Summary of Trump Network Communications

1 Introduction

The data provided with this report consists of DNS queries, answers and response codes for a server in use by the Trump Organization for many years, [1] despite a variety of claims made by the Trump Organization in response to news organization questions.

The two most frequent talkers to this server are resolvers at Russia's Moscow location of Alfa Bank and Michigan's Spectrum Health. Multiple members of Michigan's Devos family are involved in Spectrum Health facilities, business ventures in Russia and together making millions in donations to the Trump campaign/PACs. Betsy Prince Devos has been confirmed for a cabinet position in the Trump administration.

Other parties have provided a data visualization based on the same data up through the time of hostname deletion, available here along with other visual and analysis resources:

`http://ljean.com/NetworkRecords/all.html`

`http://ljean.com/NetworkRecords/`

2 mail1.Trump-Email.com Hostname Deleted

New York Times reporter Eric Lichtblau contacted *only Alfa Bank* for comment on Alfa Bank's queries to the Trump Org host. Within hours the Trump Organization reacted by having the Trump Organization owned domain name (trump-email.com) removed from the Domain Name System via zone file deletion at the Cendyn - a Trump Organization vendor [2] - authoritative name servers.

[1] The IP address `66.216.133.29` has had a stable unchanging reverse DNS of `mail1.trump-email.com` at least since 2013-09-20, publicly verifiable within data provided from global reverse DNS scans at `https://scans.io/study/sonar.rdns`. Additional effort could likely establish the stable unchanging time period of existence back to 2009 when the domain was registered.

[2] Cendyn can be publicly verified as a Trump vendor starting in 2007 `http://www.prweb.com/releases/2007/06/prweb535089.htm` with many observable significant dependencies continuing to the present time. Cendyn utilizes some of Listrak's servers in Pennsylvania and Listrak is the entity to which the IP address `66.216.133.29` is allocated in IP address whois data. The authoritative name service for `Trump-Email.com` is provided by 3 diverse Cendyn servers; the authoritative name server for the reverse DNS record for `mail1.trump-email.com` is provided by Amazon Web Services.

3 Unexplained Connection Retries

Within minutes of the `trump-email.com` zone deletion - both Michigan's Spectrum Health IP and Moscow's Alfa Bank intranet showed up making repeated efforts to reconnect to the Trump server. Why would these two entities have such an "always on" connection to the Trump server, causing them to immediately retry and search for it when it disappeared?

The Spectrum Health IP then made thousands of retry attempts for days until something at Spectrum Health was finally shut off. Spectrum Health's explanation to a news organization was that "an app" had caused the queries.

4 Replacement Hostname Created - First Queried by Alfa Bank

Four days after the trump-email.com zone was deleted by the Trump Organization, Cendyn created a new hostname based on one of their own generic domain names, contact-client.com - and named the subdomain trump1, much in the style of the original mail1.trump-email.com.

Russia's Alfa Bank was the first to query for this new hostname, seen in the data on September 27th 2016. A passive DNS system from the Farsight company similarly saw a lookup for this new hostname on September 30th 2016.

Cendyn was again asked by news organizations why did they create this new hostname trump1.contact-client.com and Cendyn stated that is was needed so that the Trump Organization could access their "CRM" - Customer Relationship Manager software which is Cendyn's service shown by public records that the Trump Organization uses.

5 Replacement Hostname Deleted

The `trump1.contact-client.com` hostname was also deleted recently[3]. The server at the IP address both hostnames pointed to never stopped functioning and could be reached on at least port 25 although it appears to reject connections from unknown clients.

Both hostnames (`mail1.trump-email.com` and `trump1.contact-client.com`) received some unusual traffic after news organizations, hired network analysts, and law enforcement were made aware of the hosts. One or more possibly automated DNS dictionary probes can be seen in the data, as well as connections from a DSL IP in Russia, and a few other unknown sources.

[3] As seen in the provided data, the `trump1.contact-client.com` host resolved without error on November 11th, 2016 and there's no record of `trump1.contact-client.com` resolving without error again. A failure response code is seen on November 28th, 2016.

6 FBI Dismisses Queries as Marketing Related

News organizations have reported that the FBI dismisses the DNS look ups by the Russian Alfa Bank as all being automated server responses to marketing emails from the Trump Organization. We have seen two examples of marketing mail from this server, but only one which was sent during the time period of nomination to election, a Florida localized event announcement. There has been no explanation of why the Michigan IP or the Russian IP are the only two consistent and regular talkers - neither of which show any signs of malware infection. No anti-spam organization has any record of recipients reporting spam from this server. "This is spam" buttons are normally clicked by someone somewhere for legitimate bulk marketing campaigns. All 3 companies (Trump Org / vendor Cendyn, Spectrum Health, and Alfa Bank) did their own network analysis but none produced any artifact of marketing emails that correlate to the observed traffic.

7 Frequency and Diversity of Query Clients for Neighboring IP Address Space

An analysis was undertaken to compare the Trump server IP address with the surrounding IP address space. The intent was to learn if the DNS queries seen to the Trump server IP were similar to neighbors, and answer questions such as "does down-sampling inherent at observer locations render the collected data useless for drawing conclusions about the companies that ask to resolve the Trump server?"

Results: servers in the surrounding IP space had normal expected volumes for marketing email servers, including wide diversity of talkers. Servers in the surrounding IP space were similar to each other and dissimilar from the Trump server. The Trump server had by comparison a minuscule DNS query count and a set of only two companies (Spectrum Health and Alfa Bank) making consistent use of the mail1.trump-email.com host pointing to the IP address: `66.216.133.29`.

The wide diversity and high volume of servers on surrounding IPs suggests that any down-sampling that may or may not be present at observation points is still resulting in an accurate picture of comparative query client diversity and inferred traffic volume.

8 DATA FIELD DETAILS

The data is formatted as follows:

- # Indicates a comment
- Timestamp time zone: UTC
- name field

The data comes from multiple observers, marked in the data as o:name. The o:name has no meaning but does accurately connect all of the observations made by each observer or observation viewpoint. A utility such as grep may be used to filter the data

to just one o:name such as the most common, o:[redacted]. The other observer names may provide either additional query / response not seen by o:[redacted], or may provide the same query / response seen by o:[redacted] with small differences in timing due to location or clock differences.

Here is a count of observations from each o:name viewpoint:

```
COUNT OBSERVER
21479 o:[redacted]
1028 o:[redacted]
 592 o:[redacted]
 446 o:[redacted]
 301 o:[redacted]
 190 o:[redacted]
 120 o:[redacted]
  89 o:[redacted]
  54 o:[redacted]
  45 o:[redacted]
  31 o:[redacted]
  15 o:[redacted]
   5 o:[redacted]
   4 o:[redacted]
   2 o:[redacted]
   2 o:[redacted]
   2 o:[redacted]
   1 o:[redacted]
   1 o:[redacted]
```

9 Query Client IP address

Please note that query clients are often recursive resolvers, not email servers and not computers at which people sit. Recursive resolvers carry out the DNS lookups on behalf of the person, app, meeting / collaboration software or messaging service.

Michigan's Spectrum Health IP: `167.73.110.8`

Russian Moscow location Alfa Bank recursive resolvers: `217.12.96.15` and `217.12.97.15`.

A few other query client IPs are briefly seen in the data although none were consistent or frequent. In analyzing each of them, they were found to have past malware infections, whereas the Spectrum Health and Alfa Bank IP addresses were found to be completely clean and free of any indicators of past malware.

10 Question section aka what host was asked for in the query

```
COUNT HOSTNAME
```

```
24288 mail1.trump-email.com
```

mail1.trump-email.com was the only host based on the Trump-Email.com domain that was seen in any queries that pointed to the IP 66.216.133.29, until after the New York Times reporter began asking questions of Alfa Bank. After that point a variety of words were stuck in front of mail1.trump-email.com such as

```
banana.mail1.trump-email.com
Hades.mail1.trump-email.com
```

and more, which can be seen in the data provided.

After the Trump-Email.com zone was deleted from the Domain Name System, these additional hostnames were requested:

```
COUNT HOSTNAME
    7 mail.trump-email.com.moscow.alfaintra.net
    3 trump-email.com.moscow.alfaintra.net
```

and 4 days later:

```
trump1.contact-client.com
```

11 Answer section aka what was the authoritative response

66.216.133.29 is the IP address always seen in the DNS response for all successful queries. The IP address 66.216.133.29 has had a stable unchanging reverse DNS of mail1.trump-email.com at least since 2013-09-20, publicly verifiable within data provided from global reverse DNS scans at https://scans.io/study/sonar.rdns. Additional effort could likely establish the stable unchanging time period of existence back to 2009 when the domain was registered. The domain owner is the Trump Organization, with hosting and vendor dependencies consistent with TrumpOrg.com. Still today no one has altered the reverse DNS of 66.216.133.29 which continues to carry the legacy pointer of mail1.trump-email.com. Reverse DNS aka PTR, is under control of a separate vendor relationship and in an apparent oversight, no one told them told to eradicate the reverse record for the mail1.trump-email.com host name.

12 Response Code aka RCODE

The standard for RCODEs aka Response Code per query can be viewed at:

```
http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml\
   #dns-parameters-6
```

During the time period shown in the data prior to the New York Times reporter asking Alfa Bank why they send DNS queries to the Trump server, all observed queries had a success response code of RCODE:No Error.

```
COUNT RCODE
3554 RCODE:No Error
```

100% failure response codes occurred after the DNS zone for the domain was ordered to be deleted at approximately 13:50 UTC on September 23rd, 2016.

Failure codes seen include:

```
COUNT RCODE
  109 RCODE:Non-Existent Domain
    1 RCODE:Query Refused
20743 RCODE:Server Failure
```