Unmasked

How Anonymous took on a computer security firm, spilled its secrets to the world, and got the attention of Congress - all to keep its own identities a secret.
Anonymous got lucky. When five of its hackers attacked security company HBGary Federal on February 6, 2011, they were doing so in order to defend the group’s privacy. It wasn’t because they hoped to reveal plans to attack WikiLeaks, create surveillance cells targeting pro-union organizations, and sell sophisticated rootkits to the US government for use as offensive cyber weapons—but that’s what they found.

In the weeks after the attack, the hackers released tens of thousands of e-mail messages and made headlines around the world. Aaron Bar, the CEO of HBGary Federal, eventually resigned; 12 Congressman called for an investigation; an ethics complaint was lodged against a major DC law firm involved with some of the more dubious plans.

Looked at from a certain angle, with one’s eyes squinted just right, the whole saga could look almost noble, a classic underdog story of rogue hackers taking on corporate and government power. On the flipside, however, the attacks caused big losses to several companies, leaked highly personal information about people’s lives, and resulted in a sustained (and fairly juvenile) attack on related security firm HBGary, Inc. And the irony was not lost on those who were attacked: Anonymous demanded transparency while offering none itself.

The many contradictions of the narrative perfectly sum up Anonymous, which claims to have no leaders, no real members, and no fixed ideology. It is whatever anyone wants it to be; start an operation, drum up enough interest from others, and you are operating under the Anonymous banner. Such an approach can lead to chaos, simultaneously providing a fertile breeding ground for ideas and an opening for total anarchy. It can also cause a rift between those who want to be digital Robin Hoods and those who are merely hacking “for the lulz.”

Few recent stories can shed so much light on a hacking movement, illuminate classified government contracting, reveal corporate bad behavior, raise doubts about the limits of Internet vigilante behavior, and show just how completely privacy has been obliterated in the digital age as the conflict between Anonymous and the two HBGarys.

That’s why Ars Technica poured so much time into researching and writing the complete narrative of the attacks and their aftermath, and it’s why we’re pleased to bring you the complete series now, packaged together for easy reading.
Anonymous to security firm working with FBI: “You’ve angered the hive”

By Jacqui Cheng

Internet vigilante group Anonymous turned its sights on security firm HBGary on Sunday evening in an attempt to “teach [HBGary] a lesson you’ll never forget.” The firm had been working with the Federal Bureau of Investigation (FBI) to unmask members of Anonymous following the group’s pro-WikiLeaks attacks on financial services companies, and was prepared to release its findings next week.

HBGary had been collecting information about Anonymous members after the group’s DDoS attacks on companies perceived to be anti-WikiLeaks. The firm had targeted a number of senior Anonymous members, including a US-based member going by the name of Owen, as well as another member known as Q. In addition to working with the FBI (for a fee, of course), HBGary’s CEO Aaron Barr was preparing to release the findings this month at a security conference in San Francisco.

Anonymous, however, felt that HBGary’s findings were “nonsense” and immediately retaliated—but this time with something other than a DDoS attack. Instead, Anonymous compromised the company’s website, gained access to the documents that HBGary had collected on its members, and published more than 60,000 of HBGary’s e-mails to BitTorrent. They also vandalized Barr’s Twitter and LinkedIn accounts with harsh messages and personal data about Barr, such as his social security number and home address.

“We’ve seen your internal documents, all of them, and do you know what we did? We laughed. Most of the information you’ve ‘extracted’ is publicly available via our IRC networks,” Anonymous wrote in a statement posted to HBGary’s site on Sunday. “So why can’t you sell this information to the FBI like you intended? Because we’re going to give it to them for free.”

HBGary cofounder and security researcher Greg Hoglund confirmed on Sunday evening that the latest attacks were sophisticated compared to the group’s past shenanigans. “They broke into one of HBGary’s servers that was used for tech support, and they got e-mails through compromising an insecure Web server at HBGary Federal,” Hoglund told KrebsonSecurity. “They used that to get the credentials for Aaron, who happened to be an administrator on our e-mail system, which is how they got into everything else. So it’s a case where the hackers break in on a non-important system, which is very common in hacking situations, and leveraged lateral movement to get onto systems of interest over time.”
As for the 60,000 e-mails that are now available to anyone with a torrent client, Hoglund argued that their publication was irresponsible and would cost HBGary millions of dollars in losses due to the exposure of proprietary information. “Before this, what these guys were doing was technically illegal, but it was in direct support of a government whistle blower. But now, we have a situation where they’re committing a federal crime, stealing private data and posting it on a torrent,” Hoglund said.

It’s unlikely that Anonymous cares about what Hoglund thinks, though. Several of the company’s e-mails indicated that Barr was looking for ways to spin its info about Anonymous as a pro-HBGary PR move, which Anonymous took special issue with. The group warned HBGary that it had “charged into the Anonymous hive” and now the company is “being stung.”

“It would appear that security experts are not expertly secured,” Anonymous wrote.
Aaron Barr believed he had penetrated Anonymous. The loose hacker collective had been responsible for everything from anti-Scientology protests to pro-Wikileaks attacks on MasterCard and Visa, and the FBI was now after them. But matching their online identities to real-world names and locations proved daunting. Barr found a way to crack the code.

In a private e-mail to a colleague at his security firm HBGary Federal, which sells digital tools to the US government, the CEO bragged about his research project.

“They think I have nothing but a hierarchy based on IRC [Internet Relay Chat] aliases!” he wrote. “As 1337 as these guys are supposed to be they don’t get it. I have pwned them! :)

But had he?

“We are kind of pissed at him right now”
Barr’s “pwning” meant finding out the names and addresses of the top Anonymous leadership. While the group claimed to be headless, Barr believed this to be a lie; indeed, he told others that Anonymous was a tiny group.

“At any given time there are probably no more than 20-40 people active, accept during heightened points of activity like Egypt and Tunisia where the numbers swell but mostly by trolls,” he wrote in an internal e-mail. (All e-mails in this investigative report are provided verbatim, typos and all.) “Most of the people in the IRC channel are zombies to inflate the numbers.”

The show was run by a couple of admins he identified as “Q,” “Owen,” and “CommanderX”—and Barr had used social media data and subterfuge to map those names to three real people, two in California and one in New York.

Near the end of January, Barr began publicizing his information, though without divulging the names of the Anonymous admins. When the Financial Times picked up the story and ran a piece on it on February 4, it wasn’t long before Barr got what he wanted—contacts from the FBI, the Director of National Intelligence, and the US military. The FBI had been after Anonymous for some time, recently kicking in doors while executing 40 search warrants against group members.

Confident in his abilities, Barr told one of the programmers who helped him on the project, “You just need to program as good as I analyze.”

But on February 5, one day after the Financial Times article and six days before Barr’s sit-down with the FBI, Anonymous did some “pwning” of its own. “Ddos!!! Fckers,” Barr sent from his iPhone as a distributed denial of service attack hit his corporate network. He then pledged to “take the gloves off.”

When the liberal blog Daily Kos ran a story on Barr’s work later that day, some Anonymous users commented on it. Barr sent out an e-mail to colleagues, and he was getting worked up: “They think all I know is their irc names!!!! I know their real fing names. Karen [HBGary Federal’s public relations head] I need u to help moderate me because I am getting angry. I am planning on releasing a few names of folks that were already arrested. This battle between us will help spur publicity anyway.”

Indeed, publicity was the plan. Barr hoped his research would “start a verbal braul between us and keep it going because that will bring more media and more attention to a very important topic.”
But within a day, Anonymous had managed to infiltrate HBGary Federal’s website and take it down, replacing it with a **pro-Anonymous message** (“now the Anonymous hand is bitch-slapping you in the face.”) Anonymous got into HBGary Federal’s e-mail server, for which Barr was the admin, and compromised it, extracting over 40,000 e-mails and putting them up on The Pirate Bay, all after watching his communications for 30 hours, undetected. In an after-action IRC chat, Anonymous members bragged about how they had gone even further, deleting 1TB of HBGary backup data.

They even claimed to have wiped Barr’s iPad remotely.

The situation got so bad for the security company that HBGary, the company which partially owns HBGary Federal, sent its president Penny Leavy into the Anonymous IRC chat rooms to swim with the sharks—and to beg them to leave her company alone. (Read the [bizarre chat log](#).) Instead, Anonymous suggested that, to avoid more problems, Leavy should fire Barr and “take your investment in aaron’s company and donate it to BRADLEY MANNINGS DEFENCE FUND.” Barr should cough off up a personal contribution, too; say, one month’s salary?

As for Barr’s “pwning,” Leavy couldn’t backtrack from it fast enough. “We have not seen the list [of Anonymous admins] and we are kind of pissed at him right now.”

Were Barr’s vaunted names even correct? Anonymous insisted repeatedly that they were not. As one admin put it in the IRC chat with Leavy, “Did you also know that aaron was peddling fake/wrong/false information leading to the potential arrest of innocent people?” The group then made that information public, claiming that it was all ridiculous.

Thanks to the leaked e-mails, we now have the full story of how Barr infiltrated Anonymous, used social media to compile his lists, and even resorted to attacks on the codebase of the Low Orbit Ion Cannon—and how others at his own company warned him about the pitfalls of his research.

---

**“I will sell it”**

Barr had been interested in social media for quite some time, believing that the links it showed between people had enormous value when it came to mapping networks of hackers—and when hackers wanted to target their victims. He presented a talk to a closed Department of Justice conference earlier this year on “specific techniques that can be
used to target, collect, and exploit targets with laser focus and with 100 percent success” through social media.

His curiosity about teasing out the webs of connections between people grew. By scraping sites like Facebook or LinkedIn, Barr believed he could draw strong conclusions, such as determining which town someone lived in even if they didn’t provide that information. How? By looking at their friends.

“The next step would be ok we have 24 people that list Auburn, NY as their hometown,” he wrote to the programmer implementing his directives. “There are 60 other people that list over 5 of those 24 as friends. That immediately tells me that at a minimum those 60 can be tagged as having a hometown as Auburn, NY. The more the data matures the more things we can do with it.”

The same went for hackers, whose family and friends might provide information that even the most carefully guarded Anonymous member could not conceal. “Hackers may not list the data, but hackers are people too so they associate with friends and family,” Barr said. “Those friends and family can provide key indicators on the hacker without them releasing it…”

His programmer had doubts, saying that the scraping and linking work he was doing was of limited value and had no commercial prospects. As he wrote in an e-mail:

Step 1 : Gather all the data
Step 2 : ???
Step 3 : Profit

But Barr was confident. “I will sell it,” he wrote.

To further test his ideas and to drum up interest in them, Barr proposed a talk at the BSides security conference in San Francisco, which takes place February 14 and 15. Barr’s talk was titled “Who Needs NSA when we have Social Media?” and his plan to draw publicity involved a fateful decision: he would infiltrate and expose Anonymous, which he believed was strongly linked to WikiLeaks.

“I am going to focus on outing the major players of the anonymous group I think,” he wrote. “Afterall - no secrets right? :) We will see how far I get. I may focus on NSA a bit to just so I can give all those freespeech nutjobs something… I just called people advocating freespeech, nutjobs - I threw up in my mouth a little.”

With that, the game was afoot.

“I enjoy the LULZ”

Barr created multiple aliases and began logging on to Anonymous IRC chat rooms to figure out how the group worked. He worked to link these IRC handles to real people, in part using his social networking expertise, and he created fake Twitter accounts and Facebook profiles. He began communicating with those he believed were leaders.

After weeks of this work, he reported back to his colleagues on how he planned to use his fake personas to drum up interest in his upcoming talk.

I have developed a persona that is well accepted within their groups and want to use this and my real persona against eachother to build up press for the talk. Pre-talk plan.

I am going to tell a few key leaders under my persona, that I have been given information that a so called cyber security expert named Aaron Barr will be briefing the power of social media analysis and as part of the talk with be dissecting the Anonymous group as well as some critical infrastructure and government organizations

I will prepare a press sheet for Karen to give to Darkreading a few days after I tell these folks under persona to legitimize the accusation. This will generate a big discussion in Anonymous chat channels, which are attended by the press. This will then generate press about the talk, hopefully driving more people and more business to us.

Barr then contacted another security company that specializes in botnet research. He suspected that top Anonymous admins like CommanderX had access to serious Internet firepower, and that this probably came through control of bots on compromised computers around the world.

Barr asked if the researchers could “search their database for specific targets (like the one below) during an
operational window (date/time span) to see if any botnet(s) are participating in attacks? Below is an attack which is currently ongoing.” (The attack in question was part of Anonymous’ “Operation Payback” campaign and was targeted at the government of Venezuela.)

The report that came back focused on the Low Orbit Ion Cannon, a tool originally coded by a private security firm in order to test website defenses. The code was open-sourced and then abandoned, but someone later dusted it off and added “hivemind mode” that let LOIC users “opt in” to centralized control of the tool. With hundreds or thousands of machines running the stress-test tool at once, even major sites could be dropped quickly. (The company recorded only 1,200 machines going after MasterCard on December 11, for instance.)

To boost the credibility of his online aliases, Barr then resorted to a ruse. He asked his coder to grab the LOIC source code. “I want to add some code to it,” Barr said. “I don’t want to distribute that, it will be found and then my persona will be called out. I want to add it, distribute it under a persona to burn and then have my other persona call out the code.”

The code to be added was an HTTP beacon that linked to a free website Barr had set up on Blogspot. He wanted a copy of the altered source and a compiled executable. His programmer, fearing Anonymous, balked.

On January 20, the coder wrote back, “I’m not compiling that shit on my box!” He even refused to grab a copy of the source code from message boards or other IRC users, because “I ain’t touchin’ any of that shit as those are already monitored.”

“Dude,” responded Barr. “Anonymous is a reckless organization. C’mon I know u and I both understand and believe generally in their principles but they are not a focused and considerate group, the[y] attack at will and do not care of their effects. Do u actually like this group?”

The coder said he didn’t support all they did, but that Anonymous had its moments. Besides, “I enjoy the LULZ.”

“Dude—who’s evil?”

At one time, Barr supported WikiLeaks. When the site released its (edited) “Collateral Murder” video of a US gunship killing Reuters photographers in Iraq, Barr was on board. But when WikiLeaks released its huge cache of US diplomatic cables, Barr came to believe “they are a menace,” and that when Anonymous sprang to the defense of WikiLeaks, it wasn’t merely out of principle. It was about power.

“When they took down MasterCard do u think they thought alright win one for the small guy!” he asked. “The first thought through most of their malcontented minds was a rush of power. That’s not ideals.”

He continued in this philosophical vein:

But dude whos evil?

US Gov? Wikileaks? Anonymous?

Its all about power. The Wikileaks and Anonymous guys think they are doing the people justice by without much investigation or education exposing information or targeting organizations? BS. Its about trying to take power from others and give it to themeselves.
I follow one law.

Mine.

His coder asked Barr how he slept at night, “you military industrial machine capitalist.”

“I sleep great,” Barr responded. “Of course I do indoor [enjoy?] the money and some sense of purpose. But I can get purpose a lot of places, few of which pay this salary.”

The comments are over the top, of course. Elsewhere, Barr gets more serious. “I really dislike corporations,” he says. “They suck the lifeblood out of humanity. But they are also necessary and keep us moving, in what direction I don’t know.

“Governments and corporations should have a right to protect secrets, sensitive information that could be damage to their operations. I think these groups are also saying this should be free game as well and I disagree. Hence the 250,000 cables. Which was bullshit… Society needs some people in the know and some people not. These folks, these sheep believe that all information should be accessible. BS. And if they truly believe it then they should have no problem with me gathering information for public distribution.”

But Anonymous had a bit of a problem with that.

The hunter and the hunted

As Barr wrapped up his research and wrote his conference presentation, he believed he had unmasked 80-90 percent of the Anonymous leadership—and he had done it all using publicly available information.

“They are relying on IP for anonymity,” he wrote in a draft of his presentation. “That is irrelevant with social media users. U use IRC and FB and Twitter and Forums and Blogs regularly… hiding UR IP doesn’t matter.”

Barr would do things like correlate timestamps; a user in IRC would post something, and then a Twitter post on the same topic might appear a second later. Find a few of these links and you might conclude that the IRC user and the Twitter user were the same person.

Even if the content differed, what if you could correlate the times that someone was on IRC with the times a Facebook user was posting to his wall? “If you friend enough people you might be able to correlate people logging into chat with people logging into Facebook,” Barr wrote.

The document contained a list of key IRC chatrooms and Twitter accounts. Facebook groups were included, as were websites. But then Barr started naming names. His notes are full of comments on Anonymous members. “Switch” is a “real asshole but knows what he’s talking about,” while “unbeliever” might be “alexander [last name redacted].”

In the end, Barr determined that three people were most important. A figure called Q was the “founder and runs the IRC. He is indeed in California, as are many of the senior leadership of the group.” Another person called Owen is “almost a co-founder, lives in NY with family that are also active in the group, including slenaid and rabbit (nicks).” Finally, CommanderX can “manage some significant firepower.” Barr believed he had matched real names to each of these three individuals.

He wasn’t doing it to actually expose the names, though. “My intent is not to do this work to put people in jail,” Barr wrote to others in the company. “My intent is to clearly demonstrate how this can be effectively used to gather significant intelligence and potentially exploit targets of interest (the other customers will read between the lines).”

He then revealed himself on Facebook to the person he believed was CommanderX. “I am not going to release names,” Barr said on February 5, using the alias Julian Goodspeak. “I am merely doing security research to prove the vulnerability of social media.” He asked for Anonymous to call off its DDoS attack on HBGary Federal, an attack that had begun earlier that day.
Some of the responses from CommanderX were a bit chilling. Late in the conversation, CommanderX warned Barr “that your vulnerabilities are far more material. One look at your website locates all of your facilities. You might want to do something about that. Just being friendly. I hope you are being paid well.”

Then came an IRC log that Barr sent around, in which a user named Topiary tried to recruit him (under the name CogAnon) for “a new operation in the Washington area” where HBGary Federal has its headquarters. The target is “a security company.”

By late afternoon on the 5th, Barr was angry and perhaps a little scared, and he asked his PR person to “help moderate me because I am getting angry. I am planning on releasing a few names of folks that were already arrested.” It’s not clear that Barr ever did this, however; he admitted in another e-mail that he could get a bit “hot” in private, though he would generally cool down before going public.

Hours later, the attack escalated from some odd DDoS traffic to a full-scale break-in of HBGary Federal systems, one that showed tremendous skill. “What amazes me is, for a security company - you had such a basic SQL vulnerability on your website,” wrote one Anonymous member later.

Days afterward, the company has still not managed to restore its complete website.

**“Danger, Will Robinson!”**

Throughout Barr’s research, though, the coder he worked with worried about the relevance of what was being revealed. Barr talked up the superiority of his “analysis” work, but doubts remained. An email exchange between the two on January 19 is instructive:

**Barr:** [I want to] check a persons friends list against the people that have liked or joined a particular group.
Coder: No it won’t. It will tell you how mindless their friends are at clicking stupid shit that comes up on a friends page, especially when they first join facebook.

Barr: What? Yes it will. I am running through analysis on the anonymous group right now and it definitely would.

Coder: You keep assuming you’re right, and basing that assumption off of guilt by association.

Barr: Noooo….its about probability based on frequency…c’mon ur way smarter at math than me.

Coder: Right, which is why i know your numbers are too small to draw the conclusion but you don’t want to accept it. Your probability based on frequency right now is a gut feeling. Gut feelings are usually wrong.

Barr: [redacted]

Coder: [some information redacted] Yeah, your gut feelings are awesome! Plus, scientifically proven that gut feelings are wrong by real scientist types.

Barr: [some information redacted] On the gut feeling thing…dude I don’t just go by gut feeling…I spend hours doing analysis and come to conclusions that I know can be automated…so put the taco down and get to work!

Coder: I’m not doubting that you’re doing analysis. I’m doubting that statistically that analysis has any mathematical weight to back it. I put it at less than .1% chance that it’s right. You’re still working off of the idea that the data is accurate. mmmm…..taco!

Later, when Barr talks about some “advanced analytical techniques” he’s been pondering for use on the Anonymous data, the coder replies with apparent frustration, “You keep saying things about statistics and analytics but you haven’t given me one algorithm or SQL query statement.”

Privately, the coder then went to another company official with a warning. “He’s on a bad path. He’s talking about his analytics and that he can prove things statistically but he hasn’t proven anything mathematically nor has he had any of his data vetted for accuracy, yet he keeps briefing people and giving interviews. It’s irresponsible to make claims/accusations based off of a guess from his best gut feeling when he has even told me that he believes his gut, but more often than not it’s been proven wrong. I feel his arrogance is catching up to him again and that has never ended well…for any of us.”

Others made similar dark warnings. “I don’t really want to get DDOS’d, so assuming we do get DDOS’d then what? How do we make lemonade from that?” one executive asked Barr. The public relations exec warned Barr not to start dropping real names: “Take the emotion out of it -> focus on the purpose. I don’t see benefit to you or company to tell them you have their real names — published or not.”

Another internal warning ended: “Danger Will Robinson. You could end up accusing a wrong person. Or you could further enrage the group. Or you could be wrong, and it blows up in your face, and HBGary’s face, publicly.”

“Quite simply, nonsense”

But Barr got his Financial Times story, and with it the publicity he sought. He also made clear that he had the real names, and Anonymous knew he would soon meet with the FBI. Though Barr apparently planned to keep his names and addresses private even at this meeting, it was easy to see why Anonymous would have doubts.

When HBGary President Penny Leavy, who was an investor in separate company HBGary Federal, waded into IRC to reason with Anonymous, she pleaded ignorance of Barr’s activities and said that they were “for security research only; the article was to get more people to the [BSides] event.” To which someone responded, “Penny: if what you are saying is true [true] then why is Aaron meeting with the FBI tomorrow morning at 11am? PLEASE KEEP IN MIND WE HAVE ALL YOUR EMAILS.” (The answer from the e-mails is that Barr was trying to drum up business with the feds, not necessarily take down Anonymous.)

As for the names in Barr’s BSides presentation, Anonymous insisted that they were wrong. “Penny please note that the names in that file belong to innocent random people on facebook. none of which are related to us at all,” said one admin.

Another user complained to Leavy that “the document that [Barr] had produced actually has my girlfriend in it. She has never done anything with anonymous, not once. I had used her computer a couple times to look at a group on
facebook or something.”

In the note posted on HBGary Federal’s website when it was taken over, Anonymous blasted Barr’s work. “You think you’ve gathered full names and addresses of the ‘higher-ups’ of Anonymous? You haven’t. You think Anonymous has a founder and various co-founders? False…. We laughed. Most of the information you’ve ‘extracted’ is publicly available via our IRC networks. The personal details of Anonymous ‘members’ you think you’ve acquired are, quite simply, nonsense.”

Oh—and remember the threatening IRC log above, the one “recruiting” Barr to attack a DC security company? Anonymous says that it was all a joke.

“I mean come on, Penny,” wrote Topiary in an IRC chat, “I messaged Aaron in PM [private message] and told him about a ‘secret’ Washington OP, then he emailed the company (including you) being entirely confident that we were directly threatening you, and he thought we didn’t know who he was.

“He seriously works at a security company?”

**Never forgive, never forget**

Anonymous doesn’t like to let up. Barr’s Twitter account remains compromised, sprinkled with profane taunts. The HBGary websites remain down. The e-mails of three key players were leaked via BitTorrent, stuffed as they were with nondisclosure agreements, confidential documents, salary numbers, and other sensitive data that had nothing to do with Anonymous.

And they have more information—such as the e-mails of Greg Hoglund, Leavy’s husband and the operator of rootkit.org (which was also taken down by the group).

When Leavy showed up to plead her case, asking Anonymous to at least stop distributing the e-mails, the hivemind reveled in its power over Leavy and her company, resorting eventually to tough demands against Barr.

“Simple: fire Aaron, have him admit defeat in a public statement,” said Topiary, when asked what the group wanted. “We won’t bother you further after this, but what we’ve done can’t be taken back. Realize that, and for the company’s sake, dispose of Aaron.”

Others demanded an immediate “burn notice” on Barr and donations to Bradley Manning, the young military
member now in solitary confinement on suspicion of leaking classified documents to Wikileaks.

The hack unfolded at the worst possible time for HBGary Federal. The company was trying to sell, hopefully for around $2 million, but the two best potential buyers started to drag their heels. “They want to see delivery on pipeline before paying those prices,” Leavy wrote to Barr. “So initial payout is going to be lower with both companies I am talking with. That said our pipeline continues to drag out as customers are in no hurry to get things done quickly so if we dont sell soon and our customers dont come through soon we are going to have cash flow issues.”

And being blasted off the ‘Net by Anonymous is practically the last thing a company in such a situation needs. After the attacks, Leavy told the Financial Times that they cost HBGary millions of dollars.

“I wish it had been handled differently,” she added.

“The Internet is here”

And who were Barr and his company up against in all this? According to Anonymous, a five-member team took down HBGary Federal and rootkit.com, in part through the very sort of social engineering Barr had tried to employ against Anonymous.

One of those five was allegedly a 16-year old girl, who “social engineered your admin jussi and got root to rootkit.com,” one Anonymous member explained in IRC.

Another, pleased with power, harassed Penny Leavy and her husband, who sat beside her during the chat: “How does it feel to get hacked by a 16yr old girl?” One can almost hear the taunt echoing from some kind of grade school playground.

The attackers are quintessentially Anonymous: young, technically sophisticated, brash, and crassly juvenile, all at the same time. And it’s getting ever more difficult to dismiss Anonymous’ hacker activity as the harmless result of a few mask-wearing buffoons.

Perhaps the entire strange story can be best summed up by a single picture, one that Barr e-mailed to two of his colleagues back on January 28. “Oh fuck,” it says beneath a picture of an Anonymous real-world protest. “The Internet is here.”

![Image of Anonymous protest with text: “OH FUCK” and “The internet is here.”]
(Virtually) face to face: how Aaron Barr revealed himself to Anonymous

By Nate Anderson

Aaron Barr, CEO of security company HBGary Federal, spent the month of January trying to uncover the real identities of the hacker collective Anonymous—only to end with his company website knocked offline, his e-mails stolen, 1TB of backups deleted, and his personal iPad wiped when Anonymous found out.

Our lengthy investigation of that story generated such interest that we wanted to flesh out one compelling facet of the story in even more detail. In a sea of technical jargon, social media analysis, and digital detective work, it stands out as a truly human moment, when Barr revealed himself to Anonymous and dialogued directly with senior leaders and “members” of the group.

The encounter began on February 5. Barr had managed to get his work written up in a Financial Times story the day before, and now strange traffic was pouring in to HBGary Federal. With his research done and his story in print, Barr needed only to work up some conference slides and prepare for a meeting with the FBI, which had been tracking Anonymous for some time. So Barr ditched the covert identities he had been using to watch the group, and on February 5 he approached a person on Facebook whom he believed was the powerful CommanderX.

Barr’s apparent motives were multiple: to mitigate any revenge upon his company, but also to meet as equals with his hacker subjects. No harm, no foul, right? Anonymous didn’t agree. (Quotes in this article are provided verbatim, typos and all.)

Barr: CommanderX. This is my research… I am not going to release names I am merely doing security research to prove the vulnerability of social media so please tell [redacted] and [redacted] or whoever else is hitting our site to stop.

CommanderX: Uhhh…. not my doing! Just as a thought… wouldn’t that be valuable data to your research?

Barr: I am done with my research…doing my slides… I am not out to gut u guys. My focus is on social media vulnerabilities only. So please tell the folks there that I am not out to get u guys… I knew you guys were a risky target but nothing risked nothing gained. People can show their bravado thats fine I can deal with that. Just want the ‘leadership’ to know what my intent is…that will filter as it needs to I am sure.

CommanderX: ‘Leadership’ lmao [laughing my ass off] it has grown beyond my control, just as I intended.
Barr: … I will talk about aliases. I won’t talk about names. But please don’t play me a chump any more than you have to to protect anons cred. I know more than IRC aliases…. u have a lot of firepower and know how in some dark corners…hell some of them may even know Greg Hoglund the CEO of our other company. So if it is some of your guys just want to make sure they don’t get too aggressive.

CommanderX: Which website?

Barr: hbgaryfederal.com

CommanderX: … I warn you that your vulnerabilities are far more material. One look at your website locates all of your facilities. You might want to do something about that. Just being friendly. I hope you are being paid well.

“Come at us, bro”

Barr then entered an Anonymous IRC chat room, where his “CogAnon” profile had already been exposed. When he showed up, this is what greeted him. (Anonymous handles have been altered in this non-public section of chat.)

[23:47] <CogAnon> guys I’ll tell you...it was only research...it has now become a criminal matter...

[23:48] <CogAnon> our website was hacked...twitter account... email.... ok...guys if thats the way u want to play it.

[23:48] <ANON2> CogAnon: come at us bro

[23:48] <CogAnon> I won’t...


[23:48] <ANON2> CogAnon: nice screencap earlier by the way, did Ted and [HBGary CEO] Penny enjoy it, faggot?

[23:49] <CogAnon> not sure why u had to make it personal...I had 2 other usecases...

[23:49] <CogAnon> but ok... I figured this might happen...I am not upset... it just takes a differnt path...

[23:51] <CogAnon> ok see you guys later...not even close to end of career... :) need to finish my talk.

[23:52] <ANON2> maybe CogAnon will enjoy what’s uploading right now

[00:18] * CogAnon is now known as AaronBarr

The material “uploading right now” was apparently Barr’s private e-mails; Anonymous had infiltrated his company e-mail server, where Barr was the admin, and had taken more than 40,000 messages from three top execs. They were then uploaded to The Pirate Bay.

“What’s coming next is the delicious cake”

The next day, February 6, the attacks turned serious, and Barr realized the extent of what Anonymous had done to him and to his company, which was currently in negotiations to sell itself to a pair of interested buyers. This was no longer a game; it looked more like war. The sheer freewheeling raucousness of what follows illustrates as well as anything the nature of Anonymous, and it’s worth quoting at length. (A few unimportant bits have been stripped for clarity, denoted by an ellipsis.)

Note that several members of the channel have already seen Barr’s e-mails. (Read the full public log.)

[23:53:49] <q> Ohai CogAnon

[23:53:56] <tflow> Hello, Mr. Barr.

[23:54:12] <Topiary> Mr. Barr and his infiltration of Anonymous; “Now they’re threatening us directly”, amirite?

[23:54:16] <tflow> I apologize for what’s about to happen to you and your company.

[23:54:20] <q> Enjoying the Superbowl, I hope?

[23:54:25] <CogAnon> high one sec. please
I really do, Mr. Barr.
You have no idea what's coming next.
CogAnon is clearly super 1337 with his PM psyops skills in the Washington area.
ok...sure I figured something like this might happen.
nah, you won't like what's coming next.
Can you guess what's coming next?
Ooh, a fun game - guess!
dude...you just don't get it. it was research on social media vulnerabilities...I was never going to release the names...
as I told CommanderX last night.
You went to press.
yeah we read the facebook conversation, and every other conversation.
With info that was largely false.
only that your research like totally failed and all your info was bullshit.
CogAnon: that article was a hit peice.
ok whatever...whoever has done this has tied my hands now though.
I suggest you go to Bloomberg and explain.
Don't you have a meeting with the FBI Monday morning?
yep...they called me.
we'll send that to your FBI friends, so they have that before your talk tomorrow.
yep...they called me.
Moral of the Story: Don't drum up business by banging on a hornet's nest.
I have a lot of people calling me.
You intended of battling anonymous in the media for media gain and attention.
well let me ask you.
you got the media attention now.
how does it feel?
?
Yep.
Oh guys, what's coming next is the delicious cake.
…

[23:58:53] <nigg> so who wants all of
[23:58:55] <nigg> his emails?
[23:59:06] <Sabu> uhm you have his emails????
[23:59:10] <Sabu> DAMN!
[23:59:14] <nigg> 2.3gb’s of gold
[23:59:15] <Topiary> sure, I’d enjoy some 68,000 emails
[23:59:19] <Topiary> can we please have 68,000 of their emails?
[23:59:21] <blergh> lol
[23:59:21] <`k> nigg not ehre
[23:59:22] <tflow> I already have them
[23:59:23] <blergh> what is this?
[23:59:25] <c0s> those emails are going to be pretty
[23:59:25] <Topiary> oh wait we totally already have them
[23:59:26] <`k> here
[23:59:27] <nigg> 68,000?
[23:59:27] <Topiary> trolololol
[23:59:50] <tflow> I have Barr’s, Ted’s and Phil’s emails
[23:59:50] <nigg> im talking
[23:59:50] <CogAnon> lol..ok guys well u got me right. :)

On February 7, Barr’s compromised Twitter account contained the following posts, which appear to be from Barr himself—though it’s hard to say. (Those from his Anonymous persecutors have a very different tone, and contain more links and profanity.)

Ok. Well this has been fun. Anon has certainly done a number on me for the last, wow has it only been 24hrs? Seems longer...

site defaced, twitter hacked, email taken...priceless.

Does this mean I have become an internet celebrity...not quite how I imagined it?

ok. So Anon has done a number on me. Probably going to take a bit to piece things together, probably more to come.

But there has been no more to come. Twitter has now locked the account, according to Anonymous.

The persecution was brutal. People began defacing images of Barr, hosting them all in a central repository for easy viewing—they even dredged up a personal picture of the man dressed as The Hulk for a round of trick-or-treating with his kid. HBGary, a part owner of HBGary Federal, sent its own President Penny Leavy into the Anonymous chat rooms to ask them to stop—or at least to keep the e-mails private. Anonymous did not, demanding instead Barr’s resignation.

Members of the group have spent today apparently prepping to release a new e-mail archive from Leavy’s husband, the respected security pro Greg Hoglund, whose own site rootkit.com was compromised by (allegedly) a 16-year-old through a bit of social engineering. The persecution continues.
Spy games: Inside the convoluted plot to bring down WikiLeaks

By Nate Anderson

When Aaron Barr was finalizing a recent computer security presentation for the US Transportation Security Administration, a colleague had a bit of good-natured advice for him: “Scare the sh*t out of them!”

In retrospect, this may not have been the advice Barr needed. As CEO of the government-focused infosec company HBGary Federal, Barr had to bring in big clients—and quickly—as the startup business hemorrhaged cash. To do so, he had no problem with trying to “scare the sh*t out of them.” When working with a major DC law firm in late 2010 on a potential deal involving social media, for instance, Barr decided that scraping Facebook to stalk a key partner and his family might be a good idea. When he sent his law firm contact a note filled with personal information about the partner, his wife, her family, and her photography business, the result was immediate.

“Thanks. I am not sure I will share what you sent last night—he might freak out.”

This rather creepy behavior became common; Barr used it as a sign of his social media prowess. Another target of his investigations went to “a Jewish Church in DC, the Temple Micah.” Someone else “married @ the Inn at Perry Cabin in St. Michaels, MD (non-denominational ceremony).” Barr was even willing to helpfully guesstimate the ages of children in photographs (“they have 2 kids, son and daughter look to be 7 and 4”).
With one potential client, Barr sifted the man’s social media data and then noted that “I am tempted to create a person from his highschool and send him a request, but that might be overstepping it.”

As the money ran out on HBGary Federal, Barr increasingly had no problem “overstepping it.” In November, when a major US bank wanted a strategy for taking down WikiLeaks, Barr immediately drafted a presentation in which he suggested “cyber attacks against the infrastructure to get data on document submitters. This would kill the project. Since the servers are now in Sweden and France, putting a team together to get access is more straightforward.”

Faking documents seemed like a good idea, too, documents which could later be “called out” so as to make WikiLeaks look unreliable.

And Barr wanted to go further, pushing on people like civil liberties Salon.com columnist Glenn Greenwald—apparently hoping to threaten their livelihoods. “These are established professionals that have a liberal bent, but ultimately most of them if pushed will choose professional preservation over cause, such is the mentality of most business professionals,” he wrote. “Without the support of people like Glenn WikiLeaks would fold.”
When the US Chamber of Commerce wanted to look into some of its opponents, Barr teamed with two other security companies and went nuts, proposing that the Chamber create an absurdly expensive “fusion cell” of the kind “developed and utilized by Joint Special Operations Command (JSOC)”—and costing $2 million a month. And if the fusion cell couldn’t turn up enough opposition research, the security firms would be happy to create honeypot websites to lure the Chamber’s union-loving opponents in order to grab more data from them.

The security companies even began grabbing tweets from liberal activists and mapping the connections between people using advanced link analysis software most often used by the intelligence community. (Some of the Chamber material was unearthed by ThinkProgress and other liberal bloggers, while The Tech Herald and Crowleaks.org first wrote about the proposed WikiLeaks attacks.)

While waiting to see if his proposals would result in work for HBGary Federal, Barr turned in January to unmask the leadership of the hacker collective Anonymous. This part of the story is well known by now (read our investigative feature): when Barr went public with his findings, Anonymous took down his website, stole his e-mails, deleted the company’s backup data, trashed Barr’s Twitter account, and remotely wiped his iPad.

In the days since the attack and the publication of Barr’s e-mails, his partners at other security firms threw him under the bus. “I have directed the company to sever any and all contacts with HB Gary,” said the CEO of Palantir.

Berico Technologies, another private security firm, said 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.”

Glenn Greenwald unleashed both barrels of his own, claiming that “what is set forth in these proposal... quite possibly constitutes serious crimes. Manufacturing and submitting fake documents with the intent they be published likely constitutes forgery and fraud. Threatening the careers of journalists and activists in order to force them to be silent is possibly extortion and, depending on the specific means to be used, constitutes other crimes as well. Attacking WikiLeaks’ computer infrastructure in an attempt to compromise their sources undoubtedly violates numerous cyber laws.”

How did Barr, a man with long experience in security and intelligence, come to spend his days as a CEO e-stalking clients and their wives on Facebook? Why did he start performing “reconnaissance” on the largest nuclear power company in the US? Why did he suggest pressuring corporate critics to shut up, even as he privately insisted that corporations “suck the lifeblood out of humanity”? And why did he launch his ill-fated investigation into Anonymous, one which may well have destroyed his company and damaged his career?

Thanks to his leaked e-mails, the downward spiral is easy enough to retrace. Barr was under tremendous pressure to bring in cash, pressure which began on November 23, 2009.

“A” players attract “A” players

That’s when Barr started the CEO job at HBGary Federal. Its parent company, the security firm HBGary, wanted a separate firm to handle government work and the clearances that went with it, and Barr was brought in from Northrup Grumman to launch the operation.

In an e-mail announcing Barr’s move, HBGary CEO Greg Hoglund told his company that “these two are A+ players in the DoD contracting space and are able to ‘walk the halls’ in customer spaces. Some very big players made offers to Ted and Aaron last week, and instead they chose HBGary. This reflects extremely well on our company. ‘A’ players attract ‘A’ players.”

Barr at first loved the job. In December, he sent an e-mail at 1:30am; it was the “3rd night in a row I have woken up in the middle of the night and can’t sleep because my mind is racing. It’s nice to be excited about work, but I need some sleep.”

Barr had a huge list of contacts, but turning those contacts into contracts for government work with a fledgling company proved challenging. Less than a year into the job, HBGary Federal looked like it might go bust.

On October 3, 2010, HBGary CEO Greg Hoglund told Aaron that “we should have a pow-wow about the future of HBGary Federal. [HBGary President] Penny and I both agree that it hasn’t really been a success... You guys are basically out of money and none of the work you had planned has come in.”
Aaron agreed. “This has not worked out as any of us have planned to date and we are nearly out of money,” he said.

While he worked on government contracts, Barr drummed up a little business doing social media training for corporations using, in one of his slides, a bit of research into one Steven Paul Jobs.

The training sessions, following the old “scare the sh*t out of them” approach, showed people just how simple it was to dredge up personal information by correlating data from Facebook, LinkedIn, Twitter, and more. At $1,000 per person, the training could pull in tens of thousands of dollars a day, but it was sporadic. More was needed; contracts were needed, preferably multi-year ones.

The parent company also had issues. A few weeks after the discussions about closing up HBGary Federal, HBGary President Penny Leavy-Hoglund (Greg’s wife), sent an e-mail to her sales team, telling them “to work a quota and to bring in revenue in a timely manner. It’s not ‘optional’ as to when it needs to close, if you haven’t met your number,
the closing needs to happen now, not later. You need to live, eat, breath and ensure you meet your number, not kind of hit it, MEET IT... Guys, no one is making their quota.”

She concluded darkly, “I have some serious doubts about some people’s ability to do their job. There will be changes coming shortly and those decisions will be new people’s to make.”

And then, unexpectedly, came the hope of salvation.

“Bond, Q, and Monneypenny”

By October 2010, Barr was under considerable stress. His CEO job was under threat, and the e-mails show that the specter of divorce loomed over his personal life.

On October 19, a note arrived. HBGary Federal might be able to provide part of “a complete intelligence solution to a law firm that approached us.” That law firm was DC-based powerhouse Hunton & Williams, which boasted 1,000 attorneys and terrific contacts. They had a client who wanted to do a little corporate investigative work, and three small security firms thought they might band together to win the deal.

Palantir would provide its expensive link analysis software running on a hosted server, while Berico would “prime the contract supplying the project management, development resources, and process/methodology development.” HBGary Federal would come alongside to provide “digital intelligence collection” and “social media exploitation”—Barr’s strengths.

The three companies needed a name for their joint operation. One early suggestion: a “Corporate Threat Analysis Cell.” Eventually, a sexier name was chosen: Team Themis.

Barr went to work immediately, tracking down all the information he could find on the team’s H&W contact. This was the result of few hours’ work:

A bit of what I have on [redacted]. He was hard to find on Facebook as he has taken some precautions to be found. He isn’t even linked with his wife but I found him. I also have a list of his friends and have defined an angle if I was to target him. He has attachment to UVA, a member of multiple associations dealing with IP, e-discovery, and nearly all of this facebook friends are of people from high school. So I would hit him from one of these three angles. I am tempted to create a person from his highschool and send him a request, but that might be overstepping it. I don’t want to embarrass him, so I think I will just talk about it and he can decide for himself if I would have been successful or not.

Team Themis didn’t quite understand what H&W wanted them to do, so Barr’s example was simply a way to show “expertise.” But it soon became clear what this was about: the US Chamber of Commerce wanted to know if certain groups attacking them were “astroturf” groups funded by the large unions.

“They further suspect that most of the actions and coordination take place through online means—forums, blogs, message boards, social networking, and other parts of the ‘deep web,’” a team member explained later. “But they want to marry these online, ‘cyber’ sources with traditional open source data—tax records, fundraising records, donation records, letters of incorporation, etc. I believe they want to trace all the way from board structure down to the individuals carrying out actions.”

H&W was putting together a proposal for the Chamber, work that Team Themis hoped to win. (It remains unclear how much the Chamber knew about any of this; it claimed later never to have paid a cent either to Team Themis or to H&W in this matter.)
Barr’s plan was to dig up data from background checks, LexisNexis, LinkedIn, Facebook, Twitter, blogs, forums, and Web searches and dump it into Palantir for analysis. Hopefully, the tool could shed light on connections between the various anti-Chamber forces.

Purpose

- Develop a corporate information reconnaissance service to aid legal investigations through the open source collection of information on target groups and individuals that appear organized to extort specific concessions through online slander campaigns.

An early version of the Team Themis goal

Once that was done, Team Themis staffers could start churning out intelligence reports for the Chamber. The team wrote up a set of “sample reports” filled with action ideas like:

- Create a false document, perhaps highlighting periodical financial information, and monitor to see if US Chamber Watch acquires it. Afterward, present explicit evidence proving that such transactions never occurred. Also, create a fake insider persona and generate communications with [union-backed Change to Win]. Afterward, release the actual documents at a specified time and explain the activity as a CtW contrived operation.
- If needed, create two fake insider personas, using one as leverage to discredit the other while confirming the legitimacy of the second. Such work is complicated, but a well-thought out approach will give way to a variety of strategies that can sufficiently aid the formation of vetting questions US Chamber Watch will likely ask.
- Create a humor piece about the leaders of CtW.

The whole team had been infected with some kind of spy movie virus, one which led them to think in terms of military intelligence operations and ham-handed attacks. The attitude could be seen in e-mails which exhorted Team Themis to “make [H&W] think that we are Bond, Q, and money penny [sic] all packaged up with a bow.”

Two million a month

But what to charge for this cloak-and-dagger work? Some team members worried that the asking price for an initial deployment was too high for H&W; someone else fired back, “Their client is loaded!” Besides, that money would buy access to Palantir, Berico, and “super sleuth Aaron Barr.”

As the Team Themis proposal went to one of the top H&W lawyers for potential approval, Barr continued his social media dumpster diving. He dug up information on H&W employees, Chamber opponents, even the H&W partner whose approval was needed to move this proposal forward. That last bit of data collection, which Barr sent on to H&W, led to the e-mail about how it might “freak out” the partner.
If the deal came through, Barr told his HBGary colleagues, it might salvage the HBGary Federal business. “This will put us in a healthy position to chart our direction with a healthy war chest,” he wrote.

Indeed it would; Team Themis decided to ask for $2 million per month, for six months, for the first phase of the project, putting $500,000 to $700,000 per month in HBGary Federal’s pocket.

But the three companies disagreed about how to split the pie. In the end, Palantir agreed to take less money, but that decision had to go “way up the chain (as you can imagine),” wrote the Palantir contact for Team Themis. “The short of it is that we got approval from Dr. Karp and the Board to go ahead with the modified 40/30/30 breakdown proposed. These were not fun conversations, but we are committed to this team and we can optimize the cost structure in the long term (let’s demonstrate success and then take over this market :)).”

The leaders at the very top of Palantir were aware of the Team Themis work, though the details of what was being proposed by Barr may well have escaped their notice. Palantir wasn’t kidding around with this contract; if selected by H&W and the Chamber, Palantir planned to staff the project with an experienced intelligence operative, a man who “ran the foreign fighter campaign on the Syrian border in 2005 to stop the flow of suicide bombers into Baghdad and helped to ensure a successful Iraqi election. As a commander, [he] ran the entire intelligence cycle: identified high-level terrorists, planned missions to kill or capture them, led the missions personally, then exploited the intelligence and evidence gathered on target to defeat broader enemy networks.”

(Update: a reader points to additional emails which suggest that the “foreign fighter campaign” operative would not actually be working on the Team Themis project. Instead, Berico and Palantir would list him and another top person as “key personnel,” drawing on their “creds to show our strengths,” but might actually staff the project with others.)

“I don’t think we can make it any further”

But the cash, which “will seem like money falling from the sky for those of us used to working in the govt sector,” was not forthcoming. H&W didn’t make a decision in November. Barr began to worry.

“All things we are chasing continue to get pushed to the right or just hang in limbo,” he wrote. “I don’t think we can make it any further. We are behind in our taxes trying to keep us afloat until a few things came through, but they are
not happening fast enough.” He noted that Palantir was asking “way too much money” from H&W.

As the weeks dragged on, Team Themis decided to lower its price. It sent an e-mail to H&W, saying that the three companies were “prepared to offer our services as Team Themis at a significantly lower cost (much closer to the original “Phase I” proposed costs). Does this sound like a more reasonable range in terms of pricing?”

But before H&W made a decision on Chamber of Commerce plan, it had another urgent request for Team Themis: a major US bank had come to H&W seeking help against WikiLeaks (the bank has been widely assumed to be Bank of America, which has long been rumored to be a future WikiLeaks target.)

“We want to sell this team as part of what we are talking about,” said the team’s H&W contact. “I need a favor. I need five to six slides on Wikileaks—who they are, how they operate and how this group may help this bank. Please advise if you can help get me something ASAP. My call is at noon.”

“Attack their weak points”

By 11:30pm on the evening of December 2, Barr had cranked out a PowerPoint presentation. It called for “disinformation,” “cyber attacks,” and a “media campaign” against WikiLeaks.

What could HBGary Federal do?

- Computer Network Attack/Exploitation
- Influence and Deception Operations
- Social Media Collection, Analysis, Exploitation
- Digital Media Forensic Analysis

This attack capability wasn’t mere bluster. HBGary had long publicized to clients its cache of 0-day exploits—attacks for which there is no existing patch. A slide from a year earlier showed that HBGary claimed unpublished 0-day exploits in everything from Flash to Java to Windows 2000.

Another slide made clear that the company had expertise in “computer network attack,” “custom malware development,” and “persistent software implants.”
In October 2010, HBGary CEO Greg Hoglund had tossed out a random idea for Barr, one that did not apparently seem unusual: “I suggest we create a large set of unlicensed windows-7 themes for video games and movies appropriate for middle east & asia. These theme packs would contain back doors.”

Barr’s ideas about WikiLeaks went beyond attacks on their infrastructure. He wrote in a separate document that WikiLeaks was having trouble getting money because its payment sources were being blocked. “Also need to get people to understand that if they support the organization we will come after them,” he wrote. “Transaction records are easily identifiable.”

As an idea that Barr knew was being prepared for a major US bank, the suggestion is chilling. Barr also reiterated the need to “get to the Swedish document submission server” that allowed people to upload leaked documents.

**Campaign Thrusts**

- Feed the fuel between the feuding groups. Disinformation. Create messages around actions to sabotage or discredit the opposing organization. Submit fake documents and then call out the error.
- Create concern over the security of the infrastructure. Create exposure stories. If the process is believed to not be secure they are done.
- Cyber attacks against the infrastructure to get data on document submitters. This would kill the project. Since the servers are now in Sweden and France putting a team together to get access is more straightforward.
- Media campaign to push the radical and reckless nature of WikiLeaks activities. Sustained pressure. Does nothing for the fanatics, but creates concern and doubt amongst moderates.
- Search for leaks. Use social media to profile and identify risky behavior.

At 7:30am the next morning, Barr had another great idea—find some way to make WikiLeaks supporters like Glenn Greenwald feel like their jobs might be at stake for supporting the organization.

“One other thing,” he wrote in his morning message. “I think we need to highlight people like Glenn Greenwald. Glenn was critical in the Amazon to OVH [data center] transition and helped WikiLeaks provide access to information during the transition. It is this level of support we need to attack. These are established professionals that have a liberal bent, but ultimately most of them if pushed will choose professional preservation over cause, such is the mentality of most business professionals. Without the support of people like Glenn WikiLeaks would fold.”

This seems an absurd claim on a number of levels, but it also upped the “creep factor” dramatically. Barr was now
suggesting that a major US corporation find ways to lean on a civil liberties lawyer who held a particular view of WikiLeaks, pressuring him into silence on the topic. Barr, the former Navy SIGINT officer who had traveled around the world to defend the US right to freedom of speech, had no apparent qualms about his idea.

“Discontinued all ties with HBGary Federal”

The fallout rained down quickly enough. In January, with H&W still not signing off on any big-dollar deals, Barr decided to work on a talk for the BSides security conference in San Francisco. He hoped to build on all of the social media work he was doing to identify the main participants in the Anonymous hacker collective—and by doing so to drum up business.

The decision seems to have stemmed from Barr’s work on WikiLeaks. Anonymous defended WikiLeaks on several occasions in 2010, even attacking the websites of Visa and MasterCard when the companies refused to process WikiLeaks donations. But Barr also liked the thrill of chasing a dangerous quarry.

For instance, to make his point about the vulnerabilities of social media, Barr spent some time in 2010 digging into the power company Exelon and its US nuclear plants. “I am going to target the largest nuclear operator in the United States, Exelon, and I am going to do a social media targeted collection, reconnaissance against them,” he wrote.

Once Barr had his social media map of connections, he could attack. As he wrote elsewhere:

Example. If I want to gain access to the Exelon plant up in Pottstown PA I only have to go as far as LinkedIn to identify Nuclear engineers being employed by Exelon in that location. Jump over to Facebook to start doing link analysis and profiling. Add data from twitter and other social media services. I have enough information to develop a highly targeted exploitation effort.

I can and have gained access to various government and government contractor groups in the social media space using this technique (more detailed but you get the point). Given that people work from home, access home services from work—getting access to the target is just a matter of time and nominal effort.

Knowing about a target’s spouse and college and business and friends makes it relatively easy to engage in a “spear phishing” attack against that person—say, a fake e-mail from an old friend, in which the target eventually reveals useful information.

Ironically, when Anonymous later commandeered Greg Hoglund’s separate security site rootkit.com, it did so through a spear phishing e-mail attack on Hoglund’s site administrator—who promptly turned off the site’s defenses and issued a new password (“Changeme123”) for a user he believed was Hoglund. Minutes later, the site was compromised.

After the Anonymous attacks and the release of Barr’s e-mails, his partners furiously distanced themselves from Barr’s work. Palantir CEO Dr. Alex Karp wrote, “We do not provide—nor do we have any plans to develop—offensive cyber capabilities... The right to free speech and the right to privacy are critical to a flourishing democracy. From its inception, Palantir Technologies has supported these ideals and demonstrated a commitment to building software that protects privacy and civil liberties. Furthermore, personally and on behalf of the entire company, I want to publicly apologize to progressive organizations in general, and Mr. Greenwald in particular, for any involvement that we may have had in these matters.”

Berico said (PDF) 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.”

But both of the Team Themis leads at these companies knew exactly what was being proposed (such knowledge may not have run to the top). They saw Barr’s e-mails, and they used his work. His ideas on attacking WikiLeaks made it almost verbatim into a Palantir slide about “proactive tactics.”
And Palantir had no problem scraping tweets from union supporters and creating linkages from them.

As for targeting American organizations, it was a Berico analyst who sent out the Team Themis “sample reports,” the documents suggesting that the US Chamber of Commerce create false documents and false personae in its effort to “discredit the organization” US Chamber Watch.

The US Chamber of Commerce expressed shock when the Team Themis work came to light. “We’re incredulous that anyone would attempt to associate such activities with the Chamber as we've seen today from the Center for American Progress,” said Tom Collamore on February 10. “The security firm referenced by ThinkProgress was not hired by the Chamber or by anyone else on the Chamber’s behalf. We have never seen the document in question nor has it ever been discussed with us.”

Indeed, the meeting between H&W and the Chamber on this issue was set to take place today, February 14. On February 11, the Chamber went further, issuing a new statement saying that “it never hired or solicited proposals from HBGary, Palantir or Berico, the security firms being talked about on the Web... The leaked e-mails appear to show that HBGary was willing to propose questionable actions in an attempt to drum up business, but the Chamber was not aware of these proposals until HBGary’s e-mails leaked.”

“No money, for any purpose, was paid to any of those three private security firms by the Chamber, or by anyone on behalf of the Chamber, including Hunton & Williams.”

As for Hunton & Williams, they have yet to comment publicly. On February 7, however, the firm celebrated its top ranking in Computerworld’s report on “Best Privacy Advisers.”
It has been an embarrassing week for security firm HBGary and its HBGary Federal offshoot. HBGary Federal CEO Aaron Barr thought he had unmasked the hacker hordes of Anonymous and was preparing to name and shame those responsible for co-ordinating the group’s actions, including the denial-of-service attacks that hit MasterCard, Visa, and other perceived enemies of WikiLeaks late last year.

When Barr told one of those he believed to be an Anonymous ringleader about his forthcoming exposé, the Anonymous response was swift and humiliating. HBGary’s servers were broken into, its e-mails pillaged and published to the world, its data destroyed, and its website defaced. As an added bonus, a second site owned and operated by Greg Hoglund, owner of HBGary, was taken offline and the user registration database published.

Over the last week, I’ve talked to some of those who participated in the HBGary hack to learn in detail how they penetrated HBGary’s defenses and gave the company such a stunning black eye—and what the HBGary example means for the rest of us mere mortals who use the Internet.

Anonymous: more than kids

HBGary and HBGary Federal position themselves as experts in computer security. The companies offer both software and services to both the public and private sectors. On the software side, HBGary has a range of computer forensics and malware analysis tools to enable the detection, isolation, and analysis of worms, viruses, and trojans. On the services side, it offers expertise in implementing intrusion detection systems and secure networking, and performs vulnerability assessment and penetration testing of systems and software. A variety of three letter agencies, including the NSA, appeared to be in regular contact with the HBGary companies, as did Interpol, and HBGary also worked with well-known security firm McAfee. At one time, even Apple expressed an interest in the company’s products or services.

Greg Hoglund’s rootkit.com is a respected resource for discussion and analysis of rootkits (software that tampers with operating systems at a low level to evade detection) and related technology; over the years, his site has been targeted by disgruntled hackers aggrieved that their wares have been discussed, dissected, and often disparaged as badly written bits of code.
One might think that such an esteemed organization would prove an insurmountable challenge for a bunch of disaffected kids to hack. World-renowned, government-recognized experts against Anonymous? HBGary should be able to take their efforts in stride.

Unfortunately for HBGary, neither the characterization of Anonymous nor the assumption of competence on the security company’s part are accurate, as the story of how HBGary was hacked will make clear.

Anonymous is a diverse bunch: though they tend to be younger rather than older, their age group spans decades. Some may still be in school, but many others are gainfully employed office-workers, software developers, or IT support technicians, among other things. With that diversity in age and experience comes a diversity of expertise and ability.

It’s true that most of the operations performed under the Anonymous branding have been relatively unsophisticated, albeit effective: the attacks made on MasterCard and others were distributed denial-of-service attacks using a modified version of the Low Orbit Ion Cannon (LOIC) load-testing tool. The modified LOIC enables the creation of large botnets that each user opts into: the software can be configured to take its instructions from connections to Internet relay chat (IRC) chat servers, allowing attack organizers to remotely control hundreds of slave machines and hence control large-scale attacks that can readily knock websites offline.

According to the leaked e-mails, Aaron Barr believed that HBGary’s website was itself subject to a denial-of-service attack shortly after he exposed himself to someone he believed to be a top Anonymous leader. But the person I spoke to about this denied any involvement in such an attack. Which is not to say that the attack didn’t happen—simply that this person didn’t know about or participate in it. In any case, the Anonymous plans were more advanced than a brute force DDoS.

**Time for an injection**

HBGary Federal’s website, hbgaryfederal.com, was powered by a content management system (CMS). CMSes are a common component of content-driven sites; they make it easy to add and update content to the site without having to mess about with HTML and making sure everything gets linked up and so on and so forth. Rather than using an off-the-shelf CMS (of which there are many, used in the many blogs and news sites that exist on the Web), HBGary—for reasons best known to its staff—decided to commission a custom CMS system from a third-party developer.

Unfortunately for HBGary, this third-party CMS was poorly written. In fact, it had what can only be described as a pretty gaping bug in it. A standard, off-the-shelf CMS would be no panacea in this regard—security flaws crop up in all of them from time to time—but it would have the advantage of many thousands of users and regular bugfixes, resulting in a much lesser chance of extant security flaws.

The custom solution on HBGary’s site, alas, appeared to lack this kind of support. And if HBGary conducted any kind of vulnerability assessment of the software—which is, after all, one of the services the company offers—then its assessment overlooked a substantial flaw.

The hbgaryfederal.com CMS was susceptible to a kind of attack called **SQL injection**. In common with other CMSes, the hbgaryfederal.com CMS stores its data in an SQL database, retrieving data from that database with suitable queries. Some queries are fixed—an integral part of the CMS application itself. Others, however, need parameters. For example, a query to retrieve an article from the CMS will generally need a parameter corresponding to the article ID number. These parameters are, in turn, generally passed from the Web front-end to the CMS.

SQL injection is possible when the code that deals with these parameters is faulty. Many applications join the parameters from the Web front-end with hard-coded queries, then pass the whole concatenated lot to the database. Often, they do this without verifying the validity of those parameters. This exposes the systems to SQL injection. Attackers can pass in specially crafted parameters that cause the database to execute queries of the attackers’ own choosing.

The exact URL used to break into hbgaryfederal.com was http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27. The URL has two parameters named pageNav and page, set to the values 2 and 27, respectively. One or other or both of these was handled incorrectly by the CMS, allowing the hackers to retrieve data from the database that they shouldn’t have been able to get.
Rainbow tables

Specifically, the attackers grabbed the user database from the CMS—the list of usernames, e-mail addresses, and password hashes for the HBGary employees authorized to make changes to the CMS. In spite of the rudimentary SQL injection flaw, the designers of the CMS system were not completely oblivious to security best practices; the user database did not store plain readable passwords. It stored only hashed passwords—passwords that have been mathematically processed with a hash function to yield a number from which the original password can’t be deciphered.

The key part is that you can’t go backwards—you can’t take the hash value and convert it back into a password. With a hash algorithm, traditionally the only way to figure out the original password was to try every single possible password in turn, and see which one matched the hash value you have. So, one would try “a,” then “b,” then “c”... then “z,” then “aa,” “ab,” and so on and so forth.

To make this more difficult, hash algorithms are often quite slow (deliberately), and users are encouraged to use long passwords which mix lower case, upper case, numbers, and symbols, so that these brute force attacks have to try even more potential passwords until they find the right one. Given the number of passwords to try, and the slowness of hash algorithms, this normally takes a very long time. Password cracking software to perform this kind of brute force attack has long been available, but its success at cracking complex passwords is low.

However, a technique first published in 2003 (itself a refinement of a technique described in 1980) gave password crackers an alternative approach. By pre-computing large sets of data and generating what are known as rainbow tables, the attackers can make a trade-off: they get much faster password cracks in return for using much more space. The rainbow table lets the password cracker pre-compute and store a large number of hash values and the passwords that generated them. An attacker can then look up the hash value that they are interested in and see if it’s in the table. If it is, they can then read out the password.

To make cracking harder, good password hash implementations will use a couple of additional techniques. The first is iterative hashing: simply put, the output of the hash function is itself hashed with the hash function, and this process is repeated thousands of times. This makes the hashing process considerably slower, hindering both brute-force attacks and rainbow table generation.

The second technique is salting; a small amount of random data is added to the password before hashing it, greatly expanding the size of rainbow table that would be required to get the password.

In principle, any hash function can be used to generate rainbow tables. However, it takes more time to generate rainbow tables for slow hash functions than it does for fast ones, and hash functions that produce a short hash value require less storage than ones that produce long hash values. So in practice, only a few hash algorithms have widely available rainbow table software available. The best known and most widely supported of these is probably MD5, which is quick to compute and produces an output that is only 128 bits (16 bytes) per hash. These factors together make it particularly vulnerable to rainbow table attacks. A number of software projects exist that allow the generation or downloading of MD5 rainbow tables, and their subsequent use to crack passwords.

As luck would have it, the hbgaryfederal.com CMS used MD5. What’s worse is that it used MD5 badly: there was no iterative hashing and no salting. The result was that the downloaded passwords were highly susceptible to rainbow table-based attacks, performed using a rainbow table-based password cracking website. And so this is precisely what the attackers did; they used a rainbow table cracking tool to crack the hbgaryfederal.com CMS passwords.

Even with the flawed usage of MD5, HBGary could have been safe thanks to a key limitation of rainbow tables: each table only spans a given “pattern” for the password. So for example, some tables may support “passwords of 1-8 characters made of a mix of lower case and numbers,” while other can handle only “passwords of 1-12 characters using upper case only.”

A password that uses the full range of the standard 95 typeable characters (upper and lower case letters, numbers, and the standard symbols found on a keyboard) and which is unusually long (say, 14 or more characters) is unlikely to be found in a rainbow table, because the rainbow table required for such passwords will be too big and take too long to generate.

Alas, two HBGary Federal employees—CEO Aaron Barr and COO Ted Vera—used passwords that were very
simple; each was just six lower case letters and two numbers. Such simple combinations are likely to be found in any respectable rainbow table, and so it was that their passwords were trivially compromised.

For a security company to use a CMS that was so flawed is remarkable. Improper handling of passwords—iterative hashing, using salts and slow algorithms—and lack of protection against SQL injection attacks are basic errors. Their system did not fall prey to some subtle, complex issue: it was broken into with basic, well-known techniques. And though not all the passwords were retrieved through the rainbow tables, two were, because they were so poorly chosen.

HBGary owner Penny Leavy said in a later IRC chat with Anonymous that the company responsible for implementing the CMS has since been fired.

**Password problems**

Still, badly chosen passwords aren’t such a big deal, are they? They might have allowed someone to deface the hbgaryfederal.com website—admittedly embarrassing—but since everybody knows that you shouldn’t reuse passwords across different systems, that should have been the extent of the damage, surely?

Unfortunately for HBGary Federal, it was not. Neither Aaron nor Ted followed best practices. Instead, they used the same password in a whole bunch of different places, including e-mail, Twitter accounts, and LinkedIn. For both men, the passwords allowed retrieval of e-mail. However, that was not all they revealed. Let’s start with Ted’s password first.

Along with its webserver, HBGary had a Linux machine, support.hbgary.com, on which many HBGary employees had shell accounts with ssh access, each with a password used to authenticate the user. One of these employees was Ted Vera, and his ssh password was identical to the cracked password he used in the CMS. This gave the hackers immediate access to the support machine.

ssh doesn’t have to use passwords for authentication. Passwords are certainly common, but they’re also susceptible to this kind of problem (among others). To combat this, many organizations and users, particularly those with security concerns, do not use passwords for ssh authentication. Instead, they use public key cryptography: each user has a key made up of a private part and a public part. The public part is associated with their account, and the private part is kept, well, private. ssh then uses these two keys to authenticate the user.

Since these private keys are not as easily compromised as passwords—servers don’t store them, and in fact they never leave the client machine—and aren’t readily re-used (one set of keys might be used to authenticate with several servers, but they can’t be used to log in to a website, say), they are a much more secure option. Had they been used for HBGary’s server, it would have been safe. But they weren’t, so it wasn’t.

Although attackers could log on to this machine, the ability to look around and break stuff was curtailed: Ted was only a regular non-superuser. Being restricted to a user account can be enormously confining on a Linux machine. It spoils all your fun; you can’t read other users’ data, you can’t delete files you don’t own, you can’t cover up the evidence of your own break-in. It’s a total downer for hackers.

The only way they can have some fun is to elevate privileges through exploiting a privilege escalation vulnerability. These crop up from time to time and generally exploit flaws in the operating system kernel or its system libraries to trick it into giving the user more access to the system than should be allowed. By a stroke of luck, the HBGary system was vulnerable to just such a flaw. The error was published in October last year, conveniently with a full, working exploit. By November, most distributions had patches available, and there was no good reason to be running the exploitable code in February 2011.

Exploitation of this flaw gave the Anonymous attackers full access to HBGary’s system. It was then that they discovered many gigabytes of backups and research data, which they duly purged from the system.

Aaron’s password yielded even more fruit. HBGary used Google Apps for its e-mail services, and for both Aaron and Ted, the password cracking provided access to their mail. But Aaron was no mere user of Google Apps: his account was also the administrator of the company’s mail. With his higher access, he could reset the passwords of any mailbox and hence gain access to all the company’s mail—not just his own. It’s this capability that yielded access to Greg Hoglund’s mail.

And what was done with Greg’s mail?
A little bit of social engineering, that’s what.

**A little help from my friends**

Contained within Greg’s mail were two bits of useful information. One: the root password to the machine running Greg’s rootkit.com site was either “88j4bb3rw0cky88” or “88Scr3am3r88”. Two: Jussi Jaakonaho, “Chief Security Specialist” at Nokia, had root access. Vandalizing the website stored on the machine was now within reach.

The attackers just needed a little bit more information: they needed a regular, non-root user account to log in with, because as a standard security procedure, direct ssh access with the root account is disabled. Armed with the two pieces of knowledge above, and with Greg’s e-mail account in their control, the social engineers set about their task. The e-mail correspondence tells the whole story:

From: Greg
To: Jussi
Subject: need to ssh into rootkit

im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?

and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?

thanks

-------------------------------------

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit

hi, do you have public ip? or should i just drop fw?

and it is w0cky - tho no remote root access allowed

-------------------------------------
From: Greg  
To: Jussi  
Subject: Re: need to ssh into rootkit  
noo i don't have the public ip with me at the moment because i'm ready for a small meeting and i'm in a rush.  
if anything just reset my password to changeme123 and give me public ip and i'll ssh in and reset my pw.  

-------------------------------------  

From: Jussi  
To: Greg  
Subject: Re: need to ssh into rootkit  
ok, it should now accept from anywhere to 47152 as ssh. i am doing testing so that it works for sure.  
your password is changeme123  
i am online so just shoot me if you need something.  
in europe, but not in finland? :-)

_jussi

-------------------------------------  

From: Greg  
To: Jussi  
Subject: Re: need to ssh into rootkit  
if i can squeeze out time maybe we can catch up. i'll be in germany for a little bit. anyway i can't ssh into rootkit. you sure the ips still 65.74.181.141?  
thanks

-------------------------------------  

From: Jussi  
To: Greg
Subject: Re: need to ssh into rootkit
does it work now?

-------------------------------------
From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
yes jussi thanks
did you reset the user greg or?

-------------------------------------
From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
nope. your account is named as hoglund

-------------------------------------
From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
yup im logged in thanks ill email you in a few, im backed up
thanks

Thanks indeed. To be fair to Jussi, the fake Greg appeared to know the root password and, well, the e-mails were coming from Greg’s own e-mail address. But over the course of a few e-mails it was clear that “Greg” had forgotten both his username and his password. And Jussi handed them to him on a platter.

Later on, Jussi did appear to notice something was up:

From: Jussi
To: Greg

Subject: Re: need to ssh into rootkit
did you open something running on high port?
As with the HBGary machine, this could have been avoided if keys had been used instead of passwords. But they weren’t. Rootkit.com was now compromised.

**Standard practice**

Once the username and password were known, defacing the site was easy. Log in as Greg, switch to root, and deface away! The attackers went one better than this, however: they dumped the user database for rootkit.com, listing the e-mail addresses and password hashes for everyone who’d ever registered on the site. And, as with the hbgaryfederal.com CMS system, the passwords were hashed with a single naive use of MD5, meaning that once again they were susceptible to rainbow table-based password cracking. So the crackable passwords were cracked, too.

So what do we have in total? A Web application with SQL injection flaws and insecure passwords. Passwords that were badly chosen. Passwords that were reused. Servers that allowed password-based authentication. Systems that weren’t patched. And an astonishing willingness to hand out credentials over e-mail, even when the person being asked for them should have realized something was up.

The thing is, none of this is unusual. Quite the opposite. The Anonymous hack was not exceptional: the hackers used standard, widely known techniques to break into systems, find as much information as possible, and use that information to compromise further systems. They didn’t have to, for example, use any non-public vulnerabilities or perform any carefully targeted social engineering. And because of their desire to cause significant public disruption, they did not have to go to any great lengths to hide their activity.

Nonetheless, their attack was highly effective, and it was well-executed. The desire was to cause trouble for HBGary, and that they did. Especially in the social engineering attack against Jussi, they used the right information in the right way to seem credible.

Most frustrating for HBGary must be the knowledge that they know what they did wrong, and they were perfectly aware of best practices; they just didn’t actually use them. Everybody knows you don’t use easy-to-crack passwords, but some employees did. Everybody knows you don’t re-use passwords, but some of them did. Everybody knows that you should patch servers to keep them free of known security flaws, but they didn’t.

And HBGary isn’t alone. Analysis of the passwords leaked from rootkit.com and Gawker shows that password re-use is extremely widespread, with something like 30 percent of users re-using their passwords. HBGary won’t be the last site to suffer from SQL injection, either, and people will continue to use password authentication for secure systems because it’s so much more convenient than key-based authentication.

So there are clearly two lessons to be learned here. The first is that the standard advice is good advice. If all best practices had been followed then none of this would have happened. Even if the SQL injection error was still present, it wouldn’t have caused the cascade of failures that followed.

The second lesson, however, is that the standard advice isn’t good enough. Even recognized security experts who should know better won’t follow it. What hope does that leave for the rest of us?
On November 16, 2009, Greg Hoglund, a cofounder of computer security firm HBGary, sent an e-mail to two colleagues. The message came with an attachment, a Microsoft Word file called AL_QAEDA.doc, which had been further compressed and password protected for safety. Its contents were dangerous.

“I got this word doc linked off a dangler site for Al Qaeda peeps,” wrote Hoglund. “I think it has a US govvy payload buried inside. Would be neat to [analyze] it and see what it’s about. DONT open it unless in a [virtual machine] obviously… DONT let it FONE HOME unless you want black suits landing on your front acre. :-)”

The attached document, which is in English, begins: “LESSON SIXTEEN: ASSASSINATIONS USING POISONS AND COLD STEEL (UK/BM-154 TRANSLATION).”

It purports to be an Al-Qaeda document on dispatching one’s enemies with knives (try “the area directly above the genitals”), with ropes (“Choking… there is no other area besides the neck”), with blunt objects (“Top of the stomach, with the end of the stick.”), and with hands (“Poking the fingers into one or both eyes and gouging them.”).

But the poison recipes, for ricin and other assorted horrific bioweapons, are the main draw. One, purposefully made from a specific combination of spoiled food, requires “about two spoonfuls of fresh excrement.” The document praises the effectiveness of the resulting poison: “During the time of the destroyer, Jamal Abdul Nasser, someone who was being severely tortured in prison (he had no connection with Islam), ate some feces after losing sanity from the severity of the torture. A few hours after he ate the feces, he was found dead.”
According to Hoglund, the recipes came with a side dish, a specially crafted piece of malware meant to infect Al-Qaeda computers. Is the US government in the position of deploying the hacker’s darkest tools—rootkits, computer viruses, trojan horses, and the like? Of course it is, and Hoglund was well-positioned to know just how common the practice had become. Indeed, he and his company helped to develop these electronic weapons.

Thanks to a cache of HBGary e-mails leaked by the hacker collective Anonymous, we have at least a small glimpse through a dirty window into the process by which tax dollars enter the military-industrial complex and emerge as malware.

**Task B**

In 2009, HBGary had partnered with the Advanced Information Systems group of defense contractor General Dynamics to work on a project euphemistically known as “Task B.” The team had a simple mission: slip a piece of stealth software onto a target laptop without the owner’s knowledge.

They focused on ports—a laptop’s interfaces to the world around it—including the familiar USB port, the less-common PCMCIA Type II card slot, the smaller ExpressCard slot, WiFi, and Firewire. No laptop would have all of these, but most recent machines would have at least two.

The HBGary engineering team broke this list down into three categories. First came the “direct access” ports that provided “uninhibited electronic direct memory access.” PCMCIA, ExpressCard, and Firewire all allowed external devices—say a custom piece of hardware delivered by a field operative—to interact directly with the laptop with a minimum amount of fuss. The direct memory access provided by the controllers for these ports mean that devices in them can write directly to the computer’s memory without intervention from the main CPU and with little restriction from the operating system. If you want to overwrite key parts of the operating system to sneak in a bit of your own code, this is the easiest way to go.

The second and third categories, ports that needed “trust relationships” or relied on “buffer overflows,” included USB and wireless networking. These required more work to access, especially if one wanted to do so without alerting a user; Windows in particular is notorious for the number of prompts it throws when USB devices are inserted or removed. A cheerful note about “Searching for device driver for NSA_keylogger_rootkit_tango” had to be avoided.

So HBGary wanted to go the direct access route, characterizing it as the “low hanging fruit” with the lowest risk. General Dynamics wanted HBGary to investigate the USB route as well (the ports are more common, but an attack has to trick the operating system into doing its bidding somehow, commonly through a buffer overflow).

The team had two spy movie scenarios in which its work might be used, scenarios drafted to help the team think through its approach:

1) Man leaves laptop locked while quickly going to the bathroom. A device can then be
inserted and then removed without touching the laptop itself except at the target port. (i.e. one can’t touch the mouse, keyboard, insert a CD, etc.) 2) Woman shuts down her laptop and goes home. One then can insert a device into the target port and assume she will not see it when she returns the next day. One can then remove the device at a later time after she boots up the machine.

Why would the unnamed client for Task B—which a later e-mail makes clear was for a government agency—want such a tool? Imagine you want access to the computer network used in a foreign government ministry, or in a nuclear lab. Such a facility can be tough to crack over the Internet; indeed, the most secure facilities would have no such external access. And getting an agent inside the facility to work mischief is very risky—if it’s even possible at all.

But say a scientist from the facility uses a memory stick to carry data home at night, and that he plugs the memory stick into his laptop on occasion. You can now get a piece of custom spyware into the facility by putting a copy on the memory stick—if you can first get access to the laptop. So you tail the scientist and follow him from his home one day to a local coffee shop. He steps away to order another drink, to go to the bathroom, or to talk on his cell phone, and the tail walks past his table and sticks an all-but-undetectable bit of hardware in his laptop’s ExpressCard slot. Suddenly, you have a vector that points all the way from a local coffee shop to the interior of a secure government facility.

The software exploit code actually delivered onto the laptop was not HBGary’s concern; it needed only to provide a route through the computer’s front door. But it had some constraints. First, the laptop owner should still be able to use the port so as not to draw attention to the inserted hardware. This is quite obviously tricky, but one could imagine a tiny ExpressCard device that slid down into the slot but could in turn accept another ExpressCard device on its exterior-facing side. This sort of parallel plugging might well go unnoticed by a user with no reason to suspect it.

HBGary’s computer infiltration code then had to avoid the computer’s own electronic defenses. The code should “not be detectable” by virus scanners or operating system port scans, and it should clean up after itself to eliminate all traces of entry.

Greg Hoglund was confident that he could deliver at least two laptop-access techniques in less than a kilobyte of memory each. As the author of books like *Exploiting Software: How to Break Code*, *Rootkits: Subverting the Windows Kernel*, and *Exploiting Online Games: Cheating Massively Distributed Systems*, he knew his way around the deepest recesses of Windows in particular.

Hoglund’s special interest was in all-but-undetectable computer “rootkits,” programs that provide privileged access to a computer’s innermost workings while cloaking themselves even from standard operating system functions. A good rootkit can be almost impossible to remove from a running machine—if you could even find it in the first place.

**Just a demo**

Some of this work was clearly for demonstration purposes, and much of it was probably never deployed in the field. For instance, HBGary began $50,000 of work for General Dynamics on “Task C” in June 2009, creating a piece of malware that infiltrated Windows machines running Microsoft Outlook.

The target user would preview a specially crafted e-mail message in Outlook that took advantage of an Outlook preview pane vulnerability to execute a bit of code in the background. This code would install a kernel driver, one operating at the lowest and most trusted level of the operating system, that could send traffic over the computer’s serial port. (The point of this exercise was never spelled out, though the use of serial ports rather than network ports suggest that cutting-edge desktop PCs were not the target.)
Once installed, the malware could execute external commands, such as sending specific files over the serial port, deleting files on the machine, or causing the infamous Windows “blue screen of death.” In addition, the code should be able to pop open the computer’s CD tray and blink the lights on its attached keyboards—another reminder that Task C was, at this stage, merely for a demo.

General Dynamics would presumably try to interest customers in the product, but it’s not clear from the e-mails at HBGary whether this was ever successful. Even with unique access to the innermost workings of a security firm, much remains opaque; the real conversations took place face-to-face or on secure phone lines, not through e-mail, so the glimpses we have here are fragmentary at best. This care taken to avoid sending sensitive information via unencrypted e-mail stands in stark contrast with the careless approach to security that enabled the hacks in the first place.

But that doesn’t mean specific information is hard to come by—such as the fact that rootkits can be purchased for $60,000.

**Step right up!**

Other tools were in use and were sought out by government agencies. An internal HBGary e-mail from early 2010 asks, “What are the license costs for HBGary rk [rootkit] platform if they want to use it on guardian for afisr [Air Force Intelligence, Surveillance, and Reconnaissance]?”

The reply indicates that HBGary has several tools on offer. “Are you asking about the rootkit for XP (kernel driver that hides in plain sight and is a keylogger that exfiltrates data) or are you asking about 12 Monkeys? We’ve sold licenses of the 1st one for $60k. We haven’t set a price on 12 Monkeys, but can.”

The company had been developing rootkits for years. Indeed, it had even developed a private Microsoft Word document outlining its basic rootkit features, features which customers could have (confirming the e-mail listed above) for $60,000.
That money bought you the rootkit source code, which was undetectable by most rootkit scanners or firewall products when it was tested against them in 2008. Only one product from Trend Micro noticed the rootkit installation, and even that alert was probably not enough to warn a user. As the HBGary rootkit document notes, “This was a low level alert. TrendMicro assaults the user with so many of these alerts in every day use, therefore most users will quickly learn to ignore or even turn off such alerts.”

When installed in a target machine, the rootkit could record every keystroke that a user typed, linking it up to a Web browser history. This made it easy to see usernames, passwords, and other data being entered into websites; all of this information could be silently “exfiltrated” right through even the pickiest personal firewall.

But if a target watched its outgoing traffic and noted repeated contacts with, say, a US Air Force server, suspicions might be aroused. The rootkit could therefore connect instead to a “dead drop”—a totally anonymous server with no apparent connection to the agency using the rootkit—where the target’s keyboard activity could be retrieved at a later time.

But by 2009, the existing generic HBGary rootkit package was a bit long in the tooth. Hoglund, the rootkit expert, apparently had much bigger plans for a next-gen product called “12 monkeys.”

12 Monkeys

The 12 Monkeys rootkit was also a contract paid out by General Dynamics; as one HBGary e-mail noted, the development work could interfere with Task B, but “if we succeed, we stand to make a great deal of profit on this.”

On April 14, 2009, Hoglund outlined his plans for the new super-rootkit for Windows XP, which was “unique in that the rootkit is not associated with any identifiable or enumerable object. This rootkit has no file, named data structure, device driver, process, thread, or module associated with it.”
How could Hoglund make such a claim? Security tools generally work by scanning a computer for particular objects—pieces of data that the operating system uses to keep track of processes, threads, network connections, and so on. 12 Monkeys simply had nothing to find. “Since no object is associated with the objectless rootkit, detection will be very difficult for a security scanner,” he wrote. In addition, the rootkit would encrypt itself to cloak itself further, and hop around in the computer’s memory to make it even harder to find.

As for getting the data off a target machine and back to the rootkit’s buyer, Hoglund had a clever idea: he disguised the outgoing traffic by sending it only when other outbound Web traffic was being sent. Whenever a user sat down at a compromised machine and started surfing the Web, their machine would slip in some extra outgoing data “disguised as ad-clicks” that would contain a log of all their keystrokes.

While the basic rootkit went for $60,000, HBGary hoped to sell 12 Monkeys for much more: “around $240k.”

0-day

The goal of this sort of work is always to create something undetectable, and there’s no better way to be undetectable than by taking advantage of a security hole that no one else has ever found. Once vulnerabilities are disclosed, vendors like Microsoft race to patch them, and they increasingly push those patches to customers via the Internet. Among hackers, then, the most prized exploits are “0-day” exploits—exploits for holes for which no patch yet exists.

HBGary kept a stockpile of 0-day exploits. A slide from one of the company’s internal presentations showed that the company had 0-day exploits for which no patch yet existed—but these 0-day exploits had not yet even been published. No one knew about them.

The company had exploits “on the shelf” for Windows 2000, Flash, Java, and more; because they were 0-day attacks, any computer around the world running these pieces of software could be infiltrated.

One of the unpublished Windows 2000 exploits, for instance, can deliver a “payload” of any size onto the target machine using a heap exploit. “The payload has virtually no restrictions” on what it can do, a document notes, because the exploit secures SYSTEM level access to the operating system, “the highest user-mode operating system defined level” available.

These exploits were sold to customers. One email, with the subject “Juicy Fruit,” contains the following list of software:

- VMware ESX and ESXi *
- Win2K3 Terminal Services
- Win2K3 MSRPC
- Solaris 10 RPC
- Adobe Flash *
- Sun Java *
- Win2k Professional & Server
- XRK Rootkit and Keylogger *
- Rootkit 2009 *

The e-mail talks only about “tools,” not about 0-day exploits, though that appears to be what was at issue; the list of software here matches HBGary’s own list of its 0-day exploits. And the asterisk beside some of the names “means the tool has been sold to another customer on a non-exclusive basis and can be sold again.”
References to Juicy Fruit abound in the leaked e-mails. My colleague Peter Bright and I have spent days poring through the tens of thousands of messages; we believe that “Juicy Fruit” is a generic name for a usable 0-day exploit, and that interest in this Juicy Fruit was high.

“[Name] is interested in the Juicy Fruit you told him about yesterday,” one e-mail reads. “Next step is I need to give [name] a write up describing it.” That writeup includes the target software, the level of access gained, the max payload size, and “what does the victim see or experience.”

Aaron Barr, who in late 2009 was brought on board to launch the separate company HBGary Federal (and who provoked this entire incident by trying to unmask Anonymous), wrote in one e-mail, “We need to provide info on 12 monkeys and related JF [Juicy Fruit] asap,” apparently in reference to exploits that could be used to infect a system with 12 Monkeys.

HBGary also provided some Juicy Fruit to Xetron, a unit of the massive defense contractor Northrop Grumman that specialized in, among other things, “computer assault.” Barr wanted to “provide Xetron with some JF code to be used for demonstrations to their end customers,” one e-mail noted. “Those demonstrations could lead to JF sales or ongoing services work. There is significant revenue potential doing testing of JF code acquired elsewhere or adding features for mission specific uses.”

As the deal was being worked out, HBGary worked up an agreement to “provide object code and source code for this specific Juicy Fruit” to Xetron, though they could not sell the code without paying HBGary. The code included with this agreement was a “Adobe Macromedia Flash Player Remote Access Tool,” the “HBGary Rootkit Keylogger Platform,” and a “Software Integration Toolkit Module.”

The question of who might be interested in these tools largely remains an unknown—though Barr did request information on HBGary’s Juicy Fruit just after asking for contacts at SOCOM, the US Special Operations Command.

But HBGary Federal had ideas that went far beyond government rootkits and encompassed all facets of information warfare. Including, naturally, cartoons. And Second Life.

**Psyops**

In mid-2010, HBGary Federal put together a PSYOP (psychological operations) proposal for SOCOM, which had issued a general call for new tools and techniques. In the document, the new HBGary Federal team talked up their past experience as creators of “multiple products briefed to POTUS [President of the United States], the NSC [National Security Council], and Congressional Intelligence committees, as well as senior intelligence and military leaders.”

The document focused on cartoons and the Second Life virtual world. “HBGary personnel have experience creating political cartoons that leverage current events to seize the target audience’s attention and propagate the desired
messages and themes,” said the document, noting that security-cleared cartoonists and 3D modelers had already been lined up to do the work if the government wanted some help.

The cartooning process “starts with gathering customer requirements such as the target audience, high level messages and themes, intended publication mediums… Through brainstorming sessions, we develop concept ideas. Approved concepts are rough sketched in pencil. Approved sketches are developed into a detailed, color end product that is suitable for publishing in a variety of mediums.”

A sample cartoon, of Iranian President Ahmadinejad manipulating a puppet Ayatollah, was helpfully included.

The document then went on to explain how the US government could use a virtual world such as Second Life to propagate specific messages. HBGary could localize the Second Life client, translating its menu options and keyboard shortcuts into local dialects, and this localized client could report “valuable usage metrics, enabling detailed measures of effects.” If you want to know whether your message is getting out, just look at the statistics of how many people play the game and for how long.

As for the messages themselves, those would appear within the Second Life world. “HBGary can develop an in-world advertising company, securing small plots of virtual land in attractive locations, which can be used to promote themes using billboards, autonomous virtual robots, audio, video, and 3D presentations,” said the document.

They could even make a little money while they’re at it, by creating “original marketable products to generate self-sustaining revenue within the virtual space as well as promote targeted messaging.”

We found no evidence that SOCOM adopted the proposal.

But HBGary Federal’s real interest had become social media like Facebook and Twitter—and how they could be used to explore and then penetrate secretive networks. And that was exactly what the Air Force wanted to do.
Fake Facebook friends

In June 2010, the government was expressing real interest in social networks. The Air Force issued a public request for “persona management software,” which might sound boring until you realize that the government essentially wanted the ability to have one agent run multiple social media accounts at once.

It wanted 50 software licenses, each of which could support 10 personas, “replete with background, history, supporting details, and cyber presences that are technically, culturally and geographically consistent.”

The software would allow these 50 cyberwarriors to peer at their monitors all day and manipulate these 10 accounts easily, all “without fear of being discovered by sophisticated adversaries.” The personas would appear to come from all over the world, the better to infiltrate jihadist websites and social networks, or perhaps to show up on Facebook groups and influence public opinion in pro-US directions.

As the cyberwarriors worked away controlling their 10 personas, their computers would helpfully provide “real-time local information” so that they could play their roles convincingly.

In addition the Air Force wanted a secure virtual private network that could mask the IP addresses behind all of this persona traffic. Every day, each user would get a random IP address to help hide “the existence of the operation.” The network would further mask this persona work by “traffic mixing, blending the user’s traffic with traffic from multitudes of users from outside the organization. This traffic blending provides excellent cover and powerful deniability.”

This sort of work most interested HBGary Federal’s Aaron Barr, who was carving out a niche for himself as a social media expert. Throughout late 2010 and early 2011, he spent large chunks of his time attempting to use Facebook, Twitter, and Internet chat to map the network of Exelon nuclear plant workers in the US and to research the members of Anonymous. As money for his company dried up and government contracts proved hard to come by, Barr turned his social media ideas on pro-union forces, getting involved in a now-controversial project with two other security firms.

But e-mails make clear that he mostly wanted to sell this sort of capability to the government. “We have other customers, mostly on offense, that are interested in Social Media for other things,” he wrote in August 2010. “The social media stuff seems like low hanging fruit.”

How does one use social media and fake “personas” to do anything of value? An e-mail from Barr on August 22 makes his thinking clear. Barr ponders “the best way to go about establishing a persona to reach an objective (in this case ft_belvoir/INSCOM/1st IO).”

The Army’s Fort Belvoir, like any secretive institution, might be more easily penetrated by pretending to be an old friend of a current employee. “Make your profile swim in a large sea,” Barr wrote. “Pick a big city, big high school, big company. Work your way up and in. Recreate your history. Start by friending high school people. In my case I am in the army so after you have amassed enough friends from high school, then start friending military folks outside of your location, something that matches the area your in, bootcamp, etc. Lastly start to friend people from the base, but start low and work your way up. So far so good.”

Once the persona had this network of friends, “I will start doing things tricky. Try to manipulate conversations, insert communication streams, etc,” said Barr. This sort of social media targeting could also be used to send your new “friend” documents or files (such as the Al-Qaeda poison document discussed above) [that] come complete
with malware, or by directing them to specially-crafted websites designed to elicit some specific piece of information: directed attacks known as “spear phishing.”

But concerns arose about obtaining and using social media data, in part because sites like Facebook restricted the “scraping” of its user data. An employee from the link analysis firm Palantir wrote Barr at the end of August, asking, “Is the idea that we’d want to ingest all of Facebook’s data, or just a targeted subset for a few users of interest?”

The more data that was grabbed from Facebook, the more chance a problem could arise. The Palantir employee noted that a researcher had used similar tools to violate Facebook’s acceptable use policy on data scraping, “resulting in a lawsuit when he crawled most of Facebook’s social graph to build some statistics. I’d be worried about doing the same. (I’d ask him for his Facebook data—he’s a fan of Palantir—but he’s already deleted it.)”

Still, the potential usefulness of sites like Facebook was just too powerful to ignore, acceptable use policy or not.

**Feeling twitchy**

While Barr fell increasingly in love with his social media sleuthing, Hoglund still liked researching his rootkits. In September, the two teamed up for a proposal to DARPA, the Defense Advanced Research Projects Agency that had been instrumental in creating the Internet back in the 1960s.

DARPA didn’t want incrementalism. It wanted breakthroughs (one of its most recent projects is the “100-Year Starship Study”), and Barr and Hoglund teamed up for a proposal to help the agency on its Cyber Insider Threat (CINDER) program. CINDER was an expensive effort to find new ways to watch employees with access to sensitive information and root out double agents or disgruntled workers who might leak classified information.

So Barr and Hoglund drafted a plan to create something like a lie detector, except that it would look for signs of “paranoia” instead.

“Like a lie detector detects physical changes in the body based on sensitivities to specific questions, we believe there are physical changes in the body that are represented in observable behavioral changes when committing actions someone knows is wrong,” said the proposal. “Our solution is to develop a paranoia-meter to measure these observables.”

The idea was to take an HBGary rootkit like 12 Monkeys and install it on user machines in such a way that users could not remove it and might not even be aware of its presence. The rootkit would log user keystrokes, of course, but it would also take “as many behavioral measurements as possible” in order to look for suspicious activity that might indicate wrongdoing.

What sort of measurements? The rootkit would monitor “keystrokes, mouse movements, and visual cues through the system camera. We believe that during particularly risky activities we will see more erratic mouse movements and keystrokes as well as physical observations such as surveying surroundings, shifting more frequently, etc.”

The rootkit would also keep an eye on what files were being accessed, what e-mails were being written, and what instant messages were being sent. If necessary, the software could record a video of the user’s computer screen activity and send all this information to a central monitoring office. There, software would try to pick out employees exhibiting signs of paranoia, who could then be scrutinized more closely.

Huge and obvious challenges presented themselves. As the proposal noted:

Detecting insider threat actions is highly challenging and will require a sophisticated monitoring, baselining, analysis, and alerting capability. Human actions and organizational operations are complex. You might think you can just look for people that are trying to gain access to information outside of their program area of expertise. Yet there are legitimate reasons for accessing this information. In many cases the activity you might call suspicious can also be legitimate. Some people are more or less inquisitive and will have different levels of activity in accessing information outside their specific organization. Some of the behaviors on systems vary widely depending on function. Software developer behavior will be very different than an HR person or senior manager. All of these factors need to be taken into account when developing detection capabilities for suspicious activity. We cannot focus on just [whether] a particular action is potentially suspicious. Instead we must quantify the legitimate reasons for the activity and whether this person has a baseline, position, attributes, and history to support the activity.

DARPA did not apparently choose to fund the plan.
Grey areas

The ideas got ever more grandiose. Analyzing malware, HBGary’s main focus, wasn’t enough to keep up with the hackers; Hoglund had a plan to get a leg up on the competition by getting even closer to malware authors. He floated an idea to sniff Russian GSM cell phone signals in order to eavesdrop on hackers’ voice calls and text messages.

“GSM is easily sniffed,” he wrote to Barr. “There is a SHIELD system for this that not only intercepts GSM 5.1 but can also track the exact physical location of a phone. Just to see what’s on the market, check [redacted]… these have to be purchased overseas obviously.”

The note concluded: “Home alone on Sunday, so I just sit here and sharpen the knife.”

Barr, always enthusiastic for these kinds of ideas, loved this one. He wanted to map out everything that would be required for such an operation, including “personas, sink holes, honey nets, soft and hard assets… We would want at least one burn persona. We would want to sketch out a script to meet specific objectives.

And, he noted, “We will likely ride in some grey areas.”

Back to basics

In January 2011, Barr had moved on to his research into Anonymous—research that would eventually do his company in. Over at HBGary, Hoglund continued his pursuit of next-gen rootkits. He had hit on a new approach that he called “Magenta.”

This would be a “new breed of Windows-based rootkit,” said a Magenta planning document, one that HBGary called a “multi-context rootkit.”

The Magenta software would be written in low-level assembly language, one step up from the ones and zeroes of the binary code with which computers do their calculating. It would inject itself into the Windows kernel, and then inject itself further into an active process; only from there would the main body of the rootkit execute.

Magenta would also inject itself routinely into different processes, jumping around inside the computer’s memory to avoid detection. Its command-and-control instructions, telling the rootkit exactly what to do and where to send the information, wouldn’t come from some remote Internet server but from the host computer’s own memory—where the control instructions had been separately injected.

“This is ideal because it’s trivial to remotely seed C&C messages into any networked Windows host,” noted Hoglund, “even if the host in question has full Windows firewalling enabled.”

Nothing like Magenta existed (not publicly, at least), and Hoglund was sure that he could squeeze the rootkit code into less than 4KB of memory and make it “almost impossible to remove from a live running system.” Once running, all of the Magenta files on disk could be deleted. Even the best anti-rootkit tools, those that monitored physical memory for signs of such activity, “would only be of limited use since by the time the responder tried to verify his results Magenta will have already moved to a new location & context.”

Hoglund wanted to build Magenta in two parts: first, a prototype for Windows XP with Service Pack 3—an old operating system but still widely installed. Second, if the prototype generated interest, HBGary could port the rootkit
“to all current flavors of Microsoft Windows.”

Shortly thereafter, Anonymous broke into HBGary Federal’s website, cracked Barr’s hashed password using rainbow tables, and found themselves in a curious position; Barr was also the administrator for the entire e-mail system, so they were able to grab e-mail from multiple accounts, including Hoglund’s.

A world awash in rootkits

The leaked e-mails provide a tantalizing glimpse of life behind the security curtain. HBGary and HBGary Federal were small players in this space; indeed, HBGary appears to have made much of its cash with more traditional projects, like selling anti-malware defense tools to corporations and scanning their networks for signs of infection.

If rootkits, paranoia monitors, cartoons, and fake Facebook personas were being proposed and developed here, one can only imagine the sorts of classified projects underway throughout the entire defense and security industry.

Whether these programs are good or bad depends upon how they are used. Just as Hoglund’s rootkit expertise meant that he could both detect them and author them, 0-day exploits and rootkits in government hands can be turned to many uses. The FBI has had malware like CIPAV (the Computer and Internet Protocol Address Verifier) for several years, and it’s clear from the HBGary e-mail leak that the military is in wide possession of rootkits and other malware of its own. The Stuxnet virus widely believed to have at least damaged Iranian nuclear centrifuge operations is thought to have originated in the US or Israeli governments, for instance.

But the e-mails also remind us how much of this work is carried out privately and beyond the control of government agencies. We found no evidence that HBGary sold malware to nongovernment entities intent on hacking, though the company did have plans to repurpose its DARPA rootkit idea for corporate surveillance work. (“HBGary plans to transition technology into commercial products,” it told DARPA.)

And another document, listing HBGary’s work over the last few years, included this entry: “HBGary had multiple contracts with a consumer software company to add stealth capability to their host agent.”

The actions of HBGary Federal’s Aaron Barr also serve as a good reminder that, when they’re searching for work, private security companies are more than happy to switch from military to corporate clients—and they bring some of the same tools to bear.

When asked to investigate pro-union websites and WikiLeaks, Barr turned immediately to his social media toolkit and was ready to deploy personas, Facebook scraping, link analysis, and fake websites; he also suggested computer attacks on WikiLeaks infrastructure and pressure be brought upon journalists like Glenn Greenwald.

His compatriots at Palantir and Berico showed, in their many e-mails, few if any qualms about turning their national security techniques upon private dissenting voices. Barr’s ideas showed up in Palantir-branded PowerPoints and Berico-branded “scope of work” documents. “Reconnaissance cells” were proposed, network attacks were acceptable, “target dossiers” on “adversaries” would be compiled, and “complex information campaigns” involving fake personas were on the table.

Critics like Glenn Greenwald contend that this nexus of private and public security power is a dangerous mix. “The real issue highlighted by this episode is just how lawless and unrestrained is the unified axis of government and corporate power,” he wrote last week.

Especially (though by no means only) in the worlds of the Surveillance and National Security State, the powers of the state have become largely privatized. There is very little separation between government power and corporate power. Those who wield the latter intrinsically wield the former.

The revolving door between the highest levels of government and corporate offices rotates so fast and continuously that it has basically flown off its track and no longer provides even the minimal barrier it once did. It’s not merely that corporate power is unrestrained; it’s worse than that: corporations actively exploit the power of the state to further entrench and enhance their power.

Even if you don’t share this view, the e-mails provide a fascinating glimpse into the origins of government-controlled malware. Given the number of rootkits apparently being developed for government use, one wonders just how many machines around the globe could respond to orders from the US military. Or the Chinese military. Or the Russian military.
While hackers get most of the attention for their rootkits and botnets and malware, state actors use the same tools to play a different game—the Great Game—and it could be coming soon to a computer near you.

Opening photo illustration contains elements from Shutterstock.
Anonymous vs. HBGary: the aftermath
By Nate Anderson

The RSA security conference took place February 14-18 in San Francisco, and malware response company HBGary planned on a big announcement. The firm was about to unveil a new appliance called “Razor,” a specialized computer plugged into corporate networks that could scan company computers for viruses, rootkits, and custom malware—even malicious code that had never been seen before.

Razor “captures all executable code within the Windows operating system and running programs that can be found in physical memory,” said HBGary, and it then “detonates’ these captured files within a virtual machine and performs extremely low level tracing of all instructions.” Certain behaviors—rather than confirmed signatures—would suggest the presence of malware inside the company.

The HBGary team headed over early to the RSA venue at the Moscone Center in order to set up their booth on the exhibition floor. Nerves were on edge. A week before, HBGary and related company HBGary Federal were both infiltrated by members of the hacker collective Anonymous, which was upset that HBGary Federal CEO Aaron Barr had compiled a dossier of their alleged real names. In the wake of the attack, huge batches of sensitive company email had been splashed across the ‘Net. HBGary employees spent days cleaning up the electronic mess and mending fences with customers.

On the RSA floor, a team put together the HBGary booth and prepared for the Razor announcement. CEO Greg Hoglund prepped his RSA talk, called “Follow the Digital Trail.”
The HBGary team left for the night. When they returned the next morning, the opening day of the conference, they found a sign in their booth. It was from Anonymous.

“We had a lot to think about,” HBGary’s Vice President of Services, Jim Butterworth, told Ars. “We had just spent the previous week trying to clean things up and get ourselves back to normal, harden our systems, [and we] continued to hear the telephone calls and the threats—and I will add, these are very serious threats.”

Now, with the appearance of the note in their RSA booth, the team felt not just electronically exposed; they felt physically threatened and stalked. “They decided to follow us to a public place where we were to do business and make a public mockery of our company,” Butterworth said. “Our position was that we respected RSA and our fellow vendors too much to allow this spectacle to occur.”

Instead, HBgary Inc. pulled out of the conference. ZDNet journalist Ryan Naraine snapped a photo from the show floor:

A group of aggressive hackers known as “Anonymous” illegally broke into computer systems and stole proprietary and confidential information from HBGary, Inc. This breach was in violation of federal and state laws, and stolen information was publicly released without our consent.

In addition to the data theft, HBGary individuals have received numerous threats of violence including threats at our tradeshow booth.

In an effort to protect our employees, customers and the RSA Conference community, HBGary has decided to remove our booth and cancel all talks.

HBGary is continuing to work intensely with law enforcement on this matter and hopes to bring those responsible to justice.

Thank you to all of our employees, our customers and the security community for your continued support.

- HBGary, Inc.
The attacks continue

On Sunday, February 6, the electronic assault had begun in earnest. As America sat down to watch the Super Bowl kickoff, five “members” of Anonymous infiltrated the website of security firm HBGary Federal. They had been probing HBGary Federal and related firm HBGary Inc. since Saturday, but on Sunday they struck gold with an SQL injection attack on HB Gary Federal’s content management system.

They quickly grabbed and decrypted user passwords from the website, which they used to move into HB Gary Federal’s hosted Google e-mail. By the time the attack was through, the hackers had compromised HB Gary Federal’s website, deleted its backup data, took over Greg Hoglund’s rootkit.com site, and locked both companies out of their e-mail accounts by changing the passwords.

While HB Gary Federal was truly “hacked,” HB Gary Inc. was not; attackers simply used existing usernames and passwords to access key systems. HB Gary had in fact hardened its Web defenses, fully patching them on the Thursday before the attack began in anticipation of some unpleasantness. Butterworth told Ars that the company was able to bring down its compromised offsite Web servers within 42 minutes of the attack’s beginning. (He also confirmed the accuracy of our earlier exclusive report on how Anonymous penetrated the two companies.)

Over the last week, this part of the story became well known. What was not visible outside the hallways of HB Gary’s Sacramento offices, however, was just how long the attacks continued. Indeed, although the electronic assault stopped soon after it began, the harassment has yet to end.

Butterworth sounded tired as he recounted the days for us—when we spoke, 17 days had passed since the initial attack. Since then, HB Gary has been flooded with phone calls and voicemails of the “you should be ashamed of yourself!” type and worse; the fax machines have been overwhelmed with Anonymous outpourings; people have been “directly threatening our employees with extortion”; threats have been made. Then came RSA.

Butterworth, with a long career in military signals intelligence and private security firms, is no stranger to the dark world of cyberattacks, but he’s used to adversaries who retreat after an electronic strike.

Instead, he believes that Anonymous has “decided to continue their antics. They’re in it for the laughs… this is a real funny game for them.” Not content with the damage they have inflicted, they “harass a company that’s trying to get back to work.” Each time a new story about the company appears in the press, Butterworth said that these attacks spike again.

“Millions in damages”

The fallout from the whole debacle endures. In the wake of the attack, HB Gary’s Penny Leavy and Greg Hoglund (they are married) entered the Anonymous IRC channel #ophbgary to plead in vain for Greg’s e-mails to stay private. (Several less relevant remarks have been removed from the transcript for easier reading.)

<+greg> so you got my email spool too then

<&Sabu> yes greg.

<@´k> greg we got everything

<+Agamemnon> Greg, I’m curious to know if you understand what we are about?

Do you understand why we do what we do?

<+greg> you realize that releasing my email spool will cause

millions in damages to HB Gary?

<@´k> yes
Asked if HBGary has in fact seen a financial impact from the Anonymous attack, Butterworth would only say, “Time will tell.” He did admit that the hack had an impact on the company—“the tainting of a brand name, a company that has a very good product”—and that “we’ve received indications that folks are having second thoughts” about working with the firm.

The company also had to devote nearly a week of its time to performing client notification, a job that must’ve been anything but pleasant. And Butterworth has been tasked with overseeing HBGary’s internal forensic investigation into the attack. He hopes to compile enough information to eventually prosecute those responsible.

“A lot of federal crime has been committed,” he said.

Despite the fact that the attackers hid themselves behind Tor software and proxy servers, he believes the company stands a “very good chance” of catching the perpetrators.

But what has the attack meant for Anonymous, HBGary Federal’s Aaron Barr, and the security companies linked with Barr’s ideas?

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

loooooooooooooooooooool

owned by anonymous. niiice.

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 don't 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.

<table>
<thead>
<tr>
<th>Palantir</th>
<th>Potential Proactive Tactics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed the fuel between the feuding groups. Disinformation. Create messages around actions to sabotage or discredit the opposing organization. Submit fake documents and then call out the error.</td>
<td></td>
</tr>
<tr>
<td>Create concern over the security of the infrastructure. Create exposure stories. If the process is believed to not be secure they are done.</td>
<td></td>
</tr>
<tr>
<td>Cyber attacks against the infrastructure to get data on document submitters. This would kill the project. Since the servers are now in Sweden and France putting a team together to get access is more straightforward.</td>
<td></td>
</tr>
<tr>
<td>Media campaign to push the radical and reckless nature of wikileaks activities. Sustained pressure. Does nothing for the fanatics, but creates concern and doubt amongst moderates.</td>
<td></td>
</tr>
<tr>
<td>Search for leaks. Use social media to profile and identify risky behavior of employees.</td>
<td></td>
</tr>
</tbody>
</table>

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 HB Gary 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 HB Gary 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 salesman(“‘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 HB Gary 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

HB Gary 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 HB Gary 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 HB Gary 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 HB Gary Federal was a separate company from HB Gary, 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 HB Gary 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.”
Embattled HBGary Federal CEO Aaron Barr quit his job yesterday as the prospect of a Congressional investigation loomed. A dozen Democrats in Congress asked various Republican committee chairs to launch probes of HBGary Federal’s idea for a “reconnaissance cell” targeting pro-union organizers.

HBGary Federal was hacked last month by Anonymous after Aaron Barr believed he had unmasked much of the group’s leadership—and Barr’s entire cache of corporate e-mails was made public. Those messages revealed that Barr had joined up with two other security firms, Palantir and Berico, to pitch the powerhouse DC law firm of Hunton & Williams on an idea to go after union-backed websites who opposed the US Chamber of Commerce. The scheme, if adopted, would have cost the Chamber up to $2 million a month.

The three companies called themselves Team Themis, and instead of providing simple “business intelligence,” they had a few other ideas:

Create a false document, perhaps highlighting periodical financial information, and monitor to see if US Chamber Watch acquires it. Afterward, present explicit evidence proving that such transactions never occurred. Also, create a fake insider persona and generate communications with [union-backed Change to Win]. Afterward, release the actual documents at a specified time and explain the activity as a CtW contrived operation.

- If needed, create two fake insider personas, using one as leverage to discredit the other while confirming the legitimacy of the second. Such work is complicated, but a well-thought out approach will give way to a variety of strategies that can sufficiently aid the formation of vetting questions US Chamber Watch will likely ask.
- Create a humor piece about the leaders of CtW.

Now, some members of Congress want an investigation. “The [Team Themis] techniques may have been developed at US government expense to target terrorists and other security threats,” said a letter signed by the representatives.
“The e-mails indicate that these defense contractors planned to mine social network sites for information on Chamber critics; planned to plant ‘false documents’ and ‘fake insider personas’ that would be used to discredit the groups; and discussed the use of malicious and intrusive software (‘malware’) to steal private information from the groups and disrupt their internal electronic communications.”

Did anything illegal happen? The letter suggests that forgery, wire fraud, and computer fraud might have taken place and that Congress should investigate the ways that private contractors turn their military contracting experience on private targets.

**Going after the lawyers**

Hunton & Williams, the middleman law firm in all this (and the middleman between a major US bank and Team Themis’ similar plan to take down WikiLeaks), has steadfastly refused to comment on the whole story. But it too may find itself in trouble after a [professional conduct complaint](PDF) was lodged against it last week in Washington, DC.

The complaint was filed by Stop the Chamber and Velvet Revolution, two of the groups targeted for the potential Chamber of Commerce campaign. It accuses the three Hunton & Williams lawyers named in the HBGary Federal e-mails of “an extended pattern of unethical behavior that included likely criminal conduct.”

Specifically, they solicited, conspired with and counseled three of its investigative private security firms to engage in domestic spying, fraud, forgery, extortion, cyber stalking, defamation, harassment, destruction of property, spear phishing, destruction of property, identity theft, computer scraping, cyber attacks, interference with business, civil rights violations, harassment, and theft.

Most of this alleged bad behavior was done, of course, by Team Themis and not by Hunton & Williams. Still, they reviewed (and appear to have had no problems with) the material. As the complaint puts it, “none of the H&W lawyers ever expressed any reservation or doubt about the unethical conduct proposed and committed by their investigators. In fact, they actively solicited and approved everything that was proposed and presented.”

The complaint asks the DC Board of Professional Responsibility to strip all three Hunton & Williams lawyers of their licenses.
Credits

Copyright Information
Copyright Condé Nast. The following disclaimer applies to the information, trademarks, and logos contained in this document. Neither the author nor Condé Nast Digital make any representations with respect to the contents hereof. Materials available in this document are provided “as is” with no warranty, express or implied, and all such warranties are hereby disclaimed. Condé Nast Digital assumes no liability for any loss, damage or expense from errors or omissions in the materials available in this document, whether arising in contract, tort or otherwise. The material provided here is designed for educational use only. The material in this document is copyrighted by Condé Nast Digital, and may not be reprinted or electronically reproduced unless prior written consent is obtained from Condé Nast Digital. Links can be made to any of these materials from a WWW page, however, please link to the original document. Copying and/or serving from your local site is only allowed with permission. As per copyright regulations, “fair use” of selected portions of the material for educational purposes is permitted by individuals and organizations provided that proper attribution accompanies such utilization. Commercial reproduction or multiple distribution by any traditional or electronic based reproduction/publication method is prohibited. Any mention of commercial products or services within this document does not constitute an endorsement. “Ars Technica” is trademark of Condé Nast Digital. All other trademarks and logos are property of their respective owners.
Table of Contents

Cover
Unmasked
1 You've Angered the Hive
2 How One Man Tracked Down Anonymous
3 Virtually Face to Face
4 Spy Games
5 Anonymous Speaks
6 Black Ops
7 The Aftermath
8 Dems Push for Investigation
credits and legal