EXCERPT of

lifehacked

HOW ONE FAMILY FROM THE SLUMS
MADE **MILLIONS** SELLING APPS

ALLEN WONG

regoapps@gmail.com

Published in the United States of America.

First Edition, 2012

Rego Apps, LLC
Kissimmee, FL 34747

www.regoapps.com

lifehacked is not associated with, endorsed or sponsored by any entity mentioned herein.

ONLINE GAME HACKING

During my freshmen year in college, there was a Korean game called GunBound® that grew popular among Asian-Americans. GunBound was a free online multiplayer game, where you choose a tank and fight against other people in teams of four. Every player takes turns trying to destroy the tanks on the other team. You earned in-game gold for every kill and win you got, and you could power up your character by buying equipment using the in-game gold.

My best friend and I were late adopters to the game, so we were constantly being crushed by my friends from high school, because they had better equipment. She and I worked really hard to earn the gold to catch up to our friends. But each time we tried to catch up, they would progress more in the game as well.

This was around the time when I started learning how to read and modify assembly language (ASM), which is a low-level programming code where each statement corresponds to machine code. Machine code is the actual set of instructions that you give a CPU to do the task given. In comparison, C++ and Java are high-level programming languages that convert your simple statements into complex machine code. But coding in assembly language meant that you were coding every line of machine code yourself.

The reason why this is significant is because when programs are running, they get stored in the RAM as machine code. Thus, to reverse engineer a computer program, you would have to understand the machine code that was written. And by understanding how the game code works, you can modify the machine code in the RAM to get the game to do what you want it to do.

In GunBound, for example, there must be a piece of game code that tells your computer that your character lost health after getting hit. By modifying that game code, you can get your computer to think that you never got hit and therefore would never lose health. This would have been easy game hack to do if this were an offline game. However, since all the computers playing in the same game had to be in sync, you would get kicked out of the game if your health reading did not match up with the health readings from the rest of the players.

Therefore, it was a challenge to hack this game, and nobody really knew how to do it. I took up that challenge, because it seemed fun to search for the vulnerabilities in the game code and hack the game to my advantage.

One of the first hacks I found for the game was an innocent one. It allowed you to bypass the vulgar language filter, and allowed you to swear in the in-game chat without it turning into a mash of asterisks and punctuation marks. I shared the hack among my friends so that we could speak freely amongst one another without ever being filtered again. But, I never told them that I was the one who made it. I also distributed the hack freely on a new blog I created.

Since I valued my anonymity, I created that blog under a false alias named Janette. The picture I used for my alias was a picture of a cute blonde girl, whose photo I found from some random website. I maintained that alias until the closure of that blog. Although I could have attached my name to the blog, I had put my ego aside in exchange for my privacy.

Eventually, I discovered more fun hacks that the game developers did not block. I created a hack that allowed users to modify the trajectory of their opponents' missiles by changing the gravity and wind physics in the game. This led to some hilarious scenarios where people shot themselves. After seeing how fun it was to modify the game, I spent more time exploring the game code and figuring out new ways to hack the game.

Another hack I made, which I nicknamed "act of Zeus", allowed you to shoot an unlimited number of lightning bolts from the sky at anywhere you chose. The ability to shoot one lightning bolt per round usually only occurred after you died (sort of like a revenge attack), and each bolt did very little damage. However, I hacked the game code to allow me to shoot as many lightning bolts as I wanted, even though it wasn't my turn and I wasn't dead. This meant that I could blast anyone into smithereens at any given time during the game.

Having that kind of power at a young age, even in a video game, was quite alluring. The whole world of hacking was alluring in general. It was a mix of curiosity and fun. But I knew that having this kind of power could have corrupted me. So, I rarely used my hacks, even if they were for good intentions. When I did use them, they were mainly targeted at cyberbullies who liked to pick on weaker people.

The best GunBound matches are between people with equal equipment stats and equal experience. The new players usually don't have much equipment, so their avatars are weaker. The more experienced players usually have better equipment and can easily beat the new players (newbies) without much skill. The bullies are the ones who have the best equipment and purposefully join the games that are full of newbies. The newbies usually are okay with starting the game, because they don't know that they're about to be slaughtered. The bullies have close to a 100% chance of winning the game and gaining the gold coins, while the newbies are left defeated with no gold coins at all. I remember that this happened to me once when I first started playing the game, and it wasn't a pleasant experience.

It was an injustice that I wanted to make right. So what I did was create a new account with no equipment at all. I would then join these games where an entire side would be full of unknowing newbies and the other side would be full of decked out bullies. I didn't do any hacks until the match was almost over, and until the bullies thought that they got another easy win. Just when the newbies started running away after realizing that they were being slaughtered like defenseless lamb, I turned on my hacks. I changed the wind and gravity physics so that during each turn, the bullies would end up shooting themselves. I, then, shot enough lightning bolts at the bullies so that their tank would not get destroyed, but it would end up being buried six feet underground. At that point, they had no place to run to, and they had no chance of shooting any one of the newbies. Their only choices were to quit the game and forfeit, or to shoot at a wall and kill themselves from the blast. The bullies had been defeated either way. Once my anti-bullying tactics became known throughout the GunBound community, there was less and less cyberbullying in the game.

MY FIRST BUSINESS VENTURE

Since the price of college books and tuition was high, I had to do what every other college student had to do: Make money on the side. And since GunBound was taking up a lot of my free time, I wanted to find a way to profit from it.

What I had been seeing were people selling their GunBound equipment online for real money. And we're only talking about a few dollars or so for an item that would take hours of playing to obtain. It was a great bargain for players who wanted the powerful items without having to play the game for hours on end. And it was good for people who played the game and wanted to make money on the side. This business model became popular when the online PC game Diablo® came out. People were selling their rare items for tens of dollars on online auction sites.

I realized that I could do pretty well in this business model because I had the advantage of my computer skills. So what I had done was create a hack that made me automatically win after a round begins. I cloned the game and modified it a bit so that it would allow me to run the game more than once on the same computer. This allowed me to play on two accounts in the same computer. Then I coded a computer script that automated the process of starting a new game against my second account. So each time the match started, my primary account would win and get gold for the win. This process, which I nicknamed “gold hack”, proved successful, and I was able to generate large amounts of gold even when I was not on my computer (whether I was sleeping or in class). I then used the gold to buy powerful items, which I then sold for real money. I also gave my best friend and some of my other friends all of the most powerful items in the game for free. Being my friend had its benefits.

I also realized that if I sold my gold hack, I would be able to make even more money. So I set the price at $10, and sold hundreds of dollars worth of hacks each day under my blonde hacker girl alias, Janette. This went on for months, and I accumulated enough profits to pay for my college books and my college tuition.

I even became legendary among the GunBound community under my alias. When I was playing, there were people in the game claiming to be or personally know my fictitious hacker alias. The most bizarre incident of this was when my friend from high school, Jason, said that his college classmate, George, claimed to be dating Janette. At the time, none of my friends (or anyone in the world for that matter) knew that I was the one who was pulling the strings behind Janette. So I played a prank on Jason's classmate. I added a new blog post on Janette's blog that said that she dumped George, because it turned out that he had a small penis and cried like a little pansy all the time. I then told Jason to look at Janette's blog, and he cracked up after seeing that post. I later revealed that I personally knew who Janette was and that I spoke to her personally. That decision to reveal my relations to her later bit me in the ass.

LIFEHACK #16: YOUR PRIVACY IS ONE OF YOUR MOST IMPORTANT ASSETS

The invention of the internet only made gossip and rumor spread faster and wider. Word about my relations to Janette traveled pretty quickly and reached many of my friends, even though I told Jason not to tell anyone. Soon, a lot of people from my high school who played GunBound found out that I was actually Janette. The people from my high school were pretty smart, so it wasn't that hard to realize that I was only using her as a cover. After that, it was only a matter of time before word broke out of the circle of friends and onto the internet forums.

Finally, on one fateful day, it happened. I found out about it when my mother called me from New York at one in the morning. I was still in my college dorm in California at the time, so my 1 A.M. was her 4 A.M. What had happened was that a person with a deep-sounding voice had called my mother at four in the morning while pretending to be a police officer. He threatened to arrest me if I didn't stop what I was doing (selling hacks and game items). Soon after she hung up, a different person called her and asked for me. She told him that I wasn't living there anymore and hung up. It was only a few seconds later that she'd receive yet another call. My mother had no idea what I had been up to or what this was all about, so she got scared and confused and called me. Her phone kept getting so many phone calls that almost every time she picked up the phone to try to call me, she'd end up unknowingly answering another phone call. When she finally got through to me, I told her over the phone that I'd stop my business immediately without really explaining what my business was. I also told her to unplug the phone lines and not to worry.

I immediately went on the GunBound community forums to find out what was going on. What happened was that someone had posted my parents' landline phone number and address on a popular GunBound hacking forum. The address was obtained by doing a reverse phone lookup on my parents' landline phone number. The phone number was obtained through a cached version of one of my old websites. It was a personal website I had made back when I was only 13. It was meant to be a phone directory for my classmates, so that we had a central location to find each others' numbers without having to ask someone else for a person's number. Being 13 meant that I wasn't yet exposed to or lectured on the dangers of revealing your personal information online.

This was a lesson that I'd never forget. The person who posted my parents' number and address thought that it was my number and address. He was not someone I had known, but rather he was a "hacker" who either did not like the idea that I was selling hacks, was a cyberbully, or just wanted to show off his 'doxing' skills. 'Doxing' was the technique used by hackers to gather information about an individual or target using resources obtained through the internet. This information was then assembled to create a target's 'dox' (a word derived from the word 'documents'). The 'dox' was like a hacker's version of a FBI profile on a person. The idea behind it was that when you got a person's 'dox', you knew more about the person, and that increased the likelihood of discovering the person's flaws and vulnerabilities.

For example, there was an infamous case of U.S. vice-presidential candidate Sarah Palin being subjected to hacking. All the hacker needed was Sarah Palin's personal information, such as where she lived and what her pet's name was, to reset her Yahoo email account's password. This allowed that hacker to access all of Sarah Palin's emails.

Nobody was able to hack my accounts, but this person did create a 'dox' on me with all of the personal information that was available online (mainly just my full name, email address, AIM® screen name, home phone number, and home address). Not everyone believed that Janette was a real person. Of those who didn't believe, many wanted to know who was behind that alias. The cover was quite good. It was good enough that people started giving me marriage proposals for being the hottest female hacker. But ultimately, that cover suffered the greatest flaw: my ego. If I had put my ego aside, I would have let Jason's classmate continue his lies and just go on with my business. But once I let that one slip-up occur, things just snowballed forward.

The people on the forums fueled by curiosity, admiration, jealousy, and/or hatred all wanted to call me. The person who had called the number the first time even recorded the conversation with my mother and posted it online. I listened to the frightfulness in my mother's voice, and I couldn't forgive myself for allowing someone to scare my mother like that. I tried burying the forum posts about me by posting random messages on other threads to try to shift the conversation. It eventually worked, but not before the damage had already been done.

I was exposed, and to save my mother from further torment, I had to close my business and lay low. I posted a message on Janette's blog from another hacker alias I made up saying that Janette's accounts have all been hacked, and all the profits from her business were stolen. It was my plan to stop hackers from trying to hack me further. I just wanted them to stop bothering me. But they wouldn't stop. Even my AIM account kept getting messages from hundreds of people as soon as I signed on. Eventually, I had to block everyone who wasn't on my friend list. Two years later, I unblocked everyone, and my AIM account still received many messages asking if I was the infamous Janette. I went back to blocking everyone again since then, and hadn't changed that privacy setting for a very long time.

I was reluctant to close up my business, because I was making thousands of dollars a week from it. But I knew that my family's safety was more important than money. The deranged person who was posing as a police officer had messaged me on AIM and threatened to kill my mother if I didn't stop my business. I felt extremely paranoid at that point, because my father worked long hours, and my fragile mother was alone in the house most of the time. I was also thousands of miles away from home, so I couldn't protect my mother myself. I could have pressed charges at that point for blackmail, but I didn't want to complicate matters more. I was just a college freshman trying to make ends meet and get through college without any trouble.

Although I didn't hand over the matter to the police, I did conduct an investigation of my own to assess the level of threat that this guy posed on my family. That's when I really had to hone my hacking skills. When that person posted an audio file of his conversation with my mother, he posted it up with a unique screen name (it was a variation of "WhiteRabbit"). By searching on that screen name, I found the forums that he frequented and his personal blog. From there, I found out that "WhiteRabbit" was just a young man from Brooklyn who was failing school. But that didn't stop me from still feeling threatened. In his blog, there were pictures of him holding a combat knife. It became obvious that this person was disturbed. His blog also did not supply any personal information about him. There was neither a full name nor a school name on that blog. This was not surprising, because he saw how easily my personal information could be abused online. His paranoia was protecting him. I had to investigate this person even further, and I had to do it fast.

I did not get much information through his blog besides the information about his failing grades and his hatred towards his teachers. I needed a full name, school address and home address in case I ever did need to find him physically. And since I wasn't about to get it through the information found online, I had to set up an elaborate scheme.

The scheme involved creating five websites that were created by different authors and put in different URLs. Each of those authors was a fabricated person, and I was the one behind all of them. One of these fake websites, named "Hackshop", was created by someone trying to sell off his GunBound hacking programs. A second website, created by a hacker named "yyy", was a blog showing off the hacker's hacks ("yyy" was a random hacker alias that I made up). A third website named "HaqBound" was for reviewing and downloading different GunBound hacks for free. A fourth website was a blog post depicting how to buy GunBound items at 10% of its original price. And finally the fifth website was a clone of the official GunBound website.

The first website, "Hackshop", was the website link that I had posted on all the GunBound forums that "WhiteRabbit" frequented. On the forums, I was asking if people knew if this "Hackshop" website was legit or not. I would also then go on another computer and use a different screen name on those forums to reply that the hacks are real and that the website was legit. This was partially true, because I really did set up an e-commerce website to sell the GunBound hacks that I had previously kept to myself (e.g. the unlimited lightning strikes, and gravity/wind modifier). I was able to create the e-commerce website fairly quickly, because I had already coded an e-commerce website when I was selling my

GunBound gold hack. It was just a matter of changing the interface so that it wouldn't look like my old shop.

On the "Hackshop" website, I had posted screenshots from a hacker named "yyy" using the available hacks. I also linked to the "yyy" blog using a link titled, "See more screenshots". This was my way of proving that the hacks were real. The users didn't know that both the "yyy" hacker and the owner of "Hackshop" were me. On the "yyy" blog, I talked about how the "Hackshop" website was going against the hacker's ethics of selling hacks for profit. The angered hacker then talked about how he found a hacks-review website called "HaqBound" that had all the hacks sold by "Hackshop" available for free.

On the "HaqBound" website, I created a list of hacks that currently worked and didn't work anymore. I made up some random hacks that didn't work, and I labeled them as "not working". I then labeled some of the hacking programs that I was selling on my "Hackshop" website as "currently working". I also posted a link to download the hacking programs for free. And next to these on the list, was a link to my fourth website, which was a tutorial on how to buy GunBound items at 90% off. I also labeled that hack as "currently working".

On that fourth website, I described how I knew someone who had worked at the company who created GunBound. I explained that GunBound employees had a URL to an employee discount shop that they could give to their friends and families so that they could to buy items at a 90% discount. I explained that the URL was password-protected to prevent abuse, but that I had hacked the password. I posted a link to that URL along with the password that gave them access to the employee discount shop. That link actually redirected users to my clone of the official GunBound website. But back then, there was a bug in the browsers that allowed hackers to mask the URL of the website they were linking to by using some fairly simple JavaScript commands. So while the link actually pointed to my clone website, the URL shown in the victim's browser was the URL to the official GunBound website.

The clone of the GunBound website was used to "phish" for passwords. As explained earlier, it was a skill that I had learned from people "phishing" on Neopets. What happened was that when people tried to log into the "employee discount shop" using their actual GunBound login information, they would unknowingly email me their username and passwords. And to make the shop look more legit, I edited some actual artwork from the game so that I could use them to decorate the employee discount shop's login page. And to make the shop seem even more legit, I made users enter the employee's password to grant them access to the shop. Obviously this made-up password worked, because I coded the whole cloned website.

After setting up this elaborate bait and trap, all I had to do was hope that WhiteRabbit would see it and fall for it. Each one of the websites I created played a role in convincing WhiteRabbit to enter his username and password. For example, "Hackshop" was a spin-off of the original shop I had to sell my gold hacks. I knew that WhiteRabbit hated these shops for whatever reason that may be. I created this hacker named "yyy" as a person WhiteRabbit could relate to. This hacker also hated "Hackshop" and recommended users go to the "HaqBound" website to get hacks for free. I knew that WhiteRabbit wanted hacks for free, because he frequented a lot of forums that discussed GunBound hacking. The purpose of “yyy” was to build WhiteRabbit’s trust in the “HaqBound” website by personally recommending it. By putting working hacks in the “HaqBound” website, I further built WhiteRabbit’s trust on the website. Many people started sharing the HaqBound website and saying how good it was. I never personally recommended HaqBound on the forums myself, because I was a new user to the forums, and usually people don’t trust links given by new users. That’s why I had to make the other established and trusted users on the forums post links to the HaqBound website for me. My plan worked, and soon everyone trusted the HaqBound website. Once I had that trust, it was easy to convince people that an employee discount shop actually existed, and they trusted me enough to follow the tutorial written on another blog. By putting the discount shop tutorial on another blog, I had shifted the blame away from HaqBound. That way, when the more veteran hackers realized that the discount shop was a phishing scam, they wouldn’t put the blame on HaqBound. I could not lose people’s trust in HaqBound or else WhiteRabbit might not visit the website himself. I also had to defend the reputation of HaqBound on the forums by replying to the whistleblowers who tried to expose the phishing scam. I said that the discount only worked for certain users and that while it worked for my older accounts, it did not work for my new ones. It was just a matter of time before HaqBound got exposed, so I was praying that WhiteRabbit would fall for the trap soon.

Finally, after three weeks, and more than a thousand phished accounts later, I had finally got WhiteRabbit’s GunBound username and password. He realized that it was scam and changed his GunBound password immediately. But, it was not his GunBound account that I was after. I immediately used his password on his personal blog. From there I found his personal email address. I used his password on his email account and quickly shifted through his emails until I found his real name, home address and phone number from an invoice he received. I also learned almost everything else about the person, such as which school he went to, and which internet provider he used. I was in and out of that email account before he had the chance to change the password.

So to recap, all I needed was a person's screen name to get all that information. Let that be a lesson to not use a unique screen name online. And try not to use the same screen name across different websites. Your screen name acts as your unique ID through the internet, and people can trace your web history by searching on that screen name on a search engine.

By getting WhiteRabbit's identity, I finally got what I wanted: Reassurance that if this person would do anything bad to my mother, I would know how to find him immediately. Without this reassurance, it was difficult for me to concentrate in class. I was also worried that something had already happened to my mother, and I'd be the one responsible for bringing an evil person to her. My worries didn't go away until months later, when people started forgetting about the matter. I had tried to delete every bit of evidence of my family's existence from the internet. I removed all of my parent's information online, including their home phone and address. I removed all my public profiles and personal websites. For about a decade after that incident, I had kept a low profile.

Fortunately, nothing really happened after that. And that's also what's great about the internet. It makes people easily distracted. Once your 15-minutes of fame are up, you quickly become old news. People will move onto other things. The same speed that you rush into stardom is roughly the same speed that you'll rush out of it.

But be warned that if you stand out, there will always be people trying hard to take you down. They will even dedicate a lot of their free time to do so. The reasoning is not always clear as to why they do it. Perhaps they feel that everyone should be equal and that the idea of you being successful threatens that equality. Perhaps they feel that the only people who become successful are the ones who are greedy and obtain wealth through ill-gotten ways. Whatever the reason is, that's just the way life is. That's why you must value your privacy and anonymity immensely. Social networks like Facebook® are taking away your most precious asset. And they are doing it for their own profits. Keep some mystery in your life. Silence your ego, and don't be so quick to announce your fortunes.

For those who are curious as to what happened to WhiteRabbit: A few months after the incident, I felt like I needed to get some revenge for what WhiteRabbit did to my mother. So I took some of my accounts, and sent several GunBound items to WhiteRabbit. Then in each account, I complained to the GunBound employees that someone stole my items. I also took some screenshots of me using hacks and modified them so that it looked like it was WhiteRabbit's character that was doing the hacking. I then posted the screenshots on my Hackshop website and pretended that I forgot to blur out my account name. I then sent a link to Hackshop to the GunBound employees and complained that a hacker named WhiteRabbit was cheating in the game. The GunBound employees ultimately flagged WhiteRabbit as a hacker and banned his GunBound account.