Written by **Alex Newman** on March 4, 2011

Feds Plotted Invasion of Social Media

The computer program the government was seeking would allow a handful of operators to control a vast army of fictitious online personalities on social-media platforms such as Facebook and Twitter. And one suggestion from a contractor hoping to win the bid involved creating fake profiles for real people — without their consent — to track or smear targeted individuals.

The Air Force request for the "Online Persona Management Service" posted last year on a federal contracting website, a screen shot of which is still available online, read:

> Software will allow 10 personas per user, replete with background , history, supporting details, and cyber presences [sic] that are technically, culturally and geographacilly [sic] consistent. Individual applications will enable an operator to exercise a number of different online persons from the same workstation and without fear of being discovered by sophisticated adversaries. Personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms. The service includes a user friendly application environment to maximize the user's situational awareness by displaying real-time local information.

Other requirements for the software included the ability to use "Virtual Private Networks" to provide unique IP addresses and locations for each of the fake online profiles. The program was also supposed to be able to protect "the identity of government agencies" engaged in the deception, while being able to blend into regular online traffic to provide "excellent cover and powerful deniability."

HBGary was one of the "security" companies to pitch its services in an effort to win the contract. And its offer went even further than what the government was originally asking for. One of the leaked e-mails from the company, for example, reads:

> Those names can be cross-referenced across Facebook, twitter, MySpace, and other social media services to collect information on each individual. Once enough information is collected this information can be used to gain access to these individuals[']social circles.
>
> Even the most restrictive and security conscious of persons can be exploited. Through the targeting and information reconnaissance phase, a person's hometown and high school will be revealed. An adversary can create a classmates.com account at the same high school and year and find out people you went to high school with that do not have Facebook accounts, then create the account and send a friend request.

Under the mutual friend decision, which is where most people can be exploited, an adversary can look at a target[']s friend list if it is exposed and find a target[']s most socially promiscuous friends, the ones that have over 300-500 friends, friend them to develop mutual friends before sending a friend request

to the target. To that end friend's account can be compromised and used to post malicious material to a target[']s wall. When choosing to participate in social media an individual is only as protected as his/her weakest friend.

Another leaked e-mail from HBGary Federal's CEO about the contract was equally unsettling. "There are a variety of social media tricks we can use to add a level of realness to all fictitious personas … Using hashtags and gaming some location based check-in services we can make it appear as if a persona was actually at a conference and introduce himself/herself to key individuals as part of the exercise, as one example," he wrote.

The revelations came from a loosely affiliated group of so-called "hacktivists" known as Anonymous. The hacker activists became notorious in recent months for shutting down websites of various Middle Eastern dictatorships and companies that were targeting the whistle-blowing organization WikiLeaks. After HBGary announced that it had some names associated with Anonymous, as well as information on the organization's structure, the group retaliated.

First, it hacked into and defaced the cyber-security firm's website, posting a scathing message (click here to see it) explaining its motivations and ridiculing the company, its "security" credentials, and its supposed discoveries about Anonymous.

"Let us teach you a lesson you'll never forget: you don't mess with Anonymous. You especially don't mess with Anonymous simply because you want to jump on a trend for public attention," read the hackers' note posted on the security firm's website. "It would appear that security experts are not expertly secured."

The group also deleted the firm's backed-up data and copied tens of thousands of company e-mails, which it then distributed online. Some of the e-mails were from company CEO Aaron Barr. He admitted in one of the messages leaked by the hackers that he was hoping to use the attack on Anonymous to drum up business.

Finally, adding insult to injury, Anonymous hacked into the CEO's Twitter profile and posted not-so-flattering messages along with the security boss's alleged address and social security number. Other company executives also had their social-networking profiles compromised. And the CEO's cellphone was wiped clean, too. Security analysts were impressed with the "true hacking skills" involved in the operation.

In a press release about the attack, Anonymous wrote: "We understand that our participants have been concerned about recent FBI raids and companies such as HBGary Federal lurking and logging our chats, so we've given all of Anonymous a message: we will fight back." The group also publicly posted all of the information about Anonymous gathered by the contractor (which supposedly planned to sell it to the Federal Bureau of Investigation) to prove that it was bogus.

"We are not a group, we are not an organization. We are just an idea," the Anonymous press release stated, noting that it has no leaders. "We will respond to those who seek to threaten us."

In addition to embarrassing HBGary — possibly beyond repair — and the federal government, the e-mails leaked by Anonymous also exposed the tactics pitched to Bank of America, the Chamber of Commerce, and other high-profile entities to attack their critics through deception and fraud. Analysts have blasted the security company, the government, and the unethical and possibly unlawful trickery being discussed by both entities.

Of course, this isn't the first time the government was caught plotting shady activities online. And it almost certainly won't be the last — especially if there are no consequences, though some members of the House of Representatives have started talking about launching an investigation. But in case it's not obvious by now, Americans should always be vigilant when using the Internet — that new "friend" might just be one of the regime's agents or agent-provocateurs.