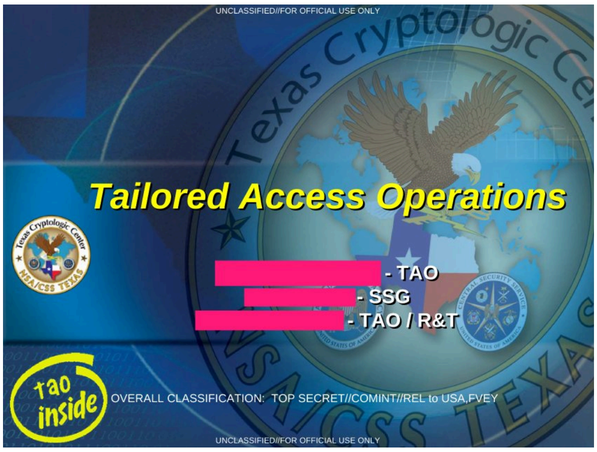
SHADOW BROKERS AND THE “SECOND SOURCE”

When I emphasized Der Spiegel’s reporting on TAO in this post on the tool for which Shadow Brokers recently released a manual, UNITEDRAKE, I was thinking along the same lines Electrospaces was here. Electrospaces lays out a universe of documents and reporting that doesn’t derive from Edward Snowden leaked documents, notes some similarity in content (a focus on NSA’s Tailored Access Operations), and the inclusion of documents from NSA’s San Antonio location. From that, Electrospaces posits that Shadow Brokers could be “identical with the Second Source.”

> With the documents published by the Shadow Brokers apparently being stolen by an insider at NSA, the obvious question is: could the Shadow Brokers be identical with the Second Source?
>
> One interesting fact is that the last revelation that could be attributed to the second source occured on February 23, 2016, and that in August of that year the Shadow Brokers started with their release of hacking files. This could mean that the second source decided to publish his documents in the more distinct and noticeable way under the guise of the Shadow Brokers.
>
> But there’s probably also a much more direct connection: the batch of documents published along with Der Spiegel’s main piece from December 29, 2013 include a presentation about the TAO unit at NSA’s Cryptologic Center in San Antonio, Texas, known as NSA/CSS Texas (NSAT):



UNCLASSIFIED//FOR OFFICIAL USE ONLY

Tailored Access Operations

[redacted] - TAO

[redacted] - SSG

[redacted] - TAO / R&T

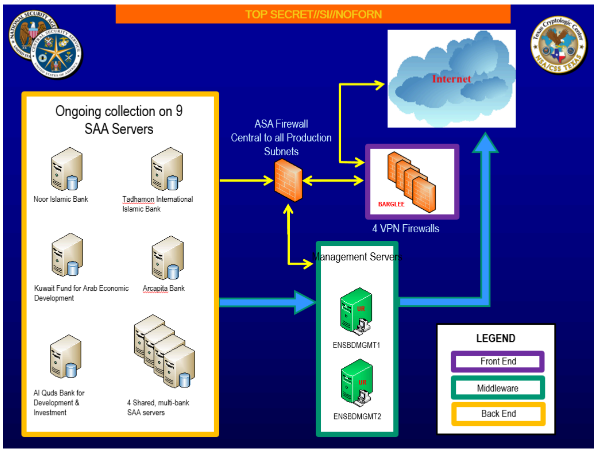
OVERALL CLASSIFICATION: TOP SECRET//COMINT//REL to USA,FVEY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Texas Cryptologic Center
NSA/CSS TEXAS
tao inside

TAO Texas presentation, published by Der Spiegel in December 2013

(click for the full presentation)*And surprisingly, the series of three slides that were released by the Shadow Brokers on April 14 were also from NSA/CSS Texas. They show three seals: in the upper left corner those of NSA and CSS and in the upper right corner that of the Texas Cryptologic Center:*



TOP SECRET//SI//NOFORN

Internet
Ongoing collection on 9 SAA Servers
Noor Islamic Bank
Tadhamon International Islamic Bank
Kuwait Fund for Arab Economic Development
Arcapita Bank
Al Quds Bank for Development & Investment
4 Shared, multi-bank SAA servers
ASA Firewall Central to all Production Subnets
BARGLEE
4 VPN Firewalls
Management Servers
ENSBDMGMT1
ENSBDMGMT2
LEGEND
Front End
Middleware
Back End

TAO Texas slide, published by the Shadow Brokers in April 2017

(click for the full

> *presentation)***NSA/CSS Texas***It’s quite remarkable that among the hundreds of NSA documents that have been published so far, there are only these two sets from NSA/CSS Texas, which is responsible for operations in Latin America, the Caribbean, and along the Atlantic littoral of Africa in support of the US Southern and Central Commands.Besides the one in San Antonio, Texas, NSA has three other regional* Cryptologic Centers *in the US: in Augusta, Georgia, in Honolulu, Hawaii and in Denver, Colorado. These four locations were established in 1995 as Regional Security Operations Centers (RSOC) in order to disperse operational facilities from the Washington DC area, providing redundancy in the event of an emergency.So far, no documents from any of these regional centers have been published, except for the two from NSA/CSS Texas. This could be a strong indication that they came from the same source – and it seems plausible to assume that that source is someone who*

> *actually worked at that NSA location in San Antonio.*

Frankly, I'm skeptical of the underlying reports that Shadow Brokers must be a disgruntled NSA employee or contractor, which derives in part from the conclusion that many of the files released include documents that had to be internal to NSA, and in part from this report that says that's the profile of the suspect the government is looking for.

> The U.S. government's counterintelligence investigation into the so-called Shadow Brokers group is currently focused on identifying a disgruntled, former U.S. intelligence community insider, multiple people familiar with the matter told CyberScoop.
>
> Sources tell CyberScoop that former NSA employees have been contacted by investigators in the probe to discover how a bevy of elite computer hacking tools fell into the Shadow Brokers' possession.
>
> Those sources asked for anonymity due to sensitivity of the investigation.
>
> While investigators believe that a former insider is involved, the expansive probe also spans other possibilities, including the threat of a current intelligence community employee being connected to the mysterious group.
>
> The investigatory effort is being led by a combination of professionals from the FBI, National Counterintelligence and Security Center (NCSC), and NSA's internal policing group known as Q Group.
>
> It's not clear if the former insider was once a contractor or in-house employee of the secretive agency. Two people

> familiar with the matter said the investigation "goes beyond" Harold Martin, the former Booz Allen Hamilton contractor who is currently facing charges for taking troves of classified material outside a secure environment.

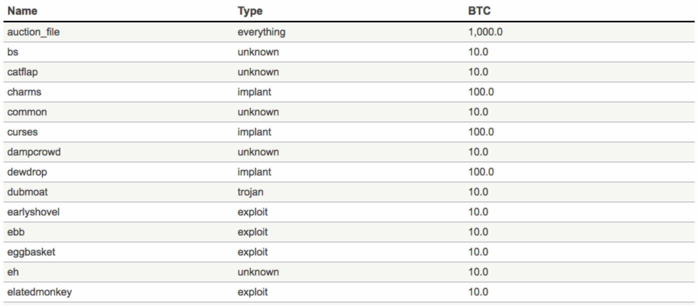
The report clearly suggests (and I confirmed with its author, Chris Bing) that the government is still testing out theories, and that the current profile (or the one they were chasing in July) happens to be an insider of some sort, but that they didn't have a specific insider in mind as the suspect.

There are a number of reasons I'm skeptical. First, part of that theory is based on Shadow Brokers making comments about Jake Williams that reflects some inside knowledge about an incident that happened while he was at NSA (Shadow Brokers has deleted most of his tweets, but they're available in this superb timeline).

> trying so hard so #**shadowbrokers** helping out…you having big mouth for former #**equationgroup** member what was name of.
>
> leak OddJob? Windows BITS persistence? CCI? Maybe not understand gravity of situation USG investigating members talked to Q group yet
>
> theshadowbrokers ISNOT in habit of outing #**equationgroup** members but had make exception for big mouth, keep talking shit @**msuiche** your next

Even there, Shadow Brokers was falsely suggesting that Matt Suiche, who's not even an American citizen, might be NSA. But things got worse in June, when Shadow Brokers thought he had doxed @drwolfff as a former NSA employee, only to have @drwolfff out himself as someone else entirely (see this post, where Shadow Brokers tried to pretend he hadn't made a mistake). So Shadow Brokers has been wrong about who is and was NSA more often than he has been right.

Another reason I doubt he’s a direct insider is because when he posted the filenames for Message 6, he listed a good many of the files as “unknown.” (Message 6 on Steemit, archived version)

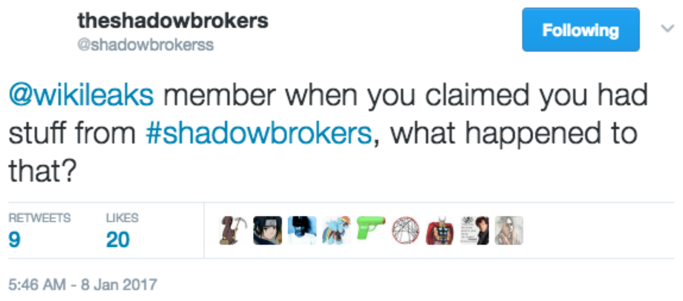


Name	Type	BTC
auction_file	everything	1,000.0
bs	unknown	10.0
catflap	unknown	10.0
charms	implant	100.0
common	unknown	10.0
curses	implant	100.0
dampcrowd	unknown	10.0
dewdrop	implant	100.0
dubmoat	trojan	10.0
earlyshovel	exploit	10.0
ebb	exploit	10.0
eggbasket	exploit	10.0
eh	unknown	10.0
elatedmonkey	exploit	10.0

That suggests that even if Shadow Brokers had some insider role, he wasn’t using these particular files directly (or didn’t want to advertise them as what they were).

And because I’m not convinced that Shadow Brokers is, personally, an insider, I’m not convinced that he necessarily is (as Electrospaces argues) “identical with the Second Source.”

Rather, I think it possible that Jacob Appelbaum and Shadow Brokers have a mutually shared source. That’s all the more intriguing given that Wikileaks once claimed that they had a copy of at least the first set of Shadow Brokers files, which Shadow Brokers recalled in January, and that Julian Assange released an insurance file days after Guccifer 2.0 first started posting hacked Democratic documents (see this post on the insurance file and this one on Shadow Brokers calling out WikiLeaks for hoarding that document).



theshadowbrokers
@shadowbrokerss

@wikileaks member when you claimed you had stuff from #shadowbrokers, what happened to that?

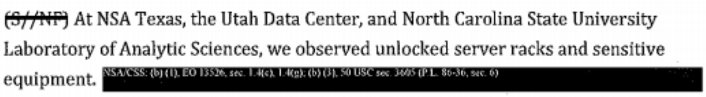
RETWEETS 9 LIKES 20

5:46 AM - 8 Jan 2017

Maybe they’re all bullshitting. But given Electrospaces’ observation that some of the files (covering intercepts of US allies, often pertaining to trade deals) for which there is no known source went straight to WikiLeaks, I think a shared source is possible.

All that said, there’s one more detail I’d add to Electrospaces’ piece. As noted, he finds the inclusion, in both the Shadow Brokers and the Appelbaum files, of documents from NSA’s San Antonio location to be intriguing. So do I.

Which is why it’s worth noting that that location is among the three where — as late as the first half of 2016 — a DOD Inspector General audit found servers and other sensitive equipment unlocked.



~~(S//NF)~~ At NSA Texas, the Utah Data Center, and North Carolina State University Laboratory of Analytic Sciences, we observed unlocked server racks and sensitive equipment. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [redacted]

An unlocked server would in no way explain all of the files included even in a narrowly scoped collection of “Second Source” files. But it would indicate that the San Antonio facility was among those that wasn’t adequately secured years after the Snowden leaks.