain correspondence from a still anonymous Gonzalez who had directed Yastremskiy to arrange for a fake passport for one of his accomplices who had been arrested and needed to leave the U.S. That accomplice was Jonathon Williams, and after a meticulous search, the federal agents were able to obtain a flash drive from him that contained information about Gonzalez, including a picture of him, a credit report, and his sister’s address. At around the same time, security service was able to analyze the messages exchanged between Yastremskiy and the anonymous supplier and found that the email that was being used was [soupnazi@efnet.ru](mailto:soupnazi@efnet.ru). Due to Anthony Gonzalez’s close relationship with the Secret Service as well as the notoriety of him and his soupnazi persona, it did not take long for the federal agents to ascertain his culpability. Anthony Gonzalez’s and his accomplices' homes were raided where they found firearms, drugs, money, and computer data. Gonzalez was later arrested in May of 2008 at the National Hotel in Miami Beach.

Charges and Consequences

Over months of interrogation, Albert Gonsalez began to offer information and lead investigators to more evidence, including more than one million dollars he had hidden in his parents' home. His court proceedings began as he was indicted in New York, New Jersey, and Massachusetts, the last two of which were combined. In March, 2010 he was accused of several credit card and fraud related crimes against major retailers such as TJX, Target, Barnes and Noble, as well as Dave and Busters resulting in loss of millions of dollars as well as personal information. He faced 15-25 years of jail time as well as restitution. Gonzalez was also facing accusations of targeting one of the largest credit card processing companies in the US, known as Heartland Payment Systems Inc, as well as other companies such as 7-Eleven. Gonzalez had helped two European based hackers perform SQL injection attacks resulting in over 100 million transactions being exposed and he faced 20 years of prison time.

Albert Gonzalez pled guilty to the charges he faced and was seeking the minimum sentence. He claimed numerous things during his trial, including that he suffered from a computer addiction and that he had an Asperger's disorder. He also mentioned that he had aided the government and cooperated fully by providing information about his accomplices as well as other cybersecurity breaches that had not been discovered. After some deliberation, in his case in March, he was sentenced to 20 years in prison. Similarly, he was also handed a 20-year sentence in the Heartland case. Both sentences would run concurrently, which meant he would spend 20 years of jail time. He was also ordered to forfeit over a million dollars and other assets. At the time, his sentencing was the most that any American had received for cyber related crime.

Recent Life and Conclusion

After his sentencing, Albert Gonzalez made an appeal on March 2011, citing that he wanted to withdraw his plea bargain. He claimed that the crimes he committed were made aware to the Secret Service as he remained on their team as an informant. He also said that they not only knew but approved of his actions and told him that “they had his back”. The Secret Service did not reply to this claim and his appeal was rejected. He continued his prison sentence at FMC Lexington and reportedly engaged in hobbies such as reading books like *Stalingrad, by Antony Beevor* and listening to NPR. As intelligence and pragmatic as ever, according to sources Albert Gonzalez developed a guide for prison he sent to one of his friends and accomplice. It included notes such as remaining neutral, being loyal only to yourself, and showing off one’s intelligence. In most interviews Gonzalez declined to talk further about his crimes, focusing more on his family and his love for computers.

For his time, Albert Gonzalez made monumental impact in the cybercrime world, operating a cyber fraud ring while simultaneously working as an informant for federal agencies and committing the largest breach of data the U.S had ever seen. It’s clear that he was a capable and intelligent leader and hacker since the beginning. Today, Albert Gonzalez remains imprisoned at FMC Lexington, a federal prison in Kentucky for inmates that require medical or mental health treatment. Many of his accomplices have already been released due to the smaller prison times they received and remain out of public life today. Meanwhile, Gonzalez remains in prison, restricted from any use of digital devices but he is soon due to be released in December of 2025.

Profile

It was not an uncommon concept, a child receiving a computer at a young age, and it certainly did not directly lead into a life of cybercrime. However, with Albert Gonzalez and many of his accomplices, that was the case which begged the question what exactly in their behavior and environment led them to do what they did. When Albert Gonzalez first received his computer he used it for ordinary things, such as playing video games and engaging in media. He was intelligent and curious, so when that virus appeared on his computer it certainly sparked his interest. In school, he was described as a nerd and despite his natural leadership traits his social standing was low. This loneliness and need to prove himself may have contributed to his growing obsession with computers and his online presence. His mother even suggested he meet with a psychologist, but he had refused.

After delving into the world of hacking and creating online relationships with other black hat hackers, Albert Gonzalez, in a way found his true calling. With people with similar mindsets to him, he was able to carry out his idea of a going against the system and proving he was above it all be defacing public websites and creating cyber chaos. They gave each other advice and tips and sometimes even carried out hacking crimes together. When the FBI became aware of his online activities, such as probing NASA servers, he was able to get off with no charges by portraying himself as a curious and intelligent kid who meant no harm. This deception took skill and was only the beginning of his unremorseful personality. He came from a modest background and used hacking to purchase things for himself, an indicator that he was partly motivated by money. He deemed college too simple, and moved out to the Northeast to pursue jobs meanwhile still nurturing his cybercrime career. This, however, would also later lead to a lack of technical skills which he would have to counteract by relying on his close friends Stephan and Patrick to create future codes for him to utilize.

He was resourceful and pragmatic and showed no loyalty but to himself. When he was caught by the government for engaging in an online cybercrime group, Shadowcrew, he managed to evade all charges by becoming a Secret Service informant. His natural charisma and patience swayed them, as well as his ability to efficiently explain the technical details of the crimes and lure his fellow cybercriminals into a trap for the Secret Service. Many of the Shadowcrew members were arrested and later when Gonzalez was asked about it, he showed signs of remorse and claimed when it came down to it, his loyalty would always be to the black hat community. He didn’t see them exactly as allies and throughout his life he would set up other hackers and would admit that their only use was to be expandable tools. He had deemed them and their skills lesser than his and viewed it as strengthening the black hat community by getting rid of the “fake” and “worthless” hackers. This didn’t stop him from remaining an informant and moving back to the government’s suggestion for his safety.

Perhaps it was his idea that he had gained the government’s trust and forged real connections with Secret Service agents, that made him confident enough to begin engaging in more cybercrime. He and some of his friends and acquaintances began building a cybercrime empire, using hacking tactics, laundering money, and committing fraud to make millions of dollars. They expanded their gang internationally dubbing it Operation Get Rich or Die Tryin, meanwhile Albert Gonzalez was binging on designer drugs, buying expensive penthouses and materials, and engaging with the Miami nightclub scene. However, he also led a modest and frugal private lifestyle when it came to his family, choosing to live in smaller homes, doing his own repairs, bargain shopping and going to free clinics. While on the outside, he did live a flashy lifestyle he also wanted to live a more traditional and stylized American lifestyle: creating a family, spending time with relatives, and helping his parents and friends. His ultimate goal wasn’t becoming filthy rich, it was the outcome of that which would be able to give him a sustainable and worry-free lifestyle that is typically seen in movies.

Albert Gonzalez seemingly also had traits of an obsessive-compulsive personality disorder, his fixation on computers and the challenges presented by network security which dropped his grades were only the tip of the iceberg. He would also seem calm and collected on the outside, but he was always fighting for control, especially as his business began to grow. He had to keep tabs and was constantly monitoring his associates, preparing in the event of a raid, making sure to only talk in encrypted channels and he was even wary of the expenditures and drug use of some of the other hackers in his crew. This, however, did not dissuade Albert’s own drug use expanding from cocaine to marijuana, ecstasy, mushrooms, LSD and more in search of the best high. This mentality would follow him to prison where he is reported to have created a guide and would be constantly looking for a way to manipulate the system for his own benefit and advantage. He had a strong desire and needed to be in control of not just his lifestyle but also of those around him and that could also be a possibility for his obsessions with hacking, where he would be able to gain that control over institutions and even the government.

Clearly, Albert Gonzalez was motivated by money but he also displayed a true obsession with computer crime, furthering his schemes and engaging in new hacking tactics he found. Albert Gonzalez also displayed sociopathic tendencies, engaging in impulsive behavior and relishing the thrill of crime. He was conniving, overly confident and conceited in his abilities, and lacked a certain amount moral. Though he cared about his family and spent time with his parents, his sister and nephew, and his girlfriend he also lived a second life. That included engaging in drug and alcohol abuse, crime, affairs, etc., that his family remained unaware of. He reportedly said to one of his accomplices that his goal was to make enough money, buy a yacht, and then retire but unfortunately the money he had already made wasn’t enough, and it was Albert Gonzalez’s obsession and greed that ultimately led to his downfall.

References

Verini, J. (2010, November 10). *The great cyberheist*. The New York Times. Retrieved November 29, 2021, from <https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html>.

Elfrink, T. (2021, November 29). *Hack Pack*. Miami New Times. Retrieved November 29, 2021, from <https://www.miaminewtimes.com/news/hack-pack-6379188?storyPage=3>.

Zetter, K. (2010, March 25). *TJX hacker gets 20 years in prison*. Wired. Retrieved November 29, 2021, from <https://www.wired.com/2010/03/tjx-sentencing/>.

ABC News Network. (n.d.). ABC News. Retrieved November 29, 2021, from <https://abcnews.go.com/Technology/story?id=8374399>.

Chabrow, E., & Ross, R. (n.d.). *Gonzalez seeks guilty plea withdrawal*. Bank Information Security. Retrieved November 29, 2021, from <https://www.bankinfosecurity.com/gonzalez-seeks-guilty-plea-withdrawal-a-3527>.

Ross, R. (n.d.). *Case analysis: Shadowcrew Carding Gang*. Bank Information Security. Retrieved November 29, 2021, from <https://www.bankinfosecurity.com/case-analysis-shadowcrew-carding-gang-a-136>.

Erdely, S. R. (2018, June 25). *Sex, drugs, and the biggest cybercrime of All time*. Rolling Stone. Retrieved November 29, 2021, from <https://www.rollingstone.com/culture/culture-news/sex-drugs-and-the-biggest-cybercrime-of-all-time-241836/>

Zetter, K. (2010, March 22). *Secret service paid TJX hacker $75,000 a year*. Wired. Retrieved November 29, 2021, from <https://www.wired.com/2010/03/gonzalez-salary/>.

*Hacking stories: Albert Gonzalez & the 'get rich or die trying' crew who stole 130 million credit-card numbers*. Black Hat Ethical Hacking. (2021, July 14). Retrieved November 29, 2021, from <https://www.blackhatethicalhacking.com/articles/free-access/hacking-stories-albert-gonzalez-the-get-rich-or-die-trying-crew-who-stole-130-million-credit-card-numbers/>.

Six defendants plead guilty in internet identity theft and Credit Card Fraud Conspiracy (November 17, 2005). (n.d.). Retrieved November 29, 2021, from <https://www.justice.gov/archive/criminal/cybercrime/press-releases/2005/mantovaniPlea.htm>.

Johnson, B., Ahmad, I., Duquette, R., & Sherman, A. (2018, November 7). *Content by Brett Johnson*. Bank Information Security. Retrieved November 29, 2021, from <https://www.bankinfosecurity.com/authors/brett-johnson-i-2241>.

*Inside the hacker's mind: Pathology meets technology*. MagellanTV. (n.d.). Retrieved November 30, 2021, from <https://www.magellantv.com/articles/inside-the-hackers-mind-sociopaths-psychopaths-and-technology>.