MY BOOB CLINIC IS PART OF AN INTERNATIONAL SPYING PLOT … BUT HILLARY'S ON IT!

By now you've likely read or at least heard about this Slate story, which uses a bunch of innuendo arising from some metadata to suggest that Trump has a secret exclusive communication method with Russia's biggest bank.

A number of people have debunked the technical claims in the article.

Former GCHQ employee Matt Tait did so in a series of tweets here. Consultant Naadir Jaawa laid out how it's a marketing server here. Consultant Robert Graham not only lays out the same spam email explanation that both Spectrum Health and Mandiant describe in the story, but notes that other malware researchers question the data in the story.

> Indeed, one journalist did call one of the public resolvers, and found other people queried this domain than the two listed in the Slate story — debunking it. I've heard from other DNS malware researchers (names remain anonymous) who confirm they've seen lookups for "*mail1.trump-email.com*" from all over the world, especially from tools like FireEye that process lots of spam email. One person claimed that lookups started failing for them back in late June — and thus the claim of successful responses until September are false.

Krypt3ia, in a post written in steps weeks ago, couldn't get answers from the "Tea Leaves" behind the story and judged that the incriminating files — which were just text files — could be recreated.

> These are the key files in the new dump but the problem I have is that they are just text files. Anyone with the know how could re-create these to look legit enough but yet still be questioned. I see no actual login to the shell and queries being run here so really coulda just done a find/replace on another query on any server you have access to.

In short, contrary to what Slate suggests, there are innocent explanations for this, and there's good reason to distrust the provenance of the data behind it.

Update: The Intercept has now explained why they passed on the story; they include spam sent to both Alfa and Spectrum from Trump, which corroborates the theory everyone else technical is settling on.

Boob Clinics usually stay out of international spy plots

Most of these debunkings have focused on the technical aspects. I want to start with this passage from Slate.

> A small portion of the logs showed communication with a server belonging to Michigan-based Spectrum Health. (The company said in a statement: "Spectrum Health does not have a relationship with Alfa Bank or any of the Trump organizations. We have concluded a rigorous investigation with both our internal IT security specialists and expert cyber security firms. Our experts have conducted a detailed analysis of the alleged internet traffic and did not find any evidence that it included any actual communications (no emails, chat, text, etc.) between Spectrum Health and Alfa Bank or any of the Trump organizations. While we did find a small

> number of incoming spam marketing emails, they originated from a digital marketing company, Cendyn, advertising Trump Hotels.")
>
> Spectrum accounted for a relatively trivial portion of the traffic. Eighty-seven percent of the DNS lookups involved the two Alfa Bank servers.

The story, remember, is that Trump has a super spooky *exclusive* hotline directly to a corrupt Russian bank. But most people covering this completely ignore that it's not completely exclusive: over 10% of the traffic reported by the anonymous researchers involves Spectrum Health.

Spectrum Health is the largest employer in Grand Rapids and West Michigan generally. It includes the Helen DeVos Children's Hospital and a Betty Ford Breast Care clinic. Spectrum Health is where I go to the doctor and Betty Ford is where I got my still cancer-free boobs squished this year. So for this story to make sense, you've got to explain why a children's hospital and a boob clinic are in cahoots with Trump and a big Russian bank.

The original version of the story tried to make much of the tie to Spectrum, finding in the children's hospital named after Richard DeVos's wife a tie to Erik Prince (Helen's daughter-in-law Betsy's brother) and the DeVos family's multinational pyramid scheme, the wealth from which has always — not just this year — been funneled into conservative causes.

> The other frequent connection to Trump's hidden server with the same distinctive human pattern is Spectrum Health, a Michigan hospital with close ties to the DeVos family (http://www.spectrumhealth.org/locations/helen-devos-childrens-hospital). The Devos family founded Amway / Alticor which operates in Russia including

> transactions with Alfa Bank such as buying insurance for 800 Alticor employees from Alfa Bank's insurance subsidiary. The Devos family has given millions of dollars in the past few months to conservative super PACs (www.fec.gov). One member of the Devos family was a founder of Blackwater.

None of that makes sense, though, especially since — while some of the DeVoses do seem to be funding Trump now and Prince has bizarrely backed the Donald (though that may stem from being shut out of State business while Hillary was in charge) — the biggest commonality between the DeVoses (who are hard core Republicans) and Trump is their multinational scheming and fondness for sports teams.

They may both be awful conservatives, but they are different kinds of awful conservatives, and there's little reason to believe they'd be in cahoots outside of belated efforts, post-dating these files, to fund Republican turnout in the state (and even there, Prince's sister Betsy is withholding direct funding).

More importantly, the DeVoses no more run this hospital than Betty Ford does.

But without the conspiracy theories implicating the DeVoses, then innocent explanations sure look a lot more plausible.

Tellingly, however, most other treatments of this story (this is an exception) have simply ignored this detail. Because once you have to calculate how a children's hospital and a boob clinic — even one, or perhaps especially one, named after Gerald Ford's wife — has a tie to this international spy plot, things start falling apart.

The reason why the boob clinic part of the story is important is it's a detail that should have led even non-technical people to at least think twice before running with the story. Slate, however, simply included Spectrum's explanation

for the files, the one that matched Mandiant's working hypothesis, and careened ahead.

The FBI has its own doubts

After Slate published, the NYT posted a story that generally reveals the FBI hasn't been able to substantiate any tie between Trump himself and Russia and has backed off its claims that Russia was trying to decide the election (a judgment I hope to return to).

It also reveals that the FBI largely agreed with what security experts concluded when they saw this claim.

> In classified sessions in August and September, intelligence officials also briefed congressional leaders on the possibility of financial ties between Russians and people connected to Mr. Trump. They focused particular attention on what cyberexperts said appeared to be a mysterious computer back channel between the Trump Organization and the Alfa Bank, which is one of Russia's biggest banks and whose owners have longstanding ties to Mr. Putin.
>
> F.B.I. officials spent weeks examining computer data showing an odd stream of activity to a Trump Organization server and Alfa Bank. Computer logs obtained by The New York Times show that two servers at Alfa Bank sent more than 2,700 "look-up" messages — a first step for one system's computers to talk to another — to a Trump-connected server beginning in the spring. But the F.B.I. ultimately concluded that there could be an innocuous explanation, like a marketing email or spam, for the computer contacts.

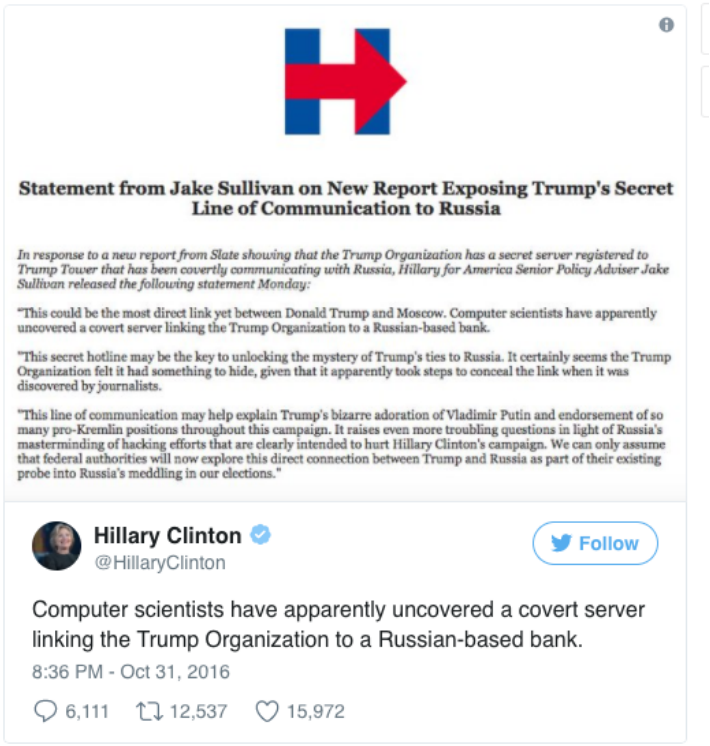
Note, this means that the FBI was already looking into this story when it got shopped to reporters in early October. So in addition to

the four or so other entities that reviewed this story and found it wanting (including me), the FBI had already had a crack at it.

Hillary Clinton and her likely National Security Advisor jump on this story

Now, as with the Kurt Eichenwald story claiming to have found a smoking gun tying Trump to Putin, people on the left didn't read the story very critically. Sure, this one is technically hard — up until you think about the boob clinic connection alleged in the middle of the spy plot. But for all its breathlessness, the Slate story simply insinuated. It proved nothing.

Which is why I'm so troubled that Hillary Clinton tweeted it four times in three hours, including a statement her likely National Security Advisor Jake Sullivan put together.



I mean, I get that it's election season and all. I get that Jim Comey gave Hillary a whopping October surprise on Friday. But one of the reasons we're supposed to elect Hillary over Trump is that she is more measured and fact-based than Donald is.

Here, she jumped on a story that at least should have given pause and created two campaign messaging pieces around it, asserting as fact that "Donald Trump has a secret server … set up to communicate privately with a Putin-tied Russian bank."

I'll repeat again: Jake Sullivan — the guy who wrote the longer statement on this — is widely assumed to be set to take on the job from which Condi Rice started a war by warning about fictional mushroom clouds.

Who are these secret researchers, anyway

Which leads me to a final question a few of the security folks are asking about this story.

In addition to his technical debunking, Robert Graham made an equally important point: researchers shouldn't be accessing this data for ad-lib investigations into presidential candidates, and it's not even clear who would have access to it all except the NSA.

> The big story isn't the conspiracy theory about Trump, but that these malware researchers exploited their privileged access for some purpose other than malware research.
>
> [snip]
>
> In short, of all the sources of "DNS malware information" I've heard about, none of it would deliver the information these researchers claim to have (well, except the NSA with their transatlantic undersea taps, of course).

And in a second post this morning, Krypt3ia started wondering who's behind this story.

> This was a non story and this was someone's troll or an IC operation of some kind. I left it at that… That is until last night when this fallacy laden report came out of Slate.
>
> Anonymous Security Professionals
>
> So here is what I believe happened with Slate and Foer. Tea, not happy with my ignoring their bullshit, went on to pimp

> at least five venues looking for a way to get this wide and Foer was the gullible one to do so. Now, with a live one on the line Tea spun their tale and added the new twist that they are in fact a group of “security professionals” with insider knowledge and that this story is really real. Of course once again they provided no real proof of Trumps servers being configured for this purpose, no evidence of actual emails, and no real forensically sound information that proves any of what they say can be proven in a court of law. This is a key thing and Slate may not care but others do. Even in the previous dumps on the i2p site that tea set up their diagram said “this is what it would look like” would is not proof, that there is speculation and not evidence.
>
> [snip]
>
> Meanwhile, the story spun by Tea and now Camp et al on Slate makes me wonder just who Tea is. Obviously Camp knows Tea and the others and this is a small world so let’s work out the connections shall we?
>
> Camp –>Vixie –> ??? let’s just assume that Camp knows these persons well and if one starts to dig you could come up with a few names of people who “would” (there’s that would again) have the kind of access to DNS data that is needed.
>
> Just sayin.

Of course, we have since learned that before Tea Leaves started pushing this story to the press, the FBI had been investigating it for two months.

Which, to my mind, raises even more questions about the anonymous researchers’ identities, because (small world and all) the FBI likely knows them, in which case they may have known

that the FBI wasn’t jumping on the story by the time they started pitching it.

Or the FBI doesn’t know them, which raises still more questions about the provenance of these files.

Ah well, if President Hillary starts a war with Russia based off Iraq-War style dodgy documents, at least I’ll have the satisfaction of knowing my boob clinic is right there on the front lines.

Update: I’ve added language to clarify that the DeVoses don’t run Spectrum.