AFTER THREE SUGGESTIONS OF DOCTORED DATA, ALFA BANK CLAIMS THEY'RE BEING FRAMED

Remember this article from CNN that renewed the Alfa Bank funny server story? It totally pissed me off for the way it cited about seven people telling it there was no there there, and then reporting that there was based off one identified source (a US official, who could be a member of Congress) and other non-identified ones.

In addition, it claimed that Dick DeVos leads Spectrum Health — my local hospital. DeVos is currently Chairman of the Board, but the company is "led" by CEO and President Rick Breon. DeVos "leads" a company called Windquest Group, which invests in boutique things like an excellent wine bar and the fancy gym I belonged to before I joined the Y. The DeVos family "owns" a lot more, notably RDV Corporation, through which they own and mismanage the Orlando Magic. There are probably a jillion servers associated with RDV corporation that could (and probably do!) conduct secret communications. Which is another way of saying that if Dick DeVos wanted to conduct secret conversations with Donald Trump at a time when he was attracting attention because he was not yet even donating money to the candidate, he might have done it via a server more directly operated by his family. Hell, since DeVos spooked up brother-in-law Erik Prince *was* supporting Trump at that time of the weird server activity, why wouldn't we expect spooky conversations to happen from one of Prince's far-flung spook properties?

But perhaps the funniest part of the CNN story is that it pointed to evidence the story had been packaged — but it didn't seem to understand

that.

> Other computer experts said there could be additional lookups that weren't captured by the original leak. That could mean that Alfa's presence isn't as dominant as it seems. But Dyn, which has a major presence on the internet's domain name system, spotted only two such lookups — from the Netherlands on August 15.

If there were lookups not recorded in the publicly released data — even if there were just two of them — then it shows that the publicly released data is incomplete.

Other outlets say was even more data sometimes excluded from the public story. The Intercept cataloged how different sets of material purportedly backing this story include different sets of IP addresses.

> On Tea Leaves' WordPress site, he claimed that "only two networks resolved the mail1.trump-email.com host." This is contradicted by the very works of analysis furnished by Tea Leaves' collaborators: The author of the white paper found that at least *19* IP addresses, all belonging to different networks except for the two that belong to Alfa Bank, had looked up Trump's server. And these are only the 19 the author was able to observe in a short time period — it can't be ruled out that there were many more, which quickly deflates the portrait of a shady Russian backchannel.
>
> The white paper included DNS look-up data, but not nearly enough to reproduce the results. Rather than the 19 IP addresses we expected to see, the data only included three, and the DNS look-ups were not for the same time period that the paper described. Tea Leaves

> published a different set of data on the dark web, which we also looked at, but this set of data only included a total of four IP addresses. When we pressed Tea Leaves for the complete set of data so we could attempt to reproduce the analysis, he gave us a new, more comprehensive set of data, but still that included a total of only eight IP addresses, and it was missing an IP address belonging to a VPN service in Utah that accounted for a significant portion of the DNS look-ups described in the paper.

And Robert Graham states that a source of his says the data for June – one of the key months in question – was altered.

> Tea Leaves and Jean Camp are showing logs of private communications. Where did these logs come from? This information isn't public. It means somebody has done something like hack into Alfa Bank. Or it means researchers who monitor DNS (for maintaing DNS, and for doing malware research) have broken their NDAs and possibly the law.
>
> The data is incomplete and inconsistent. Those who work for other companies, like Dyn, claim it doesn't match their own data. We have good reason to doubt these logs. There's a good chance that the source doesn't have as comprehensive a view as "Tea Leaves" claim. There's also a good chance the data has been manipulated.
>
> Specifically, I have as source who claims records for trump-email.com were changed in June, meaning either my source or Tea Leaves is lying.
>
> Until we know more about the source of the data, it's impossible to believe the conclusions that only Alfa Bank was

> doing DNS lookups.

Here's his latest post on this issue.

All the different sets of data (and the way the data was culled without evidence about how that was done), plus the fact that the entity behind this story goes by the name "Tea Leaves" and now refuses to talk to anyone about it, really ought to raise questions about a hoax. But not CNN. For CNN it was all proof of something there.

Now CNN reports that once in February and increasingly since CNN's story about a non-story, someone has been spoofing lookups from Trump to Alfa.

> [O]n Friday, Alfa Bank claimed hackers are now trying to perpetuate that suspicion by tricking the Trump Organization into sending communication toward the bank.
>
> [snip]
>
> One attack happened on February 18, the bank said. (The bank did not mention that to CNN before its story published on March 10.)
>
> After CNN published its story about the puzzling Trump-Alfa situation, hackers stepped up their attack on the Trump Organization with "spoofed" signals for five hours, which were then directed back towards the bank, Alfa Bank said.
>
> Hackers continued this attack on March 13, the bank said.
>
> The bank contacted the FBI and offered "complete co-operation in finding the people behind attempted cyberattacks." A US law enforcement official confirmed that the FBI was contacted.
>
> [snip]
>
> According to Alfa Bank's description of recent events, hackers have recently

> tricked a Trump Organization computer server into sending internet traffic to Alfa Bank.
>
> Hackers have "manufactured this deceit by 'spoofing' or falsifying DNS lookups to create the impression of communication between Alfa Bank and the Trump Organization," the bank said in a statement.
>
> Alfa Bank offered this analogy: "A simple analogy would be someone in the U.S. sending an empty envelope… to a Trump office… addressed to Trump, but on the back of the envelope the return address is Russia… instead of its own real address."
>
> "So, on cursory examination, Alfa Bank appears to have been receiving responses to queries it never actually sent."
>
> Alex McGeorge, head of threat intelligence at cybersecurity firm Immunity, said this is a prank "that is simple to do from pretty much any internet connected computer. We could probably manufacture this from a Starbucks."

That someone is trying to manufacture something out of nothing here should not be surprising. There's abundant reason to believe that's what was always happening. And now that the FBI has been called back in by Alfa, I do hope they find an explanation about whether this is a Hillary person trying to taint Trump or Russia trying to do a limited hangout on other more damaging Alfa stuff. Maybe both have been faking this story at different times?

In any case, at this point, the story should be about why this story got packaged in the way it did, as much as any questions about how Trump sends spam around the world.

Update: Here's the press release from Alfa.

They’re also calling the larger story a hoax.

> Alfa Bank’s working hypothesis is that an individual – possibly well known in internet research circles – may have fed selected DNS data to an anonymous cyber group to ensure they reached a specific (and erroneous) conclusion. Alternatively, the cyber group may have been complicit in the deceit. In the most recent cases, unknown individuals demonstrably attempted to insert falsified records onto Alfa Bank’s computer systems designed to create the same impression.
>
> An Alfa Bank spokesperson said: «The anonymous cyber group, which is led according to news accounts by ‘Tea Leaves,’ cannot produce evidence of a link because there never has been one. Alfa Bank believes that it is under attack and has pledged its complete cooperation to U.S. authorities to find out who is behind these malicious attacks and false stories.»