

From: BATTY, N C. (CYD) (FBI) <NCBATTY@fbi.sgov.gov>
Sent: Wednesday, September 21, 2016 4:46 PM
To: HUBIAK, JOSHUA J. (PH) (FBI) <JJHUBIAK@fbi.sgov.gov>; HEIDE, CURTIS A. (CG) (FBI) <CAHEIDE@fbi.sgov.gov>
Cc: WIERZBICKI, DANIEL S. (CG) (FBI) <DSWIERZBICKI@fbi.sgov.gov>; COTELLESSE, GERALD S. (PH) (FBI) <GSCOTELLESSE@fbi.sgov.gov>; STRANAHAN, TIMOTHY (CE) (FBI) <TMSTRANAHAN@fbi.sgov.gov>; NORWAT, BRANDON H. (CD) (FBI) <BHNORWAT@fbi.sgov.gov>; HELLMAN, SCOTT J. (CYD) (FBI) <SJHELLMAN@fbi.sgov.gov>
Subject: Analysis of Trump White Paper --- UNCLASSIFIED//FOUO
Attach: Analysis of Trump server white paper.docx

Classification: UNCLASSIFIED//FOUO
=====

Josh, Curtis, by way of update,

CG (Curtis Heide) just called to inquire about ECOU 1's involvement in the Trump matter you and I discussed yesterday. Curtis has been working (TDY) the election issues and has been called back by CD to work matters related to this white paper. CG had a copy of the white paper I forwarded to you from CD channels, and was inquiring as to whether ECOU 1 had any logs or other data from the referenced server.

I communicated to Curtis that we (CyD) haven't opened a case yet, and based on the information we know, ECOU 1 does not have an equity in this issue, as we do not see an intrusion nexus, and we assess the information to point primarily to a CD issue (as you mentioned, this could also be a public corruption issue). Therefore, ECOU 1 doesn't intend to open a case unless requested specifically by CD that we do so in a supporting role.

Curtis advised CG would be opening a CD case (105....z or other), in-line with Curtis' assignment on the 'special'. I affirmed that ECOU doesn't have an equity in the issue for now, and that which field office opens the case is a CD matter as far as we are concerned.

I told Curtis that CyD is ready and willing to assist in any way, and we were glad to open a case if requested. I also told him I had sent the white paper to PH, PH had reviewed it, also felt that CyD would open a case only as requested in a supporting role, and offered to open a CyD case if requested.

Curtis, Josh is A/SSA for PH's cyber squad. PH is ready and willing to assist as needed. Also, could you let me know what you'd like done with these (2) thumb drives? We have a chain of custody from their receipt by FBI General Counsel James Baker.

A/AD Sporre asked us to evaluate this for cyber equities, and to provide a assessment from a cyber perspective. Below is ECOU 1's assessment of the white paper and supporting documentation provided to us by CyD A/AD Sporre on 9/20/2016.

V/R

Nate

<<...>>

=====
Classification: UNCLASSIFIED//FOUO

FBI-DWS-12-0018092

SCO-016969
SCO-3500U-010031

Assessment of the provided white paper and supporting documentation on (2) thumb drives.

SUMMARY – ECOU 1 assess there is no CyD equity in this report and that the research conducted in the report reveals some questionable investigative steps taken and conclusions drawn. This opinion is drawn from the following observations:

The investigators who conducted the research appear to have done the following:

1. Searched, via publically available information, for every internet domain (a “domain” is “abc.com”) that had the word “Trump” in it.
2. Scrubbed that list of those domains for the words “mail”, “smtp”, “relay”, or “mta”. Filtering on these key words would provide possibilities of mail servers.
 - a. For any given domain name (“abc.com”), there could be an e-mail server that provides e-mail services to the domain. This service allows the owner of “abc.com” to have e-mail addresses such as “johndoe@abc.com”, etc). E-mail servers have a domain name of their own, and commonly, those domain names could be something like “mail.abc.com”, or “mail1.abc.com”, etc.
 - b. These steps are a very round-about way to identify mail servers associated with domains. A more standard process would be to look up a domain such as “trump-email.com”, and then search for attending mail servers to trump-email.com. However, this standard process would not reveal mail1.trump-email.com (because mail1.trump-email.com isn’t registered as the mail server for trump-email.com). Furthermore, if one were to only be looking for hidden mail servers, it is unlikely one would search for Donald Trump’s hidden mail servers by searching for mail servers with the name “trump” and “mail” included in them. Therefore, these two search steps could indicate the investigator already knew of the domain “mail1.trump-email.com”, and conducted these searches to reverse-support their knowledge.
3. Results from steps 1 and 2 are stated in the research paper to yield 537 domains. These results were filtered by domains that were “...registered by the Trump organization...”, which yielded 15 results.
 - a. Registration by the Trump organization appears to have been confirmed via whois lookups. This is a reliable source, but should not be deemed definitive without confirmation through formal legal process.
 - b. One of these 15 results was the domain “mail1.trump-email.com”.
4. The next steps the investigator took were:
 - a. Attempted to communicate with mail1.trump-email.com over port 25 (a mail submission port), and received an error message indicating the server did not accept communications over port 25 from the investigator’s IP address (not definitive whether the server would receive communication from others, or even many others).
 - b. Searched “...global nonpublic DNS activity...” (unclear how this was done) and discovered there are (4) primary IP addresses that have resolved the name

UNCLASSIFIED//FOUO

"mail1.trump-email.com". Two of these belong to DNS servers at Russian Alfa Bank. [When computer A wants to communicate with computer B, computer A must know computer B's IP address. In order to learn computer B's IP address, computer A conducts a DNS lookup, which essentially is a public inquiry, asking "Hello world, what is the IP address for mail1.trump-email.com?" The investigator's research indicates, over the period May 4 2016 – Sept 4 2016, two of Alfa Bank's DNS resolvers, asked the world 614 times what mail1.trump-email.com's IP address was, presumably so it (a computer at Alfa Bank) could communicate with mail1.trump-email.com. Two other IPs also conducted a statistically significant number of DNS lookups for email1.trump-email.com.

- c. Provided the identities of numerous dubious persons associated with Alfa Bank.
- 5. From the steps in # 4 above, the investigator seems to have concluded the following, which may or may not be true:
 - a. That mail1.trump-email.com is in fact a mail server and is owned by a Trump organization; this conclusion seems based off of:
 - i. The whois record
 - ii. The name "mail1" included in the domain name (though you can name a domain anything you want; the domain name "i.am.an.email.server.trump.com" is not necessarily an e-mail server for trump.com)
 - iii. That mail1.trump-email.com is responsive (though with an error message) to standard e-mail receiving port 25
 - b. That mail1.trump-email.com is "secret", or obfuscated from the general public, because:
 - i. The Russian computers must be configured specially to talk directly to mail1.trump-email.com (because you cannot find mail1.trump-email.com via a standard MX (mail server) lookup of trump-email.com).
 - c. That the [presumed] e-mail server is set up specifically to only communicate to designated IP addresses (though there is no substantiation that mail1.trump-email.com communicates with any IPs at all).
 - d. That the Russian computers have actually communicated with mail1.trump-email.com (though there is only information indicating the Russian computers have asked what mail1.trump-email.com's IP address is).
 - e. That there is no plausible reason why these communications would occur excepting for illegitimate reasons. This is because a server (such as mail1.trump-email.com) would never be found by somebody trying to send mail directly to the trump-email.com domain. A person would have to expressly search for the obscure name "mail1.trump-email.com" to find it. Therefore the Russian computers have been specially configured to communicate directly to "mail1.trump-email.com".
 - f. The communication between mail1.trump-email.com is between the Trump organization and bad actors working at Alfa Bank or associated with Alfa Bank.

UNCLASSIFIED//FOUO

FBI-DWS-12-0018094

SCO-016971
SCO-3500U-010033

UNCLASSIFIED//FOUO

In conclusion, ECOU 1 suggests there is currently no cyber intrusion component in this case and that the report provided contains questionable methods and intentions. [REDACTED]

[REDACTED] it appears suspicious that the presumed suspicious activity began approximately three weeks prior to the stated start of the investigation conducted by the researcher.

Finally, it appears abnormal that a presidential candidate, who wanted to conduct secret correspondence with the Russian government (or a Russian bank), would (1) name his secret server "mail1.trump-email.com", (2) use a domain (trump-email.com) registered to his own organization, and then (3) communicate directly to the Russian bank's IP address (as opposed to using TOR or proxy servers). ECOU 1 also assesses Russian state-sponsored technical sophistication to exceed the OpsSec of that suggested in the report.

UNCLASSIFIED//FOUO

FBI-DWS-12-0018095

SCO-016972
SCO-3500U-010034