[IP host]

hackers gone wild

the fast times & hard fall of the green hat gang

how three teenage friends, fueled by sex, drugs and illegal code, pulled off the biggest cybercrime of all time

// by sabrina rubin erdely

THEY'D BEEN HIGH ALL WEEKEND LONG – ON ECSTASY, COKE, MUSHROOMS AND acid – so there seemed little harm in doing one last bump of Special K while they packed up to leave their $5,000-a-night duplex in South Beach. For the past three days, the three friends had barely bothered leaving their hotel, as a dozen club kids in town for Winter Music Conference, the annual festival that draws DJs and ravers from all over the world, flocked to their luxury suite to partake of the drug smorgasbord laid out on the coffee table. But even stoned on industrial-grade horse tranquilizers, Albert Gonzalez remained focused on business – checking his laptop constantly, keeping tabs on the rogue operators he employed in Turkey and Latvia and China, pushing, haranguing, issuing

the nonstop party

Albert Gonzalez's crew lived a lifestyle as outrageous as their crimes. **(1)** Albert stole 170 million credit-card numbers while relaxing at places like New York's Hotel on Rivington. **(2)** Patrick Toey was his best operative, and **(3)** Stephen Watt was the group's coding genius. Their cybercrimes netted millions **(4)**, enabling Albert to throw a $75,000 birthday party for himself and Stephen at an exclusive New York club **(5)**.

orders into his cellphone in a steady voice. "Let's see if this Russian asshole has what I need," he'd say calmly. Then he would help himself to glass plates of powder, each thoughtfully cut into letters for easy identification: "E" for Ecstasy, "C" for coke.

Albert's two friends were in no shape to think about work. Stephen Watt, a freakishly tall bodybuilder, was planted on the big leather sofa, immobile as the hotel suite's potted palm. Only 23, Watt was the group's coding genius, who until recently had been employed in the IT department at Morgan Stanley, the giant Wall Street investment bank. Patrick Toey, 22, Albert's most loyal foot soldier, was lazing around the suite, staring at the Miami seascape through the two-story picture windows, letting his thoughts drift.

"Listen, I need you to do this now," Albert was saying in a firm voice as he set his laptop on the desk in the master bedroom upstairs. For weeks, he had been badgering Stephen, known in hacker circles as the "Unix Terrorist," to refine a crucial bit of code for him. They were in the midst of pulling off the biggest cybercrime ever perpetrated: hacking into the databases of some 250 companies – including Barnes & Noble, OfficeMax, 7-Eleven, Boston Market, Sports Authority and DSW – and stealing 170 million credit-card numbers. But unless Albert could get Stephen to focus, the whole thing was in danger of falling apart.

"Now that I've got you here, I need you to do it, or it's never gonna happen," Albert urged. The whites of his brown eyes had gone veiny from the K, but he was still the ringleader, still in control.

Stephen somehow managed to climb the suite's glassed-in staircase and sit down in front of the laptop, but nothing he saw on the screen made any sense – his brain was scrambled beyond comprehension. "Dude," he wailed, "I can't fucking read!"

Albert didn't miss a beat. "Patrick, what about you?" he called out. "You sober enough to do this?"

Patrick moved toward the desk as if underwater. "Uh, this is going to be difficult," he said. "But at least I can read."

Stephen pitched over onto the master bed, where, eyes closed, he groggily dictated code to Patrick, who laboriously typed it out, letter by letter. The task at hand seemed impossible, given their chemical impairment, but Stephen was notorious among hackers for his ability to dash off intricate code that could blast through even the most secure computer networks. Finally, after 10 minutes of following Stephen's directions, Patrick hit the RETURN button and declared the program functional. "Thank God," Albert pronounced, his eyes widening with relief and excitement. Together, the three friends had just succeeded at putting some finishing touches on a vast criminal enterprise, one that U.S. Attorney General Michael Mukasey would call "the single largest and most complex identity-theft case ever charged in this country."

Only 25 years old, with little more than a high school education, Albert had created the perfect bubble, a hermetically sealed moral universe in which he made the rules and controlled all the variables – and the only code that mattered was the loyalty of his inner circle. He even had an insurance policy, one designed to keep him a step ahead of the federal agents charged with tracking cybercrime: For the past four years, Albert had been working as an informant for the Secret Service, helping federal agents to identify and bust other rogue hackers. His double life as a snitch gave him an inside look at how the feds try to safeguard the nation's computer data – and reinforced his own sense of superiority. "Psychologically," his sister later told a judge, "it was feeding an obsession that in the end would become my brother's downfall."

But as Albert stood in his South Beach hotel room in March 2007, getting caught was the furthest thing from his mind. The coding work complete, he briskly snapped his laptop shut and hustled his friends down to the Loews' marble-floored lobby, where, acting as sober as possible, he settled their $17,000 bill for the weekend, paying mostly in twenties. Knowing it would take a while to count that much cash, the hotel manager ordered a round of frozen daiquiris for the gentlemen. For now, as the three friends sipped their drinks and hypnotically watched their stacks of cash being counted right in front of them, Albert felt untouchable.

While Albert Gonzalez ran his vast criminal enterprise, he also worked as an informant for the Secret Service, helping federal agents bust other rogue hackers.

When ALBERT GONZALEZ was 12, he bought a computer with the allowance he had saved up working for his father, a landscaper. At first, his new hobby seemed a harmless distraction: He played video games – car racing and wrestling, mostly – and spent hours taking the computer apart and putting it back together. He even set up computers for other families in his working-class neighborhood of Miami, where most of the residents, like Albert's father, were first-generation immigrants from Cuba. But Albert's fascination soon turned into a fixation. "It was already like an obsessive vice," his mother, Maria, would later tell a judge. By the time he entered South Miami Senior High, the once-outgoing Albert had turned isolated and untalkative, his grades plummeting as he neglected his homework in favor of the huge programming textbook he had bought. Maria begged her son to see a psychologist.

"No," Albert told her. "I am not crazy."

"You don't have to be crazy to go to a psychologist," his mother pleaded, but Albert was unmoved. "If you take me, I'm not going to talk," he warned. "I'm just going to stay quiet." When she moved the computer to his sister's room, Albert simply snuck in during the night to log on to chat rooms devoted to computer programming. Albert's father, who had fled Cuba in the 1970s on a homemade raft, took more drastic action: Enlisting the help of some policemen friends, he staged a fake arrest of Albert, trying to scare his son into returning to reality.

That didn't work either. Instead, Albert escaped further into the solace of the world of programming chat rooms – where he called himself "soupnazi," after the grumpy *Seinfeld* restaurateur. Before long, he discovered Internet Relay Chat, a web forum popular with hackers who discussed the how-tos of breaching Internet security at its highest levels. He had stumbled across a community that shared not just his computer obsession but also his caustic humor and profound alienation in a way his real-life peers didn't get. Albert and his online friends spent hours swapping tips on hacking, debating their favorite bands and trading booger jokes. By the time he graduated high school, in 1999, Albert had already hacked into the websites of NASA and the government of India – cyberfeats that had prompted visits by Miami detectives and the FBI, who warned him to cut it out.

At this point, Albert wasn't trying to cash in on his skills as a hacker; he simply relished the intellectual puzzle of network security, the powerful rush of picking the locks of high-tech vaults. It wasn't about stealing anything – it was more the gloating rights, about showing the straight-world programmers that he was better and smarter than them. But Albert wasn't just a typical misfit hacker. He was also that rarest of computer geeks: one who could actually relate to other human beings. He was the perfect fusion of the dorky and the suave – the easygoing charm of George Clooney combined with the tech-savvy drive of Steve Jobs. With his good looks and smooth confidence, Albert was never at a loss for female company. And with the guys, he was always the man with the plan. "Albert's an alpha," says a close friend who met Albert online. "If you're all sitting around doing nothing, he's the one who picks a direction and goes, and everyone goes with him."

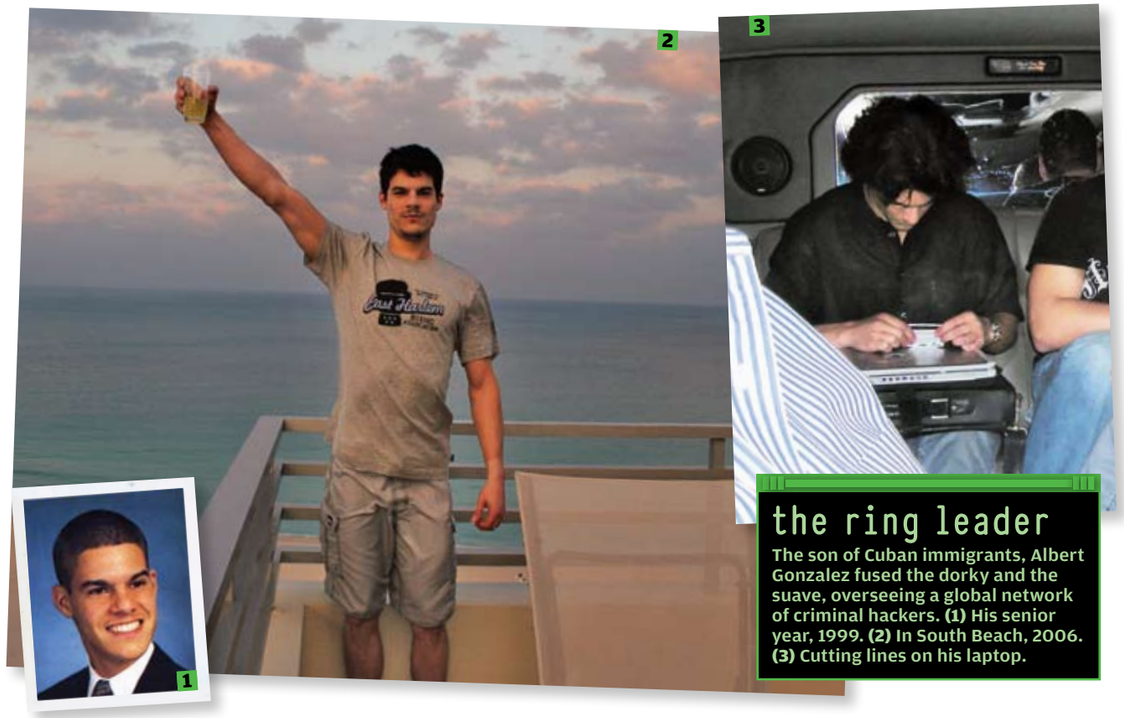
One night in 1999, a few months after graduating from high school, he decided to drive three hours from Miami to Melbourne, Florida, to meet one of his online friends, a coding whiz who went by the chat-room handle "jimjones." Stephen Watt was a gangly, high-strung, seven-foot-tall senior – only 16 years old, he had skipped a grade – with a 4.37 GPA and few friends. It was past midnight when Albert's headlights finally appeared in the driveway, where Stephen met him for fear of waking his conservative parents. The boys snuck through the house and into Stephen's room, where Albert promptly produced a homemade bong. "No, thanks, I'm good," Stephen mumbled; he had never tried drugs before. They went on to have the best weekend ever, driving aimlessly around town, hanging at the mall, talking computers. A favorite topic was their shared loathing of "white hat" hackers, who used their computer expertise to help businesses find and fix network vulnerabilities. White hats ruined all the fun for "black hat" pranksters, and Stephen – who was as histrionic as Albert was laid-back – could rant for hours about the evils of white-hat sellout phonies.

"He wasn't as interested in the ideology," Stephen would later recall. Albert just wanted to hack shit for fun – and maybe for profit. Not as a white hat, of course; he'd never sell out. Instead, he coined a new term to describe the role he saw for himself. He'd be a "green hat" – the color of money. Albert wanted a wife and kids someday, and he could already foresee that raising a family would require some serious cash. "What good will a couple million dollars do?" he asked Stephen. "You have health problems, your kids need braces, you pay for their college – your money goes right down the drain."

Albert's initial attempts to succeed in the real world got off to a rocky start. He dropped out of Miami Dade Junior College in his first semester, bored by his intro computer courses, and moved to New York to work for a dot-com firm that soon went bust. He landed another job, at Siemens, but bailed when the company moved to Pennsylvania. In 2002, unemployed and liberally self-medicating, Albert took his first stab at being a green hat: He became one of the leaders of an Internet "carding" forum called Shadowcrew, where thousands of international criminals exchanged services, from selling fake driver's licenses and Social Security cards to stolen credit- and debit-card numbers. But while Albert was good at orchestrating such deals, he didn't know how to stay off the police's radar. In 2003, he was arrested in New Jersey after withdrawing money with a fake bank card from an ATM. He had 15 phony cards in his possession.

Where another hacker might have seen jail time, Albert saw opportunity: He allowed himself to be recruited as a key informant for "Operation Firewall," a federal cybercrime task force that was trying to take down Shadowcrew. Albert proved to be a diligent snitch, ratting out his fellow hackers to the Secret Service. At the same time, he was studying the agents he worked with – their tactics, their mindset – and realizing how little they actually understood. "These people are fucking retarded about anything other than jumping in front of a bullet," he told Stephen, insisting that they knew too little about computers to have any real impact on cybercrime. In a perverse way, his work for the government only encouraged his criminal behavior and pushed his wayward ambitions into the stratosphere. In Albert's mind, his value to the Secret Service reinforced just how special his skills were – and what a unique position he was in.

"That is a very big problem with using sources," says E.J. Hilbert, a former FBI



the ring leader

The son of Cuban immigrants, Albert Gonzalez fused the dorky and the suave, overseeing a global network of criminal hackers. (1) His senior year, 1999. (2) In South Beach, 2006. (3) Cutting lines on his laptop.

PREVIOUS SPREAD, CLOCKWISE FROM TOP: COURTESY OF STEPHEN WATT; 4: COURTESY OF ANTONIA RODES. THIS PAGE, FROM LEFT: COURTESY OF SOUTH MIAMI SENIOR HIGH SCHOOL; COURTESY OF STEPHEN WATT

SABRINA RUBIN ERDELY *wrote "The Yoga Cult" in RS 1098.*

the coder

Stephen Watt was Albert's best friend, a seven-foot bodybuilder who worked at Morgan Stanley. Famed among hackers as the "Unix Terrorist," he could dash off code even while stoned on Special K.

cybercrimes agent who went undercover for Operation Firewall. "While working as an informant, Albert obtained insight. Even if his handlers tried to not show him everything, he got a pretty good idea of how things were going to play out." In October 2004, the feds arrested 28 members of Shadowcrew for stealing 1.5 million credit-card numbers – thanks in part to information supplied by Albert. By that point, however, Albert already had a big plan of his own under way. He named it "Operation Get Rich or Die Tryin'."

IT DIDN'T START OUT AS SOME well-organized criminal enterprise. "It wasn't anything *official*," recalls Patrick Toey. "It was just something I was doing for money. And as a favor to Albert. Because he was a friend."

In Patrick, Albert had found his perfect street operative. The two had become fast friends through Internet Relay Chat, but they didn't begin hanging out until four years later, in 2003, when Patrick boarded a bus from his home in Virginia Beach and headed to New York for his first "cash-out" trip as a member of Shadowcrew. Only 18, Patrick was making the trip with the blessing of his mom, who needed the rent money.

Arriving in New York, Patrick climbed into Albert's Honda Accord, where he helped himself to a pot cookie from a package at his feet. He and Albert had come prepared for their mission with stacks of blank ATM cards, procured online, upon which they had encoded stolen account data by swiping them through magnetic-stripe readers plugged into their laptops. Together the two friends began scurrying from ATM to ATM with the rigged cards, punching in the PIN numbers they had scribbled on the cards with a Sharpie. Soon the pockets of their cargo pants were bulging with twenties.

Raised in a down-and-out home with a shifting cast of characters, Patrick had started smoking pot at 11, left school at 15 and, shortly thereafter, was busted by the FBI for hacking an Internet service provider. With his lanky swagger and shorn blond hair, he bore a passing resemblance to Eminem in more ways than one: Patrick was also a furious intellect who always seemed one step away from self-immolation. An aimless loner and reliable hacker, he was quiet and laconic, except when provoked – in which case he was always up for a brawl. "If Patrick gets pushed to his limits, he's ready to throw down, a zero-to-90 kind of thing," Stephen says admiringly. "He's like the skinny guy you gotta watch out for, the one who's really fucking crazy."

Operation Get Rich began in Miami. Hackers recruited by Albert would drive up and down U.S. 1, a busy artery of strip malls and traffic lights, with their laptops open, searching for retail stores with open wireless networks, a technique called "wardriving." When they found an open network, they would park in a nearby lot or rent a hotel room close by and swiftly hack into the store's payment database. Then they would bide their time. From that point on, each time the store swiped a card, the hackers could capture its data and send it on to Albert. Albert would then forward the data to Patrick and other hacker allies across the country, who would decrypt and encode the data onto bank cards, cash them out at ATMs, and mail Albert's share to a drop box in Miami. Raised as a Catholic, Albert felt a pang of guilt about the people whose accounts he was raiding – "We're definitely going to hell for this," he told Patrick. But once the fraud was detected, Albert rationalized, the credit-card companies would restore people's money. "And he didn't give a fuck about the credit-card companies," says Patrick.

It was a decent plan but inefficient and risky: Each exploit was limited to a single store, and the hackers were sitting ducks out there in the parking lot for hours at a time. "Being parked out front with an eight-foot antenna isn't the most graceful way of getting in," observes Patrick. What Albert needed was a "sniffer code," a hacking program that would intercept payment data at a higher level. With a well-crafted code, he could follow the chain of network vulnerabilities up from a retail store and into its parent company's larger corporate database, capturing far more data with far less exposure. Albert lacked the technical skills to write such a code himself, but he knew exactly who to call for help. He fired off an IM to Stephen Watt.

By then, Stephen was working in the IT department at Morgan Stanley in New York, having graduated from college at 19, but he found the nine-to-five existence of cubicles and coffee breaks stifling. He lived for the weekends, when he would head to after-hours clubs and trip on LSD, which had quickly become a cornerstone of his lifestyle. He also spent his off-hours writing whatever computer code Albert asked for, including programs to break into networks at bizrate.com and Florida International University. Conventional ethics meant nothing compared to the brotherhood of the hackers. "I never had a moral problem giving him something," Stephen says. "As a friend, my willingness to please him may have overshadowed the way I saw my own moral responsibility." Despite having never lived in the same city, he and Albert had grown even closer over the years. At one point, when Stephen and his live-in girlfriend broke up, Albert had flown up from Miami to help him move, telling Stephen that he needed to drive the U-Haul because Stephen was such a lousy driver. "He spent more money getting to me than I spent on the move," recalls Stephen.

So when Albert asked him to write a sniffer code, Stephen was happy to oblige. He dashed it off in 10 hours – an eye blink, in hacker time – giving it the throwaway title "blabla." He knew better than to ask what Albert needed it for. "Albert was very careful not to give any of the people he worked with, myself included, too much information," Stephen says. "But we all knew what we were getting into."

COURTESY OF STEPHEN WATT, 2

USING STEPHEN'S SNIFFER code, Albert and his crew could now hack their way into corporate networks and download debit- and credit-card numbers by the millions – along with user info, passwords and PIN numbers. Albert would then transfer the data onto servers that Patrick had set up in Latvia, Singapore, China and Ukraine, where associates Albert had recruited online would use the information to drain bank accounts and ATMs worldwide. By late 2005, the money being FedExed to Albert's drop box in Miami was arriving in stacks of up to $370,000. Operation Get Rich was paying off.

But Albert wasn't satisfied. Reaping the cash via ATMs, he realized, was too risky – after all, that's what had gotten him caught before. It would be safer and more profitable to simply sell the card numbers to other people and let them worry about getting the cash. So Albert enlisted the services of Maksym Yastremskiy, a 22-year-old Ukrainian cybercrime lord. ("The card 'dumps' are all run by Russians," says Patrick, "so they have the most clientele.") Yastremskiy arranged to have the payment data encoded onto bank cards, which were then sold at nightclubs all over the world for $300 a pop, of which Albert got half. To launder the money before wiring it to Miami, Albert used the offshore Internet-based payment systems WebMoney and E-gold. He had become the consummate businessman, even coining a name for his venture: Green Hat Enterprises. It was a huge, globe-spanning operation, with Albert at its epicenter. "He's just a genius at bringing people together," says Patrick.

Albert had a lot of players to keep tabs on, a feat made even more difficult by his insistence that they talk business only via encrypted IMs. He checked constantly on Yastremskiy – who, trotting across Eastern Europe, was seven hours ahead – asking for the latest sales figures and urging him to sell his cards "fast fast." Albert had two Russian hackers on the payroll as well, who did much of his online dirty work. In New York, there was a Barclays programmer who helped Albert launder as much as $800,000 but whose behavior was becoming so erratic that Stephen bought a drug-testing kit to threaten him with, at Albert's behest. Back in Miami, Albert was keeping a wary eye on a hacker employee who was starting to flash his newfound wealth a bit too conspicuously, spending close to six figures for a replica of a chain featured in the rap song "Diamonds on My Neck."

As Operation Get Rich or Die Tryin' got under way, money – drained from banks around the world – was Fed-Exed to Albert's drop box in Miami, arriving in stacks of up to $370,000.

Business was booming. "I have a goal," Albert gleefully IM'd Yastremskiy. "I want to buy a yacht like Roman Abramovich" – one of the world's wealthiest men and owner of the world's largest private luxury boat. Albert started pulling in so much cash that he complained to Stephen that he had been forced to count $340,000 by hand because his money counter was broken from overuse. "Fucking BULLSHIT," he IM'd. "This is the 2nd money counter to break this year." Stephen responded with several pages worth of LOLs.

He and Albert talked every day, discussing everything – including Albert's double life as a government informant. At one point, Albert even brought Stephen down to the Secret Service's headquarters in Washington and introduced him to his handlers, who were interested in utilizing Stephen's technical skills. (Stephen declined their pitch.) In an IM, Albert reported that he had wowed federal agents with a presentation on how "malware" – malicious hacking programs – had evolved over the years.

"It's easy to impress these people," he boasted to Stephen. "And that's good."

AS ALBERT'S CRIMINAL EMPIRE grew, he began to indulge in the lifestyle of a minimogul – and he wanted his friends to share in all the debauched experience that his new wealth allowed. In 2005, Albert and his crew made their first trip to Winter Music Conference in South Beach, where they hit the Miami clubs. But the scene annoyed them: Bouncers with attitudes, waiting in line for drinks, sneaking into the bathroom to do drugs – it seemed beneath them. "We didn't want to rub up against the prickly shaved forearms of the guidos," recalls Stephen. "Even though there's great music, the crowd is garbage, people that look like fucking Ronnie and J-WOWW from *Jersey Shore*."

So when the friends headed back to South Beach the following year, it was with a different mind-set: They were finished partying with the masses. Now that they had money, they could control their own reality, and design it to their exacting standards. They booked a top-of-the-line suite at the Loews and stayed in all weekend, fortifying themselves with "magic milkshakes" – an insane concoction of cookies-and-cream Häagen-Dazs, skim milk, Ecstasy, mushrooms and LSD. Albert and his crew had long since left weed behind, finding it dull and unrewarding (though they kept a stash of top-quality bud for the girls who passed through their suite). These days, they were seeking the most intense drug experience possible, spinning the wheel of chemical roulette and hoping it landed them at some new, more advanced level of perception.

That summer, to celebrate his 25th birthday, Albert threw himself and Stephen a dual birthday bash in New York, at a cost of $75,000. He rented Sky Studios' penthouse duplex, with its soaring Manhattan view and rooftop pool, and he flew up his favorite pair of DJs, Oscar G and Ralph Falcon, from Miami. "The party was spectacular," recalls Sandra Martinetto, a friend of Stephen's who attend-

ed the party. "Everybody there was beautiful, glamorous, there was a good vibe – it was packed, like all of New York City was there." Some revelers drank champagne from flutes; others sipped water spiked with MDMA. Patrick Toey made the trip up from Virginia, making it the first night – after years of online friendship and criminal co-conspiracy – that he, Albert and Stephen were together in the same room. Stephen spent much of the party working the door, using his imposing height to make sure the right people got in and the wrong ones stayed out. Patrick, dehydrated from all the Ecstasy, couldn't figure out which water glasses were spiked and wound up guzzling them all, plunging himself into slack-jawed serotonin overload. Albert – always the practical, assured organizer – worked the room, having a blast. On the table, uneaten, sat a white birthday cake with the party's sponsor inscribed in green icing: GREEN HAT ENTERPRISES, their own private joke.

As Operation Get Rich continued, their tastes ratcheted upward. By summer 2007, when Albert spent a month in New York, he was dining on Kobe beef and $50-a-shot Johnnie Walker Blue Label. Late night, he and Stephen would head to a club – Cain, PM Lounge, Marquee, the Box – tripping on the psychedelic research chemical 2C-I and dropping $900 for a bottle-service table to draw the girls. When it came time to pay the tab, Albert would peel off a two-inch wad of cash and quote T.I.: "Rubber-band man/Wild as the Taliban." He took home a different girl any night he pleased.

Although Albert styled himself as a high-roller, at heart he remained a frugal immigrant's son. The whole time he was in New York, he crashed at Stephen's one-bedroom apartment in Greenwich Village because he didn't want to waste money on a hotel. "Fuck all the flashy bullshit," he would tell Patrick. "Just getting by is enough when you know you have all that money stored somewhere." He flew coach, bought himself a modest one-bedroom condo in Miami and went to a free clinic when he needed to see a doctor – even though, as he told Stephen, it meant rubbing elbows in the waiting room "with people that look like Trick Daddy." The same guy who spent $75,000 on a single party would spend an hour bargain-shopping online for a $300 printer. "Don't waste your money on a plumber – I can do it," he assured Stephen, repairing his friend's toilet and doing a half-dozen other fix-it projects during his month-long stay.

On the surface, Albert seemed as in control as ever, making everything look effortless: always in motion but never rushed, always finding time to squeeze in his workouts to fine-tune his now-bulging muscles. But the stress of his double life was starting to get to him. As a criminal mastermind, he was keeping daily tabs on a growing constellation of international associates who were stealing data worth millions of dollars. At home, however, he maintained a conventional family life: helping his dad with his landscaping work, doting on his toddler nephew, wooing his on-and-off girlfriend, Jenny Bulas, and her circle of Miami-princess friends. He went to bed each night with his laptop beside him, plugged in but with the battery removed – "just in case," he said, fearing a police raid. Some nights he would be too wired to sleep, and Stephen would play Chopin's nocturnes on his upright piano to lull his friend into slumber. "I used to joke with him, 'If only you were a woman,'" recalls Stephen.

On top of everything, Albert was still working as a federal informant, drawing what he told Stephen was an annual salary of $75,000. (When friends back home asked what he did for a living, he would say vaguely that it involved something computer-related for "the government.") He gave lectures to federal agents on cybercrime and had Stephen and Patrick write code that his handlers could use in their undercover operations. "Me and Albert talked all the time about how fucking crazy it was that he was able to do all this while he was working for the Secret Service," recalls Patrick. "We'd be laughing about it. But I don't know how he dealt with all the stress, living these separate lives."

> Albert booked a suite in Miami, where all weekend he and his friends tripped on "magic milkshakes" – a concoction of Häagen-Dazs, skim milk, Ecstasy, mushrooms and LSD.

His double life was almost blown when another informant told the feds that Albert was using the screen name "k1ngchili" to commit cybercrimes. To disprove the charge, Albert paid a ringer to log in as "k1ngchili" whenever he showed up at Secret Service headquarters. Working as an informant was crucial to his criminal enterprise: Prosecutors later admitted that Albert used government intel to tip off his friends when they popped up on the FBI's radar. Patrick says Albert once warned him to stop selling stolen data on a certain Internet forum, since it was in the cross hairs of an investigation that was about to end in arrests.

It was a lot to juggle – and as Albert's crime operation grew, so did everyone's anxiety. In 2007, when Stephen, Albert and Patrick met up in South Beach for Winter Music Conference, the tension hit a new high. Patrick spent the weekend in agony, curled up on a rollaway cot with an ulcer. At one point, Stephen, in a drug-fueled frenzy, began freaking out: He had recently discovered that *he* had been the victim of credit-card fraud; someone in China had taken out a $4,000 cash advance on his American Express card.

"That fucking Chinaman!" Stephen shouted, standing on the coffee table in bare feet and shorts, balling his fists to the sky. "I am going to hunt him down to the end of the Earth! I will take a sword and drive it through his spine!" Albert and Patrick laughed hysterically as the rant went on and on. Then Stephen suddenly turned to Albert.

"If I found out it was you—" Stephen growled. He thought he saw a shadow of concern cross Albert's face. "Seriously, dude," Stephen said. "I want to know if you had anything to do with this."

Patrick froze, but Albert was as cool as ever. "Hold on a second," he told Stephen, pulling out his laptop. "What's your card number?" Stephen flicked his wallet at Albert and left the room to snort another line. When he returned, Albert and Patrick were all smiles.

"You found it?" Stephen asked.

"Surprisingly enough, I did not have your card," Albert said pleasantly. "I searched everything, and it wasn't in there."

"OK, we're cool." Stephen took a deep breath. "It's only me and the Chinaman now." And just like that, everything was good again.

PATRICK LOOKED UP YEARNINGLY at the dropper bottle atop the fridge. Its label advertised a breath freshener, but Patrick knew it was full of liquid LSD. Unfortunately, he had tons of work to do for Albert – he needed to focus. With a sigh of regret, he turned back to his laptop.

By the fall of 2007, Patrick was living in Miami, staying in Albert's condo. Back in Virginia, he'd been living with his mother and running low on money, as always – prosecutors would later say that despite his essential role as Albert's "trusted subordinate," Patrick made only $80,000 from Operation Get Rich. "I thought going to Miami would be kind of fun," he recalls. A few months before, he had driven down in his Acura Integra – the first car he'd ever owned, proudly bought with his criminal proceeds – only to discover that Albert's condo was no swinging bachelor pad but a sorry-looking dump with no blinds on the windows, no sheets on the bed, and little furniture other than a cheap orange couch and a tiny TV. It was located in a Spanish-speaking neighborhood of recent immigrants; within days, someone had stolen Patrick's car. He was stranded, didn't speak the language – and all Albert did was steadily prod him via IM to make sure he was on top of his workload.

Patrick's job was to probe corporate networks for vulnerabilities to a malware attack known as a "sequel injection," which overwhelms the victim's system with meaningless commands until the system gives up and defaults to using the malicious code. As he sat in front of his laptop all day, mindlessly tapping away, he sent a steady stream of IMs to Stephen complaining about the tedium. "Finding these vulnerabilities, you can train a monkey to do it," Patrick says. "But at the same time, hacking is about the path of least resistance. There's no need to overly complicate things if a simple sequel injection can work." To ease the boredom, Patrick kept a full stash of amusements on hand – dozens of Ecstasy pills, an eight ball of coke, a half-liter of ketamine, shrooms, a vial of acid – and spent his off-hours wandering around Albert's barrio in an altered state. "Don't send any more drugs to Patrick," Albert scolded Stephen. "He's been hacking a lot of shit lately" – that is, doing good work.

Albert needed his best soldier in top form: Operation Get Rich was shifting into its most ambitious phase. Although Patrick's attacks were simple, the overall scheme that Albert had devised was quite sophisticated. Rather than sitting outside shopping malls to probe every store within striking distance for vulnerabilities, Albert and Patrick now reviewed lists of Fortune 500 companies to find juicy targets. Then, to find out what kind of computer systems a firm used, they would swing by one of its retail stores and scope out the terminals at the checkout counters. After hacking into corporate databases through company websites, they unleashed Patrick's malware, which they had pretested against 20 different antivirus programs to make sure its presence wouldn't be detected. Using Stephen's sniffer code – which he and Patrick had retooled in South Beach after Albert's incessant nagging – they then downloaded the credit-card data in small, well-timed chunks, so as not to alert a victim's server administrator with unusual amounts of activity. When they were done, they neatly erased their digital footprints as they exited the system and installed invisible "back doors" to provide them with future access. They had thought through every angle, right down to the chain of 20 encrypted IP-address proxies they used to obscure their own location.

COURTESY OF ANTONIA RODES

the foot soldier

Patrick Toey was a street kid from Virginia who dropped out of school at 15. After meeting Albert online, he helped hack into corporate networks in what he now calls "Operation Get Busted or Go to Prison Tryin'."

Still, when Patrick stopped to consider what they were doing, he couldn't help but panic. ("Operation Get Busted or Go to Prison Tryin'," he calls it.) Albert reasoned with him to chill out. After all, he told Patrick, they weren't going to stay in the game forever. Albert's long-term plan was to save enough of their criminal earnings to buy a business – maybe a tire shop – and go legit. On his laptop, Albert jotted a note to himself: "15 million is what I want to have total before I start moving to 2nd phase of laundering it."

Even when warning signs appeared, Albert brushed them off. He might have been the world's leading cybercriminal, but he was also a federal informant, pulling down a paycheck from the U.S. government; he knew from firsthand experience that the feds were tripping over their own feet when it came to catching hackers. One day in March 2008, Albert and Patrick were on their way back from a recon mission at a Miami big-box store when Albert, speeding down the highway in his BMW with D. Ramirez on the stereo, suddenly turned the music down.

"Yo, I think we're being followed," Albert said, eyes on the rearview mirror. Patrick laughed nervously in disbelief, but as Albert slowed for their exit, the faded-gold Camaro several car lengths behind them exited too. Albert drove down a street with two right-hand turning lanes and pulled in behind a bus that was making a stop. "If they get behind us now," he said, "they're definitely tailing us."

The car slowly pulled behind them.

"Shit," Albert muttered. When the bus lumbered forward, Albert made the right turn – and then another sudden right down a side street, followed by three more quick rights, until he had somehow maneuvered *behind* the Camaro. ("He's a ridiculously good driver," says Patrick.) As they followed the car that had been tailing them, Albert took out his phone, called Stephen in New York and ordered him to call one of his Secret Service contacts. "You gotta ask him this question," Albert told him. "Who's following us? Is it the boys in blue or the boys in green?" Blue, for the local cops, could be trouble. But green, for the Secret Service, would be even more worrisome. Why would his own handlers be tailing him?

Stephen relayed the question, and a few minutes later, he was yelling the answer in Albert's ear: "He said it's the boys in green! The boys in green!"

"OK," said Albert, smooth as could be. He stopped tailing the Camaro and drove back to the condo, where he sat down to think. In the end, Albert decided it was nothing to worry about. "Remember," he reminded Patrick as they helped themselves to the vial of LSD. "It's not what they know, it's what they can *prove*."

ALBERT WAS ARRESTED IN MAY 2008 by a team of federal agents. They found him holed up in the National, a luxury hotel in South Beach, with a gorgeous six-foot-tall volleyball player he'd been seeing on the side. Also in the hotel room were a Glock 27, two laptops and $22,000 in cash. Buried in the backyard of [*Cont. on 90*]

[*Cont. from 71*] his parents' house, agents found a barrel with $1.1 million in cash wrapped in plastic bags.

The feds had been tipped off after Maksym Yastremskiy, Albert's Ukrainian cardhawker, was arrested outside a Turkish nightclub in July 2007. When agents got a look at Yastremskiy's laptops, they found millions of stolen card numbers, a program used to hack into corporate retailers – and logs of encrypted chats with Albert. Once they cracked the code, investigators were able to tie Yastremskiy and Albert, along with an Estonian hacker nicknamed "Jonny Hell," to the siphoning of 5,000 card numbers from a Dave & Buster's, a security breach that cost the restaurant chain $600,000 to repair. Ironically, it was this relatively small hack – not the cybercrime of the century – that Albert originally found himself busted for a year later. But once the feds opened up his computers and began connecting the dots, they were astounded by the scope of the operation their trusted informant was running. The government indicted 11 members of Green Hat Enterprises from five countries, accusing Albert of reaping $1.6 million from his worldwide enterprise. Prosecutors estimated that the scheme cost its corporate victims, banks and insurers $200 million, but they maintain that the economic damage is likely far greater. "The magnitude of the loss is enormous," says Stephen Heymann, a U.S. attorney who prosecuted the case. "Because of the impact on so many thousands of businesses and banks and millions of people, it's impossible to quantify the full vastness of the crime."

The morning of Albert's arrest, Patrick Toey woke up at the Miami condo with half a dozen agents pointing tactical weapons at him. He started cooperating even before speaking with a lawyer. "I don't feel good about it," he says, sitting in his mother's house in Virginia Beach days after his sentencing in April. "It's not something I really wanted to do. Albert was one of my best friends. From my perspective, he still is. But taking the rest of my life into consideration, it was kinda something I had to do." For his cooperation, which the government cited as crucial in bringing down Albert's operation, Patrick received a prison sentence of five years, after facing a maximum of 22. Under the terms of his pre-prison release, he is forbidden from using a computer for any reason – not even to e-mail his fiancee, whom he had met online. "I don't know if Albert understands," he says quietly. "Even though if it was me, I definitely wouldn't forgive me for what I did."

Stephen Watt pleaded guilty to writing the sniffer code that proved key to Albert's operation but continues to insist that he never knew it was being used for illegal purposes, noting that he made no money from Albert's crimes. (The uncompensated nature of his devotion stunned investigators; questioning his motives, they asked Patrick whether Stephen and Albert were lovers.) The prosecution argued that Stephen must have known what Albert was up to: After all, the two spoke or IM'd daily, sharing "all their exploits: sexual, narcotic and hacking," and openly discussed Albert's sale of stolen card data. The judge agreed, sentencing Stephen to two years in prison and ordering him to pay a share of the $172 million restitution.

A few weeks after the judge's ruling, stomping around the Manhattan apartment he owns with his new wife, a real estate agent, Stephen bristles at the suggestion that he is anything other than a black-hat hacker. His motives, he insists, are ideological, not financial. "I'm a computer criminal, not a thief," he says. "That's my statement, and I'm sticking to it." For the next five hours, he offers a complete tour of the alarmingly neat apartment – books arranged by subject, clothes lined up by color – pausing only to snort ketamine off the top of his bookshelf, where he keeps a minipharmacy of pills, powders and vials. He shows off credit-card offers he's been getting on Albert's behalf – "Albert Gonzalez, you have been pre-approved!" – ever since Stephen added him as a secondary cardholder on his AmEx.

> "Albert was one of my best friends," Patrick says quietly. "But I definitely wouldn't forgive me for what I did."

"I walked a dangerous line," Stephen says, coming precariously close to a confession. "I did things I shouldn't have, and honestly, I had no problem participating in or enjoying the spoils of Albert's game. Am I morally responsible? Do I bear some guilt in this? Yes. Do I have any apologies to make?" He gives a derisive snort. "Uh, the answer is definitely *no*."

Albert, ever the realist, pleaded guilty and cooperated fully with the feds as soon as he realized that Patrick had turned state's witness. In return, after facing a maximum of life in prison, he was sentenced to 20 years – the longest punishment for a computer crime in U.S. history. "I never gave a thought to the millions of people whose lives I impacted," a penitent Albert told the judge at his sentencing, his dream of being a green hat replaced by olive-green prison garb. "I'm humbled by the 22 months I've spent in prison," he continued, as his parents wept in the front row. "I have no one to blame but myself."

It was a moving display of remorse. But one has to wonder if Albert was being more forthright in a letter he wrote me from prison, politely declining to share his story. "I'm fearful of what the DOJ's reaction may be if I was to go on record with the events of the past 10+ years," he wrote in his neat, spiky printing. "The motherfuckers have already proven to be untrustworthy and vindictive." Always the loyal friend, he added a concerned postscript: "Is Stephen OK? I haven't heard from him in two weeks."

To prepare Stephen for jail, Albert sent his friend a six-page typewritten letter explaining in detail how prison works: how the different races interact, how to properly climb onto a top bunk without offending your cellmate, even how to fart without stinking up the cell. He called it, with simple pragmatism, "A Guide to Being Successful in Jail." "Think Switzerland," Albert wrote. "When you're like Switzerland you have no loyalty to anyone or any group. Your loyalty should be to yourself, and your motto should be Google's: Don't do evil." The key, he added, is to show other prisoners that "we're str8 shooters who are highly intelligent. For some reason, people respect you if your IQ is over 130. You'll know you've reached this point when someone turns to you and says, 'Yo Stephen, when was JFK assassinated?'"

Even behind bars, Albert was still studying the angles, calculating the odds, figuring out how to hack the system to his advantage. "I hate the first couple of weeks when you arrive at a new facility, because it reminds me of the first couple weeks of school," Albert continued in his letter to Stephen. "You don't know anyone, and if you're anything like I was in school, antisocial, it's not enjoyable. The good thing is, we're one of the coolest motherfuckers on the planet, so we don't have a hard time meeting people once we're confident of our surroundings."

Then Albert's new surroundings forced him to cut his letter short. "I'm being rushed to finish because it's last call to get into the showers," he told Stephen. "Keep your head up and don't fear this. It's really not that hard. Remember, Switzerland."

Rolling Stone (ISSN 0035-791x) is published biweekly except for the first issue in July and at year's end, when two issues are combined and published as double issues, by Wenner Media LLC, 1290 Avenue of the Americas, New York, NY 10104-0298. Canadian Goods and Service Tax Registration No. R125041855. International Publications Mail Sales Product Agreement No. 450553. The subscription price is $39.96 for one year. The Canadian subscription price is $52.00 for one year, including GST, payable in advance. Canadian Postmaster: Send address changes and returns to P.O. Box 63, Malton CFC, Mississauga, Ontario L4T 3B5. The foreign subscription price is $80.00 for one year, payable in advance. Periodicals postage paid at New York, NY, and additional mailing offices. Canada Poste publication agreement #40683192. Postmaster: Send address changes to Rolling Stone Customer Service, P.O. Box 8243, Red Oak, IA 51591-1243.