1/7/2010 4:57 PM Steckman to Barr First mention of IARPA asking for an intelligence platform.

http://hbgary.anonleaks.ch/aaron_hbgary_com/10180.html
==========

Aaron,

Can you send me first and last name of those folks? Just need it for their account submittal.

Yeah, we saw that IARPA thing. They are basically asking for Palantir which is kind of odd. We are going to respond with something like, "Hey, this is already built, but we'll take your money for some R&D"

-----Original Message-----
From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Thursday, January 07, 2010 8:02 AM
To: Matthew Steckman
Subject: Re: Conference Call

Hey Matt,

No worries. I think we will be able to turn something around pretty quickly here for integration, then just a matter of what do we want to demo.

Developers:
Kam@hbgary.com
michael@hbgary.com
scott@hbgary.com
and if it is any benefit aaron@hbgary.com

How about Friday? I am open.

Aaron

Also, do you know anything about the IARPA BAA, link listed below. Maybe a bit of a stretch but it seems like there could be some applicability.

http://www.iarpa.gov/solicitations_kdd.html

==========

1/7/2010 5;13 PM Barr to Steckman

http://hbgary.anonleaks.ch/ted_hbgary_com/4338h.html This one is just lost in Google's eyes, so a related link from Ted Vera shows more about the connection to Netwitness.

Ok will do.

Do u have a partnership with netwitness? I have this idea that a few small and compatible companies can make some serious headway. What

about using something like that BSA to do the integration? Palantir is the core with 2-4 other smalls that fit a piece of the puzzle?

Aaron

From my iPhone

On Jan 7, 2010, at 5:57 PM, Matthew Steckman <mailto:msteckman@palantirtech.com> wrote:

> Aaron,
>
> Can you send me first and last name of those folks? Just need it for their account submittal.
>
> Yeah, we saw that IARPA thing. They are basically asking for Palantir which is kind of odd. We are going to respond with something like, "Hey, this is already built, but we'll take your money for some R&D"
>
> -----Original Message-----
> From: Aaron Barr [mailto:aaron@hbgary.com]
> Sent: Thursday, January 07, 2010 8:02 AM
> To: Matthew Steckman
> Subject: Re: Conference Call
>
> Hey Matt,
>
> No worries. I think we will be able to turn something around pretty quickly here for integration, then just a matter of what do we want to demo.
>
> Developers:
> Kam@hbgary.com
> michael@hbgary.com
> scott@hbgary.com
> and if it is any benefit aaron@hbgary.com
>
> How about Friday? I am open.
>
> Aaron
>
> Also, do you know anything about the IARPA BAA, link listed below. Maybe a bit of a stretch but it seems like there could be some applicability.
>
> http://www.iarpa.gov/solicitations_kdd.html
>
>
>
> On Jan 6, 2010, at 6:09 PM, Matthew Steckman wrote:
>
>> Sorry I was sucky and late to the call. Just forward me the email addresses of the developers on the call and Ill hook them up with our resources.
>>
>> Let me know if you want to chat sometime this week.

>>
>> -Matt
>>
>> Matthew Steckman
>> Palantir Technologies | Forward Deployed Engineer
>> msteckman@palantirtech.com | 202-257-2270
>>
>>
>> -----Original Message-----
>> From: Aaron Barr [mailto:aaron@hbgary.com]
>> Sent: Wednesday, January 06, 2010 4:37 PM
>> To: Matthew Steckman
>> Subject: Conference Call
>>
>> Hey Matt,
>>
>> We have a conference call scheduled for right now right?
>>
>> Aaron Barr
>> CEO
>> HBGary Federal Inc.
>>
>>

1/19/2010 8:30 AM Barr to Steckman First mention of Endgame Systems.

http://hbgary.anonleaks.ch/aaron_hbgary_com/8290.html

Matt,

This company has some very interesting capability for Botnets, Zero days, internet crawling. I have a few meetings schedules over the next week. I think they would be great to add to our partnership. Maybe next week or the following I would like to bring them in to your space and we can all sit down and talk collectively.

Hows that sound?

Aaron Barr
CEO
HBGary Federal Inc.

1/21/2010 8:39 AM Barr to Steckman Cyber Intelligence crew named

http://hbgary.anonleaks.ch/aaron_hbgary_com/5776.html

Hey Matt,

Since we are meeting at your place I thought I should let you know that the crowd is growing a bit for our Tuesday meeting. I think we will have all parties from the "cyber intelligence consortium" represented.

HBGary - Rich Cummings (CTO), myself, and Bob Slapnik.
Netwitness - Brian Girardi.
EndGames - John, Ryan, and one other.
Splunk - haven't talked to them yet, probably will today or tomorrow, but they mentioned an interest in partnership.
Xetron - Brian Masterson

so I am guessing about 10 people not counting Palantir? I can scale it back if thats to much for that day.

Are you close on the press release? :) If I can get it to our PR person today or tomorrow she is going to get it ready for a Monday release.

Thanks,
Aaron Barr
CEO
HBGary Federal Inc.

1/25/2010 11:26 AM Barr to cyber-intel coalition. First mention of Jacob Olcott.
http://hbgary.anonleaks.ch/aaron_hbgary_com/3454.html

Hey Guys,

FYI. I meet with Jake from time to time to discuss cybersecurity issues. He is the staff director for the house subcommittee for emerging threats, cybersecurity, and S&T. That is the same subcommittee that sponsored the CSIS paper for cybersecurity recommendations for the 44th presidency, chaired by Jim Lewis.

I am getting lots of good responses to this concept. I think I mentioned to all of you separately that what I would like to shoot for in late spring is a cyber intelligence summit, led by us, maybe co-sponsored by the CSIS?

See you all tomorrow.

Aaron

Begin forwarded message:

>
> 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.
>

1/27/2010 5:25 PM Barr to Steckman Structure of the system revealed – Endgame data, Palantir as framework.

http://hbgary.anonleaks.ch/aaron_hbgary_com/264.html

Thanks.

I have been talking with the folks from HBGary that attended the meetings yesterday. I think the Consortium concept is still a good idea and one I will continue to push along. That said I think there is something quicker that we can do with existing partnerships that will show a lot of value add.

The combination of HBGary data with EndGame Systems data in the Palantir framework, specifically we are working scenarios around Project Aurora and GhostNet. We have a lot of data on both. Fortunately I know you already have significant data on Ghostnet. Greg has a bug right now around this idea and is working this himself in his offtime. He installed Palantir today and is starting to input data.

Aaron

On Jan 27, 2010, at 6:21 PM, Matthew Steckman wrote:

Just sent in the request.

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantirtech.com | 202-257-2270

-----Original Message-----
From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Tuesday, January 26, 2010 10:43 PM
To: Matthew Steckman
Subject: Add to Dev Portal

Hey Matt,

Can you add Rich Cummings, rich@hbgary.com, to have access to the dev portal?

Thanks,
Aaron Barr
CEO
HBGary Federal Inc.

1/29/2010 2:34 PM Steckman to Barr Splunk is mentioned, but they seem to have had little interest in Barr's schemes.
http://hbgary.anonleaks.ch/aaron_hbgary_com/12766.html

Ha, yeah, I only got Bill Hornish's card from Splunk, don't know what that guy's name was...

Endgames followed up with us. We are meeting at Blackhat to discuss stuff.

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantirtech.com<mailto:msteckman@palantirtech.com> | 202-257-2270

From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Friday, January 29, 2010 3:32 PM
To: Matthew Steckman
Subject: Re: cyber consortium

Brian Girardi - Netwitness
Brian Masterson - NGES Xetron
Aaron Barr - HBGary
Rich Cummings - HBGary
Bob Slapnik - HBGary
Bill Hornish - Splunk
? - Splunk (you know the talkative guy)
John Farrell - Endgames
S. Alan Carroll - Endgames
David Miles - Endgames
Matt Steckman - Palantir

Aaron

On Jan 29, 2010, at 10:59 AM, Matthew Steckman wrote:

Do you have a list of who attended the meeting on Tuesday?

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantirtech.com<mailto:msteckman@palantirtech.com> | 202-257-2270

Aaron Barr
CEO
HBGary Federal Inc.

2/4/2010 12:54 AM Barr to Steckmna Chris and John from Endgame – leadership.
http://hbgary.anonleaks.ch/aaron_hbgary_com/8317h.html

Matt,

Please keep this close hold as it is in draft. Getting this down for Aurora is

good but it is more the format and process, the right data that is most important so we can do this more quickly for the future events.

I would love your comments and expertise on this. I spoke with Chris and John
from EndGame today, they have been working on their own Aurora report. We
combine our reports, makes sense. They do the C2, we do the Malware. We need to
get better at using Palantir, watching Greg, Rich, and Myself try to hammer
through it without any training is a bit painful.

I want to include 4 sections right at the front. Social, C2, Vehicle, Remediation. The essential information to understand the threat followed by
indepth technical analysis. Best way to digest is visual. I see a Palantir chart
in the Social, C2, and Vehicle sections.

Lets talk about this.

Aaron

Begin forwarded message:

> ***From: *Greg Hoglund <greg@hbgary.com <mailto:greg@hbgary.com>>**
> ***Date: *February 3, 2010 7:08:51 PM EST**
> ***To: *Phil Wallisch <phil@hbgary.com <mailto:phil@hbgary.com>>, Rich Cummings**
> **<rich@hbgary.com <mailto:rich@hbgary.com>>, Marc Meunier**
> **<mmeunier@verdasys.com <mailto:mmeunier@verdasys.com>>, aaron@hbgary.com**
> **<mailto:aaron@hbgary.com>**
> ***Cc: *penny@hbgary.com <mailto:penny@hbgary.com>**
> ***Subject: **DRAFT of DDR Report for Aurora***
>
> The attached word doc is my DRAFT for this report. Aaron, I would love to get
> Endgames to add some content to the RECENT ACTIVITY section.
> We could have spent several more days tearing this thing apart. Frankly, I
> need some current C&C servers and droppers. Our sample is a few weeks old.
> However, that said, there should be MORE than enough information in here to
> help DuPont understand that Aurora was not on the memory image they sent to us.
> Shawn is preparing an innoculation shot, I want to deliver it to DuPont
> tommorow. Marc, you might want to insert a short paragraph detailing how to
> use DG to remove that registry key and subsequent file. I know DG can do this
> kind of thing.
> Any additional data is welcome. I want to make sure that DG is highlighted.

> The Respond section at the end has plenty of room to talk about using DG to
> eliminate that malware off a machine.
> -Greg

3/11/2010 8:59 PM. Barr to Steckman Booz Allen Hamilton underperforming.Going to see 1st IO.

http://hbgary.anonleaks.ch/aaron_hbgary_com/11977h.html

Matt. I can't remember but did u say you were in NTOC or not in NTOC? I think you said not.

Not sure if you heard but NTOC is re-competing the contract a few years early. Lots of speculation as to why, most of it coming back as BAH is underperforming. CSC and ManTech have reached out to us for potential teaming for the proposal, both of whom I have talked to about the Threat Intelligence concept, so stay tuned.

Also I am going to go see 1st IO jointly with Fidelis to talk about our joint capabilities for malware/network analysis and protection. I plan to discuss Threat Intelligence with them as well.

Both Brian and I have been off the Threat Intelligence rails the last few weeks working the DARPA proposal, which has been extended until Mar 29th. I am going to have a conversation with him tomorrow on our path forward for GovCon. Neither of us want to put anything out there (and I am sure you don't either) unless it is ready for prime time. Will let you know.

Aaron

On Mar 11, 2010, at 12:47 PM, Aaron Zollman wrote:

> Aaron –
>
> Just to close the loop, we met with Fidelis at the RSA conference and may try to explore what a partnership would look like. We don't have quite the pressing need for data anymore, so we have some time. Thanks again for the introduction.
>
> _____
> Aaron Zollman
> Palantir Technologies | Embedded Analyst
> azollman@palantirtech.com | 202-684-8066
>
> From: Aaron Barr [mailto:aaron@hbgary.com]
> Sent: Tuesday, February 23, 2010 4:43 AM
> To: Aaron Zollman
> Cc: Matthew Steckman
> Subject: Re: Datasets
>
> Aaron,
>

> Sorry for the delay. We don't keep network data around turns out, but Rich (CTO) is checking with some other partners to see if we can get some (Fidelis and Netwitness). I will let you know shortly.
>
> That said, we kicked off the Threat Intelligence Center work last Friday. As part of this effort we are going to start collecting proxy/network/netflow data.
>
> Aaron
>
> On Feb 19, 2010, at 12:41 PM, Aaron Zollman wrote:
>
>
> Hello Aaron B!
>
> I met Greg and (I think) Rich and Shaun in Sacramento on Tuesday to help introduce them to the platform; it was great to learn more about how you track and respond to coordinated attacks.
>
> Right now, I'm trying to model a fast-flux coordinated botnet in Palantir and show how someone with access to a good amount of passive DNS or proxy traffic can build a visual picture of the nodes involved in coordination, and how control and activity transfer over time.
>
> Rather than try and mock up a dataset from scratch, do you guys have some historical logs to share, say from a few days of Storm, that might make for a more believable or accurate model?
>
> Thanks -
>   Aaron Z.
>
>
> _____
> Aaron Zollman
> Palantir Technologies | Embedded Analyst
> azollman@palantirtech.com | 202-684-8066
>
> From: Matthew Steckman
> Sent: Friday, February 19, 2010 6:31 AM
> To: Aaron Barr
> Cc: Aaron Zollman
> Subject: Datasets
>
> Aaron,
>
> Id like to introduce you to one of our cyber technical SMEs, Aaron Zollman. Do you think you could work with him to get us some mock datasets to play around with in Palantir?
>
> Ill let him pick up the thread from here, you should see an email from him with a description of what we're looking for sometime today.
>
> Thanks,
> Matt
>
> Matthew Steckman
> Palantir Technologies | Forward Deployed Engineer

> msteckman@palantirtech.com | 202-257-2270
>

3/21/2010 9:14 AM Steckman to Barr 1st IO put in a budget request for Palantir?

http://hbgary.anonleaks.ch/aaron_hbgary_com/11866h.html

Just got back from the honeymoon, all is well, and I am tan.....

Yes we are at NTOC, I forwarded your question to Trae to see what he's heard about it up there.

1st I/O allegedly put a budget request in for us, albeit a very small one. Talk up interoperability!!! Make them think that they are no longer buying separate tools but a connected suite...you know the schpeel. Who are you meeting with, Jamie Guzman is our contact.

Agreed on GovCon, just let me know how youd like to proceed.

Best,
Matt

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantirtech.com<mailto:msteckman@palantirtech.com> | 202-257-2270

From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Thursday, March 11, 2010 10:00 PM
To: Matthew Steckman
Subject: Re: Datasets

Matt. I can't remember but did u say you were in NTOC or not in NTOC? I think you said not.

Not sure if you heard but NTOC is re-competing the contract a few years early. Lots of speculation as to why, most of it coming back as BAH is underperforming. CSC and ManTech have reached out to us for potential teaming for the proposal, both of whom I have talked to about the Threat Intelligence concept, so stay tuned.

Also I am going to go see 1st IO jointly with Fidelis to talk about our joint capabilities for malware/network analysis and protection. I plan to discuss Threat Intelligence with them as well.

Both Brian and I have been off the Threat Intelligence rails the last few weeks working the DARPA proposal, which has been extended until Mar 29th. I am going to have a conversation with him tomorrow on our path forward for GovCon. Neither of us want to put anything out there (and I am sure you don't either) unless it is ready for prime time. Will let you know.

Aaron

On Mar 11, 2010, at 12:47 PM, Aaron Zollman wrote:

Aaron -

Just to close the loop, we met with Fidelis at the RSA conference and may try to explore what a partnership would look like. We don't have quite the pressing need for data anymore, so we have some time. Thanks again for the introduction.

Aaron Zollman
Palantir Technologies | Embedded Analyst
azollman@palantirtech.com<mailto:azollman@palantirtech.com> | 202-684-8066

From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Tuesday, February 23, 2010 4:43 AM
To: Aaron Zollman
Cc: Matthew Steckman
Subject: Re: Datasets

Aaron,

Sorry for the delay. We don't keep network data around turns out, but Rich (CTO) is checking with some other partners to see if we can get some (Fidelis and Netwitness). I will let you know shortly.

That said, we kicked off the Threat Intelligence Center work last Friday. As part of this effort we are going to start collecting proxy/network/netflow data.

Aaron

On Feb 19, 2010, at 12:41 PM, Aaron Zollman wrote:

Hello Aaron B!

I met Greg and (I think) Rich and Shaun in Sacramento on Tuesday to help introduce them to the platform; it was great to learn more about how you track and respond to coordinated attacks.

Right now, I'm trying to model a fast-flux coordinated botnet in Palantir and show how someone with access to a good amount of passive DNS or proxy traffic can build a visual picture of the nodes involved in coordination, and how control and activity transfer over time.

Rather than try and mock up a dataset from scratch, do you guys have some historical logs to share, say from a few days of Storm, that might make for a more believable or accurate model?

Thanks -
Aaron Z.

Aaron Zollman
Palantir Technologies | Embedded Analyst
azollman@palantirtech.com<mailto:azollman@palantirtech.com> | 202-684-8066

From: Matthew Steckman
Sent: Friday, February 19, 2010 6:31 AM
To: Aaron Barr
Cc: Aaron Zollman
Subject: Datasets

Aaron,

Id like to introduce you to one of our cyber technical SMEs, Aaron Zollman. Do you think you could work with him to get us some mock datasets to play around with in Palantir?

Ill let him pick up the thread from here, you should see an email from him with a description of what we're looking for sometime today.

Thanks,
Matt

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantirtech.com<mailto:msteckman@palantirtech.com> | 202-257-2270

3/21/2010 9:34 AM Barr to Steckman Talking to Jerry Bodman and Robert Nissen of NSA.

http://hbgary.anonleaks.ch/aaron_hbgary_com/7096h.html

Hey Matt,

Glad to hear you had a good time.

So things are going well for us lately, lots of good feedback on Threat Intelligence. So we talked with Dave Luber who runs the ANO. He is going to run a test pilot of DDNA and also wants to talk about standing up a Threat Monitoring center with our malware repository and a few engineers. I am supposed to talk with him more about that next week. Also going up to NSA to talk with Jerry Bodman and Robert Nissen the last week of March, they are interested in the same. I am not sure what shop they are from yet. Also got a group out of DSO (think that might be IOC but not sure) that wants to talk about product integration and threat monitoring.

Sounds like Xetrons meeting with 10th flt went well, more to come with their technical staff.

As for the booth. I spoke with Tim. We are going to have an HBGary booth and we are going to talk about Aurora as a starting point and our efforts around Threat Intelligence. We will have some initial Palantir

integration shots, but not a live demo. Tim thought that was good especially us being a strong cyber company, the flavor would be beneficial. So not the package I would want, but it is what I got. :) This will be strictly an HBGary booth.

Thoughts?

Aaron

3/21/2010 9:47 AM Steckman to Barr 1st IO technical lead is LTC Ted Wagner

http://hbgary.anonleaks.ch/aaron_hbgary_com/4266.html

As to 1st IO I will be meeting with Ted Wagner. He is the Technical Lead on 1st IO. Also a reserve Colonel for an army cyber and IO group (can't remember the name).

Aaron

On Mar 21, 2010, at 10:14 AM, Matthew Steckman wrote:

> Just got back from the honeymoon, all is well, and I am tan……
>
> Yes we are at NTOC, I forwarded your question to Trae to see what he's heard about it up there.
>
> 1st I/O allegedly put a budget request in for us, albeit a very small one. Talk up interoperability!!! Make them think that they are no longer buying separate tools but a connected suite…you know the schpeel. Who are you meeting with, Jamie Guzman is our contact.
>
> Agreed on GovCon, just let me know how youd like to proceed.
>
> Best,
> Matt

4/22/2010 12:04 PM Barr to Steckman
The Google hates this message. Here is the closest one we could find.
http://hbgary.anonleaks.ch/aaron_hbgary_com/9013.html

Hey guys,

I would like to talk to you next week about NSA. Looks like we are on a path to put our threat management center there. ANO, V22, and blue team are interested in it.

Aaron

From my iPhone

6/23/2010 6:40 PM Steckman to Barr "I am talking with 1st IO, NSA IA, and OSD this week about New Media and the vulnerabilities it creates for organizations." - Sure you are Aaron, sure you are.

http://hbgary.anonleaks.ch/aaron_hbgary_com/3507.html

If you have time to chat tonight/tomorrow can you give me a buzz, I've got a prop for you.
------Original Message------
From: Aaron Barr
To: Matthew Steckman
Cc: Trae Stephens
Subject: Re: NICE PRESS!
Sent: Jun 23, 2010 9:36 AM

Thanks. Yes he is.

He previewed this talk at the NSA REBL conference last week. I gave a talk on Social Networking, Exploitation, and Persistent Internet Operations. I was just told this morning that our two talks received the strongest positive feedback of all the talks. Attached is my slides for that presentation. I am talking with 1st IO, NSA IA, and OSD this week about New Media and the vulnerabilities it creates for organizations.

We are developing a curriculum to offer organizations on New Media. We are also going to start working on a new media mapping capability leveraging Fidelis XPS and HBGary Active Defense. Things are just too slow going because I don't have the work yet to hire enough people for what I want to do but we will get there. New Media is the new and future exploitation vehicle and I hope to ride the front of that wave (on both sides).

Hey how about a Pong challenge next Friday. I will make sure Bob is there.

Aaron

On Jun 23, 2010, at 9:18 AM, Matthew Steckman wrote:

> Aaron,
>
> Kudos:
http://mobile.darkreading.com/9287/show/571d636618a7ba35b7e9bae872fc5bfd/
>
> Greg is going to crush it at BlackHat.
>
> Best,
> Matt
>

> Matthew Steckman
> Palantir Technologies | Forward Deployed Engineer
> msteckman@palantir.com | 202-257-2270
>

Aaron Barr
CEO
HBGary Federal Inc.

10/19/2010 3;56PM Steckman to Barr & Ryan Team Themis started with Hunton Williams contacting Palantir.

http://hbgary.anonleaks.ch/aaron_hbgary_com/12671h.html

Patrick, Aaron,

I have spoken to both of you about offering a complete intelligence solution to a law firm that approached us. As I see it now, Berico would prime the contract supplying the project management, development resources, and process/methodology development. HBGary would provide subject matter expertise on "digital intelligence collection" and "social media exploitation" as well as potential analysts. Palantir would like to keep our role in this as transactional as possible, being available for consult when needed for complex data integration and modeling issues. Our guess at this point is that this will be a hosted Palantir solution.

Eli and I are spearheading this from the Palantir side and would like to get together before we approach the law firm with our offer. Are you two available to meet this Friday, say 10am to go over some details?

Best,
Matt

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantir.com<mailto:msteckman@palantirtech.com> | 202-257-2270

Follow @palantirtech<twitter.com/palantirtech>
Watch youtube.com/palantirtech
Attend Palantir Night Live<http://www.palantirtech.com/government/pnl>

10/28/2010 3:58 PM Ryan to Barr, cc: Steckman Data dump on Hunton Williams people. Another one that Google is a bit coy about providing.
http://hbgary.anonleaks.ch/aaron_hbgary_com/1612.html

Aaron:

Yep, pretty scary how easy it is to gather that info! I like it...

I've attached my current (very rough) draft of the proposal. Please take a look at let me know what you think. Just wanted to get bullets/ideas down and started to craft some initial thoughts. In particular, still need some help in thinking through the following:

1) How do we best define the problem? Is this only a "cyber" phenomena or are we looking to cast a wider net and investigate other forms of these "corporate campaigns"? What other forms/methods are adversaries using to attack corporations and other clients of H&W? I'm still trying to wrap my head around exactly the problem they're looking to solve/tackle. Any ideas/thoughts here would be particularly helpful

2) Does the estimate timeline and level of effort/labor sound about right to you? Should we differentiate between collectors and analysts or group them together to give us more flexibility? Thoughts on key responsibilities for each role?

3) Please let me know if you have other text you'd like to include under key personnel and company background sections. Also, should we shift the company backgrounds to the end of the proposal?

4) What should we call this? I just took a stab and called it a "Corporate Threat Analysis Cell"...open to better ideas. Also, what should we name the Berico-HBGary-Palantir Team...need something catchy?

Please let me know what you think. Here's what I propose for the way ahead to prep for the proposal meeting next week:

-Fri - phone call sync (Aaron, Pat, Eli, Matt) - propose 30 min at 1100 EST; focus is to divide responsibilites for proposal writing/production so we can work it over the weekend

-Sat-Sun - refine proposal

-Mon - face-to-face proposal writing/finalization/edits (Aaron, Pat)

-Tues - red team edits (Berico, HBGary, Palantir); brief rehearsal (either over phone or in person)

-Wed - meeting at H&W offices - 1200hrs

Thanks,
Pat

On Wed, Oct 27, 2010 at 4:14 PM, Aaron Barr <aaron@hbgary.com> wrote:

> A bit of what I have on John. 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.
>
> ***John W. Woods Jr. - DC***
> * Linkedin **John Woods*<http://www.linkedin.com/profile?viewProfile=&key=3967829&authToken=rBd6&authType=OUT_OF_NETWORK&locale=en_US&srchindex=1&srchid=bb3e3f4e-52d7-4ccb-9c3f-43d2ca05c4e0-1&srchtotal=235&pvs=ps&goback=%2Efps_*1_*1_*1_*1_Partner_CP_Hunton+%26+WIlliams_*51_C_Y_*1_*1_*1_false_1_R_true_N%2CG%2CI%2CED%2CL%2CFG%2CTE%2CFA%2CSE%2CP%2CCS%2CF%2CDR%2CCC%2CPC_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2_*2>
> * Facebook **John Woods*<http://www.facebook.com/profile.php?id=1420043523&ref=sgm>
> * Email: jwoods@hunton.com*
> * Phone: (202) 955-1513*
> * Hometown: Lynnfield, MA*
> * DOB: 01/13/1968 (42)*
> * Residence: 105 Tonbridge Rd. Richmond, VA*
> * High School: Lynnfield High School '86*
> * BA: Colby College 1990*
> * JD: University of Virginia 1995*
> * Contribute approx. $250 in '08*
> * Political Donations: Gave money to John McCain *
> * Father John W Woods Jr. (78)*
> * Mother Judith E Woods (74)*
> * Sister Susan Leslie Hood (39)*
> * Wife Jane K Noland Woods (40)*
> * Facebook **Jane N. Woods*<http://www.facebook.com/profile.php?id=1413804154&ref=search>
> * Met in College?*
> * DOB: 06/28/1969*
> * Court: Speeding 71/55 08/17/2006*
> * Hometown: Newport News, VA*

> * High School: Hampton Roads Academy '87*
> * UVA*
> * Political Contributions: 8/29/01 homemaker *
> * 1000 Sen. John Warner*
> * 6/30/01 homemaker 1000 Sen. John Warner*
> * Father owns Noland Company*
> * Annual Revenue $100-$500M*
> *A Runner. Member of GRIPLA.ORG (Greater Richmond Intellectual Property
> Law Association. Has a blackberry and has installed the Facebook app for
> blackberry.*
> *
> *
> On Oct 26, 2010, at 4:24 PM, Patrick Ryan wrote:
>
> Hey Aaron:
>
> Again, it was great to meet you yesterday. I'm starting work on an outline
> for the proposal we'll pitch next Thurs, but wanted to share the bio I found
> on John Woods - our primary POC at Hunton & Williams. Sounds like he has a
> very solid background in the type of work we'll be doing, so it should be
> good to work with him and also get a chance to feel him out a bit on what
> exactly his expectations are:
>
> http://www.hunton.com/bios/bio.aspx?id=16017
>
> How's your investigation into the company coming? Once I complete the
> first iteration of the outline, I will send your way for feedback and your
> thoughts.
>
> Thanks,
> Pat
>

11/1/2010 9:10 AM Barr to Ryan & Steckman Barr pursuing Bob Tata of Hunton Williams.

http://hbgary.anonleaks.ch/aaron_hbgary_com/4310.html

All,

Something for us to consider. I have been doing a bit of research on H&W just to show methodology, benefit. Show the power of open source, link analysis, etc. I did not include any paid data sources in this information, this was all gathered just doing linkedin, facebook, search analysis.

Here is some information that I have gathered that we can think about including. Of course using Palantir and automating some of the collection will make this a lot more powerful and complete.

235 Linked in Profiles currently employed with H&W
68 LInked in Profiles of Partners currently with H&W
Corporate email address structure: abarr@hunton.com (first initial, last name @ hunton.com

email addresses are great to use to see if people have used them to sign up for other accounts, for example jwoods@hunton.com signed up for a sabre.com account using this email address (the UVA football team - his alma mater).

or

Bob Tata and his wife, Anne Ferrell, live in Virginia Beach with their four children, Peyton, Carter, Riley.
Also found a spam list containing other possible email addresses for btata.
btata56207@msn.com
btata@att.net
btata@bellsouth.net
btata@hunton.com
btata@massed.net
btata@msn.com
btata@usa.net
btata@worldnet.att.net
This is a rather large group that just gets larger through associates, attorneys, etc. Lots you can tell about individual people from social link and artifact analysis. For example. John Woods does rarely uses his Facebook account. 95%+ of his friends are from his hometown/high school. To get to him I would create someone from his past, find someone he went to high school with on Classmates.com that doesn't have a FB profile and create him/her. Either that or I would go through a professional association, but thats harder to pull off.

Through greater analysis of partners, attorneys and associates we might be able to determine sensitive information about clients or other relationships based on connections.

Sean Beard and JR Williams are the firms social butterflies in Richmond, VA. They are connected to an immense list of employees but do not seem to have an out of work social relationship. Bob Tata and Stuart Rapael share a significant number of employees in the DC area but also share social connection and family connections.

Overall many of the employees have strong ties to their work and to their alma mater, most belong to different associations related to their profession. All of these are also angles for information collection and when developing profiles to get into their social circles.

Successfully collecting and penetrating this group and any group is all about gaining an understanding of how the groups and individuals function, what roles they play, etc. Gaining access to these groups are about taking this information and developing profiles and social

exploitation methods that are consistent with the social relationships and artifacts available.

John Woods information:

Linkedin John Woods
Facebook John Woods
Email: jwoods@hunton.com
Phone: (202) 955-1513
Hometown: Lynnfield, MA (11,500 people)
DOB: 01/13/1968 (42)
Residence: 105 Tonbridge Rd. Richmond, VA
High School: Lynnfield High School '86 (small)
BA: Colby College 1990
JD: University of Virginia 1995
Contribute approx. $250 in '08
Political Donations: Gave money to John McCain
Father John W Woods Jr. (78)
Mother Judith E Woods (74)
Sister Susan Leslie Hood (39)
Wife Jane K Noland Woods (40)
Facebook Jane N. Woods
Met in College?
DOB: 06/28/1969
Court: Speeding 71/55 08/17/2006
Hometown: Newport News, VA
High School: Hampton Roads Academy '87
UVA
Political Contributions: 8/29/01 homemaker 1000 Sen. John Warner
6/30/01 homemaker 1000 Sen. John Warner
Father owns Noland Company
Annual Revenue $100-$500M
A Runner. Member of GRIPLA.ORG (Greater Richmond Intellectual Property Law Association. Has a blackberry and has installed the Facebook app for blackberry.

PARTNERS:
Michael O'Shea - DC
Linkedin Michael O'Shea
Scott Burton - LA
Linkedin Scott Burton
Jay Halloway - Richmond
Linkedin Jay Holloway
J. Michael Martinez de Andino - Rich
Linkedin J. Michael Martinez de Andino
Walfrido Martinez - NY
Linkedin Walfrido Martinez
Frederick Eames - DC
Linkedin Frederick Eames
Facebook Fred Eames
Oil City, PA
11/15/1964 (45)
7710 Falstaff Rd Mclean VA 22102
Allegheny College
George Washington Univ Law
Wife Beth Eames

Brother Bob Eames
Ellis Butler - DC
Linkedin Ellis Butler
Facebook Ellis Butler
Tim Goettel - Raleigh-Durham NC
Linkedin Tim Goettel
Facebook Tim Goettel
Twitter: @timgoettel
Tom Kaufman - DC (owner)
Linkedin Tom Kaufman
Facebook Thomas F Kaufman
Walter Andrews - DC
Linkedin Walter Andrews
Facebook Walter Andrews
Michael Sweeney - DC
Linkedin Michael Sweeney
Peter Brudenall - London
Linkedin Peter Brudenall
Scott Austin - Dallas/Fort Worth, TX
Linkedin Scott Austin
Facebook Scott Austin
W. Jeffery Edwards - RIchmond
Linkedin W. Jeffery Edwards
Facebook - W. Jeffery Edwards
Deidre Duncan - DC
Linkedin Deidre Duncan
Facebook Deidre Glasser Duncan
Miles Haberer - Dallas
Linkedin Miles Haberer
Randy Parks - Richmond
Linkedin Randy Parks
Alex Mcgeoch - Dallas
Linkedin alex mcgeoch
John Delionado - Miami
Linkedin John Delionado
Cyane Crump - Richmond
Linkedin Cyane Crump
Michael Phelps - DC
Linkedin Michael Phelps
John Adams - DC
Linkedin John Adams
Joseph Stanko - DC
Linkedin Joseph Stanko
Melvin (Mel) Tull - RIchmond, VA
Linkedin Melvin (Mel) Tull
Carlos Loumiet - Miami
Linkedin Carlos Loumiet
Thomas Anderson - DC
Linkedin Thomas Anderson
Pete Johnson - Richmond
Linkedin Pete Johnson
Matt Jenkins - Richmond
Linkedin Matt Jenkins
John McGranahan - DC
Linkedin John McGranahan
Facebook John McGranahan
Keila Ravelo - NY

Linkedin Keila Ravelo
Facebook Keila Ravelo
Mark Duedall – Atlanta
Linkedin Mark Duedall
Stuart Raphael – DC
Linkedin Stuart Raphael
Facebook Stuart Raphael
Relationship with Bob Tata Carol Baker Kane, Bruce Braun
John Epps – Richmond
Linkedin John Epps
Jack Molenkamp – DC
Linkedin Molenkamp Jack
Michelle A Mendez – Dallas
Linkedin Michelle A Mendez
Ray Hartwell – DC
Linkedin Ray Hartwell
Steven Becker – NY
Linkedin Steven Becker
Maya Eckstein – Richmond
Linkedin Maya Eckstein
Art Schmalz – DC
Linkedin Art Schmalz
Douglass Selby – Atlanta
Linkedin Douglass Selby
Kyle Sampson – DC
Linkedin Kyle Sampson
Kurt Powell – Atlanta
Linkedin Kurt Powell
Sheldon Bradshaw – DC
Linkedin Sheldon Bradshaw
Kelly Faglioni – RIchmond
Linkedin Kelly Faglioni
Facebook Kelly Learish Faglioni
Lisa Sotto – NY
Linkedin Lisa Sotto
Facebook Lisa Sotto
Email: lsotto@hunton.com
Phone: (212) 309-1223
Bob Tata – Norfolk
Linkedin Bob Tata
Facebook Bob Tata
Relationship with Stuart Raphael Carol Baker Kane, Bruce Braun
Greg Cope – Richmond
Linkedin Greg Cope
Laurence Posorske – DC
Linkedin Laurence Posorske
Aaron Simpson – NY
Linkedin Aaron Simpson
Facebook Aaron Simpson
Email: asimpson@hutton.com
Phone: (212) 309-1126
Ian Band – DC
Linkedin Ian Band
Facebook Ian Band
David Higbee – DC
Linkedin David Higbee
Jeff Harvey – Richmond

Linkedin Jeff Harvey
JR Smith - Richmond
Linkedin JR Smith
Facebook J.R. Smith
Bing Maisog - China
Linkedin Bing Maisog
David Wells - Miami
Linkedin David Wells
Brian Buroker - DC
Linkedin Brian Buroker
Bridget Treacy - London
Linkedin Bridget Treacy
Bruce Hoffman - DC
Linkedin Bruce Hoffman
Robin Teskin - DC
Linkedin Robin Teskin
Kim Magee - Richmond
Linkedin Kim Magee
Sean Beard - Richmond
Linkedin Sean Beard
Facebook Sean Beard
John Beardsworth - Richmond
Linkedin John Beardsworth
Wendell Taylor - DC
Linkedin Wendell Taylor
Facebook Wendell Taylor
Jonathan Wilan - DC
Linkedin Jonathan Wilan
Facebook Jonathan Wilan
Torsten Kracht - DC
Linkedin Torsten Kracht
Michael Oakes - DC
Linkedin Michael Oakes
Facebook Michael Oakes
Christopher Kuner - Belgium
Linkedin Christopher Kuner

Bob Tata and Stuart Raphael share Daniel Fitzpatrick
Bob Tata and Stuart Raphael share with Hugh Patton.
Bob Tata and Stuart Raphael share Janet and Paul Nolan
Bob Tata and Stuart Raphael share Jay Felton.
Bob Tata and Stuart Raphael share John B. Howard.
Bob Tata and Stuart Raphael share Joseph Perkins.
Bob Tata and Stuart Raphael share Kim Reed
Bob Tata and Stuart Raphael share Kirk and Margit Nahra
Bob Tata and Stuart Raphael share Laurie C Sahatjian
Bob Tata and Stuart Raphael share Leanne Shaltis Fallin
Bob Tata and Stuart Raphael share Christopher and Maria Olsen
Bob Tata and Stuart Raphael share Nancy Maloney Williams
Bob Tata and Stuart Raphael share Pete Killough

JR Smith, Wendell Taylor, and Sean Beard share Mandy Beasley Tornabene
JR Smith and Sean Beard share Anne Weir
JR SMith, Sean Beard, and Wendell Taylor share Barry Meek
JR Smith and Sean Beard share Bill Newton
Sean Beard and Wendell Taylor share Brian Richardson ?

JR Smith and Sean Beard share Bryan Rhode ?
JR Smith and Sean Beard share Carolyn Mitchell
Sean Beard and Tim Goettel share Charlene Killian (Hunton & Williams)
Sean Beard and Aaron Simpson share Will Homiller >
JR Smith and Sean Beard share Charles Powers
JR Smith and Sean Beard share Charlotte McAfee ?
JR Smith, Sean Beard, and Wendell Taylor share Chris Anderson (Hunton & WIlliams)
Sean Beard and Wendell Taylor share Chris Hewett Call ?
JR Smith and Sean Beard share Chris Jones ?
JR Smith, Sean Beard, and Wendell Taylor share Chris Lemons
JR Smith, Sean Beard, Wendell Taylor, and Kelly Faglioni share Christine Christi Klein
Sean Beard and Wendell Taylor share Christy Kiely
JR Smith and Sean Beard share Courtney Walsh Nolde
JR Smith and Sean Beard share Daniela Rost
JR SMith, Sean Beard, and Wendell Taylor share Diane Sox
Ellis Butler, JR Smith, Sean Beard, and Wendell Taylor share Doug Garrou
JR Smith, Sean Beard, Wendell Taylor share Edward T. White
JR SMith, Sean Beard, Wendell Taylor share Elizabeth Breen
JR SMith, Sean Beard, Wendell Taylor share Jason Jacoby
JR SMith and Sean Beard share Jim Pinna
JR Smith and Sean Beard share Jim White
JR Smith and Sean Beard share Katherine Laxton Alvarez

11/3/2010 9:23PM Steckman to Barr & Ryan
http://hbgary.anonleaks.ch/aaron_hbgary_com/3240.html

Patrick, Aaron,

We have confirmed that 100k is a good number for a firm fix price for the first month. We'd like to structure it something like 1x for the first month, 5x for the next two months, 10x for a permanent solution (spilt between all of us). When you draft up a pricing proposal just swing it our way and we can fill in the Palantir section. We'll include a description of the support that will be provided. We'd like to structure it as Palantir supporting the prime Berico, versus Palantir supporting the end customer.

I spoke to my wife about hourly rates. She said that a jr. associate with a law degree from a top school and 0 years of experience doing research on a case like this would bill about 300 an hour. So, 300 an hour times 40 hours a week = 12,000, times 4 weeks = 48,000 a month. So I think you guys were right on with the 50k mark.

Nice job today.

Best,
Matt

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantir.com<mailto:msteckman@palantirtech.com> | 202-257-2270

Follow @palantirtech<twitter.com/palantirtech>
Watch youtube.com/palantirtech
Attend Palantir Night Live<http://www.palantirtech.com/government/pnl>

11/8/2010 6:11 PM Ryan to Woods, cc: Steckman & Barr
http://hbgary.anonleaks.ch/aaron_hbgary_com/9228.html Another one google is coy about.

John:

Good to talk earlier - I think we're both on the same page and are working
towards achieving the same endstate. Please see high-level breakdown below
of our expected level of effort and responsibilities. As we discussed, we
may need to adjust based on the answers to our questions and additional
guidance from Richard tomorrow. Let me know if you have any further
questions or need more detail. I look forward to hearing how your meeting
goes.

Phase I (Roles and Key Tasks):

1) Berico (2x FTE)
   [Expect to have 1x Senior Analyst/PM and 1x All-Source Analyst]
   -Overall project management and close interaction with H&W lead
   -Ensure rapid stand-up of Palantir instance and analytical capability
   -Manage all data integration and analytical efforts
   -Produce detailed products/assessments based on H&W requirements
   -Provide additional data integration support (as needed)

2) HBGary Federal (2x FTE)
   [Expect to have 1x Senior Collector/Analyst and 1x Engineer/Data Integrator]
   -Lead data integration of existing data and identify new, relevant data
sources
   -Develop customized helpers within Palantir to support analysis/visualization
   -Provide cyber and social media exploitation/analysis support

3) Palantir (1x as needed)
   [Expect to have 1x Forward-Deployed Engineer]
   -Lead stand-up and implementation of Palantir instance for H&W
   -Provide secure data storage and maintenance of hosted instance
   -Provide technical consulting (as needed)

Regards,
Pat

On Mon, Nov 8, 2010 at 5:54 PM, Patrick Ryan
<pryan@bericotechnologies.com>wrote:

> I'll be available on my cell phone at 719-433-1323.
>
> Thanks,
> Pat
>
>
> On Mon, Nov 8, 2010 at 5:48 PM, Woods, John <jwoods@hunton.com>
wrote:
>
>> Where can I reach you in 15 mins?
>>
>> ------------------------------
>> ***From***: Patrick Ryan <pryan@bericotechnologies.com>
>> ***To***: Patrick Ryan <patrick@bericotechnologies.com>
>> ***Cc***: Woods, John; Aaron Barr <aaron@hbgary.com>; Matthew Steckman <
>> msteckman@palantir.com>; Eli Bingham <ebingham@palantir.com>;
Gilman,
>> Neil
>> ***Sent***: Mon Nov 08 17:43:31 2010
>> ***Subject***: Re: Team Themis Cost Proposal - Phase I
>>
>> Hey John, just wanted to ensure you got my note earlier. I'm
available
>> until about 8pm tonight or could make time tomorrow morning as well.
>>
>> Thanks,
>> Pat
>>
>> On Sun, Nov 7, 2010 at 6:38 PM, Patrick Ryan <
>> patrick@bericotechnologies.com> wrote:
>>
>>> John:
>>>
>>> Thanks. This estimate was based only on our initial discussion
last
>>> week, so the answers to those questions could potentially cause us
to adjust
>>> our level of effort. I would be happy to talk you through our
thought
>>> process and answer any questions you may have. I'm available to
talk
>>> anytime from 9-12...please let me know when is best for you.
>>>
>>> Regards,
>>> Pat
>>>
>>>
>>> On Sun, Nov 7, 2010 at 3:21 PM, Woods, John <jwoods@hunton.com>
wrote:
>>>
>>>> Patrick -
>>>>
>>>> Thanks for this. I am meeting on Tuesday morning with the team at
HW
>>>> who has gathered the underlying data, so I should be able to
answer a number

>>>> of these questions for you shortly thereafter. I think I would
>>>> consider some sort of initial firm fixed price agreement, but I am
wondering
>>>> if we have a cart/horse problem. I think it would be better if I
>>>> could answer the questions you outline below before giving me a
final
>>>> estimate. I do not know the answers to many of the questions, so
it is
>>>> difficult for me to judge whether the level of effort imbedded in
your
>>>> proposal is accurate. Patrick, are you around morning on Monday
to walk me
>>>> through what everyone would be doing under the current proposal
and to get
>>>> clarification on a few of the questions?
>>>>
>>>> Regards,
>>>> JWWjr.
>>>> ------------------------------
>>>> *From:* Patrick Ryan [mailto:patrick@bericotechnologies.com]
>>>> *Sent:* Friday, November 05, 2010 4:39 PM
>>>> *To:* Woods, John
>>>> *Cc:* Aaron Barr; Matthew Steckman; Eli Bingham; Katherine Crotty;
>>>> Jeremy Glesner; Aaron Marshall
>>>> *Subject:* Team Themis Cost Proposal - Phase I
>>>>
>>>> John:
>>>>
>>>> It was great to meet you Wednesday. After speaking with you and
>>>> learning more about the project, we are all extremely excited to
move
>>>> forward and provide support to your team.
>>>>
>>>> Per your request, please see our attached cost proposal for Phase
I.
>>>> Based on our initial discussions about the duration and concrete
nature of
>>>> the deliverables/tasks associated with this phase, we feel that a
firm-fixed
>>>> price model is the best option. The cost includes all software
>>>> licenses/services, project management, analysis, and
>>>> engineering/development. Pending your approval of the cost
estimate, we can
>>>> sit down and develop a more detailed Scope of Work with specific
tasks. As
>>>> we discussed during the meeting, we feel that the powerful
combination of
>>>> software and services that Team Themis (Palantir-Berico-HBGary)
offers will
>>>> provide dramatic improvements in capability for Hunton & Williams.
Our
>>>> initial estimate of the time to complete Phase I is approximately
30 days,
>>>> but we request the following additional information about your
current data
>>>> set in order to allow us to better scope our estimated time and
level of

>>>> effort:
>>>>
>>>> 1) What type of data is it? (Financial Records, Union Rosters, IP
>>>> addresses)
>>>>
>>>> 2) Is the data structured or unstructured (i.e. free text vs.
>>>> spreadsheets)?
>>>>
>>>> 3) How many pages of unstructured data do you have?
>>>>
>>>> 4) What format(s) is the data in? (excel, csv, sql)
>>>>
>>>> 5) Where is the data? Is it centrally located?
>>>>
>>>> 6) How many GB of data do you have overall?
>>>>
>>>> 7) How was the data gathered?
>>>>
>>>> 8) How old is the data we'll get? What duration of time does it
>>>> cover?
>>>>
>>>> 9) Do we have access to the union in question's membership lists?
>>>>
>>>> 10) What are the typical workflows that you are currently performing
>>>> with the data?
>>>>
>>>> 11) In the past, what has been the most difficult steps in your
>>>> analysis?
>>>>
>>>> 12) Do you have any products and conclusions from the past, as well
>>>> as the data that you used to come to those conclusions that we could see to
>>>> try to replicate the workflow and see where we need to get?
>>>>
>>>> 13) Are there different levels of classification for the data
>>>> (believe it is all open-source, but want to confirm)?
>>>> We look forward to your response and to working together in the future.
>>>>
>>>> Regards,
>>>> Pat
>>>>
>>>> --
>>>> Patrick Ryan
>>>> Deputy Director, Analysis
>>>> Berico Technologies
>>>> pryan@bericotech.com
>>>> 719-433-1323 (c)
>>>> 703-224-8300 (o)
>>>>
>>>>
>>>

>>>
>>> --
>>> Patrick Ryan
>>> Deputy Director, Analysis
>>> Berico Technologies
>>> pryan@bericotech.com
>>> 719-433-1323 (c)
>>> 703-224-8300 (o)
>>>
>>>
>>
>

11/16/2010 7:39 AM Barr to Steckman Xetron (Masterson?) has a personal relationship with 10th fleet head.
http://hbgary.anonleaks.ch/aaron_hbgary_com/9279.html

No I am not and have very little entrance there.

The person to talk with (not sure your relationship) is Xetron. The guy who runs Xetron in Cincinatti has a personal relationship with the Admiral. They have been in to brief them a few times.

Aaron

On Nov 15, 2010, at 2:42 PM, Matthew Steckman wrote:

> Are you doing anything interesting here? Looking for an intro if you have it, cyber related or BIG Navy workflows (tracking, tactical ops, resourcing, etc).
>
> -Matt
>
> Matthew Steckman
> Palantir Technologies | Forward Deployed Engineer
> msteckman@palantir.com | 202-257-2270
>
> Follow @palantirtech
> Watch youtube.com/palantirtech
> Attend Palantir Night Live
>

Aaron Barr
CEO
HBGary Federal, LLC

11/24/2010 1:00 PM Kremin to all Themis

http://hbgary.anonleaks.ch/aaron_hbgary_com/11986h.html

Team,

I've attached a Labor Cat breakdown/excel Katie has started. It is NOT yet
shaped for this effort, however it will provide the framework that HBGary
can insert their SMEs into, as well as the personnel that Palantir will
have at-hand to support the initiative.

She specifically did not include 'Hours' within this framework, as she
wanted to provide the max-participation outlook (as they are looking at this
to specifically justify each of our monthly bills).

At the bottom is a "Services" Section, she left it open for Palantir to talk
their product costs within the format/detail they desire.

Although this outlines traditional education/years experience, she highly
encourage everyone to talk as in-depth as possible to what special skillset
the individuals will be bringing to the contract and how that differentiates
us (ie. outline "Influence Operations SME" versus "Consultant" and explain
what they bring that is above and beyond a normal analyst).

If you can please include this information/erase everything else, we will
compile into one. We will need resumes as well for key personnel and what
labor cat they are going to be billed within this excel. We will work on our
end to put them all into the same format.

Thanks
Sam

--
Samuel Kremin
Analyst/Consultant
Berico Technologies
703.473.1493

12/2/2010 3:32 PM BofA => Wikileaks
http://hbgary.anonleaks.ch/aaron_hbgary_com/2374.html

That works. I'll send an invite.

Here is the summary of my call:

They are pitching the bank to retain them for an internal investigation
around wikileaks. They basically want to sue them to put an injunction
on releasing any data. DOJ called the GC of BofA and told them to hire

Hunton and Williams, specifically to hire Richard Wyatt who I'm beginning to think is the emperor. They want to present to the bank a team capable of doing a comprehensive investigation into the data leak. Currently they are recommending:

-Hire H&W as outside council on retainer
-Use Palantir for network/cyber/insider threat investigation
-Use Berico/HBGary to analyze wikileaks the organization (people, history, where they are located) Apparently if they can show that wikileaks is hosting data in certain countries it will make prosecution easier.
-Use a team of GD/PWC forensics investigators.

They have a half hour with the GC of the 3rd largest bank in the world to plead their case.

They want 5-6 slides from Palantir-HBGary-Berico outlining what we can do. It's due tomorrow morning.

Matthew Steckman
Palantir Technologies | Forward Deployed Engineer
msteckman@palantir.com | 202-257-2270

Follow @palantirtech
Watch youtube.com/palantirtech
Attend Palantir Night Live

-----Original Message-----
From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Thursday, December 02, 2010 4:29 PM
To: Eli Bingham
Cc: Matthew Steckman; BERICO-Sam.Kremin
Subject: Re: URGENT - OPPORTUNITY

How about 530

>From my iPhone

On Dec 2, 2010, at 4:26 PM, Eli Bingham <ebingham@palantir.com> wrote:

> Fine by me.
>
>
>
> Sent from a phone
>
> -----Original Message-----
> From: Matthew Steckman
> Sent: Thursday, December 02, 2010 01:24 PM Pacific Standard Time
> To: HBGARY-Aaron.Barr
> Cc: BERICO-Sam.Kremin; Eli Bingham
> Subject: RE: URGENT - OPPORTUNITY
>
> Just spoke with John. I've got details.
>
>

>
> Can everyone jump on a conference call at 5pm?
>
> Dial-in: 866-740-7142
> Conference code: 4941574
>
>
>
> Matthew Steckman
> Palantir Technologies | Forward Deployed Engineer
> msteckman@palantir.com <mailto:msteckman@palantirtech.com> | 202-257-2270
>
>
>
> Follow @palantirtech
>
> Watch youtube.com/palantirtech
>
> Attend Palantir Night Live <http://www.palantirtech.com/government/pnl>
>
>
>
> From: Aaron Barr [mailto:aaron@hbgary.com]
> Sent: Thursday, December 02, 2010 4:16 PM
> To: Woods, John
> Cc: BERICO-Sam.Kremin; Matthew Steckman; Eli Bingham
> Subject: Re: URGENT - OPPORTUNITY
>
>
>
> Sure thing. I will work on it tonight. Sam?
>
>
>
> Aaron
>
> From my iPhone
>
>
> On Dec 2, 2010, at 3:55 PM, "Woods, John" <jwoods@hunton.com> wrote:
>
> Richard and I am meeting with senior executives at a large US Bank tomorrow regarding Wikileaks. We want to sell this team as part of what we are talking about. 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.
>

12/3/2010 7:27 AM Barr to Steckman
http://hbgary.anonleaks.ch/aaron_hbgary_com/1791.html
==========

A few other thoughts. Obvious when attacking any adversary you attack their week points. In this case their strength is their global following and volunteer staff. This allows them to have a very loose organization, probably little if any direction or coordination is actually passed it is just inferred as part of the cause. Julien pronounces and the minions follow. Larger infrastructure is fairly pointless to attack because they have so many other points so many other organizations that are willing to distribute the information and help them get new hosting services.

Weak points.
Financial. They are under increasing financial pressure because authorities are blocking their funding sources. Need to help enumerate these. Also need to get people to understand that if they support the organization we will come after them. Transaction records are easily identifiable.
Security. As I pointed out. Need to get to the swedish document submission server. Need to create doubt about their security and increase awareness that interaction with Wikilieaks will expose you.
Mission. As we have already seen there is a fracture amongst the followers because of a belief that Julien is going astray from the cause and has selected his own mission of attacking the US.

Despite they publicity, I do not believe Wikileaks is in a healthy position right now. I think their weakness are causing great stress in the organization and we need to capitalize on those.

Aaron

On Dec 3, 2010, at 7:45 AM, Matthew Steckman wrote:

> Here is the collated first cut to brief John with at 9. I am going to send this to him at 8:15, unless you guys have any comments before then.
>
> Matthew Steckman
> Palantir Technologies | Forward Deployed Engineer
> msteckman@palantir.com<mailto:msteckman@palantirtech.com> | 202-257-2270
>
> Follow @palantirtech<twitter.com/palantirtech>
> Watch youtube.com/palantirtech
> Attend Palantir Night Live<http://www.palantirtech.com/government/pnl>
>
> <winmail.dat>

12/3/2010 7:32 Barr to Steckman Greenwald
http://hbgary.anonleaks.ch/aaron_hbgary_com/7793.html

One other thing. I think we need to highlight people like Glenn Greenwald. Glenn was critical in the Amazon to OVH transition and helped wikileaks provide access to information during the transition. It is this level of support we need to attack. These are established proffessionals 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.

Aaron