THE FBI DOWNLOADED CIA'S HACKING TOOLS USING STARBUCK'S WIFI

One of the most interesting details from the yesterday's Joshua Schulte trial involved how the FBI obtained the Vault 7 and Vault 8 materials they entered into evidence yesterday. Because the FBI did not want to download the files onto an existing FBI computer (in part, out of malware concerns) and because they didn't want to use an FBI IP address, they got a new computer and downloaded all the files at Starbucks.

> Q. What were some of the parts of that plan?
>
> A. So, one of the parts would be to obtain a separate computer that wasn't connected, that wasn't a previous government computer or connected to our network.
>
> Another component was to just use public wi-fi and not a government-attributable internet connection. And the third part would be to find the best way to store this unique piece of evidence in the best way possible.
>
> Q. Let's talk about each of those steps. I think you said that you got a nongovernment computer, is that correct?
>
> A. Correct.
>
> Q. Why is that?
>
> A. Just so that when we entered it into evidence, we wouldn't be taking something from the network and essentially putting it aside indefinitely. And then also, we did not want to download information from the internet, which could potentially contain viruses or malware, to an FBI

system.

Q. Do you have an understanding of what was contained within the disclosures made by WikiLeaks?

A. I do.

Q. And what is that information?

A. They were information about CIA hacking tools and cyber-exploitation tools.

Q. What, if any, impact did that have on your decision to use a nongovernment computer?

A. Anytime you download something from the internet, you take a risk. And then given what type of information we were going to acquire, we wanted to take an extra — many extra steps of security to maintain the integrity of our systems as well as be able to get the information and then store it properly.

Q. I think the second part of the plan was using public space to download the leak. Is that correct?

A. Correct.

Q. Why didn't you download the leak from an FBI facility?

A. So, anytime actions on the internet are traceable as well as downloads, and we didn't want to use an FBI system. And given the type of information we were going to acquire, we didn't want to use an FBI system to download the information which could then be traced back to us and potentially implicate the IP address and potentially other investigations.

Q. And why would that be problematic for the FBI?

A. So, anytime actions on the internet

> are traceable as well as downloads, and we didn't want to use an FBI system. And given the type of information we were going to acquire, we didn't want to use an FBI system to download the information which could then be traced back to us and potentially implicate the IP address and potentially other investigations.
>
> Q. And why would that be problematic for the FBI?

The explanation is interesting for more than the seeming validation of Starbuck's WiFi quality.

It's also interesting given details of timing and download method.

> Q. When did you first go to Starbucks to download the leak?
>
> A. In March of 2018.
>
> Q. And how did you download the leak once you were there?
>
> A. I went to the – used an internet browser, went to the WikiLeaks website first. Didn't really see a quick way to download all the – the large volume of information, so WikiLeaks had also provided a torrent website, which is essentially just – it was about 15 hyperlinks that connected to zip files to download the bulk of the information that they released.
>
> Q. What is a torrent website?
>
> A. It's a – it looked – just a blank website, but it had 15 hyperlinks, and each time you clicked on one of the links, it asked if you wanted to save the associated zip file. And then I saw there were 15 of those, and then I just downloaded it that way.
>
> Q. And what is a zip file?

A. Zip file is just a way to compress information. So if you want to send a ton of files over an email or kind of website to website, you can use software to compress that information in a more easily storable format.

Q. Why did you go to the torrent instead of downloading it directly from the website?

A. I did – I tried – I perused the website for a little and didn't see – given the volume of the information, there wasn't, to my appearance, a good way to capture all of it. And I knew of this – from our investigation I knew of this torrent address, which had been provided by WikiLeaks too, if you wanted to essentially bulk download all the information.

Q. Did you download those zip files to the computer?

A. I did.

Q. And were you able to unzip those zip files?

A. I was.

Q. Were you able to download any of WikiLeaks's public statements on that computer?

A. I was.

Q. And how did you do that?

A. Via screenshots.

Q. And you said you downloaded the zip files to the computer?

A. Correct.

Q. How long did that downloading process take?

A. Around an hour.

> Q. And approximately how much data was found on those zip files?
>
> A. Approximately 1.4 gigabytes.

One thing this does is explain that it took an hour to download just what got published on WikiLeaks. This will become a critical detail in proving that the files had to have been stolen from inside CIA — basically the "download speed" argument thrown back at the Russian hack denialists.

By revealing that that amounted to just 1.4GB of material, prosecutors have revealed that what WikiLeaks published was just a fraction of the 1TB of material that, per his contemporaneous Google searches, Schulte stole.

The other thing this description reveals is that WikiLeaks did not include Vault 8, the one case (beyond Marble, the obfuscation tool Schulte wrote) where they published source code, in their Torrent download of the files.

> Q. Did there come a time when you went back to Starbucks to download additional materials?
>
> A. I did.
>
> Q. Approximately when did that happen?
>
> A. In May of 2018.
>
> Q. And why did you go back to download additional materials?
>
> A. Through the investigation, we determined that the zip files which I had downloaded contained Vault 7, but it did not contain the Vault 8 release, and we wanted to capture the entirety of what WikiLeaks had put out there from March 2017 to November of 2017.
>
> Q. Were you able to download Vault 8 when you went back?

> A. I was.
>
> Q. How did you do that?
>
> A. So, it was a lot less information. I was able to just go to the release that WikiLeaks specified as Vault 8 and download the singular files in that way. It's just — it's a kind of like right click, save as.
>
> Q. And did you download the Vault 8 leak on the same computer that you downloaded the Vault 7 leaks?

I'm not sure why WikiLeaks wouldn't include Vault 8, but I find the decision very curious.

Finally, this story is really interesting from an investigative standpoint. The FBI didn't download the files they were going to enter into evidence in this trial until March and May of 2018, a year after the leak and a year after they identified Schulte as the leaker. Someone — possibly the CIA, which started to investigate the leak even before the first dump — had done a forensic comparison of the first release within days after the leak. The FBI had access to that.

But they went back a year later and prepared the evidence for that trial.

During the entire period of the Schulte prosecution, prosecutors made it clear the case *may* involve classified information (so his attorneys needed to be able to get clearance). Starting in January 2018, they made clear the leak would be charged.

But — particularly given the child porn charges he faces would have the same kind of prison sentence that the Espionage charges against him will — they could have forgone the trial (I had heard discussion that just the porn would be charged, so it's possible that was the initial plan). Yes, they want to make an example of him, but the CIA has had to declassify an unbelievable amount of sensitive information to put Schulte on trial. Plus, the cost for

prosecuting this crime is enormous. So I wonder whether they didn’t make the final decision to do this prosecution until 2018.

If so, that would parallel the timing of the Julian Assange prosecution in interesting ways. He was charged in December 2017, then indicted in March 2018, literally the same month that FBI obtained the Vault 7 files to enter into evidence.