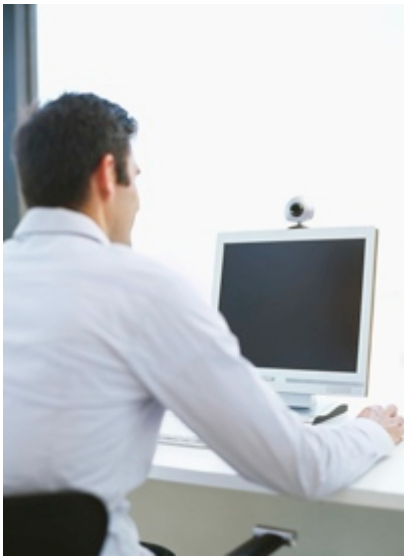
Written by **Daniel Sayani** on June 10, 2011

Federal Govt Has Recruited One-Fourth of U.S. Hackers as Informants



The FBI and Secret Service have successfully infiltrated the underground world of computer hackers in the United States, and now 25 percent of these hackers are — for fear of a long prison sentence — secretly informing the government about their peers. In fact, the community is riddled with paranoia and mistrust as it is not clear who is part of this "army of informants."

In an interview with the London-based *Guardian*, Eric Corley, publisher of the hacker quarterly known as *2600*, said that in some cases, popular illegal forums used by cyber criminals as marketplaces for stolen identities and credit card numbers have been run by hacker turncoats acting as FBI moles. In others, undercover FBI agents posing as "carders" — hackers specializing in ID theft — have themselves taken over the management of crime forums, using the intelligence gathered to put dozens of people behind bars.

"Owing to the harsh penalties involved and the relative inexperience with the law that many hackers have, they are rather susceptible to intimidation," Corley told *The Guardian*.

"It makes for very tense relationships," said John Young, who runs Cryptome, a website depository for secret documents along the lines of WikiLeaks. "There are dozens and dozens of hackers who have been shopped by people they thought they trusted."

The best-known example of the phenomenon is Adrian Lamo, a convicted hacker who turned informant on Bradley Manning, who is suspected of passing secret documents to WikiLeaks. Manning had entered into a prolonged instant messaging conversation with Lamo, whom he trusted and asked for advice. Lamo repaid that trust by promptly handing over the 23-year-old intelligence specialist to the military authorities. Manning has now been in custody for more than a year.

For acting as he did, Lamo has earned himself the epithets of "Judas" and the "world's most hated hacker," though he has insisted that he acted out of concern for those he believed could be harmed or even killed by the WikiLeaks publication of thousands of U.S. diplomatic cables.

"Obviously it's been much worse for him [Manning] but it's certainly been no picnic for me," Lamo has said. "He followed his conscience, and I followed mine."

The latest challenge for the FBI in terms of domestic U.S. breaches is the anarchistic cooperatives of "hacktivists" that have launched several high-profile cyber-attacks in recent months that are each

designed to make a statement. In the most recent case, a group calling itself Lulz Security launched an audacious raid on the FBI's own linked organization InfraGard. The raid, which was a blatant two fingers up at the agency, was said to have been a response to news that the Pentagon was poised to declare foreign cyber-attacks an act of war.

Lulz Security shares qualities with the hacktivist group Anonymous, which has launched attacks against companies including Visa and MasterCard as a protest against their decision to block donations to WikiLeaks. While Lulz Security is so recent a phenomenon that the FBI has yet to get a handle on it, Anonymous is already under pressure from the agency. There were raids on 40 of its addresses in the United States and five in Britain in January, and a grand jury has been hearing evidence against the group in California at the start of a possible federal prosecution.

Kevin Poulsen, senior editor at *Wired* magazine, believes the collective is classically vulnerable to infiltration and disruption. "We have already begun to see Anonymous members attack each other and out each other's IP addresses. That's the first step towards being susceptible to the FBI."

Barrett Brown, who has acted as a spokesman for the otherwise secretive Anonymous, says it is fully aware of the FBI's interest. "The FBI are always there. They are always watching, always in the chat rooms. You don't know who is an informant and who isn't, and to that extent you are vulnerable."

Last month, the United States disclosed its International Strategy for Cyberspace, further indicating the move toward increased Internet scrutiny. The document revealed that the U.S. government could respond to cyber-attacks with military force, especially if someone were to pull off a serious cyberspace hack against America, its allies, its partners, or in such a way as to threaten its interests:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.

The 30-page document says that military force is now an option. It's thus possible that America will one day start a war in response to corporate or governmental computer systems being breached.

As far back as July 2001, the Department of Justice, FBI, and other federal agencies have actively sought to hire hackers, according to a CNET investigation:

> "The objective of coming and having a 'Meet the Fed' panel is to give folks who have not crossed the line yet a positive alternative," said Jim Christy, a supervisory special agent for the Department of Defense. "There is a whole lot of talent here — let's put that talent to good use."
>
> Rather than enemies meeting across the table, the session instead resembled a collegial meeting of the minds. At the end of the one-hour session, hackers mobbed the panel to continue the discussion and, in many cases, to inquire about jobs.
>
> Paul Smulian, chief of staff for the DOD's Directorate of Information Assurance in the Command, Control, Communications and Intelligence, or C3I, section, said that the government is actively looking for those technical hackers who have acted responsibly and ethically.

"Some of our most secret agencies across the country are looking at people with skills that the people in the audience have," he said after the session.

Perhaps inspiring this decision are reports from 2008 that reveal that the Department of Homeland Security's website is extremely vulnerable to hackers. Keith A. Rhodes, chief technologist at the U.S.

Government Accountability Office, secretly broke into the Department of Homeland Security network and deleted, updated, and captured information — all without anyone knowing he was even in there.

"I would label them [DHS] as being at high risk," Rhodes told *Information Week* the day after a congressional hearing into the security of the government agency tasked with being the leader of the nation's cyber security. He explained,

> There was no system we tested that didn't have problems. There was nothing we touched that didn't have weaknesses, ranging from WAN to desktops. … If we had continued the audit we would have found more. We curtailed the audit because we just kept finding problems. At a certain point, we just ran out of room in our basket.

Constitutionalists can only hope, however, that the liberties of the American public will be preserved amid the government's stealth mission to utilize hacking as a way of pursuing its policies — a scenario which can, if allowed to escalate to unconstitutional and unreasonable means, erode the freedom of U.S. citizens to utilize the Internet and other technologies as they see fit.