KIRKLAND & ELLIS LLP
AND AFFILIATED PARTNERSHIPS

655 Fifteenth Street, N.W.
Washington, D.C. 20005

Viet D. Dinh, P.C.
To Call Writer Directly:
(202) 879-5017
viet.dinh@kirkland.com

(202) 879-5000

www.kirkland.com

Facsimile:
(202) 879-5200

July 21, 2017

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510-6050

The Honorable Dianne Feinstein
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510-6050

Re: Alfa Bank

Dear Chairman Grassley and Ranking Member Feinstein:

Representatives of Alfa Bank, a privately owned Russian bank, previously briefed Committee staff on Alfa Bank's investigations into malicious attempts to attack its computer networks and spurious allegations that the bank maintained a secret communications link with the Trump Organization. I write today to transmit the final report of an independent investigation by Stroz Friedberg, a leading U.S. computer forensics firm, which "found no evidence of any connections or communications between Alfa-Bank and The Trump Organization occurring in 2017." That conclusion followed a similar independent investigation last year by Mandiant, another leading U.S. firm, which concluded that there was no evidence of substantive contact, such as emails or financial links, between Alfa Bank and the Trump Organization in 2016. The Stroz Friedberg and Mandiant reports are attached hereto as Exhibits I and II, respectively.

Both independent investigations confirm what Alfa Bank has stated clearly and consistently: Neither the bank nor its owners have had any relationship of any kind with the Trump Organization at any time, including over the past year. Alfa Bank has responded to spurious allegations against it and attempts to intrude into its computer networks like any other victim of such malice—by conducting full and independent investigations, contacting and cooperating with law enforcement authorities, and making all the facts available.

The absurd accusations against Alfa Bank began last year, when some media outlets published stories just before the 2016 presidential election claiming that computer servers belonging to Alfa Bank and the Trump Organization had been covertly communicating. These stories were published after select media outlets received highly confidential and highly private Domain Name Server (DNS) logs—which appear to have been obtained in an unauthorized or improper manner by an individual known only as "Tea Leaves"—that allegedly showed "activity" between a server belonging to a Trump-affiliated marketing company and a server affiliated with Alfa Bank. Although allegations of such a backdoor communication channel are plainly outlandish, Alfa Bank nevertheless hired Mandiant to conduct an independent review of the matter. To no one's surprise at Alfa Bank, Mandiant concluded that there was no evidence of substantive contact, such as emails or financial links, between Alfa Bank and the Trump Organization in 2016. Mandiant's hypothesis was that any server-related activity between Alfa Bank and the Trump Organization was the result of an automated email-based campaign to market Trump properties to Alfa Bank employees, as many other observers had likewise concluded.[1] Alfa Bank shared these findings with the U.S. Department of Justice and the Federal Bureau of Investigation.

Earlier this year, Alfa Bank was the target of a renewed wave of suspicious cyber-activity. In short, unidentified third-parties using hundreds of external IP addresses had repeatedly queried the bank's servers for an invalid hostname: "mail.trump-email.com.moscow.alfaintra.net." This invalid hostname combines or "concatenates" two possible hostnames: "mail.trump-email.com" and "moscow.alfaintra.net." Although the concatenated hostname has never existed, Alfa Bank's servers received over 20,000 queries for it in March 2017 alone.

In response to that suspicious activity, Alfa Bank immediately alerted the U.S. Department of Justice and retained Stroz Friedberg to conduct another independent investigation. Consistent with Mandiant's investigation, Stroz Friedberg's investigation "found no evidence of any connections or communications between Alfa-Bank and The Trump Organization occurring in 2017." The firm concluded that the appearance of the hostname "mail.trump-email.com.moscow.alfaintra.net" in Alfa Bank's DNS logs did not by any means suggest that Alfa Bank had been communicating with the Trump Organization. To the contrary, Stroz Friedberg's "analysis revealed that a broad group of people simply sent queries for the term 'mail.trump-email.com.moscow.alfaintra.net' to Alfa-Bank DNS servers" in 2017. Moreover, Stroz Friedberg examined several months of Alfa Bank emails for any mention of the word "Trump" and found only "false-positive results," such as news-alert emails from the Washington Post.

Thus, two of the leading cybersecurity firms in the United States have determined that there is no sign of any connection between Alfa Bank and the Trump Organization in any of the data

[1] *See, e.g.*, Sam Biddle et al., *Here's the Problem with the Story Connecting Russia to Donald Trump's Email Server*, The Intercept (Nov. 1, 2016), http://bit.ly/2fezLlh.

they examined. But the pattern of suspicious cyber-activity aimed at Alfa Bank—combined with the fact that some of its DNS logs appear to have been improperly obtained and disclosed—led to concerns that Alfa Bank had been the victim of a malicious and potentially unlawful effort to manufacture the false appearance of a relationship between Alfa Bank and the Trump Organization. In April, I and Stroz Friedberg met in Chicago with representatives of the Department of Justice and the Federal Bureau of Investigation to share the preliminary results of Stroz Friedberg's investigation. The bank pledged its full cooperation with government authorities, which continue to examine whether Alfa Bank has been the victim of illegal conduct.

* * *

The independent investigation by Stroz Friedberg was supervised by my partner Brian Benczkowski, the nominee to be Assistant Attorney General for the Criminal Division. I am happy to confirm that Alfa Bank has waived a contractual confidentiality provision so that Mr. Benczkowski can testify to the fact and scope of his work, while of course protecting any applicable privileges. As the victim of an apparent malicious hoax, Alfa Bank remains eager to get to the bottom of the false allegations against it, and stands ready to assist the Committee and all other government authorities as needed.

If any additional information would be useful, please call me at 202-879-5017. Thank you for your time and attention to this important matter.

Sincerely,

Viet D. Dinh

Counsel for Alfa Bank

Enclosures

EXHIBIT I

STROZ FRIEDBERG
an Aon company

Summary of Cyber Incident Investigation

Prepared for:

Kirkland & Ellis LLP & Alfa Bank JSC

Prepared by:

Stroz Friedberg, LLC

July 19, 2017

TABLE OF CONTENTS

I. SUMMARY OF INVESTIGATION

Kirkland & Ellis LLP, on behalf of its client Alfa Bank JSC ("Alfa-Bank"), engaged Stroz Friedberg, LLC ("Stroz Friedberg") on March 14, 2017, to provide technical and digital forensics services in support of Alfa-Bank's investigation of claims that the bank purportedly communicated with The Trump Organization. This document provides a high-level summary of Stroz Friedberg's work on this matter.

In February 2017, Alfa-Bank observed suspicious entries in its DNS[1] logs showing that Alfa-Bank servers received 16 queries, such as "mail.trump-email.com.MOSCow.ALFaintRa.nEt" (an invalid hostname), from external IP addresses.[2] These DNS requests were identical to the unverified DNS queries that were previously highlighted by security researcher Professor L. Jean Camp in 2016. Then, in March 2017, Alfa-Bank servers received more than 20,000 additional suspicious DNS queries for the same host name.

Kirkland & Ellis and Alfa-Bank asked Stroz Friedberg to conduct an independent investigation into the suspicious 2017 DNS queries to determine, to the extent possible, if they resulted from communications between Alfa-Bank and The Trump Organization. Kirkland & Ellis also informed Stroz Friedberg that Alfa-Bank received similar DNS queries in 2016, but those queries were outside our scope. Another incident response company, Mandiant, has already investigated and reported on the 2016 activity. The only aspect of the 2016 information Stroz Friedberg was asked to examine was the information posted online by Professor Camp. Stroz Friedberg was asked to determine, to the extent possible, whether the information might have originated from Alfa-Bank servers, and if so, whether there was any indication of how this information was obtained from Alfa-Bank systems.

A. ANALYSIS OF LOG AND EMAIL DATA

Stroz Friedberg searched Alfa-Bank's available aggregated log data and email archives for information related to bank communications to determine, to the extent possible, whether any communications occurred between Alfa-Bank and The Trump Organization. Specifically, Stroz Friedberg searched, among other data sources:

- DNS logs from all DNS servers in use at Alfa-Bank from February 18, 2017 to March 23, 2017
- Firewall logs from all firewalls at Alfa-Bank from February 20, 2017 to March 23, 2017
- The email archive containing all messages sent or received by email servers at Alfa-Bank from January 29, 2017 to April 6, 2017

[1] DNS, or the Domain Name System, is the system on the internet for converting easier to use alphanumeric names into numeric IP addresses computers need to connect to one another.

[2] IP addresses are the unique numbers assigned to computers to facilitate communication on the internet or across other computer networks.

These sets of information incorporated all available log and email data available at the time our searches were executed. We searched the available data using a broad set of search terms designed to return any communications between Alfa-Bank and The Trump Organization. For example, we searched the DNS logs for the word "trump" as well as any email message where the word "trump" appears in the sender, recipients, subject, or body of the email message. In total, we searched the available data using more than 20 broad keywords. Stroz Friedberg then analyzed the results of those searches to determine the nature of those search hits and to formulate follow-up searches.

From this data, Stroz Friedberg identified 321 unique IP addresses from across the world (many associated with Amazon Web Services) that sent the suspicious DNS queries containing the word "trump" to Alfa-Bank. We then searched the available log data to identify all other log entries containing those IP addresses to determine, to the extent possible, how those devices from those suspicious IP addresses interacted with Alfa-Bank systems. The combined efforts of the broad search, followed by specific follow-up searches, returned hundreds of thousands of DNS log entries, almost two million entries from the firewall logs, and several thousand email messages, all of which Stroz Friedberg analyzed and reviewed as part of its investigation.

Based on our analysis of the available 2017 email and log data, Stroz Friedberg found no evidence of any connections or communications between Alfa-Bank and The Trump Organization occurring in 2017. Nor did our analysis of the suspicious DNS requests made against the DNS servers at Alfa-Bank for "mail.trump-email.com.moscow.alfaintra.net" reveal any evidence to support claims that Alfa-Bank was exchanging email messages or other communications with The Trump Organization in 2017. Specifically, Stroz Friedberg observed:

- All mentions of "Trump" in email messages were false-positive results, i.e., were not communications with President Trump or anyone in The Trump Organization. The vast majority of the email messages mentioning "Trump" were news alert emails or market research emails from web sites such as Bloomberg.net, Barclays.com, Factiva.com, The Wall Street Journal (wsj.com), and WashingtonPost.com.
- None of the messages we reviewed contained any US government email addresses. Nor did they contain any Trump-related email addresses in the address fields of the messages.
- We identified no DNS queries for any host at trump.com, which should have existed if there were actually any email or other type of communication with The Trump Organization.
- All queries relating to trump-email.com were made by outside parties querying Alfa-Bank's DNS servers. These queries appear to have originated from multiple outside parties from a variety of source IP addresses. Further, the high volume of queries requesting IP addresses for a wide variety of host names other than "mail.trump-email.com.moscow.alfaintra.net" is consistent with the type of traffic often seen coming from security researchers or attackers checking or testing a company's security. While some of these queries appear random, the vast majority of the queries relate to actual systems at Alfa-Bank, which could have been uncovered by researching domain names with similar domain registration information.

B. ANALYSIS OF DATA POSTED BY PROFESSOR CAMP

Stroz Friedberg analyzed data posted to Professor Camp's website that appears to originate from Alfa-Bank systems. That data included certain DNS requests dated September 2016 that are substantively identical to DNS requests identified in 2017. As seen in the chart below, the only difference between several 2016 requests and some of the 2017 requests is capitalization:

September 2016	mail.trump-email.com.moscow.alfaintra.net
February 2017	mail.trump-email.com.MOSCow.ALFaintRa.nEt
March 2017	mail.trump-email.com.moscow.alfaintra.net

Multiple news articles and blog posts speculated that these 2016 and 2017 DNS queries are indicative of communication between Alfa-Bank and The Trump Organization. These articles and posts generally cited the invalid hostname "mail.trump-email.com.moscow.alfaintra.net," which is a concatenation of two separate names ("mail.trump-email.com" and "moscow.alfaintra.net"), as evidence of communication. Our analysis of the available 2017 data, however, does not support the supposition that communication occurred in 2017. Rather, our analysis revealed that a broad group of people simply sent queries for the term "mail.trump-email.com.moscow.alfaintra.net" to Alfa-Bank DNS servers.

Further, we found no evidence of unauthorized access to the Alfa-Bank's DNS servers in any of the 2017 data we reviewed. We examined the DNS logs, firewall logs, and network packet captures for any evidence of an outside party interacting with Alfa-Bank's systems in a suspicious way beyond the DNS queries. None of the data we reviewed revealed any suspicious traffic or connections other than the already identified DNS queries.

The information posted online by Professor Camp appears to include DNS log data from Alfa-Bank. However, because the information is from 2016 (when Alfa-Bank's practice was to preserve DNS log data only for 24 hours), log data at the bank no longer exists for that timeframe. As such, we were unable to verify whether or not the information is valid. Additionally, the format of the data does not match the format of actual logs at Alfa-Bank. If the DNS log data posted by Professor Camp is actual DNS log data from Alfa-Bank, it has been edited and placed into a different format. It is unknown how or from whom Professor Camp obtained this unverified data, seemingly from Alfa-Bank systems.

C. CONCLUSIONS

Our investigation revealed no actual connections or communications between Alfa-Bank and President Trump or The Trump Organization in any of the 2017 data we analyzed and no evidence of a compromise of the Alfa-Bank DNS servers in 2017. Because the concatenated name "mail.trump-email.com.moscow.alfaintra.net" has been widely published, it is likely that the suspicious queries came from researchers and/or would-be attackers who learned of this name from online sources and then issued queries to Alfa-Bank's DNS servers.

STROZ FRIEDBERG
an Aon company

About Stroz Friedberg

Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. Our focus is on cybersecurity, with leading experts in digital forensics, incident response, and security science; investigation; eDiscovery; intellectual property; and due diligence. Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong. Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at https://www.strozfriedberg.com/.

EXHIBIT II

MANDIANT®

A FireEye® Company

ALFA-BANK

Investigation Report (DRAFT)

November 04, 2016

SECURITY CONSULTING

CONTENTS

MANAGEMENT SUMARY

Intrusion Timeline

Skadden, Arps, Slate, Meagher & Flom LLP retained Mandiant on behalf of Alfa-Bank to support an investigation into unexplained DNS requests. *The New York Times* approached Alfa-Bank and alleged that Alfa-Bank was maintaining contact with the Trump Organization via the server "mail1.trump-email.com" from their DNS (domain name service) servers. They indicated they had evidence to support that allegation.

The New York Times provided a scan of several pages of what appeared to be passive DNS logs showing DNS requests for the host "mail1.trump-email.com". This domain was registered to an online marketing platform called "Cendyn", who promotes hotels owned by the Trump Organization.

The New York Times alleges that these communications were not merely DNS requests, but some form of communication channel between Donald Trump and Alfa-Bank's DMZ (demilitarized zone) DNS servers. According to Alfa-Bank, *The New York Times* further alleges that Alfa-Bank communicates trading information using the DNS connection mentioned above.

When Mandiant was engaged, a Russian security firm, Group IB, had already drafted a report that outlines the DNS environment in question and "whois" registrations (i.e., information to register a domain name including contact information such as name, email address, mailing address, and more).

Mandiant reviewed the report and initiated a detailed analysis of the DNS logs, email logs, Deep Discovery Inspector (DDI) logs, proxy logs, and email archives in coordination with the Alfa-Bank Team.

Log retention periods for DNS logs were set to 24 hours. Neither Alfa-Bank nor Mandiant could recover historical data beyond that period of time.

Tests were conducted that indicated using the domain in question would spark many DNS requests from different security appliances over the course of two days after mail entry. This was verified by sending a test email containing a test domain name to a specific internal account, and in parallel scanning the DNS and Deep Discovery Inspector logs for that domain name. However, there is no evidence indicating that scenario occurred for the requests between May and September 2016.

Findings

The evidence that *The New York Times* provided is consistent with passive DNS logs These types of logs are generated when a sensor on the network path between the requestor and the resolving server generate a DNS request. In the case of "mail1.trump-email.com" and "trump1.contact-client.com", the responsible DNS servers are "ns1.cdcservices.com", "ns2.cdcservices.com", and "ns3.cdcservices.com" as depicted in Figure 6. This means that when DNS requests from any computer on the Internet try to resolve the IP address for the domains above, the actual traffic goes to one of the three responsible DNS servers. The DNS servers belong to GoDaddy, a major network hosting provider.

Alfa-Bank has rules in place that only allow outbound traffic on port 25 (mail communication) to their mail servers. This indicated that direct communication on mail ports between Alfa-Bank DNS servers and "mail1.trump-email.com" and "trump1.contact-client.com" would have been blocked by the firewall.

In addition, on September 30, 2016, Alfa-Bank began blocking outgoing traffic to the two domains.

As GoDaddy hosts many more websites and domains, it is not possible for Alfa-Bank to block communication to the three mentioned DNS servers without interfering with normal usage of the Internet for their employees.

INVESTIGATION DETAILS

Domain Name Service

The Domain Name Service (DNS) is defined in “Request for Comment” 1035 (RFC1035).

“The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations.” (RFC1035)

Communication on the Internet is based on numerical IP addresses. As those are hard to remember for humans, the global Domain Name System acts like a phonebook and resolves textual domain names to IP addresses.

Thirteen logical root servers are the main authority for resolution. However, authority for actual domain names is typically delegated to so-called authoritative domain name servers responsible for a top-level domain. Examples of top-level domains (TLD) would include: .gov, .com or .mil.

Those authoritative domain name servers then point at a domain name server responsible for a certain domain, such as “trump-email.com”. The client that attempts to resolve the domain name contacts this domain name server to get the IP address currently assigned to the host delivering services under “trump-email.com”.

There are different types of requests. Two of those are important, in order to understand the technical details in this report:

- **Type A requests**: Requests to resolve the IP address for a specific domain name
- **Type MX requests**: Request domain name or IP address of the mail servers responsible to deliver email to all users with @<domain name> addresses.

At this point, the DNS resolution stage, there has not been any communication to the target host. The only communication that has occurred at this stage is communication to the responsible domain name server.

Evidence Provided by *The New York Times*

The New York Times provided Alfa-Bank with 61 pages of what appear to be passive DNS logs indicating requests from two servers in the Autonomous System zone (AS) AS15632 registered to “Alfa-Bank Moscow Russia” as shown in Figure 1.

Announced By		
Origin AS	**Announcement**	**Description**
AS15632	217.12.96.0/23	Alfa-Bank Moscow Russia

Figure 1: Details to AS15632

The files that *The New York Times* provided show events between May 4, 2016 and September 21, 2016. Figure 2 shows an example of the log entries provided by *The New York Times*. Every entry contains a timestamp, an IP address of one out of two Alfa-Bank servers, and the hostname mail1.trump-email.com.

There is no information showing the type or the content of the communication. However, “email look-ups” suggest only DNS MX lookups in technical terms.

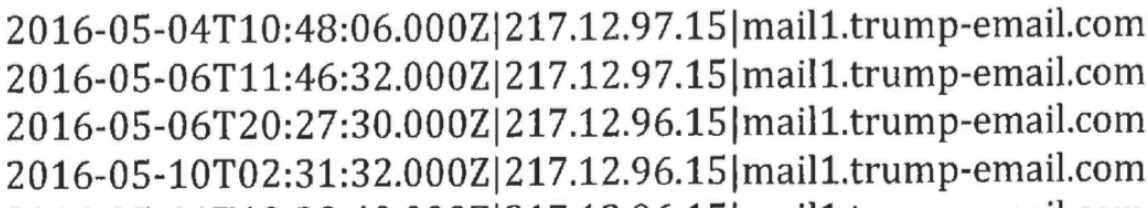


Figure 2: Excerpt of Logs Provided by NYT

Relevant Domains and Hosts

This paragraph describes hosts, domain-names, and systems relevant to this investigation.

“trump-email.com”

This is the parent domain for “mail1.trump-email.com” and holds the registrar information. The domain was registered in the name of “Trump Orgainzation” (sic). The administrative contact information is an organization called “Cendyn”, as shown in Figure 3. “Cendyn” is a company offering hospitality marketing. A 2007 news article indicates that “Cendyn has been selected as The Trump Organization's exclusive interactive marketing agency” (http://www.prnewswire.com/news-releases/cendyn-is-tapped-for-interactive-marketing-services-by-the-trump-organization-58251682.html). It is not unusual for marketing companies to register domains in the name of their customers.

After September 22, 2016 the “whois” entry was changed, and reference to Cendyn no longer exists in the registration.

The domain name is still hosted by GoDaddy and was first registered in August 14, 2009, as depicted in Figure 4. The following DNS servers are responsible to resolve resources in the “trump-email” domain.

- ns1.cdcservices.com
- ns2.cdcservices.com
- ns3.cdcservices.com

Those DNS servers host thousands of domain names for different customers.

Domain Name: TRUMP-EMAIL.COM
Registry Domain ID: 1565681481_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2016-06-29T14:27:44Z
Creation Date: 2009-08-14T20:06:37Z
Registrar Registration Expiration Date: 2017-07-01T03:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Trump Orgainzation
Registrant Organization: Trump Orgainzation
Registrant Street: 725 Fifth Avenue
Registrant City: New York
Registrant State/Province: New York
Registrant Postal Code: 10022
Registrant Country: US
Registrant Phone: +1.2128322000
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: emcmullin@cendyn.com
Registry Admin ID: Not Available From Registry
Admin Name: Emily McMullin
Admin Organization: Cendyn
Admin Street: 1515 N Federal Highway
Admin Street: Suite 419
Admin City: Boca Raton

Figure 3: Whois Data for trump-email.com

```
Domain Name: TRUMP-EMAIL.COM
Registrar: GODADDY.COM, LLC
Sponsoring Registrar IANA ID: 146
Whois Server: whois.godaddy.com
Referral URL: http://www.godaddy.com
Name Server: NS1.CDCSERVICES.COM
Name Server: NS2.CDCSERVICES.COM
Name Server: NS3.CDCSERVICES.COM
Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Updated Date: 29-jun-2016
Creation Date: 14-aug-2009
Expiration Date: 01-jul-2017
```

Figure 4: DNS Servers for trump-email.com

"mail1.trump-email.com"

This is the server shown in the logs provided by *The New York Times*. At the time Mandiant initiated their investigation, none of the three responsible DNS server resolved the domain name "mail1.trump-email.com". However, Alfa-Bank provided a report done by Group IB that indicated that the "mail1.trump-email.com" previously resolved to the IP address "66.216.133.29".

"217.12.96.15" and "217.12.97.15"

These IP addresses belong to Linux DNS servers located in Alfa-Bank's DMZ. At the time Mandiant initiated their investigation, Alfa-Bank's log retention period was set to 24 hours. Alfa-Bank indicated this was due to normal operations generating a high volume of requests; therefore, physical space for log storage was not economically feasible.

"trump1.contact-client.com"

The FQDN (Fully Qualified Domain Name) "trump1.contact-client.com" was another domain that pointed to the IP 66.216.133.29, which was formerly used by "mail1.trump-email.com".

Mandiant verified that "trump1.contact-client.com" still resolves to the IP address "66.216.133.29", as shown in Figure 5.

```
#  nslookup trump1.contact-client.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   trump1.contact-client.com
Address: 66.216.133.29
```

Figure 5: Nslookup for trump1.contact-client.com

"contact-client.com"

This is the parent domain for "trump1.contact-client.com". According to "whois" information, the domain was registered to "Charles Deyo". "Charles Deyo" was the name of the Cendyn CEO, as depicted in Figure 6. The webpage hosted at "contact-client.com" redirects to the "Cendyn" webpage.

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: CONTACT-CLIENT.COM
Registrar URL: http://www.godaddy.com
Registrant Name: Charles Deyo
Registrant Organization:
Name Server: NS3.CDCSERVICES.COM
Name Server: NS2.CDCSERVICES.COM
Name Server: NS1.CDCSERVICES.COM
DNSSEC: unsigned
```

Figure 6: whois information for contact-client.com

Investigated Evidence

Alfa-Bank provided access to the following evidence on site in Moscow. The files are too large to effectively transfer them electronically.

Type	Retention Period	Notes
DNS logs for 217.12.96.15 and 217.12.97.15	24 hours	DNS logs are now stored in ArcSight and available since October 7, 2016
Mail Server Logs	6 Months	timestamp, source, target, verdict
Proxy Server Logs	6 Months	timestamp, source, target, verdict
Deep Discovery Inspector	6 Months	
Mail archives	12 Months	

Table 1: Logs and Retention Periods

All logs have been analyzed. The analyst searched specifically for the general name “trump” and the IP addresses listed in the “Relevant domains and hosts” section. Furthermore, Mandiant conducted time based proximity analysis on randomly selected days where *The New York Times* logs show events.

Findings

Emails from “contact client.com”

Examining the mail logs indicated that emails from various hosts of the “contact-client.com” domain are incoming. Figure 7 shows an example of the incoming email request from “contact-client.com”. Queries for “trump1.contact-client.com” in the mail logs provided no results.

```
Jul 27 2016 23:13:31,Spam,BLOCKED,66.216.179.229,J3BICIDUC119HR4TOT14BDJ5SDRHH8BB1K1HD8E953@b.contact-client.com,ekaufman@alfabank.com,No Virus found
```

Figure 7: Example for Incoming contact-client.com email

Emails from trump-email.com

The mail logs did not show mails from or to trump-email.com addresses in the available timeframes (Figure 8).

Figure 8: ArcSight Queries for Mail Log

DNS Lookup Peaks Caused by Deep Discovery Inspector

During the investigation, Mandiant, in conjunction with Alfa-Bank, observed that Trend Micro Deep Discovery Inspector resolves all domain names mentioned in email bodies multiple times. This is to not only to determine if the domain name itself is flagged malicious, but also to determine if the currently assigned IP address shows up in a blacklist.

Further tests with other domain names indicated that Deep Discovery Inspector would try to resolve the domain name again, irregularly over the course of two days.

To test that, Alfa-Bank added the domain name “dns-servertrump-email.com” to an email message body. The domain "dns-servertrump-email.com" was fictitious. It was an attempt by Alfa-Bank to ensure, that any other source resolving that domain name did not exist on the Alfa-Bank network. This caused 11 automated DNS requests within the first 14 seconds of the mail coming in. In particular, the requests were A and AAAA requests, meaning simple DNS lookups for IPv4 and IPv6 addresses.

The investigation at Alfa-Bank generated mail traffic internally in Alfa-Bank, and between Alfa-bank and their security vendors containing the investigated domain names. These emails automatically lead to the generation of additional DNS requests for those domains originating from Deep Discovery Inspector.

Additional requests were generated by Alfa-Bank when they used “nslookup” to resolve the hosts’ IP address for further log file investigations.

trump-email.com Used for Promotion

Mandiant also investigated how the “trump-email.com” domain was used in the past. Figure 9 shows that the domain formerly offered hotel promotion deals for a Trump hotel.

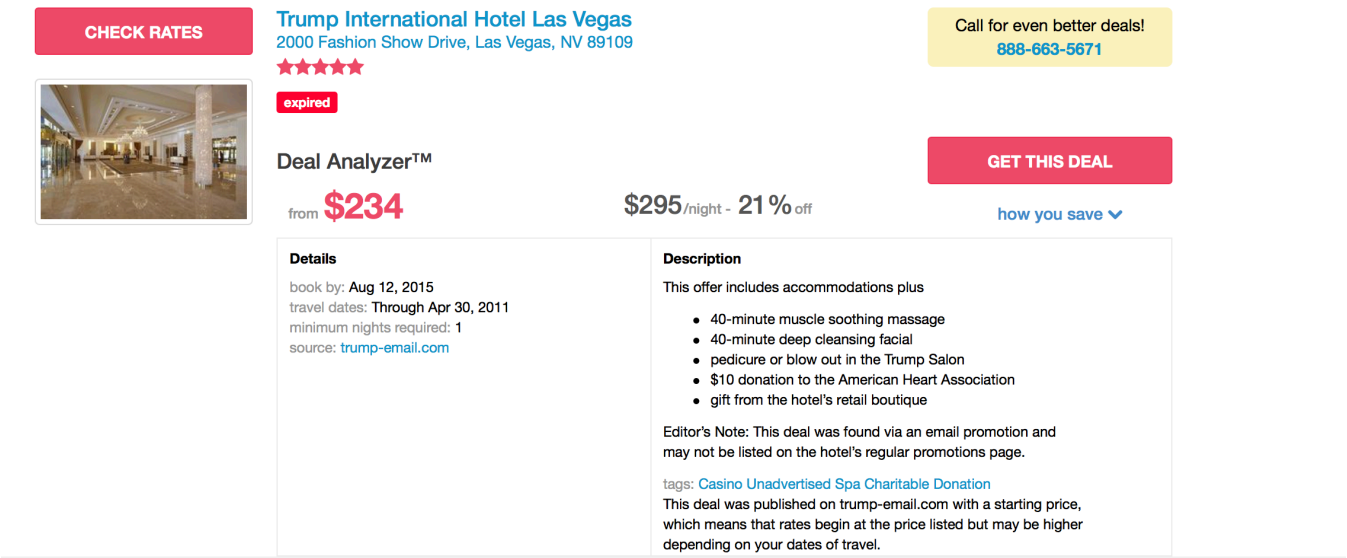


Figure 9: Hotel Promotion Using trump-email.com

Related Emails in Mail Archive

Analysis of the Alfa-Bank mail archives indicated three emails with hits for “mail1.trump-email.com domains”. Two hits were the same promotion mail to two different users as shown in Figure 10. The third email was a different promotion email and is listed in Figure 11.

Two of the three emails were delivered via the “mail1.trump-email.com” server. The email sender, and links in the mail body, point to contact-client.com.

Inspirational Travel & Exciting Savings

TH

Trump Hotel Collection <TrumpHotelCollection@contact-client.com>
Thursday 4 February 2016 at 17:23
An: smizenin@alfabank.ru

View this email with images

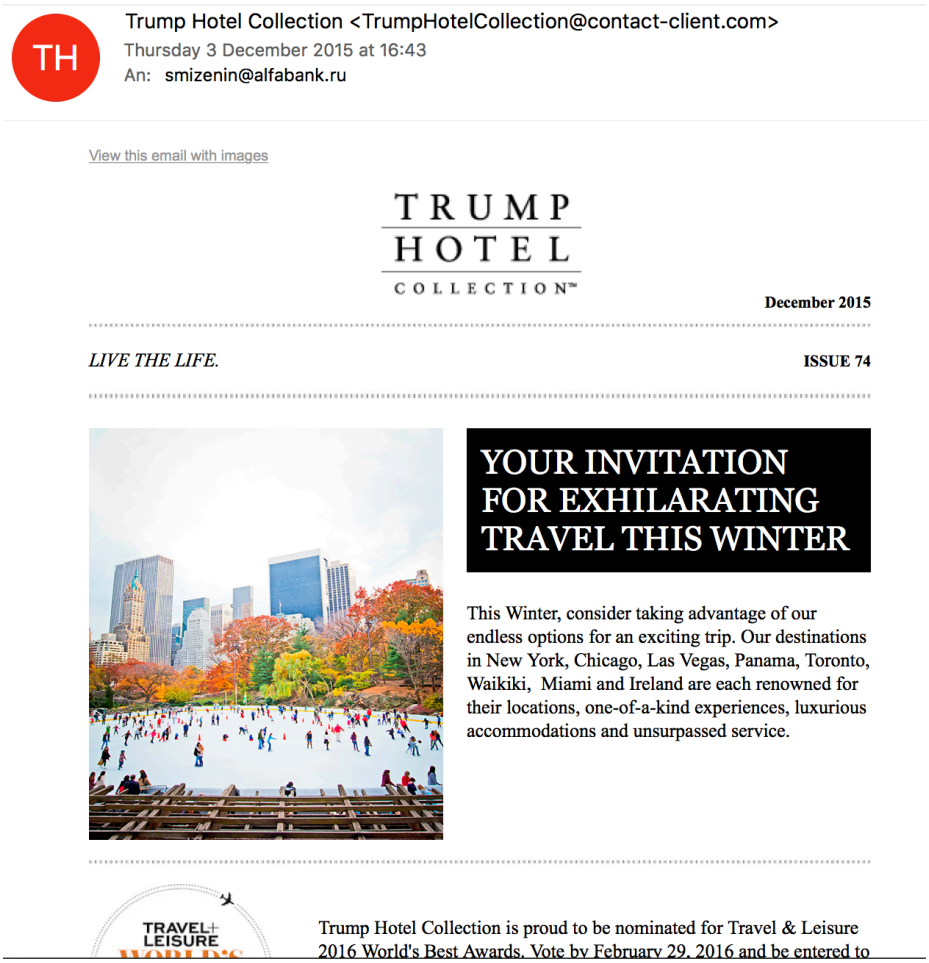
TRUMP
HOTELS™

February 2016

LIVE THE LIFE. **ISSUE 76**

INSPIRATIONAL TRAVEL & EXCITING SAVINGS

Figure 10: Promotion Mail in Feb. 2016



TH

Trump Hotel Collection <TrumpHotelCollection@contact-client.com>
Thursday 3 December 2015 at 16:43
An: smizenin@alfabank.ru

View this email with images

TRUMP
HOTEL
COLLECTION™

December 2015

LIVE THE LIFE.

ISSUE 74

YOUR INVITATION FOR EXHILARATING TRAVEL THIS WINTER

This Winter, consider taking advantage of our endless options for an exciting trip. Our destinations in New York, Chicago, Las Vegas, Panama, Toronto, Waikiki, Miami and Ireland are each renowned for their locations, one-of-a-kind experiences, luxurious accommodations and unsurpassed service.

TRAVEL+ LEISURE

Trump Hotel Collection is proud to be nominated for Travel & Leisure 2016 World's Best Awards. Vote by February 29, 2016 and be entered to

Figure 11: Promotion Mail in Dec. 2015