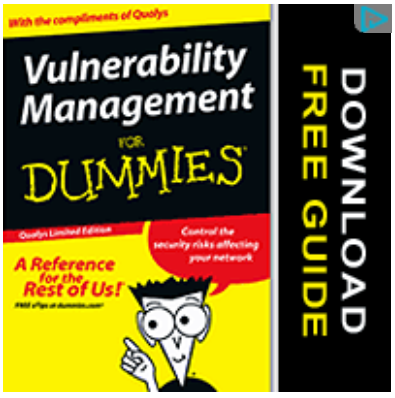
Report: HBGary used as an object lesson by Anonymous

by Steve Ragan - Feb 7 2011, 12:30

HBGary hacked by Anonymous.

- Email
- RSS
- Comment
- Facebook
- Twitter
- Digg
- FARK
- Slashdot



Aaron Barr, the CEO of HBGary Federal, told the Financial Times this weekend that he used clues found online to discover the identities of key Anonymous members. Anonymous reacted to the story and Barr's claims with a massive attack aimed at the security firm, leveraging local root exploits, shared passwords, and social engineering.

In an interview with the Financial Times, Barr said that by using services such as LinkedIn, Classmates.com, Facebook, as well as IRC itself, he was able to connect the dots and identify several high-level Anonymous members, including "Owen" and "Q", two people mentioned by their IRC names in the actual news report.

Having spent several months on IRC with people who associate under the banner of Anonymous, The Tech Herald can confirm that Q and Owen are actual names used by people on the AnonOps network. However, they are not the leaders they are made out to be by the Financial Times' story. Anonymous has no leaders. Even hinting at such a thing on IRC will invoke a long lecture on the topic.

Out of all of the people who participate in the various Anonymous operations, only 30 or so are consistently active. Of that group, only ten "are the most senior and co-ordinate and manage most of the decisions," Barr explained to the Financial Times.

The Tech Herald has seen Barr's research. [PDF] While there is plenty of information, several operation names and dates are out of order, and many of the names associated with membership are incorrect. When it comes to the ten "most senior people", they are actually network administrators.

They work to keep the IRC servers online. Their proper titles include Services Root Administrator, Network Administrator, and Operator. AnonOps is an IRC network, Anonymous is something entirely different. Those who manage the IRC servers might be part of Anonymous, but they are not co-founders or leaders. They are highly active people, but that is what is needed to maintain an IRC network such as theirs.

After the Financial Times story broke, including Barr's claims of infiltration, Anonymous responded. The response was brutal, resulting in full control over hbgary.com and hbgaryfederal.com. They were also able to compromise HBGary's network, including full access to all their financials, software products, PBX systems, Malware data, and email, which they released to the public in a 4.71 GB Torrent file.

In a statement emailed to The Tech Herald, Anonymous called Barr's actions media-whoring, and noted that his claims had amused them.

"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," the statement directed to HBGary and Barr said.

"You have blindly charged into the Anonymous hive, a hive from which you've tried to steal honey. Did you think the bees would not defend it? Well here we are. You've angered the hive, and now you are being stung. It would appear that security experts are not expertly secured."

The attack against HBGary is a classic example of leverage. It started with an SQL Injection attack on hbgaryfederal.com. From there, Anonymous discovered and cracked the passwords used on the site.

As it turns out, many of these passwords were used on Google Apps. Access to Apps, along with the use of shared passwords, led to the compromise Barr's Twitter account and a LinkedIn account.