THE MOSCOW PROJECT

Breaking Down the Mueller Report

The Stolen DNC Data That Wasn't Released

(Mueller Report Volume 1, p 41-51; *U.S. v. Viktor Netyksho, et al*)

Toplines

- **Russian military-intelligence hackers stole confidential political data from the Democratic National Committee that they did not release through WikiLeaks.**
- **WikiLeaks only released emails. It did not release the DNC analytics and campaign plans.**
- **Russian intelligence stole data from the DNC as late as September 20, 2016.**
- **What did they do with the valuable information they stole but did not release**?

Key Facts from the Report

- Russian hackers from the GRU, the Kremlin's military-intelligence directorate, conducted multiple rounds of hacking that resulted in the theft of sensitive data and emails from the Democratic National Committee and Clinton campaign chairman John Podesta.
- They gained access to the servers of the Democratic National Committee as early as the summer of 2015; John Podesta's emails were compromised in March 2016.
- Russian intelligence worked with a cutout, WikiLeaks, to disseminate the stolen information.
- Metadata on files found on the computers of Russian hackers suggests that they had completed their transfer of emails stolen from John Podesta's inbox to WikiLeaks in mid-September 2016.
- On September 20, 2016, after Russia transferred files to WikiLeaks, members of the same Russian military-intelligence unit "also successfully gained access to DNC computers hosted on a third-party cloud-computing service. These computers contained test applications related to the DNC's analytics," which the hackers copied and stole.
- Analytics are some of the most critical assets a campaign owns, often valued at hundreds of thousands of dollars.
- WikiLeaks never released any of the data it stole in the final attack, and there is no discussion in either the indictment or the Mueller report of what the GRU did with the data.
- The indictment and the report also indicate additional hacks and transfers of information that never became public, including the transfer of stolen materials to an undisclosed congressional candidate.

Overview

According to *U.S. v. Viktor Netyksho, et al*, on September 20, 2016, GRU hackers carried out an attack that resulted in them gaining access to "DNC computers hosted on a third-party cloud-computing service. These computers contained test applications related to the DNC's analytics." However, neither the indictment nor the Mueller report appears to say what the Kremlin ultimately did with the data stolen in that attack.

This type of stolen data, as described in the indictment, appears to be information that would likely be more useful if kept private than if disseminated. Stolen analytical data could be useful not only as additional information on targets that Democrats hoped to reach, but also as a means of better anticipating, and therefore better countering their campaigns.

The Trump campaign has denied any coordination with the GRU hackers. However, on at least one occasion GRU hackers sent informal Trump advisor Roger Stone stolen information on the Democratic Party's turnout models and asked for his feedback, which Stone gave (Volume 1, p. 44).

What makes the September attack particularly interesting is that it took place significantly after the email hack and release, which has a clear dissemination strategy. The GRU's Cozy Bear and Fancy Bear units hacked into the DNC's servers in the summer of 2015 and April 2016, respectively, and released the emails in July 2016. Meanwhile, the successful penetration of Podesta's inbox occurred on March 16, 2016. According to the Mueller report, metadata on files published by WikiLeaks suggest that the hackers transferred the data to WikiLeaks by September 19, 2016 (Volume 1, p. 47). In other words, by the time the GRU carried out the September hack, they were already effectively finished with the hacking operations that resulted in the release of emails during the campaign.

The report also suggests that there was additional information that the hackers obtained but did not release. For example, Russian hackers appear to have breached the Republican National Committee as well as the DNC prior to the 2016 election. However, while WikiLeaks released more than 20,000 emails and other documents from the DNC, and an additional 30,000 from Podesta's inbox, the hackers only released "approximately 300 emails from a variety of GOP members, PACs, campaigns, state parties, and businesses," and did so not through WikiLeaks but through DC Leaks, a website the hackers themselves operated (Volume 1, p. 41-42). This suggests that the hackers either didn't steal as many emails from the RNC or, more likely given their and WikiLeaks's shared goal of preventing a Clinton presidency and electing Donald Trump, that they simply did not release all of what they obtained.

Additionally, the report says that, "on August 15, 2016, the Guccifer 2.0 persona sent a candidate for the U.S. Congress documents related to the candidate's opponent" (Volume 1, p. 43). It remains unknown who the congressional candidate was, and what, if any, of the stolen data ended up being used during the election.

Key Questions for the Investigation

- What political data did the Russian government steal that it did not release?
- Did they share any of that data with the Trump campaign, or any other campaign?
- Were the 300 RNC emails published through DC Leaks the entirety of what was stolen from the RNC, or did the hackers decline to publish information?
- Does the Kremlin still possess information obtained in 2016 that it could use to disrupt future American elections? If so, are there precautions that the government can take to blunt the potential impact?
- Who was the congressional candidate who received stolen data from Guccifer 2.0?
    - Were they aware that they were communicating with operatives of a hostile foreign government engaged in an active attack on American democracy?
    - What data did they receive, and was it otherwise included in the files published through WikiLeaks?
    - Is that candidate now a Member of Congress?