From: GAYNOR, RYAN C. (CD) (FBI) <RCGAYNOR@fbi.sgov.gov>
Sent: Thursday, October 13, 2016 5:45 PM
To: WIERZBICKI, DANIEL S. (CG) (FBI) <DSWIERZBICKI@fbi.sgov.gov>; HEIDE, CURTIS A. (CG) (FBI) <CAHEIDE@fbi.sgov.gov>; SANDS, ALLISON (CG) (FBI) <ASANDS@fbi.sgov.gov>
Cc: PIENTKA, JOE (WF) (FBI) <JPIENTKA@fbi.sgov.gov>; MOFFA, JONATHAN C. (CD) (FBI) <JCMOFFA@fbi.sgov.gov>
Subject: FW: Online information --- [redacted]
Attach: [Untitled].pdf

Classification: [redacted]
Classified By: [redacted]
Derived From: FBI NSIC dated 20120629
Declassify On: 50X1-HUM
==========
TRANSITORY RECORD

CG,

I am interested on your thoughts on the attached paper. This was found online at the address noted at the top of the paper (mediafire.com). Looks like the argument in this paper is largely supported by activity likely caused by our investigation and other acts by [redacted] but I would like your technical opinion on this paper. Is this related to the [redacted] and do we have information which can you help explain the 'new' trump email domain now pointed at the original server?

As Always, Thank you for the great work on this,
-Ryan

==========[redacted]==========
Classification: [redacted]

GOVERNMENT EXHIBIT
0270
21-CR-582 CRC

Below is from:

http://www.mediafire.com/file/qc68pt5k6wn9f64/gdd.zip

Global DNS Data

This site provides neutral, factual DNS data, showing how networks communicate with each other.

1. Lookups for mail1.trump-email.com
   This data shows communications between Trump, Spectrum, and Russian Alfa Bank networks.
2. Network Diagram Scenario
   This diagram (png file: 183769 bytes) shows how parties communicated via email using different servers.
3. Check back for more
4. Leave questions at: `tea.leaves@tuta.io`

Summary:

- Trump and Russia's largest private bank communicate via hidden server since at least 2016 May
- Confronted with questions by NYT reporter, Alfa Bank denies any relationship
- Hidden server belonging to Trump then disappears (no one but Alfa Bank was asked)
- Deleted host name mail1.Trump-Email.com is replaced with trump1.contact-client.com
- Russian Alfa Bank is the first host seen to contact the new trump1. server

Comments:

Trump's FEC filings fail to disclose any foreign bank account in Russia or relationship with the Russian Alfa Bank.

Network logs show a distinctively human pattern of communications between a hidden server dedicated for use by the Trump Organization and the Russian financial company Alfa Bank, which has close ties to the Kremlin. Trumpcampaign advisors also have relationships with Alfa Bank and related Alfa-Group / LetterOne.

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.

Trump's hidden server appears to be a specially configured outbound email server. The email server type normally would handle outbound bulk advertising or transactional mail for a large enterprise to customers, powerful enough to deliver millions of emails per day. (http://www.marketerspublishinggroup.com/PMTA-UsersGuide-4.0.pdf). Different in every way from traffic seen on adjacent servers managed by the same server company, this specially configured server has been exclusively corresponding with Alfa-Bank and Spectrum since at least May 2016 with a cadence and rate of a human conversation. See the graph of the connections here.

The stealth server has had two different names:

mail1.Trump-Email.com (zone deleted on Friday, 2016-Sept-23 after the Russian Alfa-Bank was asked by the New York Times to explain the communications)

and on 2016-Sept-27 a new name showed up:

trump1.contact-client.com

When a reporter from the New York Times (NYT) asked the Russian Alfa Bank for comment about the apparent communications, Alfa Bank denied any relationship with the Trump Organization. The NYT reporter communicated with no one other than the Russian Alfa Bank - yet the Trump-Email.com domain began showing signs of panicked reconfiguration within hours of the New York Times asking the Russian Alfa Bank why they were making connections to Trump-Email.com. While no errors were seen in all the months prior to this question from the reporter - suddenly errors appeared. Two of the authoritative name server hosts deleted the zone, while the third authoritative just erased the IP from the configuration line and continued to answer authoritatively. This mistake can still be demonstrated at the time of this writing.

The Trump Organization deleted the Trump-Email.com zone shortly before 10 AM Eastern US time on Friday Sept 23rd after the NYT reporter called

Alfa Bank. This suggests a cover-up attempt by Trump and Alfa Bank. It suggests communication from Alfa Bank warning the Trump Organization to take action to remove the evidence of the hidden server domain, mail1.Trump-Email.com.

The physical server itself was never changed; just the hostname mail1.Trump-Email.com stopped pointing to that physical server and the hostname was effectively deleted from the global Domain Name System (DNS).

By September 27th 2016, the Trump Organization had created a new host trump1.contact-client.com pointing to the exact same physical server previously operating as mail1.Trump-Email.com.

The Russian Alfa Bank was the first to contact the newly renamed host, strongly indicating again that Trump and Alfa Bank are coordinating with each other and have a very close relationship. After this discovery, they are likely moving conversations to a new channel.

Trump has a bank account with the Russian Alfa Bank, which may explain the need for hidden server communications. Alfa Bank / Alfa Group / LetterOne has expressed interest in investing billions in US health care companies, which could include Michigan's Spectrum Health or could be regarding the financial relationships Amway/Alticor has with the Russian Alfa Bank insurance company.

F.A.Q.

Are you sure the Trump-Email.com domain really belongs to the Trump Organization?

We have 100% confidence. You can verify the complete whois record by going to the Godaddy.com website and clicking on WHOIS. While whois records can be forged, we also judge authenticity based on the resources used by each domain name. A very detailed analysis has been made of thousands of Trump Organization domain names, vendors and hosting resources, confirming that this domain without question belongs in the same group.

Excerpt from Trump-Email.com whois record:

```
Registrant Name: Trump Orgainzation
Registrant Organization: Trump Orgainzation
Registrant Street: 725 Fifth Avenue
Registrant City: New York
Registrant State/Province: New York Registrant
State/Province: New York
```

Registrant Postal Code: 10022
Registrant Country: US Registrant Country: US
Registrant Phone: +1.2128322000