THE SHADOW BROKERS: “A NICE LITTLE NSA YOU’VE GOT HERE; IT’D BE A SHAME IF…”

When President Obama discussed how to retaliate against Russia for hacking the DNC last Friday, he described the trick of finding “an appropriate response that increases costs for them for behavior like this in the future, but does not create problems for us.” Aside from questions of efficacy, Obama raised something that a number of people looking for a big explosive response seem to have forgotten: that any response may create problems for us.

Which is why I find it curious that — aside from this one piece by Krypt3ia — no one factored in another cyber-attack on the US in discussions about retaliation, one that is, at least in execution, on-going: the release of NSA tools by a group calling itself the Shadow Brokers.

I’ve put a rough timeline (!) below. But as it shows, several weeks after the initial release of the DNC emails led to Debbie Wasserman Schultz’s resignation, the Shadow Brokers posted the first of what have thus far been 6 messages. Especially recently, the timing of the Shadow Brokers releases correlates in interesting ways with developments in the DNC hack. At the very least, the coincidence suggests the threat of further exposure of NSA’s hacking may be a factor in discussions about a response.

Release One: Burning US firewall providers

The first Shadow Brokers post announced an auction of Equation Group (that is, NSA offensive hacking) files. It released enough files to make it clear that a number of firewall companies, including several American companies,

had been targeted by the NSA. Accompanying the release was a rant that indirectly pointed to the Clintons — discussing blowjobs and running for President — but at that point, there was not much focus about whether these files were related to the Russian hacking and, more importantly, not a ton of focus on the files in discussions of the Russian hacking. That is, while many people assumed Russia might be the culprit, that it might fell out of the discussion.

Two weeks later, the FBI arrested Hal Martin, a(nother) Booz Allen contractor that — the NYT story that revealed his arrested — served as a ready scapegoat for the files.

The very next day, Shadow Brokers posted its second message, the first of several proving that it was not, personally, Hal Martin. It was basically a play on Team America's Kim Jong Il character, asking why everyone was so stupid.

A few days later, on September 5, President Obama gave Vladimir Putin the first of several warnings about the hacking — understood to be the DNC hacking (reportedly, no one knew about the Podesta hack yet, even though the emails had been stolen in March).

Almost a month passed before Shadow Brokers posted again, on October 1, basically whining about no one playing in the auction. The following two weeks are critical in the DNC hack rollout.

On October 7, two leaks distract from the IC attribution announcement

On October 7, three things happen (well, more, but I'll come back to that): First, ODNI and DHS released their statement blaming Russia for the hack. The WaPo published the Access Hollywood

“Grab them by the pussy” video. And WikiLeaks started releasing the Podesta emails.

Side note: This weekend, Podesta complained about the latter two events, describing how they came out just an hour apart. People even disputed the claim. But in neither Podesta’s comment nor the fact-check are people mentioning that it’s not so much the Podesta emails distracted from the Trump video (which I don’t think to be the case anyway, because the GrabThemByThePussy really did distract us for a while), but both — and especially the video — distracting from the Russia implication.

A week later, the same NBC team that has been the recipient of other DNC hack related leaks published a dick-wagging story promising that the CIA was about to cyber-retaliate for the hacks.

The next day, Shadow Brokers released message number 4 calling off the auction. The Shadow Brokers post also crassly spoofs airplane Loretta Lynch’s meeting with Bill Clinton (there a cultural reference here I don’t get), bringing the message content of the SB series still closer to the context of the Hillary emails.

Release Two: ID alleged NSA targets and threaten the election

Thus far, mind you, Shadow Brokers had just released enough to seriously compromise America’s firewall companies and their relationship with the NSA — but had mostly just been making noise since the first release. That changed on October 30, less than two weeks before the election.

Most of the focus on this release has been on the data released: a set of IP addresses seemingly showing the addresses NSA had hacked or used as a proxy. The IP addresses were dated, so the release wasn’t exposing ongoing

operations, probably. But it did reveal a significant number of academic targets. It also showed that, several years before we drummed up the Iraq War, we were targeting the Organization for the Prohibition of Chemical Weapons. Unlike the first release, then, this one didn't so much help anyone hack. Instead, it identified who had been hacked, and the degree to which these were not obvious targets.

But the message from that release is, in retrospect, just as important. It includes a reference to the NBC dick-wagging story about CIA hacking Russia. It questions why the focus has been on the DNC hack and not the Shadow Brokers release, "hacking DNC is way way most important than EquationGroup losing capabilities. Amerikanskis is not knowing USSA cyber capabilities is being screwed." It invited people to hack the election.

> On November 8th, instead of not voting, maybe be stopping the vote all together? Maybe being grinch who stopped election from coming? Maybe hacking election is being the best idea? #hackelection2016.

And then it demanded payment or the bleeding would continue. "How bad do you want it to get? When you are ready to make the bleeding stop, payus,"

The next day, according to NBC, for the first time in his Administration, President Obama used the "Red Phone" communication system with Russia and discussed war, albeit in muddled terms.

Now, even aside from this timing, it makes more sense that Obama was reacting to the Shadow Brokers release than the DNC ones. Though Dems have suggested Russia kept hacking after the spring, that appears to have been more phishing attempts, not known theft of documents. As for the DNC and Podesta files, as Obama said on Friday, those files had already been stolen. Short of stopping WikiLeaks (and Ecuador had cut off Julian Assange's wifi access by then,

presumably in response to US pressure, though it had little impact on the release of the Podesta files), there was nothing that a call could do about the ongoing leaks pertaining to Hillary. There were, admittedly, the probes of state voter registration sites, but the IC has consistently stopped short of attributing those to Russia.

But a response to a threat to hack Russia?

Which would seem to suggest the IC believes that these Shadow Brokers files are coming from Russia.

Release Three: A broad array of alleged tools, including those that hacked Belgacom

Then things went quiet again for a while, until the leakapalooza starting on December 9, which was basically an effort by the Dems and some spooks to pressure Trump and/or delegitimize his election. Significantly, however, the December 9 WaPo story also reported, for the first time, that CIA knew who the cut-outs between Russia's hackers and Wikileaks were, something James Clapper said the IC didn't have as late as November 17. In addition, the NYT published its long piece describing the hack, told in a way to put the Dems in the best possible light (which is a polite way of saying it is not hard-hitting news).

So on December 14, a Motherboard post from a persona named Bocefus Cleetus points to a ZeroNet site with a set of files listed for individual sale (and aggregating all the past messages).

With regards to the files, here is HackerHouse's analysis, here is the Grugq's post on the technical aspect of the files, and a few of Shadow Brokers' most recent tweets allegedly

describe what some of the files are. The short version though is, like the original release, these are dated files, some of them triggering known interests of commentary on NSA's hacking. There's a good deal of variety in tools, some of which sound cool. One of them, at least according to Hacker House, is likely one of the tools used to hack Belgacom.

Interestingly, HackerHouse and the Grugq disagree as to what this array suggests about the source of the files. The Grugq argues that these files must come from inside the NSA, because there'd be no other explanation for all of them to be in the same place.

> ## *Why High Side?*
>
> The easiest way to tell this is high side [inside NSA's classified networks] gear, not a back hack from an ops box is that there is simply too much here. Its hard for me to explain because it requires a level of information security knowledge combined with understanding how cyber operations are conducted (which is different from pen tests or red teaming.)
>
> ## *The TAO of Cyber*
>
> Cyber operations are basically designed with operational security in mind. The operators create a minimal package of tooling needed for conducting exactly, only and specifically the operation they are doing. This means, for example, if they are hitting a telco Call Data Records (CDR) box, they will plan for what they are going to do on that specific computer and prepare the tools for only that plan and that computer. If those tools are captured, or there is a back hack up to their staging point, the loss is compartmented.

But HackerHouse argues they must be from a staging site (that is, external to the NSA) because they are binary files.

> The bulk of these projects are not provided in source code form and instead appear to be binary files, which further strengthens the hypothesis that these files were compromised from an operational staging post or actively obtained from a field operation. If they had been in source code format then this would suggest an insider leak is more likely, binary files are often used in operations over their source code counterpart.

For what it's worth, in the first post, Shadow Brokers claims it tracked EG's traffic. "We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group." But it is worth noting that, 4 months after the first leak, tech folks are still disputing whether these must have come from inside our outside the NSA.

Assuming no one buys these files, then, the release has done several things. First, it provided Belgacom and other potential targets of US hacking more evidence they might use to identify an NSA hack. As such, it seems consistent with the earlier releases: not so damaging for current operations as it is for the exposure of who and how the US targets civilian targets.

But it also tells the NSA more about what Shadow Brokers has — at least some of the tools it has (in the first post, SB claimed NSA didn't know what it had), but also where they were obtained.

Cleetus' close commentary on recent

events

Which brings me to the message (post one, post two) of presumed Shadow Brokers persona, Bocefus Cleetus (as others have argued, a possible allusion to "ventriloquist dummy of FSB"), which the Grugq wrote about here. I suspect (this is a wildarseguess) Cleetus may serve as a temporally contingent way to alert the public to files that may have been out there for a while.

As the Grugq notes, the first message is interesting for its invocation of Rage against the Machine's "People of the Sun" juxtaposed against a background and fake discourse targeting caricatured Neo-Nazi Trump voters. He reads the former as a warning about invading brown people, but I think — given the stylistic fluidity across the six Shadow Brokers' messages — it might better be understood as mixed metaphors. RATM where one has been led to expect Hank Williams Jr.

There's also a reference to fake news. As with the October 30 release (assuming Cleetus is a persona of Shadow Brokers), this is also a piece responding to very current events.

But Cleetus' second message that is a far more interesting comment on immediate events. For example, from the first, it invokes NYT's blockbuster (which is remarkably favorable to the DNC) story on the hack, which has now been translated into Russia. Here's Cleetus' first line:

> After my shadow brokers tweet I was contacted by an anonymous source claiming to be FBI. Yep I know prove it? I wasn't able to get'em to verify their identity.

Here's an early line from the NYT story:

> "I had no way of differentiating the call I just received from a prank call," Mr. Tamene wrote in an internal memo,

> obtained by The New York Times, that detailed his contact with the F.B.I.

This line from Cleetus:

> The NSA has the global surveillance capabilities to intercept all the DNC and Podesta emails.

Seems to reflect Bill Binney's theory, which is that the NSA would know if there were really a hack because it would have seen the traffic.

> In other words, any data that is passed from the servers of the Democratic National Committee (DNC) or of Hillary Rodham Clinton (HRC) – or any other server in the U.S. – is collected by the NSA. These data transfers carry destination addresses in what are called packets, which enable the transfer to be traced and followed through the network.
>
> [snip]
>
> The bottom line is that the NSA would know where and how any "hacked" emails from the DNC, HRC or any other servers were routed through the network. This process can sometimes require a closer look into the routing to sort out intermediate clients, but in the end sender and recipient can be traced across the network.

There's the reference to the now-forgotten stink when Trump interviewed Mike Rogers.

> Clapper and Carter tried to get Rogers fired. They also called for the breakup of NSA.

That was first reported by the same folks who set off this leakapalooza.

> The heads of the Pentagon and the nation's intelligence community have

> recommended to President Obama that the director of the National Security Agency, Adm. Michael S. Rogers, be removed.
>
> The recommendation, delivered to the White House last month, was made by Defense Secretary Ashton B. Carter and Director of National Intelligence James R. Clapper Jr., according to several U.S. officials familiar with the matter.
>
> Action has been delayed, some administration officials said, because relieving Rogers of his duties is tied to another controversial recommendation: to create separate chains of command at the NSA and the military's cyberwarfare unit, a recommendation by Clapper and Carter that has been stalled because of other issues.

What ever happened to Trump's imminent plan to replace James Clapper with Mike Rogers amidst a big rearrangement of the spook desk chairs, I wonder? Has he completely forgotten Clapper is out of here on January 20, at noon sharp, Clapper said?

In any case, *those* bits directly echo very current news. But the rest of the post posits a fight between DOD and CIA, some of it rooted in equally real, if more dated, pissing contests.

> Look it up for yerself! DOD and CIA have had a turf war going back to the Afghanistan and Iraq Wars bout whose job it was to run paramilitary operations. A turf war over the next "domain of battle" with all the government cheese.

One reason Shadow Brokers' positing of a NSA-CIA spat — which the Grugq argues could not be real — is so interesting is because most of the recent reporting has forgotten NSA's centrality in all this and instead focused on an FBI-CIA split, which was artificially resolved by pre-

empting the President's press conference on Friday.

I don't think there's really an NSA-CIA pissing contest, though there may be an interesting detail here or there I'll return to.

But it brings us full circle. President Obama, in urging calm, invoked the kind of retaliation that might, "create problems for us." Those comments took place as if only the DNC and Podesta hacks were at issue (indeed, he made Martha Raddatz qualify what leaks the IC had blamed on Russia, and that's what she said). But it appears likely that the IC connects Shadow Broker to the other two. And the whole time we've been talking about retaliating, the Shadow Brokers has not so much been undercutting the NSA's bread and butter, but letting our allies and other neutral parties see precisely whom we conduct this dragnet on.

That sounds like something that might "create problems for us."

On October 30, Shadow Brokers taunted, "When you are ready to make the bleeding stop, payus, so we can move onto the next game." I think we're still in that first game.

Shadow Brokers Timeline

August 13: Message 1 Equation Group Warez Auction Invitation

> The name, in general, is a play on the villain from Mass Effect.
>
> GitHub, Reddit, Tumblr (see note), with takedowns as stolen property
>
> Message on Pastebin
>
> Claims files obtained by following EG traffic, claims EG doesn't know what it lost
>
> > We follow Equation Group traffic.

> We find Equation Group source range. We hack Equation Group.
>
> [snip]
>
> Equation Group not know what lost. We want Equation Group to bid so we keep secret. You bid against Equation Group, win and find out or bid pump price up, piss them off, everyone wins.

Rant about wealthy elites who don't get blowjobs who run for President

> We have final message for "Wealthy Elites". We know what is wealthy but what is Elites? Elites is making laws protect self and friends, lie and fuck other peoples. Elites is breaking laws, regular peoples go to jail, life ruin, family ruin, but not Elites. Elites is breaking laws, many peoples know Elites guilty, Elites call top friends at law enforcement and government agencies, offer bribes, make promise future handjobs, (but no blowjobs). Elites top friends announce, no law broken, no crime commit. Reporters (not call journalist) make living say write only nice things about Elites, convince dumb cattle, is just politics, everything is awesome, check out our ads and our prostitutes. Then Elites runs for president. Why run for president when already control country like dictatorship? What this have do with fun Cyber Weapons Auction? We want make sure Wealthy Elite recognizes the danger cyber weapons, this message, our auction, poses to their wealth and control. Let us spell out for Elites. Your wealth and control depends on

> electronic data. You see what “Equation Group” can do. You see what cryptolockers and stuxnet can do. You see free files we give for free. You see attacks on banks and SWIFT in news. Maybe there is Equation Group version of cryptolocker+stuxnet for banks and financial systems? If Equation Group lose control of cyber weapons, who else lose or find cyber weapons? If electronic data go bye bye where leave Wealthy Elites? Maybe with dumb cattle? “Do you feel in charge?” Wealthy Elites, you send bitcoins, you bid in auction, maybe big advantage for you?

August 27: Hal Martin arrested

August 28: Message 2 “Why is everyone so fucking stupid”

A play on Team America’s “I’m so ronery“

Additional details on auction, Pastebin

September 1: Message 6 files signed

September 5: Obama and Putin discuss DNC hacks at G-20

September 25: Sam Adams Award presentation; Craig Murray meets intermediary tied to Podeseta leak

October 1: Message 3 “Why you no like?”

More details on the auction. Medium

> Q: Why saying “don’t trust us”?
>
> A: TheShadowBrokers is making comment on trust-less exchanges.

> TheShadowBrokers is thinking is no thing now as trust-less. “Don’t Trust” is not equal to “Is Scam”. TheShadowBrokers is thinking no way to exchange secrets (auction files) without one party trusting other. If seller trust buyer and buyer no pay, then no more secrets. If buyer trust seller and seller no deliver, the no more sales. TheShadowBrokers is having more things to sell. Reputation is being another benefit of public auction.

October 7: IC Attribution of DNC hack to Russia, Podesta email release starts, Access Hollywood video

October 14: NBC story, CIA Prepping for Possible Cyber Strike Against Russia

> Vice President Joe Biden told “Meet the Press” moderator Chuck Todd on Friday that “we’re sending a message” to Putin and that “it will be at the time of our choosing, and under the circumstances that will have the greatest impact.”

October 15: Message 4 “Yo Swag Me Out”

> Calls off auction and provides spoof (I’m missing what this is a reference to) of Loretta Lynch/Bill Clinton plane conversation

October 17: Ecuador cuts off Assange’s Internet access

October 30: Message 5 Trick or Treat for Amerikanskis

> Medium announcement
>
> A reference to October 14 NBC story and Biden’s threat to Putin, mocking relative

focus on DNC hacks over Equation Group hacks

> Why is DirtyGrandpa threating CIA cyberwar with Russia? Why not threating with NSA or CyberCommand? CIA is cyber B-Team, yes? Where is cyber A-Team? Maybe threating is not being for external propaganda? Maybe is being for internal propaganda? Oldest control trick in book, yes? Waving flag, blaming problems on external sources, not taking responsibility for failures.

A challenge about whether the DNC hack is more important that the EG hack

> But neverminding, hacking DNC is way way most important than EquationGroup losing capabilities. Amerikanskis is not knowing USSA cyber capabilities is being screwed?
>
> [snip]
>
> Maybe political hacks is being more important?

A call for people to hack the elections

> TheShadowBrokers is having suggestion. On November 8th, instead of not voting, maybe be stopping the vote all together? Maybe being grinch who stopped election from coming? Maybe hacking election is being the best idea? #hackelection2016. If peoples is not being hackers, then #disruptelection2016, #disruptcorruption2016. Maybe peoples not be going to work, be finding local polling places and protesting, blocking , disrupting , smashing equipment, tearing up ballots? The wealthy

> elites is being weakest during elections and transition of power.

A threat that it will get worse

> How bad do you want it to get? When you are ready to make the bleeding stop, payus, so we can move onto the next game. The game where you try to catch us cashing out!

October 31: Obama contacts Putin on Red Phone for first time in presidency, reportedly warns he'll treat an attack on the election as an act of war.

November 26: Anonymous White House statement on election integrity

December 9: Obama calls for a review of hacking; WaPo releases releases story claiming CIA believes Russia did the hack to elect Trump

December 13: NYT story on DNC hack that leads with detail that FBI called DNC but staffer didn't believe he was FBI.

December 14 (?): Message 6 "Black Friday/Cyber Monday Sale" (file signed September 1; Mustafa al-Bassam seemed to know they were coming if not already out there)

December 14: Message 6B Bocefus Cleetus 1 "Are the Shadow Brokers selling NSA tools on ZeroNet?"

- Reference to Rage Against the Machine People of the Sun
- Possible reference to Hank Williams Jr, Dukes of Hazard (perhaps ventriloquist doll for FSB)
- Reference to fake news

December 15: Shadow Brokers interview with Motherboard

December 16, 5:21 AM(?): Message 6A Bocefus

Cleetus 2, ""New Theory: Shadow Brokers Incident is a Deep State Civil War between CIA vs NSA"

- Reference to NYT story on how DNC got hacked
- Reference to Bill Binney theory on hack
- Seeming rewriting of perceived FBI-CIA feud
- Reference to (now forgotten) Trump interview with Mike Rogers
- Reference to larger discussions of bureaucratic organization

> DOD and CIA have had a turf war going back to the Afghanistan and Iraq Wars bout whose job it was to run paramilitary operations. A turf war over the next "domain of battle" with all the government cheese.

December 16, 2:40PM: Obama press conference

January 1, 2017 [Update} Shadow Brokers complains it did not get included in Obama's sanctions list