

# CONFIDENTIAL

**From:** Rodney Joffe rjoffe@centergate.com   
**Subject:** White Paper  
**Date:** September 14, 2016 at 8:35 PM  
**To:** Manos Antonakakis antonakakis@gmail.com, David Dagon dagon@sudo.sh, April D Lorenzen april@zetalytics.com

---

Please read as if you had no prior knowledge or involvement, and you were handed this document as a security expert (NOT a dns expert) and were asked:

"Is this plausible as an explanation?".

NOT to be able to say that this is, with out doubt, fact, but to merely be plausible.

Do NOT spend more than a short while on this (If you spend more than an hour you have failed the assignment). Hopefully less.

:-)

Many thanks



White-  
Paper-1.txt

GOVERNMENT EXHIBIT

**0132**

21-CR-582 CRC

Antonakakis\_Gmail\_00000011

## CONFIDENTIAL

### White Paper #1 - Auditable V2

#### Findings:

The Trump organization uses a very unusually-configured "secret" email server in Pennsylvania for current and ongoing email communications with Alfa Bank (Moscow), and with Alfa Bank (Moscow) through another unusually-configured server (a "Tor exit node") at Spectrum Health in Michigan.

These servers are configured for direct communications between the Trump organization and Alfa Bank to the exclusion of all other systems.

The only plausible reason for this server configuration is to hide the considerable recent email traffic occurring between the Trump organization and Alfa Bank.

#### Discussion:

1. On approximately July 28, 2016, a lookup in global DNS for all the hostnames with a domain name that has the word "Trump" in it yielded 1,933 domains. [File: PTR-Contains-Trump-1933.txt]
2. Another look-up for all domains registered by the Trump organization yielded 3,352 domains. [Filename: Trump-Domains-Registered-3352.txt]
3. Searching the data set in #1 for hostnames containing "mail," "smtp," "relay," or "mta" yielded 537 unique hostnames (i.e., machine names). (Includes irrelevant results such as "Trumpets for America.") [Filename: Trump-And-Mail-MTA-Relay-Etc-537.txt]
4. Of the 537 unique hostnames in #3, 15 were registered by the Trump Organization. [Filename: Trump-Owned-And-Mail-Systems-15.txt]
5. Manual verification (by manually looking at the hosting location, the name servers and the domain ownership details) confirmed that the 15 hostnames registered by the Trump Organization (in #4) were owned and controlled by the Trump Organization. [Filename: Trump-Owned-And-Mail-System-WHOIS-15.txt]
6. A search of global nonpublic DNS activity revealed from which IP addresses in the world systems looked up these 15 domains, in the 90 day period from May 4 - Sept. 4, 2016. [Sample of output of search - Filename: MX-Lookups-For-15-Trump-Related-Domains.txt]
7. A computerized and manual scan of those results for anomalous data of any kind to identify anomalous data was undertaken.
8. That search yielded 14 domains with no anomalous data (e.g., trump-mail.com, trumpuniversity.com, and trumpsoho.com) and 1 that did contain anomalous data:

mail1.trump-email.com (IP address 66.216.133.29)

Antonakakis\_Gmail\_00000012

## CONFIDENTIAL

[Filename: Log-Of-DNS-Lookups-For-mail1.trump-email.com-851.txt]

9. trump-email.com, the "parent" domain for mail1.trump-email.com, is registered to the Trump organization, so mail1.trump-email.com is a Trump-controlled mail server. [See following WHOIS lookup and file referenced in #4]

10. Over the 90-day period from May 4 - Sept. 4, 2016, there were 19 external IP addresses (in yellow) from which A record searches originated for mail1.trump-email.com:

326 look-ups from 217.12.97.15 [Alfa Bank]  
288 look-ups from 217.12.96.15 [Alfa Bank]  
230 look-ups from 167.73.110.8 [Spectrum Health]  
98 look-ups from 50.207.241.62 [Domo, Inc., Salt Lake City. VPN provider]  
4 look-ups from 66.155.252.34 [malware on it]  
4 look-ups from 63.118.233.31 [malware on it]  
4 look-ups from 192.216.142.4 [malware on it]  
3 look-ups from 63.118.233.30 [malware on it]  
2 look-ups from 74.217.49.226 [malware on it]  
2 look-ups from 69.74.121.66 [malware on it]  
2 look-ups from 198.175.230.159 [malware on it]  
2 look-ups from 198.175.230.158 [malware on it]  
2 look-ups from 109.110.227.141 [malware on it]  
2 look-ups from 69.30.221.250 [malware on it]  
2 look-ups from 69.30.210.242 [malware on it]  
1 look-up from 79.134.218.13 [Obit ISP, St. Petersburg, owned by Alfa Bank]  
1 look-up from 69.30.198.202 [malware on it]  
1 look-up from 203.12.160.3 [malware on it]  
1 look-up from 204.101.0.66 [malware on it]

(These are the outside servers looking to send email to mail1.trump-email.)

11. A number of things about mail1.trump-email.com and the activity surrounding it stood out as being very unusual.

i. This is a very small number of source IP addresses: the number of IP addresses looking up the mail1.trump-email.com host name is minuscule—only 19 over ninety days. A normal mail server would have look-ups over a 90-day period coming from thousands to tens-of-thousands of different IP addresses.

ii. This is a very unusual distribution of source IP addresses: 4 IP addresses have significantly more lookups (97%) than the other 15 (3%). A normal distribution for mail look-ups would be fairly uniform in range, i.e., from each IP address would come a similar number of look-ups for any given domain name.

iii. The majority of lookups for this mail server are for the A (regular) record by Alfa Bank and not the MX (mail record). This is significant because it shows a mail server set up to masquerade as a regular (non-mail) server. (An A record search is the appropriate look-up for another form of communication (such as a VPN

Antonakakis\_Gmail\_00000013

## CONFIDENTIAL

or secure connection, a text connection, etc).)

- The top 2 IP addresses are the 2 main DNS servers belonging to Alfa Bank.
- Of the 975 total look-ups from the 19 IP addresses, 87% are from Alfa Bank or Spectrum Health (an Alfa Bank pass-through, discussed below).
- Add the suspicious look-ups from Domo, and 97% of the look-ups are suspect.

iv. mail1.trump-email.com is configured to only accept email from pre-determined and pre-approved IP addresses. When one tries to connect to mail1.trump-email.com (using telnet to port 25, the mail submission port), you get the response "lvpmta14.lstrk.net does not accept mail from you ([incoming IP address])." ["lvpmta" stands for "litrak virtual private mail transfer agent"]

This shows mail1.trump-email.com to be an active mail server (since there was a response from port 25) but one that highly restricts the sources from which it will accept email.

v. The Spectrum Health IP address is a TOR exit node used exclusively by Alfa Bank, i.e., Alfa Bank communications enter a Tor node somewhere in the world and those communications exit, presumably untraceable, at Spectrum Health. There is absolutely no reason why Spectrum would want a Tor exit node on its system. (Indeed, Spectrum Health would not want a TOR node on its system because, by its nature, you never know what will come out of a TOR node, including child pornography and other illegal content.)

vi. The 4th most active IP address (after Alfa Bank and Spectrum Health) belongs to DOMO, a commercial cloud and VPN service provider located in Utah. VPNs to public VPN providers such as DOMO are often used to obfuscate the source of Internet traffic.

vii. The Alfa Bank name servers are not respecting the TTL for the mail1.trump-email.com hostname. This requires either modification of standard configuration (which takes skill and effort) or it indicates a manual loop-up. This is highly unusual because Alfa Bank is a large sophisticated global organization, i.e., this was not done in error. (Fingerprinting of the name servers at Alfa Bank indicate modern resolver code; all of the modern resolvers respect TTL.) [Filename: DNS-Lookups-For-mail1.trump-email.com-Through-9-14.txt]

12. An updated search on Sept. 14, 2016 of the prior 90 days (i.e., June 17-Sept 14) shows a total of 3,553 look-ups for mail1.trump-email.com from only 9 IP addresses:

2,817 from the two Alfa Bank IP addresses;  
729 from the Spectrum Health Tor node; and  
7 from miscellaneous sources (3 internal and 4 from malware).

During this period, 99.8% of the look-ups for mail1.trump-email.com come from Alfa Bank or the Spectrum Tor node.

Antonakakis\_Gmail\_00000014

## CONFIDENTIAL

[Filename: DNS-Lookups-For-mail1.trump-email.com-Through-9-14.txt]

While there are possible explanations for the configurations of mail1.trump-email.com and the Spectrum Health TOR node, there is no plausible explanation other than obfuscation of communications between mail1.trump-email.com and Alfa Bank.

—

Antonakakis\_Gmail\_00000015