# RE: FD-1023 Draft Content --- UNCLASSIFIED

**From:** "SANDS, ALLISON (CG) (FBI)" <asands@fbi.sgov.gov>
**To:** "TRIFILETTI, CHRISTOPHER D. (SI) (FBI)" <cdtrifiletti@fbi.sgov.gov>, "VOS, DAVID (CG) (FBI)" <dvos@fbi.sgov.gov>
**Date:** Fri, 07 Oct 2016 08:59:18 -0400

Classification: UNCLASSIFIED
==========

Thank you Chris! Does this include everything from the conversation yesterday? Un fortunately I couldn't be there and my team isn't in yet.

---

**From: TRIFILETTI, CHRISTOPHER D. (SI) (FBI)**
**Sent: Thursday, October 06, 2016 4:54 PM**
**To: VOS, DAVID (CG) (FBI); SANDS, ALLISON (CG) (FBI)**
**Subject: RE: FD-1023 Draft Content --- UNCLASSIFIED**

**Classification: UNCLASSIFIED**
==========

**David / Allison,**

**This is the actual text from the final 1023 I submitted, with a few grammatical and spelling corrections, etc.:**

**Source Reporting:**

**CHS provided the following answers to questions regarding information previously provided and other related information:**

**Where is the DNS visibility coming from to provide the DNS logs? Unknown, CHS was told they were collected lawfully; CHS' understanding is that FBI's Tom Grasso may arrange a call for investigators with the author of the whitepaper, David Degon of Georgia Tech, however CHS believes Degon also likely did not gather it himself.**

**Is it possibly still a marketing server misconfigured or a spam blocking device or IDS doing DNS resolutions? If this server was used to send bulk email, every server in world would try to resolve it, especially in email as a form of spam prevention; if it was a spam campaign, it could not do domain spoofing at the IP layer; if that were the case it would look more like other email and first server to connect to new host wouldn't likely be Russian.**

**Why would a bad actor name it after Trump, which seems so obvious? This is opinion, but if one wants to hide from the USIC, they can either do it via encryption and private accounts in privacy centric countries, or can do it a way that would not look suspicious, in this case using a worldwide spamming network that has reasonable email traffic worldwide.**

**Is it possible Cendyn named the domain? Yes, Cendyn has control of both domains, they were the ones who named it and controlled it each time.**

**Is it possible they relinqueshed control? Trump Organization representatives claim so, but in 2010 the domain ownership was changed to the Trump Organization, then the nameservers were assigned to Cendyn. Russian servers were the first to lookup the new domain name.**

**Could that be an intrusion response? It could be, but subdomain wouldn't/shouldn't be known to or visited by an intrusion responder.**

**What about someone doing a lookup of the IP to the new hostname? There should be no way for a lookup to see that, unless misconfigured by Cendyn to allow world to see zone file, i.e. a**

dns zone transfer, which is almost unheard of and required intentional steps to misconfigure.

Why when looking at the mx record is there almost no activity? It may be the case it was not used for mail activity, but would have to be some application layer connections as mx should show lookup, which it did not; anything sent by Windstream would be dropped since it is not listed in mx records; notably, email reputation services show no history of significant email from the IP address.

What kind of responses are you getting from the Trump Organization representatives? No technical answers are being given, only denying any Trump involvement.

Who have you discussed this with in the Trump Organization? The two calls have been arranged by Trump's Campaign Media Coordinator, Hope Hicks; the particpants on the calls are a Director of IT for the Trump Organization and a Web Development Manager.

What have they said on the calls so far? On call yesterday they seemed to accidentally confirm the DNS traffic occurred, but then would not share any data; as of today they are denying it and are not providing any answers.

Could this be IDS activity? This could be IDS activity, but that wouldn't usually involve DNS host names, should only be IP addresses, and A record lookups shouldn't be occurring.

Have you connected to any ports on the IP address? No, as everything was being taken down already and also did not want to touch it; that said, port scans reported by others indicated only port 25 listening and also only accepting email from select ip addresses, or maybe none at all; this is not typical as most mail servers will accept mail from any source, then filter internally.

How is that different than open relay? It is the opposite of open relay, which will take and send all mail; in the case of the Trump mail server, it is not allowing any inbound email and appears to reject all email, or maybe just allows specific ips, which is what Degon's whitepaper says it does.

Is there any indication of actual mail being sent? Only based on evidence on DNS traffic; no actual email observed, but observed traffic indicates some layer 7 activity.

What does Spectrum Health say about their IP address being involved? They said it was likely a misconfigured application reaching out to the server.

What does Cendyn say about their IP address being involved? They said they have customers in Russia who may have server(s) reaching out, but to see that they would have to reference the Trump email server, and that would have to have been manually configured.

How inclusive was the list of DNS lookups you provided? Unknown; the analysis is based on what given; would have to contact author of whitepaper to follow-up.

Why did domain tools not appear on those logs? Domain tools only looks at domain or common hostnames.

Wouldn't spam have to show a great number of lookups? Yes, which is the important question; if this is full DNS data then the lack of other lookups shows targeted rather/strange than routine/normal activity.

Why use the same IP address after changing domain name? Because many nation state actors reuse same infrastructure and make mistakes or cut corners, i.e. reuse of mail registration names, leaving Cyrillic characters in leaked DNS data, etc.

What would solve the puzzle for researchers like Degon? They need some explanation from the source, the Trump Organization or their providers.

Is the key that a blind DNS request was made for the new hostname? Yes, the log activity is suggestive; also that Alfa Bank was on the new hostname so fast was interesting, unless they were told by someone like Cendyn and went looking; which can't be confirmed unless one or more of the involved entities provides data.

What else is surprising? CHS is surprised that the Trump representatives are offering such strange explanations that don't make sense, i.e. mail forwarding, analytical A name lookups by unusual non-analytical entities.

Anything else? It is also surprising that Alfa Bank hired FireEye, which seems unusual given cost and exposure, but given the lead time, Alfa Bank could have already covered their tracks, provided the wrong systems or data, etc.

Is the Washington Post going to print their story soon? They will probably print soon, in next day or son, mostly because of lackluster responses from the Trump representatives.

What will you do if your analysis is wrong? Analysis thus far and comments made have only been based on the data known; CHS has reserved judgement to be open to new data and would refine or restate analysis based on any new data or findings.

Is there any indication of lookups going in other direction? CHS does not have; this could mean they were not collected by original source or maybe not available due to monitoring method, i.e. DNS resolutions may have been on another non-monitored IP

Does this mean the collection source may be at Cendyn level and not at a higher level of visibility such as an ISP or backbone provider? Yes.

Is this possibly a targeted campaign from Alfa Bank by an entity posing as a Trump domain? Could be, but in that case we should see SPF lookups, which is not present in collected data; what this means depends on if data collected correctly or fully.

Does whitepaper say that the sensors cannot see text dns lookups? Possible, not sure.

---

From: TRIFILETTI, CHRISTOPHER D. (SI) (FBI)
Sent: Thursday, October 06, 2016 4:47 PM
To: VOS, DAVID (CG) (FBI); SANDS, ALLISON (CG) (FBI)
Subject: FD-1023 Draft Content --- UNCLASSIFIED

**Classification: UNCLASSIFIED**
==========

David / Allison,

Here is the draft of the FD-1023 I did today for our discussion with my CHS, it should be approved and go to your file soon:

Where is the DNS visibility coming from to provide the DNS logs? Unknown, CHS was told they were collected lawfully; CHS' understanding is that FBI's Tom Grasso may arrange a call for investigators with the author of the whitepaper,

David Degon of Georgia Tech, however CHS believes Degon also likely did not gather it himself.

Is it possibly still a marketing server misconfigured or a spam blocking device or IDS doing DNS resolutions? If this server was used to send bulk email, every server in world would try to resolve it, especially in email as a form of

spam prevention; if it was a spam campaign, it could not do domain spoofing at the IP layer; if that were the case it would look more like other email and first server to connect to new host wouldn't likely be Russian.

Why would a bad actor name it after Trump, which seems so obvious? This is opinion, but if one wants to hide from the USIC, they can either do it via encryption and private accounts in privacy centric countries, or can do it a way that

would not look suspicious, in this case using a worldwide spamming network that has reasonable email traffic worldwide.

Is it possible Cendyn named the domain? Yes, Cendyn has control of both domains, they

were the ones who named it and controlled it each time.

Is it possible they relinqueshed control? Trump Organization representatives claim so, but in 2010 the domain ownership was changed to the Trump Organization, then the nameservers were assigned to Cendyn. Russian servers were the first

to lookup the new domain name.

could that be an intrusion response? It could be, but subdomain wouldn't/shouldn't be known to or visited by an intrusion responder.

What about someone doing a lookup of the IP to the new hostname? There should be no way for a lookup to see that, unless misconfigured by Cendyn to allow world to see zone file, i.e. a dns zone transfer, which is almost unheard of and

required intentional steps to misconfigure.

Why when looking at the mx record is there almost no activity? It may be the case it was not used for mail activity, but would have to be some application layer connections as mx should show lookup, which it did not; anything sent by

Windstream would be dropped since it is not listed in mx records; notably, email reputation services show no history of significant email from the IP address.

What kind of responses are you getting from the Trump Organization representatives? No technical answers are being given, only denying any Trump involvement.

Who have you discussed this with in the Trump Organization? The two calls have been arranged by Trump's Campaign Media Coordinator, Hope Hicks; the particpants on the calls are a Director of IT for the Trump Organization and a Web

Development Manager.

What have they said on the calls so far? On call yesterday they seemed to accidentally confirm the DNS traffic occurred, but then would not share any data; as of today they are denying it and are not providng any answers.

Could this be IDS activity? This could be IDS activity, but that wouldn't usually involve DNS host names, should only be IP addresses, and A record lookups shouldn't be occurring.

Have you connected to any ports on the IP address? No, as everything was being taken down already and also did not want to touch it; that said, port scans reported by others indicated only port 25 listening and also only accepting email

from select ip addresses, or maybe none at all; this is not typical as most mail servers will accept mail from any source, then filter internally.

How is that different than open relay? It is the opposite of open relay, which will take and send all mail; in the case of the Trump mail server, it is not allowing any inbound email and appears to reject all email, or maybe just allows

specific ips, which is what Degon's whitepaper says it does.

Is there any indication of actual mail being sent? Only based on evidence on DNS traffic; no actual email observed, but observed traffic indicates some layer 7 activity.

What does Spectrum Health say about their IP address being involved? They said it was likely a misconfigured application reaching out to the server.

What does Cendyn say about their IP address being involved? They said they have customers in Russia who may have server(s) reaching out, but to see that they would have to reference the Trump email server, and that would have to have

been manually configured.

**How inclusive was the list of DNS lookups you provided? Unknown; the analysis is based on what given; would have to contact author of whitepaper to follow-up.**

**Why did domain tools not appear on those logs? Domain tools only looks at domain or common hostnames.**

**Wouldn't spam have to show a great number of lookups? Yes, which is the important question; if this is full DNS data then the lack of other lookups shows targeted rather/strange than routine/normal activity.**

**Why use the same IP address after changing domain name? Because many nation state actors reuse same infrastructure and make mistakes or cut corners, i.e. reuse of mail registration names, leaving Cyrillic characters in leaked DNS data,**

**etc.**

**What would solve the puzzle for researchers like Degon? They need some explanation from the source, the Trump Organization or their providers.**

**Is the key that a blind DNS request was made for the new hostname? Yes, the log activity is suggestive; also that Alfa Bank was on the new hostname so fast was interesting, unless they were told by someone like Cendyn and went looking;**

**which can't be confirmed unless one or more of the involved entities provides data.**

**What else is surprising? CHS is surprised that the Trump representatives are offering such strange explanations that don't make sense, i.e. mail forwarding, analytical A name lookups by unusual non-analytical entities.**

**Anything else? It is also surprising that Alfa Bank hired FireEye, which seems unusual given cost and exposure, but given the lead time, Alfa Bank could have already covered their tracks, provided the wrong systems or data, etc.**

**Is the Washington Post going to print their story soon? They will probably print soon, in next day or son, mostly because of lackluster responses from the Trump representatives.**

**What will you do if your analysis is wrong? Analysis thus far and comments made have only been based on the data known; CHS has reserved judgement to be open to new data and would refine or restate analysis based on any new data or**

**findings.**

**Is there any indication of lookups going in other direction? CHS does not have; this could mean they were not collected by original source or maybe not available due to monitoring method, i.e. DNS resolutions may have been on another**

**non-monitored IP**

**Does this meand the collection source may be at Cendyn level and not at a higher level of visibility such as an ISP or backbone provider? Yes.**

**Is this possibly a targeted campaign from Alfa Bank by an entity posing as a Trump domain? Could be, but in that case we should see SPF lookups, which is not present in collected data; what this means depends on if data collected**

**correctly or fully.**

**Does whitepaper say that the sensors cannot see text dns lookups? Possible, not sure.**

**Regards,**

**Chris**

==========

**Classification: UNCLASSIFIED**

==========
**Classification: UNCLASSIFIED**

==========
**Classification: UNCLASSIFIED**