Aaron Barr to Rosemary Wenchel of OSD 3 Dec 2009. This is Office of the Secretary of Defense. Barr admits to being in charge of the cyber and SIGINT (signal intelligence) business units.

==========

Hello Rosemary,

I spoke to you briefly at the AFCEA conference this week about Attribution. I find myself in an ironic position, my previous position was as Northrop Grumman's Technical Lead for their Cyber Campaign and the Technical Director for the Cyber and SIGINT BU. I have had many conversations with Bill Studeman and Rich Haver where I adamantly disagreed that we can tackle Attribution for some key reasons: We have no accurate representation/characterization of our cyber resources, very little situational awareness, little integration of CND/CNE and multi-INT...for starters. Then I took the position as HBGarys CEO for and started seeing the problem a bit differently.

You can mask the IP, the routes you take on the net, but you can't hide the attributes of the binary itself. If there was a malware genome that characterized, categorized the functions, the authors fingerprints in code, and then were able to associate that information with externals, maybe some bit of attribution is possible.

So starting out I am taking the capabilities of my company, HBGary, to do malware identification and characterization, author fingerprinting and marrying those with Palantir to do meta link analysis of cyber externals. I think this approach will be a very good first step, but I want to go further. Are there any folks you could point me to that would be interested in discussing and/or participating in this type of effort? I met at the conference Ralph Ghent from NSAs Cyber Operations Integration office, who is going to put me in contact with some folks at Carnegie Melon that are working on parts of this.

I also noticed your responsibilities span Information Operations. I spent 7 years building a net-centric based influence capability for a non-DoD customer that was amazing in capability but insular and narrow in scope. I think such a persistent capability would be very beneficial to the militaries mission. So wondering if there would be anyone you are aware of that would be interested to discuss current government capabilities and relevance to DoD missions.

I also have some ideas and experience working with new interactive technologies (MMO, VWs, Mobile geo-referenced applications) and how those can be used for better influence, strategic communications, collection.

Thank You,
Aaron Barr

http://hbgary.anonleaks.ch/aaron_hbgary_com/9387.html Aaron Barr to Irving Lachow. 6 May 2010. Lachow has an OSD email and one for the National Defense University. This whole thread of discussion is about technology and its applications.
POSTED: Magpii

==========

Irv,

Some topics for our discussion.

•C&C: Use of keyword tables in malware to communicate c&c servers . Could use google adwords or Twitter accounts. Each Trojan has a keywords table and based on parameters will concatenate words from the table into a phrase and do keyword searches on Twitter for posts to DynDNS (fast flux) URLs.
•Persistent Comms: encrypted P2P or bittorrent
•Commercially available products for comms.
•MMO plugins: comms, IO, etc
•Complete commercial operations. Magpii.
•Mobile services and apps.
•Amateur Photo journalism
•Cloud applications
•Threat intelligence. Automate data ingest and correlation. Malware, open source, c&c data.
•Hive approach to network intelligence.
•Aggregation of small company capabilities for advanced detection and protection. Damballa/EGS, Netwitness, HBGary.
•Social media

Aaron

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/7507.html Irving Lachow to Ray Owen of Farallon Research, copying Aaron Barr. 6 May 2010. “working in the IC” = Barr was a Navy SIGINT (signal intelligence) guy before he took the job with Northrop Grumman.
POSTED: Magpii

==========

Ray,
I'd like to introduce you to Aaron Barr. Aaron spent some time working in the IC before moving to NG. He has been thinking about the same problem that the "cyber accelerator" is meant to solve. In fact, his way of thinking is extremely similar to yours. Aaron's has some very interesting ideas that could dovetail nicely with both the accelerator and the CID demos. The two of you have to get together and chat. Can I set something up the week of the 17th?
Regards,
Irv

Irving Lachow, Ph.D.
Director, Cyber Programs
Special Capabilities Office

http://hbgary.anonleaks.ch/aaron_hbgary_com/1266.html Irving Lachow to Aaron Barr. 6 May 2010. We don't find out what DAC is but later in the thread we'll see that Barr was seeking funding for a social media start who's sole purpose was spying on Americans.
POSTED: Magpii

Aaron,
All of the DAC funds are committed for this year. If we want to do something in FY10, we'll need to find someone who is willing to support this themselves (maybe with end-of-year funds). Maybe you can work with your buddies at Palantir to scope out who would be willing to fund such a pilot.
Cheers,
Irv

Irving Lachow, Ph.D.
Director, Cyber Programs
Special Capabilities Office

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/15511h.html Colonel Lincoln Leibner, US Army Operations & Technology Office to Aaron Barr. 7 May 2010. This was facilitated by Irving Lachow. FOUO = For Official Use Only.
POSTED: Magpii
==========
Classification: UNCLASSIFIED
Caveats: FOUO

Irv, are we good for 1200 at your space? ~ Lincoln

Lieutenant Colonel Lincoln Leibner
United States Army
Operations and Technology Office
703-697-7131

From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Friday, May 07, 2010 16:58
To: Leibner, Lincoln D LTC MIL US USA DCS G-3/5/7
Cc: Lachow, Irving Mr OSD ATL
Subject: Re: Can we meet on the 12th at 1300? (UNCLASSIFIED)

Good for me.
Aaron

Sent from my iPad

On May 7, 2010, at 4:55 PM, "Leibner, Lincoln D LTC MIL US USA DCS G-3/5/7" <lincoln.leibner@us.army.mil> wrote:

Classification: UNCLASSIFIED
Caveats: FOUO

Can we do 1200?

Lieutenant Colonel Lincoln Leibner
United States Army
Operations and Technology Office
703-697-7131

From: Lachow, Irving Mr OSD ATL [mailto:Irving.Lachow@osd.mil]
Sent: Friday, May 07, 2010 16:38
To: Leibner, Lincoln D LTC MIL US USA DCS G-3/5/7; 'Aaron Barr'
Subject: Can we meet on the 12th at 1300?

Irving Lachow, Ph.D.

Director, Cyber Programs

Special Capabilities Office

NIPR: irving.lachow@osd.mil

SIPR: irving.lachow@osd.smil.mil

JWICS: irving.lachow@osdj.ic.gov

Office: (703) 746-1226

Cell: (202) 556-0591

Classification: UNCLASSIFIED
Caveats: FOUO

Classification: UNCLASSIFIED
Caveats: FOUO

==========

http://hbgary.anonleaks.ch/aaron_hbgary_com/5049.html Aaron Barr to Colonel Lincoln Leibner. 13 May 2010. We'll later learn the plan is to fund a social media startup that will offer enough value that people will submit to being micromonitored by the U.S. government.
POSTED: Magpii
==========

Yes something like that. As a commercial solution a few things this solution doesn't have to worry about:
1) hiding itself on the phone, and I mean really hiding itself.
2) hiding the communications traffic going out.
But there are ways to accomplish this.

There are also other ways to approach this. Most people are concerned about privacy until they get something in return for what they give up. I remember a few years ago the thought of providing information about what you were interested in, where you were, etc. evoked strong emotions. It still does but the tide is quickly shifting and people are readily giving up their private information because they feel they are personally benefiting from what they give up. Concerns over privacy interestingly are becoming less and less of an issue commercially, at an individual level. The special interest groups will keep it in the news though.

You had mentioned a few specific platforms, this being one of them. We can deep dive on any one of these as we have experience in pretty much all of them, including Virtual Worlds, MMOs, and mobile devices.

It was good meeting you Lincoln. Let me know how I can help.

Aaron

On May 13, 2010, at 8:24 AM, Leibner, Lincoln D LTC MIL US USA DCS G-3/5/7 wrote:

> Classification: UNCLASSIFIED
> Caveats: FOUO
>
>
http://www.informationweek.com/news/mobility/security/showArticle.jhtml?articleID=224700437&queryText=mobile%20and%20spy%20and%20tracks%20and%20android
>
>
> Lieutenant Colonel Lincoln Leibner
> United States Army
> Operations and Technology Office
> 703-697-7131
> Classification: UNCLASSIFIED
> Caveats: FOUO

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/6686.html Aaron Barr to Ray Owen and Nathan Atherley of Farallon Research and Irving Lachow. 20 May 2010. The social media Trojan horse is named Magpii – short for "Magnify Personal Identifying Information". You will see the PII acronym used in other places – it's an industry standard term.
POSTED: Magpii
==========
Thoughts on service that sets it apart. Btw we have a registered name we were thinking of using, Magpii. The slogan is "where the web meets

life". It's all about storing and organizing information as you live.

Each spot on the map has a page, categorized; Business pages, events, landmarks, etc. So instead of web pages you have location pages. Users have their own personal information management pages where they can organize their preferences, calendar, associations, etc. As you upload content the content is associated with location pages as well as your personal page.

Picture a partnership with national parks or smithsonian. Your standing near the lincoln memorial and you see a list of events, other peoples comments on their experience, photos. Read a history of the monument, save this as a favorite so you then get fed information about events at this place on your personal page.

We can link in many different services. Yelp for business reviews and comments under the business pages. Facebook and Twitter for user list and associations, eventful for events, etc.

A good article on why VCs think Foursquare is worth $100m.

http://www.businessinsider.com/why-vcs-think-foursquare-is-worth-100-million-2010-4
Foursquare was just offered $10

All this and their service really provides little of substantive value. The way I would break the local advertising market is this. I would not do what everyone else is doing and focusing on chains and retail channel partners. I would pick three target markets, DC, Denver, San Francisco. Hire college students to knock on doors, show businesses the service and offer the first year free for early adopters. My channel partners would be local governments, national parks, event coordinators. Focus on delivering the content and engaging the local businesses at a grassroots level. Have to lure the users with substantive content.

Dave,

Attached is the brief you requested.

I found the presentation you mentioned. I agree good message. I read some comments concerning it being a little over the top, maybe, but its hard when the vulnerabilities and the risk are so great.

I agree most organizations are very reactive. I think most are starting to turn and willing to spend money on technology and people that will make them more secure, but I think most don't know how to go about building for protection. They build for compliance, which doesn't at all keep you secure today, but that is what they know how to build to, they don't know how to build to protect their specific organization.

The measures of effectiveness are definitely difficult to quantify. But I think there are ways to do it. As follow-on to training I think

organizations need to test their employees, try to compromise them. If nothing else that can provide valuable statistics on what is working and whats not getting through.

Let me know when is a good time to get together.

==========

http://hbgary.anonleaks.ch/aaron_hbgary_com/4082.html David Merritt, CIO for the Office of Secretary of Defense to Aaron Barr. 18 Jun 2010. This isn't all that related to the rest of the thread off this discussion. Included here because this is the bulk of the conversation Barr had with OSD and here we see him talking to a very senior person. POSTED: Magpii

==========

On Jun 18, 2010, at 7:57 AM, Merritt, David CTR OSD CIO wrote:

> Look for a briefing from SAIC called Killing with Keyboards. Its targeted to the military industrial base, but it has a good message.
>
> My background includes MCI, RSA, Pentasafe, as well as being a former 163x. One thing I remember is in the private sector (as you most likely has seen), the attitude is that of extreme reactive--we aren't going to spend money unless we really really have to...either through a breach or compliance to governance/regulation. When you can show the exfiltration, they then see the light.
>
> When the DTM came out opening access to SNSs, we cringed and waited for the first of the breaches.
>
> I'm surprised that people don't block pdfs with javascript. Then you just have to deal with user awareness. When I was at MCI we had a pro services offering of a quarterly security stand down to brief the employees. The hard part is user perception.--if you are doing thing right, how do you know its working (vs they weren't being manipulated)..
>
> I live in Reston. Maybe we need to get together for a few beers.
>
> Rich Cummings was by to brief us a month or so ago.
>
> Two techs I like is yours and palintar...but we are low on budget right now.
>
> What you might consider is the "embedded analyst" like palintar has. That way the customer has "0 day" engagement capability.
>
> Dave
> -------------------------
> David D. Merritt, CISSP, CISM, ITIL
> Office of the Secretary of Defense
> 703.699.3568
>
>

> ----- Original Message -----
> From: Aaron Barr <aaron@hbgary.com>
> To: Merritt, David CTR OSD CIO
> Sent: Fri Jun 18 07:23:05 2010
> Subject: Re: REBL
>
> Dave,
>
> Absolutely. I am down at the FIRST conference and don't have it with
> me but I will send it when I get back. A few questions.
>
> I am thinking of developing a training curriculum to help people and
> organizations understand the threats of social networks and related
> technologies and what can be done to improve exposure of information.
> Do you think that would be of interest to organizations as a service?
>
> Second, any interest in getting together and discussing how we
> incorporate this knowledge, our malware analysis capability with some
> partner technology such as Fidelis. If it's ok I will forward to you
> a datasheet for you to review.
>
> Aaron
>
> Sent from my iPad
>
> On Jun 17, 2010, at 8:12 AM, "Merritt, David CTR OSD CIO"
> <David.Merritt.ctr@osd.mil> wrote:
>
>> Aaron,
>>
>> Can I get a copy of the presentation you and Greg gave at Johns
Hopkins this week?
>>
>> Dave
>>
>> Haze gray and under way make a fine Navy day...
>> -------------------------
>> David D. Merritt, CISSP, CISM, ITIL
>> Office of the Secretary of Defense
>> 703.699.3568

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/2410.html Tom Conroy of Northrop Grumman introducing Brian Hibblen of OSD and Aaron Barr.8 Jul 2010. Nothing so exciting here, just putting Conroy in context – he is a big player in other ways.
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.

==========
The Google can’t find this one for linking, but it’s David Merritt, CIO of the Office of the Secretary of Defense, asking if the corpus of malware Aaron Barr is using was compiled from Greg Hoglund’s RootKit.com 21 Jul 2010.
POSTED: Magpii
==========

What format is required for processing within the tool?

Were these compiled from rootkit.com?

Dave

David D. Merritt, CISSP, CISM, ITIL
OSD CIO IA
703-697-2051 :desk

-----Original Message-----
From: Aaron Barr [mailto:aaron@hbgary.com]
Sent: Friday, July 16, 2010 10:27 PM
To: Aaron Barr
Subject: Attribution

I am sending this request to a small group of individuals. Please do not forward this email to third parties. HBGary is working hard to help solve the attribution problem. We have developed a fingerprint tool which extracts toolmarks left behind in malware executables. We use these toolmarks to cluster exploits together which were compiled on the same computer system or development environment. Notice the clusters in the graphic below. These groupings illustrate the relationships between over 3000 malware samples.

We need your help to further validate and improve the tool. Eventually youcan imagine combining this data with open source and intelligence data. I can see attribution as potentially a solvable problem. We need your malware samples, as many as you can provide. This is not something we are looking to profit from directly, we will be giving this tool away at Blackhat, so helping us improve the tool will help the community beat back the threat.

If possible please have your representative CISOs or cybersecurity personnel send malware samples in a password protected zip file. Provide the password via phone 719-510-8478 or fax to: 720-836-4208 we need your samples as soon as possible. Samples provided will not be shared with third parties and your participation will be held in strict confidence.

In exchange for your help, I will provide you with a summary report of our findings and you will have made a significant contribution to securing America's networks.

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/11967.html Aaron Barr to Chris ??? at Endgame Systems. 18 Jul 2010. The message bounced, but it puts Endgame, the operators of IPtrust.com, in the middle of this discussion

---

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/916.html Aaron Barr to David Merritt OSD CIO 21 Sep 2010. They're talking about how Russian funded flash games for social networks are a threat vector. This is deadly serious – it's a well known problem among security folk.
POSTED: Magpii
==========

Ha. I will check it out.

I figured out a new social media exploit vector using the evite systems yesterday. I unleashed it on our own company and got nearly 100% click through. I have a social media pen test methodology which works very successfully for targeted exploitation. This is going to

become the norm I think. Hold on it's going to be a fun ride.

Aaron

Sent from my iPhone

On Sep 21, 2010, at 1:04 PM, "Merritt, David CTR OSD CIO" <David.Merritt.ctr@osd.mil> wrote:

> ChatRoulette.com is a new interesting site...random webcam chats...and of
> course Russian funded and built.
>
> But then facebook and zenga games are heavily funded by Moscow...
>
> http://techcrunch.com/2010/03/16/chatroulette-stats-male-perverts/
>
> Dave

---

http://hbgary.anonleaks.ch/aaron_hbgary_com/10285.html Rosemary Wenchel to Mark Peterson, Ray Owen of Farallon Research and Aaron Barr. We don't know what she sent or who specifically at the DoJ received it, but it was 3 Feb 2011, so we can make some educated guesses, and this gives us her title and information about her job, which we didn't have previously.

==========

Sent from OSD OGC to DoJ/FBI

Rosemary Wenchel
Director
Cyber, Warfighter Innovation and Strategic Engagement
OSD OUSD(I)/J&CWS
rosemary.wenchel@osd.mil
703.697.3829

Anons have been using the name "Metal Gear" to describe a project involving Booz Allen Hamilton. We can't find any use of that phrase, nor have we identified where BAH is involved.

What we do have is a clear sign that two very senior people at the Office of the Secretary of Defense were steering resources towards Barr and his project Magpii, a social media effort that would quietly include pervasive spying as a feature. The motivation appears to be an arms race with Russian flash game developers.

Are you laughing? Well, don't – NATO members agreed in 2010 that if they could properly attribute a cyber attack they would be able to use a kinetic response.