From:	SANDS, ALLISON (CG) (FBI) <ASANDS@fbi.sgov.gov>
Sent:	Wednesday, October 5, 2016 5:07 PM
To:	SANDS, ALLISON (CG) (FBI) <ASANDS@fbi.sgov.gov>; MARIC, PAUL M. (CD) (FBI) <PMMARIC@fbi.sgov.gov>; PIENTKA, JOE (WF) (FBI) <JPIENTKA@fbi.sgov.gov>; AUTEN, BRIAN J. (CD) (FBI) <BJAUTEN@fbi.sgov.gov>; STOFER, JOHN F. (CD) (FBI) <JFSTOFER@fbi.sgov.gov>; GAYNOR, RYAN C. (CD) (FBI) <RCGAYNOR@fbi.sgov.gov>
Cc:	WIERZBICKI, DANIEL S. (CG) (FBI) <DSWIERZBICKI@fbi.sgov.gov>; HEIDE, CURTIS A. (CG) (FBI) <CAHEIDE@fbi.sgov.gov>
Subject:	Status update on ALFA BANK case --- [redacted]

[redacted]: [redacted]/[redacted]

Classified By: C00B95Q73
Derived From: FBI NSIC dated 20130301
Declassify On: 20411231
==========

[redacted]

Good afternoon,

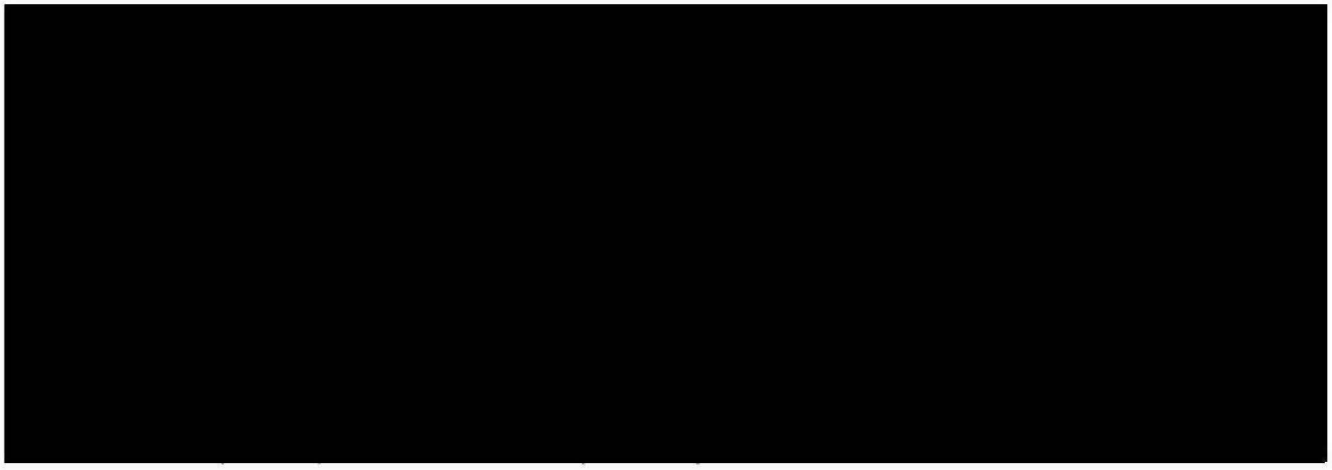
We have several important updates this afternoon and I want to be sure everyone is on the same page.

- We spoke to a CHS in [redacted] who said he was contacted by David Dagon at Georgia Tech to provide technical analysis on the white paper. [redacted]. He believed that the white paper was credible, and was going to share that assessment this afternoon to the Washington Post. Prior to his interview with the Washington Post, he was speaking to representatives of the Trump Organization who wanted to "explain their side of the story." [redacted] claims of suspicious activity have already been debunked by our analysis of the logs from Central Dynamics and [redacted] Other claims of suspicious activity were in fact the result of investigative activity taken by the FBI and by Alfa Bank:

  - *1. CHS assessed it was suspicious that the mail1.trump-email.com domain was taken down after the white paper came out.* This occurred because the FBI alerted Central Dynamics that they were still hosting the mail1.trump-email.com domain on their DNS tables. Because they had already turned ownership of this domain to Trump Organization via GoDaddy several years ago, they updated their DNS tables to correct the oversight. This is why the suspect domain "disappeared."

  - 2. *CHS also claimed that a "new" hostname— trump1.contact-client.com—was then created, and that Alfa Bank was the first IP address to ping on that new host name.* We believe this is not a new hostname

and that Alfa Bank pinged it during their internal research in response to the whitepaper



- The aforementioned CHS, as well as David Dagan, are expected to directly contradict FBI assessments and will report that there is credible evidence of covert communications between Trump email servers and Alfa bank. Their assessments do not change ours, but pose a challenge in refuting their claims using only open source information.

- We are analyzing logs provided by Central Dynamics. So far, these logs do not show any evidence of the covert channel mentioned in the white paper. Central Dynamics provided all of the firewall logs affiliated with the 4 Alfa Bank IP addresses of interest, and in no instance is there any record of any of those IP addresses communicating with the mail1.trump-email.com IP address.

- Server logs from Listrak, the ISP that hosts the domain, are forthcoming, and should offer definitive evidence of the nature of any activity between Alfa Bank DNS servers and any email domains associated with IP address 66.216.133.29. We have also reached out to the agent in Miami to obtain more specific logs on this particular IP address, to be sure we aren't missing anything captured in the firewall logs already provided.

- We are going to speak to David Dagon, and see if he has any new information for us.

- The CHS believes the article will be published in the Washington Post and New York Times on Sunday.

As always, I am happy to answer any questions and will continue to keep you updated as things develop.

Best,

Special Agent Allison Sands

Chicago Division/ CY-1
desk: 312-829-8628

mobile: 312-965-5872

From: SANDS, ALLISON (CG) (FBI)
Sent: Monday, September 26, 2016 5:20 PM

To: MARIC, PAUL M. (CD) (FBI); PIENTKA, JOE (WF) (FBI); AUTEN, BRIAN J. (CD) (FBI); STOFER, JOHN F. (CD) (FBI); GAYNOR, RYAN C. (CD) (FBI)
Cc: WIERZBICKI, DANIEL S. (CG) (FBI); HEIDE, CURTIS A. (CG) (FBI)
Subject: Status update on ALFA BANK case ---[redacted]

Classification: [redacted]

Classified By: C00B95Q73
Derived From: FBI NSIC dated 20130301
Declassify On: 20411231
==========

Good afternoon,

We have several updates on the ALFA BANK case to pass along:

- The agent in Miami who has been working with Central Dynamics received an email from an executive at Central Dynamics stating that they checked the servers for the last 30 days, and the only IP they detected hitting the server was 167.73.11.8. This is the IP address mentioned in the white paper that resolves to SPECTRUM HEALTH. It is unclear at this time what kind of communication was this "hit" is referring to. We are still waiting on the server logs to conduct our own forensic investigation of any network activity on this domain.

- NSLs are in draft and will soon be available for delivery to LISTRAK, the ISP that hosts the trump-email.com domain, and GoDaddy.com. We will seek to obtain any logs available on the LISTRAK server that relate to the trump-email.com domain, and subscriber data, any domains and subdomains affiliated with subscriber, IP logs, and billing information on trump-email.com domain from GoDaddy.com

[redacted]

- Open source research on the current and historical lists of Tor exit nodes published by the Tor Project (torporject.org) covering the time period of May 4 2016 - Sept 4 2016, revealed no matches to the SPECTRUM HEALTH IP (167.73.110.8). Normally, a Tor exit node would appear in this list if it were active during the reviewed time period. Under normal conditions, the historical data used for searching is captured at a rate of once per hour, every hour, every day. This is further evidence that the white paper's claim about SPECTRUM HEALTH being an exit node – exclusive for ALFA BANK or otherwise -- is not supported by technical analysis. As far as we know, there is no way to create an exclusive TOR exit node- doing so would by default decrease the anonymity of the Tor user. Further, in addition to being a technically questionable practice, the use of Tor networks in general is inconsistent with Russia's TTPs for obfuscating its network activities.

As always, I'm happy to answer any questions.

Best,

Special Agent Allison Sands

Chicago Division/ CY-1
desk: 312-829-8628

mobile: 312-965-5872

From: SANDS, ALLISON (CG) (FBI)
Sent: Friday, September 23, 2016 1:53 PM
To: SANDS, ALLISON (CG) (FBI); MARIC, PAUL M. (CD) (FBI); PIENTKA, JOE (WF) (FBI); AUTEN, BRIAN J. (CD) (FBI); STOFER, JOHN F. (CD) (FBI)
Cc: WIERZBICKI, DANIEL S. (CG) (FBI); HEIDE, CURTIS A. (CG) (FBI)
Subject: Status update on ALFA BANK case ---[redacted]

Classification: [redacted]

Classified By: C00B95Q73
Derived From: FBI NSIC dated 20130301
Declassify On: 20411231
==========

Good afternoon,

Miami followed up this morning with Central Dynamics who confirmed that the mail1.trump-email.com domain is an old domain that was set up in approximately 2009 when they were doing business with Trump Organization that was never used. They released the domain via GoDaddy to the Trump Organization over a year ago; however, the DNS tables were not updated and that domain still pointed to Central Dynamics servers. As of this afternoon, a WHOIS look-up revealed that the mail1.trump-email.com no longer resolves to Central Dynamics, indicating they likely updated their DNS tables after the FBI informed them of the oversight. This email domain is no longer pointing to any active mail server.

Central Dynamics provided reviewed a picture of a Barracuda (spam filter) service connected to server [trump-email.com]. The information displayed by the Barracuda spam filter for trump-email.com indicates that during an unspecified time period, 15 inbound emails were received, 1 was allowed to pass through the filter, and 1 outbound email was marked as spam and blocked. The information provided only reflects email smtp traffic, and we have requested that Miami obtain logs for the email server on which the domain was residing to identify whether or not there was any other traffic (non-smtp) that indicates malware or another ALFA BANK traffic (including the alleged DNS queries) residing on the server.

[redacted]

Respectfully,

Allison Sands

From: SANDS, ALLISON (CG) (FBI)
Sent: Thursday, September 22, 2016 4:53 PM
To: MARIC, PAUL M. (CD) (FBI); PIENTKA, JOE (WF) (FBI); AUTEN, BRIAN J. (CD) (FBI); STOFER, JOHN F. (CD) (FBI)

Cc: WIERZBICKI, DANIEL S. (CG) (FBI); HEIDE, CURTIS A. (CG) (FBI)
Subject: RE: Status update on ALFA BANK case --- [redacted]

Classification: [redacted]

Classified By: C00B95Q73
Derived From: FBI NSIC dated 20130301
Declassify On: 20411231
==========

Miami made contact with Central Dynamics, who confirmed that trump-email.com is a legitimate mail server that is used by Trump Hotels. Agent spoke to an executive at Central Dynamics, who agreed to cooperate with the FBI and will provide logs as requested. Agent will return to Central Dynamics tomorrow morning to meet with the technology support staff. We will provide Central Dynamics with the three IP addresses of specific interest for ALFA BANK and SPECTRUM HEALTH and specifically request for any logs related to that network traffic. Central Dynamics also provides email support for Trump.com, but moved the trump.com email servers to another server due to the high frequency of malicious attacks to those accounts.

Best,

Special Agent Allison Sands

Chicago Division/ CY-1
desk: 312-829-8628

mobile: 312-965-5872

From: SANDS, ALLISON (CG) (FBI)
Sent: Thursday, September 22, 2016 4:22 PM
To: PIENTKA, JOE (WF) (FBI); AUTEN, BRIAN J. (CD) (FBI); STOFER, JOHN F. (CD) (FBI); MARIC, PAUL M. (CD) (FBI)
Cc: WIERZBICKI, DANIEL S. (CG) (FBI); HEIDE, CURTIS A. (CG) (FBI)
Subject: Status update on ALFA BANK case --- [redacted]

Classification: [redacted]

Classified By: C00B95Q73
Derived From: FBI NSIC dated 20130301
Declassify On: 20261231
==========

Good afternoon,

As of 1500 today 9/22/16, CG CY-1 have conducted the following investigation actions in support of the forthcoming case on ALFA BANK:

- FBI CG CY-1 submitted an EC to open a full investigation - pending ASAC and SAC approval
- CY-1 Computer scientists extracted files from source thumb drive for future analysis on OPWAN.
- Case agents coordinated with Cyber Division (POC Scott Hellman) to examine technical inconsistencies in the white papers methodologies and conclusions. Overall, ECOU assesses that the claims put

forth in the white paper are invalid. Some key points:

- There is no network traffic between the ALFA BANK and the trump-email.com domains, only DNS queries;

- There is no evidence to support that the suspect email is currently tied to the TRUMP ORGANIZATION- the details of the registration do not match any of the legitimate TRUMP ORGANIZATION mail servers;

- An error message on port 25 does not indicate that the server is set up specifically to only communicate to designated IP addresses; and

- A "secret" communications portal is unlikely to have "email" or "trump" in the domain name and would unlikely communicate directly to ALFA ABNK's IP address.

- There is a lack of supporting evidence tying the ALFA BANK to the SPECTRUM HEALTH DNS queries.

- Case agents researched the legitimate mail servers affiliated with trump.com, and mail1.trump-email.com is not among them. Trump.com appears to be protected by a anti-DDOS service called CLOUDFARE in San Francisco, where trump-email.com does not.

- Research on the trump-email.com domain, the parent domain to the suspect mail1.trump-email.com, revealed that the domain is registered to Central Dynamics Corporation, Boca Raton, FL. According to open source, Central Dynamics provides IT services to the Hotel industry that did some marketing for the Trump Organization in approximately 2007-2009 (the mail1.trump-email.com domains was created in August 2009). Case agents cut a lead to Miami (POC SSA Jason Manar) to contact Central Dynamics to gather information about the **trump-email.com domain** using a ruse that the FBI is contacting them to see if this is a legitimate email account and not a spoof email account having the potential to send spear-phishing or other cyber criminal threats, and Highlight that the Registrant Organization was listed as ***Trump Orgainzation*** [sic] which could be an indication of malicious intent. Requested server logs if possible.

- A WHOIS search revealed that the suspect email domain is being hosted on a Listrak server in Litiz, PA. Case agents contacted Philadelphia (POC SA Joshua Hubiak) and put Harriburg RA on standby to contact Listrak to gather any information possible about the trump-email.com domain. Philadelphia will wait to approach Listrak pending the outcome of the conversation with Central Dynamics. (NSL will be issued tomorrow if warranted)

- IP addresses associated with the suspect email domain mail1.trump-email.com (IP address 66.216.133.29) and SPECTRUM HEALTH, the suspected TOR exit node (IP address 167.73.110.8) were run through [redacted] records (POC David Garn). Results are as follows:

[redacted]

[redacted]

Respectfully,

Special Agent Allison Sands

Chicago Division/ CY-1
desk: 312-829-8628

mobile: 312-965-5872

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

==========
Classification: [redacted]

FBI-DWS-01-0001910
SCO_FBIPROD_006382

SCO-008674