Anonymous vs. Aaron Barr

A Postmortem Study

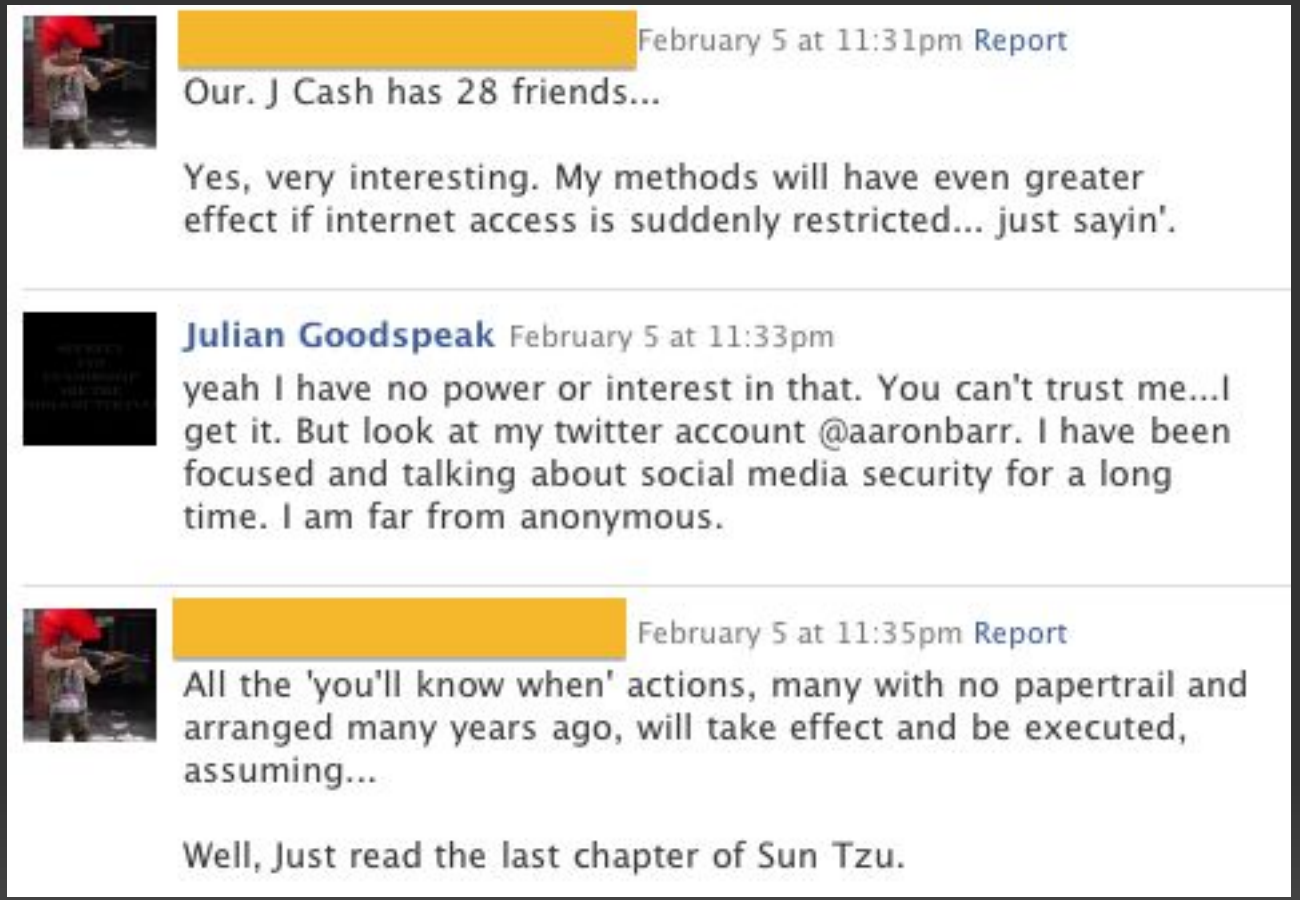
Justin Hall
Senior Security Architect, CBTS

About your speaker

Our story begins...

Who is Anonymous?

Kicking the hornet's nest.


[redacted] February 5 at 11:31pm Report
Our. J Cash has 28 friends...

Yes, very interesting. My methods will have even greater effect if internet access is suddenly restricted... just sayin'.

Julian Goodspeak February 5 at 11:33pm
yeah I have no power or interest in that. You can't trust me...I get it. But look at my twitter account @aaronbarr. I have been focused and talking about social media security for a long time. I am far from anonymous.

[redacted] February 5 at 11:35pm Report
All the 'you'll know when' actions, many with no papertrail and arranged many years ago, will take effect and be executed, assuming...

Well, Just read the last chapter of Sun Tzu.

Now you've done it.

rootkit.com cleartext passwords

On February 6, 2011, as part of their attack on HBGary, the Anonymous group social engineered administrator of rootkit.com, Jussi Jaakonaho, to gain root access to rootkit.com. The entire MySQL database backup was then released by Anonymous and announced using HBGary's CEO Twitter account, @aaronbarr: *Sup, here's rootkit.com MySQL Backup http://stfu.cc/rootkit_com_mysqlbackup_02_06_11.gz #hbgary #rootkit #anonymous*. The table below is the list of accounts found in rootkit.com MySQL database backup with passwords in cleartext.

JtR is used to translate the password to cleartext_password. Most of the passwords were successfully acquired by feeding a password dictionary (17.5MB) to JtR and the rest are being acquired by using JtR incremental mode. Among the passwords found at rootkit.com, the following are the 10 most used passwords:

Rank	Password	Accounts
1	123456	1023
2	password	392
3	rootkit	341
4	111111	190
5	12345678	181
6	qwerty	175
7	123456789	170

Anonymous has some fun.

HBGary Email Viewer

greg@hbgary.com

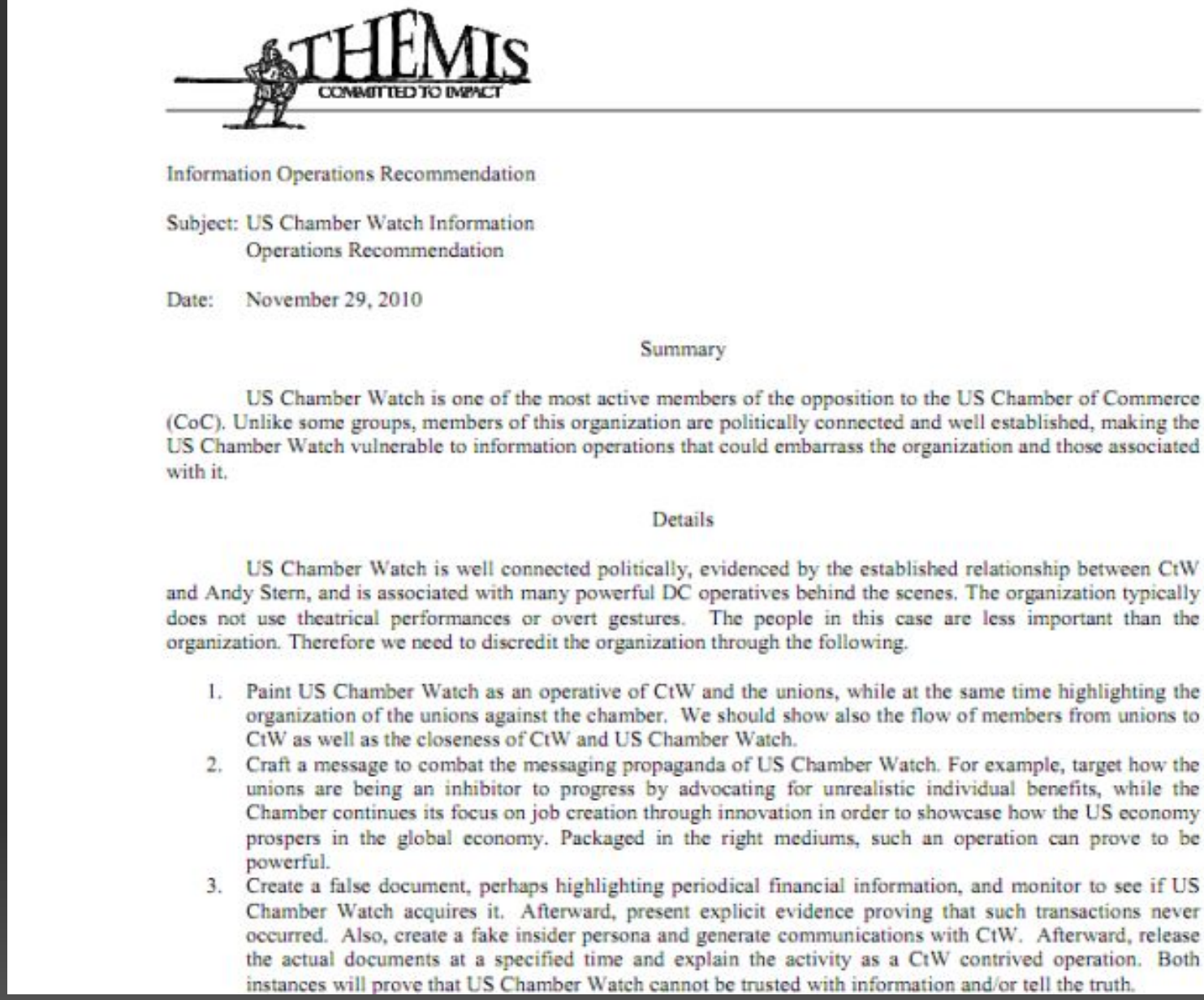
Next page >>

Jumplist...

Tweet 0

Sender	Subject	Date	Attachments
"John Zee" <zee@airmail.net>	#>	Can You Suggest A Chief Technology Officer? NW Security (LAX)		1
jussi jaakonaho <jussij@gmail.com>	#> Re: need to ssh into rootkit	Sun Feb 6 2011 20:15:54	
Aaron Barr <aaron@hbgary.com>	#> Re: Google Alert - HBgary	Sun Feb 6 2011 20:06:11	
Martin Pillion <pillion@gmail.com>	#> Aaron's story has hit slashdot and yahoo...	Sun Feb 6 2011 19:31:41	
Karen Burke <karenmaryburke@yahoo.com>	#> Fw: Google Alert - HBgary	Sun Feb 6 2011 19:02:42	
Karen Burke <karenmaryburke@yahoo.com>	#> Slashdot Coverage	Sun Feb 6 2011 19:01:39	
Karen Burke <karen@hbgary.com>	#> Re: RSAC 2011 Podcast HT1-402 - Follow the Digital Trail: UsingForensics to Identify Attackers and Malware Authors	Sun Feb 6 2011 17:57:35	
HBGary INC <support@hbgary.com>	#> [HBGary] Password Lost/Changed	Sun Feb 6 2011 17:56:17	
"Penny Leavy-Hoglund" <penny@hbgary.com>	#> Some Stories	Sun Feb 6 2011 17:45:08	
<Stuart_McClure@McAfee.com>	#> RE: tShot	Sun Feb 6 2011 17:08:12	
Karen Burke <karenmaryburke@yahoo.com>	#> Fw: Google Alert - HBGARY	Sun Feb 6 2011 16:54:50	
"Penny Leavy-Hoglund" <penny@hbgary.com>	#> RE: Now we are being directly threatened.	Sun Feb 6 2011 16:51:35	
Aaron Barr <aaron@hbgary.com>	#> Now we are being directly threatened.	Sun Feb 6 2011 16:25:28	1
Karen Burke <karen@hbgary.com>	#> Attachments	Sun Feb 6 2011 15:57:28	
Karen Burke <karen@hbgary.com>	#> Re: Final - for me.	Sun Feb 6 2011 15:53:14	

9GB of internal email made public.



THEMIS
COMMITTED TO IMPACT

Information Operations Recommendation

Subject: US Chamber Watch Information Operations Recommendation

Date: November 29, 2010

Summary

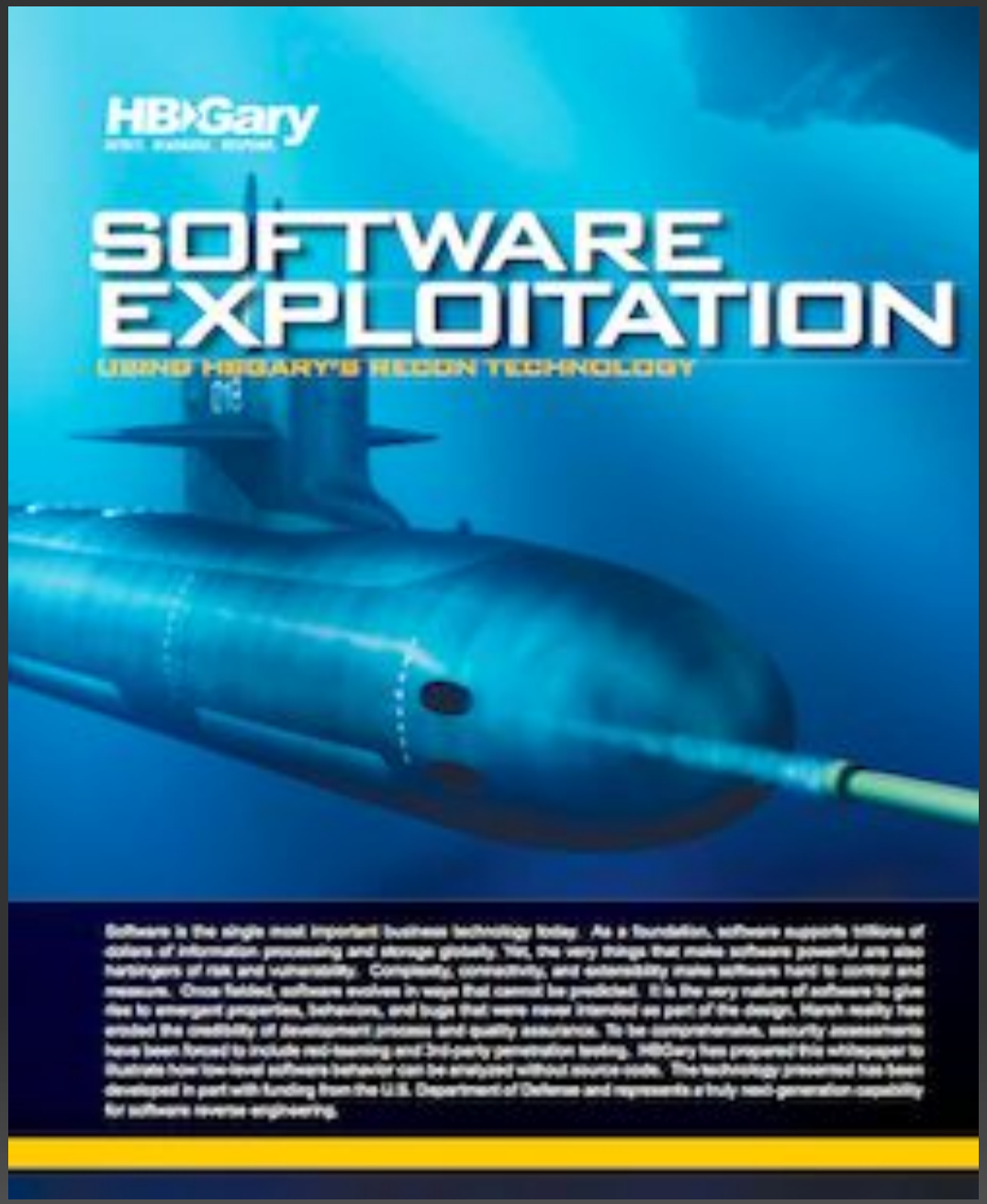
US Chamber Watch is one of the most active members of the opposition to the US Chamber of Commerce (CoC). Unlike some groups, members of this organization are politically connected and well established, making the US Chamber Watch vulnerable to information operations that could embarrass the organization and those associated with it.

Details

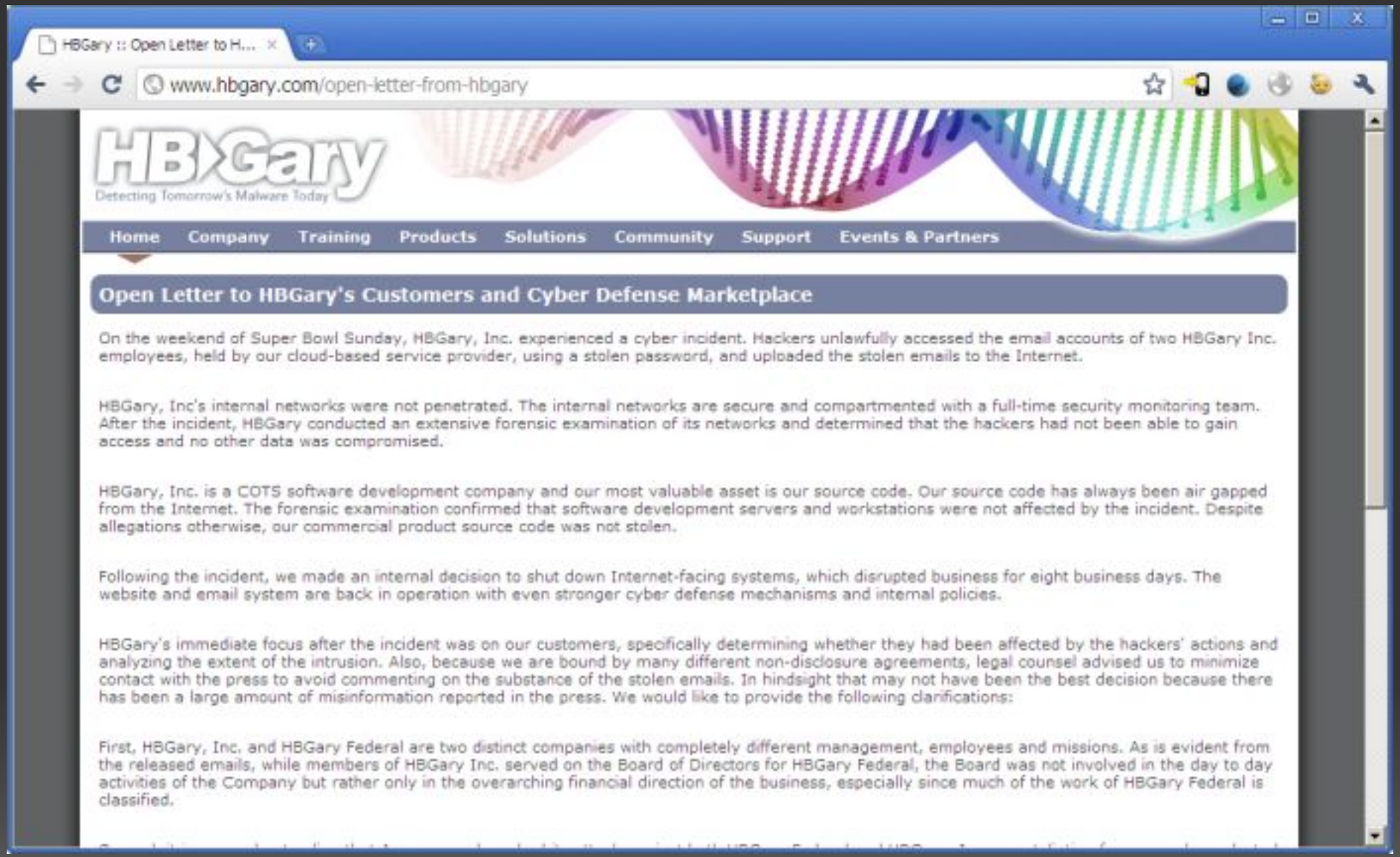
US Chamber Watch is well connected politically, evidenced by the established relationship between CtW and Andy Stern, and is associated with many powerful DC operatives behind the scenes. The organization typically does not use theatrical performances or overt gestures. The people in this case are less important than the organization. Therefore we need to discredit the organization through the following.

1. Paint US Chamber Watch as an operative of CtW and the unions, while at the same time highlighting the organization of the unions against the chamber. We should show also the flow of members from unions to CtW as well as the closeness of CtW and US Chamber Watch.
2. Craft a message to combat the messaging propaganda of US Chamber Watch. For example, target how the unions are being an inhibitor to progress by advocating for unrealistic individual benefits, while the Chamber continues its focus on job creation through innovation in order to showcase how the US economy prospers in the global economy. Packaged in the right mediums, such an operation can prove to be powerful.
3. Create a false document, perhaps highlighting periodical financial information, and monitor to see if US Chamber Watch acquires it. Afterward, present explicit evidence proving that such transactions never occurred. Also, create a fake insider persona and generate communications with CtW. Afterward, release the actual documents at a specified time and explain the activity as a CtW contrived operation. Both instances will prove that US Chamber Watch cannot be trusted with information and/or tell the truth.

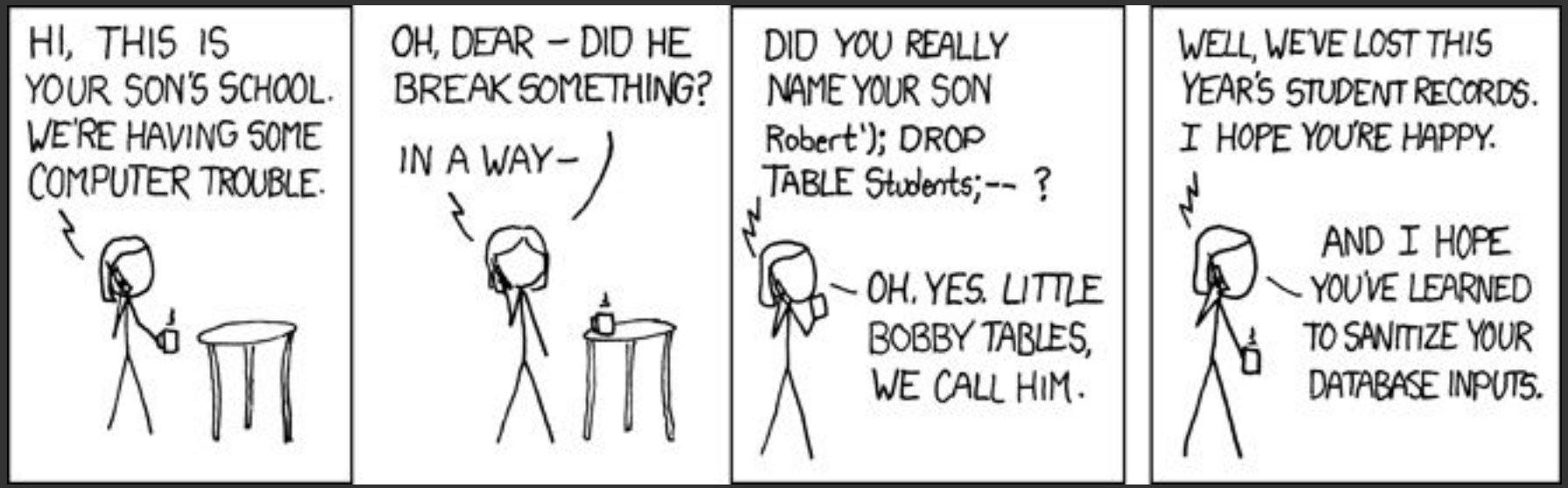
Team Themis' campaign.



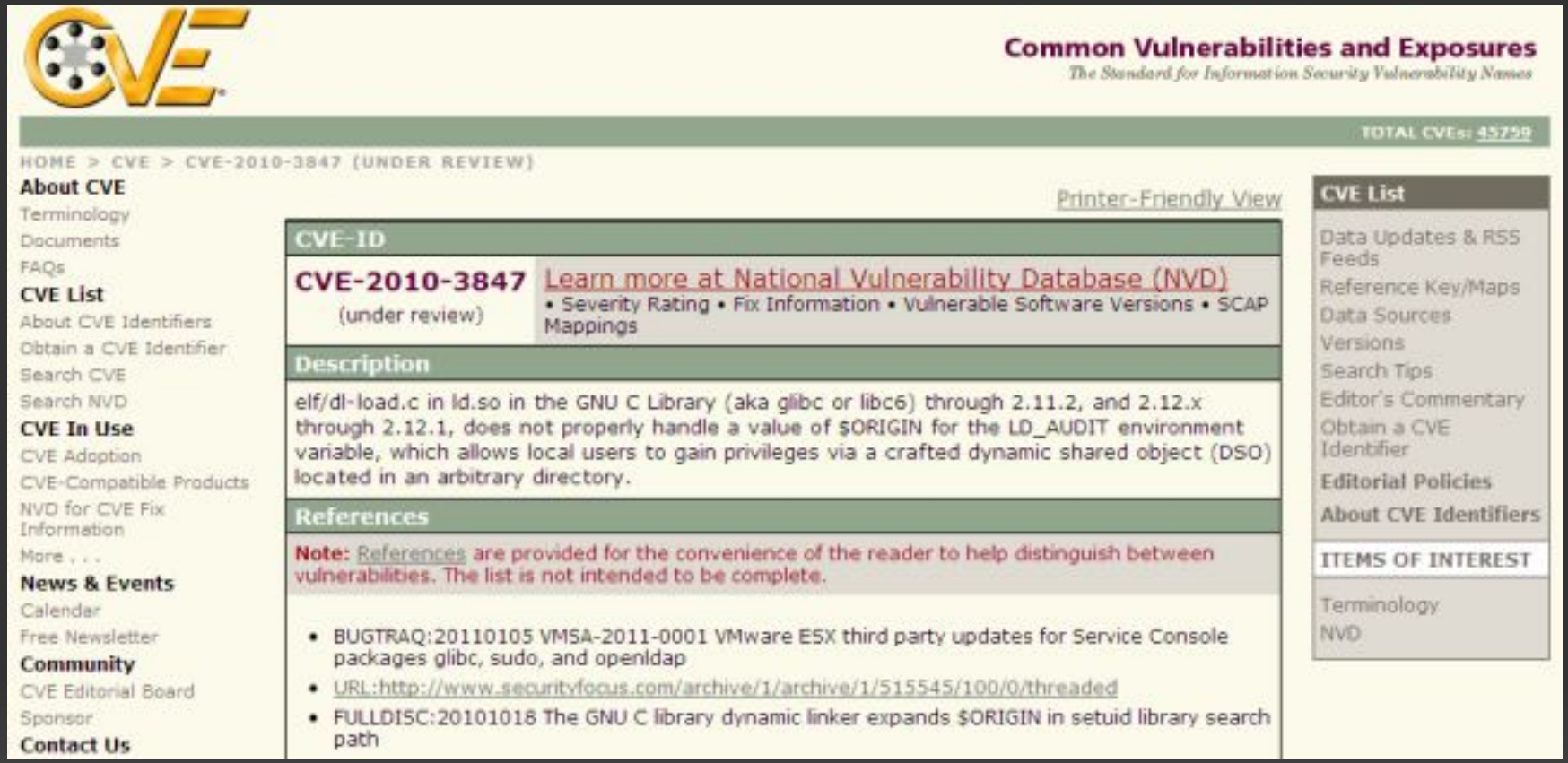
Custom rootkits for sale.


HBGary :: Open Letter to H...
www.hbgary.com/open-letter-from-hbgary
HBGary
Detecting Tomorrow's Malware Today
Home
Company
Training
Products
Solutions
Community
Support
Events & Partners
Open Letter to HBGary's Customers and Cyber Defense Marketplace
On the weekend of Super Bowl Sunday, HBGary, Inc. experienced a cyber incident. Hackers unlawfully accessed the email accounts of two HBGary Inc. employees, held by our cloud-based service provider, using a stolen password, and uploaded the stolen emails to the Internet.
HBGary, Inc's internal networks were not penetrated. The internal networks are secure and compartmented with a full-time security monitoring team. After the incident, HBGary conducted an extensive forensic examination of its networks and determined that the hackers had not been able to gain access and no other data was compromised.
HBGary, Inc. is a COTS software development company and our most valuable asset is our source code. Our source code has always been air gapped from the Internet. The forensic examination confirmed that software development servers and workstations were not affected by the incident. Despite allegations otherwise, our commercial product source code was not stolen.
Following the incident, we made an internal decision to shut down Internet-facing systems, which disrupted business for eight business days. The website and email system are back in operation with even stronger cyber defense mechanisms and internal policies.
HBGary's immediate focus after the incident was on our customers, specifically determining whether they had been affected by the hackers' actions and analyzing the extent of the intrusion. Also, because we are bound by many different non-disclosure agreements, legal counsel advised us to minimize contact with the press to avoid commenting on the substance of the stolen emails. In hindsight that may not have been the best decision because there has been a large amount of misinformation reported in the press. We would like to provide the following clarifications:
First, HBGary, Inc. and HBGary Federal are two distinct companies with completely different management, employees and missions. As is evident from the released emails, while members of HBGary Inc. served on the Board of Directors for HBGary Federal, the Board was not involved in the day to day activities of the Company but rather only in the overarching financial direction of the business, especially since much of the work of HBGary Federal is classified.

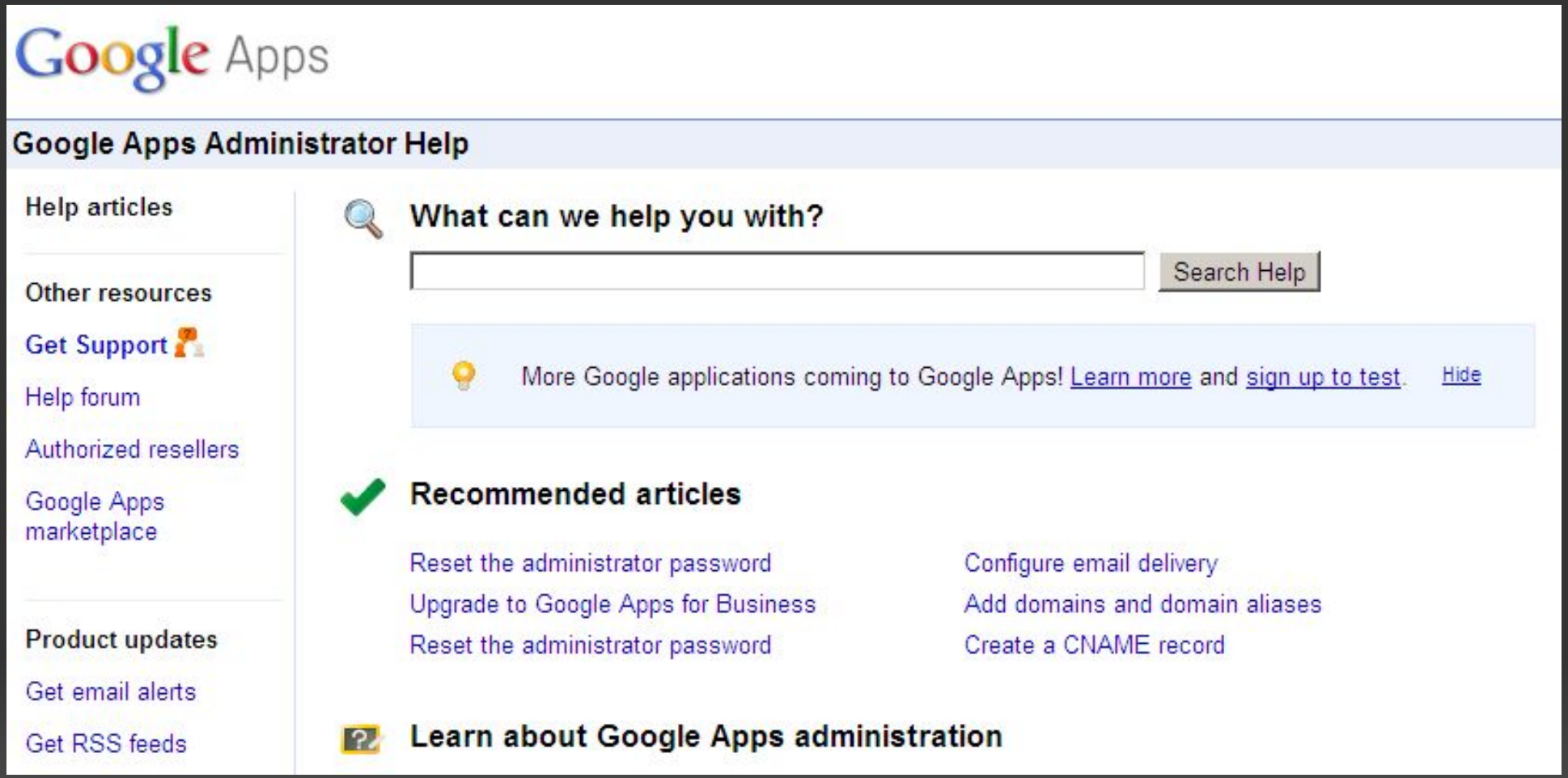
Kablooey



How did they break in?
Step 1: SQL Injection



Step 2: Shared credentials & privilege escalation



Step 3: Shared credentials & email harvesting

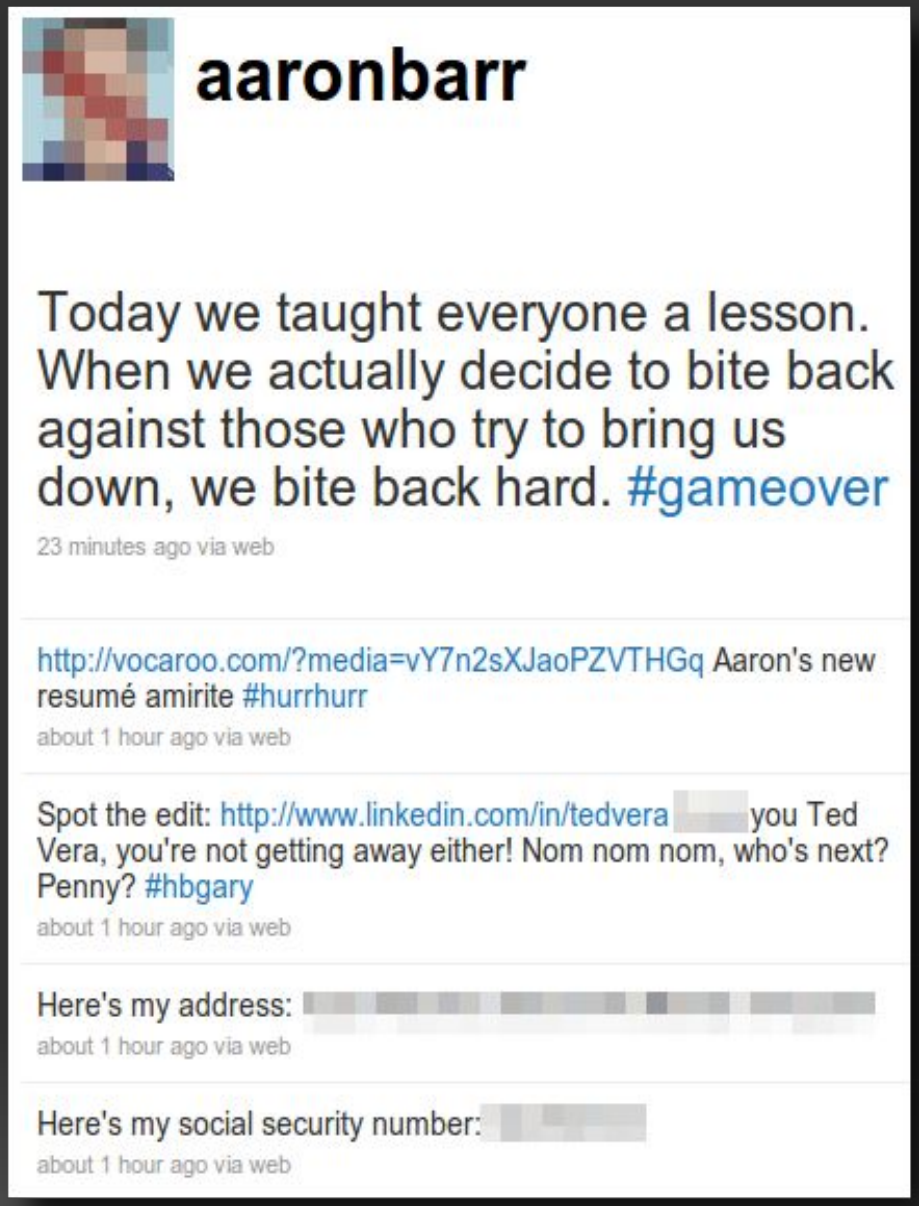
From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?
thanks

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
no i dont have the public ip with me at the moment because im ready for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me public ip and ill ssh in and reset my pw.

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
ok,
it should now accept from anywhere to 47152 as ssh. i am doing testing so that it works for sure.
your password is changeme123

Step 4: Social Engineering



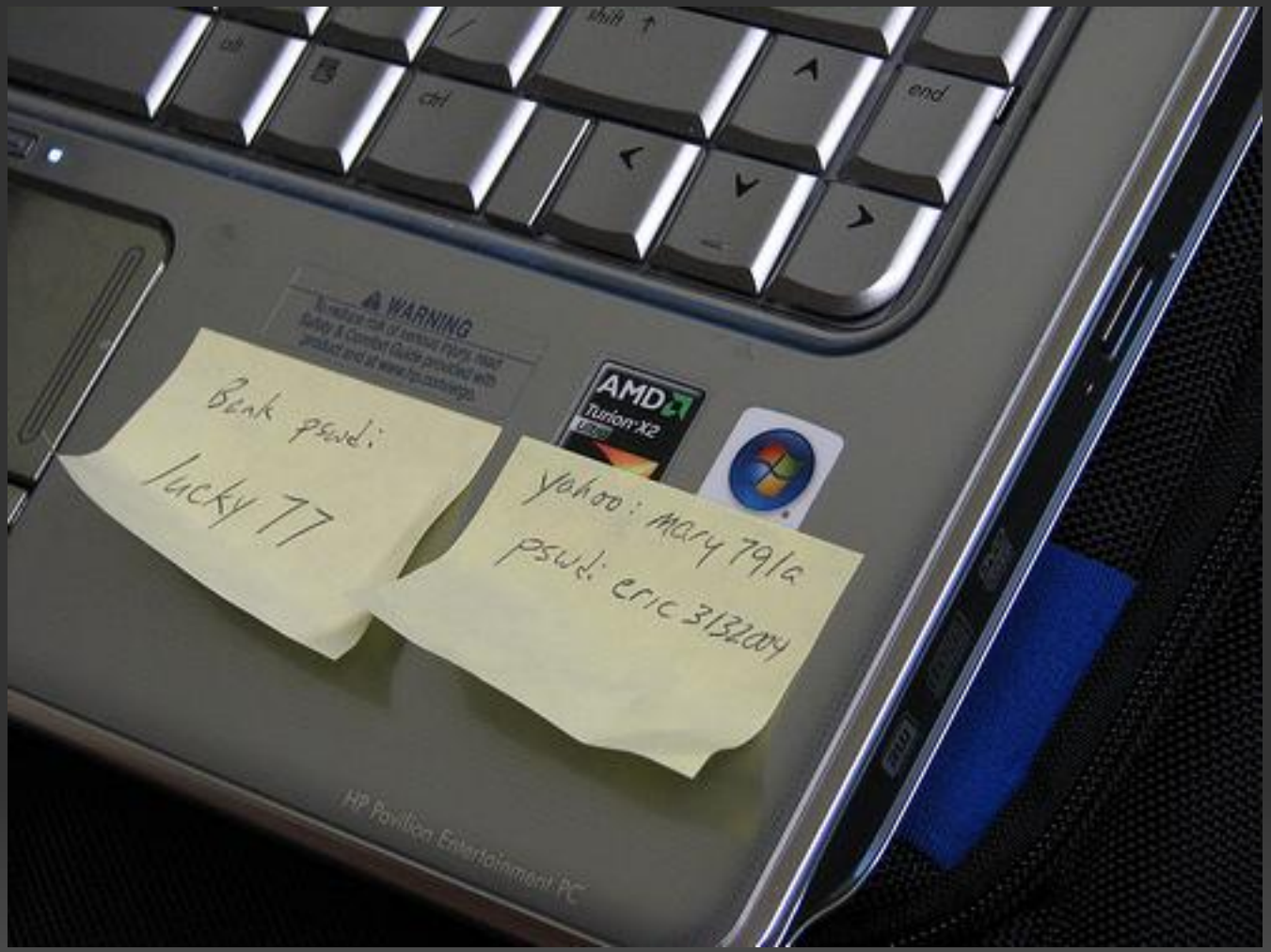
Step 5: Shared credentials & social networking

So what have we learned?

The Internet is still the wild west.

Be careful with your security research.

Develop your organization's security program.



NEVER use shared credentials!

From:	Greg Hoglund <greg@hbgary.com>
To:	John Verducci <john@studioem.com>, "Penny C. Hoglund" <penny@hbgary.com>, Aaron Barr <aaron@hbgary.com>, Karen Burke <karen@hbgary.com>
Date:	Wed, 29 Sep 2010 23:08:44 -0700
Subject:	viral marketing idea involving rap
click here to show full headers	
Attachments:	This e-mail does not have any attachments.

Team,

Please watch this video. It has the F word be warned.
http://www.youtube.com/watch?v=VgvM7av1o1Q

This is CCP. They are a customer of HBGary's. They are a game company, which might explain their off-the-wall antics.

I watch this and imagine our people at HBGary talking shit about Chinese Hackers and how Mandiant can't touch us. And yes, we use their First Name. Guidance too.

Maybe too bold, but I can't help but think the Jim's and Jeffrey's of the world would watch this and think "Holy Shit HBGary is Core". They would. And it would be viral. I can't help but think this would translate into more sales.

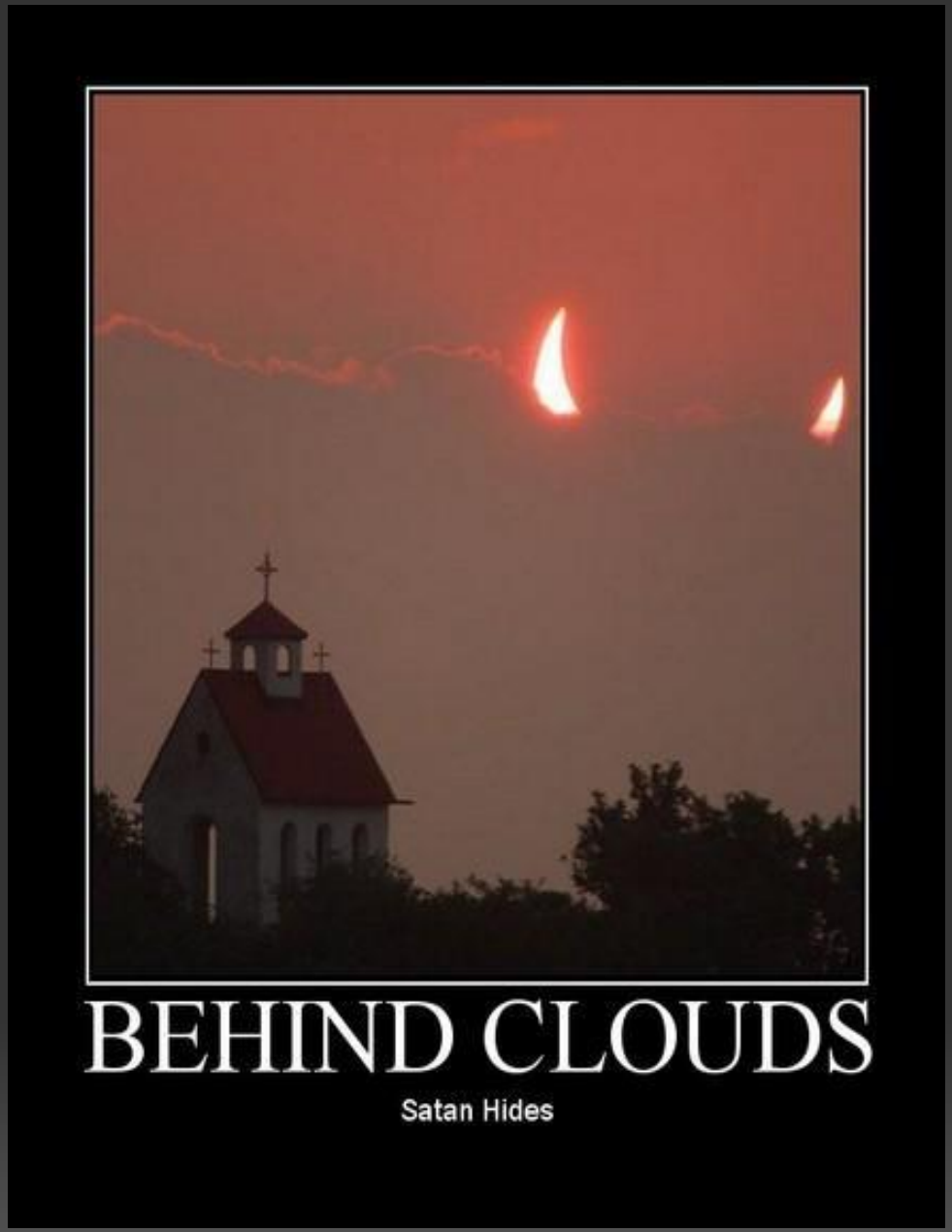
Can we organize a music video like this? Is this too left-field for a "security company". Why not - we are on the frontier - we are on the edge?

Can we have something like this developed for less than $20,000 ?? Is this just a dumb idea?

-Greg

ps. here is their outtake video - give you an idea how this was a real production (http://www.youtube.com/watch?v=g9E-iTpJ3U8)

Know what's in your email.



Be careful with cloud services.

Know your public exposure.

Questions?

justin.hall@cbts.cinbell.com