THE DNC'S EVOLVING STORY ABOUT WHEN THEY KNEW THEY WERE TARGETED BY RUSSIA

This week's front page story about the Democrats getting hacked by Russia starts with a Keystone Kops anecdote explaining why the DNC didn't respond more aggressively when FBI first warned them about being targeted in September. The explanation, per the contractor presumably covering his rear-end months later, was that the FBI Special Agent didn't adequately identify himself.

> When Special Agent Adrian Hawkins of the Federal Bureau of Investigation called the Democratic National Committee in September 2015 to pass along some troubling news about its computer network, he was transferred, naturally, to the help desk.
>
> His message was brief, if alarming. At least one computer system belonging to the D.N.C. had been compromised by hackers federal investigators had named "the Dukes," a cyberespionage team linked to the Russian government.

> The F.B.I. knew it well: The bureau had spent the last few years trying to kick the Dukes out of the unclassified email systems of the White House, the State Department and even the Joint Chiefs of Staff, one of the government's best-protected networks.
>
> Yared Tamene, the tech-support contractor at the D.N.C. who fielded the call, was no expert in cyberattacks. His first moves were to check Google for "the Dukes" and conduct a cursory search of the D.N.C. computer system logs to look for hints of such a cyberintrusion. By his own account, he did not look too hard even after Special Agent Hawkins called back repeatedly over the next several weeks — in part because he wasn't certain the caller was a real F.B.I. agent and not an impostor.

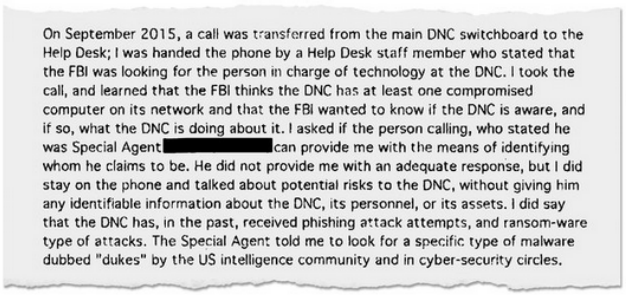
This has led to (partially justified) complaints from John Podesta about why the FBI didn't make the effort of driving over to the DNC to warn the higher-ups (who, the article admitted, had decided not to spend much money on cybersecurity).

This NYT version of the FBI Agent story comes from a memo that DNC's contractor, Yared Tamene, wrote at some point after the fact. The NYT describes the memo repeatedly, though it never describes the recipients of the memo nor reveals precisely when it was written (it is clear it had to have been written after April 2016).

> "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.
>
> [snip]
>
> "The F.B.I. thinks the D.N.C. has at least one compromised computer on its network and the F.B.I. wanted to know if

> the D.N.C. is aware, and if so, what the D.N.C. is doing about it," Mr. Tamene wrote in an internal memo about his contacts with the F.B.I. He added that "the Special Agent told me to look for a specific type of malware dubbed 'Dukes' by the U.S. intelligence community and in cybersecurity circles."
>
> [snip]
>
> In November, Special Agent Hawkins called with more ominous news. A D.N.C. computer was "calling home, where home meant Russia," Mr. Tamene's memo says, referring to software sending information to Moscow. "SA Hawkins added that the F.B.I. thinks that this calling home behavior could be the result of a state-sponsored attack."
>
> [DNC technology director Andrew] Brown knew that Mr. Tamene, who declined to comment, was fielding calls from the F.B.I. But he was tied up on a different problem: evidence suggesting that the campaign of Senator Bernie Sanders of Vermont, Mrs. Clinton's main Democratic opponent, had improperly gained access to her campaign data.
>
> [snip]
>
> One bit of progress had finally been made by the middle of April: The D.N.C., seven months after it had first been warned, finally installed a "robust set of monitoring tools," Mr. Tamene's internal memo says. [my emphasis]

The NYT includes a screen cap of part of that memo (which reveals that the DNC had already been exposed to ransomware attacks by September 2015), but not the other metadata or a link to the full memo.



On September 2015, a call was transferred from the main DNC switchboard to the Help Desk; I was handed the phone by a Help Desk staff member who stated that the FBI was looking for the person in charge of technology at the DNC. I took the call, and learned that the FBI thinks the DNC has at least one compromised computer on its network and that the FBI wanted to know if the DNC is aware, and if so, what the DNC is doing about it. I asked if the person calling, who stated he was Special Agent [redacted] can provide me with the means of identifying whom he claims to be. He did not provide me with an adequate response, but I did stay on the phone and talked about potential risks to the DNC, without giving him any identifiable information about the DNC, its personnel, or its assets. I did say that the DNC has, in the past, received phishing attack attempts, and ransom-ware type of attacks. The Special Agent told me to look for a specific type of malware dubbed "dukes" by the US intelligence community and in cyber-security circles.

An internal memo by Yared Tamene, a tech-support contractor at the D.N.C., expressed uncertainty about the identity of Special Agent Adrian Hawkins of the F.B.I., who called to inform him of the breach.

One reason I raise all this is because the evidence laid out in the story contradicts, in several ways, this August report, relying on three anonymous sources (at least some of whom are probably members of Congress, but then so was the DNC Chair at the time).

> The FBI did not tell the Democratic National Committee that U.S officials suspected it was the target of a Russian government-backed cyber attack when agents first contacted the party last fall, three people with knowledge of the discussions told Reuters.
>
> And in months of follow-up conversations about the DNC's network security, the FBI did not warn party officials that the attack was being investigated as Russian espionage, the sources said.
>
> The lack of full disclosure by the FBI prevented DNC staffers from taking steps that could have reduced the number of confidential emails and documents stolen, one of the sources said. Instead, Russian hackers whom security experts believe are affiliated with the Russian government continued to have access to Democratic Party computers for months during a crucial phase in the U.S. presidential campaign, the source said.
>
> [snip]
>
> In its initial contact with the DNC last

> fall, the FBI instructed DNC personnel to look for signs of unusual activity on the group's computer network, one person familiar with the matter said. DNC staff examined their logs and files without finding anything suspicious, that person said.
>
> When DNC staffers requested further information from the FBI to help them track the incursion, they said the agency declined to provide it. In the months that followed, FBI officials spoke with DNC staffers on several other occasions but did not mention the suspicion of Russian involvement in an attack, sources said.
>
> The DNC's information technology team did not realize the seriousness of the incursion until late March, the sources said. It was unclear what prompted the IT team's realization.

In August, anonymous sources told Reuters that FBI never told DNC they were being attacked by Russians until … well, Reuters doesn't actually tell us when the FBI told DNC the Russians were behind the attack, just that Democrats started taking it seriously in March.

But in the pre-Trump Russian hack bonanza, the NYT has now revealed that an internal memo says that the DNC had been informed in November, not March.

And even that part of the explanation doesn't make sense. As a number of people have noted, Brown is basically saying he didn't respond to a warning — given in November — that a DNC server was calling home to Russia because he was dealing with a NGP-VAN breach that happened on December 18. He would have had over two weeks to respond to Russia hacking the DNC before the NGP-VAN issue, and that would have been significantly handled by NGP.

Moreover, even the September narrative invites

some skepticism. Tamene admits the FBI Special Agent, “told me to look for a specific type of malware dubbed ‘Dukes’ by the U.S. intelligence community and in cybersecurity circles.” And he describes “His first moves were to check Google for “the Dukes” and conduct a cursory search of the D.N.C. computer system logs to look for hints of such a cyberintrusion.” Had Tamene Googled for “dukes malware” any time after September 17, 2015, this is what he would have found.

> Today we release a new whitepaper on an APT group commonly referred to as “the Dukes”. We believe that the Dukes are a well-resourced, highly dedicated, and organized cyber-espionage group that has been working for the Russian government since at least 2008 to collect intelligence in support of foreign and security policy decision-making. [my emphasis]

So had this initial report taken place after September 17, Tamene would have learned, thanks to the second sentence of a top Google return, that he was facing a “highly dedicated, and organized cyber-espionage group that has been working for the Russian government. ” Had he done the Google search he said he did, that is, he would almost certainly have learned he was facing down Russian hackers.

Had he clicked through to the report — which is where he would have gone to find the malware signatures to look for — he would have seen a big pink graphic tying the Dukes to Russia.

It’s certainly possible the alert came before the white paper was released (though if it came after, it explains why the FBI would have thought simply mentioning the Dukes would be sufficient). But that would suggest Tamene remembered the call and his Google search for the Dukes in detail sometime in April but not in September when this report got a fair amount of attention.

None of this is to excuse the FBI (I've already started a post on that part of this). But it's clear that Democrats have been — at a minimum — inconsistent in their story to the press about why they didn't respond to warnings sooner. And given the multiple problems with their explanation about what happened last fall, it's likely they did get some warning, but just didn't heed it.

Update: When I wrote this this morning, I had read this tweet stream and this story but not the underlying Shadow Brokers related post, by someone writing under the pseudonym Boceffus Cleetus it relates to, which is basically a Medium post introducing the latest sale of Shadow Broker tools. It wasn't until I read this post — and then the second Boceffus Cleetus post that I realized Boceffus Cleetus posted (his) original post — along with a reference to the name magnified back when this hack started — the day after the NYT wrote a story of the hack from DNC's perspective.

As the tweet stream lays out, Boceffus Cleetus is a play on ventriloquism, (duh, speaking for others) and the Dukes of Hazard. Both analyses of this argue that the reference to "Dukes of Hazard" is, in turn, a reference to the name given to the FSB hacking efforts (the other I've used is "Cozy Bear") in the report I linked above — that is, to the name F-Secure had given the FSB hackers, most notably in the report I linked above. I didn't make too much of it until I read this second Boceffus Cleetus post, which in seemingly one sentence lays out Bill Binney's theory of the DNC hack (that is, that NSA handed it on) with a country drawl and a lot of conspiracy theory added.

> 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. But y'all don't be runnin away yet, suspend yer disbelief and check out their claims. What if the Russian's

> ain't hacking nothin? What if the shadow brokers ain't Russian? Whatcha got as the next best theory? What if its a deep state civil war tween CIA and ole NSA? A deep state civil war to see who really runs things. NSA is Department of Defense, military. The majority of the military are high school grads, coming from rural "Red States", conservatives. The NSA has the global surveillance capabilities to intercept all the DNC and Podesta emails. CIA is college grads only and has the traditions of the urban yankee northeastern and east coast ivy leaguers, "Blue State", liberals.

It's all mostly gratuitous — an attempt to feed (as explicitly named "fake news") some of the alternate explanations out there right now.

But I find the portrayal of an NSA-CIA feud notable, in part, because the mostly likely reason *FBI* (which is where Boceffus Cleetus' fictional source came from) didn't tell the DNC who was hacking them back in September 2015 is because the actual tip — that Russia was hacking the DNC — came from the NSA. But FBI had to hide that. So instead, they used the name for FSB that was current at the time.

I'll add, too, that this plays on Craig Murray's claim that a national security person leaked him the Podesta documents.

So what's the point? Dunno. I defer to theGrugq's third post, in which he argues this post is signaling to show NSA the Russian hackers must have access to NSA's classified networks, because they've accessed a map of everything.

> This dump has a bit of everything. In fact, it has too much of everything. The first drop was a firewall ops kit. It had everything that was supposed to be used against firewalls. This dump, on the other hand, has too much diversity

> and each tool is comprehensive.
>
> The depth and breadth of the tooling they reveal can only possibly be explained by:
>
> 1. *an improbable sequence of hack backs which got, in sequence, massive depth of codenamed implants, exploits, manuals,*
> 2. *access to high side data*
>
> [snip]
>
> It is obvious that this data would never leave NSA classified networks except by some serious operator error (as I believe was the case with the first ShadowBrokers leak.) For this dump though, it is simply not plausible. There is no way that such diverse and comprehensive ops tooling was accidentally exposed. It beggars belief to think that any operator could be so careless that they'd expose this much tooling, on multiple diverse operations.
>
> There are, based on my count, twenty one (21) scripts/manuals for operations contained in this dump. They cover too many operations for a mistake, and they are too comprehensive for a mistake.

Remember, Obama has been stating assuredly that the US has far more defensive and offensive capability than Russia. The latter might well be true. But the latter is nuts, if for no other reason than we have so much more to secure. The former *might* be true. But not if hackers can log into NSA's fridge and steal their beer.

I'm not entirely sure what to make of this. But against the background of increasing dick-

wagging, it’ll be interesting to see how it plays out.