Notorious hacktivist shares methods, motives

November 10 2014, by Martha Mendoza

This March 5, 2012 file photo provided by the Cook County Sheriff's Department in Chicago shows Jeremy Hammond. Once the FBI's most-wanted cybercriminal, Hammond is serving one of the longest sentences a U.S. hacker has received, 10 years, the maximum allowed under his plea agreement last year. (AP Photo/Cook County Sheriff's Department, File)

Cocaine dealers, bank robbers and carjackers converge at Manchester Federal Prison in rural Kentucky—and then there is Jeremy Hammond, a tousle-haired and talented hacker whose nimble fingers have clicked and tapped their way into the nation's computing systems. Among those whose data he helped expose: the husband of the federal judge who sentenced him.

"From the start, I always wanted to target government websites, but also police and corporations that profit off government contracts," he says. "I hacked lots of dot-govs."

An Associated Press report this week found the $10 billion-a-year effort to protect the federal government's extensive computer systems is struggling to keep up with a daily bombardment of cyberattacks from thieves and hostile states that grab Social Security numbers, peruse Pentagon secrets and hijack critical websites. Human error, by way of employee missteps, is often to blame.

Those behind these incidents are a motley group: foreign spies, intellectual property thieves, personal identity peddlers, and, increasingly, politically motivated hacktivists like Hammond. Once the FBI's most-wanted cybercriminal, Hammond is serving one of the longest sentences a U.S. hacker has received—10 years, the maximum allowed under his plea agreement last year.

"This is the nicest room in the place," he said when the AP recently sat down with him in a drab cinderblock visiting room to talk about how and why he did what he did. Prison authorities barred cameras and recorders, citing security.

A hacktivist for more than a decade, Hammond, 29, was arrested in 2012 after penetrating the U.S.-based security think tank Stratfor, whose clients include the U.S. Department of Homeland Security and the

Defense Department.

He'd been working with a subgroup of the loose-knit hacking movement "Anonymous" to disrupt the networks of Sony Pictures, the Public Broadcasting Service, the Arizona Department of Public Safety and others when a member of the group enlisted him to help break into Stratfor's systems.

Some breaches in Hammond's life had been a challenge. He'd search the code on websites he wanted to target, combing through the symbols and letters of computing languages for security flaws to exploit. He'd create user accounts on the sites, and then test for ways in. It could take months of trying, and sometimes he gave up.

But the Stratfor hack was a cinch, he said. Basic security was not in place, a flaw later acknowledged by Stratfor CEO George Friedman. "We did not encrypt credit card files," Friedman said. "This was our failure."

Hammond was like a kid in a candy shop: "I was like damn man, this is crazy."

The hackers posted emails between Stratfor employees and clients on the WikiLeaks website (some 5 million exchanges, they claimed), along with credit card data from a client list that included Northrop Grumman, the Marine Corps and Time Warner Cable. They used some of the credit card numbers to donate money to the Red Cross, according to court records.

Among the thousands whose emails were disclosed was the husband of the federal judge who sentenced Hammond. She chose not to recuse herself, noting that no harm was done. Her husband's email address was exposed but already publicly available, and no actual correspondence or

credit card information was revealed.

Federal prosecutors said the Stratfor hack resulted in more than a million dollars in losses to individuals, and threatened public safety. A hacking "recidivist," they called Hammond.

Raised in the Chicago suburb of Glendale Heights with his twin brother Jason by their father, a musician, Hammond said he was a "nonconformist, anti-authority" kid. At 8, he tried his hand at designing video games. A few years later, he started hacking.

Then came 9/11. Hammond was 16, and considered some of the government's anti-terrorism actions "police state measures."

"I had a sense of duty to take action," he said.

With his brother, he protested, started an underground school newspaper and then organized a high school walkout when the U.S. invaded Iraq in 2003. That year, Hammond also launched HackThisSite.org, where hackers of all skill levels can hone their abilities and share tips.

He considered hacking a means of social justice, and he did it in secret while pursuing civil disobedience and protest in public, as well.

He started the University of Illinois at Chicago with a full scholarship, cooked and gave food to homeless people and set up a free public computer lab.

He also hacked into the university's computer science department website, and then told administrators about the vulnerability. They kicked him out, according to court records.

That summer, at 19, with a black scarf tied around his neck, Hammond

was both heckled and cheered as he encouraged the audience at the hacking conference DEFCON to engage in a campaign of "electronic civil disobedience" against the upcoming Republican National Convention in New York.

"There's going to be a series of defacements, financial disruption, email flood campaigns," he promised, and some GOP websites did later report technical difficulties.

As Hammond's social and political actions mounted, so did his arrest record. He pleaded guilty to battery after fighting with anti-gay protesters at a Chicago Pride Parade and was again taken to jail after joining hundreds of counter-demonstrators at a neo-Nazi rally.

A hack into the website of a group that was harassing Iraq War opponents got Hammond sentenced, in 2008, to 20 months in federal prison. Once out, he got involved in local activist movements, then public protests and then more hacking.

Working from a coffee shop or inside a vacant building with Wi-Fi nearby, Hammond used a Tor web browser that prevents people from learning the user's location, and he identified himself only with nicknames including "Anarchaos" and "crediblethreat."

He always had a day job—at a computer repair store and, later, as a web developer for an advertising firm. Hammond's brother, who lived with him, told the sentencing judge that "no one around him had any inkling that he was getting involved in the group called Anonymous."

Three months after the Stratfor leak, on March 5, 2012, Hammond was smoking pot and chatting with friends in the kitchen of his Chicago home when the front door was kicked in. Someone threw a flash bang.

"There were all these dudes with assault rifles," he said.

Everyone else hit the floor, but Hammond dashed to his bedroom to slam shut his encrypted Mac laptop.

The FBI caught Hammond with the assistance of Hector Xavier Monsegur, a famous hacker known as Sabu who helped law enforcement infiltrate Anonymous and convict eight hackers in all.

Hammond, up for release in 2020, spends his days folding laundry and sewing, studying Spanish, playing chess and reading books supporters send him.

Asked about the larger danger posed by cybercriminals, he laughed at the idea that some consider such attacks as threatening to national security as terrorism.

"I mean, I didn't kill anybody," he said.

At the same time, he knows the risk of nation states or others using a computer to do harm is real.

"If I was capable of doing these things on my own or with my team, what about a well-financed team that trained for years?"

To this day, Hammond is unsure how agents cracked his encryption program and got what they needed to land him back in prison. But he has one idea: "My password was really weak."

It was his cat.

"Chewy," he said, looking down at his hands. "Chewy 123."