November 10, 2010

The Great Cyberheist

By JAMES VERINI

One night in July 2003, a little before midnight, a plainclothes N.Y.P.D. detective, investigating a series of car thefts in upper Manhattan, followed a suspicious-looking young man with long, stringy hair and a nose ring into the A.T.M. lobby of a bank. Pretending to use one of the machines, the detective watched as the man pulled a debit card from his pocket and withdrew hundreds of dollars in cash. Then he pulled out another card and did the same thing. Then another, and another. The guy wasn't stealing cars, but the detective figured he was stealing something.

Indeed, the young man was in the act of "cashing out," as he would later admit. He had programmed a stack of blank debit cards with stolen card numbers and was withdrawing as much cash as he could from each account. He was doing this just before 12 a.m., because that's when daily withdrawal limits end, and a "casher" can double his take with another withdrawal a few minutes later. To throw off anyone who might later look at surveillance footage, the young man was wearing a woman's wig and a costume-jewelry nose ring. The detective asked his name, and though the man went by many aliases on the Internet — sometimes he was cumbajohny, sometimes segvec, but his favorite was soupnazi — he politely told the truth. "Albert Gonzalez," he said.

After Gonzalez was arrested, word quickly made its way to the New Jersey U.S. attorney's office in Newark, which, along with agents from the Secret Service's Electronic Crimes Task Force, had been investigating credit- and debit-card fraud involving cashers in the area, without much luck. Gonzalez was debriefed and soon found to be a rare catch. Not only did he have data on millions of card accounts stored on the computer back in his New Jersey apartment, but he also had a knack for patiently explaining his expertise in online card fraud. As one former Secret Service agent told me, Gonzalez was extremely intelligent. "He knew computers. He knew

fraud. He was good."

Gonzalez, law-enforcement officials would discover, was more than just a casher. He was a moderator and rising star on Shadowcrew.com, an archetypal criminal cyberbazaar that sprang up during the Internet-commerce boom in the early 2000s. Its users trafficked in databases of stolen card accounts and devices like magnetic strip-encoders and card-embossers; they posted tips on vulnerable banks and stores and effective e-mail scams. Created by a part-time student in Arizona and a former mortgage broker in New Jersey, Shadowcrew had hundreds of members across the United States, Europe and Asia. It was, as one federal prosecutor put it to me, "an eBay, Monster.com and MySpace for cybercrime."

After a couple of interviews, Gonzalez agreed to help the government so he could avoid prosecution. "I was 22 years old and scared," he'd tell me later. "When you have a Secret Service agent in your apartment telling you you'll go away for 20 years, you'll do anything."

He was also good-natured and helpful. "He was very respectable, very nice, very calm, very well spoken," says the Secret Service agent who would come to know Gonzalez best, Agent Michael (a nickname derived from his real name). "In the beginning, he was quiet and reserved, but then he started opening up. He started to trust us."

The agents won his trust in part by paying for his living expenses while they brought him to their side and by waiting for Gonzalez to work through his withdrawal. An intermittent drug addict, Gonzalez had been taking cocaine and modafinil, an antinarcoleptic, to keep awake during his long hours at the computer. To decompress, he liked Ecstasy and ketamine. At first, a different agent told me, "he was extremely thin; he smoked a lot, his clothes were disheveled. Over time, he gained weight, started cutting his hair shorter and shaving every day. It was having a good effect on his health." The agent went on to say: "He could be very disarming, if you let your guard down. I was well aware that I was dealing with a master of social engineering and deception. But I never got the impression he was trying to deceive us."

Gonzalez's gift for deception, however, is precisely what made him one of the most valuable cybercrime informants the government has ever had. After his help enabled officials to indict more than a dozen members of Shadowcrew, Gonzalez's minders at the Secret Service urged him to move back to his hometown, Miami, for his own safety. (It was not hard for Shadowcrew users to figure out that the one significant figure among their ranks who hadn't been arrested was probably the unnamed informant in court documents.) After aiding another investigation,

he became a paid informant in the Secret Service field office in Miami in early 2006. Agent Michael was transferred to Miami, and he worked with Gonzalez on a series of investigations on which Gonzalez did such a good job that the agency asked him to speak at seminars and conferences. “I shook the hand of the head of the Secret Service,” Gonzalez told me. “I gave a presentation to him.” As far as the agency knew, that’s all he was doing. “It seemed he was trying to do the right thing,” Agent Michael said.

He wasn’t. Over the course of several years, during much of which he worked for the government, Gonzalez and his crew of hackers and other affiliates gained access to roughly 180 million payment-card accounts from the customer databases of some of the most well known corporations in America: OfficeMax, BJ’s Wholesale Club, Dave & Buster’s restaurants, the T. J. Maxx and Marshalls clothing chains. They hacked into Target, Barnes & Noble, JCPenney, Sports Authority, Boston Market and 7-Eleven’s bank-machine network. In the words of the chief prosecutor in Gonzalez’s case, “The sheer extent of the human victimization caused by Gonzalez and his organization is unparalleled.”

At his sentencing hearing in March, where he received two concurrent 20-year terms, the longest sentence ever handed down to an American for computer crimes, the judge said, “What I found most devastating was the fact that you two-timed the government agency that you were cooperating with, and you were essentially like a double agent.”

IN APRIL, I visited Gonzalez at the Wyatt Detention Center in Central Falls, R.I., situated by a river and a pleasant place as jails go. Once muscular and tan, Gonzalez, who turned 27 and 28 behind bars, was pallid and thin. His khaki uniform hung on him baggily, and his eyes were bloodshot behind wire-rim glasses. Occasionally a mischievous smile played on his face; otherwise, he looked through the wire-glass partition with a sympathetic but inscrutably intense stare.

He didn’t want to talk about his crimes at first, so in a soft voice he told me about his ex-girlfriend, who had stopped visiting him (“I can’t blame her”), about what he’d been reading (“Stalingrad,” by Antony Beevor; “Into Thin Air,” by Jon Krakauer; essays by Ralph Waldo Emerson), about his thoughts on recent high-profile computer breaches in the news. The public’s ignorance about his chosen criminal field baffled him. He had become a fan of National Public Radio at Wyatt, and had recently listened to a discussion of hackers on “Fresh Air.” (“Terry Gross is a great host,” he wrote me earlier in a letter, but “these authors and co-

authors can't possibly be making decent earnings. Are they?") He talked about his childhood and family. His father, Alberto Sr., is a landscaper who as a young man left Cuba on a raft and was picked up by a Coast Guard cutter in the Florida straits. He and Albert share a birthday with Gonzalez's 5-year-old nephew, "whom I love more than anyone in this world," Gonzalez said. His nephew's mother, Maria, Gonzalez's sister and only sibling, "always learned by listening to our parents' advice." He didn't.

Gonzalez bought his first PC, with his own money, when he was 12. He took an interest in computer security after it was infected with a downloaded virus. "We had to call the technician who sold it to us, and he came over," he said in one letter. "I had all these questions for him: 'How do I defend myself from this? Why would someone do this?' " He got over his indignation easily enough, and by the time he was 14 had hacked into NASA, which resulted in a visit by F.B.I. agents to his South Miami high school. Undeterred, Gonzalez formed a cooperative of "black hats" — curiosity-driven hackers with an antiauthoritarian bent — and acquired a reputation. He gave an interview to the online magazine ZDNet under his new screen name, soupnazi: "Defacing a site to me is showing the admins [and] government . . . that go to the site that we own them," he said. On the side he was also purchasing clothing and CDs online with stolen credit-card numbers. He ordered the merchandise delivered to empty houses in Miami, and then had a friend drive him to pick it up during lunch period.

By the time he dropped out of Miami Dade College during his freshman year, Gonzalez had taught himself, by reading software manuals, how to hack into Internet service providers for free broadband. He discovered he could go further than that and co-opted the log-ins and passwords of managers and executives. "On their computers would always be a huge stash of good information, network diagrams, write ups," he said, audibly enthralled at the memory. "I would learn about the system architecture. It was as if I was an employee."

Gonzalez's closest friend, Stephen Watt, who is now serving a two-year prison sentence for coding a software program that helped Gonzalez steal card data, describes Gonzalez as having "a Sherlock Holmes quality to him that is bounded only by his formal education." Like the other hackers who would go on to form the inner circle of Gonzalez's criminal organization, Watt met Gonzalez when both were teenagers, on EFnet, an Internet relay chat network frequented by black hats. Watt and Gonzalez interacted strictly online for a year, though each lived in South Florida. Once they began spending time together, in Florida and New York, Watt, who is 27, noticed that Gonzalez's talents as an online criminal carried over into his life away from the

computer. “He could spot wedding rings at 50 yards. He could spot a Patek Philippe at 50 yards. He would have been a world-class interrogator. He was very good at figuring out when people were lying.”

Like many hackers, Gonzalez moved easily between the licit and illicit sides of computer security. Before his first arrest, in the A.T.M. lobby, Gonzalez made his way from Miami to the Northeast after he hacked into a New Jersey-based Internet company and then persuaded it to hire him to its security team. The transition from fraudster to informant was not too different.

After he agreed in 2003 to become an informant, Gonzalez helped the Justice Department and the Secret Service build, over the course of a year, an ingenious trap for Shadowcrew. Called Operation Firewall, it was run out of a makeshift office in an Army repair garage in Jersey City. Gonzalez was its linchpin. Through him, the government came to, in hacker lingo, own Shadowcrew, as undercover buyers infiltrated the network and traced its users around the world; eventually, officials even managed to transfer the site onto a server controlled by the Secret Service. Meanwhile, Gonzalez patiently worked his way up the Shadowcrew ranks. He persuaded its users to communicate through a virtual private network, or VPN, a secure channel that sends encrypted messages between computers, that he introduced onto the site. This VPN, designed by the Secret Service, came with a special feature: a court-ordered wiretap.

Gonzalez worked alongside the agents, sometimes all day and into the night, for months on end. Most called him Albert. A couple of them who especially liked him called him Soup, after his old screen-name soupnazi. “Spending this much time with an informant this deeply into a cybercrime conspiracy — it was a totally new experience for all of us,” one Justice Department prosecutor says. “It was kind of a bonding experience. He and the agents developed over time a very close bond. They worked well together.”

On Oct. 26, 2004, Gonzalez was taken to Washington and installed in the Operation Firewall command center at Secret Service headquarters. He corralled the Shadowcrew targets into a chat session. At 9 p.m., agents began knocking down doors. By midnight, 28 people across eight states and six countries had been arrested, most of them mere feet from their computers. Nineteen were eventually indicted. It was by some estimates the most successful cybercrime case the government had ever carried out.

“I did find the investigation exciting,” Gonzalez told me of turning against Shadowcrew. “The intellectual element. Unmasking them, figuring out their identities. Looking back, it was kind of

easy, though. When someone trusts you, they let their guard down."

He did say, however, that he "actually had a bad conscience" about it. "I had a moral dilemma, unlike most informants." On another occasion, when he was discussing the same subject, Gonzalez wrote to me in a letter, "This distinction is very important . . . my loyalty has always been to the black-hat community."

Those captured by the government with his help are less interested in this distinction. "Shadowcrew was not a forum of thugs," a member who occasionally laundered money for Gonzalez told me. This casher served two years in prison thanks to Operation Firewall. "He was a coward who betrayed us all, and I suppose if you believe in karma, he got what he deserved in the end."

Before being arrested, Gonzalez had actually vouched for this casher to the higher-ups at Shadowcrew. He had gone out of his way to help many members, according to the federal prosecutor in New Jersey, Scott Christie, who worked with him on Operation Firewall. Christie says that based on their exchanges when Gonzalez was being recruited as an informant, Gonzalez seemed to be "less interested in money than in building up Shadowcrew." He "gave back to the members in the way of education and personal benefit. Unlike other cybercriminals, he wasn't just out for gain."

Indeed, no one I spoke with compared him to a gangster or a mercenary — preferred honorifics among hackers — but several likened him to a brilliant executive. "In the U.S., we have two kinds of powerful, successful business leaders. We have people like Bill Gates and Steve Jobs, who are the most sophisticated of electronic technicians and programmers," says Steve Heymann, the Massachusetts assistant U.S. attorney who, in the spring of 2010, secured a combined 38 years of prison time for Gonzalez and his co-conspirators for their corporate breaches. "Then we have others, like the C.E.O.'s of AT&T or General Electric, who are extremely good in their area but also know when to go to others for expertise and how to build powerful organizations by using those others. Gonzalez fits into that second category."

BY THE TIME Gonzalez returned to Miami after Operation Firewall, in late 2004, he was already exploring the vulnerability of corporate wireless networks. Just as data security had been an afterthought for many businesses in their rush to get online in the 1990s, creating opportunities for the likes of Shadowcrew, many firms had taken no precautions as they eagerly adopted WiFi in the early 2000s. Gonzalez was especially intrigued by the possibilities of a

technique known as “war driving”: hackers would sit in cars or vans in the parking lots of big-box stores with laptops and high-power radio antennae and burrow through companies’ vulnerable WiFi networks. Adepts could get into a billion-dollar multinational’s servers in minutes.

Gonzalez reconnected with an old friend from EFnet, Christopher Scott, who was willing to do grunt work. Scott began cruising the commercial stretches of Route 1 in Miami, looking for war-driving targets. His experiments at BJ’s Wholesale Club and DSW met with success. He stole about 400,000 card accounts from the former, a million from the latter. He described the breaches and passed card numbers to Gonzalez.

The following summer, Scott parked outside a pair of Marshalls stores. He enlisted the help of Jonathan James, a minor celebrity among Miami black hats for being the first American juvenile ever incarcerated for computer crimes. (At 15, he hacked into the Department of Defense; he lived under house arrest for six months.) Scott cracked the Marshalls WiFi network, and he and James started navigating the system: they co-opted log-ins and passwords and got Gonzalez into the network; they made their way into the corporate servers at the Framingham, Mass., headquarters of Marshalls’ parent company, TJX; they located the servers that housed old card transactions from stores. Scott set up a VPN — the system Gonzalez and the Secret Service used to ensnare Shadowcrew — so they could move in and out of TJX and install software without detection. When Gonzalez found that so many of the card numbers they were getting were expired, he had Stephen Watt develop a “sniffer” program to seek out, capture and store recent transactions. Once the collection of data reached a certain size, the program was designed to automatically close, then encrypt, compress and forward the card data to Gonzalez’s computer, just as you might send someone an e-mail with a zip file attached. Steadily, patiently, they siphoned the material from the TJX servers. “The experienced ones take their time and slowly bleed the data out,” a Secret Service analyst says.

By the end of 2006, Gonzalez, Scott and James had information linked to more than 40 million cards. It wasn’t a novel caper, but they executed it better than anyone else had. Using similar methods, they hacked into OfficeMax, Barnes & Noble, Target, Sports Authority and Boston Market, and probably many other companies that never detected a breach or notified the authorities. Scott bought a six-foot-tall radio antenna, and he and James rented hotel rooms near stores for the tougher jobs. In many cases, the data were simply there for the taking, unencrypted, unprotected.

“For a long time, probably too long a time, computer security was something that was just dollars and cents off the bottom line — it doesn’t bring in money,” Heymann told me when I asked why war-driving hackers were able to steal data so easily. “At the same time, in these cases, companies were beginning to warehouse vast amounts of information” far more swiftly than they were coming to understand the vulnerabilities of their systems. A result was what he called “a primeval muck that creates a period when dramatic, costly attacks can get at vast amounts of resources.”

At the same time that Gonzalez was stealing all this bank-card data, he was assembling an international syndicate. His favored fence was a Ukrainian, Maksym Yastremskiy, who would sell sets of card numbers to buyers across the Americas, Europe and Asia and split the proceeds with him. Gonzalez hired another EFnet friend, Jonathan Williams, to cash out at A.T.M.’s across the country, and a friend of Watt’s in New York would pick up the shipments of cash in bulk sent by Williams and Yastremskiy. Watt’s friend would then wire the money to Miami or send it to a post-office box there set up by James through a proxy. Gonzalez established dummy companies in Europe, and to collect payment and launder money he opened e-gold and WebMoney accounts, which were not strictly regulated (e-gold has since gone out of business). He also rented servers in Latvia, Ukraine, the Netherlands and elsewhere to store the card data and the software he was using for the breaches. Finally, he joined up with two Eastern European hackers who were onto something visionary. Known to him only by their screen names, Annex and Grig, they were colluding to break into American card-payment processors — the very cash arteries of the retail economy.

“I’ve been asking myself, why did I do it?” Gonzalez told me over the phone from prison recently. “At first I did it for monetary reasons. The service’s salary wasn’t enough, and I needed the money. By then I’d already created the snowball and had to keep doing it. I wanted to quit but couldn’t.” He claims his intentions were partly admirable. He genuinely wanted to help out Patrick Toey, a close friend and hacker who would later do much of the more sophisticated legwork involved in Gonzalez’s hacking into corporate networks. Unlike Gonzalez and Watt, Toey, who is 25, had a rough upbringing. After dropping out of high school, he supported his mother and his younger brother and sister by hacking. Gonzalez invited Toey to live in his condominium in Miami, rent-free. Gonzalez owned it, but he enjoyed living at home with his parents more. He says he loved his mother’s cooking and playing with his nephew, and he could more easily launder money through his parents’ home-equity line of credit that way.

Gonzalez relished the intellectual challenges of cybercrime too. He is not a gifted programmer — according to Watt and Toey, in fact, he can barely write simple code — but by all accounts he can understand systems and fillet them with singular grace. I often got the impression that this was computer crime's main appeal for Gonzalez.

But he also liked stealing. "Whatever morality I should have been feeling was trumped by the thrill," he told me. And he liked spending. Partly but not entirely in jest, he took to referring to his scheme as Operation Get Rich or Die Tryin', after the 50 Cent album and movie. Gonzalez would not discuss with me just how rich he got, but he certainly was seeing profits in the millions of dollars. Little of that found its way to Toey, however, and probably none to Watt. For himself, Gonzalez bought, in addition to the condo, a new BMW 330i. He often stayed in luxury hotel suites in Miami on a whim. He took frequent trips to New York, where he and Watt — who worked by day in the I.T. department of Morgan Stanley and later developed securities-trading software and moonlighted as a nightclub promoter — spent thousands on hotels, restaurants, clubs and drugs. Lots of drugs. "I don't know when he slept," Agent Michael says, referring to Gonzalez's lifestyle during the time they worked together.

It seems clear now that Gonzalez didn't mind betraying people. What would come to anger the Secret Service most is that he used information from their investigations to enrich himself. "He would be working for the service during the day, and then come home and talk to me, and I'd be selling dumps for him," Toey told me, referring to databases of stolen card information. Gonzalez sold dumps to hackers who he knew were under investigation, in effect setting them up. In the case of one Miami suspect being investigated by the service, Toey told me: "We basically ripped [him] off and sold him databases that were all dead and expired. They came from a company where a breach was being investigated by the service. He got caught with the database, and it looked like he'd done it." Toey and Gonzalez then split the profits. (Gonzalez confirmed this account of events.)

When I asked Toey how he felt about using information from government investigations to betray other hackers, including black hats, he said: "I didn't like it at all that he did it. But at the same time, I don't know any of those people." He added, "More money for us."

Agent Michael investigated the Miami suspect, but he did not know until I told him that Gonzalez had set the man up. "It doesn't surprise me," he said. "Looking back, we knew what he wanted us to know. . . . He was leading a double life within a double life."

BY THE SPRING of 2007, Gonzalez was tired of working for the Secret Service. “He wasn’t showing up on time,” according to Agent Michael, who began talking with other agents about cutting Gonzalez loose. “He didn’t want to be there.” He was also tired of war driving. He wanted a new challenge. He found one in a promising technique called SQL injection.

SQL (usually pronounced “sequel”) stands for Structured Query Language, the programming language that enables most commercial Web sites to interact with their associated databases. When you log on to the Web site of a clothing store to buy a sweater, for example, the site sends your commands in SQL back to the databases where the images and descriptions of clothing are stored. The requested information is returned in SQL, and then translated into words, so you can find the sweater you want. But there is a vulnerability here: such databases in a company’s servers often exist in proximity to other all-too-accessible databases with more sensitive information — like your credit-card number.

SQL is the lingua franca of online commerce. A hacker who learns to manipulate it can penetrate a company with frightening dependability. And he doesn’t need to be anywhere near a store or a company’s headquarters to do so. Since SQL injections go through a Web site, they can be done from anywhere.

Gonzalez urged Watt and Toey to experiment with SQL. Watt wasn’t interested. “I had objections to what he was doing on a moral level — and on top of that, I took an intellectual exception,” Watt says. “If Albert said we were going to go after the Church of Scientology or Blackwater, I would have dove in headfirst.” Toey, however, said he felt he owed Gonzalez. He began poking around on the sites of businesses that seemed vulnerable — or for which he had a philosophical distaste. “I just didn’t like what they did,” he said of the clothing chain Forever 21. The clothes were poorly made, he said, and the employees poorly paid. “It’s just everything I hate about this country in one store.”

Under the assault of Toey’s expertise and contempt, Forever 21 didn’t stand a chance. “I went to their Web site, and I looked at their shopping-cart software, and within five minutes, I found a problem,” he said, with his customary concision. “Within 10 minutes we were on their computers and were able to execute commands freely. From there we leveraged access until we were the domain administrators. Then I passed it over to Albert.”

What came next was the truly inspired step. Gonzalez focused on TJX in part because it stored old transactions, but he found that many of the cards were expired. He needed a way to get to

cards right after customers used them. It was possible, he learned, to breach the point-of-sale terminals at stores, the machines on checkout counters through which you swipe your card at the supermarket, the gas station, the department store — just about anywhere you buy something.

Gonzalez and Toey took reconnaissance trips to stores around Miami to look at the brands and makes of their terminals. He downloaded schematics and software manuals. Earlier, Jonathan Williams visited an OfficeMax near Los Angeles, loosened a terminal at a checkout counter and walked out of the store with it. Hackers working with an Estonian contact of Gonzalez's hacked into the Maryland-based Micros Systems, the largest maker of point-of-sale systems, and stole software and a list of employee log-ins and passwords, which they sent to Gonzalez.

Now once Toey got him into a system, Gonzalez no longer had to sift through databases for the valuable stuff. Instead, he could go straight to the servers that processed the cards coming from the terminals, in the milliseconds before that information was sent to banks for approval. He tried this on JCPenney, the clothing chain Wet Seal and the Hannaford Brothers grocery chain, in the last instance compromising more than four million cards. His Estonian contact used the technique on Dave & Buster's. "Every time a card was swiped, it would be logged into our file," Toey says. "There was nothing anyone could do about it."

When they pieced together how Gonzalez organized these heists later, federal prosecutors had to admire his ingenuity. "It's like driving to the building next to the bank to tunnel into the bank," Seth Kosto, an assistant U.S. attorney in New Jersey who worked on the case, told me. When I asked how Gonzalez rated among criminal hackers, he replied: "As a leader? Unparalleled. Unparalleled in his ability to coordinate contacts and continents and expertise. Unparalleled in that he didn't just get a hack done — he got a hack done, he got the exfiltration of the data done, he got the laundering of the funds done. He was a five-tool player."

Gonzalez and Toey were returning from a trip to Toys "R" Us to check out its terminals one afternoon in the spring of 2008 when a sports car with tinted windows pulled up behind them at a red light. Gonzalez became suspicious and turned into a bus lane. The sports car followed. When the light turned green, Gonzalez didn't move. The car didn't move. After waiting for minutes, in a static game of chicken, car horns blaring, Gonzalez suddenly accelerated into oncoming traffic before doing a U-turn and turning into an alley. The pursuing car flew by, Gonzalez pulled out behind him, sped up alongside the car and peered inside. Gonzalez and

Toey made out a police light on the dashboard. It was a surveillance car.

Gonzalez had by that point stopped working as an informant, according to the service. Instructions had come down to the Miami field office to start tailing him. Maybe the most valuable cybercrime informant it had ever employed, the key to Operation Firewall, was now being investigated. And the Secret Service wasn't alone: the F.B.I. was looking into a wireless intrusion at Target's headquarters that originated at one of its Miami stores. The store, the bureau discovered, was in the line of sight of Gonzalez's condo, in ideal range for a war-driving antenna.

But Gonzalez wasn't worried. He was certain he'd covered all his tracks.

KIM PERETTI KNOWS Gonzalez as well as almost anyone in the government. She has worked with him. She has also prosecuted him — though Peretti does not come across as a federal prosecutor. Younger in appearance than her 40 years, she grew up in Wisconsin and is girlish, even bubbly, in person, apt to express frustration with phrases like "Oh, sugar!" Peretti was hired to the Justice Department's Computer Crime and Intellectual Property Section shortly after 9/11. Peretti made a point of getting to know the agents in the Secret Service's Electronic Crimes Task Force because she knew that they were, like her, eager to make a name in going after cybercriminals. She lobbied to be assigned to Operation Firewall, and in 2003 she was.

When I met Peretti at a restaurant near her new office in McLean, Va. — she left the government in May to take a job at PriceWaterhouseCoopers — she was wearing a blue skirt suit and designer glasses. "She's got the whole Sarah Palin eyewear thing going on," Gonzalez had written to me in a letter, by way of explaining that it wasn't at all unpleasant being investigated by her. But their relationship goes back further than that. Much of what Peretti knows about cybercrime she learned from working with Gonzalez.

"Albert was an educator," she said, describing their experience on Operation Firewall. "We in law enforcement had never encountered anything like" him. "We had to learn the language, we had to learn the characters, their goals, their techniques. Albert taught us all of that." They worked as well together as any investigative team she has been a part of, she said.

When we met, Peretti brought with her a poster-size screen shot of Shadowcrew's homepage as it appeared the day after the raids. Secret Service technicians had defaced it with a photograph

of a shirtless, tattooed tough slouching in a jail cell. The text said, “Contact your local United States Secret Service field office . . . before we contact you!”

By the time she was 35, thanks to Operation Firewall and Gonzalez, Peretti was the Justice Department’s chief prosecutor of cybercrime in Washington. But in 2005, even as she was litigating the Shadowcrew case, she encountered a new cybercrime wave unlike anything that had come before. “The service keeps calling me, saying, ‘We’ve got another company that contacted us,’ ” she said. “The volume was getting bigger and bigger. There was just an explosion.”

In the days before Christmas 2006, the Justice Department and Stephen Heymann, the assistant U.S. attorney in Massachusetts, received a series of frantic calls from TJX’s attorneys. The company had been contacted by a credit-card company, because a rapidly growing number of cards used at Marshalls and T. J. Maxx stores seemed to have been stolen. TJX had examined its Framingham, Mass., servers, and what it found was catastrophic. According to its own account, for about a year and a half, cards for “somewhere between approximately half to substantially all of the transactions at U.S., Puerto Rican and Canadian stores” were believed stolen. It was the biggest theft of card data in U.S. history, and there wasn’t a lead in sight.

“At that point we had quite literally the entire world as possible suspects,” Heymann told me in May, when we met in his office in the federal court building overlooking Boston Harbor. With his father, Philip, a deputy attorney general in the Clinton administration, Heymann teaches courses on criminal law at Harvard Law School. He had been deputy chief of the Massachusetts U.S. attorney’s criminal division and then set up one of the first computer-crime units in the country, so he was well versed in the comparative challenges. “If you’ve got a murder scene, there’s blood, there’s fingerprints. If you have a hacker going into a company, the critical information can be lost the moment the connection is broken. The size of the networks might be so large and so confusing that they’re very hard to understand and search. The people involved may only be known by screen names. Figuring that out is very different from figuring out who Tony the Squirrel is,” he said. Heymann had never seen anything like the TJX breach.

Then, in 2007, attorneys for Dave & Buster’s called the Secret Service. That company, too, had been breached, but this was different. The thieves had managed to access its point-of-sale system. By that summer, Peretti and Heymann had huge amounts of data, lots of potential leads and no clue as to whom they were chasing. “For the first six to nine months, it was tiring,

exhaustive, thorough," Heymann told me. "I'd like to tell you it was also brilliant and incisive and led to the key lead, but it wasn't." They were in desperate need of a break.

They finally got one, courtesy of Peretti's old friends at the Secret Service. For two years, it turned out, an undercover agent in its San Diego office had been buying card dumps from Maksym Yastremskiy, Gonzalez's fence. The agent traveled to Thailand and Dubai to meet with the Ukrainian, and in Dubai he furtively copied the hard drive in Yastremskiy's laptop. Technicians at the Secret Service combed through it and discovered, to their joy, that Yastremskiy was a meticulous record keeper. He had saved and catalogued all of his customer lists and instant messages for years. In the logs, they found a chat partner who appeared to be Yastremskiy's biggest provider of stolen card data. But all they had for the person was an I.M. registration number — no personal information.

In July 2007, Yastremskiy was arrested in a nightclub in Turkey, and the Secret Service turned up a useful lead. The anonymous provider had asked Yastremskiy to arrange a fake passport. One of the provider's cashers had been arrested, and he wanted to get his man out of the United States. The only problem: he didn't say where the casher had been arrested.

So agents phoned every police station and district attorney's office around the country that had made a similar arrest or brought a similar case. After weeks of these calls, their search led them to a prison cell in North Carolina, where Jonathan Williams was being held. He had been arrested with $200,000 in cash — much of which had been intended for Gonzalez — and 80 blank debit cards; the local authorities hadn't linked him to a larger criminal group, and they couldn't have known about Gonzalez. The Secret Service agents plugged in a thumb drive in Williams's possession at the time of his arrest and found a file that contained a photograph of Gonzalez, a credit report on him and the address of Gonzalez's sister, Maria, in Miami. (He was also arrested with a Glock 9-millimeter pistol and two barrels for the gun, one threaded to fit a silencer.) The file was "a safety precaution, in case [Gonzalez] tried to inform on me," Williams told me from prison in June. Officials then traced packages Williams had sent to the post-office box in Miami. This led the Secret Service to Jonathan James. They pulled James's police records and found that in 2005 he was arrested by a Palmetto Bay, Fla., police officer who found him in the parking lot of a retail store in the middle of the night. The officer didn't know why James and his companion, a man named Christopher Scott, were sitting in a car with laptops and a giant radio antenna, but she suspected they weren't playing World of Warcraft.

The real eureka moment came when Secret Service technicians finally got the I.M. registration information for whoever was providing Yastremskiy with bank-card data. There was no address or name, but there was an e-mail address: soupnazi@efnet.ru. It was a dead giveaway to anyone who knew Gonzalez. Peretti remembers vividly the afternoon in December 2007 when agents called her and told her to come to their office. They sat her down and showed her the e-mail address. “And they looked at me,” Peretti said. “They’ve got 10 agents looking at me. Three minutes passed by, I was sitting there like a dull person. And then I was like, ‘Oh, my God!’ ”

Gonzalez knew the Secret Service was investigating Yastremskiy, but he continued to move databases through him. When I asked Gonzalez why, he said, “I never thought he would leave Ukraine.” The country has no extradition policy with the U.S. But Yastremskiy did leave. “It wasn’t until he got busted,” Gonzalez told me, that he realized his mistake.

Operation Get Rich or Die Tryin’ unraveled fast. Christopher Scott’s home and Gonzalez’s condo were raided simultaneously. Agents seized Scott, along with nine computers and 78 marijuana plants; in Gonzalez’s place they found various designer drugs and a half-asleep Patrick Toey. Toey was flown to Boston to testify before a grand jury. He directed Heymann and Peretti to the e-gold and WebMoney accounts and to servers located abroad. The servers eventually led them to Watt, who returned to his Greenwich Village apartment to find agents and a battering ram awaiting him. The Gonzalezes’ home was raided, but Albert was not there.

Peretti knew that if they didn’t find him soon, he would disappear. “Albert had said during Firewall how afraid he was of spending any time in prison,” she said. “I knew he’d be gone the next day.”

They found him at 7 in the morning on May 7, 2008, when agents rushed into his suite at the National Hotel in Miami Beach. With him were a Croatian woman, two laptops and $22,000. Over time, he started talking. Months later, he led Secret Service agents to a barrel containing $1.2 million buried in his parents’ backyard. Attorney General Michael Mukasey himself held a news conference in August 2008 to announce the indictment. “So far as we know, this is the single largest and most complex identity-theft case ever charged in this country,” he told reporters. Gonzalez’s attorney assured him the government’s case was weak. Electronic evidence often didn’t hold up, he said.

That was before attorneys for Heartland Payment Systems Inc., in Princeton, N.J., called Peretti in early January 2009. One of the largest card-payment processors in the country, Heartland,

which services about a quarter of a million businesses, had been hacked. But not just hacked — owned in a way no company had ever been owned. As Peretti would soon learn from Gonzalez, he had helped the two Eastern European hackers, Annex and Grig, slip into Heartland via SQL injection. By the time Heartland realized something was wrong, the heist was too immense to be believed: data from 130 million transactions had been exposed. Indictments were brought against Gonzalez in New Jersey, New York and Massachusetts (where the cases were eventually consolidated). At a loss for anything else to say, Gonzalez's attorney told a reporter: "He's really not a bad guy. He just got way in over his head."

On May 18, 2008, Jonathan James shot himself in the head. He left a suicide note saying he was convinced the government would try to pin Gonzalez's crimes on him because of the notoriety James had gained as a teenage hacker.

AT HIS SENTENCING in March, Gonzalez, who pleaded guilty to all charges, sat almost motionless. As far as I saw, he didn't once look back at the gallery in the federal courtroom in Boston, where his mother sat stoically while his father wept into a handkerchief as Gonzalez's sister consoled him. Nor did he glance at Heymann, as he told the court that Gonzalez had committed the worst computer crimes ever prosecuted; nor at Peretti, nor his old colleagues from the Secret Service, who also sat in the gallery. Gonzalez just leaned forward and peered straight ahead at the judge, as though — the set of his head was unmistakable — staring intensely at a computer.

He spoke just once, a few sentences at the end. "I blame nobody but myself," he said. "I'm guilty of not only exploiting computer networks but exploiting personal relationships, particularly one that I had with a certain government agency who believed in me. This agency not only believed in me but gave me a second start in life, and I completely threw that away." Accounting for time served and good behavior, Gonzalez is expected to get out of prison in 2025.

In May, Toey began a five-year sentence, and Scott started a seven-year sentence. Yastremskiy was given 30 years in a Turkish prison, a fate apparently so grim he's lobbying to be extradited to the U.S. so he can be imprisoned here. Watt, who maintains that he was never fully aware of what Gonzalez wanted to use his software for, and who refused to give information on Gonzalez to the grand jury or prosecutors, was sentenced to two years.

According to Attorney General Eric Holder, who last month presented an award to Peretti and the prosecutors and Secret Service agents who brought Gonzalez down, Gonzalez cost TJX,

Heartland and the other victimized companies more than $400 million in reimbursements and forensic and legal fees. At last count, at least 500 banks were affected by the Heartland breach. But the extent of the damage is unknown. “The majority of the stuff I hacked was never brought into public light,” Toey told me. One of the imprisoned hackers told me there “were major chains and big hacks that would dwarf TJX. I’m just waiting for them to indict us for the rest of them.” Online fraud is still rampant in the United States, but statistics show a major drop in 2009 from previous years, when Gonzalez was active.

The company line at the Justice Department and the Secret Service is that informants go bad all the time, and that there was nothing special about Gonzalez’s case. As Peretti put it, “You certainly feel anger” — but “you’re not doing your job if you fall into the trap of thinking the criminal you’re working with is your best friend.” The agent in charge of the Criminal Investigative Division at the Secret Service told me: “It’s unfortunate. We try to take measures. But it does happen. You need to deal with criminals to get other criminals. Albert was a criminal.”

Heymann lauds how the Secret Service handled things. “When you find out one of your informants has committed a crime,” he said, “you can hide the fact, which unfortunately does happen from time to time. You can play it down — soft-pedal it, try to make it go away. Or you can do what I think the Secret Service very impressively did here, which is to go full bore.” He said that after Gonzalez became a suspect, “the size of the investigation, the amount of assets, all increased significantly. That reflects enormous integrity.”

But Gonzalez did have friends in the government, and there is no question some of them feel deeply betrayed. Agent Michael was the most candid with me about this: “I put a lot of time and effort into trying to keep him on the straight and narrow and show him what his worth could be outside of that world, keep him part of the team. And he knows that, and he knew what good he could have done with his talent.” He continued, “We work with a million informants, but for me it was really tough with him.”

After his sentencing, Gonzalez was transferred from Wyatt to the Metropolitan Detention Center in Brooklyn (before ultimately ending up in a prison in Michigan). Situated between a loud stretch of the Brooklyn-Queens Expressway and Gowanus Bay, M.D.C. is brutal, even for a prison. Populated by hardened offenders, it is among the last places a nonviolent government informant would want to be. “The place is terrible,” Agent Michael said. “But you know what?

When you burn both ends of the candle, that's what you get." Even Gonzalez was impressed by the government's indifference to his comfort. He says he always knew it would stick it to him somehow, "but I never thought it would be this badly."

"I've been asking myself a lot why didn't I ever feel this way while I was doing it," Gonzalez told me, when I spoke with him in June. An inmate at M.D.C. who didn't like informants had recently threatened to kill him, he said. It was his 29th birthday, and the 5th birthday of his nephew. Gonzalez's sister wanted to bring her son to New York to visit, but Gonzalez told her not to. "I didn't want him to get scared, seeing me in here," he told me. Instead, Gonzalez was spending the day reading a biography of Warren Buffett.

I asked him how he felt when he thought about people like Agent Michael and Peretti. "They're part of the betrayals," he said.

During the legal proceedings, the court ordered Gonzalez to undergo a psychological evaluation. "He identified with his computer," the report reads. "It is hard, if not impossible, even at the present for Mr. Gonzalez to conceptualize human growth, development and evolution, other than in the language of building a machine."

As we spoke, Gonzalez recalled how he first became obsessed with computers as a child. "I remember so many times having arguments with my mother when she'd try to take the computer power cord from me, or she'd find me up at 6 a.m. on the computer when I had to be at school at 7:30. Or when I'd be out with [my girlfriend] and not paying any attention to her because I'd be thinking about what I could do online."

He reflected on his days with Shadowcrew, and on his decision to help the government. "I should have just done my time in 2003," he said. "I should have manned up and did it. I would be getting out about now."

James Verini is a writer in New York. This is his first article for the magazine.