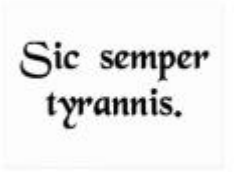
WHY THE DNC WAS NOT HACKED BY THE RUSSIANS by Binney and Johnson



By

William Binney, former Technical Director NSA

Larry Johnson, former State CT and CIA

https://turcopolier.typepad.com/sic_semper_tyrannis/2019/02/why-the-dnc-was-not-hacked-by-the-russians.html#more

The FBI, CIA and NSA claim that the DNC emails published by WIKILEAKS on July 22, 2016 were obtained via a Russian hack, but more than three years after the alleged "hack" no forensic evidence has been produced to support that claim. In fact, the available forensic evidence contradicts the official account that blames the leak of the DNC emails on a Russian internet "intrusion". The existing evidence supports an alternative explanation--the files taken from the DNC between 23 and 25May 2016 and were copied onto a file storage device, such as a thumb drive.

If the Russians actually had conducted an internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. The NSA had an opportunity to make it clear that there was irrefutable proof of Russian meddling, particularly with regard to the DNC hack, when it signed on to the January 2017 "Intelligence Community Assessment," regarding Russian interference in the 2016 Presidential election:

- We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; **NSA has moderate confidence.**

The phrase, "moderate confidence" is intelligence speak for "we have no hard evidence." Thanks to the leaks by Edward Snowden, we know with certainty that the NSA had the capability to examine and analyze the DNC emails. NSA routinely "vacuumed up" email traffic transiting the U.S. using robust collection systems (whether or not anyone in the NSA chose to look for this data is another question). If those emails had been hijacked over the internet then NSA also would have been able to track the electronic path they traveled over the internet. This kind of data would allow the NSA to declare without reservation or caveat that the Russians were guilty. The NSA could admit to such a fact in an unclassified assessment without compromising sources and methods. Instead, the NSA only claimed to have moderate confidence in the judgement regarding Russian meddling. If the NSA had hard intelligence to support the judgement the conclusion would have been stated as "full confidence."

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed--which accuses 12 Russian GRU military personnel and an entity identified as,

Guccifer 2.0, for the DNC hack—because the available forensic evidence indicates the emails were copied onto a storage device.

According to a DOJ press release on the indictment of the Russians, Mueller declares that the emails were obtained via a "spearphising" attack:
In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. **They also were able to hack**into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) **through these spearphishing techniques to steal emails and documents,**covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to these networks.

The officials in Unit 26165 coordinated with officials in Unit 74455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hacktivists" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2016 between 4:19PM and 4:56PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.(https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election)

Notwithstanding the DOJ press release, an examination of the Wikileaks DNC files do not support the claim that the emails were obtained via spearphising. Instead, the evidence clearly shows that the emails posted on the Wikileaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at Wikileaks. The emails posted on Wikileaks were saved using the File Allocation Table (aka FAT) computer file system architecture.

An examination of the Wikileaks DNC files shows they were created on 23, 25 and 26 May respectively. The fact that they appear in a FAT system format indicates the data was transfered to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the Wikileaks files. Every single one of these time stamps end in even numbers. If you are not familiar with the FAT file system, you need to understand that when a date is stored under this system the data rounds the time to the nearest even numbered second.

We have examined 500 DNC email files stored on Wikileaks and all 500 files end in an even number—2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

The DNC emails are in 3 batches (times are GMT).

Date	Count	Min Time	Max Time	FAT	Min Id	Max Id
2016-05-23	10520	02:12:38	02:45:42	x	3800	14319
2016-05-25	11936	05:21:30	06:04:36	x	1	22456
2016-08-26	13357	14:11:36	20:06:04	x	22457	44053

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power - in other words, an infinitely high order.

This data alone does not prove that the emails were copied at the DNC headquarters. But it does show that the data/emails posted by Wikileaks did go through a storage device, like a thumbdrive, before Wikileaks posted the emails on the World Wide Web.

This fact alone is enough to raise reasonable doubts about Mueller's indictment accusing 12 Russian soldiers as the culprits for the leak of the DNC emails to Wikileaks. A savvy defense attorney will argue, and rightly so, that someone copied the DNC files to a storage device (Eg., USB thumb drive) and transferred that to Wikileaks.

We also tested the hypothesis that Wikileaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Larter file) that was released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If Wikileaks employed a standard protocol for handling data/emails received from unknown sources we should expect the File structure of the DNC emails to match the file structure of the Podesta emails. The evidence shows otherwise.

There is further compelling technical evidence that undermines the claim that the DNC emails were downloaded over the internet as a result of a spearphising attack. Bill Binney, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the internet as a result of a spearphising attack. It is a simple matter of mathematics and physics.

Shortly after Wikileaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claimimg that "he" hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as proof that "he" had hacked from the DNC.
Taking Guccifer 2.0 at face value—i.e., that his documents were obtained via an internet attack—Bill Binney conducted a forensic examination of the metadata contained in the posted documents based on internet connection speeds in the United States. This analysis showed that the highest transfer rate was 49.1 megabytes per second, which is much faster than possible from a remote online connection. The 49.1 megabytes speed coincides with **the download rate for a thumb drive**.

Binney, assisted by other colleagues with technical expertise, extended the examination and ran various tests forensic from the Netherlands, Albania, Belgrade and the UK. The fastest rate obtained -- from a data center in New Jersey to a data center in the UK--was 12 megabytes per second, which is less than a fourth of the rate necessary to transfer the data, as it was listed from Guccifer 2.
The findings from the examination of the Guccifer 2.0 data and the Wikileaks data does not prove who copied the information to a thumbdrive, but it does provide and empirical alternative explanation that undermines the Special Counsel's claim that the DNC was hacked. According to the forensic

evidence for the Guccifer 2.0 data, the DNC emails were not taken by an internet spearphising attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret information leaked by Edward Snowden. If the DNC emails had been hacked via spearphising (as alleged by Mueller) then the data would have been captured by the NSA by means of the Upstream program (Fairview, Stormbrew, Blarney, Oakstar) and the forensic evidence would not modify times - the data would be presented as sent.

Second, we have the public reporting on the DNC and Crowdstrike, which provide a bizarre timeline for the alleged Russian hacking.

It was 29 April 2016, when the DNC claims it became aware its servers had been penetrated (see https://medium.com/homefront-rising/dumbstruck-how-crowdstrike-conned-america-on-the-hack-of-the-dnc-ecfa522ff44f). No claim yet about who was responsible.

According to CrowdStrike founder, Dimitri Alperovitch, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A CrowdStrike intelligence analyst reportedly told Alperovitch that:
Falcon had identified not one but two Russian intruders: Cozy Bear, a group CrowdStrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

(https://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/)

And what did CrowdStrike do about this? Nothing. According to Michael Isikoff, CrowdStrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been “discovered.” This is nonsense. If a security company detected a thief breaking into a house and stealing its contents, what sane company would counsel the client to do nothing in order to avoid alerting the thief?

We know from examining the Wikileaks data that the last message copied from the DNC network is dated Wed, 25 May 2016 08:48:35. No DNC emails were taken and released to Wikileaks after that date.

CrowdStrike waited until 10 June 2016 to take concrete steps to clean up the DNC network. Alperovitch told Esquire’s Vicky Ward that:
Ultimately, the teams decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office.

https://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/
Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumbdrive. But the culprit had not yet been identified. We know one thing for certain—CrowdStrike did not take steps to shutdown and repair the DNC network until 18 days after the last email was copied from the server.

The final curiosity is that the DNC never provided the FBI access to its servers in order for qualified FBI technicians to conduct a thorough forensic examination. If this had been a genuine internet hack, it would be very easy for the NSA to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that has not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates persons within our law enforcement and intelligence community taking part in a campaign of misinformation, deceit and incompetence. It is not a pretty picture.