TWO (THREE) POSSIBILITIES ON THE "WIKILEAKS" ARCHIVE STORY

Don Jr's testimony to Congress yesterday has brought out several new details on the evidence he was provided. In this post I want to look at the report that someone sent key Trump figures a link to a Wikileaks archive and an encryption key.

> Candidate Donald Trump, his son Donald Trump Jr. and others in the Trump Organization received an email in September 2016 offering a decryption key and website address for hacked WikiLeaks documents, according to an email provided to congressional investigators.
>
> The September 14 email was sent during the final stretch of the 2016 presidential race.
>
> CNN originally reported the email was released September 4 — 10 days earlier — based on accounts from two sources who had seen the email. The new details appear to show that the sender was relying on publicly available information. The new information indicates that the communication is less significant than CNN initially reported.
>
> After this story was published, The Washington Post obtained a copy of the email Friday afternoon and reported that the email urged Trump and his campaign to download archives that WikiLeaks had made public a day earlier. The story suggested that the individual may simply have been trying to flag the campaign to already public documents.
>
> CNN has now obtained a copy of the

> email, which lists September 14 as the date sent and contains a decryption key that matches what WikiLeaks had tweeted out the day before.

First, note there's no explanation in the story why these are described as Wikileaks emails, aside from the fact that Julian Assange has on occasion posted archives with a key. Indeed, it sounds like this archive is more closely related to the DC Leaks side of the house, given the reference to Colin Powell emails in the larger story. So absent a more fulsome explanation of what makes these WikiLeaks documents, I wouldn't necessarily bet that these documents are related to Wikileaks.

Second, one possible explanation for this archive is that it's the same one that is the center of the skeptics' theory. They focus on an archive called NGP/VAN (but which is not NGP/VAN), which was curated on September 1. In public form, the archive was pointed to by Guccifer 2.0 on September 12, but never posted on his site.

> the files were posted during a speech given in London by another hacker as a proxy for G2.0 on that day. The Forensicator relies on a copy posted by NatSecGeek. And while on Twitter G2.0 pointed to the speech the day before it was given, he never actually pointed back to the data on his WordPress site.
>
> It's true that the "speech" that was read for G2.0 relied on and posted a link to these files at the conference.
>
> > *This scheme shows how NGP VAN is incorporated in the DNC infrastructure. It's for detailed examination, if you are interested. And here are a couple of NGP VAN's documents from their network. If you r*

> > *interested in their internal documents, you can have them via the link on the screen. The password is usual. It's also on the screen. You may also ask the conference producers for them later.*
>
> But at the very least, it seems any analysis of these forensics needs to account for the hand-off and proxy involved.

The timing of this would suggest that (if this is the same archive) three days after the archive was curated but over a week before it was posted publicly, top campaign officials got a link.

But there is another possibility, a detail I've often alluded to but never laid out publicly. There is or was a grand jury investigation into some script kiddies that tried to hijack Guccifer 2.0's password or ID or something like that. It is or was in Philadelphia, based on the location of an archive involved. As I understand it the thought was that this effort was unrelated to the chief Russian info op, but was a lead the FBI had to chase down. I've been waiting to see if that grand jury investigation was ever going to show up publicly, and it's one possible explanation for this email.

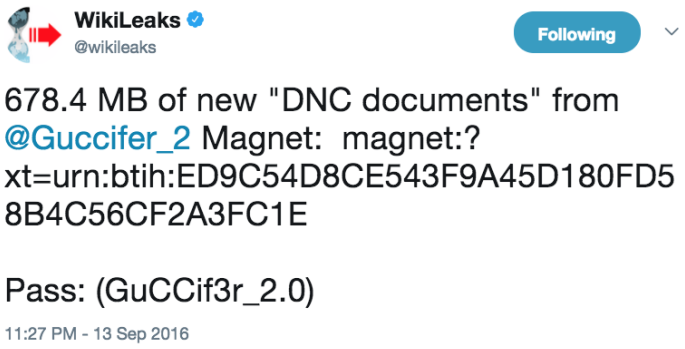
Update: I should make clear, I lay out three possibilities here:

1. These are actually DC Leaks emails, not WikiLeaks ones; this is consistent with what recipients of those emails say about timing.
2. This is the NGP/VAN archive released in mid-September, associated with Guccifer

2.0.

3. This is an effort from the unknown skiddies being investigated in Philly.

Update: By description, WaPo makes it clear that this was an email sending the Trumps to this material, though using a different link and password.



That means it is, in fact, the NGP/VAN materials at the heart of the skeptics' counterarguments about Guccifer being Russian (number 2, above), being sent under an apparently Anglo name (albeit with a few errors; making number 3 possible), but branded as Guccifer 2.0 materials, not WikiLeaks materials (sort of, 1).

In other words, the emails are much more interesting for all these other related theories than for the fact that the Trump folks received it, apparently unsolicited.

Update: I've subbed in the corrected language from CNN confirming that this was a September 14 email.