Anonymous vs. HBGary: the aftermath

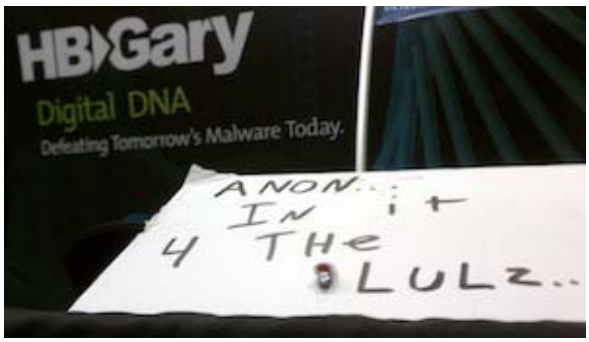
By Nate Anderson | Published 7 months ago

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 e-mail 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."



At RSA: "Anon: In it 4 the lulz..."

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:

HBGary's withdrawal note
ZDNet

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 HBGary Federal's content management system.

They quickly grabbed and decrypted user passwords from the website, which they used to move into HBGary Federal's hosted Google e-mail. By the time the attack was through, the hackers had compromised HBGary 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.

The HBGary saga:

Anonymous to security firm working with FBI: "You've angered the hive"

How one security firm tracked down Anonymous—and paid a heavy price

(Virtually) face to face: how Aaron Barr revealed himself to Anonymous

Spy games: Inside the convoluted plot to bring down WikiLeaks

Anonymous speaks: the inside story of the HBGary hack

Black ops: How HBGary wrote backdoors for the government

While HBGary Federal was truly "hacked," HBGary Inc. was not; attackers simply used existing usernames and passwords to access key systems. HBGary 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 HBGary'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, HBGary 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, HBGary'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 HBGary?

<@`k> yes

<+c0s> greg: another reason its not out yet.

<+Agamemnon> yes we do greg

<@`k> greg is will be end of you :) and your company
```

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?