1

"Genocide": From Columbine to Hacking

In high *school, they were known by their nicknames, "Reb" and "VoDKa." They were quiet, shy and gentle, and content to be by themselves. They played video games, collected baseball cards, and watched movies. They worked together producing videos for the school's news network. As young boys, they served as Boy Scouts and played Little League baseball and soccer.*

They were smart too; VoDKa took part in the high school's gifted student program and, along with Reb, had acquired a keen interest in computers. VoDKa even built his own computer at home and dreamed of becoming a computer science major in college. Both boys worked as system administrators for the school's computer lab and maintained their own Web pages.

But 18-year-old Eric Harris and 17-year-old Dylan Klebold were definitely not like other teenagers. They were outsiders who were filled with violence, hatred, and a blind devotion to Adolf Hitler's Nazi rhetoric. On April 20, 1999, that blind hatred erupted, not with an online rampage through the school's computer network, but with double-barrel shotguns, semiautomatic rifles and pistols, 30 homemade hand grenades, pipe bombs filled with nails, and a propane tank rigged with explosives. The four-and-a-half hours of chaos that Harris and Klebold unleashed on that day at Columbine High School in Littleton, Colorado, ended not with Web page defacements or billions of dollars in damages to online businesses, but with the senseless deaths of 12 other teenagers and a teacher. Nobody saw it coming, least of all the two boys' parents.

The first funeral for the victims at Columbine hadn't even taken place yet when the so-called experts began to blame the Internet for the increase in school violence and the growing disconnection from mainstream society of America's teenagers. Suddenly,

any teenager who spent too much time on the Internet and less time taking part in social events or wore black clothes to school immediately became a potential school shooter. America's teenagers were out of control, the experts said. They ran down a laundry list of school shootings to prove their point. All of the kids who had been arrested for school violence during the last few years had similar characteristics. They were loners, geeks who felt persecuted by others. They didn't fit in, at least not with the most popular kids in school or with the jocks.

Of course, there was another group of teens who was believed to share similar characteristics but of which even less was known. This other group even had its own subculture. These kids belonged to a murky underground of criminals and miscreants. This was the group responsible for hacking into corporate computer systems, stealing credit card numbers, and replacing the content of Web pages with vulgar, disturbing, and sometimes hate-filled messages. Suddenly, if you were a teenage hacker, you were a Harris or a Klebold waiting to happen, according to the experts.

But ignorance breeds contempt.

^()<[]>()*^*

It was around the time of the Columbine massacre, at the same time that word of mass tortures, rapes, and killings began filtering out of Kosovo, that "Genocide" thought seriously about changing his hacker nickname. He thought about it again after the September 11 terrorist attacks that killed more than 2,500 people at the World Trade Center in New York, at the Pentagon outside Washington, D.C., and in Pennsylvania.

But changing your screen name is not that easy. The hacker subculture has a strong undertow. The longer you wait before you try to get out, the deeper you sink into it. Genocide has been hacking since he was 14. That was 12 years ago. Changing his name now would be like committing suicide or faking his own death. A hacker's handle is his identity. It encompasses everything from his reputation in the underground to his capabilities and resume of hacking exploits all in one word or phrase. If Genocide were to change his name now, he would, in effect, become nobody again. He'd be just another wannabe. And Genocide is not a wannabe. He's the real deal.

If you were to ask him why he chose such a horrible word for his hacker handle, a word that produces images in peoples' minds of Nazi death camps and mass grave sites, Genocide would tell you that his decision had nothing to do with expressing support for such acts. Rather, he was making a statement designed to prove to people that they had become immune to being shocked by the horrors of orchestrated murder in the world. People still ask him what the name is all about, but the answer is always the same. A lot of people just

don't get it. And if he could change it, he probably would. But he can't. So we should just get over it. Genocide is a fact in the world. Yes, it's an evil fact. It also happens to be the hacker nickname of a kid who grew up in Fairbanks, Alaska. But it doesn't make him Hitler, the butcher of Belgrade, or Osama bin Laden. He's just a hacker.

^()<[]>()*^*

There weren't a lot of computers in Fairbanks when Genocide was a teenager. He certainly didn't have one at home like most kids today do. In fact, he didn't even have electricity, a telephone, or running water in his house. In that respect, Genocide offers a truly unique profile of a teenage hacker.

He grew up in a 20-foot by 20-foot shack in the backwoods of Alaska. It was a single-level house with floors and walls made of plywood, and a plastic vapor barrier on the inside to keep out the moisture. In some places, you could see straight through to the insulation in the walls. Genocide cut wood every day to feed the inefficient wood-burning stove that shielded him, his younger brother, and his mother from the biting cold at night. The family had to take showers, wash their clothes, and make telephone calls in downtown Fairbanks, some 35 or 40 minutes' drive away.

Because of its location in central Alaska, Fairbanks is known as the Golden Heart of Alaska. It sits 358 miles north of Anchorage and only 188 miles south of the Arctic Circle. Fairbanks is a staging point for North Slope villages such as Barrow and the oil fields of Prudhoe Bay. It's a place where summer days last forever and the shortest winter day enjoys less than three hours of sunlight. Temperatures in and around the central regions of Alaska range from 65 degrees below zero—a challenge for even the most efficient of wood-burning stoves—to +90 degrees in the summer. It's a pristine setting distinguished by flat, treeless tundra landscapes that are surrounded by the frozen white peaks of kingly mountains that rise up and glimmer beneath the aurora borealis. One look at the surrounding area from the side of the hill where Genocide's house was located and you will see computers and the Internet for what they really are: crude inventions of mortal men.

Genocide's parents had been divorced since he was five years old. His mother raised him and his younger brother alone and relied on food stamps to keep them fed. She had injured her back while working for United Parcel Service (UPS) and was no longer able to earn a paycheck. His mother's strength and will to survive, however, spoke volumes to Genocide and inspired him. She was stern and taught him how a man was supposed to act. A man should be strong, but gentle. A man was supposed to provide for his

family. Genocide took these lessons to heart. His father, a pilot for a freight airliner, paid him little attention when he was young and offered an example of what not to do.

As a teenager, Genocide built an extension to the family's house, providing two extra bedrooms for himself and his brother. Nothing came easy. Everything the family had, which wasn't much, they earned or made with their own hands. Teenage life was filled with a series of tough lessons for Genocide.

Wrestling was always a big sport at West Valley High School in Fairbanks. Genocide wrestled in the 160-pound weight class during his freshman year and would move up to the 171-pound class during his junior year. He was 5-feet 11-inches tall, with black hair and dark brown eyes and a quiet demeanor that tempered his muscular, wrestler's physique. When he was 16, he finally shed his braces. After eight years of wearing them, he was relieved to be able to smile without exposing a mouth full of metal. He stayed in shape by competing on the swim team during the off-season. Although wrestling and swimming took up a lot of his time, Genocide also found time for jazz band, choir, and even a little acting in school plays. He particularly remembers playing the role of the phantom in *Phantom of the Opera*.

Schoolwork, on the other hand, was never a big attraction for Genocide. English, math, history—what a waste of time. He had a particular distaste for chemistry. Needless to say, he had nothing to brag about when be brought home his report cards, if he brought them home at all. There was one subject area, however, that provided a rare bright spot on his record: computers. Genocide's discovery of computers marked the first time in his life that he truly wanted to learn.

Nothing sparked his interest the way computers did. There was a mystery to computers that made them irresistible. They were the gateway to the unknown, linked by telephone wires that connected him to the far reaches of the world. Sure, that was part of it. But the other part of the allure came from Genocide's ability to use computers to transcend the rules and his normal group of friends in ways he had never before imagined. He was outside of himself when he was sitting in front of a computer. And there were no real, tangible limits to the digital world like there were in the physical world. There were only challenges to overcome.

Most of Genocide's high school hacking career was spent causing chaos on the school's network. He experimented by playing practical jokes. He put the library computers into endless loops running 30-frame pornographic videos and coded Macintosh screen savers that crashed the machines and couldn't be

removed. Genocide had no idea that what he was doing could technically be called hacking. But it was hacking. It was experimentation, exploration. And Genocide was learning.

A year or two earlier, Genocide's cousin Tony—he didn't have a hacker nickname; he was just Tony—taught him valuable lessons in social engineering. This was the art of collecting information from unsuspecting individuals by asking seemingly harmless questions or by pretending to be somebody you're not. Tony was known as sort of a small-time local crime boss—you know: the kid whose name is the first to pop into your mind whenever something is missing or broken. He had taught Genocide at an early age the finer points of phone phreaking—replicating the tone used by the telephone companies to initiate long-distance telephone calls—and how to build the tone-generating blue boxes that had been made famous by the first generation of phone phreakers. Such skills came in handy to a kid who didn't have a telephone at home. Genocide had met his first hacker and gained an intimate understanding of the telephone network before he even owned a computer.

But Genocide quickly abandoned blue boxes when he began noticing that the police were picking off his cousin's friends. One by one, Genocide's phone phreaker associates were disappearing from the scene. The days of the phone phreaks were over, even in the backwoods of Fairbanks, Alaska. The telephone companies were too smart, too technologically advanced for that small-time stuff to go unnoticed.

None of that mattered now. Or did it? He had to figure out a way to pass chemistry in his junior year. He didn't know why the hell he needed chemistry in the first place. You could tell somebody that the initials Li on the periodic table stood for the element lithium, or that little strips of paper turned different colors when you dipped them into a liquid that contained hydrochloric acid. But who really cared? Genocide didn't. Regardless, the class had been dogging him for a while, and if he didn't pass, he wouldn't graduate.

He was in the chemistry lab after school one day making up work, as usual, when his mind started to piece together the answer to his problem. It had been sitting right there in front of him the entire time. It was a Macintosh computer on his teacher's desk. He'd watched her use it before, especially after big tests when she would stay late to enter all of the grades into some sort of database. He realized then that this wasn't a stand-alone system; it was part of the school's network. Now he was looking at something he could understand. A network. Genocide stood at the brink of his first hack, and the pay-off would be huge. He'd get to graduate on time with the rest of his friends.

But he would have to time it just right. When his teacher came in and sat down at the computer, like she always did after the last period of the day, to help the strugglers, like him, he would have to spring into action. He'd have to catch her off-guard, hit her with a flurry of questions to keep her off balance. And that's what he did. She came into the classroom holding a stack of papers from the recent test that the class had taken. None of the other students in the room paid much attention. There was nothing unusual about the teacher's arrival; she arrived at the same time every day. Genocide, sitting at a desk with his head buried in a book, glanced up and watched her closely. If he jumped up too soon, he would blow it. He needed to time his offensive so that he asked his first question as she was entering her password.

If school officials were concerned about the security of the network, they didn't tell Genocide's chemistry teacher. She threw the tests down on the desk and sat down in front of the computer, her back conveniently to the class. Genocide grabbed his notebook and his pencil and walked through the rows of lab tables toward the front of the class. Of course, nobody else in the class suspected anything. Genocide kept information about this operation highly compartmented and protected. He was the only one who knew of his plan, and he wasn't about to start bragging.

The teacher glanced down at the keyboard and prepared to peck away at her password using, as she always did, her two index fingers. This took a lot of concentration, you understand. She was focused. That's when Genocide hit her with a barrage of questions, feigning interest in chemical compounds and equations.

"I can't get these equations to balance," he said. "Is elemental hydrogen diatomic? In single replacement, is one reactant always an element? Does it matter if the element is written first or second on the reactant side of the equation?"

As always, his teacher remained focused. She preferred to do one thing at a time. Genocide stared over the top of his notebook, peering down over her shoulder as she typed. He scribbled in his notebook. But instead of working on the equation, he was actually writing down the teacher's login ID and password to the network. She turned around slowly, with a look on her face that said she hadn't quite heard or understood what he had asked. She was a thinker. Multitasking didn't come naturally to her.

"I'm sorry," she said. "Did you have a question?"

"Yes. I just wanted to know if hydrogen is diatomic," Genocide responded.

"Yes, of course. Remember that," she said.

"I'll try. Thanks."

The next day, Genocide arrived at school early and went into another classroom where he regularly attended speech lessons. There was a Mac in that classroom, too. He jumped on the computer and entered his chemistry teacher's name and password and hit Enter. It was that simple. He found her personal directory on a restricted network drive. Then he scrolled down and found his name and double-clicked it. In less than 30 seconds, he pulled up his entire work history in chemistry. At the top of the list was his grade for the last exam. It was a 63. A click of the mouse, a tap on the Delete key, and bingo: he now had a 73. That was just enough to boost his average for the course into the low D range. Nobody noticed one digit. Graduation was no longer an issue for Genocide. He'd be receiving a diploma next year with everybody else in his class.

^()<[]>()*^*

He wasn't exactly proud of his first semi-hacking exploit, but Genocide never pretended to always play by the rules anyway. That was a good thing, because from that point on he rarely did. His grade-changing caper may not have been what most hackers, including himself, would consider a hack in the true sense of the word, but that was okay. Genocide was just getting started.

At about the same time that Genocide discovered his lust for computers, his mother started taking college courses part time at the University of Alaska. And since they had no running water at their house, Genocide began accompanying her to the college in the evenings to make use of the facilities. The best part about going to the college with his mother, however, was that she had access to the school's network. Of course, his mother had written her login name and password on a piece of paper.

Genocide stole time on the campus network while his mother was in class. The system administrator was a complete poser who didn't know the first thing about securing the system. It was a virgin Unix network run by a virgin administrator whose first rule of thumb was to do no harm. Genocide operated under no such restrictions. He explored the inner workings of the network using his mother's account. He surfed various bulletin boards and spent countless hours reading and learning about various commands, operating systems, and hardware design—you name it, he read it.

Like all true hackers, Genocide quickly became bored with reading about hacking and decided it was time for some hands-on exploration of the university system. He typed:

man [*command*]

A list of commands that could be used on the system filled his screen. He tried commands he was unfamiliar with and explored some more. He tried various logins to see if he could gain system administrator access. He knew that on Unix systems there were a few basic default login-password combinations that lame system administrators, like the one who ran the school lab, rarely ever changed. He tried the ones that he knew:

Root …root

Admin …admin

Sysadmin …sysadmin

Guest …guest

Nothing worked. This wasn't really a big deal. Unix systems didn't record every failed login attempt the way older VAX machines using the virtual memory system, or VMS, operating system did. The school had just upgraded from a VAX system to Unix, so Genocide felt free to explore and learn at will. He was also sort of glad that none of the default logins worked. Breaking in was more fun.

So he told the computer to list the password file for him:

Cat /etc/passwd

Done. To his amazement, the password file wasn't shadowed. That meant it hadn't been replaced by a special token and stored in a separate, unreachable file. To the contrary, it was right there for the taking, although it was encrypted.

That's when he discovered his first version of Crack, a program that decodes user passwords using brute force. Crack was designed to ferret out insecurities in Unix passwords by scanning the contents of a password file and picking out users who had chosen weak passwords, such as common words in the dictionary. These types of users were everywhere on college networks.

Genocide's first successful run of the Crack program was nearly his last. He was still learning and hadn't realized what a system resource hog the Crack program could be. And that could be a problem. Unless the system administrator was completely brain dead, he would be able to tell that something was not right on the network. Genocide allowed the program to continue to run in the background as he opened a new command window and started to spy on the other users in the lab to see if anybody was on to him. The lab was full that night. Nobody seemed to know or care about what he was doing.

At the command prompt, he typed **w**, which told the computer to list all of the users currently online. The list also reported when each user had logged in, what machine the user was sitting at, whether the user had been idle and for how long, and what programs the user was running. That last piece of data was the most important element: with a simple keystroke, Genocide had launched countersurveillance against the system administrator while his password-cracking program ran in the background.

The program needed about 40 more seconds to finish cracking the password file. Genocide took one more look to see what the other network users were up to. That's when he noticed that the system administrator was running a command called a w fstbo. Genocide knew immediately what was happening. The admin had noticed that he was using Crack against the password file. The increase in the server load averages that resulted from Genocide's use of the Crack program must have tipped him off. Maybe this guy wasn't brain dead after all. Genocide also realized that the admin could tell where he was sitting just by looking at the terminal number that was running the program. Genocide freaked out, killed the program and his network session, and ran.

He waited until he was out of the building before he looked back. By that time, another student had already plopped down in front of the computer that Genocide had been using. Computers were hard to come by on campus, and if you got up you lost your terminal in a matter of seconds. This time, Genocide didn't mind. He looked back and saw the admin accusing the student who was now sitting in front of Genocide's system of hacking passwords. Both the admin and the student seemed confused by the fact that the student hadn't even logged on to the network yet.

From that point on, Genocide craved the taste of adrenaline he got from hacking. This was what hacking was all about. The rush and the challenge, the unquenchable thirst for knowledge and the need to push the limits. Hacking was the act of doing something that others said couldn't be done. Hackers solved puzzles that others said couldn't be solved and overcame obstacles that were thought to be insurmountable. Hackers didn't cringe in the face of impossible odds. They became energized when outnumbered. And, most of all, hackers didn't quit. Genocide would eventually get another chance to crack the password file, and he'd be successful. But cracking that password file was just the beginning, and Genocide knew that. For a hacker, learning to crack passwords was like a mechanic learning how to use a wrench.

There would be many other successful hacks and cracks that year. Fairbanks was the perfect proving ground for a young hacker to flex his muscles, spread his wings a little. Genocide was building a portfolio,

collecting tools for his hacker toolbox, and gaining a reputation among some of the other regulars in the computer lab. More important, the son of the student had become a student himself. Genocide was a freshman in college studying art and music, and now he had his own authorized access. And he was beginning to make friends, hacker friends.

^()<[]>()*^*

They each knew who the others were, but in the beginning they kept their distance. They were feeling each other out, like a rag-tag army trying to distinguish the officers from the foot soldiers. Genocide had become a regular presence in the computer lab, along with four other hackers. They talked a little, but not much, mostly about security, coding, viruses, and the like. Over time, the hackers became more comfortable with each other. They had struck up a friendship and a feeling of solidarity. Each of the hackers also brought unique skills to the table. Some were better than others at coding or hacking specific operating systems. Gradually, the group realized that they were task organized, with an expert on staff to address any potential challenge.

WiZDom was about five years older than Genocide. He was an ex-Army vet who worked on trucks to make ends meet. At the time, WiZDom was studying for a degree in computer science. He specialized in coding, period. That was what he did best. He wasn't very good with operating system configurations, or anything else for that matter. But a skilled code monkey he was.

Genocide had met Astroboy when he was in high school, but neither knew that the other was into computers. Astroboy was good at working with Macintosh systems, so he instantly became the group's Mac guy and remains so to this day. He, too, was into art, and like most artists had a good imagination.

Alexu was two years older than Genocide and was studying for a degree in music education. Computers were a hobby for Alexu. Years earlier, he had been a regular BBS surfer, and as a result, he had a solid understanding of telephony and old-school Internet hardware design. Alexu also was a gaming nerd in the truest sense of the word. If there was a computer game to be played, this guy had played it. His favorite game was a command-line version of Dungeons and Dragons.

Malcom was the enigma of the group. Nobody was sure exactly how old he was, but from his looks, Malcom couldn't have been more than a year older than Genocide. His background was a well-kept secret. Malcom was by far the best of the group at Linux operating systems. He harbored a weird contempt

for graphical user interfaces, though. He insisted on using his laptop running Linux without X Windows (an emulator that offers users the familiar Windows interface). Malcom had also been to the infamous annual hacker conference in Las Vegas known as DefCon before Genocide knew what DefCon was. As a result, Malcom would become Genocide's gateway into that portion of the underground.

A friendly competition emerged within the group, which grew slowly beyond the original 5 members to include about 10 other nameless, ever-changing faces. Somebody would come up with a theory, and it would be up to the rest of the group to either prove or disprove it. They fed off of each other's ideas. Discussions of the theoretical eventually led to outright competitions among the group—virus-writing competitions, to be exact. Genocide, WiZDom, Alexu, Astroboy, and Malcom would each write their own virus in assembly code. Then all of the viruses would be unleashed on the campus network simultaneously. Whoever's virus was left standing at the end of the rampage won.

The members of the group shared similar views about hacking, the inherent freedom of information, and the benefits of knowledge sharing. All were equally pissed off at the ignorance of the media and the general population when it came to understanding what a hacker was. Sure, the five of them had acknowledged during private discussions various "criminal" hacking exploits that they had been involved in, but hackers were not criminals. Those who would censor information and block the pursuit of knowledge were the criminals. Hackers were the defenders of these very basic human rights, according to Genocide and his newfound compatriots. All had agreed on these issues and discovered a sort of intellectual brotherhood within their small gathering. What they had actually done, however, was lay the foundation for what would become the Genocide2600 hacker group.

^()<[]>()*^*

The hacker ethic was all about sharing knowledge. There was no tenet more basic to the hacker community than the freedom of information. All information was created equal and unbound. Knowledge was of no use if it could not be shared. So before they even knew they were a group, Genocide, WiZDom, Alexu, Astroboy, and Malcom formed a local chapter of the 2600 hacker organization and started to share their "skilz"—their skills—with anybody who would listen.

Malcom had come up with the idea for the meetings after he read one of the old issues of 2600 magazine. There were 2600 chapters all over the country,

and they all met once a month on Fridays at seven o'clock. Everybody thought it was a great idea and took turns teaching the dozen or so individuals who showed up at the meetings about computer security, telephony, computer media, cryptography, government systems, or whatever their individual specialties had made them uniquely qualified to discuss.

This was a time of great learning for Genocide. He refined his skills in gaining access to password files and cracking them, creating dictionary files for brute-force cracks, exploiting race conditions in server software—that is, taking advantage of another application's use of system resources, such as files, devices, or memory—and injecting instructions into a system by overloading an application with more data than it was designed to handle, to cause what is known as a buffer overflow. He also gained a deeper understanding of human nature, especially as it applied to the way people choose login IDs and passwords. From there, he moved on to some light coding, root kit setup, tactics for erasing log trails, and strategies for becoming an invisible "ghost" on a system.

In addition to being a time of intense learning and technical development for Genocide, this also was a time of rare fortune for him and his family. Genocide and his mother for the first time could afford to wire their home with electricity and a telephone (although to this day running water remains elusive). They paid the telephone company to run the line from a neighbor's house. With the telephone line also came a 75-meghertz Pentium computer that Genocide bought using money from his student loan. Suddenly, the kid who had been living *The Life and Times of Grizzly Adams*—the 1977 television series starring Dan Haggerty as a wilderness hero whose best friend is a grizzly bear named Ben—could boast of having the fastest computer of the group.

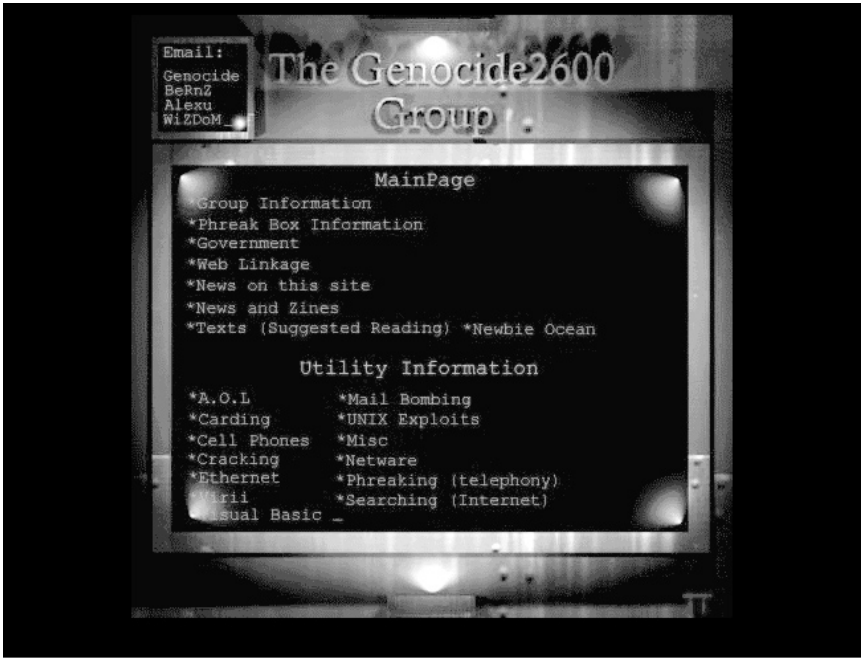
The 2600 group continued to hold meetings for more than a year, eventually becoming recognized by the university as an official extracurricular educational organization. Genocide had unofficially taken charge of the group through his own initiative. He was, after all, the tactician who enjoyed reading history and dissecting the battle plans of great military leaders like Napoleon and Frederick the Great. These were timeless lessons from a timeless profession, and Genocide applied them to the hacker's battlefield with great success. This was what made him different from the others in the group. He thought strategically.

After the 2600 meetings, the core group of hackers—Genocide, Alexu, Astroboy, Malcom, and WiZDom-would find a secluded computer room at the university to try out their newfound information or theories on hacking. Their meeting room was located in the same building as the school's

auditorium, known as the Great Hall. Outside the room where they held their meetings was a small alcove that housed a soda machine, a candy machine, and a row of pay phones. The candy and soda sustained the hackers and kept the wheels turning through long hours of number crunching and other mind-boggling calculations.

Standard procedure called for the group to dial out from an anonymous number at the university to one of the local ISPs, usually either PolarNet or AlaskaNet, using a hacked Point-to-Point Protocol, or PPP, account. After connecting to the ISP, they proceeded to use telnet—a terminal emulation program that allows a system to connect to a server—to connect to a student account at the local school network, where Genocide had already managed to gain root access. From there, they could do anything they wanted.

Genocide also set up a Web site on the university network and aptly named it Genocide2600—although the directory structure on the university network pointed to an obscure page: http://icecube.acf-lab.alaska.edu/~fstbo. The Web site quickly grew into a major hub of hacking and cracking information. All of the information that was shared by the group at the monthly meetings was at first distributed on floppy disks for the cost of only the disks and then later made available for free on the Genocide2600 Web page.



The original Genocide2600 Web page

In addition to the increasing amount of information on how to take advantage of Unix security flaws, the original Genocide2600 Web site became a repository for dozens of text "philes"—files—about old-school hacking and phreaking. A hacker could visit the Genocide2600 site and learn how to defeat the FBI's lock-in trace capabilities, accept a free long-distance call by lowering the voltage on the phone, make a low-budget two-party phone line, take advantage of a "post pay" public phone—a rural oddity where a caller gets a dial tone first and inserts coins to pay for the call after the other party answers—and make free calls, play tones into a phone and get free credit, tap standard house phone lines, get 12-volt "thief power" from a phone cable, hack and take down a phone company, make a phone busy forever, and construct a chrome box that could switch traffic lights from red to green. These were the building block skills that posers and less experienced hackers chose to ignore. For Genocide, however, studying these old-school tactics was the equivalent of learning the ABCs before trying to read.

Eventually, the university got wind of the type of information that was being stored on the Genocide2600 Web page and asked Genocide to remove it from the university network. So he buried it deeper.

^()<[]>()*^*

It was around the time when the university started to be a pain in the ass to deal with and the dozen or so pinheads who attended the meetings began to show less and less interest that the real transformation of Genocide and the other hackers took place. This was when they became a real group: Genocide2600.

Of course, in reality the transformation was far less dramatic. As Genocide recalled, one of the group members suggested that the group go over to his house to try some of the tactics and techniques they had talked about at the latest 2600 meeting. The exact words were something like "hey, why don't we run over to my house? I have two machines, a sister, and pizza."

Those simple words changed everything, including the group's social order and the way they interacted with one another. They were no longer faceless peers in a classroom, but people who could measure each other's strengths and weaknesses. As each hacker worked on a particular problem, the others could guess his next move by simply looking over his shoulder. Some of them also began to develop individual techniques but didn't realize it at the time. But a technique can be dangerous. It can act like a fingerprint and lead the police right to your computer. It was because of this that Genocide made a concerted effort to avoid becoming trapped in any one technique.

A few months later, the group held its first off-site meeting at Genocide's house, where they conducted a major break-in. They started scanning the target system, which we'll call "Moon," at 10 P.M. Within an hour, the group had gained root access to the system. At first glance, it looked like a standard corporate server with loads of useless information. It soon became clear to Genocide, however, that the system was actually a major repository of computer security information and hacking tools—not a far stretch of the imagination in an area of Alaska surrounded by two military bases and a university.

Genocide discovered dozens of software tools that were designed to break into computers as a means of testing security. He took them all—about 14 megabytes worth of hacking and cracking tools. Although the "Moon" hack ended the group's use of the PolarNet account, it significantly increased the value and the visibility of the Genocide2600 Web page. The page grew quickly, as did calls by the university to have it removed from the network. So Genocide buried it even deeper.

Genocide2600 was on the map. The tools and scripts the group managed to pilfer were vital to establishing the group as a force and a presence in the underground. "Suddenly we had tools that no one else had, scripts that no one else had seen, and knowledge that no one else possessed on intrusion techniques and new methodologies," Genocide recalled. The heist also was a big score for the hacker movement in general because a lot of the tools that the Genocide2600 crew had managed to get their hands on had been designed to assist the white-hat hacker community: the good guys. These were the software applications that security administrators used to ferret out the bad guys, like Genocide.

About 500 e-mail messages a week poured in from wannabe hackers asking Genocide to help them learn how to hack. Genocide's answer, if he answered at all, was always the same: go learn yourself like the rest of us did.

The increased availability of hacking tools and scripts also helped boost attendance at the group's Friday-night 2600 meetings. But Genocide was careful to warn the other members of the group not to discuss anything illegal. Anybody was free to attend the meetings as long as they took place on school property and were held under the auspices of a university educational program. From time to time, the meetings attracted university officials and professors. And although the stuffed shirts would never publicly condone the methods used to gather the information, they also would never say that they didn't learn something from the meetings.

But it was the presence of one particular stranger at the next meeting that got everybody's attention. This guy wasn't your typical 1960s-holdout

university professor. For one thing, he was dressed in a navy blue suit and tie. And he sat in the back of the room, listening to the presentations, emotionless. He seemed to be fixated on Genocide.

As the meeting came to a close, the attendees mingled and began filtering out of the room. This was normal. Presentations often raised more questions than could be answered in the time allotted to the meeting, and the attendees often continued their conversations as they left. The newest visitor to the meetings hadn't left, however. He was still in the back of the room, only now he was standing like everybody else. Genocide looked at him and saw a man with his hands in his trouser pockets, staring at the attendees with a smirk on his face, as if he knew their darkest secrets or had been rifling through the contents of their bedroom dressers only moments earlier.

When the last of the wannabes had left the meeting, the stranger in the back of the room walked up to Genocide and asked Genocide if he would take a walk. Genocide said sure, and the two walked down the hall away from the crowd that still mingled about. That's when the guy in the blue suit showed Genocide his FBI credentials and told him he was leading an investigation that would prove Genocide's involvement in the hack into the "Moon" server. He also ran down some of the evidence he had gathered so far, including the contents of the Genocide2600 Web page. Satisfied that he had put the fear of God into Genocide, the FBI agent simply walked off. The FBI had other tentacles in motion, however, that Genocide would soon learn about.

One of the first things Genocide did was call his mother from the university. He was genuinely scared. But as the thoughts raced through his mind, he realized that maybe this was what the FBI had hoped he would do. As a result, the conversation he was planning to have with his mother took a radical turn. Genocide remembers the conversation as follows:

Mom: Hello?

Genocide: Hi, mom; how's your back?

Mom: Same as usual; do you need a ride home?

Genocide: Naw, I'm fine... Listen, I've got some news...

Mom: Okay—what's wrong?

Genocide's mother always seemed to know from the sound of her sons' voices when they had done something they shouldn't.

Genocide: I think everything is going to be okay, but there are some people here at the school who think I did something, and they are plenty pissed off at me.

Mom: What exactly are we talking about here?

Genocide: It has to do with computers; they think I broke into some high-brow server somewhere and...

Mom: In the school? Did you?

Genocide: No! No!

Mom: Can you prove it wasn't you?

Genocide: It's impossible for me to prove I wasn't there.

Mom: Then it's simple; you just tell them it wasn't you. They will check in the server and find out it wasn't you, and then you'll be on your way.

Genocide: It's not quite that easy mom.

Mom: Sure it is.

Genocide: Mom, it's the FBI.

The mention of those three little letters—FBI—sucked all of the sound out of the telephone. It was as dead and motionless as a black hole in outer space. Genocide could imagine the look on his mother's face at that very moment. She was pissed. Seething. Unable to speak.

Mom: I hope for your sake you didn't fuck yourself. Does your brother know?

Genocide: No, I barely found out. No one knows but you and me right now…well, and the stiff in the suit.

Mom: How do you know it's the FBI and not some trick?

Genocide: Mom, the guy confronted me face to face, showed me his badge, and then told me he was here to prove I broke into that place.

Silence again filled the telephone receiver. Genocide's social engineering skills were never good enough to conceal his own sense of fear from his mother. Not even the best hacker can defeat a mother's ability to detect bullshit.

Genocide: I think I'll be all right.

Mom: I sure as hell hope you'll be. We don't need this right now.

Genocide: I know. I think they may want to talk to you.

Mom: Why me?

Genocide: Because they probably think I'd talk to you about it.

Mom: You mean like now?

Genocide: I guess.

Mom: That's asinine!

Genocide: I thought you might think of it that way.

Mom: Get home.

Genocide: Okay. I'm on my way.

^()<[]>()*^*

Not long after the FBI showed up at the 2600 club meeting, the university froze Genocide's network account. They wanted to find the Genocide2600 Web page and review its contents for links to the hack against the "Moon" server. Although dozens of software programs and text files were found, the authorities could not link Genocide to the hacked PolarNet account. In addition, although the FBI knew that the dial-up connection made during the "Moon" hack was initiated from the university, they couldn't prove who was sitting in front of the computer at the time of the hack. They could prove that Genocide was in possession of classified government data that was not supposed to be in the public domain, but there was no smoking gun that pointed to him as the person responsible for stealing it. Genocide told them that he had downloaded it from the Internet, and that he couldn't remember where he found it. Three weeks and a dozen missed classes later, Genocide's access to the university network was restored—as if the school's system administrator had ever really been capable of keeping him out.

Genocide wasn't home when the FBI showed up at his house and began questioning his mother about his upbringing, personal relationships, and computer use. The questions drilled deep into Genocide's past. The agents were trying hard to build a profile of the young hacker. Fortunately for Genocide, his mother didn't know the first thing about his hacking capabilities. And even if Genocide had told her, she probably wouldn't have known what he was talking about. The FBI also asked about Genocide's relationship with his brother, suspecting that one of them was acting as the mentor and the other as the hacking protégé.

Genocide was indeed the older brother and the mentor. His younger brother looked up to him and was the type of person who could not refuse a challenge. Although Genocide influenced his brother's computer use, he

always believed that his younger brother was the more intelligent of the two and a "genius" when it came to math problems. But patience and persistence are important personality traits in a hacker, and Genocide's brother had neither. His brother often quickly grew bored with things, and working on computers went from being an obsession to something he did just to pass the time. Genocide's brother is currently passing the time in a Fairbanks jail for an offense unrelated to hacking.

The 2600 group was never quite the same after the FBI reared its head and crashed the party. The less committed members of the group stopped attending the meetings out of fear of being kicked out of school. Then the university slammed the door on all 2600 group meetings. That was when Genocide and the rest of the core members of the group formed the official Genocide2600 group. They would never again meet in a public place or advertise their meetings, but their dedication to the hacker ethic would remain intact.

^()<[]>()*^*

It was late on a Friday night, and the Genocide2600 group was holding one of its planning sessions. Of course, the discussion repeatedly turned to Genocide's run-in with the pinhead in the blue suit from the FBI. From there, the rant moved on to the university's complete lack of understanding of the hacker lifestyle, the importance of hackers to the Internet security community, and the school newspaper's obsession with the so-called dangerous hacker who'd been hijacking student network accounts. The hacker ethic was under assault. The forces of ignorance were on the offensive.

But that never changed Genocide's way of thinking about hacking. He never said that he abided by the law 100 percent of the time. Sometimes bending the rules was necessary. The hacker community, the government, and the general Internet community were the equivalent of three superpowers engaged in an arms race. If one of those superpowers were allowed to develop offensive hacking tools in secret, like the owners of the "Moon" server, then the balance of power might be tipped in favor of one group. That, in turn, could lead to a dangerous situation, especially if the one group with all of the tools was the government. In addition, banning one group from having access to knowledge about hacking could spark a heated revolt and lead to the creation of more dangerous hacking tools. Hackers, therefore, were a legitimate force and were as important to the balance of power in the Internet security arena as any other group of users, especially the government.

Hacking was all about the pursuit of truth and not allowing one group of people to deny other groups access to the truth. Allowing the truth to be hidden was unacceptable to Genocide. The true crime was not hacking, but the reluctance of others to rip the veil from the sheep's eyes. "We aren't the criminals that need to be put away. We are the ones you should praise," Genocide wrote in his Hacker's Manifesto in 1997. Sure, other groups and individuals had published manifestos, but none were like this one:

The Social Base of the Hacker
The Genocide2600 Manifesto

> *People generally believe that hackers have malicious intent as a general rule. This, pardon my language, is a crock of shit and obviously the idea/ramblings of the most generally uninformed people on the net. I do admit that "YES" there are those that are out to only destroy, and yes this group does occasionally add to that at a very small percentage (this will be explained later). But for the most part, we are in the pursuit of knowledge. I do not claim to be a 100% law abiding person, nor does the group. Obviously, if you have heard of us, or even after reading this, you will be shaking your head at this point.*
>
> *People for all time have feared what they do not understand, what they do not know. You don't know us; you don't understand us. Some have labeled us as terrorists, others as criminals. Ok. Sure. Whatever. Go ahead take the criminals and terrorists away that fight for your rights. After you have lost the battle because your soldiers are gone at your own hand, you'll have no one to blame but yourself. We fight with the greatest tools of all, our intellect and courage.*
>
> *As a whole we believe in a collective good. We believe that people who try to shut out other people, or people who try to censor our actions, language and activities are the people who deserve none of the above. We cling to our most basic civil rights. We also believe in retribution for what is lost. Eye for an eye mentality is spoken here. Take back what is yours. Bottom line is this: Don't [f***] with us. We do [f***] back.*

These were dark times for hackers. But Genocide had crafted a rallying call for his group. They had a higher calling, a mission, a cause, and a raison d'être. He recalled the group of young hackers acknowledging privately that what they were doing was wrong, but nobody considered their hacking exploits criminal. Or, well, maybe it was. "Perhaps we knew in the back of our mind but we didn't want to admit it at the time," Genocide recalled many years later. "It didn't seem like the wrong path. It was adventurous. All of us were adventurous. It was like leaving an etched path to find your own way. We

were doing things and going places that most people never even dreamed of. It's sort of the same thrill that a trailblazer gets."

It didn't matter that nobody understood them, or that people didn't take the time to even try to understand. The Genocide2600 group decided it would play its small part in the defense of the hacker ethic. And what better place to show people the good side of hacking than in the chat rooms of America Online, where child pornographers still managed to trade their lowly merchandise.

Attacking pedophiles online was not only a good way to spend a few hours during one of the group's Friday-night versions of modern-day LAN parties; it was also a lot of fun. "It's just something I couldn't stomach," Genocide recalled later. "One of those unforgivable things man does to man. I feel the same way about things like women being beaten by men, people being denied education, freedom of speech. This just was a problem where I might be able to make a difference, and honestly, no matter the energy or resources I or the group exhausted, if one child feels the benefit, then it was all worth it."

A program called AOHell, written by another hacker named Da Chronic, was the tool that the group used to hack into private AOL chat rooms in search of child pornographers and zap them with e-mail bombs that would crash their systems right in the middle of their depraved, heinous dealings. Genocide and the rest of the group scanned the chat rooms for pedophile low-lifes, and the AOHell program alerted them to individuals who were discussing child pornography. When they found somebody engaged in this activity, they attacked like a pack of wolves. Within seconds, their prey's Internet connection would be broken. Then the scumbag would reconnect, and wham! The Gencoide2600 hackers hit him again.

Sure, using the AOHell program was technically against the law. But for a hacker not to take action in this situation would be the equivalent of a pedestrian who witnesses an automobile accident and refuses to help the injured for fear of a lawsuit. It would be unconscionable. And real hackers were not unconscionable villains. Genocide was a real hacker.

^()<[]>()*^*

By this point, Genocide's hacking had taken on a life of its own, as had the Genocide2600 group. For months, Genocide struggled to figure out how a college degree in art fit into his life. The answer was that it didn't. And so he left Fairbanks without a degree and began peddling his hacker skilz in search of his pot of gold in the computer industry.

The move was a professional success, and a personal disaster. Genocide paid a steep price for the relatively high-paying job he obtained in the computer security industry. Unable to accept the fact that he was leaving Fairbanks, Genocide's mother "disowned him," to use Genocide's words. So he moved to Oregon alone and without the support of the mother who had shown him endless reserves of strength during his years growing up in a small shack on the side of a hill in central Alaska. Genocide looked back on the episode as another of life's tough, unfortunate lessons.

The move to Oregon, however, did not mean the end of the Genocide2600 group. By now, the group was many times larger than its original five members and spanned several states. Genocide hand-picked regional organizers from the pool of new recruits. Most remained out of the public spotlight, anonymous, behind the veil. Genocide took the biggest risk of the group by maintaining the public Web site. But that was okay. After all, Genocide was the organizer, the planner, the tactician, and the leader.

After he settled into his new digs in Oregon, Genocide moved the Genocide2600 Web site to a new Web server in Portland called Aracnet, where the site's traffic really began to skyrocket. Pirated "warez"—wares—and serial numbers were bigger than ever. And so was the group's popularity. Journalists started to call, and the number of e-mails from admiring wannabe hackers looking for training doubled.

Then the flame war started, with a popular antivirus software vendor leading the charge against Genocide's pirated serial number business. Aracnet froze Genocide's Internet account. Genocide faced possibly thousands of counts of software piracy. But when you're as good as Genocide and his hand-picked team of hackers, things have a way of disappearing from servers, of getting up and moving on their own.

Genocide's account at Aracnet was a simple shell account. To keep him out while the software vendor and the FBI amassed evidence of his software piracy, the ISP implanted an asterisk in his encrypted password file. This is what it looked like:

Before:
genocide:2a08ivnO:1001:1001::0:0:Genocide,,,:/home/genocide:/usr/local/bin/bash

After:
genocide:*2a08ivnO:1001:1001::0:0:Genocide,,,:/home/genocide:/usr/local/bin/bash

The addition of the asterisk changed the password to something that could not be guessed because of the unique method Unix uses to perform one-way

password encryption. It was simple, but very smart. However, if the administrators at the ISP had been really smart, they would have created a "tar ball"—a Unix command that creates a tape archive, or tar, that combines multiple files into a single, tightly wrapped file, like a ball of tar. Then they could have given it a random name and stored it on a secret server for the feds to access and build their case.

Instead, the system administrators left the account exactly as Genocide had created it. Bad idea. All Genocide and the other members of the Genocide2600 group had to do was find a hackable server, gain root access, unfreeze the account, back out and erase their tracks, and then log back in using the freshly unfrozen account. From there, deleting data was simple.

With the evidence gone, Genocide2600 remained untouchable. Operations continued at their normal pace. An East Coast cell was established under the tutelage of an expert at social engineering. Now the group was national. And not everybody was a hacker in the technical sense of the word. There were people of all ages and professions, some of whom were complete computer novices but who also donated their time and expertise to the group. Specialization took on new meaning.

^()<[]>()*^*

The timing of the voicemail from the FBI agent was uncanny. It had been only three days since Genocide had seen to it that the evidence of the serial number and pirated software operation had been conveniently lost.

It was about 10 o'clock in the morning. Genocide was at work. His pager began to beep, like it always did when he had an urgent message waiting for him on his home answering machine. He called his machine and entered the secret code to retrieve his messages. There was only one. It was from a man who called himself Mr. Jerkins. He said he was from the FBI, and he wanted to meet with Genocide for a talk.

There are only a few telephone calls that a person might receive during a lifetime that will undoubtedly make the hair on the back of the neck stand up. One is a call from a neighbor while you're on vacation informing you that your home caught on fire. Another is a call from your stockbroker apologizing and then saying you should have sold when you had the chance. Another is a call from an FBI agent who wants to get together with you and "talk."

Genocide went into a state of panic and called an emergency meeting of the local Genocide2600 members for later that night. They must have played the tape a dozen times. They nearly wore the tape thin trying to figure out if this Mr. Jerkins was some poser playing a joke. The voice sounded official, but that

wasn't proof enough. His choice of words was cool and detached, and he dispensed them with no obvious slip-ups immediately evident to Genocide's social engineering experts. There was only one way to find out for sure. A meeting was set up.

Mr. Jerkins and three other agents showed up at Genocide's apartment the next day. They were five minutes early. They asked if there was someplace they could go to talk. Having lived in Oregon for only three months, the only safe, public place Genocide could think of was the local burger joint down on Glenn Echo Street about a mile away. They all hopped into a late-model Ford Crown Victoria and drove down the road. Nobody talked. Mr. Jerkins drove with all the seriousness of a funeral procession.

Heads turned when the four suits walked into the restaurant flanking a young guy in a black leather jacket and a black shirt that said "Un-natural disaster, can you feel hells laughter?" The agents waited while Genocide ordered—burger, fries, and a coke; nothing fancy. Oh, and a shake. Burgerville made the best shakes in Milwaukie, Oregon.

Jerkins did all the talking. As soon as he opened his mouth, it became clear that the agents were there to pressure Genocide to switch sides. There was no arm twisting involved, but the agents' intent was clear. Genocide had skills they could use—and better to have him on their side than working against them. They threw a brown manila folder on the table, but Mr. Jerkins put his hand on it when Genocide tried to take a look at it. It was, ostensibly, Genocide's FBI file. Jerkins alluded to all of the information they had collected on Genocide while watching him, both online and offline. They told Genocide that they knew where he was heading, even if he wasn't so sure. Federal prison was the way Jerkins put it.

Genocide feigned being the wide-eyed youth that the feds thought he was. Not once, however, did he let on that they were right about him, that they had him figured out. He told them that he would need to think about their "offer" for a day or two.

Almost as soon as the Ford Crown Victoria pulled up at his apartment, Genocide hopped out and slammed the door. He went straight into his apartment and thought about what the agents had just asked of him. That lasted for about a nanosecond. There was no way he was going to do it. Genocide couldn't be rolled that easily. He rifled through his dresser drawers and got out several fake IDs and a phony passport. Then he counted the money he had in his wallet and factored in how much he had in the bank. What he came up with, however, wouldn't get him very far. Running was not an option.

He threw his IDs back in the drawer. A deep sense of relief came over him. Running was for Mitnick, not for Genocide. So he went to his computer and began drafting an e-mail to the other members of Genocide2600. His hands seemed to shake uncontrollably, but he managed it. The e-mail was simple:

> *I've just been offered a job.*
> *In two weeks the Genocide2600 server goes up, the new dawn.*
> *http://www.Genocide2600.com.*
>
> *-Genocide*
> *Head of the Genocide2600 Group*
> **Embrace Freedom**

The new Genocide2600 Web site

^()<[]>()*^*

To this day, Genocide is reluctant to provide more details about the hacking exploits that led the FBI to his doorstep and the many other hacks that the authorities doubtless know nothing about. Like many hackers who have cut

their teeth doing not-so-popular and not-so-legal things, Genocide understands the finer points of the statute of limitations.

But there is one current activity that Genocide is happy to talk about: his work with EHAP, Ethical Hackers Against Pedophilia. EHAP is a nonprofit organization composed of hackers and other concerned citizens that use, in the words of the organization's mission statement, "unconventional and legal tactics" to help law enforcement officials track down adults who exploit children online. Genocide has spent the last several years helping EHAP rid the Internet of those who traffic in child pornography. It has been one of the most satisfying aspects of Genocide's hacking career. He has passed information on suspected pedophiles to some of the very same FBI agents who paid him a visit years earlier.

At the age of 26, Genocide bears the scars of an experienced hacker. There are other scars, too. It's been about a year since a short-lived marriage ended in divorce. Likewise, his mother remains a stranger to him. But the memory of that small, wooden shack that sits on the side of a hill in Fairbanks, Alaska, shines bright. It is a symbol of what a person can do, of earning his hacker stripes and rising up from nothing and landing a well-paying job for a major computer hardware and software manufacturer. "I'm just your standard mild-mannered security guy," he says.

Genocide2600 now claims more than 100 members from coast to coast. But the days when hackers had the upper hand because of clueless system administrators are over, acknowledges Genocide. "Today, admins are sharp, weathered hackers themselves, and they're college trained and field tested," he says. "This calls for a whole new approach for hackers. You can't just pick up a script, kick it off, and watch as systems fall to you without getting tracked right back to your front door and busted all in one single movement."

Genocide2600 has certainly evolved since its formation in 1995. Some members of the group are married and have kids. Others are single, mere kids themselves. But the questions about the group's namesake continue. And that brings us to where we started: ignorance breeds contempt.

When it comes to the hacker underground, people choose to see what they want to see and believe what the media feeds them. Genocide would change the name if he could. But there's too much history there. And it was never about hate and racism anyway. The Genocide2600 group is not the band of Internet terrorists that the name might imply to some people.

"The point is, we could be your neighbor or your babysitter for all you know," says Genocide. "We could be the kid filling your gas in your car. It doesn't matter. All you really need to know is that we are spreading as fast as knowledge…at the speed of information."