http://hbgary.anonleaks.ch/aaron_hbgary_com/9303.html HBGary Federal CEOAaron Barr to Northrop Grumman Senior VP Intelligence Division Tom Conroy 3 Dec 2009 POSTED: Barr/Conroy
==

Tom,

First I just have to say...I have not had this much fun since Ted and I were working with you to win Romas and Bluebird. I spent the last few days at the AFCEA solutions conference and had lots of folks, government and industry, wanting to talk with me. HBGary, and this is as unbias as I can make it, has some amazing technology that I think will be very significant in the near future. Their Malware Genome and Digital DNA products are the future of cyber protection, based on behavior and characteristics of malware, and they work. Right now we have a malware genome of 3500 traits/characteristics and it catches 75% of all malware, including zero day attacks.

I have been working with Palantir and Xetron to develop this group that is going to try and tackle some bits of Attribution. I received some advise from some NSA folks at the conference to also include Carnegie Melon as they are just starting a similar effort for NSA, so I will reach out to them.

Brian Masterson will probably reach out to you for some advice/direction. Xetron is very worried about IS. My EXTERNAL opinion, IS has lost or never had its way for cyber, Xetron is the best thing Northrop has going and they are hungry to make a difference. I told Brian you would be an advocate as much as you could. For that matter, having gone around these last few weeks talking with various companies (GD, SAIC, CSC, Mantech) Northrop is drastically falling behind in cyber. Northrop has hitched its wagon to NCR and TU, both of which are the absolute wrong things to develop a successful cyber strategy on. Just my opinion.

I am meeting with Bill Luti Monday morning. I am extremely curious what he wants to talk about, looking forward to it.

Aaron

==
http://hbgary.anonleaks.ch/aaron_hbgary_com/5594.html Aaron Barr to John Jolly, cc: Tom Conroy 4 Dec 2009 Note NSA staff member Ralph Denty and possible involvement of Carnegie Mellon developing software for the NSA.
POSTED:Barr/Conroy
==

John,

Not sure if you know, but I am no longer with Northrop. My current position is as CEO of HBGary Federal, a wholly owned subsidiary of HBGary. HBGary builds malware detection and analysis products. Their history is steeped in Forensics, but their recent products and technology roadmap is focused more on malware detection and incident response.

Specifically a product launched last spring called Digital DNA and another product launched last month called ReCON. They currently have a malware genome with 3500 traits/characteristics identified. Using their memory capture and analysis tools they look at the function and behavior of software and compare that to the malware genome and attribute a threat score indicating the likely hood of it being malware. Using the genome they are also doing comparisons of malware for authorship identification. I think this has possibilities for attribution if linked with capabilities like Palantir. I am currently in discussions with Palantir to partner on an attribution based capability. Currently we claim 75% identification of zero day malware and believe further build outs of the genome and partnerships with other technologies will get us into the 80-90% range.

I spoke to Ralph Denty from NSA cybersecurity operations integration, he is putting me in contact with some folks from Carnegie Melon, who have been recently charted by NSA to look at developing something similar. We also have a current partnership with Mcafee and have integrated Digital DNA into their ePO product which is currently the base for HBSS.

My question is is their any interest from a TU perspective, specifically Tutiledge, in including this type of capability? I think there are some longer term efforts on forward deployed systems using this type of methodology that could eventually detect evolutions of attacks and develop defensive capabilities against them before they ever reach you systems.

Aaron Barr
CEO
HBGary Federal Inc.

==
http://hbgary.anonleaks.ch/aaron_hbgary_com/15025h.html Tom Conroy to Aaron Barr 26 Jan 2010. Note introduction of House staff member Jacob Olcott. Note presence of Endgame Systems, Netwitness, and Splunk in addition to HBGary Federal, Palantir, and Berico.
POSTED:Create Spy Coalition
==

It is pretty impressive. Now think of our opponents who are unfettered by government constraints, and in fact are encouraged to be as entrepreneurial as they can be. And overlay that with the number of smart people they have available to advance their cause, combined with enthusiasm for success unfettered by high expectations of wealth. It's

downright scary. In the long run we'll likely have to make fundamental changes in the way the internet is implemented to close ALL the loopholes to hacking, something not likely in our lifetime but essential
to security I would think.

From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Monday, January 25, 2010 11:38 PM
To: Conroy, Thomas W.
Cc: Barnett, Jim H.
Subject: Fwd: Idea

I love being able to do stuff like this now.

I sent an email back to Jake suggesting that our consortium could be the
fast moving prototype capability to his non-profit. We will see how the
conversation progresses.

Aaron

Begin forwarded message:

From: "Olcott, Jacob" <Jacob.Olcott@mail.house.gov>

Date: January 25, 2010 11:46:15 AM EST

To: "Aaron Barr" <aaron@hbgary.com>

Subject: RE: Idea

Aaron - sounds cool! We've actually been discussing an approach like this on the CSIS commission lately (the idea they've been hashing around
is how to achieve greater situational awareness, but they've been proposing a non-profit agency to allow everyone to access specific information).
Would like to discuss with you - busy this week and next, but maybe early Feb?

-----Original Message-----
From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Friday, January 22, 2010 8:49 AM
To: Olcott, Jacob
Subject: Idea

Jake,

I have put together a subset of highly capable companies for the purposes of improving threat intelligence, believing that we have to improve our knowledge of the threat before we can improve our security. Once we have a better threat picture we integrate more proactive/reactive security capabilities and more effectively manage enterprise security based on our knowledge of the threat.

A good cyber intelligence capability needs to cover and integrate all areas of cyber: executable, host, network, internet, and social analysis. These companies represent a best of breed, complete end-to-end cyber intelligence picture. Using Palantir as the framework for organizing the data feeds from the other companies and overlaying that data with other social network analysis.

Application - HBGary (automated malware detection based on traits and code fingerprinting)
Host - Splunk (host based security monitoring)
Network - Netwitness (Network Forensics, full textual analysis)
Internet - EndGames (External network monitoring, botnet C2 monitoring, zero days)
Social - Palantir (link analysis framework for intelligence)

I am bringing these companies together in an consortium, they have all bought in. Rather than a typical integrator model, keeping the product companies at arms length, a consortium puts us all on a more level playing field and forces us to think about the right solution rather than a particular offering.

As we talked about before. There are significant organizational and contractual impedance's from bringing together the necessary pieces to enhance our cybersecurity. So it occured to me, why not do for cyber intelligence what Space-X did for space exploration and satellite deployments. Forget the bureaucracy, develop the complete solution externally from the mad house. The individual products from these companies alone are significant, imagine what can be produced once we integrate them.

What do you think?

===

http://hbgary.anonleaks.ch/aaron_hbgary_com/6934.html from Northrop Grumman executive Jim Barnett to Aaron Barr 27 Jan 2010. Offer from House staffer Jacob Olcott permitting them to write U.S. cyber security legislation under discussion.
POSTED:Barr/Conroy

===

Now that's a trick question...us (assume you mean NGC...no "I" in us) and Aaron? I am not certain those are seperable, good news. But beyond the fun and chaos, I would let Aaron run and not engage NGC...perhaps Jacob has Larry, or Linda, or Kathy, or Tim on his list...but we probably won't hear from them.
What we could do, for NGC, is alert them to the bill and pending action and let the NGC system engage...it's Wednesday and there is an EXCOM tommorrow.
I like Jacobs approach...he is right about the window...thoughts for AAron SEPCOR.

From: Conroy, Thomas W.
To: 'aaron@hbgary.com' <aaron@hbgary.com>; Barnett, Jim H.
Sent: Wed Jan 27 18:00:55 2010
Subject: Re: Fwd: request for amendments - cyber bill

Jim -
How do we get the best result from this, both for Aaron and for us?

From: Aaron Barr <aaron@hbgary.com>
To: Conroy, Thomas W.; Barnett, Jim H.
Sent: Wed Jan 27 17:55:33 2010
Subject: Fwd: request for amendments - cyber bill

Wow. Any thoughts? I have some work to do.

Aaron

From my iPhone

Begin forwarded message:

From: "Olcott, Jacob" <Jacob.Olcott@mail.house.gov>
Date: January 27, 2010 6:45:14 PM EST
To: "Olcott, Jacob" <Jacob.Olcott@mail.house.gov>
Subject: request for amendments - cyber bill

One of the interesting things about working for Congress is that you can go long stretches of time where you never seem to have traction on an issue, and then suddenly a window of opportunity presents itself and you have a brief moment to take advantage of it. This is one of those moments for cybersecurity here in the House of Reps.

Several months ago, the Science and Technology Committee marked up a Cyber R&D bill. You can find the bill here: <http://www.rules.house.gov/111/LegText/111_hr4061_txt.pdf> http://www.rules.house.gov/111/LegText/111_hr4061_txt.pdf. As you can tell, this was a fairly noncontroversial bill. The Speakerâ€™s office decided today that they want this bill on the floor next week (likely Wednesday or Thursday).

Hereâ€™s how the procedure works. Members are allowed to write amendments to the bill. They submit them to the Rules Committee. On Monday night, the Rules Committee will consider those amendments, and rule them either â€œin orderâ€� or â€œout of order.â€� Amendments are supposed to be â€œgermaneâ€� to the section of the bill that is being amended (there is a test for this, but basically an amendment has to relate to the subject matter under consideration). Amendments that are ruled â€œin orderâ€� can then be raised by that member on the floor â€“ and put to a vote of the House.

As you can see from the text, the bill contains provisions on R&D, cyber workforce, strategic planning, social and behavioral cyber research, the focus of NSF grants, scholarship for service, NIST research, international standards, identity management, cyber awareness into legislation. Lots of good and interesting subjects that can be improved and enhanced through the amendment process. For those looking for an opportunity, this is a great way to address some of these issues in a bill that will be voted on by the House of Representatives.

Members have already been asking me for amendments, and I am busy drafting. You are a trusted ally, and I would really appreciate if you can take a look at this bill, see if you have some ideas about ways to improve it, and send them to me. Please be creative! I will take your submissions, turn them into amendment language, and send them to members who are interested in amending this bill.

Sorry for the late notice, but I need your proposals by not later than FRIDAY at NOON. If youâ€™re not comfortable drafting an amendment, feel free to submit an â€œideaâ€� to me and I will do my best to turn it into legislative language that the members can use.

Thanks for your help.

Jake

Jacob Olcott

Subcommittee Director and Counsel

Emerging Threats, Cybersecurity, S&T Subcommittee

Committee on Homeland Security (Majority)

202-226-2623

==

http://hbgary.anonleaks.ch/aaron_hbgary_com/783.html Jim Barnett to Aaron Barr 27 Jan 2010. Discussing how to use access in House via Jacob Olcott to steer earmarks to fund their scheme. Excerpt for brevity
POSTED: unclasified

==

Sure...but you need to think about how you want to "steer" this to an appropriation mark reflective of a members ammendment.
Jacob is pro staff who has the ability to influence members on his committee and specifically sub...review those members and then look for a "constituency angle" and write accordingly.
You can take the "good government" approach but that's too easy.
Let me know if I can help.
Jim

http://hbgary.anonleaks.ch/aaron_hbgary_com/14481h.html Aaron Barr to Tom Conroy 29 Jan 2010. Describing language to be inserted into cybersecurity bill, reference to direct communication with Jacob Olcott included inline.
POSTED: Barr/Conroy
===

How about carribean breeze.
4100 N Fairfax Dr
Arlington, VA 22203

Aaron

From my iPhone

On Jan 29, 2010, at 6:38 AM, "Conroy, Thomas W." <Tom.Conroy@ngc.com> wrote:

On your way into DARPA today, pick a convenient restaurant and send me a quick email. I'll come to you and that will minimize your time away from the session. And if it looks too good to leave, let me know and we'll reschedule.
Tom

From: Aaron Barr <aaron@hbgary.com>
To: Barnett, Jim H.; Conroy, Thomas W.
Sent: Fri Jan 29 05:09:39 2010
Subject: Fwd: Input

Here is the input I sent in.

Aaron

From my iPhone

Begin forwarded message:

From: Aaron Barr <aaron@hbgary.com>
Date: January 29, 2010 6:02:39 AM EST
To: Jake Olcott <Jacob.Olcott@mail.house.gov>
Subject: Input

Jake,

I wish I had more time. But here is some input. Hope it helps. Let me know if there is anything else I can do.

Aaron

SEC 103. CYBERSECURITY STRATEGIC RESEARCH AND DEVELOPMENT PLAN

Describe how the program will incentivize the collaboration of academia, small and large businesses to work together to develop more significant capabilities. (my point here is there is lots of talent, capability, overlap, but often they don't collaborate for reasons of market share, territory, etc). Grants for innovative integration. Small companies are laser focused on immediate revenue and growth. Difficult to get them to think about collaboration.

Describe how the program will provide access to government mission sets and information for the purposes of real world research, development, and testing. (In many cases, you might have good ideas, good technology but you need a real world environment/data to test against which is difficult to get unless you secure a contract).

Describe how the programs national research infrastructure will provide expertise to mission owners on the effectiveness of new technologies. (It would be effective to have a technology shop that could provide the real world testing on new technologies and provide expert opinion to the government on technology effectiveness)

Describe how the program will facilitate development and implementation of newly developed technologies. Once you have a new technology then you have to go sell it, which can be a matter of contacts, etc, things that don't have anything to do with the quality of the technology.

Describe how the program will develop a national challenge based on priorities to effectively evaluate and reward best in class capabilities in those areas referenced. How can we innovatively foster the creation of new ideas. Provide a national challenge in different areas at a government sponsored cybersecurity event. This would allow virtual nobodies that have developed amazing capability to get instant recognition and exposure.

SEC. 104. SOCIAL AND BEHAVIORAL RESEARCH IN CYBER-SECURITY

Develop a program to incentivize people to think and act more securely in how the use systems, and develop systems.

Develop incentives to more effectively share cybersecurity related information amongst government, academia, and industry.

Programs to inform public of compromised systems, attack types, methods. More publicly digestible information on the threats and methods of attack.

SEC. 105. NATIONAL SCIENCE FOUNDATION CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAMS

SEC. 106. FEDERAL CYBER SCHOLARSHIP FOR SERVICE PROGRAM

SEC. 107. CYBERSECURITY WORKFORCE ASSESSMENT

Incentivize industry and government to bring on college students part time in larger numbers, mechanisms to get them in the clearance process, get them experience, introduced to what is actually happening in the national cybersecurity efforts.

Develop a set of cybersecurity programs; to teach general users, acquisitions forces to help them write cyber requirements, and more technical for personnel who work on the systems so they better understand both why and how to secure systems.

Develop technical coaching and mentorship programs to grow the current base into technical experts.

SEC. 108. CYBERSECURITY UNIVERSITY-INDUSTRY TASK FORCE

Develop a program to tie university research to industry sponsorships. I sat through the review of a bunch of academic papers and it was obvious the are technically sharp but operationally ignorant..get them involved more effectively in working on industry R&D.

SEC. 109. CYBERSECURITY CHECKLIST DEVELOPMENT AND DISSEMINATION

SEC. 110. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY RESEARCH AND DEVELOPMENT

Develop cybersecurity taxonomy and metrics standards.

Develop standards for research, engage international communities, establish more cross functional committees and act as government POC to track all cyber related research (allowing agencies to quickly see what is being done and facilitate collaboration).

Continually assess gaps in cyber defense research, development and implementation. Annual assessments of cyber intrusions and investigations/remediation. Publicly available documentation.

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/2483h.html Jim Barnett to Aaron Barr 29 Jan 2010, revealing they will influence the Senate side and naming Tim McKnight, who seems to be either an NG employee or perhaps a Senate staffer. This is an excerpt. POSTED: Barr/Conroy

===

Good stuff Aaron...

Just so ya know...it looks like NGC will duck on this one...see what "companion" shows up on the Senate side...see if they can figure out what they want to do to influence that for conference.

As it turns out, Tim McKnight was also part of Jacob's outreach so there was discussion within the corporation but not much real action.

Jim

Jim Barnett to Aaron Barr 29 Jan 2010, revealing they will influence the Senate side and naming Tim McKnight, who seems to be either an NG employee or perhaps a Senate staffer.
Jim Barnett to Aaron Barr 29 Jan 2010, revealing they will influence the Senate side and naming Tim McKnight, who seems to be either an NG employee or perhaps a Senate staffer. Tom Conroy to Aaron Barr, cc: Brian Masterson, CTO of Northrop Grumman division Xetron 11 Feb 2010

===

Brian - Were you aware? Are there any issues here we should be aware of?
Aaron - Gathering momentum, hopefully. Hope we can all make it through the snow.

From: Thompson, Bill (Xetron)
Sent: Thursday, February 11, 2010 1:57 PM
To: Conroy, Thomas W.
Cc: Jadik, John; Simoni, Martin P. (Xetron)
Subject: HBGary Federal

Tom,

I just found out that you have a meeting set up with Aaron Barr from HBGary Federal tomorrow afternoon. We have been working with Aaron to define the subject effort for some time and I would like to attend the meeting if you feel that it is appropriate. I was not able to get you by phone to discuss. Therefore, I am going to plan on attending unless I hear otherwise.

Please let me know if this presents a problem,

Bill Thompson
Manager - Cyber Solutions
Northrop Grumman - Xetron

http://hbgary.anonleaks.ch/aaron_hbgary_com/178h.html Tom Conroy to Aaron Barr 22 Feb 2010. Xetron apparently competes with Northrop Grumman staff at a location known as Millersville. Conroy helps him navigate the choppy corporate waters.
POSTED: Barr/Conroy

Phew. Heavy. I'm on my way to the Leadership Conference and I'll try to carry the message.

From: Aaron Barr <aaron@hbgary.com>
To: Conroy, Thomas W.
Sent: Mon Feb 22 15:27:17 2010
Subject: Re: Millersville

Phrases were they don't understand/listen to the customer, and are not producing anything of value. This came from folks from GMU, a few small companies, AGNOSC, Sourcefire. It was just shocking to get that much negative input in a short period of time. I figured there was not a lot of recourse but thought it was feedback you should hear.

Meeting with Xetron went very well. I was impressed with NGES Information Geometry capability. I had a meeting with Mike Van Putte today and discussed our Threat Intelligence concept. He was interested in our approach but it sounded to evolutionary for his funding. A few other government folks, that were sitting with him that represent part of the end customers for the cyber genome, caught us later and said what we were developing was exactly what was needed and no one is approaching it that way. Good input. We will continue to press.

Aaron

On Feb 22, 2010, at 4:20 PM, Conroy, Thomas W. wrote:

Do you get a sense for what causes the negative feelings? People (most likely), which ones, and what is the antibody producing behavior?

Probably not much we can do about it though, short of new management.

How did your trip to Zetron go?

From: Aaron Barr <aaron@hbgary.com>
To: Conroy, Thomas W.
Sent: Mon Feb 22 14:56:11 2010
Subject: Millersville

Tom,

I have been getting a lot of negative feedback about Millersville in talking with a lot of different companies, universities, and government at the DARPA Cyber Genome industry day. This conversation starts with me talking about partnering with Northrop working on some threat intelligence capabilities (generic). Once I mention its with Xetron not Millersville the tone changes. Just thought it was good information to share with you.

Aaron Barr

CEO
HBGary Federal Inc.

Aaron Barr
CEO
HBGary Federal Inc.

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/2410.html Tom Conroy to Aaron Barr, introducing Brian Hibbeln at osd.mil 8 Jul 2010. Conroy reveals he met Barr when he was at TASC and Barr was an NG employee. NG acquired then later sold TASC. OSD is the Office of the Secretary of Defense.
POSTED: Magpii

===

Aaron and Brian -

Allow me to introduce you to each other.

Brian, I worked with Aaron while I was at TASC and he was my go to person in establishing some of the most unique and highly successful internet programs for the IC that I know of. He and his team produced some truly remarkable and extremely innovative capabilities that have changed the way the Agency does business.

Aaron and I had lunch yesterday and he has left TASC and Northrop Grumman and is now with a small company (HB Gary) developing a similarly innovative and value adding capability for them across a broader range of customers. Knowing how you value talent and capability, and are able to bring together just the right mix of users, visionaries, and funding sources, I realized you two would be like catalysts in a mix of free hydrogen and free oxygen. Heat, light, and explosive impacts will almost certainly result.

Please get in direct contact and see if you don't agree this is a partnership made in heaven.

Good luck to you both.

Tom

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/3682.html Aaron Barr to Tom Conroy 2 Aug 2010. Meeting with InQTel & FBI.
POSTED: Barr/Conroy

Tom,

Nice to see you today. As always I will look to build capabilities that make a difference and will look to those organizations that I know to support efforts as they arise.

I wanted to share a dialog I had with the CEO of HBGary proper regarding the future of cybersecurity.... I would be interested in your thoughts. I am meeting with InQTel next week, talking with MITRE, and the FBI. Working to develop a standard for threat intelligence, a threat repository, a methodology to share information on threats. There are not many people that seem to understand both security and path of technology. Threats are llke, they take the path of least resistance, but inevitably with time, they are successful. We still believe we can build better mousetraps... we can't. The only way to get ahead of the problem is what I discuss below. I am just struggling to implement. In Northrop I was too encumbered by a bureaucracy. In a small business I am, well small. I know influential people... well you know the challenges. (PS. I haven't forgot about the news idea, just been busy trying to make payroll. :)) I called today and am waiting to hear back from the contact you gave me. Greg Hoglund and I are beginning to write a book about the future of technology and security that has this as the skeleton.

The trajectory of technology = Mobility + Social + Cloud

This = perimeterless environment, + promiscuous networking + open PII.

Computer security is not possible, not remotely given the current trajectory of security. Even host based behavioral detection can not keep up with this without significant additional capabilities. I see only two paths to improving this. As the stakes are raised to organized crime and nation state FIS (Foreign Intelligence Services) anything is possible. Backbone compromises, Supply Chain compromises, specialized insider threats, legitimate commercial services.

Choices to better security.
Complete rework of the computer and communications architecture. (not likely and certainly not within 5 years). There are some technologies short of this that will help; broad distribution and management of personal certs and pervasive encryption. But the implementation of this is a bugger. Again long ways away.
or
Intelligence, Incident Response, and IO.

The area Incident Response requires some clarification because I don't mean it in the traditionally understood sense. I mean human and system response to abnormal cyber conditions. I mean system and mission resiliency in the face of compromise and attack. This requires good intelligence, we can improve human and system response with better intelligence.

IO requires some intelligence but is more a feeder to intelligence. All offense all the time. Forward deployed and embedded capabilities that can give us insight, I&W, knowledge of threats, their intent and capabilities. This is a blended approach of all of the capabilities available. Coordinated campaigns

Intelligence. This is a bugger. Some of it because of organizational and bureaucratic boundaries. Some of it is we just don't know how to organize the data. Threats are complex as we have discussed. How do you develop a threat focused intelligence capability?

Aaron Barr
CEO
HBGary Federal Inc.

http://hbgary.anonleaks.ch/aaron_hbgary_com/8618.html Tom Conroy to Aaron Barr 6 Aug 2010. Seeking a meeting with Dawn Meyerriecks at Director of National Intelligence. Cassie is Conroy's administrative assistant.
POSTED: Barr/Conroy

I want to schedule a meeting for you and me with Dawn Meyerriecks, DDNI/Acquisition and Technology, ASAP. Call me with your general calendar constraints and I'll see what I can do. Cassie is out so we're
both in a world of hurt.

Tom

==

http://hbgary.anonleaks.ch/aaron_hbgary_com/9109.html Aaron Barr to Tom Conroy 12 Aug 2010. This goes to the level of the Deputy Director of the NSA. Kind of a faux pas here, proper spooks were very careful to keep stuff out of email, Barr on the other hand is quite messy.
POSTED: Barr/Conroy

==

Sent from my iPad

Begin forwarded message:

From: <paula.bucher@dni.gov>
Date: August 12, 2010 9:01:41 AM EDT
To: <aaron@hbgary.com>
Subject:* *Meesage from Dawn Meyerriecks

Mr. Barr,

Dawn asked me to pass this message to you.

The information has been passed to the Deputy Dir of NSA and someone
will be
contacting you.

Paula H Bucher

Executive Assistant for the

DDNI Acquisition and Technology

703-275-3240

http://hbgary.anonleaks.ch/aaron_hbgary_com/4307.html Aaron Barr to Tom Conroy. 18 Aug 2010. The "folks up north" refers to the National Security Agency, based at Fort George Meade, between Washington D.C. and Baltimore. HBGary Federal's offices are southwest of D.C.
POSTED: Barr/Conroy
==

Hi Tom,

I just wanted to close the loop on the conversation. I got a call late last week and gave the folks up north a call on a secure line, gave them my information in detail. They said if they had any follow up that was needed they would give me a call. So I think that is it.

Something that occurred to me. Maybe they are ok with the level of information that is discernible? This whole thing, if not a fluke, is very interesting in that it happened, was allowed, etc. Maybe a current change? No need to take unnecessary risks though.

Aaron

http://hbgary.anonleaks.ch/aaron_hbgary_com/12950h.html 20 Aug 2010. Aaron Barr reveals to Tom Conroy that Dawn Meyerriecks is introducing him to Lisa J. Porter on the ugov portal. This system is a cross agency information sharing portal.
POSTED: Barr/Conroy
==

FYI...

Sent from my iPad

Begin forwarded message:

From: <dawn.meyerriecks@dni.gov>
Date: August 20, 2010 6:12:01 PM EDT
To: <lisa.j.porter@ugov.gov>, <aaron@hbgary.com>
Subject: *e-Intro*

Lisa -

Aaron is the individual I mentioned that came to me with the interesting code fragment analysis.

Aaron -

Lisa is the brilliant scientist we are lucky to have running IARPA.

Thought you two might have an interesting conversation. J

Thanks! Dawn

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/4012.html Aaron Barr to Tom Conroy 18 Nov 2010. This is speculative – is what they were reporting to the NSA earlier the discovery of Stuxnet?

==

FYI. Did you have more insight on this?

Aaron

Stuxnet Virus Now Biggest Threat To Industry<http://rss.slashdot.org/~r/Slashdot/slashdot/~3/v_lDuabXF_Q/story01.htm>

digitaldc writes "A malicious computer attack that appears to target Iran's nuclear plants can be modified to wreak havoc on industrial control systems around the world, and represents the most dire cyberthreat known to industry, government officials and experts said Wednesday. They warned that industries are becoming increasingly vulnerable to the so-called Stuxnet worm as they merge networks and computer systems to increase efficiency. The growing danger, said lawmakers, makes it imperative that Congress move on legislation that would expand government controls and set requirements to make systems safer."

<http://www.facebook.com/sharer.php?u=http%3A%2F%2Fit.slashdot.org%2Fstory%2F10%2F11%2F18%2F140253%2FStuxnet-Virus-Now-Biggest-Threat-To-Industry%3Ffrom%3Dfb>
<http://twitter.com/home?status=Stuxnet+Virus+Now+Biggest+Threat+To+Industry%3A+http%3A%2F%2Fbit.ly%2FaS9Pci>

Read more of this story<http://it.slashdot.org/story/10/11/18/140253/Stuxnet-Virus-Now-Biggest-Threat-To-Industry?from=rss>at Slashdot.

<http://da.feedsportal.com/r/83966956716/u/49/f/530758/c/32909/s/fc47320/a2.htm>

Sent from my iPad

This fragment has been much quoted and finding the original on hbgary.anonleaks.ch has been problematic. Aaron Barr admits to sticking his penis into the Anonymous hornets nest, informing Dawn Meyerriecks at the Director of National Intelligence on 28 Jan 2011.

Hi Dawn,

I have been doing some research on the Anonymous group of wikileaks fame for an upcoming presentation. I have put together what I believe is a significant data set on this group, how it's organized, individuals. I shared some of this with Tom and he recommended that I should mention this to you to see if there is any interest in discussing my results, methodologies, and significance of social media for analysis and exposure.

Aaron

This fragment has also been quoted to death. Conroy instructed Barr to get him a clean, coherent message as to what he had on Anonymous. This is the result.

==

Tom,

I have been researching the Anonymous group over the last few weeks in preparation for a social media talk I will be giving at the BSIDES conference in San Francisco on Feb. 14th. My focus is to show the power of social media analytics to derive intelligence and for potential exploitation. In the talk I will be focusing how effective it is to penetrate three organizations, one military (INSCOM), one Critical Infrastructure (Nuclear PowerPlant in PA), and the Anonymous Group. All penetrations passed social media exploitation are inferred (i.e. I am not delivering any payload).

I am surprised at the level of success I am having on the Anonymous group. I am able to tie IRC Alias to Facebook account to real people. I have laid out the organizations communications and operational structure. Determined the leadership of the organization (mostly - some more work here to go).

I have to believe this data would be valuable to someone in government, and if so I would like to get this data in front of those that are interested prior to my talk, as I imagine I will get some press around the talk and the group will likely change certain TTPs afterwards.

Thanks for your help.

Aaron

http://hbgary.anonleaks.ch/aaron_hbgary_com/6449h.html Aaron Barr to Tom Conroy 29 Jan 2011. Bill Wansley is a very senior executive at Booz Allen Hamilton. Mike McConnell has not been identified to our knowledge.
POSTED: Barr/Conroy

===

Tom,

I forgot to mention. I had a meeting yesterday with Bill Wansley over at Booz yesterday. He said Mike McConnell is walking around like the cat that got the canary because their is something to happen or be released soon that is very significant in the cyber arena. Any knowledge?

Aaron

http://hbgary.anonleaks.ch/aaron_hbgary_com/9394.html Tom Conroy to Aaron Barr 6 Feb 2011. Speculating that the model of an offshore intel operation collecting data and selling it to the government is the correct way to circumvent privacy laws.
POSTED: Barr/Conroy

Do you suppose there might be a market for an offshore intel gathering organization that would sell results?

-----Original Message-----
From: Aaron Barr <aaron@hbgary.com>
Date: Fri, 4 Feb 2011 20:50:08
To: <conroy.tom@gmail.com>
Subject: Re: Research Data

BTW,

The conversation was very interesting today. The admit they had no idea this was happening until it hit the streets. They have no idea how to manage things like this in the future. And the agree they are not capable of doing the right activities (like I did) to be better prepared in the future because of authority and policy restrictions.

So I gave them a model that might work. I will do the work based on my understanding of need on my dime... put together a report... and sell them the report.

They liked that. I am working up 5 slides to hopefully brief Glenn next Friday.

Aaron

On Feb 4, 2011, at 8:46 PM, Tom Conroy wrote:

> Any chance you would be OK dragging me along to visit Dawn. Its not necessary and it is purely selfish of me to ask, but.... What do you think?
> From: Aaron Barr <aaron@hbgary.com>
> Date: Fri, 4 Feb 2011 20:05:18 -0500
> To: Tom Conroy<conroy.tom@gmail.com>
> Subject: Fwd: Research Data
>
> Interesting Day.
>
> So I have been contacted by OSD (Rosemary), FBI, USG, and now DNI...all today.
>
> I have a meeting with FBI/OSD Monday @ 11am.
>
> Met with some folks at my old customer today (I should fill u in on that).
>

> And looks like a meeting to be set up with Dawn...
>
> Let me know if you would like to get together.
>
> Aaron
>
>
> Begin forwarded message:
>
>> From: <dawn.meyerriecks@dni.gov>
>> Date: February 4, 2011 7:56:55 PM EST
>> To: <aaron@hbgary.com>
>> Cc: <conroy.tom@gmail.com>, <catherine.m.white@dni.gov>
>> Subject: RE: Research Data
>>
>> Yes....always enjoy our chats and would be interested in an update on our other conversation. I've cc:-ed Cathy, who can set this up.
>>
>> Thanks! Dawn
>>
>> -----Original Message-----
>> From: Aaron Barr [mailto:aaron@hbgary.com]
>> Sent: Friday, January 28, 2011 5:37 PM
>> To: Dawn Meyerriecks
>> Cc: Tom Conroy
>> Subject: Research Data
>>
>> Hi Dawn,
>>
>> I have been doing some research on the Anonymous group of wikileaks fame for an upcoming presentation. I have put together what I believe is a significant data set on this group, how it's organized, individuals. I shared some of this with Tom and he recommended that I should mention this to you to see if there is any interest in discussing my results, methodologies, and significance of social media for analysis and exposure.
>>
>> Aaron
>

We've read this several times since it was released.

Conroy worked at TASC and Barr was his contact at Northrop Grumman. NG bought TASC in 2001 and sold it in 2009.

http://www.tasc.com/about_us/history/

Barr viewed Conroy as a mentor and consulted him frequently. Conroy was planning leave NG and did so at the end of 2010, landing at an unnamed company in the D.C. area that helped him to keep his clearances.

Conroy, assisted by Barnett, both of Northrop Grumman, were introducing HBGary Federal around, apparently with an eye on using a more nimble private company to circumvent both their own employers stodgy approach as well as U.S. laws regarding privacy, intelligence gathering, and various fraud statutes that cover what the military refers to as “information operations”.

The U.S. government was caught flat footed by the vigorous defense Anonymous offered when actions were taken against Wikileaks. They had expected to shut the Wikileaks operation down quickly and discredit what was released. Wikileaks survived, distributed itself, and when HBGary went after Anonymous the situation got dramatically worse.

That ends what can be discerned from reading the 164 messages either to or from Conroy that were found in Aaron Barr’s mailbox.

What is known from revelations over the last few days is that th3j35st3r (The Jester), the Islamophobic U.S. Nationalist hacking group, has also made the mistake of engaging Anonymous. Two of the members have been outed as the 2010 winners of the DoD Cyber Crime Center’s forensic challenge. There are hints in other messages in Barr’s inbox that indicate they were in contact with DC3.

The story of Anonymous and HBGary is far from over …