COMMENTARY

Stratfor Hacker: FBI Entrapment Shaped My Case

Mathew J. Schwartz | October 04, 2013 09:06 AM

Is the FBI allowed to entrap suspected computer criminals? That question is at the heart of a request for leniency by Jeremy Hammond, who's due to be sentenced on November 15 for hacking private intelligence contractor Stratfor, among other business and government sites.

Hammond, appearing in a Manhattan federal courtroom in May, pleaded guilty to one related count of computer fraud and abuse, as part of a plea agreement. "For each of these hacks, I knew what I was doing was wrong," Hammond told judge Loretta Preska, the *Chicago Sun-Times* **reported**. He now faces up to 10 years in jail, and the prospect of paying up to $2.5 million in restitution to Stratfor.

But in advance of his upcoming sentencing by Judge Preska, Hammond's supporters are asking for leniency, noting that Hammond hacked for ethical reasons, rather than to make a profit. They've also accused the FBI of entrapment, referring to tricking someone into committing a crime for the purpose of then arresting them. Hammond, notably, **has accused former LulzSec leader turned FBI informant "Sabu"** -- real name: Hector Xavier Monsegur -- of inciting participants of the Anonymous Operations (AnonOps) IRC channel, including himself, to hack into a number of systems, including Brazilian government servers for which Sabu reportedly distributed stolen access credentials.

[Take heed of the security warnings that seem to pop up every day. Read WordPress Attacks: Time To Wake Up.]

"Sabu was used to build cases against a number of hackers, including myself. What many do not know is that Sabu was also used by his handlers to facilitate the hacking of targets of the government's choosing -- including numerous websites belonging to foreign governments," Hammond said in an August **statement**.

What proof can Hammond offer? Attorney Margaret Ratner Kunstler, who's a member of Hammond's defense team, told me via email that "all but publicly filed documents are covered by [a] protective order," meaning related evidence has been sealed, at the request of prosecutors. Accordingly, "proof is only in the form of failure of government to deny" Hammond's allegations, she said.

An FBI spokeswoman, reached by phone, declined to comment on Hammond's allegations.

This **wouldn't be the first time** that the bureau's computer crime investigators have been accused of employing these types of tactics. "The FBI intended to entrap me via Sabu for as long as possible to incriminate my activities at the highest level," said former LulzSec participant Jake Davis last month, in an **ongoing Q&A session** on the Ask.fm website. Davis, who used the handle "topiary," handled the LulzSec's PR, but didn't take part in any of its actual hacking activities. He was **arrested by British police** in July 2011.

"One week I told Sabu that I had no intention of involving myself in any more crime -- organized by him -- and that I wanted to switch to helping the activist movement solely through art and writing," said Davis, who's now served related jail time in the United Kingdom and been released. "That same week my home was raided. It's nothing new, we were just another set of pawns in the FBI's strategy."

If that was the FBI's strategy, however, what may surprise is that the bureau wouldn't have broken any laws or investigation guidelines. "Unfortunately, there are numerous cases holding that this type of scenario -- very common in child pornography cases where agents pose as either children or brokers of child pornography -- does not constitute impermissible entrapment," sentencing expert Jeff Ifrah, an attorney who's previously chaired American Bar Association criminal justice and white collar crime committees, told me via email.

Page 2: What Did The FBI Know?

1 | 2 | Next Page »

COMMENTARY

Stratfor Hacker: FBI Entrapment Shaped My Case

What Did The FBI Know?

It's clear that Monsegur, who was **quietly arrested by the FBI** in June 2011 and immediately turned informant -- before later pleading guilty to a number of charges -- was being run by the FBI. Furthermore, prosecutors have said that he's monitored around the clock, and restricted to using an FBI-provided computer that records everything he does.

That means that Sabu, and thus the FBI, knew about the Stratfor hack before it happened. Notably, Hammond, using the handle "Sup_g," told Sabu on Dec. 6, 2011, that he planned to hack Stratfor, then did so a week later. Sabu, meanwhile, directed Hammond to upload the stolen data to a server that was really controlled by the FBI. But on Dec. 24, after Sabu reportedly attempted to sell the Stratfor data to Julian Assange at WikiLeaks -- he declined the offer -- Hammond publicly released the data. Two days later, Sabu tied Sup_g to another alias, "Anarchaos," that the bureau knew belonged to Hammond. But several months followed before the FBI arrested Hammond.

Could Stratfor's customer database have been protected -- and $2.5 million in damages and cleanup costs avoided? "Jeremy is about to get sentenced for the Stratfor part based on *their assessed damages*," alternative media expert **Nigel Parry**, who's been following Hammond's case, told me via email. "And a lot of those damages -- after we get beyond the early part of the hack that netted the credit card numbers (i.e. Stratfor's email losses, its data deletion) -- seem to me to be the direct result of the FBI's blatant hands-off approach and Stratfor's inept sysadmins, who didn't have a single backup of their data?!"

[Was entrapment involved in the Silk Road arrest? Read Silk Road Founder Arrested.]

The FBI appears to stand on solid legal ground here. "Unfortunately, there are numerous cases holding that the government has no obligation to mitigate damages, or intervene in a criminal investigation to mitigate the fallout or consequences," attorney Jeff Ifrah said. "There have been cases that have held in different contexts that the government may have been a contributing factor or intervening factor in the loss, but that type of logic ... has not been applied in a loss calculation scenario at a federal criminal sentencing proceeding," he said.

In other words, there's no precedent for getting a sentence -- or restitution -- reduced, owing to FBI entrapment. "In a sentencing context, the only relevant determination is foreseeable loss, or in some circumstances, actual loss," Ifrah said. "But courts default to the former and thus that becomes a crutch to ignore what role the FBI -- in this case -- did or did not play," he said.

The moral of the story: the FBI can entrap hackers, and businesses that have been owned by said hackers may get used as bait. So, would-be hackers, beware the FBI. And businesses -- especially ones that bill themselves as being private intelligence contractors, yet which store credit card data in plaintext format and see a crucial database get owned by a simple SQL injection attack -- make sure your information security defenses are strong enough to prevent you becoming hackbait.

ABOUT THE AUTHOR