Anonymous vs. HBGary: the aftermath

By Nate Anderson | Published 7 months ago

Anonymous

For Anonymous, the most obvious result of the hack was publicity, glorious publicity. The attack has been covered in every outlet from Ars to the BBC and back again, though the group was unbelievably lucky to stumble on a cache of e-mails involving dirty tricks against WikiLeaks and using intelligence assets against pro-union websites. Without those revelations, the hack and e-mail release might have looked far more self-interested—Anonymous protecting its mask.

Why have the attacks on HBGary Inc. continued? We spoke to people with knowledge of the initial Anonymous hack. All have denied the existence of continuing operations against HBGary and note that the IRC channel used for coordination, #ophbgary, has been shuttered; most expressed disbelief that these attacks are even happening.

We asked HBGary for a copy of some of the faxes received at its offices, but were told that the fax machines had been turned over to the authorities as part of the investigation. HBGary did pass along a representative e-mail that an employee received last week (all header information has been removed):

```
Subject: Security Problem

looooooooooooooooooool
owned by anonymous. niiiice.
hope your strategy wont work and ppl of this planet will become free
without beeing surpressed or monitored.
shame on you for your "business" - it is ppl like you who try to stop
human revelation all in the name of allmighty america.
nice to see you failing hard and getting exposed yourself. how does it
feel, suckers ?
i am looking forward to see your next fail.

greets
one of your monitored sheep that actually dont like to be monitored.

ps: please do us (the human race that is not trying to be nazis like
you) a favor and get aids and die slow and painfull,
thanks in advance.
```

The real impact of the attacks on Anonymous may not be felt for months, or even years. HBGary says it is working with the authorities on the case, and one presumes that the FBI is interested in busting those responsible. The FBI has previously arrested those associated with mere denial of service attacks, and it recently executed 40 search warrants in connection with Anonymous' Operation Payback.

In a press release regarding the search warrants, the FBI reminded Anonymous that "facilitating or conducting a DDoS [Distributed denial of service] attack is illegal, punishable by up to 10 years in prison, as well as exposing participants to significant civil liability."

Butterworth, who touted his own (lengthy) list of advanced security credentials during our call, told us that based on his investigation so far, the Anonymous "operational security was not that good… they're pretty dirty."

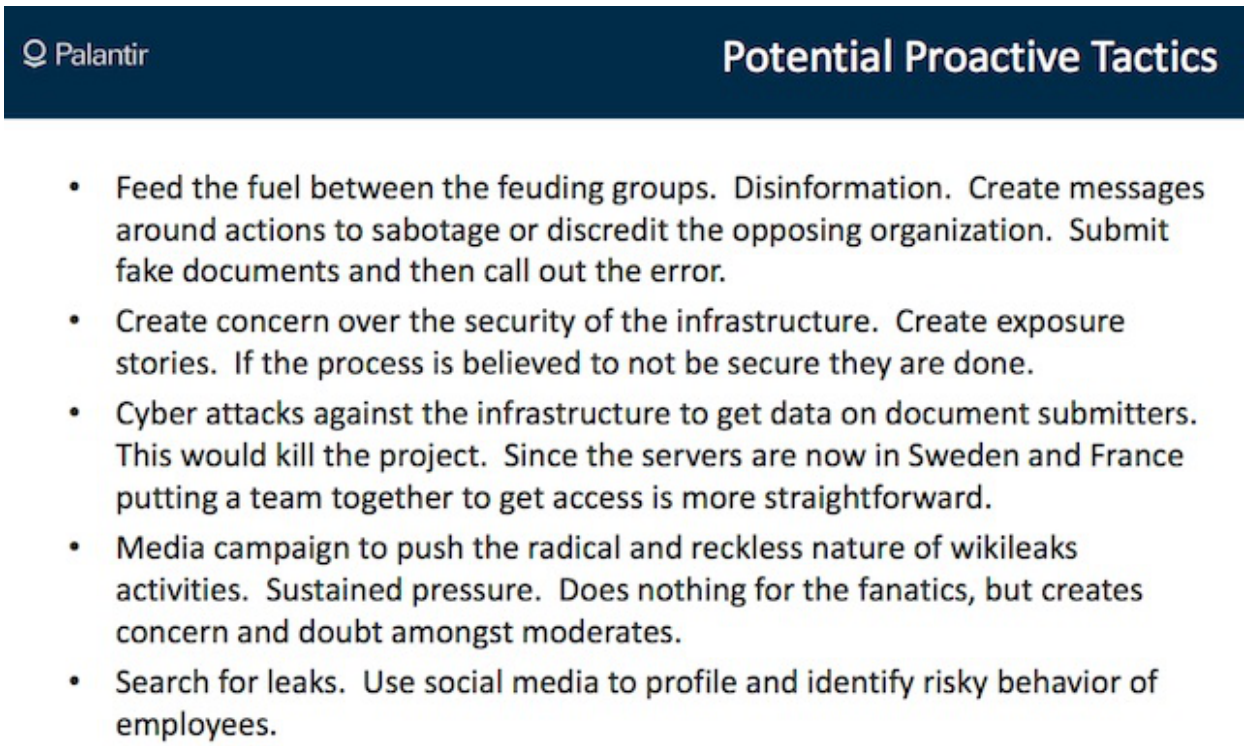
If he's right, the Anonymous attack, so far free of consequences, might end with some serious ones indeed.

Palantir

Those consequences have already been felt at the link analysis firm Palantir, based in Silicon Valley. The company was

part of "Team Themis," a group comprised of Palantir, Berico, and HBGary Federal, which got involved with the DC law firm Hunton & Williams. Hunton & Williams was looking for ways to help the US Chamber of Commerce, and later a major US bank, deal with troublesome opponents (pro-union websites and WikiLeaks, respectively.)

As a member of Team Themis, Palantir became part of Aaron Barr's plans to go after WikiLeaks, put pressure on commentators like Salon.com's Glenn Greenwald, and set up a surveillance cell for the Chamber of Commerce. No one in the e-mails that we saw objected to any of the proposed ideas.



Palantir adopting Barr's ideas about WikiLeaks

When news of the proposals came out, Palantir said it was horrified. Dr. Alex Karp, the company's CEO, issued a statement: "We make data integration software that is as useful for fighting food borne illness as it is to fighting fraud and terrorism. Palantir does not make software that has the capability to carry out the offensive tactics proposed by HBGary. Palantir never has and never will condone the sort of activities recommended by HBGary. As we have previously stated, Palantir has severed all ties with HBGary going forward."

As we noted in our initial report on the situation, several of the key ideas had come from Aaron Barr—but they were quickly adopted by other team members, including Palantir. I asked the company for more information on why Barr's ideas had shown up in Palantir-branded material. The company's general counsel, Matt Long, supplied the following answer:

> We did make a mistake—one of a fast growing company with lots of decentralized decision making authority. Initial results of our ongoing internal diagnostic show that a junior engineer allowed offensive material authored by HBGary to end up on a slide deck with Palantir's logo. The stolen emails conclusively show that Aaron Barr from HBGary authored the content which was collated well past midnight for an early morning presentation the next day. This doesn't excuse the incident, but hopefully it brings much needed context to a context-less email dump.

That junior engineer, a 26-year-old, has been put on leave while his actions are being reviewed.

"We should have cut ties with HBGary sooner and raised internal concerns about this sooner," Long told me. "This is a

huge mistake for sure; we aren't making excuses. But our company never approved hacking or carrying out dirty tricks on anyone."

As for the engineer's e-mail in which he said that the Team Themis project "got approval from Dr. Karp and the Board" on a new revenue sharing plan, Long said that it was simply "classic salesmanship ('I need to get my manager's permission for that. I really argued hard for you and got you this deal'). In our case we don't have sales people so it is very transparent/obvious coming from a 26-year-old engineer. Dr. Karp and the Board did not know about the specifics of the proposal—including pricing."

Berico

Berico, one of the three companies involved with Team Themis, initially promised a response to our questions about its handling of the situation. The company later changed its mind and declined to comment.

Berico did issue one public statement back on February 11, saying that it "does not condone or support any effort that proactively targets American firms, organizations or individuals. We find such actions reprehensible and are deeply committed to partnering with the best companies in our industry that share our core values. Therefore, we have discontinued all ties with HBGary Federal."

The company added that it was "conducting a thorough internal investigation to better understand the details of how this situation unfolded and we will take the appropriate actions within our company."

Aaron Barr

HBGary Federal was in the process of selling itself after the company couldn't meet revenue projections and had difficulty paying taxes and salaries. On January 19, Penny Leavy (the largest single investor in HBGary Federal) suggested in an e-mail to Aaron Barr that he give the two companies considering a purchase a set of deadlines. Under her projected scenario, the two firms would bid on February 4 and HBGary Federal would make a final decision on February 7. On February 6, Anonymous attacked.

What happened to Barr? Anonymous loudly and angrily demanded that Penny Leavy fire him, since his list of Anonymous names could allegedly have gotten "innocent people" into serious trouble. Leavy made clear that HBGary Federal was a separate company from HBGary, one in which she owned only a 15 percent stake, and that she couldn't simply "fire" the CEO.

Barr, too, had a stake in HBGary Federal. He couldn't just be fired—but he told Ars that he has taken a leave of absence from the company in order to focus on some other things.

When he finally regained control of his Twitter account last week, Barr's first new message since the attack said just about all there was left to say: "My deepest personal apology to all those that were negatively effected [sic] by the release of my e-mail into the public."