# THE UNIVERSE OF HACKED AND LEAKED EMAILS FROM 2016: DNC EMAILS

When Mueller's team released George Papadopoulos' plea deal last year, I noted that the initial denials that Papadopoulos had advance warning of the emails the Russians were preparing to hack and leak did not account for the entire universe of emails known to have been stolen. A year and several Mueller indictments later, we still don't have a complete understanding of what emails were being dealt when. Because that lack of understanding hinders understanding what Mueller might be doing with Roger Stone, I wanted to lay out what we know about four sets of emails. This series will include posts on the following:

- DNC emails
- Podesta emails
- DCCC emails
- Emails Hillary deleted from her server

The series won't, however, account for two more sets of emails, anything APT 29 stole when hacking the White House and State Department in 2015, or anything released via the several FOIAs of the Hillary emails turned over to the State Department from her home server. It also won't deal with the following:

- Emails from two Hillary staffers who had their emails released via dcleaks
- The emails of other people released by dcleaks, which includes Colin Powell, some Republican party officials

(including some 2015 emails Peter Smith sent to the IL Republican party), and others with interests in Ukraine
- A copy of the Democrats' analytics program copied on AWS
- The NGP/VAN file, which was not directly released by Guccifer 2.0, but is central to one of the skeptics' theories about an alternative source other than Russia

## DNC Emails

The "DNC emails" are generally thought of as the 44,000 emails WikiLeaks released on July 22, 2016. The GRU indictment describes the theft and conveyance of those emails this way:

> Between on or about May 25, 2016 and June 1, 2016, the Conspirators hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees. During that time, YERMAKOV researched PowerShell commands related to accessing and managing the Microsoft Exchange Server.
>
> [snip]
>
> On or about June 22, 2016, Organization 1 sent a private message to Guccifer 2.0 to "[s]end any new material [stolen from the DNC] here for us to review and it will have a much higher impact than what you are doing." On or about July 6, 2016, Organization 1 added, "if you have anything hillary related we want it in the next tweo [sic] days prefable [sic]

> because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after." The Conspirators responded, "ok . . . i see." Organization 1 explained, "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting."
>
> After failed attempts to transfer the stolen documents starting in late June 2016, on or about July 14, 2016, the Conspirators, posing as Guccifer 2.0, sent Organization 1 an email with an attachment titled "wk dnc link1.txt.gpg." The Conspirators explained to Organization 1 that the encrypted file contained instructions on how to access an online archive of stolen DNC documents. On or about July 18, 2016, Organization 1 confirmed it had "the 1Gb or so archive" and would make a release of the stolen documents "this week."
>
> On or about July 22, 2016, Organization 1 released over 20,000 emails and other documents stolen from the DNC network by the Conspirators. This release occurred approximately three days before the start of the Democratic National Convention. Organization 1 did not disclose Guccifer 2.0's role in providing them. The latest-in-time email released through Organization 1 was dated on or about May 25, 2016, approximately the same day the Conspirators hacked the DNC Microsoft Exchange Server.

Raffi Khatchadourian (who has done as much work as anyone else on the known universe of emails) noted that by the time the July 14 exchange had happened, Julian Assange had already said he had emails and Guccifer 2.0 had already said he had shared them with WikiLeaks.

> On June 12th, three days before the creation of Guccifer 2.0, Assange announced that he had a substantial trove of Clinton-related e-mails that were pending publication. Likewise, Guccifer 2.0 proclaimed, on its very first post on the WordPress site, “The main part of the papers, thousands of files and mails, I gave to Wikileaks. They will publish them soon.” Again and again, the G.R.U. officers tried to drive home this point—which, of course, was evidently the main point of creating the persona. “I sent a big part of docs to WikiLeaks,” Guccifer 2.0 told the editor of the Smoking Gun that same day. On June 17th, Guccifer 2.0 said in another e-mail, “I gave WikiLeaks the greater part of the files.” (For e-mail, the G.R.U. gave Guccifer 2.0 another fake identity: Stephan Orphan.)
>
> In other words, both the G.R.U. and Assange appear to have confessed to the transmission and reception of a large trove of Clinton-related e-mails in mid-June, before Guccifer 2.0 was apparently created. The indictment does not address this. There is no way to say precisely what that trove was—if it was the Podesta archive given to WikiLeaks much earlier than is generally presumed, or the D.N.C. e-mails, or both, or something else. (There is also the possibility that both parties were not speaking truthfully.) But, if Assange did have the D.N.C. e-mails before Guccifer 2.0 was created, then the details in the indictment take on new meaning. Some version of the following may be true: it is mid-June, with the convention approaching, and Assange is about to release a bombshell, when he notices the sudden appearance of Guccifer 2.0, a “hacker” edging into his turf, inviting journalists to write in. So he writes in, asking for material

> that interests him. He has already gone through the D.N.C. e-mails and has recognized that the trove highlights conflict within the Democratic Party. He signals that he wants more on that specific issue. The G.R.U. is happy to comply, through its new cutout. Perhaps some of it overlaps with what the G.R.U. already provided, making Guccifer 2.0's confessions literally accurate. Perhaps it is the same irrelevant dross that Guccifer 2.0 fed to others.
>
> Last year, I visited Assange several times in the Ecuadorian Embassy in London. He often emphasized to me that the sourcing of his election publications was complex. I usually took this as a dodge. But the sourcing may indeed have been multilayered. There are many conceivable ways that G.R.U. officers could have provided e-mails to WikiLeaks before they created Guccifer 2.0. They could have used the WikiLeaks anonymous-submission system. They could have used a different fictitious online persona. They could have used a human intermediary. Last year, James Clapper told me, "It was done by a cutout, which of course afforded Assange plausible deniability." In January, 2017, Clapper oversaw a formal intelligence assessment on Russian meddling. At the time, more than one news organization reported that a classified version of the assessment made clear that the intermediaries between the G.R.U. and WikiLeaks were already known. (Certainly, the intelligence community would also have been in possession of Guccifer 2.0's Twitter D.M.s at that time, too.) One intelligence official, describing the report, indicated to Reuters last year that the e-mails relayed to WikiLeaks had followed a "circuitous route," by a series of handoffs, on their journey from Moscow. Such a scenario seems to be

> at odds with the idea that Guccifer 2.0 merely sent WikiLeaks an encrypted link to download it all in one swoop.

An earlier Khatchadourian piece describes WikiLeaks experiencing some pressure to publish before the convention.

> In early July, for example, Guccifer 2.0 told a Washington journalist that WikiLeaks was “playing for time.” There was no public evidence for this, but from the inside it was clear that WikiLeaks was overwhelmed. In addition to the D.N.C. archive, Assange had received e-mails from the leading political party in Turkey, which had recently experienced a coup, and he felt that he needed to rush them out. Meanwhile, a WikiLeaks team was scrambling to prepare the D.N.C. material. (A WikiLeaks staffer told me that they worked so fast that they lost track of some of the e-mails, which they quietly released later in the year.) On several occasions, and in different contexts, Assange admitted to me that he was pressed for time. “We were quite concerned about meeting the deadline,” he told me once, referring to the Democratic National Convention.
>
> His original release date for the D.N.C. archive, he explained, was July 18th, the Monday before the Convention; his team missed the deadline by four days. “We were only ready Friday,” he said. “We had these hiccups that delayed us, and we were given a little more time—” He stopped, and then added, strangely, “to grow.”

Khatchadourian’s earlier mention of a July 18 deadline is quite interesting, given the response from WikiLeaks to a Guccifer 2.0 email, promising to publish that week, on the 18th.

Khatchadourian also describes WikiLeaks as doing significant work to verify the emails — more than they could have done in the time between July 14 and July 22.

> Once they were in Assange's hands, his overriding concern was to insure that they were genuine. "We had quite some difficulties to overcome, in terms of the technical aspects, and making sure we were comfortable with the forensics," he recalled. As an Australian, he had only a vague grasp of the way the D.N.C. operated, which made deciphering the political significance of the e-mails difficult. "It's like looking at a very complex Hieronymus Bosch painting from a distance," he told me. "You have to get close and interact with it, then you start to get a feel." Often, a first encounter with a WikiLeaks database submission can be overwhelming—as one former staffer told me, "My heart sinks a bit."
>
> To work on the material, Assange had to coördinate with operatives outside the building, and avoid surveillance inside it. "I have a lot of security issues in the Embassy," he told me. "It's not like you can be comfortable with your source material and read it." He would not tell me how many people worked on the project, except that the number was small. "We're all secret squirrels now," he said.

All this raises questions about how much verification WikiLeaks did, and if instead this was a tale told to Khatchadourian, not to mention why they had confidence publishing them would not blow up on them.

Now, I have suggested that one possible second source of the emails — or at least one alternate explanation that Russia and WikiLeaks might claim that could provide GRU some plausible

deniability — would be via the contents of email boxes stolen using passwords released just before the DNC hack from Yevgeniy Nikulin's past hacks of Linked-In and MySpace. Nikulin has utterly stalled his prosecution until February by refusing not only to cooperate with his defense (though he has had repeated contacts from Russian diplomatic officials), but also with a competency evaluation. So we won't learn anything (and Nikulin won't be coerced to cooperate) anytime soon as a result of his extradition to the US.

But, as part of an effort to track changes to WikiLeaks' website and the DNC emails, Emma Best identified what at first appeared to be a change in one email but ultimately just revealed that the cache includes both the sent and received copies of some emails.

> After pointing this out on Twitter and listing the 36 known instances, one user checked a copy of the DNC emails they had retrieved months before. They found what appeared to be a modification to the email — a missing piece of metadata that identified the internal IP address that sent the email. After several hours of searching and comparing five different caches of DNC emails, the difference was both confirmed and explained — WikiLeaks' copy of the DNC emails comes from several accounts, which resulted in some duplicates in their cache. The internal message ID for the duplicates would be the same, but differences in metadata would appear based on whether the email was being sent or received, and in the case of the former what device and client was sending the emails. Since the x-originating-ip metadata which seemed to appear and then disappear is added by the server when it's sent, it would naturally be missing from the sender's copy of the email. This addresses the most alarming question regarding the DNC

> emails, but does nothing to address the rest.

There are reasons to believe that this means the email in question comes from the Microsoft Exchange server and not from someone's own mailbox (Update: though I may be 100% wrong on this point). Which, if my speculation that WikiLeaks might invoke the Nikulin alternate theory, might still show Assange got the emails in one batch early on, but then published what he got via the delivery identified in the indictment *and didn't spend much time vetting that delivery*.

Meanwhile, it's crucial to note, as Khatchadourian does in his earlier piece, that emails Guccifer 2.0 claimed were DNC documents when he released them the day after the WaPo revealed the DNC had been hacked didn't come from the DNC; those that have been identified came, instead, from John Podesta. It wasn't until July 6 that the Guccifer 2.0 documents billed as DNC ones actually were.

> But then, on July 6th, just before Guccifer 2.0 complained that WikiLeaks was "playing for time," this pattern of behavior abruptly reversed itself. "I have a new bunch of docs from the DNC server for you," the persona wrote on WordPress. The files were utterly lacking in news value, and had no connection to one another—except that *every item* was an attachment in the D.N.C. e-mails that WikiLeaks had. The shift had the appearance of a threat. If Russian intelligence officers were inclined to indicate impatience, this was a way to do it.

The notion that the Guccifer 2.0 persona may have — in addition to discrediting the WaPo article and providing a quick cover for the Russian attribution of the hack — served to pressure Assange to keep to some kind of July 18

deadline raises more stakes on that detail from the GRU indictment, but also may relate to the kind of signaling we saw elsewhere.

Update: I should have laid out some of the logic behind emails we've got. First, WikiLeaks has claimed that all the emails they have come from the "accounts" of seven identified people.

> The leaks come from the accounts of seven key figures in the DNC: Communications Director Luis Miranda (10520 emails), National Finance Director Jordon Kaplan (3799 emails), Finance Chief of Staff Scott Comer (3095 emails), Finanace Director of Data & Strategic Initiatives Daniel Parrish (1742 emails), Finance Director Allen Zachary (1611 emails), Senior Advisor Andrew Wright (938 emails) and Northern California Finance Director Robert (Erik) Stowe (751 emails).

Khatchadourian says they actually come from ten accounts.

> The twenty thousand or so D.N.C. e-mails that WikiLeaks published were extracted from ten compromised e-mail accounts, and all but one of the people who used those accounts worked in just two departments: finance and strategic communications. (The single exception belonged to a researcher who worked extensively with communications.)

DNC automatically deleted emails after 30 days if they weren't specifically saved (which is where this exfiltration estimate came from, which was off from the Mueller date by a week). Emails that precede the 30 day window (so April 19 or 25) or that weren't part of one of the identified accounts may indicate another source.

*As I disclosed July, I provided information to the FBI on issues related to the Mueller investigation, so I'm going to include*

*disclosure statements on Mueller investigation posts from here on out. I will include the disclosure whether or not the stuff I shared with the FBI pertains to the subject of the post.*