INFORMATION IN AMENDED DNC LAWSUIT REVEALS THAT ROGER STONE IS AT SIGNIFICANTLY GREATER RISK FOR CFAA INDICTMENT

Back in November, I wrote a post considering whether Roger Stone could be charged in a CFAA conspiracy. I noted that the last hack noted in the GRU indictment may have post-dated communications Stone had with Guccifer 2.0, in which Stone scoffed at the analytical information released as part of the DCCC hack. I pointed to this passage from the GRU indictment, showing that the GRU hack of the DNC analytics hosted on an AWS server may have post-dated those conversations between Guccifer 2.0 and Stone.

I'm writing a response to the Wikileaks defense against the DNC lawsuit for its involvements in the 2016 election attack, and so have only now gotten around to reading the amended complaint against Stone and others that the DNC filed in the wake of the GRU indictment. And it reveals that the AWS hack was far worse than described in the GRU indictment — and it continued well after that Stone conversation with Guccifer 2.0.

None of this long passage is footnoted in the complaint. It has to be based on the DNC's own knowledge of the AWS hack.

> On September 20, 2016, CrowdStrike's monitoring service discovered that unauthorized users—later discovered to be GRU officers—had accessed the DNC's cloud-computing service. The cloud-computing service housed test

> applications related to the DNC’s analytics. The DNC’s analytics are its most important, valuable, and highly confidential tools. While the DNC did not detect unauthorized access to its voter file, access to these test applications could have provided the GRU with the ability to see how the DNC was evaluating and processing data critical to its principal goal of winning elections. Forensic analysis showed that the unauthorized users had stolen the contents of these virtual servers by making exact duplicates (“snapshots”) of them and moving those snapshots to other accounts they owned on the same service. The GRU stole multiple snapshots of these virtual servers between September 5, 2016 and September 22, 2016. The U.S. government later concluded that this cyberattack had been executed by the GRU as part of its broader campaign to damage to the Democratic party.
>
> In 2016, the DNC used Amazon Web Services (“AWS”), an Amazon-owned company that provides cloud computing space for businesses, as its “data warehouse” for storing and analyzing almost all of its data.
>
> To store and analyze the data, the DNC used a software program called Vertica, which was run on the AWS servers. Vertica is a Hewlett Packard program, which the DNC licensed. The data stored on Vertica included voter contact information, such as the names, addresses, phone numbers, and email addresses of voters, and notes from the DNC’s prior contacts with these voters. The DNC also stored “digital information” on AWS servers. “Digital information” included data about the DNC’s online engagement, such as DNC email lists, the number of times internet users click on DNC

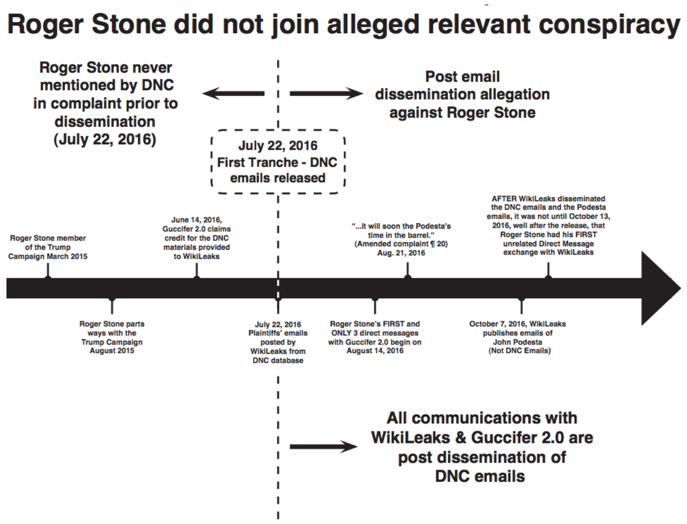
> advertisements (or “click rates”), and the number of times internet users click on links embedded in DNC emails (or “engagement rates”). The DNC also used AWS to store volunteer information—such as the list of people who have signed up for DNC-sponsored events and the number of people who attended those events.
>
> Vertica was used to both store DNC data and organize the data so that DNC computer engineers could access it. To use the Vertica data, DNC employees could not simply type a plain-English question into the database. Instead, DNC engineers needed to write lines of computer code that instructed Vertica to search for and display a data set. The computer engineers’ coded requests for data are called “queries.”
>
> When the DNC wanted to access and use the data it collected, the DNC described the information it wanted to retrieve, and DNC computer engineers designed and coded the appropriate “queries” to produce that data. These queries are secret, sensitive work product developed by the DNC for the purpose of retrieving specific cross-sections of information in order to develop political, financial, and voter engagement strategies and services. Many of these queries are used or intended for use in interstate commerce. The DNC derives value from these queries by virtue of their secrecy: if made public, these queries would reveal critical insights into the DNC’s political, financial, and voter engagement strategies. DNC computer engineers could save Vertica queries that they run repeatedly. In 2016, some of the DNC’s most frequently used Vertica queries—which revealed fundamental elements of the DNC’s political and financial strategies— were stored on the AWS servers.

> When the DNC wanted to analyze its data to look for helpful patterns or trends, the DNC used another piece of software called Tableau. Tableau is commercial software not developed by DNC engineers. Instead, the DNC purchased a license for the Tableau software, and ran the software against Vertica.
>
> Using Tableau, the DNC was able to develop graphs, maps, and other visual reports based on the data stored on Vertica. When the DNC wanted to visualize the data it collected, the DNC described the information it wanted to examine, and DNC computer engineers designed and coded the appropriate "Tableau queries" to produce that data in the form requested. These Tableau queries are secret, sensitive work product developed by the DNC for the purpose of transforming its raw data into useful visualizations. The DNC derives value from these queries by virtue of their secrecy: if made public, these queries would reveal critical insights into the DNC's political, financial, and voter engagement strategies and services. Many of these queries are used or intended for use in interstate commerce.
>
> DNC computer engineers could also save Tableau queries that they ran repeatedly. In 2016, some of the DNC's most frequently used Tableau queries—which revealed fundamental elements of the DNC's political and financial strategies—were stored on the AWS servers.
>
> The DNC's Vertica queries and Tableau Queries that allow DNC staff to analyze their data and measure their progress toward their strategic goals—collectively, the DNC's "analytics,"—are its most important,

> valuable, and highly confidential tools. Because these tools were so essential, the DNC would often test them before they were used broadly.
>
> The tests were conducted using “testing clusters”—designated portions of the AWS servers where the DNC tests new pieces of software, including new Tableau and Vertica Queries. To test a new query, a DNC engineer could use the query on a “synthetic” data set—mock-up data generated for the purpose of testing new software—or a small set of real data. For example, the DNC might test a Tableau query by applying the software to a set of information from a specific state or in a specific age range. Thus, the testing clusters housed sensitive, proprietary pieces of software under development. As described above, the DNC derives significant value from its proprietary software by virtue of its secrecy: if made public, it would reveal critical insights into the DNC’s political, financial, and voter engagement strategies and services, many of which are used or intended for use in interstate commerce.
>
> The DNC protected all of the data and code in its AWS servers by, among other things, restricting access to authorized users. To gain access to the AWS servers themselves, an authorized user had to take multiple steps. First, the authorized user would have to log onto a Virtual Private Network (VPN) using a unique username and password. Second, once the user entered a valid and password, the system would send a unique six-digit code (PIN) to the authorized user’s phone, and the user would have 30 seconds to type it into the computer system. This two-step process is commonly known as “two-factor authentication.”

> Authorized users would also employ a two-factor authentication system to access Tableau visualizations. First, they would log into a Google account with a unique username and password, and then they would enter a pin sent to their cell phones.
>
> Finally, the DNC’s AWS servers were protected with firewalls and cybersecurity best practices, including: (a) limiting the IP addresses and ports with which users could access servers; (b) auditing user account activities; and (c) monitoring authentication and access attempts.
>
> On September 20, 2016, CrowdStrike’s monitoring service discovered that unauthorized users had breached DNC AWS servers that contained testing clusters. Further forensic analysis showed that the unauthorized users had stolen the contents of these DNC AWS servers by taking snapshots of the virtual servers, and had moved those replicas to other AWS accounts they controlled. **The GRU stole multiple snapshots of these servers between September 5, 2016 and September 22, 2016**. The U.S. later concluded that this cyberattack had been executed by the GRU as part of its broader campaign to damage to the Democratic party. The GRU could have derived significant economic value from the theft of the DNC’s data by, among other possibilities, selling the data to the highest bidder.
>
> The software would also be usable as executable code by DNC opponents, who could attempt to re-create DNC data visualizations or derive DNC strategy decisions by analyzing the tools the DNC uses to analyze its data. [my emphasis]

In other words, at least one of those snapshots was stolen after Stone suggested he would like better analytics data than what GRU had publicly released via HelloFL. So he can no longer say that his communications with Guccifer 2.0 preceded all the hacking. Which the nifty timeline Stone's attorney submitted in conjunction with his motion to dismiss doesn't account for at all.


Roger Stone did not join alleged relevant conspiracy
Roger Stone never mentioned by DNC in complaint prior to dissemination (July 22, 2016)
Post email dissemination allegation against Roger Stone
July 22, 2016 First Tranche - DNC emails released
Roger Stone member of the Trump Campaign March 2015
June 14, 2016, Guccifer 2.0 claims credit for the DNC materials provided to WikiLeaks
"...it will soon the Podesta's time in the barrel." (Amended complaint ¶ 20) Aug. 21, 2016
AFTER WikiLeaks disseminated the DNC emails and the Podesta emails, it was not until October 13, 2016, well after the release, that Roger Stone had his FIRST unrelated Direct Message exchange with WikiLeaks
Roger Stone parts ways with the Trump Campaign August 2015
July 22, 2016 Plaintiffs' emails posted by WikiLeaks from DNC database
Roger Stone's FIRST and ONLY 3 direct messages with Guccifer 2.0 begin on August 14, 2016
October 7, 2016, WikiLeaks publishes emails of John Podesta (Not DNC Emails)
All communications with WikiLeaks & Guccifer 2.0 are post dissemination of DNC emails

Given Stone's history of non-denial denials for crimes he commits, I'd say this stunted timeline doesn't help him much.

Here's Stone's motion to dismiss. As with his nifty timeline, he does not address — at all — the communications between him and Guccifer 2.0 regarding analytics. It does, however, include this tagline.

> He is the First Amendment running, not walking; but his conduct cannot be adjudged a civil wrong.

Past history says Stone's rat-fuckery tends to be easily found in his swiss cheese denials, and I'd say this is one example.

Note that, a week after DNC submitted its amended complaint on October 4, WikiLeaks released a proprietary AWS document showing the locations of all AWS's servers around the world — something that is not all that newsworthy, but something that would be incredibly valuable for those trying to compromise AWS. That was one of its only releases since the crackdown on Assange has intensified.

As I disclosed in 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.