OSINT on Trump Network Communications

1 Introduction

This document summarizes public information about the Trump Organization network, with a focus on communications with Russia and Spectrum Health. Sources include websites, press statements, and public network information.

2 Background

In the fall of 2016, reporters investigated connections between the Trump Organization and a Russian bank. Network data showed communications between Trump, Spectrum Health in Michigan, and Alfa Bank in Russia. One article summarized the data in detail:

```
http://www.slate.com/articles/news_and_politics/cover_story/2016/10/\
  was_a_server_registered_to_the_trump_organization_\
  communicating_with_russia.html
```

Key findings, not disputed by any party, include:

- Network data clearly showed numerous interactions between computers owned by Trump, and networks in Spectrum Health and Alfa Bank.
- When a reporter asked Alfa Bank (and only Alfa Bank) about the network communications, Trump immediately took down his server.
- Days later, Trump created a second network host. The first organization to contact this new host was Alfa Bank, and communications traffic among the parties possibly resumed.

Eventually, the Trump Organization released a press statement, stating that the servers were in fact used for banking transactions with Alfa Bank. Trump's explanation was that computers were instead used by a non-employee. For their part, Spectrum and Alfa Bank still deny any banking-related communications took place.

In the last days before the 2016 election, the press coverage focused on the esoteric nature of the network data, and Trump's admission received no coverage. Indeed, only the Spectrum and Alfa Bank denials were quoted in the press.

This document describes Trump's admitted relations between computers in the Trump Organization and a Russian bank, and important questions researchers should ask about the admitted connection to a Russian entity.

3 Reports and Press Statements

In a statement released to a small number of reporters, the Trump Organization conceded their network was in communications with a Russian bank, between May and October of 2016. The press statement still appears in the Twitter feed of an NBCNews reporter:

```
https://twitter.com/alivitali/status/793253775087702016

https://pbs.twimg.com/media/CwI0GPKXgAEO1XT.jpg
```

In material part, the statement explains the network communications between the Trump Organization and a Russian network:

```
A thorough network analysis conducted by Cendyn at the request of The
Trump Organization determined an existing banking customer of Cendyn,
completely unrelated to Trump, recently used Cendyn's "Metron"
Meeting Management Application to send communication to Alfa Bank.com.
```

The full statement appears as Figure 1 in Appendix A. The press release is also quoted in full in this source:

```
http://www.complex.com/life/2016/11/\
   donald-trump-server-communicating-with-russia
```

The Cendyn report referenced by the press release is not public. But Cendyn addresses subpoena and privacy issues here:

```
http://www.cendyn.com/privacy-policy/

980 N. Federal Highway, 2nd Floor, Boca Raton, FL 33432
Phone 561-750-3173
ONE@cendyn.com
```

Spectrum Health responded to reporters questions by conducting an investigation. They claim to have found no evidence of communications with the Trump Organization. What evidence they did find they claimed was the result of marketing (spam messages), and that additional DNS traffic "were caused by a software application error". Spectrum's statement to reporters is preserved as Figure 3, in Appendix C.

3.1 Analysis

The three parties have all released contradictory press statements. In general, Alfa Bank and Spectrum deny any banking communications took place, while Trump admits there were banking transactions (albeit from a non-employee who could access Trump's computers).

Researchers may wish to consider the following questions:

- The Trump press statement was released by:

```
HOPE HICKS
COMMUNICATIONS
Donald J. Trump for President, Inc.
W 646.736.2608
C  203.273.0226
```

The press office for *Donald J. Trump for President, Inc.* may have drafts of the press statement, internal reviews of the Cendyn report, communications about the statement, and related comments. In particular, the Trump Organization *must* have communications with Alfa Bank, from whom it first learned about the public interest in his network connections to Russia.

- Researchers should inquire about this "non-employee" blamed by Trump for the network traffic. Taking the Trump press statement at its word, it is not clear how such a person would (a) have access to Trump's computers at Cendyn; (b) would presumably make use of Trump's Cendyn computers via the Trump Tower network or other authorized networks; (c) why such a person would conduct banking transactions with Alfa Bank (which has no branches in the United States); and (d) how such access, by a non-employee, would persist for months. While no information is available on this topic, it may well be that the non-employee is nonetheless an agent of the Trump Organization, in certain contexts.

- When circulated, the Trump press statement included a footer that linked to a logo created by Michael Coleman, LLC, a design consultant for Kushner Companies and various Trump properties. The link merely displayed a Trump logo, and appeared as:

```
http://michaelcoleman.net/files/\
    djtpac/emailfooter1.png[donaldjtrump.com]
```

  Individuals (*foreign and domestic*) who received the Trump statement on or before the morning of October 17 EDT may have resolved this URL while reading the press statement. For example, if a draft of the press release were provided to a foreign organization, their examination of the document would create log events with the michaelcoleman.net web serer. Logs for the `michaelcoleman.net` server are maintained by GoDaddy, who hosts the design firm's website. GoDaddy's policy and recommendations for subpoena service appear here:

```
https://www.godaddy.com/agreements/\
    showdoc.aspx?pageid=CIVIL_SUBPOENA
```

- Mandiant security was retained by Alfa Bank to study network logs showing communications between Trump and Alfa Bank. A press release summarized their findings:

```
http://alfabank.com/media/news/2016/11/01/
```

This statement is preserved in Appendix B, Figure 2. In part, Mandiant asserts that "[n]either Alfa Bank nor its principals, including Mikhail Fridman and Petr Aven, have or have had any contact with Mr. Trump or his organizations."

The Mandiant statement conflicts with the Trump/Cendyn statement, which admits that Trumps computers were in fact being used for banking transactions with Alfa Bank (albeit from a non-employee who had access to Trump's computers from May to November 2016.) It is not clear how Cendyn (the source of banking transactions between Trump's computers and Alfa Bank) can conclude there were banking events, while Alfa Bank and Mandiant (looking at the same network traffic), reached the opposite conclusion.

Mandiant's study is characterized as a "deep dive" into the Alfa Bank network, yet reached the opposite conclusion as Cendyn.

Mandiant may have drafts of their study, and perhaps emails or communications with Alfa Bank, Trump, Cendyn and others. Mandiant issued press comments to reporters as early as late September, 2016, through the office of Stuart McKenzie, Mandiant Vice President for EMEA (London).

Mandiant is a subsidiary of FireEye, and can be reached at this address:

```
FireEye  Federal DC
12011 Sunset Hills Road, Ste. 400
Reston, VA 20190
T: +1 703-935-1700
F: +1 703-464-0010
```

- Spectrum Health claims to have conducted an investigation, which is not public. There may be drafts of their internal report, or discussions about its content.

- After the Trump server was taken down (in response to reporters questions directed to Alfa Bank), Spectrum's networks continued to contact the expired Trump host. Spectrum characterizes any incidental communications with Trump as mere marketing information (spam). In their press statement, Spectrum excuses the repeated attempts to contact an expired server as a "software application error".

  There's no plausible case that the numerous DNS lookups from Spectrum's network were caused by marketing email alone. From the facts Spectrum offered, Trump had sent only a few marketing emails, and in any event, had taken down his server. Spectrum's internal report might indicate what "software application" caused their networks to repeatedly attempt to communicate with Trump's machines.

  Spectrum's privacy policies, subpoena advice, and contact information appears at:

  `http://www.spectrumhealth.org/policies/patient-privacy`

http://www.spectrumhealth.org/about-us/contact-us

4 Related Network Resources

Network communications on the Internet often leave a trail, in the form of netflow logs. These logs reside with the various routers and networks that transit packets. Third parties, such as telecommunications companies and ISPs, may have such logs for the various prefixes (or network blocks) used by Trump, Alfa Bank and Spectrum.

4.1 Trump Network Resources

DNS SPF records for trump-email.com include the following prefixes:

```
198.91.42.0/23
64.135.26.0/24
64.95.241.0/24
206.191.130.0/24
63.251.151.0/24
69.25.15.0/24
```

Cendyn (aka CDC Services) provided authoritative name server resolution services for the forward resolution of mail1.trump-email.com and trump1.contact-client.com. While the Cendyn authority IPs have recently changed, during all relevant times, the authority IPs were:

```
198.91.42.1
64.135.26.101
64.135.26.103
```

During all relevant times, the network for Trump Organization used the following prefix:

```
192.154.117.32/27
```

The host mail1.trump-email.com and later trump1.contact-client.com resolved to 66.216.133.29, which appears in Listrak's netblock:

```
66.216.133.0/24
```

4.2 Alfa Bank Network Resources

Alfa Bank owns several network blocks, including ranges used by their corporate network:

```
217.12.96.0/23
```

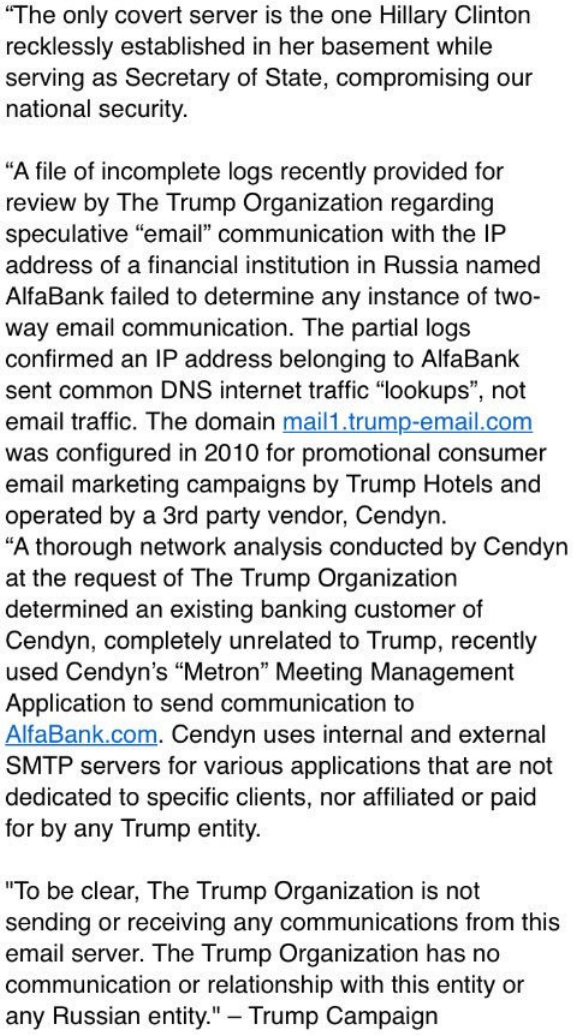
4.3 Spectrum Health Network Resources

Spectrum Health owns several networks, including:

```
198.51.9.0/24
167.73.0.0/16
```

Network flows to/from the Trump and Cendyn prefixes from/to the Alfa Bank and/or Spectrum networks may have transited other carriers, from the period of May 2016 to November 2016. Large telcos such as Verizon, AT&T, and CenturyLink maintain sampled flow records for operational reasons, and traffic between these above prefixes may be recorded. Peering relations can also be discovered through public databases, such as `http://bgp.he.net`.

Appendix A



"The only covert server is the one Hillary Clinton recklessly established in her basement while serving as Secretary of State, compromising our national security.

"A file of incomplete logs recently provided for review by The Trump Organization regarding speculative "email" communication with the IP address of a financial institution in Russia named AlfaBank failed to determine any instance of two-way email communication. The partial logs confirmed an IP address belonging to AlfaBank sent common DNS internet traffic "lookups", not email traffic. The domain mail1.trump-email.com was configured in 2010 for promotional consumer email marketing campaigns by Trump Hotels and operated by a 3rd party vendor, Cendyn.
"A thorough network analysis conducted by Cendyn at the request of The Trump Organization determined an existing banking customer of Cendyn, completely unrelated to Trump, recently used Cendyn's "Metron" Meeting Management Application to send communication to AlfaBank.com. Cendyn uses internal and external SMTP servers for various applications that are not dedicated to specific clients, nor affiliated or paid for by any Trump entity.

"To be clear, The Trump Organization is not sending or receiving any communications from this email server. The Trump Organization has no communication or relationship with this entity or any Russian entity." – Trump Campaign

Figure 1: Statement of Donald J. Trump for President, Inc. regarding Trump Organization computers communicating with Russian banks. From `https://twitter.com/alivitali/status/793253775087702016`

Appendix B: Statement of Alfa Bank

01 November 2016 – Alfa Bank says no connection between Alfa Bank and Trump and any suggestion to the contrary is false —

Earlier today in the US, Slate published an article titled -Was a Trump Server Communicating With Russia? Alfa Bank wishes to make clear that there is no connection between Alfa Bank and Donald Trump, the Trump campaign, or the Trump organization. Any suggestion to the contrary by this article is false.

Alfa Bank hired Mandiant, one of the world's foremost US cyber security experts, to investigate and it has found nothing to support the allegations. Mandiant found no substantive contact, email or financial link between Alfa Bank and the Trump Campaign or Organization during its investigation. Mandiant have conducted a deep dive and investigated Alfa Bank's IT systems both remotely and on the ground in Moscow and there was no evidence of notable contact between the alerted domain and Alfa Bank.

Neither Alfa Bank nor its principals, including Mikhail Fridman and Petr Aven, have or have had any contact with Mr. Trump or his organizations. Fridman and Aven have never met Mr. Trump nor have they or Alfa Bank had any business dealings with him. Neither Alfa Bank nor its officers have sent Mr. Trump or his organisation any emails, information or money. Alfa Bank does not have and has never had any special or exclusive internet connection with Mr. Trump or his entities. The assertion of a special or private link is patently false.

Mandiant has made clear to Alfa Bank that the information reporters gave us – given to them by an anonymous cyber group - is inconclusive and does not suggest an exclusive internet connection between Alfa Bank and Trump.

Mandiant's working hypothesis is that the activity the reporters' sources allege was caused by email marketing/spam campaign by a marketing server, which triggered security software. This activity may indeed have been initiated by someone for the purpose of discrediting parties to this traffic.

Commenting on these allegations Mandiant said

Mandiant, a FireEye company, has been retained by Alfa Bank to investigate information given to them by various media. The information that has been presented is a list of dates, times, IP Addresses and Domain Names. The list appears to be a scanned copy of a printed log. There is no information which indicates where the list has come from. The list contains approx. 2800 look ups of a Domain Name over a period of 90 days. The information presented is inconclusive and is not evidence of substantive contact or a direct email or financial link between Alfa Bank and the Trump Campaign or Organization. The list presented does not contain enough information to show that there has been any actual activity opposed to simple DNS look ups, which can come from a variety of sources including anti-spam and other security software.

As part of the ongoing investigation, Alfa Bank has opened its IT systems to Mandiant, which has investigated both remotely and on the ground in Moscow. We are continuing our investigation. Nothing we have or have found alters our view as described above that there isn't evidence of substantive contact or a direct email or financial link between Alfa Bank and the Trump Campaign or Organization.

Founded in 1990, Alfa-Bank is one of the largest private banks in Russia, which offers a wide range of products and operates in all sectors of the financial market, including interbank, corporate and retail lending, deposits, payment and account services, foreign exchange operations, cash handling services, investment banking, and trade finance, as well as other ancillary services to corporate and retail customers.

According to its IFRS Consolidated Financial Statements as of 31 December 2015, the Alfa Banking Group, which comprises Joint Stock Company Alfa-Bank as well as its subsidiary financial companies, had total assets of $31.5 bn, gross loans of $21.7 bn, and total equity of $4.3 bn. Net profit after tax for 2015 amounted to $480 mln.

As of December 31, 2015 the Alfa Banking Group serves around 255,000 corporate customers and 13.6 mln individuals (including 1.9 mln individual customers of PJSC <<Baltiyskiy Bank>>), while the branch network consists of 745 offices across Russia and abroad, including a subsidiary bank in the Netherlands and financial subsidiaries in the United Kingdom and Cyprus.

Figure 2: Statement of Alfa Bank, quoting Mandiant study, from `http://alfabank.com/media/news/2016/11/01/`

Appendix C: Statement of Spectrum Health

10-6-16 8:38 a.m.

We have conducted a thorough investigation with independent cyber security firms and found no evidence of emails, file transfers or any other communications involving either Alfa Bank or any of the Trump organizations. Any report suggesting that our systems were used for communications between these organizations is not supported by the facts of our investigation. Furthermore, Spectrum Health has no relationship with Alfa Bank or any of the Trump organizations.

Our investigation did find internet traffic between Spectrum Health and an independent marketing firm that owns and administers servers for companies in the hospitality industry. Our experts confirmed that this traffic was made up entirely of automated attempts to convert the domain name to an IP address. None of this traffic was email or other communications. Additional analysis determined these failed DNS inquiries were caused by a software application error. Importantly, there is no indication that any data on our systems has been breached or compromised.

At Spectrum Health, data privacy and security is a top priority, and we take very seriously our duty to protect the personal information of our patients, members and employees.

You asked whether we have contacted the Federal Bureau of Investigation regarding this situation. Since we do not have any credible evidence that warrants involving law enforcement, we have not contacted any authorities.

Figure 3: Statement of Spectrum Health