We Are Anonymous

Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency

Parmy Olson

LITTLE, BROWN AND COMPANY
New York Boston London

CHAPTER 26

The Real Sabu

What ended up happening to Hector "Sabu" Monsegur? After the arrests of Topiary and Tflow, he continued leading the revived Antisec movement, tweeting from the account he had labeled "The Real Sabu" to a growing stable of tens of thousands of followers. Sometimes he incited revolution—"I love the smell of cyberwar in the morning #fuckisrael"—and sometimes he funneled supporters into the Antisec chat channel, "irc.anonops.li payload is coming soon!" When his handlers needed him to pull in the reins, he complied, cautioning Anonymous on September 21, 2011, that attempts to DDoS Wall Street financial firms was "a fail...Not because of lack of manpower, but rather, wrong direction. Own them, don't waste resources DDoSing."

For someone who had been so loud about hating the police, it had not been all that hard to get Sabu to work for the FBI. On June 8, 2011, the day after he had gone missing from LulzSec and caused distress among his clique of hacker friends, Sabu went to court, where a judge decided to release him from police custody on bail. The condition was that he let the FBI supervise his every movement online and in real life.

For the next two months, as LulzSec finished its hacking spree and the group's founding members, Topiary and Tflow, were arrested, Sabu continued to quietly work with the Federal Bureau of Investigation. According to later reports, he proved to be a devoted informant. He continued to stay up until the early hours most nights, talking to other hackers and finding out about upcoming attacks. If rumors swirled that Anonymous or LulzSec were about to hit a government or company, he would try to talk to the hackers involved to corroborate the attack was about to happen. Perhaps for once Monsegur felt like he was getting the respect that he deserved—this time from the police.

On August 15, he stood before a judge at a second secret hearing in the Southern District Court of New York and pleaded guilty to twelve charges, mostly related to computer hacking. Sabu agreed to help the FBI, and federal prosecutors agreed not to try Sabu for several other crimes he had committed outside the world of hacking. These included carrying a handgun, selling one pound of marijuana in 2010 and four pounds of weed in 2003, buying stolen jewelry and electronics, and running up $15,000 in charges on the credit card of a former employer. And there were plenty of other misdemeanors Sabu had carried out online; detectives found out he had hacked into an online casino and, in 2010, had hacked into a car parts company and shipped himself four car engines worth $3,450. Given how enthusiastically Sabu had boasted about his decade "underground" in which he had "owned entire governments," there was possibly plenty more the police missed. But the Feds were more interested in the other prosecutions that Sabu could help them with.

"Since literally the day he was arrested, the defendant has been cooperating with the government proactively," U.S. district attorney James Pastore, the prosecuting lawyer, told the judge during the August hearing. "He has been staying up sometimes all night engaging in conversations with co-conspirators that are helping

the government to build cases against those co-conspirators." Pastore read out the charges and said they could lead to a total maximum sentence of a hundred and twenty-two and a half years in prison. If Monsegur followed his "cooperation agreement" with the federal government, he could get a shorter sentence.

The judge then turned to Monsegur and asked if he was willing to plead guilty.

"Yes," he answered. Monsegur could now skip any sort of trial. He read out a statement in which he admitted to a stream of illegal actions between 2010 and 2011.

"I personally participated in a DDoS attack on computer systems, PayPal, MasterCard, and Visa," he said. "I knew my conduct was illegal." He repeated the admission after listing every count on his indictment, from accessing the servers of Fox, to PBS, to Infragard Atlanta.

"Very well," said the judge. "The plea is accepted." The judge agreed to delay publishing the court docket because Monsegur could be in "great personal danger" if he were identified. Among the apparent risks laid out in court: hackers could send hundreds of pizzas to Monsegur's apartment or have a SWAT team sent to his home (tactics well known to 4chan users like William).

"It's actually called swatting," District Attorney Pastore had explained.

After the hearing, Sabu continued to collaborate with the FBI, working sometimes daily from the FBI offices. The Feds replaced his laptop, which was so old it was missing the Shift, L, and 7 keys, with a new laptop that contained key-logging software that monitored everything he typed. They put video surveillance in his home to monitor his physical movements. They allowed him to continue the public charade of being America's most wanted hacker, encouraging others to join the Antisec movement for which he had positioned himself as its leader, even taunting the police and his critics.

"Sources inside Interpol tell me (besides 'They like butter on their toast') that I'm next to get raided," he announced on Twitter in August. "Is everyone excited by this news?" Later he added: "Message to Interpol: SUCK MY DICK."

But many people in Anonymous had their suspicions about Sabu. Why had everyone else who had founded LulzSec been caught while the loudmouthed ringleader who was widely known to live in New York and be of Puerto Rican descent was still at large?

Among the more suspicious was Mike "Virus" Nieves, a hacker whom Sabu had collaborated with during LulzSec. On August 16, a day after Sabu's second court appearance, where he had agreed in writing to work for the FBI, Virus accused Sabu outright of being a snitch. The conversation started when Sabu first approached Virus and made the veiled accusation that a friend of Virus's was an informant. Virus saw through this deliberate tactic straightaway. It was a typical strategy among hacker informants: to faze someone who suspected you of being a snitch, you accused *him* of being a snitch. Their long and eventually hostile chat took place two weeks after Jake Davis had walked out of his first court appearance.

"Regarding Topiary," Virus told him. "You ratted him out. It's so obvious, Sabu."

"You better watch your fucking mouth because I'm not a rat," Sabu wrote back. "And I definitely didn't rat my own boy." Virus wasn't listening.

"I can spot a rodent a mile away," he said, adding for good measure, "'Antisec,' what a fucking joke."

"For a fucking joke it's doing more mayhem than it did a decade ago," Sabu retorted.

"You don't even get what Antisec was about," said Virus. "You're not owning whitehats. Just dumbass foreign .govs."

"I was actually involved," said Sabu. "Big difference man. I

don't sit here and run automated tools. I'm a seasoned security researcher going back to mid-to-late 90s."

"You're a low-level blackhat that got owned," Virus shot back. "I'm done being your friend. You're way too shady and I'm too old for this childish crap. Your lame-ass Antisec movement is hitting anything it can." In truth, Sabu's Antisec followers were often thwarted when they tried to hit out at "anything they could." The FBI was taking advantage of Sabu's cult-leader status by following up each hacker who presented a vulnerability to his mentor in the hope of a pat on the head. Sabu sometimes received more than two dozen vulnerabilities a day, and each time he would alert his FBI handlers. By August of 2011, he had helped the FBI patch a hundred and fifty vulnerabilities in computer networks that other hackers were targeting or was at least helping to mitigate the damage. Over the coming months, he would reportedly assist in alerting about three hundred government and corporate organizations about potential attacks by hackers with Anonymous, allowing them to patch flaws in their networks.

As Virus brought his standoff with Sabu to an end, he waxed pragmatic about what Sabu was probably doing. "Quite frankly, I don't care if you're working with the Feds to clean up the mess you created and getting your so called 'friends' arrested," he said. "It's human nature."

"My nigga," said Sabu. "You seriously need to stop saying that."

"Or?"

"We'll meet up in Manhattan and talk it out face to face."

"I know your tactics, and you won't gain access to any of my shit," said Virus.

"Bro, you know me less than the Feds do," Sabu said, momentarily hinting at his working relationship the FBI. "But let's be real."

The two went back and forth about how offensive *snitch* was

before Sabu observed, "You're talking a lot of shit, like you have some issue with me. I always gave you mad love even from the first day I met you."

"I don't care for your love," said Virus with finality. "There is no 'love' on the internet." This seemed to ring true above all else. Sabu may have been a skilled rooter who could find network vulnerabilities and exploit them, but his greatest skill was hacking into people's minds. He lied to the very team members he had brought together and led, all the while helping the police build up charges against them and corroborate their identities. All the more impressive was that Sabu's charisma and lies were so effective that other hackers continued working with him, even after Topiary, Tflow, and Kayla were arrested, and even as other hackers remained suspicious of him. It was even said to be an open secret among hackers in New York City that "Sabu" was Monsegur, with one rumor doing the rounds that local hackers had sprayed graffiti on his building.

On the same day as Sabu's confrontation with Mike Virus, a group of self-styled anti-Anonymous investigators published a blog post claiming to dox Sabu. This time it included a photo of a large Latino-looking man in his late twenties, wearing a leather jacket and a hat. The photo was of Monsegur. It also showed a detailed history of his exploits, and his IP address. It was perhaps the most comprehensive dox to date. The following day, August 17, Sabu posted a cryptic message on Twitter, invoking a quote from the movie *The Usual Suspects* about the film's mythical bad guy, Keyser Söze: "The greatest trick the devil ever pulled was convincing the world he did not exist. And like that…he is gone." For the next few weeks, nobody heard a peep from Sabu on public IRC or Twitter. Most assumed that he had either fled or been caught. Then exactly a month later, on September 17, he started tweeting again, starting with:

"They tried to snitch me out, troll me, dox every one around

me, bait me into endless arguments but there's one thing they can't do: STOP ME!"

All at once, Sabu dived back into the world of Anonymous and Antisec, jumping into conversations on public IRC channels and asking to hear reports from other Antisec hackers. For the most part, he didn't join in any attacks. Other hackers close to Sabu at the time do not remember him hacking anything for the months after he came back. They knew that he was bragging publicly on Twitter about attacks he had carried out but assumed this was part of his role as a mouthpiece for Anonymous and Antisec. Sabu instead pushed the "younger ones" with Anonymous by praising them and offering to help facilitate attacks, one source said.

At one point, for instance, he offered to help Anonymous hackers in Brazil get root access to government servers. (Hacktivism is extremely popular in Brazil, in part because the country has the highest rate of Twitter usage and also because of long-standing controversy over government corruption.) Sabu acted as the mediator, talking to the Brazilian hacktivists, then telling his crew of hackers what the Brazilians wanted to deface. His crew rooted the Brazilian servers and then sent Sabu the login credentials to pass on to the Brazilian hackers.

"We can't remember one [hack] he did, even before he got busted," said one hacker who had been working with Sabu from at least late 2011. "He liked to say he did it all. He did not."

It is unclear to what extent Sabu was allowed to hack with impunity during his time assisting the FBI. There are different accounts. Some say that in his role to corroborate the public claims by Anonymous that a company or government agency had been hacked, he would enter the targeted network and check that the vulnerability was there. Others have said he would simply check the claims out by talking to other hackers in private IRC rooms. It was probably a bit of both. For the most part, he was either giving advice, barking orders, or trying to keep on top of what was going on. For instance, he asked a hacker named Sup_g who had stolen data from nychiefs.org in December of 2011, "What's the latest with that nychiefs ownage? You done with it or?"

That month, Sabu helped the FBI get a glimpse inside one of Anonymous's biggest attacks and bait that same hacker. The attack was on Stratfor, an Austin-based intelligence service that made money selling a newsletter to clients who included the Department of Homeland Security.

On December 6, Sup_g approached Sabu about Stratfor, excitedly, in a private IRC channel.

"Yo, you round? Working on this new target," he said.

"Yo," said Sabu. "I'm here." Sup_g pasted a link to the admin panel for Stratfor.com, saying that it could lead to credit card data that he was confident he could decrypt.

Sabu notified his FBI handlers. Over the next few days, Sup_g and other hackers dubbed the Stratfor hack *lulzxmas* and deemed it a landmark attack for Anonymous and Antisec. A week later, Sup_g spent around eight hours getting into the company's network, and the following day, December 14, he told another hacker that he was now in Stratfor's e-mails.

"We in business baby," he said. "Time to feast upon their [e-mail] spools.... I think they'll just give up after this goes down." As the FBI looked on, apparently helpless, the hackers stole 60,000 credit card numbers, along with records for 860,000 clients of Stratfor, staff e-mails and financial data, and a whopping 2.7 million confidential e-mails. At the FBI's direction, Sabu told the crew to store it all on a New York server.

On Christmas Eve, December 24, the hackers defaced the Stratfor site and published the credit card details of 30,000 Stratfor clients, claiming they had used them to donate $1 million to charity—even publishing receipts. The FBI later confirmed that the credit cards had been used to make at least $700,000 in fraud-

ulent charges. Stratfor had to stop charging a subscription for its all-important newsletter and it estimated the breach cost it $2 million in damages and lost revenue.

Sabu might not have stopped the breach, but he did help the FBI identify the person behind the Stratfor attack, Sup_g. He did this by corroborating that Sup_g also went by another nickname, Anarchaos. On December 26, Sabu approached Sup_g online, going perhaps a little over the top in playing the role of the still-outlawed hacker.

"Yo yo," he said. "I heard we're all over the newspapers. You mother fuckers are going to get me raided. HAHAHAHA."

"Dude it's big," said Sup_g.

"If I get raided anarchaos your job is to cause havoc in my honor," Sabu said, subtly dropping Sup_g's other nickname, anarchaos, and adding a heart—<3—for good measure.

"It shall be so," Sup_g replied, unaware that he had just implicated himself. Over the next few months, as the Feds pored over chat logs with Sup_g on Sabu's computer, they pieced together enough personal information to build up a picture of who the hacker really was. It led them to twenty-seven-year-old Jeremy Hammond, a political activist from Chicago who wore long dreadlocks and was a practicing freegan—federal agents reported seeing him looking in dumpsters for food once they started physical surveillance. His mother later told reporters that Hammond had been a computer genius who couldn't stop his urge to "get the goat of America."

The FBI may well have had a bigger target in mind than the dreadlocked Hammond: Julian Assange. Soon after the hackers breached Stratfor's e-mails and started rummaging through them, they noticed that many e-mails talked about WikiLeaks. The hackers decided it made sense to pass them over to the whistle-blower organization and that WikiLeaks would do a better job at disseminating them anyway.

It is possible, though not conclusive, that as the FBI watched what was about to happen, they hoped to take advantage of the Stratfor hack and gather more evidence against Assange so they could finally extradite him to the United States. The FBI later denied to the *New York Times* that they "let [the Stratfor] attack happen for the purpose of collecting more evidence," going on to claim the hackers were already knee-deep in Stratfor's confidential files on December 6. By then, they added, it was "too late" to stop the attack from happening. Court documents, however, show that the hackers did not access the Stratfor e-mails until around December 14. On December 6, Sup_g was not exactly "knee-deep" in Stratfor files: he had simply found encrypted credit card data that he thought he could crack.

It is also telling that Sabu, the man who had jumped into Anonymous to help avenge Assange, suddenly seemed very keen to talk to the WikiLeaks founder once his FBI handlers were watching. Beyond the initial contact he made during LulzSec, hacker sources have said, Sabu tried especially hard to speak to Assange again and again after the Stratfor hack, "bugging" Assange's assistant to talk to him.

"Sabu was trying to contact [Assange] for a long time," one hacker said. Others add that when Sabu first heard that Anonymous was planning to give the Stratfor e-mails to WikiLeaks, he "freaked out," then called WikiLeaks by telephone and demanded to speak to Assange directly. It is unclear if he got through to Assange himself or just his assistant, but according to several sources, Sabu then asked for money in exchange for the Stratfor e-mails. Assange apparently said no.

When the Stratfor hackers got wind of news that Sabu had asked for money for the e-mails they had stolen, they were shocked, and quickly transferred the e-mails to WikiLeaks' server for free. WikiLeaks has not denied, publicly or in private, that Sabu asked for money from the organization. But if Wiki

Leaks had paid for them, American authorities might have had a much stronger case against Assange. It seems doubtful that the FBI had the time or inclination to decide from the top down that it wanted to play along and try to nab WikiLeaks, but perhaps an agent somewhere had the idea to nudge Sabu to ask Assange for money, and see what came of it.

Once WikiLeaks had the Stratfor e-mails, it formed partnerships with twenty-five media organizations, including *Rolling Stone* and *Russia Reporter,* and published a drip-feed of confidential information. WikiLeaks called them the Global Intelligence Files.

News commentators noted that this marked the first time WikiLeaks was sourcing files from data that had been hacked by Anonymous. Till then, hardly anyone outside of LulzSec's hacking community, WikiLeaks, and the FBI had known that Assange had been dealing to Sabu and other Anon hackers since June of 2011. That of course did not mean there was a solid partnership in place. Two separate hacker sources said that for a long time, Assange did not trust Sabu. Exactly why is unclear, but Assange would not have been the only one to sense that something was off.

"There is one thing that really struck me as funny after he came back," said another hacker, referring to when Sabu had returned to LulzSec after going missing for twenty-four hours (his secret FBI raid in June 2011). "He suddenly talked about his family. He mentioned in a private chat to me that he had two kids." This was deeply unsettling. Despite the unspoken rule in Anonymous to never talk about your personal life, Sabu was suddenly saying things like "My family is the most important thing." Before then, he had never talked about his two daughters. Another oddity: when others from Anonymous were questioned by police and then allowed to come back online, they mentioned to other hackers how strange it was that the authorities never asked them about Sabu.

Sabu was unflinching when he denied to hackers, and in interviews, that he was "Hector Monsegur," using the implausibility of the situation to his advantage and tweeting on June 26, 2011, "How many of you actually fell for that bad whois info? Haha. First off 'hector montsegur' has been posted every day for the last six months." He repeated this line to others in private.

Surprisingly, though, Sabu admitted to his closest hacker friends that the several acts of doxing him—and there were others besides Emick who came up with Hector Monsegur—were correct. This, again, was bizarre, but many assumed it was Sabu's usual nihilism, the guy whose favorite saying was, "I've gone past the point of no return." Sabu seemed to relish the trouble he was getting himself into and at some point down the line, they figured, he would get busted.

In late November of 2011 and then again in January of 2012, a hacker confronted Sabu about not hacking into any targets himself. "Man, get your hands dirty for once," the hacker told him in exasperation, adding that it was the only way to prove to others that he was not a snitch. Sabu responded with histrionics, claiming he had done plenty for the cause already, then adding that "haters" wanted to hunt him down. As Sabu ranted, the hacker typed out an emoticon for weariness, -.- , and went back to work.

Despite their suspicions, most of Sabu's associates never really believed that this veteran revolutionary hacktivist who was so passionate about his cause could really be a snitch.

"The idea was so horrid. And we weren't sure who to trust to talk about it," the same hacker said. Sabu had such a strong psychological hold on his crew that they actually feared asking around about his true intentions lest the volatile figure suddenly flip out on them.

While Sabu was an informant, his lies were aimed at not only other hackers but also journalists. Together with his FBI handlers, he would lie to reporters who hoped for an online inter-

view. Sometimes the reporters were speaking to federal agents, other times it was Sabu but with the agents looking over his shoulder. In the end, it was just another disinformation campaign.

Throughout his volatile year with Anonymous, Sabu had proved himself to be a masterful liar. But there was one thing he could not seem to fabricate: his name. At one point in 2011, before his FBI arrest, Hector Monsegur dropped the nickname Sabu online and started trying to use the new nickname Kage or Kaz in private IRC channels. The goal was to start anew, burn the old Sabu name, and avoid arrest and doxing. Had he maintained the new names, he might never have been raided by the FBI and might still be living with his two kids in his Lower East Side apartment today, watching YouTube videos and paying the bills with stolen credit card numbers. But Monsegur couldn't manage the new online identity. After a few weeks, he went back to using Sabu.

This was the dilemma for hackers in Anonymous. There were practical problems when someone who was well connected in the hacker underground, like Sabu, took on a new name. He would lose his contacts and the trust he had with them. Sabu had brought in dozens of useful contacts from his time underground to work with LulzSec, Anonymous, and Antisec. Hector Monsegur could never have orchestrated all that collaboration without the name Sabu. In the end, ego and a thirst for control got the better of him.

By early 2012, FBI administrators had begun to go back and forth over when they should out Sabu as their informant. So far, he had helped fix a number of vulnerabilities in targeted networks, helped identify Jeremy Hammond, and helped bring charges on Donncha "Palladium" O'Cearrbhail, from Ireland. In early January of 2012, O'Cearrbhail (a Gaelic name that's pronounced "Carol") had hacked into the Gmail account of a member of the Irish national police, an officer who routinely sent e-mails from his official police account to his Gmail account. One of the e-mails contained details of a conference call that was to occur on January 17 between FBI agents and Britain's Metropolitan Police to discuss the LulzSec and Anonymous investigation. Palladium quickly notified Sabu that he would be listening in and recording it.

"I am happy to leak the call to you solely," he said excitedly. "This will be epic!"

After recording the eighteen-minute call, Palladium passed the audio file to Sabu, who then passed it to the FBI to corroborate that it was real. It was. When Sabu didn't publish the file online, someone else put it up on YouTube, much to the delight of the Anon community and embarrassment of the FBI. Behind the scenes, the FBI went on to identify Palladium (thanks to a search warrant they'd gotten on a friend's Facebook account) and level a significant charge against the hacker (thanks to Sabu's chat logs). Sabu had helped gather evidence against five people, all told: Topiary, Kayla, Tflow, Sup_g (Jeremy Hammond), and Palladium.

In early 2012, police on both sides of the Atlantic got ready to press charges against the five Anons. The time to out Sabu was soon, but choosing a date wasn't easy.

"There were constant problems with the relationships between the British authorities and the FBI," said one person with knowledge of the FBI investigation into LulzSec and Anonymous. Though Sabu was in New York, at least four LulzSec hackers lived in the British Isles, which meant Britain's Metropolitan Police were more eager than their American counterparts to pull the trigger and charge them. While the Americans had a major informant who could help them grab more hackers at large, the Brits had four hackers they were ready to send through the court system.

The FBI wanted to capitalize on their Lower East Side snitch as much as possible. He had helped patch those flaws, and the announcement of his arrest and the revelation of his duplicity would devastate the socially disruptive ideas of Anonymous and Antisec. But the Feds could not know for sure how useful Hector Monsegur would continue to be. Though he was smart and well connected, he was also a loose cannon. One evening in early February, a cop from the NYPD encountered Hector at another apartment in his neighborhood. He asked Hector for his ID.

"My name is Boo. They call me Boo," Hector replied. "Relax. I'm a federal agent. I am an agent of the federal government." It seemed that Hector had started to believe that he was both Sabu and a bona fide FBI agent. That same evening he was charged with criminal impersonation.

Just as complicated: In monitoring Sabu, the Feds were getting a look at how quickly things moved in the worlds of Anonymous and Antisec. Sabu saw scores of ideas for attacks floated every day, and while some got thrown out, others were followed up faster than the FBI's red tape might allow. Hackers bragging on Twitter, Internet drama, lulz—this was all new territory for the FBI.

When London's Met finally told the FBI that they had a "drop-dead" date of March 7 to arrest and publicly charge the person alleged to be Kayla, a date from which they could not budge, the Feds agreed to out Hector just before that deadline too. Everything would come out into the open at the same time: the suspected identities of Kayla, Pwnsauce, Palladium, and Stratfor hacker Sup_g, and the news that Sabu had been working with the FBI for an extraordinary eight months. It was a bombshell, and the police were about to drop it squarely on Anonymous.

CHAPTER 27

The Real Kayla, the Real Anonymous

Seven months earlier, on September 2, 2011, British police had pulled up to a family-sized house in the quiet English suburb of Mexborough, South Yorkshire. It was a cold and gray morning. One of the officers had a laptop open and was watching the @lolspoon Twitter feed, waiting for the hacker known as "Kayla" to post another tweet. When she did, several more burst in the house through a back entrance, climbed the stairs to the bedroom of Ryan Mark Ackroyd, walked in, and arrested him. Ackroyd was twenty-five and had served in the British army for four years, spending some of that time in Iraq. Now he was unemployed and living with his parents. Appearance-wise he was short, had deep-set eyebrows and dark hair in a military-style crew cut. When he spoke, the voice that emerged was a deep baritone, and the accent strongly northern English. Ackroyd's younger sister, petite and blond, was, perhaps tellingly, named Kayleigh.

In the same way police had simultaneously questioned Jake Davis's brother, detectives also synchronized Ackroyd's arrest with that of his younger brother, Kieron, who was serving in the army in Warminster, England. After questioning Kieron, the po-

a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," a/k/a "ghost," a/k/a "anarchacker," the defendants, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, which would and did cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least $5,000 to one and more persons during any one year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I).

OVERT ACTS

39. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about December 14, 2011, HAMMOND exchanged online chat messages with a co-conspirator not named as a defendant herein ("CC-1"), in which HAMMOND stated that he had gained unauthorized access to Stratfor's computer network.

b. On or about December 19, 2011, a co-conspirator not named herein ("CC-2") uploaded data stolen from

Stratfor to a computer server located in the Southern District of New York.

c. On or about December 26, 2011, HAMMOND exchanged online chat messages with co-conspirators not named herein ("CC-3" and "CC-4"), in which HAMMOND stated that he and his co-conspirators had decrypted the passwords for the user accounts of 4,500 Stratfor clients.

d. On or about December 26, 2011, HAMMOND exchanged online chat messages with CC-3 and CC-4, in which they discussed exploiting credit card information that had been stolen from Stratfor's computer servers.

(Title 18, United States Code, Section 1030(b).)

COUNT FOUR

(COMPUTER HACKING - STRATFOR)

The Grand Jury further charges:

40. The allegations in paragraphs 1 through 6 and 31 through 36 of this Indictment are repeated and realleged as though fully set forth herein.

41. From at least in or about December 2011, up to in or about March 2012, in the Southern District of New York and elsewhere, JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," a/k/a "ghost," a/k/a "anarchacker," the defendant, willfully and knowingly caused the

transmission of a program, information, code and command, and, as a result of such conduct, intentionally caused and attempted to cause damage without authorization, to a protected computer, which caused and attempted to cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least $5,000 to one and more persons during any one year period, to wit, HAMMOND and others gained unauthorized access to computer systems used by Stratfor, a company which provides information analysis services for its clients, and, among other things, defaced Stratfor's website; stole confidential data from Stratfor's computer network, including Stratfor employees' emails, as well as personally identifying information and credit card data for Stratfor's clients; publicly disclosed at least some of that data by dumping it on certain Internet websites; used at least some of the stolen credit card data to make unauthorized charges; and deleted data on Stratfor's computer network.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), 1030(c)(4)(B)(i), and 2).